

CONTRATO CERRADO RELATIVO AL **"SERVICIO DE SEGURIDAD PERIMETRAL PARA LA RED LOCAL DE OFICINAS NACIONALES"**, QUE CELEBRAN, POR UNA PARTE, EL **COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA**, REPRESENTADO POR LA **MTRA. KARINA SALAZAR HERNÁNDEZ,** EN SU CARÁCTER DE **DIRECTORA DE INFRAESTRUCTURA Y ADQUISICIONES,** EN ADELANTE **"EL CONALEP"** Y, POR LA OTRA **SCITUM, S.A. DE C.V.**, EN LO SUCESIVO **"EL PRESTADOR DE SERVICIOS"**, REPRESENTADO POR EL **C. EDGAR HERNÁNDEZ SOTO**, EN SU CALIDAD DE APODERADO LEGAL, A QUIENES DE MANERA CONJUNTA SE LES DENOMINARÁ **"LAS PARTES"**, AL TENOR DE LAS, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

DECLARACIONES

I. "EL CONALEP" declara que:

I.1. Es un organismo público descentralizado del Estado, con personalidad jurídica y patrimonio propios, creado por Decreto presidencial del 27 de diciembre de 1978, publicado en el Diario Oficial de la Federación el 29 del mismo mes y año, cuyo objeto es la impartición de educación profesional técnica, con la finalidad de satisfacer la demanda de personal técnico calificado para el sistema productivo del país, así como educación de bachillerato dentro del tipo medio superior, de conformidad con los diversos que reforman dicho Decreto que creó a **"EL CONALEP"** de fecha 22 de noviembre de 1993, publicado en el Diario Oficial de la Federación el 08 de diciembre de 1993, y de fecha 29 de julio de 2011, publicado en el Oficial de la Federación, el 04 de agosto de 2011.

I.2. Conforme a lo dispuesto por el artículo 39 fracción XII del Estatuto Orgánico del Colegio Nacional de Educación Profesional Técnica, numeral 1.8.1, función 13, del Manual General de Organización del Colegio Nacional de Educación Profesional Técnica, en el que se regulan las atribuciones de la **MTRA. KARINA SALAZAR HERNÁNDEZ**, en su carácter de **DIRECTORA DE INFRAESTRUCTURA Y ADQUISICIONES**, con R.F.C. SAHK810729TH1, designada a través de la Junta Directiva del Colegio Nacional de Educación Profesional Técnica en Primera Sesión Extraordinaria de fecha 28 de enero del 2025; nombramiento protocolizado de fecha 1 de febrero del 2025, signado por el **MTRO. RODRIGO ALEJANDRO ROJAS NAVARRETE**, **DIRECTOR GENERAL del CONALEP**; suscribe el presente instrumento de conformidad con lo establecido en el numeral 1.8.1., función 13, del Acuerdo DG-DCAJ-05/2021, por el que se actualiza el Manual General de Organización del Colegio Nacional de Educación Profesional Técnica, quien podrá ser sustituida en cualquier momento, bastando para tales efectos un comunicado por escrito, firmado por el servidor público facultado para ello, informando a **"EL PRESTADOR DE SERVICIOS"** para los efectos del presente contrato.

I.3. De conformidad con lo dispuesto en el numeral 1.2 del Manual General de Organización del Colegio Nacional de Educación Profesional Técnica, numeral 13 de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Colegio Nacional de Educación Profesional Técnica suscribe el presente instrumento el **MTRO. JULIAN JAVIER ROBLES RIVAS**, en su carácter de **DIRECTOR CORPORATIVO DE TECNOLOGÍAS APLICADAS**, con **R.F.C. RORJ7312163W3**, responsable para administrar y verificar el cumplimiento de las obligaciones que deriven del objeto del presente contrato, en adelante **"ADMINISTRADOR DEL CONTRATO"** quien podrá ser sustituido en



cualquier momento en su cargo o funciones, bastando para tales efectos un comunicado por escrito y firmado por el servidor público facultado para ello, dirigido al representante de **"EL PRESTADOR DE SERVICIOS"** para los efectos del presente contrato, encargado del cumplimiento de las obligaciones contraídas en el presente instrumento jurídico.

I.4. La adjudicación del presente contrato se llevó a cabo mediante procedimiento de Invitación a Cuando Menos Tres Personas de Carácter Nacional, número **IA-11-L5X-011L5X001-N-25-2025**, realizado al amparo de lo establecido en los artículos 134 de la Constitución Política de los Estados Unidos Mexicanos, 35 fracción II y VI, 47, 48, 49, 53 y 54 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Publico; y 51 de su Reglamento, así como en las demás disposiciones aplicables.

I.5. Cuenta con recursos suficientes y con autorización para ejercerlos en el cumplimiento de sus obligaciones derivadas del presente contrato, como se desprende de la suficiencia presupuestal número 06695, partida presupuestal 33301, de fecha 17 de junio de 2025, autorizada por la Titular de la Dirección de Administración Financiera de **"EL CONALEP"**.

I.6. Se encuentra inscrito en el Registro Federal de Contribuyentes con el alfanumérico **CNE781229BK4**.

I.7. Tiene establecido su domicilio en calle 16 de septiembre No. 147 norte, Col. Lázaro Cárdenas, Metepec, Estado de México, Código Postal 52148 mismo que señala para los fines y efectos legales del presente contrato.

II. "EL PRESTADOR DE SERVICIOS", por conducto de su apoderado legal declara que:

II.I Es una persona moral legalmente constituida mediante Escritura Pública 122,788 de fecha 7 de diciembre de 2000, ante la fe del Licenciado Salvador Godínez Viera, Titular de la Notaria Púbica número 42 del Distrito Federal hoy Ciudad de México, cuyo testimonio se encuentra debidamente registrado en el Registro Público de Comercio del Distrito Federal hoy día Ciudad de México, con el folio mercantil número 269860 de fecha 10 de enero de 2001; y sus diversas modificaciones a sus estatus, mediate escritura pública número 123,330 de fecha 1 de marzo de 2001 otorgada ante la Fe del Notario Público Licenciado Salvador Godínez Viera, Titular de la Notaria Púbica número 42 del Distrito Federal hoy Ciudad de México, cuyo testimonio se encuentra debidamente registrado en el Registro Público de Comercio del Distrito Federal hoy día Ciudad de México, con el folio mercantil número 269860 de fecha 27 de marzo de 2001; mediante escritura pública numero 88,163 de fecha 21 de diciembre de 2006, otorgada ante la fe del Notario Público Licenciado Carlos de Pablo Serna, Titular de la Notaria Púbica número 137 del Distrito Federal hoy Ciudad de México, en la cual se formaliza la reforma total a los estatutos sociales e inscrita en el folio mercantil 269860 el 17 de enero de 2007, mediante escritura pública número 90926 de fecha 31 de octubre de 2007, otorgada ante la fe del Notario Público Licenciado Carlos de Pablo Serna, Titular de la Notaria Púbica número 137 del Distrito Federal hoy Ciudad de México, inscrita en el folio mercantil 269860 de fecha 13 de noviembre de 2007, conta modificación al objeto social.



II.2 El **C. Edgar Hernández Soto**, en su carácter de apoderado legal, cuenta con poder amplio suficiente para suscribir el presente contrato y obligar a su representada en los términos del mismo, lo cual acredita mediante Instrumento Libro 4432, Escritura Número 177,055, de fecha 26 de agosto de 2020, otorgada ante la fe del Notario Público Número 54 de la Ciudad de México, Lic. Homero Díaz Rodríguez, mismo que bajo protesta de decir verdad manifiesta que, no le han sido limitado ni revocado en forma alguna.

II.3 El **C. Edgar Hernández Soto**, se identifica con Credencial para Votar con fotografía, expedida por el Instituto Nacional Electoral.

II.4 Conforme a su objeto social se dedica, entre otros, a la prestación de toda clase de servicios permitidos por la legislación aplicable, especialmente la prestación de los servicios de consultoría, desarrollo, instalación y soporte de sistemas de comunicación y programas de cómputo, la administración, diseño e implantación de sistemas, equipos, centros y programas de cómputo, y en general la prestación de servicios de informática en todas sus variantes a personas físicas y morales.

II.5 Reúne las condiciones técnicas, jurídicas y económicas, y cuenta con la organización y elementos necesarios para el cumplimiento del presente instrumento.

II.6 Se encuentra inscrito en el Registro Federal de Contribuyentes expedido por la Secretaría de Hacienda y Crédito Público con el alfanumérico **SCI001208M74**.

II.7 Tiene capacidad jurídica para contratar y reúne las condiciones legales, técnicas y económicas necesarias para obligarse a la entrega de los servicios, objeto de este contrato.

II.8 Acredita el cumplimiento de sus obligaciones fiscales en términos de lo dispuesto en el artículo 32-D del Código Fiscal de la Federación vigente, incluyendo las de Aportaciones Patronales y Entero de Descuentos, ante el Instituto del Fondo Nacional de la Vivienda para los Trabajadores y las de Seguridad Social ante el Instituto Mexicano del Seguro Social, conforme a las Opiniones de Cumplimiento de Obligaciones Fiscales emitidas por el SAT, INFONAVIT e IMSS, respectivamente.

II.9 Para los efectos derivados de este instrumento señala como su domicilio fiscal y legal el ubicado en la Av. Periférico Sur, número 3190 piso 1, Col. Jardines del Pedregal, Álvaro Obregón, C.P. 01900, Ciudad de México.

II.10 Bajo protesta de decir verdad, manifiesta que a la fecha no se encuentra inhabilitado por autoridad, dependencia o entidad alguna para formular propuestas o para la celebración del presente instrumento, en virtud de no encontrarse en los supuestos previstos en el artículo 71 y 90 de la LAASSP.





II.11 Conoce el contenido de la LAASSP, y su Reglamento, la publicación, contenido y alcance de las Políticas, Bases y Lineamientos en materia de Adquisiciones, Arrendamientos y Servicios del Colegio Nacional de Educación Profesional Técnica; asimismo reconoce la facultad de la Dirección de Infraestructura y Adquisiciones para la aplicación de penas convencionales.

III. De "LAS PARTES":

III.1 Que es su voluntad celebrar el presente contrato y sujetarse a sus términos y condiciones, por lo que de común acuerdo se obligan de conformidad con las siguientes:

CLÁUSULAS

PRIMERA. OBJETO DEL CONTRATO.
"EL PRESTADOR DE SERVICIOS" acepta y se obliga a proporcionar a **"EL CONALEP"** el **"SERVICIO DE SEGURIDAD PERIMETRAL PARA LA RED LOCAL DE OFICINAS NACIONALES"**, en los términos y condiciones establecidos en el fallo, así como en los Anexos Técnico y Económico **(ANEXO A Y ANEXO B)** respectivamente, que forman parte integrante del presente instrumento.

SEGUNDA. MONTO DEL CONTRATO.
"EL CONALEP" pagará a **"EL PRESTADOR DE SERVICIOS"** como contraprestación por el servicio objeto de este contrato, un monto de **$110,125.26 (CIENTO DIEZ MIL CIENTO VEINTICINCO PESOS 26/100 M.N.)** sin IVA incluido, considerando los precios unitarios de su oferta económica.

Los precios unitarios del presente contrato, expresados en moneda nacional son los establecidos conforme al ANEXO B Anexo Económico.

El precio unitario es considerado fijo y en moneda nacional PESO MEXICANO hasta que concluya la relación contractual que se formaliza, incluyendo todos los conceptos y costos involucrados en la prestación del "SERVICIO DE SEGURIDAD PERIMETRAL PARA LA RED LOCAL DE OFICINAS NACIONALES", por lo que **"EL PRESTADOR DE SERVICIOS"**, no podrá agregar ningún costo extra y los precios serán inalterables durante la vigencia del presente contrato

TERCERA. ANTICIPO.
Para el presente contrato **"EL CONALEP"** no otorgará anticipo a **"EL PRESTADOR DE SERVICIOS"**.

CUARTA. FORMA Y LUGAR DE PAGO.
La forma de pago será en moneda nacional (pesos mexicanos), a mes vencido por partida completa una vez realizado el servicio a entera satisfacción de "**EL CONALEP"**, previa revisión y validación correspondiente por parte del titular de la Dirección Corporativa de Tecnologías Aplicadas, en un plazo no mayor de 17 días hábiles posteriores a la



presentación del CFDI "Comprobante Fiscal Digital a través de internet" (anteriormente factura) correspondiente la cual deberá contener todos los requisitos fiscales vigentes, de conformidad en lo establecido en el artículo 73 de la LAASSP, siempre y cuando reúna todos los requisitos establecidos por el Código Fiscal de la Federación y esté debidamente requisitada.

La factura deberá contener el desglose del consumo de cada uno de los conceptos considerados para el método de evaluación incluido en la descripción del servicio, cuya multiplicación por el precio unitario ofertado dará como resultado el monto total de la factura. La que deberá ir acompañada de los formatos de toma de lectura y de las hojas de contadores de los equipos, acompañado del visto bueno de por parte del Administrador del Contrato, o quien este designe.

El pago por la prestación del servicio comenzará a correr a partir del siguiente día hábil de que el servicio quede debidamente configurado y en operación, a entera satisfacción de **"EL CONALEP"**, previa revisión y validación del Administrador del Contrato.

De acuerdo con las disposiciones fiscales, "**EL PRESTADOR DE SERVICIOS"** deberá enviar el archivo PDF y .XML de cada factura, dentro de los primeros 5 días hábiles posteriores al mes en el que se proporcionó el servicio, al correo electrónico despinosa@conalep.edu.mx; mamarquez@conalep.edu.mx.

El CFDI o factura electrónica se deberá presentar desglosando el impuesto cuando aplique.

"EL PRESTADOR DE SERVICIOS" manifiesta su conformidad que, hasta en tanto no se cumpla con la verificación, supervisión y aceptación de la prestación de los servicios, no se tendrán como recibidos o aceptados por el Administrador del presente contrato.

Para efectos de trámite de pago, **"EL PRESTADOR DE SERVICIOS"** deberá ser titular de una cuenta bancaria, en la que se efectuará la transferencia electrónica de pago, respecto de la cual deberá proporcionar toda la información y documentación que le sea requerida por **"EL CONALEP"**, para efectos del pago.

"EL PRESTADOR DE SERVICIOS", deberá presentar la información y documentación que **"EL CONALEP"** le solicite para el trámite de pago, atendiendo a las disposiciones legales e internas de **"EL CONALEP".**

El pago de la prestación de los servicios recibidos quedará condicionado proporcionalmente al pago que **"EL PRESTADOR DE SERVICIOS"**, deba efectuar por concepto de penas convencionales y, en su caso, deductivas.

Para el caso que se presenten pagos en exceso, se estará a lo dispuesto por el artículo 73, párrafo tercero, de la **"LAASSP".**

QUINTA. LUGAR, PLAZOS Y CONDICIONES DE LA PRESTACIÓN DE LOS SERVICIOS.

Lugar de ejecución del servicio: Se realizará en las instalaciones de Oficinas Nacionales del CONALEP, en calle 16 de septiembre No. 147 Col. Lázaro Cárdenas, Metepec, Estado de México, C.P. 52148, con base a lo establecido en el Anexo A. "Descripción técnica del arrendamiento".



Tiempo de ejecución del servicio:
El periodo del servicio deberá ser a partir del día siguiente a la notificación de fallo y hasta el 31 de diciembre de 2025.

"EL PRESTADOR DE SERVICIOS", se obliga a observar las condiciones establecidos en el Anexo A. "Descripción técnica del arrendamiento", adjunto a este instrumento.

SEXTA. VIGENCIA
"LAS PARTES" convienen en que la vigencia del presente contrato será a partir **12 de julio de 2025 al 31 de diciembre de 2025.**

SÉPTIMA. MODIFICACIONES DEL CONTRATO.
"LAS PARTES" están de acuerdo que **"EL CONALEP"** por razones fundadas podrá ampliar el monto o la cantidad del servicio, de conformidad con el artículo 74 de la LAASSP, siempre y cuando las modificaciones no rebasen en su conjunto el 20% (veinte por ciento) de los establecidos originalmente, el precio unitario sea igual al originalmente pactado y el contrato esté vigente. La modificación se formalizará mediante la celebración de un Convenio Modificatorio.

"EL CONALEP", podrá ampliar la vigencia del presente instrumento, siempre y cuando, no implique incremento del monto contratado o de la cantidad del servicio, siendo necesario que se obtenga el previo consentimiento **de "EL PRESTADOR DE SERVICIOS"**.

De presentarse caso fortuito o fuerza mayor, o por causas atribuibles a **"EL CONALEP"**, se podrá modificar el plazo del presente instrumento jurídico, debiendo acreditar dichos supuestos con las constancias respectivas. La modificación del plazo por caso fortuito o fuerza mayor podrá ser solicitada por cualquiera de **"LAS PARTES"**

En los supuestos previstos en los dos párrafos anteriores, no procederá la aplicación de penas convencionales por atraso.

Cualquier modificación al presente contrato deberá formalizarse por escrito, y deberá suscribirse por el servidor público de **"EL CONALEP"** facultado para ello, o quien lo sustituya, para lo cual **"EL PRESTADOR DE SERVICIOS"** realizará el ajuste respectivo de la garantía de cumplimiento, en términos del artículo 91, último párrafo del Reglamento de la LAASSP, salvo que por disposición legal se encuentre exceptuado de presentar garantía de cumplimiento.

"EL CONALEP" se abstendrá de hacer modificaciones que se refieran a precios, anticipos, pagos progresivos, especificaciones y, en general, cualquier cambio que implique otorgar condiciones más ventajosas a un proveedor comparadas con las establecidas originalmente.

OCTAVA. GARANTÍA(S)

A) CUMPLIMIENTO DEL CONTRATO.





Conforme a los artículos 69, fracción II, 70, fracción I (dependencias) o II (entidades), de la LAASSP; 85, fracción III, 103 de su Reglamento; y 166 de la Ley de Instituciones de Seguros y de Fianzas, **"EL PRESTADOR DE SERVICIOS"**, se obliga a constituir una garantía la cual podrá ser, indivisible por el cumplimiento fiel y exacto de todas las obligaciones derivadas de este contrato; mediante fianza expedida por compañía afianzadora mexicana autorizada por la Comisión Nacional de Seguros y de Fianzas, a favor de **"EL CONALEP"**, por un importe equivalente al 10.0% del monto total del contrato, sin incluir el IVA.

Dicha fianza deberá ser entregada a **"EL CONALEP"**, a más tardar dentro de los 10 días naturales posteriores a la firma del presente contrato.

Si las disposiciones jurídicas aplicables lo permiten, la entrega de la garantía de cumplimiento se podrá realizar de manera electrónica.

En caso de que **"EL PRESTADOR DE SERVICIOS"** incumpla con la entrega de la garantía en el plazo establecido, **"EL CONALEP"** podrá rescindir el contrato y dará vista al Órgano Interno de Control para que proceda en el ámbito de sus facultades.

La garantía de cumplimiento no será considerada como una limitante de responsabilidad de **"EL PRESTADOR DE SERVICIOS"**, derivada de sus obligaciones y garantías estipuladas en el presente instrumento jurídico, y no impedirá que **"EL CONALEP"** reclame la indemnización por cualquier incumplimiento que pueda exceder el valor de la garantía de cumplimiento.

En caso de incremento al monto del presente instrumento jurídico o modificación al plazo, "**EL PRESTADOR DE SERVICIOS"** se obliga a entregar a **"EL CONALEP"**, dentro de los 10 (diez días) naturales siguientes a la formalización del mismo, de conformidad con el último párrafo del artículo 91, del Reglamento de la "LAASSP", los documentos modificatorios o endosos correspondientes, debiendo contener en el documento la estipulación de que se otorga de manera conjunta, solidaria e inseparable de la garantía otorgada inicialmente.

Cuando la contratación abarque más de un ejercicio fiscal, la garantía de cumplimiento del contrato podrá ser por el porcentaje que corresponda del monto total por erogar en el ejercicio fiscal de que se trate, y deberá ser renovada por **"EL PRESTADOR DE SERVICIOS",** cada ejercicio fiscal por el monto que se ejercerá en el mismo, la cual deberá presentarse a **"EL CONALEP"** a más tardar dentro de los primeros diez días naturales del ejercicio fiscal que corresponda.

Una vez cumplidas las obligaciones a satisfacción, el servidor público facultado por **"EL CONALEP"** procederá inmediatamente a extender la constancia de cumplimiento de las obligaciones contractuales y dará inicio a los trámites para la cancelación de la garantía cumplimiento del contrato, lo que comunicará a **"EL PRESTADOR DE SERVICIOS".**

CARTA DE VICIOS OCULTOS.

"EL PRESTADOR DE SERVICIOS", se obliga con **"EL CONALEP"** a entregar al inicio del servicio, una garantía por la calidad de este, por un periodo de 6 meses, la cual se constituirá por la carta de vicios ocultos, pudiendo ser mediante la póliza de garantía, conforme a los artículos 69, fracción II, 70, fracción I (dependencias) o II (entidades), de la LAASSP; y 103 de su Reglamento.





NOVENA. OBLIGACIONES DE "EL PRESTADOR DE SERVICIOS".

A. Prestar los servicios en las fechas o plazos y lugares establecidos conforme a lo pactado en el presente contrato y anexos respectivos.
B. Cumplir con las especificaciones técnicas, de calidad y demás condiciones establecidas en el presente contrato y sus respectivos anexos.
C. Asumir la responsabilidad de cualquier daño que llegue a ocasionar a **"EL CONALEP"** o a terceros con motivo de la ejecución y cumplimiento del presente contrato.
D. Proporcionar la información que le sea requerida por la Secretaría Anticorrupción y Buen Gobierno y el Órgano Interno de Control, de conformidad con el artículo 107 del Reglamento de la LAASSP.

DÉCIMA. OBLIGACIONES DE "EL CONALEP"

1. Otorgar las facilidades necesarias, a efecto de que **"EL PRESTADOR DE SERVICIOS"** lleve a cabo en los términos convenidos la prestación de los servicios objeto del contrato.
2. Realizar el pago correspondiente en tiempo y forma.
3. Extender a **"EL PRESTADOR DE SERVICIOS"**, por conducto del Servidor Público facultado, la constancia de cumplimiento de obligaciones contractuales inmediatamente que se cumplan éstas a satisfacción expresa de dicho servidor público para que se dé trámite a la cancelación de la garantía de cumplimiento del presente contrato.

DÉCIMA PRIMERA. ADMINISTRACIÓN, VERIFICACIÓN, SUPERVISIÓN Y ACEPTACIÓN DE LOS SERVICIOS.

El Administrador del presente contrato el **MTRO. JULIAN JAVIER ROBLES RIVAS**, en su carácter de **DIRECTOR CORPORATIVO DE TECNOLOGÍAS APLICADAS**, con **R.F.C. RORJ7312163W3**, es el responsable de administrar y verificar que el servicio cumpla con las especificaciones solicitadas en el Anexo No. 1 "Descripción Técnica del Servicio" y demás condiciones establecidas en el contrato, siendo el único facultado para solicitar a la Titular de la Dirección de Infraestructura y Adquisiciones las penalizaciones, deductivas y liberaciones de pago que correspondan, no obstante, podrá designar a un supervisor de contrato mediante oficio.

"EL CONALEP", a través del administrador del contrato, rechazará los servicios, que no cumplan las especificaciones establecidas en este contrato y en sus Anexos, obligándose **"EL PRESTADOR DE SERVICIOS"** en este supuesto a realizarlos nuevamente bajo su responsabilidad y sin costo adicional para **"EL CONALEP"**, sin perjuicio de la aplicación de las penas convencionales o deducciones al cobro correspondientes.

"EL CONALEP", a través del administrador del contrato, podrá aceptar los servicios que incumplan de manera parcial o deficiente las especificaciones establecidas en este contrato y en los anexos respectivos, sin perjuicio de la aplicación de las deducciones al pago que procedan, y reposición del servicio, cuando la naturaleza propia de éstos lo permita.





DÉCIMA SEGUNDA. PENAS CONVENCIONALES.

De conformidad con el artículo 75 de la LAASSP, 95 y 96 de su Reglamento, "**EL CONALEP"** aplicará con motivo de incumplimiento en la prestación del servicio, las penas convencionales de acuerdo con lo siguiente:

En el arrendamiento:

El prestador del servicio se obliga a pagar al CONALEP una pena convencional del 2% sobre el monto mensual del pago previsto para los equipos no entregados, instalados, configurados y puestos en marcha, conforme a lo descrito en el apartado "ENTREGABLES" del Anexo 1. "Descripción técnica del arrendamiento" por cada día natural de atraso para la respectiva contratación.

La misma pena se aplicará en el caso de no proporcionar la mesa de ayuda en el plazo establecido en el apartado "Mesa de ayuda", y no presentar lo señalado en el apartado "Entregables" en el plazo establecido; por cada día natural de atraso.

El total de la pena convencional no podrá exceder el montó de la garantía de cumplimiento sin considerar el impuesto al valor agregado (I.V.A.), de conformidad con lo establecido en el artículo 75 y 76 de la LAASSP.

En los entregables:

El prestador del servicio se obliga a pagar al CONALEP una pena convencional por no presentar los entregables mensuales en los plazos establecidos en el apartado "ENTREGABLES" del Anexo 1. "Descripción técnica del arrendamiento". Dicha pena será del 2% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso. El total de la pena convencional no podrá exceder el monto de la garantía de cumplimiento sin considerar el impuesto al valor agregado (I.V.A.), de conformidad con lo establecido en el artículo 75 y 76 de la LAASSP y 96 del RLAASSP.

- **El pago de las penas será a través de notas de crédito sin IVA, aplicables en los CFDI's mensuales durante la vigencia del Contrato, o en su caso, deducidas del pago mensual correspondiente.**

2.8.2 Deductivas

Se aplicará una deductiva al oferente por el cumplimiento parcial o deficiente en el arrendamiento. Dicha deductiva será del 2% sobre el monto de la facturación del mes inmediato anterior correspondiente al equipo que no sea sustituido o reparado en los términos y plazos establecidos en el presente anexo por cada día natural de atraso. Lo anterior, de conformidad en lo establecido en el artículo 75 y 76 de la LAASSP y 97 del RLAASSP.

Igual porcentaje, se aplicará como deductiva en los casos que el oferente suspenda el arrendamiento por cualquier causa injustificada, esto es fuera de los casos de fuerza mayor o caso fortuito debidamente acreditado y documentado en términos de la normatividad aplicable, por cada día natural que suspenda el arrendamiento, independientemente de que no se pagaría arrendamiento por el tiempo que dure la suspensión.

Adicional a lo anterior, se aplicarán deductivas por cada día natural de incumplimiento en los tiempos de atención y solución de fallas o la petición de la reasignación o reubicación de equipos, así como en los niveles de atención señalados en el apartado "Niveles de atención".





En caso de que los conceptos en los que subsistan el cumplimiento parcial o la deficiencia sean equivalentes al importe de la garantía otorgada por el oferente del arrendamiento, el administrador del contrato podrá optar por cancelar total o parcialmente el servicio aplicando la pena convencional máxima al Oferente, lo anterior, en términos del artículo 100 del Reglamento de la Ley antes citada, o bien, optar por rescindir el contrato.

- **El pago de las deductivas será a través de notas de crédito con el IVA adicionalmente, aplicables en los CFDI's mensuales durante la vigencia del Contrato, o en su caso, deducidas del pago mensual correspondiente.**

El envío de las notas de crédito ya sean DEDUCTIVAS o PENALIZACIÓN deberán enviarse por separado

Cuando **"EL PRESTADOR DE SERVICIOS"** quede exceptuado de la presentación de la garantía de cumplimiento, en los supuestos previsto en la **"LAASSP"**, el monto máximo de las penas convencionales por atraso que se puede aplicar, será del 20% (veinte por ciento) del monto de los servicios adquiridos fuera de la fecha convenida, de conformidad con lo establecido en el tercer párrafo del artículo 96 del Reglamento de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público.

DÉCIMA TERCERA. LICENCIAS, AUTORIZACIONES Y PERMISOS

"EL PRESTADOR DE SERVICIOS" se obliga a observar y mantener vigentes las licencias, autorizaciones, permisos o registros requeridos para el cumplimiento de sus obligaciones.

DÉCIMA CUARTA. INSTALACIONES

"EL PRESTADOR DE SERVICIOS", se obliga bajo su costa y riesgo, a prestar los servicios, en las instalaciones referidas en el presente contrato.

DÉCIMA QUINTA. PÓLIZA DE RESPONSABILIDAD CIVIL

Para la prestación de los servicios materia del presente contrato, no se requiere que **"EL PRESTADOR DE SERVICIOS"** contrate una póliza de seguro por responsabilidad civil.

DÉCIMA SEXTA. TRANSPORTE

"EL PRESTADOR DE SERVICIOS" se obliga bajo su costo y riesgo, a transportar los bienes e insumos necesarios para la prestación del servicio, desde su lugar de origen, hasta las ubicaciones que se requiera por parte del administrador del servicio y/o las señaladas en el **ANEXO TÉCNICO** del presente contrato.

DÉCIMA SÉPTIMA. IMPUESTOS Y DERECHOS.

"EL CONALEP" y **"EL PRESTADOR DE SERVICIOS"**, serán responsables individualmente del cumplimiento de sus respectivas obligaciones fiscales, así como del entero y pago de los impuestos y demás contribuciones causadas en virtud del contrato que se formalice, en los términos de las leyes aplicables, por lo que, ni **"EL CONALEP"** y **"EL PRESTADOR DE SERVICIOS"**, serán considerados como obligados solidarios en lo que se refiere a dichas obligaciones de carácter fiscal.





“El CONALEP”, únicamente pagará el Impuesto al Valor Agregado de conformidad con las disposiciones fiscales vigentes, por lo que todos los demás impuestos, derechos y gastos que se generen correrán por cuenta del licitante adjudicado, asimismo, para el pago de dicho impuesto se aplicará lo correspondiente a la normatividad vigente de la Ley del Impuesto al Valor Agregado.

DÉCIMA OCTAVA. PROHIBICIÓN DE CESIÓN DE DERECHOS Y OBLIGACIONES.
“EL PRESTADOR DE SERVICIOS” no podrá ceder total o parcialmente los derechos y obligaciones derivados del presente contrato, a favor de cualquier otra persona física o moral, con excepción de los derechos de cobro, en cuyo caso se deberá contar con la conformidad previa y por escrito de **“EL CONALEP”**.

DÉCIMA NOVENA. CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES.
"LAS PARTES" acuerdan que la información que se intercambie de conformidad con las disposiciones del presente instrumento, se tratarán de manera confidencial, siendo de uso exclusivo para la consecución del objeto del presente contrato y no podrá difundirse a terceros de conformidad con lo establecido en las Leyes General y Federal, respectivamente, de Transparencia y Acceso a la Información Pública, Ley General de Protección de Datos Personales en posesión de Sujetos Obligados, y demás legislación aplicable.

Para el tratamiento de los datos personales que **“LAS PARTES”** recaben con motivo de la celebración del presente contrato, deberá de realizarse con base en lo previsto en los Avisos de Privacidad respectivos.

Por tal motivo, **“EL PRESTADOR DE SERVICIOS”** asume cualquier responsabilidad que se derive del incumplimiento de su parte, o de sus empleados, a las obligaciones de confidencialidad descritas en el presente contrato.

Asimismo **“EL PRESTADOR DE SERVICIOS”** deberá observar lo establecido en el Anexo aplicable a la Confidencialidad de la información del presente contrato.

VIGÉSIMA. SUSPENSIÓN TEMPORAL DE LA PRESTACIÓN DE LOS SERVICIOS.
Con fundamento en el artículo 80 de la LAASSP y 102, fracción II, de su Reglamento, **“EL CONALEP”** en el supuesto de caso fortuito o de fuerza mayor o por causas que le resulten imputables, podrá suspender la prestación de los servicios, de manera temporal, quedando obligado a pagar a **“EL PRESTADOR DE SERVICIOS”**, aquellos servicios que hubiesen sido efectivamente prestados, y en su caso, se reintegrarán los anticipos no amortizados, así como, al pago de gastos no recuperables previa solicitud y acreditamiento.

Una vez que hayan desaparecido las causas que motivaron la suspensión, el contrato podrá continuar produciendo todos sus efectos legales, si **“EL CONALEP”** así lo determina; y en caso que subsistan los supuestos que dieron origen a la suspensión, se podrá iniciar la terminación anticipada del contrato, conforme lo dispuesto en la cláusula siguiente.

VIGÉSIMA PRIMERA. TERMINACIÓN ANTICIPADA DEL CONTRATO
“EL CONALEP” cuando concurran razones de interés general, o bien, cuando por causas justificadas se extinga la necesidad de requerir los servicios originalmente contratados y se demuestre que de continuar con el cumplimiento



de las obligaciones pactadas, se ocasionaría algún daño o perjuicio a **"EL CONALEP"**, o se determine la nulidad total o parcial de los actos que dieron origen al presente contrato, con motivo de la resolución de una inconformidad o intervención de oficio, emitida por la Secretaría Anticorrupción y Buen Gobierno, podrá dar por terminado anticipadamente el presente contrato sin responsabilidad alguna para **"EL CONALEP"**, ello con independencia de lo establecido en la cláusula que antecede.

Cuando **"EL CONALEP"** determine dar por terminado anticipadamente el contrato, lo notificará al **"EL PRESTADOR DE SERVICIOS"** hasta con 30 (treinta) días naturales anteriores al hecho, debiendo sustentarlo en un dictamen fundado y motivado, en el que se precisarán las razones o causas que dieron origen a la misma y pagará a **"EL PRESTADOR DE SERVICIOS"** la parte proporcional de los servicios suministrados, así como los gastos no recuperables en que haya incurrido, previa solicitud por escrito, siempre que estos sean razonables, estén debidamente comprobados y se relacionen directamente con el presente contrato, limitándose según corresponda a los conceptos establecidos en la fracción I, del artículo 102 del Reglamento de la LAASSP.

VIGÉSIMA SEGUNDA. RESCISIÓN

"EL CONALEP" podrá iniciar en cualquier momento el procedimiento de rescisión, cuando **"EL PRESTADOR DE SERVICIOS"** incurra en alguna de las siguientes causales:

a) Contravenir los términos pactados para la prestación de los servicios pactados en el presente contrato;
b) Transferir en todo o en parte las obligaciones que deriven del presente contrato a un tercero ajeno a la relación contractual;
c) Ceder los derechos de cobro derivados del contrato, sin contar con la conformidad previa y por escrito de **"EL CONALEP";**
d) Suspender total o parcialmente y sin causa justificada la prestación de los servicios objeto del presente contrato;
e) No realizar arrendamiento de los bienes en tiempo y forma conforme a lo establecido en el presente contrato y sus respectivos anexos;
f) No proporcionar a los Órganos de Fiscalización, la información que le sea requerida con motivo de las auditorías, visitas e inspecciones que realicen;
g) Ser declarado en concurso mercantil, o por cualquier otra causa distinta o análoga que afecte su patrimonio;
h) En caso de que compruebe la falsedad de alguna manifestación, información o documentación proporcionada para efecto del presente contrato;
i) No entregar dentro de los 10 (diez) días naturales siguientes a la fecha de firma del presente contrato, la garantía de cumplimiento del mismo;
j) Cuando la suma de las penas convencionales exceda el monto máximo de la garantía de cumplimiento del contrato;
k) Cuando la suma de las deducciones al pago, excedan el límite máximo establecido para las deducciones;
l) Divulgar, transferir o utilizar la información que conozca en el desarrollo del cumplimiento del objeto del presente contrato, sin contar con la autorización de **"EL CONALEP"** en los términos de lo dispuesto en la **CLÁUSULA DÉCIMA OCTAVA DE CONFIDENCIALIDAD Y PROTECCIÓN DE DATOS PERSONALES** del presente instrumento jurídico;



m) Impedir el desempeño normal de labores de **"EL CONALEP"**;
n) Cambiar su nacionalidad por otra e invocar la protección de su gobierno contra reclamaciones y órdenes de **"EL CONALEP"**, cuando sea extranjero, y.
o) Incumplir cualquier obligación distinta de las anteriores y derivadas del presente contrato.

"EL CONALEP" de conformidad con lo dispuesto en los artículos 77 de la LAASSP y 98 segundo párrafo del Reglamento podrá rescindir administrativamente sin declaración judicial.

Para el caso de optar por la rescisión del contrato, **"EL CONALEP"** comunicará por escrito a **"EL PRESTADOR DE SERVICIOS"** el incumplimiento en que haya incurrido, para que en un término de 5 (cinco) días hábiles contados a partir del día siguiente de la notificación, exponga lo que a su derecho convenga y aporte en su caso las pruebas que estime pertinentes.

Transcurrido dicho término **"EL CONALEP"**, en un plazo de 10 (diez) días hábiles siguientes, tomando en consideración los argumentos y pruebas que hubiere hecho valer **"EL PRESTADOR DE SERVICIOS"**, determinará de manera fundada y motivada dar o no por rescindido el contrato, y comunicará a **"EL PRESTADOR DE SERVICIOS"** dicha determinación dentro del citado plazo.

Cuando se rescinda el contrato, se formulará el finiquito correspondiente, a efecto de hacer constar los pagos que deba efectuar **"EL CONALEP"** por concepto del contrato hasta el momento de rescisión, o los que resulten a cargo de **"EL PRESTADOR DE SERVICIOS".**

Iniciado un procedimiento de conciliación **"EL CONALEP"** podrá suspender el trámite del procedimiento de rescisión.

Si previamente a la determinación de dar por rescindido el contrato se realiza la prestación de los servicios, el procedimiento iniciado quedará sin efecto, previa aceptación y verificación de **"EL CONALEP"** de que continúa vigente la necesidad de la prestación de los servicios, aplicando, en su caso, las penas convencionales correspondientes.

"EL CONALEP" podrá determinar no dar por rescindido el contrato, cuando durante el procedimiento advierta que la rescisión del mismo pudiera ocasionar algún daño o afectación a las funciones que tiene encomendadas. En este supuesto, **"EL CONALEP"** elaborará un dictamen en el cual justifique que los impactos económicos o de operación que se ocasionarían con la rescisión del contrato resultarían más inconvenientes.

De no rescindirse el contrato, **"EL CONALEP"** establecerá con **"EL PRESTADOR DE SERVICIOS"** otro plazo que le permita subsanar el incumplimiento que hubiere motivado el inicio del procedimiento, aplicando las sanciones correspondientes. El convenio modificatorio que al efecto se celebre deberá atender a las condiciones previstas por los dos últimos párrafos del artículo 74 de la LAASSP.





No obstante, de que se hubiere firmado el convenio modificatorio a que se refiere el párrafo anterior, si se presenta de nueva cuenta el incumplimiento, **"EL CONALEP"** quedará expresamente facultada para optar por exigir el cumplimiento del contrato, o rescindirlo, aplicando las sanciones que procedan.

Si se llevara a cabo la rescisión del contrato, y en el caso de que a **"EL PRESTADOR DE SERVICIOS"** se le hubieran entregado pagos progresivos, éste deberá de reintegrarlos más los intereses correspondientes, conforme a lo indicado en el artículo 73, párrafo cuarto, de la LAASSP.

Los intereses se calcularán sobre el monto de los pagos progresivos efectuados y se computarán por días naturales desde la fecha de su entrega hasta la fecha en que se pongan efectivamente las cantidades a disposición de **"EL CONALEP"**.

VIGÉSIMA TERCERA. RELACIÓN Y EXCLUSIÓN LABORAL

"EL PRESTADOR DE SERVICIOS" reconoce y acepta ser el único patrón de todos y cada uno de los trabajadores que intervienen en la prestación del servicio, deslindando de toda responsabilidad a **"EL CONALEP"** respecto de cualquier reclamo que en su caso puedan efectuar sus trabajadores, sea de índole laboral, fiscal o de seguridad social y en ningún caso se le podrá considerar patrón sustituto, patrón solidario, beneficiario o intermediario.

"EL PRESTADOR DE SERVICIOS" asume en forma total y exclusiva las obligaciones propias de patrón respecto de cualquier relación laboral, que el mismo contraiga con el personal que labore bajo sus órdenes o intervenga o contrate para la atención de los asuntos encomendados por **"EL CONALEP"**, así como en la ejecución de los servicios.

Para cualquier caso no previsto, **"EL PRESTADOR DE SERVICIOS"** exime expresamente a **"EL CONALEP"** de cualquier responsabilidad laboral, civil o penal o de cualquier otra especie que en su caso pudiera llegar a generarse, relacionado con el presente contrato.

Para el caso que, con posterioridad a la conclusión del presente contrato, **"EL CONALEP"** reciba una demanda laboral por parte de trabajadores de **"EL PRESTADOR DE SERVICIOS"**, en la que se demande la solidaridad y/o sustitución patronal a **"EL CONALEP"**, **"EL PRESTADOR DE SERVICIOS"** queda obligado a dar cumplimiento a lo establecido en la presente cláusula

VIGÉSIMA CUARTA. DISCREPANCIAS.

"LAS PARTES" convienen que, en caso de discrepancia entre la convocatoria a la licitación pública, la invitación a cuando menos tres personas, o la solicitud de cotización y el modelo de contrato, prevalecerá lo establecido en la convocatoria, invitación o solicitud respectiva, de conformidad con el artículo 81, fracción IV del Reglamento de la LAASSP.

VIGÉSIMA QUINTA. CONCILIACIÓN.

"LAS PARTES" acuerdan que para el caso de que se presenten desavenencias derivadas de la ejecución y cumplimiento del presente contrato podrán someterse al procedimiento de conciliación establecido en los artículos 109, 111 y 112 de la LAASSP y 126 al 136 de su Reglamento.





VIGÉSIMA SEXTA. DOMICILIOS

"LAS PARTES" señalan como sus domicilios legales para todos los efectos a que haya lugar y que se relacionan en el presente contrato, los que se indican en el apartado de Declaraciones, por lo que cualquier notificación judicial o extrajudicial, emplazamiento, requerimiento o diligencia que en dichos domicilios se practique, será enteramente válida, al tenor de lo dispuesto en el Título Tercero del Código Civil Federal.

VIGÉSIMA SÉPTIMA. LEGISLACIÓN APLICABLE

"LAS PARTES" se obligan a sujetarse estrictamente para la prestación del servicio objeto del presente contrato a todas y cada una de las cláusulas que lo integran, sus Anexos que forman parte integral del mismo, a la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público, su Reglamento; al Código Civil Federal; a la Ley Federal de Procedimiento Administrativo; al Código Federal de Procedimientos Civiles; a la Ley Federal de Presupuesto y Responsabilidad Hacendaria y su Reglamento.

VIGÉSIMA OCTAVA. JURISDICCIÓN

"LAS PARTES" convienen que, para la interpretación y cumplimiento de este contrato, así como para lo no previsto en el mismo, se someterán a la jurisdicción y competencia de los Tribunales Federales con sede en la Ciudad de México, renunciando expresamente al fuero que pudiera corresponderles en razón de su domicilio actual o futuro.

"LAS PARTES" manifiestan estar conformes y enterados de las consecuencias, valor y alcance legal de todas y cada una de las estipulaciones que el presente instrumento jurídico contiene, por lo que lo ratifican y firman en las fechas especificadas.

POR "EL CONALEP"

NOMBRE	CARGO	R.F.C.
KARINA SALAZAR HERNÁNDEZ	DIRECTORA DE INFRAESTRUCTURA Y ADQUISICIONES	SAHK810729TH1
JULIÁN JAVIER ROBLES RIVAS	DIRECTOR CORPORATIVO DE TECNOLOGÍAS APLICADAS	RORJ7312163W3





POR "EL PRESTADOR DE SERVICIOS"

NOMBRE	RAZÓN SOCIAL	R.F.C.
EDGAR HERNÁNDEZ SOTO	SCITUM, S.A. DE C.V.	SCI001208M74

Cadena original:

cf10d3eb4b80f1fdd74306ab6e6152f1822b19451b959eba448ba2d0b2beb22b

Firmante: JULIAN JAVIER ROBLES RIVAS
RFC: RORJ7312163W3

Número de Serie: 00001000000519109829
Fecha de Firma: 31/07/2025 12:07

Certificado:

MIIGPjCCBCagAwIBAgIUMDAwMDEwMDAwMDA1MTkxMDk4MjkwDQYJKoZIhvcNAQELBQAwggGEMSAwHgYDVQQDDBdBVVRPUklEQUQgQ0VSVElGSUNBRE9SQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxKjAoBgkqhkiG9w0BCQEWG2NvbnRhY3RvLnRlY25pY29Ac2F0LmdvYi5teDEmMCQGA1UECQwdQVYuIEhJREFMR08gNzcsIENPTC4gR1VFUlJFUk8xDjAMBgNVBBEMBTA2MzAwMQswCQYDVQQGEwJNWDEZMBcGA1UECAwQQ0lVREFEIERFIE1FWElDTzETMBEGA1UEBwwKQ1VBVUhURU1PQzEVMBMGA1UELRMMU0FUOTcwNzAxTk4zMVwwWgYJKoZIhvcNAQkCE01yZXNwb25zYWJsZTogQURNSU5JU1RSQUNJT04gQ0VOVFJBTCBERSBTRVJWSUNJT1MgVFJJQlVUQVJJT1MgQUwgQ09OVFJJQlVZRU5URTAeFw0yMzA0MTMxOTIzMDlaFw0yNzA0MTMxOTIzNDlaMIHaMSMwIQYDVQQDExpKVUxJQU4gSkFWSUVSIFJPQkxFUyBSSVZBUzEjMCEGA1UEKRMaSlVMSUFOIEpBVklFUiBST0JMRVMgUklWQVMxIzAhBgNVBAoTGkpVTElBTiBKQVZJRVIgUk9CTEVTIFJJVkFTMQswCQYDVQQGEwJNWDEnMCUGCSqGSIb3DQEJARYYamphdmllcnJvYmxlc3JAZ21haWwuY29tMRYwFAYDVQQtEw1ST1JKNzMxMjE2M1czMRswGQYDVQQFExJST1JKNzMxMjE2SERGQlZMMTgwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCoE3gltp+KMFew20oLCRGmMqs+nByJO8XIROql7IZ3y4lJphLr7a784DWcr3f0BbNETW2OUgEm/hNCr4N8rKJd9kIIQRRzNUUMuPXz5ZGuj4PC2ZCdCNWKo3fxq/ZPuiamPyhxbSgCyNee2Cgjd1t09EbgnamEvcaCx8ViFlZDVEft3oQjwh36k3DsWlQgNB+k/bFOa/QlNyeMlWErF11gVe4PHvs+QEyvyt9y1QaYTqAREY8V4kmUwWUjFuON6BukYPOLWf/02cQAfBzw7KUyOJvmH9Ap22C35k4KDTlqjgA7JFWN6ntFUYvcROWRJzeGIDfTvDlHnvXhPn4oLsfzAgMBAAGjTzBNMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgPYMBEGCWCGSAGG+EIBAQQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDBAYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggIBAF+Vzdi/cmcTQ1Uae/8Z9W9mJd1YL1EbV/FXYzpIyWpIPdvjmo6NNBhLWQ/W+P/WUWGxUJCd1u30rRbYs4iU4oaR91FI9eI1geB3vLjSLQNgU/J0bkOUnTKLeQ7rNl78aPRX1Z9QCBqEfeOpE3PRspr3cUuiAnyku8cl7hfNUE2rXRRr7qzasyKp1WcoOm5U2MD6my+Ok23tBEOhPLn4XQ9s9O58y0X/0PXxduO8iD+gugshYMmRTVBb0SA66QRgiwRQwBoMKck4k6DtCXjmNxAC+pgY2keszVEz9zBRnzfCVSp9OFdehcFM61SGy8hBD1+4DkwDSVaNdqjCKc55LOoBd5uUWq6rewvArtG5iiyqVKuxBXnywKY2TaTPhaEZBCH2KzwiZe3EGMvRpvjp3jGoAkqwlgHOLif9gAf/EAgqOgyW0B2/biWjA2cEexTAQEx/LwP8FMnTeNvwiVvNY7b4+IKUYTRz5SX5aJCaZ8V4QqUda4iMg6BlR+C78pRzlo98+9QSudlJQvd003cYzyvYOnsKinvGzx15Pg1PgpU0Uz+lNgqiyiZfSMvGrGzLdEG7jKIHjaKqVJISiwmcJkqEiD2zGpM4nbY7vLo2suf9glRXKaZMeOu5Doiiuzhs4UKI9zpKv4DJCSsXk+K2Eqh0mVTLS0EjfmfAPHLXuNu2

Firma:

Fn4XaPe/L8JeCYFIq9o0eycSLSfHB+XtIVrN59VFGqgVknT8iSlOHdlmTTunTqIZdHLcPKXyJZc0ATl5oytCILO6+8s0BCDZEr5WNOQZh6NGs7lKnAzr3MhwfUL/QjwwUlX5zOMuQTGU/NOiiPHYLtDZOtew8OdR8AllhxNUl4NIgbQXoXd/Mw1x63z8LT9ePHGM7JilfWlW6SJaZI+TTmFXRuV1ojQCMXjnj90w06HgM0dV1SJy7KoM1hK4i9l1nXqGOjAmon7akWc7gVQdLA2I9k1KzTqnGQcDT2DOBmgJ/3c0tlCsETVj9Z0XszsYbFniVXACADEOuDB2EJDR4g==

Firmante: KARINA SALAZAR HERNANDEZ
RFC: SAHK810729TH1

Número de Serie: 00001000000701530711
Fecha de Firma: 31/07/2025 12:27

Certificado:

MIIGRzCCBC+gAwIBAgIUMDAwMDEwMDAwMDA3MDE1MzA3MTEwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29iLm14MSYwJAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTIzMDgwNzE5MDIxNFoXDTI3MDgwNzE5MDI1NFowgdIxITAfBgNVBAMTGEtBUklOQSBTQUxBWkFSIEhFUk5BTkRFWjEhMB8GA1UEKRMYS0FSSU5BIFNBTEFaQVIgSEVSTkFOREVaMSEwHwYDVQQKExhLQVJJTkEgU0FMQVpBUiBIRVJOQU5ERVoxCzAJBgNVBAYTAk1YMSUwIwYJKoZIhvcNAQkBFhZrYXJpbmFzYWxoQGhvdG1haWwuY29tMRYwFAYDVQQtEw1TQUhLODEwNzI5VEgxMRswGQYDVQQFExJTQUhLODEwNzI5TVRTTFJSMDIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQD6ElFFwLB6UBdBc6r/wF9GhbyXfBeGrOFk/RFJD/0CbnloaOpYKb0cpeFVm87wkSOQrI+hsI1JxN6mYjn0cC7GP8RToW6X1ZA78fw/qbTAnAYojnlvP/k3ZgArfTwjDdDUEm97Fp6mKEAgcUBwAUVPa0Uw8IwFMHJ+zxadW9Xrtx5A3nUBZY94gKyzic5TPx5Wo3AYES985mAtz0cyFWrKo/my1vTNTj8FPYCwqHT3SeyMDCHlxpnuyYf0HOrSXnffmdFfO/mT24EPPL0oAGFdxn9+kA+JazWuROnEqvIoAfFZXq81xtpL617DYJgsP+8OQmN79SLWvn2pH5ukZwWNAgMBAAGjTzBNMAwGA1UdEwEB/wQCMAAwCwYDVR0PBAQDAgPYMBEGCWCGSAGG+EIBAQQEAwIFoDAdBgNVHSUEFjAUBggrBgEFBQcDBAYIKwYBBQUHAwIwDQYJKoZIhvcNAQELBQADggIBAJ3gHqrGdtpQz39LlmRVGhVRntFJAEsT5l5u8zW9nF8c8tL9D2F+cPyipuPctbKllCJkYiYFCZ45H53PkGGuuG0JRNDpSmF4rqa0AgkdEHivsJ/4eJNMJKS+fefSrET0fVrKlsm5UJLjGYyENyvX8EhPyDD4Gdd5VpblcOnS/a7Sx+5ckzMiFRk0L9oHHcaHVT7bOfk8h06wk8Q7Q/kx6moHihZcJPYWJf7eIEc4TrLDnP2hLKIzv5GJY5FuVZdQwHBACqp1qZzQYiIPxxXiNYmXlZjVeyftywymxkgY1dzFBd/LlV8ihJ6NTsYtoU+/4uvBa5Szr2ql2Rt413cNTivzAeFGBs4pSXiV6++e6EuGumYaw4jhpjQTOtGlKfZI7pJw6ClO85av61FJQo++v6MKpVfjW62KSsE/ySGFYE3nh2SmZE1lxOdmGSe7uobeK7D/DpDRZcQUccNgkwrEWfLTCIv5Avjtsb5l66exRPkQ1Fl0A9MaMrAA3MY2pALYRPzR139xmjn5cS1qGbqbTAwvz1bZ7fX2gfcGXpaDM6liXMjH0s3r8C8OtZQM7mApTuIeDS7eNoHpmSHuBYJRGrYuAoa6sKltyEJHIuPt8nKTNN+ZQnlwfJu6zb/B+wjoZw7Jx7S8bmzUuW4NGETBj1o0hy/p1iIvDN+8thMbYiJ3

Firma:

YCwEolw1fUrmU228Ug4TxuPunWBdso2BlcX4rfjibE19ZCqiNxDfs9bdpxxio/Zl8aoEGZ3oDnQ8qV17CdAywtyi4BwPeajeGWH9pyH3tG4/WyjBXlJMpijp9aclq68EYywBZUUZGYCFMAoqY/tWtRjII1L9TzG0ZufAkLEV5fnNIwcTnUvtBUoTxUmhWsrxTeCq9XWp3OfUypB7MnaTArGQ4sXQU6CLoNyl7g2rr8NGiEwsW10dpb+WAlQDYgm6X5Rj2YZPjfPvuyiuEJHMs8Es9oFMIECxXg4tTvdW8KntnGSOtEOTPz7cJD4524zs6dv6bb8hgQ9skK6mf8x5bw==

Firmante: SCITUM SA DE CV
RFC: SCI001208M74

Número de Serie: 00001000000705507169
Fecha de Firma: 31/07/2025 18:22

Certificado:

MIIGQjCCBCqgAwIBAgIUMDAwMDEwMDAwMDA3MDU1MDcxNjkwDQYJKoZIhvcNAQELBQAwggGVMTUwMwYDVQQDDCxBQyBERUwgU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEuMCwGA1UECgwlU0VSVklDSU8gREUgQURNSU5JU1RSQUNJT04gVFJJQlVUQVJJQTEaMBgGA1UECwwRU0FULUlFUyBBdXRob3JpdHkxMjAwBgkqhkiG9w0BCQEWI3NlcnZpY2lvc2FsY29udHJpYnV5ZW50ZUBzYXQuZ29iLm14MSYwJAYDVQQJDB1Bdi4gSGlkYWxnbyA3NywgQ29sLiBHdWVycmVybzEOMAwGA1UEEQwFMDYzMDAxCzAJBgNVBAYTAk1YMQ0wCwYDVQQIDARDRE1YMRMwEQYDVQQHDApDVUFVSFRFTU9DMRUwEwYDVQQtEwxTQVQ5NzA3MDFOTjMxXDBaBgkqhkiG9w0BCQITTXJlc3BvbnNhYmxlOiBBRE1JTklTVFJBQ0lPTiBDRU5UUkFMIERFIFNFUlZJQ0lPUyBUUklCVVRBUklPUyBBTCBDT05UUklCVVlFTlRFMB4XDTI0MDMwMTIyMjk1NVoXDTI4MDMwMTIyMzAzNVowgc0xGDAWBgNVBAMTD1NDSVRVTSBTQSBERSBDVjEYMBYGA1UEKRMPU0NJVFVNIFNBIERFIENWMRgwFgYDVQQKEw9TQ0lUVU0gU0EgREUgQ1YxCzAJBgNVBAYTAk1YMSkwJwYJKoZIhvcNAQkBFhpub3JtYS5qdWFyZXpAc2NpdHVtLmNvbS5teDElMCMGA1UELRMcU0NJMDAxMjA4TTc0IC8gSlVQTjc3MDYxN0I3NTEeMBwGA1UEBRMVIC8gSlVQTjc3MDYxN01ERlJNUjAzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAjCYHmEoDosYeWaVmDWJuOXPRWISkQi9B5SC4S9lnohQwPzMkuGQgkk+kZT6UjLOSzbM7qwN/b0dABx1FpnlqR6PFNB4D15lh2swhM8RLPHRmwDb+u2N+orC5rITWiykK6NBHf4XZ2j5HDrK04PEkqtJxf/RHLXU1UzbK56FxvIareNDVwZfnr7stKn01JZ3F7UhJYEUNiXL2dLwGL68aBzNvYUEJecCp74MZ9Laubz75UZ9OPeCmDIJizluo/fSqr7oO9/hZRK7OQr9FPR8435DS6f0neh0bQoqT82kIhZQNZP7nWGPZSUUtNxqm5ow84hxZ3FXDkArn0kliuaeOHQIDAQABo08wTTAMBgNVHRMBAf8EAjAAMAsGA1UdDwQEAwID2DARBglghkgBhvhCAQEEBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwQGCCsGAQUFBwMCMA0GCSqGSIb3DQEBCwUAA4ICAQBYfTk1GfUmCnCzyGOpJRkL5GfmX62D9utwMVOWEiGK/GzLju4qtxy+TpDPEPelKUOkIdbFyxBJmSv9MlwnluUcFbvhuSH0dWoDNA0A2MK7uOaZZLv+Mr2s1JOFdm9/uv5eQJsBJewZMdgfMLzZGcl7k2DUjk8k3SdjYvdyuRcEASYR6BVDwU7Twl0MpnZFwhRXrzFSbByCWXhyr6ZKaKi7A14xpKHpJ+jruYA8VmGpiPUXhZTe7KwZotbIKOXb7B3aJKmULlvl4bdy1Lm0EhcfblE6+jia0aS5cLbGriIrE62fx1qexxb+oICyxw0sTO0tHB+taS0t+f7Glnz2rRht5wD0Om0JSamLArH7pHbhwI45cwOHL2MD2fVzHMIhhJEb9y/j+KHCLuYWbaUN+jDdaGDlhHZGi5AiJU2mGYUr22Jt+kMP/v00QM2iENW/8V6ABjAPP6ZILWuNp8prp7NPBOZuxyZKANRD2i3LgGfZ58ljRQKm84Cy3JhG1+r/am3VEsGlCTKoynrXWoPfTzBs2Io25cjdhFiMEPnb4LmyEog59CWgYf6mAqYCKfBFB2nKtwr2UyES7PgxI47fnhahulwALvDLk871fwuTXDyvrIP15CGtKY3T0sJCKVKhSH93kWakdbz24BGJG5G9lM7Wx7qOSPEg9rWTrFs+ziFtgQ==

Firma:

SQQo8L73ud6QceMyvCkBdqK4O5ZuwT72GbAzAocUB4PjHhc/1PJXcxFfmWHe6x99VKEglhyr4bQ/ctkLRZ8JFnTxybT69JjBqRV9maucIh/lnK1OO0Wm5GaEOQPWXgS7S3F0pX+kDxWE1d+BIWVoniMxabo/dvGP
jCG51cDvIjN2LASqqgUlWcnjxe09L0T2gSiGS9AYFUjPxazaoEutWsQLZY+QYrxrkzKMJ4JO7PFq06axRO/7WoiaWPYol4Zv5rUtJwkAQnX0sHVi8Bk031j6BlZMN43FdApPCihsnNAGuTrIokp4RDxlZ6IBYztV
EVspbxDrawwsZbBy4AlwXQ==

ANEXO 1
DESCRIPCIÓN TECNICA DEL ARRENDAMIENTO

CIUDAD DE MÉXICO, A 8 DE JULIO DE 2025

COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA
PRESENTE.

CON RELACIÓN A LA **INVITACIÓN A CUANDO MENOS TRES PERSONAS NACIONAL ELECTRÓNICA No. IA-11-L5X-011L5X001-N-25-2025 "SERVICIO DE SEGURIDAD PERIMETRAL PARA LA RED LOCAL DE OFICINAS NACIONALES"**

EDGAR HERNÁNDEZ SOTO, ME PERMITO SOMETER A SU CONSIDERACIÓN LA SIGUIENTE PROPOSICIÓN TÉCNICA:

PARTIDA	DESCRIPCIÓN TÉCNICA COMPLETA DEL SERVICIO
Arrendamiento de Equipos de Seguridad Firewall	**PROPUESTA TÉCNICA** **Anexo Técnico** **Arrendamiento de Equipos de Seguridad Firewall** **Conforme al contrato marco vigente** **Descripción Técnica del Arrendamiento** **Scitum S.A. de C.V.** en lo sucesivo **SCITUM**, considera lo siguiente: El **COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA** en lo sucesivo **CONALEP** requiere del **Arrendamiento de Equipos de Seguridad Perimetral de red (Firewall)**, que comprende el equipo de seguridad perimetral, integrando un modelo estándar que permita un análisis del tráfico de información que cursa al interior y exterior, logrando administración de los servicios de Internet y de publicaciones. El equipamiento que **SCITUM** oferta en su propuesta incluye como mínimo los elementos de hardware, software y funcionalidades requeridas en el presente anexo técnico. Para garantizar la operación de seguridad de red, **SCITUM**, en caso de resultar adjudicado, oferta en su propuesta, soluciones en las que el fabricante esté ubicado y reconocido dentro de los cuadrantes de Gartner más reciente divulgado a la fecha de inicio del procedimiento de contratación, o en algún otro reporte reconocido por la industria a nivel internacional.

Con base al último Cuadrante mágico de Gartner publicado para firewalls, se respalda que el firewall tipo 1 propuesto por **SCITUM**, se encuentra en el cuadrante de CHALLENGERS.



SCITUM, en caso de resultar adjudicado, considera que el equipo de seguridad FIREWALL se suministrará de acuerdo con lo especificado en las características técnicas descritos en el presente anexo técnico.

ESPECIFICACIONES TÉCNICAS:

Partida	Cantidad	Descripción	Periodo
Única	1	"Servicio de seguridad perimetral para la red local de Oficinas Nacionales" que corresponde al proyecto "Fortalecimiento a la seguridad de la información", en adhesión al contrato de marco para el "Arrendamiento de equipo de seguridad Firewall y NAC para las Dependencias y Entidades de la Administración Pública Federal"	A partir del día siguiente a la notificación del fallo y hasta el 31 de diciembre de 2025

Productos que se integran en la partida:

No. Partida	Partida Contrato Marco	Apartado Contrato Marco	Nombre	Cantidad de equipos
1	1	5.2.1	Firewall Tipo 1	2 equipos, uno principal y uno redundante

FUNCIONALIDADES DEL EQUIPO DE SEGURIDAD FIREWALL

SCITUM, en caso de resultar adjudicado, incluye en su propuesta, todo el licenciamiento de hardware y software necesario y proporcionar de inicio, la totalidad de servicios de seguridad con las funcionalidades asociadas que se requieran, de acuerdo con los perfiles y a las cantidades indicadas para el Firewall incluido en el presente anexo técnico y soportará configuraciones en alta disponibilidad, por lo que se implementará un esquema de alta disponibilidad activo/pasivo, en el cual el firewall activo pueda procesar todo el tráfico.

SCITUM entiende que, se deberá implementar un esquema de alta disponibilidad activo/pasivo, en el cual el firewall activo pueda procesar todo el tráfico

I. control de políticas

- Permite a los usuarios configurar políticas de seguridad en función del tiempo, grupo de usuarios/grupo de seguridad, protocolo de capa de aplicación, ubicación geográfica, dirección IP, puerto, grupo de nombre de dominio, categoría de URL, tipo de acceso, tipo de terminal y grupo de dispositivos.
- Deben de ser capaces de manejar protocolos tales como RADIUS o KERBEROS.

II. Enrutamiento

- Admite rutas estáticas y protocolos de enrutamiento dinámicos como RIP, OSPF, BGP e IS-IS en sus últimas versiones estables.
- El enrutamiento basado en políticas admite las siguientes condiciones coincidentes: dirección IP de origen, dirección IP de destino, tipo de servicio, tipo de aplicación, usuario/grupo de usuarios/grupo de seguridad, interfaz de entrada y prioridad DSCP.
- Deberá de soportar la encapsulación de tráfico IPv4 e IPv6.
- Protocolos Avanzados de VPN

III. Especificaciones IKE Versión 1, Versión 2

- Modo de negociación: Automático, Main, Aggresive (soportado únicamente en topología hub and spoke star)
- Encriptación: AES-256, AES-192, AES-128, 3DES, DES
- Autenticación: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5
- Integridad Hash: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5, AES.
- PRF: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5, AES-128
- Grupo DH: 1, 2, 5, 14, 15, 16, 18, 19, 20, 21

Av. Periférico Sur No. 3190, Piso 1
Colonia Jardines del Pedregal, Alcaldía Álvaro Obregón,
C.P. 01900, Ciudad de México
Tel. +52 (55) 9150.7400
ventas@scitum.com.mx

IV. Especificaciones IPSec

- Cuenta con Modo de encapsulación: Automático, Transport, Tunnel
- Protocolo de seguridad: ESP, AH, AH-ESP
- ESP Encriptación: GCM256, GCM192, GCM128, GMAC256, GMAC192, GMAC128, AES-256, AES-192, AES-128, 3DES y DES
- ESP Autenticación: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5
- PFS: 1,2,5,14,15,16,18,19,20 y 21
- DPD modos: Periodic, On-Demand
- L2TP
- L2TP OVER IPSEC
- GRE
- MULTIPOINT GRE

V. Identificación de aplicaciones 1Pv6

- Soportar el protocolo IPv6.
- Compatible con IPv6'sobre túneles GRE de IPv4 y túneles 6R.

VI. Control de tráfico

a) Admite políticas de control de tráfico basadas en el protocolo de la capa de aplicación, incluida la configuración del ancho de banda máximo, el ancho de banda garantizado y la prioridad del tráfico del protocolo.
b) Admite garantía de ancho de banda basada en usuarios y direcciones IP.
c) Admite el número máximo de conexiones por dirección IP o usuario.
d) Admite el tráfico basado en la ubicación geográfica y el análisis de amenazas.
e) Soporta la gestión de cuotas de tráfico de usuarios.
f) Soporta traffic shaping.
g) Proporciona protección y soporte al menos a las tecnologías de Voz sobre IP: SIP, H.323, H.460, ICE/STUN para tráfico cifrado y calidad de servicio.
h) Permite la distribución por DHCP para IPv4 e IPv6 en sus interfaces LAN y subinterfaces (Vlans) en interfaces LAN.

VII. Gestión de políticas

a) Admite la prevención de datos para identificar y filtrar archivos y contenido (diferentes tipos de información, como tarjetas de identificación, tarjetas de crédito, tarjetas de débito y de seguridad social) en tránsito.
b) Admite el filtrado de URL mediante la implementación de un servidor de URL local.
c) Admite el filtrado de DNS para mejorar el rendimiento del filtrado de páginas web.
d) Es compatible con SafeSearch para filtrar el contenido no saludable devuelto por los motores de búsqueda como Google, Yahoo, MSN.
e) Las reglas de firewall tendrán vigencia con base a fechas (incluyendo día, mes y año).

VIII. Contar con soporte NAT

	a) Admite funciones NAT completas y NAT ALG para múltiples protocolos de capa de aplicación, incluidos ILS, DNS, PPTP, SIP, FTP, ICQ, RTSP, QQ, MSN y MMS. b) Admite la generación de una alarma si el uso del grupo de direcciones NAT de origen supera el umbral. c) Hacer traslación de direcciones estático, uno a uno. d) Hacer traslación de direcciones dinámicas, muchos a uno. **IX. Prevención de intrusiones y antivirus** a) Admite la personalización de plantillas de pol1ticas de prevención de intrusiones basadas en escenarios. b) Admite la prevención de craqueo de fuerza bruta para servicios de aplicaciones comunes (HTTP, FTP, SSH, SMTP e IMAP, VoIP, SIP) y software de base de datos (MySQL), oracle y MSSQL). c) Admite el filtrado basado en nombres de dominio malintencionados para bloquear C&C. d) Soporte de detección y bloqueo de ataques. **X. Protección de seguridad de tráfico cifrado** a) Brinda protección de seguridad de tráfico cifrado b) Descifra el tráfico HTTPS, POP3S, SMTPS e IMAPS y realiza filtrado de datos, auditoría y protección de seguridad en el tráfico descifrado. c) Soporta descifrado refinado basado en categorías de URL para mejorar el rendimiento del descifrado. d) Descifra el tráfico y lo refleja en dispositivos de terceros para auditoria y detección de seguridad. **XI. Autenticación de usuario de acceso a la, red** a) Compatible con AD (directorio activo), SSO (Single sing-on) RADIUS SSO (Single Sing-On), autenticación NTLM, sin autenticación, autenticación MAC y autenticación SMS. b) Compatible con grupos de seguridad dinámicos para autorizar dinámicamente organizaciones horizontales. c) Soporta múltiples dominios de autenticación para cumplir con los requisitos de administración independiente y autenticación de múltiples sucursales. d) Soporta la personalización de la página del portal y cuestionarios para promover el marketing. **XII. Gestión centralizada** a) Admite la actualización mediante una unidad flash USB para reducir los costos de O&M. b) Proporciona interfaces API de integración hacia el norte, como RESTCONF y NETCONF para conectarse a plataformas de administración de terceros. c) Soportar los protocolos SNMP RFC 1157, SNMPV2C o SNMPV3. **XIII. Autenticación 802.lX** a) Admite el paso del proceso de autenticación 802.lX para garantizar la seguridad del acceso a la red Wi-Fi o en la LAN.

XIV. Selección de enlace ascendente inteligente

a) Selecciona de forma inteligente los enlaces del operador en función de las direcciones IP de destino, admite la configuración de la interfaz activa/en espera y el equilibrio de carga por porcentaje.
b) Soportar QoS basada en colas inteligentes.

Las funcionalidades y características antes descritas aplican para cada uno de los tipos de Firewall descritos en el presente anexo técnico.

CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS

Cantidad de equipos ofertados: 2 equipos, uno para funcionar como equipo principal y el otro como equipo redundante en HA, en caso de falla del equipo principal, el equipo redundante tomara el rol de equipo principal de manera automática y sin intervención alguna.

Las funcionalidades y características antes descritas aplican para cada uno de los tipos de Firewall solicitados y se apegarán a las características técnicas que se describen a continuación:

FIREWALL TIPO 1

Indicador	Requisitos de especificación técnica
Requisitos de configuración física	≥ 2,000 Usuarios de VPN SSL simultáneos ≥ 5,000 Túneles de VPN IPSec ≥ Soporte de 10 Firewalls virtuales
Arquitectura de hardware	Capacidad de soportar Fuentes de poder redundantes interna o externa.
Requisitos de interfaces	≥ 32 Número máximo de puertos ≥ 16 Puertos 10/100/1000 baseT GE. ≥ 16 Puertos ópticos 1GE SFP
Tarjetas de bypass de puertos eléctricos	
Requisitos de desempeño	≥ 8 Gbps Rendimiento IPV4 de Firewall (Throughput). ≥ 8 Gbps Rendimiento IPv6 de Firewall (Throughput). 3.5 Gbps Rendimiento Protección Real de Firewall (EMIX Throughput) 2.5 Gbps Rendimiento inspección SSL. ≥ 4,000,000 Número de conexiones simultáneas. ≥ 5,000 Número de conexiones simultáneas SSL VPN (Throughput). ≥ 5,000 Número de conexiones nuevas por segundo. ≥ 512 Mb IPsec VPN Throughput (AES-128+SHA1, 1420-byte) .

CARACTERÍSTICAS DE ADMINISTRACIÓN

- Será visible y configurable desde la interfaz GUI

- Las interfaces mostrarán el estado de las conexiones
- Se podrá desplegar graficas con las direcciones IP con más sesiones concurrentes o mayor consumo de ancho de banda.
- La GUI podrá ser configurada en inglés y/o español.
- Permitirá obtener respaldos manuales de la configuración, así como poder inyectar archivos de configuración anteriores.
- Brindará soporte a servidores Syslog para envió de bitácoras.

SISTEMA DE MONITOREO Y REPORTEO

- Ofrecerá mecanismos de reporteo, análisis y almacenamiento de bitácoras.
- Mostrará por lo menos el top 10 de las direcciones IPs de red LAN con mayor consumo de ancho de banda por minutos, horas, días, semanas o el último mes.
- Mostrará por lo menos el top 10 de las aplicaciones con mayor consumo por minutos, horas, días, semanas o el último mes.
- Mostrará por lo menos el top 10 de sitios web con mayor consumo por minutos, horas, días, semanas o el último mes.
- Mostrará por lo menos el top 10 de fuentes con mayor número de ataques a la institución por minutos, horas, días, semanas o el último mes, con grado de severidad.
- Ofrecerá la búsqueda avanzada en los registros almacenados.
- Los reportes serán bajo demanda y/o de manera programada y cíclica.
- Permitirá la personalizar los reportes.
- Dará almacenamiento a la información por lo menos de 1 mes y contará con la posibilidad de grabar dicha información o reportes en un dispositivo de almacenamiento externo.
- En caso de que el reportador sea externo, tomará los datos en almacenamiento externo y elaborar los reportes solicitados.
- Aviso de interrupción del servicio vía correo electrónico a un máximo de 5 cuentas. de correo, en un horario de 5x8 durante la duración del contrato.

NORMAS:
NOM-019-SCFI-vigente y/o UL norma equivalente internacional: Seguridad de Equipo de Procesamiento de Datos.

MANUALES DEL EQUIPO DE SEGURIDAD FIREWALL Y NAC
SCITUM, en caso de resultar adjudicado, entregará manual del equipo para su instalación, configuración y operación en idioma español, además deberá proporcionar la liga del sitio Web en el cual se puede descargar.

MÉTODO DE EVALUACIÓN
SCITUM, entiende que el método de evaluación de las propuestas será binario.

CRITERIOS APLICABLES PARA EL ARRENDAMIENTO DE EQUIPO DE SEGURIDAD FIREWALL

SCITUM, en su cotización considera lo siguiente:

	• Las especificaciones plasmadas en el presente documento son los requerimientos mínimos para la contratación. • Todos los equipos arrendados incluidos los de reemplazo, deberán ser nuevos. • Se realizará la instalación, configuración y puesta a punto de los equipos objeto de arrendamiento, en las instalaciones que el **CONALEP** le indiquen además de garantizar la integración y compatibilidad de los componentes de hardware descritos en el presente anexo técnico, así como los elementos necesarios para la integración y funcionalidad total requerida por el **CONALEP** • **SCITUM**, en caso de resultar adjudicado, del equipo arrendado de seguridad FIREWALL incluye en su propuesta, el suministro de todos los accesorios necesarios, para la correcta integración, operación y funcionalidad de los equipos. • **SCITUM**, en caso de resultar adjudicado, incluye en su propuesta todo el licenciamiento, actualizaciones, Hardware, software y accesorios necesario para el correcto funcionamiento de los equipos descritos en el presente anexo técnico durante la vigencia de la garantía. • **SCITUM** entiende que se aplicarán los criterios de adjudicación señalados en el apartado "Forma de Adquisición" de este anexo técnico. • **SCITUM**, en caso de resultar adjudicado, entregará dentro de los primeros quince días posteriores a la fecha de adjudicación del contrato, un plan de trabajo donde se describan las actividades que se tienen que realizar para la correcta entrega, instalación, configuración y puesta a punto de los equipos arrendados por el **CONALEP**, con aprobación de estas. • **SCITUM** entiende que el tiempo de entrega, configuración y puesta a punto de los equipos objeto del arrendamiento, Se realizará en las instalaciones que el **CONALEP** indique en un plazo no mayor a noventa (90) días naturales a partir del día hábil siguiente a la fecha de la adjudicación del contrato. • **SCITUM**, en caso de resultar adjudicado, realizará la entrega del equipo de seguridad FIREWALL y NAC requeridos por el **CONALEP** en los domicilios indicados. • **SCITUM**, en caso de resultar adjudicado, cuenta con medios de comunicación para reportar solicitudes de atención, fallas de equipo (mesa de ayuda). Los medios para reportar fallas, al menos deberán ser un número convencional, un celular y un correo electrónico. • **SCITUM** el tiempo de atención en sitio se otorgará de forma continua, las 24 horas, los 7 días a la semana, los 365 días del año. Cada solicitud de atención deberá solventarse en un plazo no mayor a 6 horas naturales a partir del levantamiento del reporte; dicho plazo podrá ser de hasta 24 horas naturales únicamente cuando se trate de reparaciones que impliquen el reemplazo de partes o componentes. • **SCITUM**, en caso de resultar adjudicado, es responsable en el caso de que se violen derechos de propiedad industrial, patentes o derechos de autor, respecto al software y/o hardware utilizados en los equipos arrendados, dejando en todo momento a salvo a él **CONALEP**.

- **SCITUM**, en caso de resultar adjudicado, proveerá los recursos humanos necesarios para cumplir las tareas de:
  - Maniobra, carga, descarga, desembalaje, ensamblado, retiro de empaques y entrega de los equipos.
  - Instalación, configuración y puesta a punto de los equipos de acuerdo con las recomendaciones y mejores prácticas del fabricante.
- **SCITUM** entiende que, el fabricante o los fabricantes que se contemplan en la solución cuentan con una oficina de representación debidamente conformada en México. **Av. Santa Fe No. 440 Piso 15 Colonia Santa Fe, Ciudad de México CP 05348 Teléfono (52) 55 5282 8600**

ENTREGABLES

Los entregables se definen como la entrega de los equipos, documentación inicial, final y reportes mensuales inherentes al presente Anexo Técnico, los cuales se derivan de la contratación específica que celebre al amparo del Contrato Marco, es responsabilidad del **SCITUM**, en caso de resultar adjudicado, entregarlos al Administrador del Contrato del **CONALEP**.

El administrador del **CONALEP** y el representante designado por **SCITUM** serán responsables de dar seguimiento y asegurarse del cumplimiento a lo establecido en el presente anexo técnico.

SCITUM, en caso de resultar adjudicado, proporcionará dentro de los 10 días hábiles posteriores a la entrega, instalación y puesta a punto de los equipos, los entregables que a continuación se indican:

- Relación y configuración del equipo arrendado, así como el licenciamiento propuesto para el arrendamiento por parte del SCITUM a él **CONALEP**, en el que se indique ubicación, marca, modelo y el número de serie de los equipos que integran el arrendamiento de equipos de seguridad FIREWALL y NAC

SCITUM, en caso de resultar adjudicado, entregará el procedimiento de recepción de reportes para la atención y resolución de fallas de los equipos dentro de los cinco (5) días hábiles posteriores a la adjudicación del contrato.

Dentro de los primeros quince (15) días naturales posteriores a la adjudicación del contrato, SCITUM, en caso de resultar adjudicado, entregará lo siguiente:

- Cronograma de actividades.
- El plan de trabajo detallado para la instalación, configuración y puesta a punto de los bienes ofertados para las Dependencias o Entidades, con aprobación de estas. El plan de trabajo deberá incluir la definición, desarrollo y mantenimiento de un plan de pruebas para validar la correcta instalación, configuración y puesta a punto.
- **SCITUM**, en caso de resultar adjudicado, entregará una matriz de escalamiento que permita al **CONALEP** contactar al personal designado

por SCITUM para asegurar el cumplimiento conforme al presente anexo técnico. De igual manera, el SCITUM proporcionará un documento donde se plasme el procedimiento que seguirá para resolución de incidentes.

Memoria técnica dentro de los primeros diez (10) días hábiles posteriores a la puesta en operación del equipo de seguridad FIREWALL conteniendo lo siguiente:

- Relación de equipos utilizados para la implementación de la solución
- Diagramas de conectividad incluyendo entre otros, el número de puertos requeridos para la operación de la solución propuesta, el tipo de comunicación requerida (unidireccional o bidireccional), etc. Los diagramas se incluirán dentro de la memoria técnica en formato electrónico (Microsoft Office Visio).
    - Se Indicará claramente mediante diagrama, la conectividad en su origen (Equipo Marca, Modelo, Serie y Puerto), destino(Equipo Marca, Modelo, Serie y Puerto), así como la función de cada cable Ethernet o Fibra que se implementen, estos deben ser etiquetados ya sean del oferente o de la institución que se vaya a utilizar, para el funcionamiento de la solución.
    - Configuración de cada equipo que conforme la solución y una breve descripción de su finalidad.
    - Políticas de filtrado, conforme a lo indicado por el CONALEP, y que servicios permiten cada una de ellas, especificar que incluye la política de bloqueo o política final por default.
    - Nombre de los agrupamientos y que IP's incluyen en cada uno.
    - Las políticas que se aplican a cada agrupamiento al inicio del proyecto.
    - La protección del IDS/IPS o similar que se aplicaran.
    - Las configuraciones WAN utilizadas en el puerto de los equipos.
    - Configuraciones de balanceo WAN

  Los puntos no previstos serán ajustados a entera satisfacción del CONALEP.
- Registro de las pruebas de disponibilidad realizadas.
- **SCITUM**, en caso de resultar adjudicado, incluirá una copia del respaldo de los equipos de la solución implementada en medio magnético.
- En caso de sustitución de equipos o cambio de configuración en los mismos, la memoria técnica será actualizada por **SCITUM**.

Entregables mensuales

- Entrega dentro de los primeros 10 días hábiles siguientes a la conclusión del mes que se pretende facturar, de los siguientes documentos:
    - Relación total de los equipos entregados en arrendamiento por parte de **SCITUM**, en caso de resultar adjudicado, a entera satisfacción del Administrador del Contrato del **CONALEP.**
        - Top 50 de las aplicaciones que consumen como mínimo 80% del servicio de Internet.

- Top de los usuarios que en conjunto consumen como mínimo 80% del servicio de Internet.
- Top 50 de los sitios que son bloqueados en su acceso al servicio de Internet.
- Top 50 de los usuarios con más bloqueos en su acceso al servicio de Internet.
- Informe del IDS/IPS o similar, que incluya IP y puerto de Origen e IP y puerto 2 Destino.
- Promedio de sesiones concurrentes por día.
- Mayor número de sesiones nuevas en un lapso de 1 hora.
- Accesos por medio de VPN
- Bitácora de conexiones.
- Top 100 de los sitios web, con mayor consumo en el mes.
- Listado de los tipos y cantidades de ataque y amenazas recibidos en el mes.
- Top 50 de los equipos con mayores amenazas en el mes.
- Gráfica de las vulnerabilidades detectadas, más concurrentes en el mes.
- Los errores y desempeño de las interfaces en el equipo
- Lista de las actualizaciones de los diferentes rubros
- Grafica mensual del consumo de Internet con segmentación diaria.
- Grafica mensual del consumo de los recursos (CPU, Memoria, etc.) de los equipos que conforman la solución.
- En caso de reemplazo de alguno de los equipos, derivado de fallas concurrentes, SCITUM formalizara el cambio con hoja membretada y firmada por su representante legal, indicando claramente Marca, Modelo y Serie del equipo que se retira y del equipo que ingresa como remplazo.
- Reporte mesa de ayuda, deberán incluir:
  - Nombre completo del solicitante
  - Nombre del técnico o persona que atiende
  - Status (Abierto-Cerrado)
  - Fecha y Hora Solicitud
  - Fecha y Hora de Solución
  - Requerimiento solicitado
  - Tiempo de Solución
- Reporte de incidencias.

PLAZO DE ENTREGA DE LOS EQUIPOS DEL ARRENDAMIENTO
La entrega de los equipos arrendados, su instalación, configuración y puesta a punto se deberá realizar en un plazo no mayor a 90 días naturales a partir del día hábil siguiente a la fecha de adjudicación del contrato.

SCITUM comprende que se hará constar la entrega en mención, a través de acta administrativa levantada para ello, suscrita por el Administrador del Contrato, **SCITUM** y de los testigos respectivos.

SCITUM comprende que de tenerse incumplimientos por parte de **SCITUM** en los tiempos señalados para la realización de las entregas iniciales o posteriores, se aplicarán las penas convencionales a que haya lugar, de conformidad con el apartado "Penas y Deductivas".

MEDIOS PARA REPORTAR FALLAS DEL EQUIPO DE SEGURIDAD FIREWALL

- **SCITUM**, en caso de resultar adjudicado, entregará el procedimiento de recepción de reportes y atención de fallas de los equipos, dentro de los 5 días hábiles posteriores a la fecha de adjudicación del arrendamiento.
- **SCITUM**, en caso de resultar adjudicado, proporcionará un correo electrónico y un número telefónico del centro de atención telefónica del **SCITUM**, sin costo de llamada para el **CONALEP**, como medios para reportar fallas.
- **SCITUM**, en caso de resultar adjudicado, entregará una matriz de escalamiento que permita al **CONALEP** contactar al personal designado por el **SCITUM** para asegurar el cumplimiento conforme al presente documento. De igual manera, **SCITUM** proporcionará un documento donde se plasme el procedimiento que seguirá para resolución de incidentes.

MESA DE AYUDA

SCITUM, en caso de resultar adjudicado, pondrá a disposición del **CONALEP** una mesa de ayuda dentro de los 5 días hábiles anteriores a la fecha de inicio de la prestación del arrendamiento para que el **CONALEP** mediante la presentación de reportes, pueda solicitar la atención, diagnóstico y solución de fallas de los equipos arrendados, para lo cual **SCITUM**, en caso de resultar adjudicado como el proveedor del arrendamiento proporcionará números convencionales y celulares, además de correos electrónicos del representante de **SCITUM**.

NIVELES DE ATENCIÓN

Los tiempos de atención y solución de fallas requeridos son:

- **SCITUM**, en caso de resultar adjudicado, se compromete a dar cumplimiento a los niveles de atención.
- **SCITUM**, en caso de resultar adjudicado entiende que el tiempo de atención en sitio se otorgará de forma continua, las 24 horas, los 7 días a la semana, los 365 días del año. Cada solicitud de atención se solventará en un plazo no mayor a 6 horas naturales a partir del levantamiento del reporte; dicho plazo podrá ser de hasta 24 horas naturales únicamente cuando se trate de reparaciones que impliquen el reemplazo de partes o componentes.

De implicarse la reparación de los equipos señalados en las dos viñetas anteriores, se atenderá lo siguiente:

- Si el tiempo de reparación excede el tiempo establecido en los puntos antes mencionados, al día siguiente hábil, **SCITUM**, en caso de resultar adjudicado, entregará un equipo de respaldo con las mismas características mientras se soluciona el problema.
- Si la reparación excede los 30 días naturales a partir de la fecha del reporte, al día siguiente hábil, **SCITUM**, en caso de resultar adjudicado, entregará a

cambio, instalará, configurará y pondrá a punto un equipo nuevo con las características iguales al arrendado u otro equipo de características superiores.

- Si el equipo presenta más de cinco fallas dentro de un periodo de 30 días naturales, **SCITUM**, en caso de resultar adjudicado, lo sustituirá por uno de características iguales o superiores, en un plazo no mayor a un día hábil a partir del quinto reporte de falla en el mes, incluyendo el tiempo de atención.

En caso de reasignación o reubicación, se atenderá lo siguiente:

- Dicha solicitud será atendida a partir del levantamiento del reporte por parte del Administrador del Contrato, en un plazo no mayor a dos (2) días hábiles cuando dicho cambio se realice dentro del mismo inmueble y en un plazo de tres (3) días hábiles cuando el cambio implique la reasignación o reubicación de los equipos en inmuebles diferentes del **CONALEP**. Los plazos antes mencionados podrán ampliarse hasta por cinco (5) días hábiles cuando las reasignaciones o reubicaciones se realicen en las zonas foráneas. En todos los casos, se considerarán días laborables y en un horario de 9:00 a 19:00 horas. Dichos periodos incluirán el tiempo de atención.

Otros supuestos:

- En caso de robo o daño de los equipos destinados al arrendamiento por causas atribuibles **SCITUM** durante los procesos de entrega, o durante su instalación y/o configuración, **SCITUM**, en caso de resultar adjudicado, los sustituirá por equipos con características iguales o superiores, dentro del plazo señalado en el numeral 16 "Plazo de entrega de los equipos en arrendamiento", sin otorgarse plazos adicionales para tal efecto y sin costo para el **CONALEP.**

SCITUM, en caso de resultar adjudicado, proporcionará durante la vigencia de la garantía los niveles de atención descritos en la siguiente tabla:

Actividad	Descripción	Alcance	Nivel de servicio
Entregables	**SCITUM** entregará los equipos arrendados. **SCITUM** entregará de forma electrónica, archivos con la relación en el que se indique la marca, modelo y número de serie, así como las remisiones de entrega firmadas por el responsable de las áreas que designe el	Arrendamiento de equipo de seguridad Firewall	Dentro de los 90 días naturales a partir de la fecha de adjudicación del contrato.

		Administrador del Contrato del **CONALEP** para la entrega de los equipos.		
	Entregables	Relación y configuración del equipo arrendado, así como el licenciamiento propuesto para el arrendamiento por parte **SCITUM** a él **CONALEP**, en que se indique ubicación, marca, modelo y el número de serie de los equipos que integran el arrendamiento de equipos de seguridad FIREWALL y NAC.	Arrendamiento de equipo de seguridad Firewall y NAC	Dentro de los 10 días hábiles posteriores a la entrega, instalación y puesta a punto de los equipos.
	Entregables	**SCITUM**, en caso de resultar adjudicado, entregará: Cronograma de actividades. El plan de trabajo detallado para la instalación, configuración y puesta a punto de los bienes ofertados para el **CONALEP**, con aprobación de estas. El plan de trabajo deberá incluir la definición, desarrollo y mantenimiento de un plan de pruebas para validar la correcta instalación, configuración y puesta a punto. **SCITUM** entregará una matriz de escalamiento que permita al **CONALEP** contactar al personal designado por el SCITUM para asegurar el cumplimiento conforme	Arrendamiento de equipo de seguridad Firewall	Dentro de los primeros QUINCE (15) días naturales posteriores a la fecha de la adjudicación del contrato

		al presente anexo técnico. De igual manera, SCITUM proporcionará un documento donde se plasme el procedimiento que seguirá para resolución de incidentes.		
	Entregables	**SCITUM** entregará el procedimiento de recepción de reportes y atención de fallas de los equipos, dentro de los cinco (5) días hábiles posteriores a la adjudicación del contrato.	Arrendamiento de equipo de seguridad Firewall	Dentro de los 5 días hábiles posteriores a la adjudicación del contrato.
	Entregables	Memoria técnica conteniendo: Relación de equipos utilizados para la implementación de la solución. Diagramas de conectividad Incluyendo entre otros, el número de puertos requeridos para la operación de la solución propuesta, el tipo de comunicación requerida (unidireccional o bidireccional), etc. Los diagramas se incluirán dentro de la memoria técnica en formato electrónico (Microsoft Office Visio). Registro de las pruebas de conectividad realizadas. **SCITUM** incluirá una copia del respaldo de los equipos de la solución	Arrendamiento de equipo de seguridad Firewall	Dentro de los primeros diez (10) días hábiles posteriores a la puesta en operación de los equipos de seguridad Firewall.

		implementada en medio magnético. En caso de sustitución de equipos o cambio de configuración en los mismos, la memoria técnica será actualizada por **SCITUM**.		
	Entregables mensuales	SCITUM entregará: Relación total de los equipos entregados en arrendamiento por parte del SCITUM a entera satisfacción del Administrador del Contrato, del **CONALEP.**, Reporte de incidencias.	Arrendamiento de equipo de seguridad Firewall	Dentro de los primeros 10 días hábiles siguientes a la conclusión del mes que se pretende facturar.
	Mesa de ayuda	**SCITUM**, en caso de resultar adjudicado, pondrá a disposición del **CONALEP** una Mesa de Ayuda para el levantamiento de reportes de fallas de los equipos.	Arrendamiento de equipo de seguridad Firewall	Dentro de los 5 días hábiles anteriores a la fecha del inicio de la prestación del servicio.
	Atención de fallas en el **CONALEP**	Atención y reparación de fallas y problemas relacionadas con los equipos	Todos los equipos objeto del arrendamiento que se detallan en el presente Anexo Técnico	El tiempo de atención en sitio se otorgará de forma continua, las 24 horas, los 7 días de a semana, los 365 días del año. Cada solicitud de atención se solventará en un plazo no mayor a 6 horas naturales a partir del levantamiento

					del reporte; dicho plazo podrá ser de hasta 24 horas naturales únicamente cuando se trate de reparaciones que impliquen reemplazo de partes o componentes De implicarse la reparación de los equipos señalados en las dos viñetas anteriores, se atenderá lo siguiente: Si el tiempo de reparación excede el tiempo establecido en los puntos antes mencionados, al día siguiente hábil, **SCITUM** entregará un equipo de respaldo con las misas características mientras se soluciona el problema. Si la reparación excede los 30 días naturales a partir de la fecha del reporte, al día siguiente hábil,

				SCITUM entregará a cambio, instalará, configurará y pondrá a punto un equipo nuevo con las características iguales al adquirido u otro equipo de características superiores. Si el equipo presenta más de cinco fallas dentro de un periodo de 30 días naturales, SCITUM lo sustituirá por uno de características iguales o superiores, en un plazo no mayor a un día hábil a partir del quinto reporte de falla en el mes incluyendo el tiempo de atención.
	Reasignación o reubicación de los equipos otorgados en arrendamiento.	Atención para la reasignación o reubicación de los equipos en las instalaciones o sedes del **CONALEP**	Todos los equipos objeto del arrendamiento.	En caso de reasignación o reubicación, se atenderá lo siguiente: Dicha solicitud Se atenderá a partir del

					levantamiento del reporte por parte del Administrador del Contrato, en un plazo no mayor a dos (2) días hábiles cuando dicho cambio se realice dentro del mismo inmueble y en un plazo de tres (3) días hábiles cuando el cambio implique la reasignación o reubicación de los equipos en inmuebles diferentes del **CONALEP**. Los plazos antes mencionados podrán ampliarse hasta por cinco (5) días hábiles cuando las reasignaciones o reubicaciones se realicen en las zonas foráneas. En todos los casos, se considerarán días laborables y en un horario de 9:00 a 19:00 horas. Dichos periodos incluirán el tiempo de atención.

De tenerse incumplimientos por parte de **SCITUM**, en caso de resultar adjudicado, en los tiempos de atención y solución de fallas o ante la petición de la reasignación o reubicación de los equipos, así como en los niveles de servicio señalados anteriormente, se aplicarán las deductivas a que haya lugar, de conformidad con el apartado "Penas y Deductivas".

INSTALACIÓN

SCITUM entiende que la instalación, configuración y puesta a punto de los bienes ofertados será realizada por SCITUM, en caso de resultar adjudicado, y de común acuerdo con el **CONALEP**.

- Para la instalación, configuración y puesta a punto de los bienes ofertados, **SCITUM**, en caso de resultar adjudicado, entregará un plan de trabajo al Administrador del contrato del **CONALEP**, quien aprobará dicho plan.
- **SCITUM** entiende que el **CONALEP** determinará la ubicación física en donde se requiera instalar los equipos.
- **SCITUM** entiende que el **CONALEP** proporcionará el número de políticas de seguridad, objetos, perfiles de seguridad y reglas de NAT con las que se cuente en los firewalls, de manera que se realice un estimado más certero del esfuerzo necesario para llevar a cabo la instalación, configuración y puesta a punto de los equipos y el software.
- **SCITUM** entiende que el **CONALEP** indicará el número de usuarios existentes detrás del firewall, así como la cantidad de segmentos de red a proteger.

CAPACITACIÓN

- Incluirá dos cursos de capacitación del Firewall para al menos cuatro personas.
- Impartidos en las instalaciones de Oficinas Nacionales del **CONALEP**, avalados por el fabricante, con una duración mínima de 40 horas.
- Los cursos de capacitación incluirán la operación, administración y configuración de los bienes propuestos.
- La fecha en que se realizará la capacitación será definida entre **SCITUM** y el **CONALEP**.

LUGAR, FECHA Y CONDICIONES DE ENTREGA

SCITUM, en caso de resultar adjudicado, prestará el "Servicio de seguridad perimetral para la red local de Oficinas Nacionales" en los sitios que el **CONALEP** determine, con base a lo establecido en el Anexo 1. "Descripción técnica del arrendamiento".

Fecha: El servicio se proveerá de acuerdo con lo establecido en el Anexo 1. "Descripción técnica del arrendamiento", ajustado al contrato marco para el "Arrendamiento de equipo de seguridad Firewall y NAC para las Dependencias y Entidades de la Administración Pública Federal", a partir del día siguiente a la notificación del fallo y hasta el 31 de diciembre de 2025.

	Condiciones de entrega: **SCITUM**, en caso de resultar adjudicado, entregará el servicio con base a lo establecido en el Anexo 1. "Descripción técnica del arrendamiento" y podrá incrementarse hasta en un 20% la cantidad del servicio prestado, conforme al artículo 52 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), previa aceptación de **SCITUM**, en caso de resultar adjudicado, sobre el incremento. **FORMA DE ADJUDICACIÓN** **SCITUM**, entiende que el procedimiento contempla una partida como se indica en el Anexo 1. "Descripción técnica del arrendamiento", y la adjudicación se realizará por partida completa a un solo proveedor, que oferte el precio más bajo o las mejores condiciones para el **CONALEP**. **TRANSICIÓN DEL ARRENDAMIENTO** Treinta días naturales previos al término del contrato, **SCITUM**, en caso de resultar adjudicado, y el **CONALEP** acordaran el proceso de transición del retiro controlado de los equipos utilizados para el arrendamiento, con la finalidad de que no se afecte la operación y los niveles de servicio requeridos por el **CONALEP** correspondiente en el presente anexo técnico. Derivado de lo anterior, **SCITUM**, en caso de resultar adjudicado, se obliga a: a) Participar en las reuniones que soliciten las Dependencias o Entidades para realizar la transición con **SCITUM**, en caso de resultar el proveedor adjudicado al final del contrato. b) Durante este proceso de transición **SCITUM** seguirá prestando el arrendamiento por un periodo máximo de 90 días naturales sin costo para el **CONALEP** a partir de la conclusión del contrato, el que podrá ser reducido en la medida que el nuevo Proveedor que resulte adjudicado implemente el servicio. c) En caso de recisión del contrato del servicio objeto del presente anexo técnico, este no podrá ser suspendido hasta que se asegure la transición en los términos previstos en el párrafo que antecede d) Al concluir el periodo de transición, **SCITUM** retirará sus equipos dentro de los 15 días natura es siguientes. **FORMA DE PAGO** El pago se realizará a mes vencido por partida completa, toda vez realizado el servicio a entera satisfacción del **CONALEP**, previa revisión y validación del cumplimiento del servicio por parte del Titular de la Dirección de Tecnologías, como administrador del contrato, o por quien este designe, en un plazo no mayor a 20 días naturales posteriores a la presentación del CFDI "Comprobante Fiscal Digital a través de Internet" (anteriormente factura) correspondiente la cual deberá contener todos los requisitos fiscales vigentes, de conformidad con lo establecido en el Artículo 51 de la Ley de Adquisiciones, Arrendamientos y Servicios del Sector Público (LAASSP), siempre y cuando reúna todos los requisitos establecidos por el Código Fiscal de la Federación y esté debidamente requisitada.

	SCITUM comprende que lo anterior, quedará condicionado proporcionalmente al pago que **SCITUM** como proveedor del arrendamiento deba efectuar por concepto de penas convencionales o deducciones con motivo del incumplimiento parcial o total al mes correspondiente, en que pudiera incurrir respecto a la prestación del servicio. Para el presente procedimiento queda especificado que el pago por el arrendamiento comenzará a correr a partir del siguiente día hábil de que el equipo en arrendamiento quede debidamente configurado y en operación, a entera satisfacción del **CONALEP**. **PENAS CONVENCIONALES Y DEDUCTIVAS** **En el arrendamiento:** **SCITUM**, en caso de resultar adjudicado, se obliga a pagar al **CONALEP** una pena convencional del 2% sobre el monto mensual del pago previsto para los equipos no entregados, instalados, configurados y puestos en marcha, conforme a lo descrito en el apartado "ENTREGABLES" del Anexo 1. "Descripción técnica del arrendamiento" por cada día natural de atraso para la respectiva contratación. **SCITUM** comprende que la misma pena se aplicará en el caso de no proporcionar la mesa de ayuda en el plazo establecido en el apartado "Mesa de ayuda", y no presentar lo señalado en el apartado "Entregables" en el plazo establecido; por cada día natural de atraso. El total de la pena convencional no podrá exceder el montó de la garantía de cumplimiento sin considerar el impuesto al valor agregado (I.V.A), de conformidad con lo establecido en el artículo 53 de la LAASSP. **En los entregables:** **SCITUM**, en caso de resultar adjudicado, se obliga a pagar al **CONALEP** una pena convencional por no presentar los entregables mensuales en los plazos establecidos en el apartado "ENTREGABLES" del Anexo 1. "Descripción técnica del arrendamiento". Dicha pena será del 2% del valor del costo mensual del arrendamiento del equipo, por cada día natural de atraso. El total de la pena convencional no podrá exceder el monto de la garantía de cumplimiento sin considerar el impuesto al valor agregado (I.V.A.), de conformidad con lo establecido en el artículo 53 de la LAASSP. **Deductivas** Se aplicará una deductiva a **SCITUM** por el cumplimiento parcial o deficiente en el arrendamiento. Dicha deductiva será del 2% sobre el monto de la facturación del mes inmediato anterior correspondiente al equipo que no sea sustituido o reparado en los términos y plazos establecidos en el presente anexo por cada día natural de atraso. Lo anterior, de conformidad en lo establecido en el artículo 53 bis de la LAASSP.

	Igual porcentaje, se aplicará como deductiva en los casos que el oferente suspenda el arrendamiento por cualquier causa injustificada, esto es fuera de los casos de fuerza mayor o caso fortuito debidamente acreditado y documentado en términos de la normatividad aplicable, por cada día natural que suspenda el arrendamiento, independientemente de que no se pagaría arrendamiento por el tiempo que dure la suspensión. Adicional a lo anterior, se aplicarán deductivas por cada día natural de incumplimiento en los tiempos de atención y solución de fallas o la petición de la reasignación o reubicación de equipos, así como en los niveles de atención señalados en el apartado "Niveles de atención". En caso de que los conceptos en los que subsistan el cumplimiento parcial o la deficiencia sean equivalentes al importe de la garantía otorgada por SCITUM como proveedor del arrendamiento, el Administrador del Contrato podrá optar por cancelar total o parcialmente el arrendamiento aplicando la pena convencional máxima a SCITUM, lo anterior, en términos del artículo 100 del Reglamento de la Ley antes citada, o bien, optar por rescindir el contrato en término de la Ley. **GARANTÍA DE CUMPLIMIENTO Y CARTAS ADICIONALES (PARA SCITUM EN CASO DE SER EL LICITANTE ADJUDICADO)** 1. Las obligaciones derivadas de la suscripción del contrato respectivo serán garantizadas por **SCITUM** en caso de ser adjudicado mediante la entrega de una póliza de fianza expedida por una institución autorizada en los términos de las disposiciones aplicables, a favor del Colegio Nacional de Educación Profesional Técnica; dicha garantía será constituida por el 10% del monto total del contrato, de conformidad con los Artículos 81 fracción II y 85 fracción III del Reglamento de la LAASSP. • La garantía será entregada dentro de los 10 días naturales siguientes a la fecha de firma del contrato respectivo. Para la expedición de la fianza se observará el texto que se entregará a **SCITUM** en caso de ser el licitante adjudicado. • La garantía de cumplimiento del contrato será indivisible. 2. **SCITUM** en caso de ser el licitante adjudicado a la entrega de los bienes arrendados, presentará el escrito al que alude la Regla 9 "FORMATO PARA DAR CUMPLIMIENTO A LA REGLA 9 DE LAS REGLAS PARA LA DETERMINACIÓN, ACREDITACIÓN Y VERIFICACIÓN DEL CONTENIDO NACIONAL DE LOS BIENES QUE SE OFERTAN Y ENTREGAN EN LOS PROCEDIMIENTOS DE CONTRATACIÓN, ASÍ COMO LAAPLICACIÓN DEL REQUISITO DE CONTENIDO NACIONAL EN LA CONTRATACIÓN DE OBRAS PÚBLICA", a fin de ratificar la manifestación que presenta en su propuesta referente a la Regla No. 8 del grado de contenido nacional de los bienes ofertados, por lo que el área encargada de recibir los bienes conservará documentos originales y proporcionará copia al área contratante a efecto de que exista evidencia en el expediente de contratación.

3. **SCITUM** en caso de ser el licitante adjudicado presentará carta en papel membretado con firma autógrafa (no rúbrica), en el formato que le proporcione el CONALEP, en la que se compromete a cumplir satisfactoriamente con las especificaciones requeridas en el texto de la convocatoria y sus anexos están libres de defectos y vicios ocultos, y en caso de ser adjudicado, el arrendamiento cumplirá con las mismas características a las ofertadas.

CONFIDENCIALIDAD
SCITUM presenta en su propuesta técnica carta en papel membretado firmada por el representante legal, donde se compromete a mantener absoluta confidencialidad de la información a la cual tengan acceso siendo responsable de cada uno de los integrantes del personal asignado para el desarrollo y operación del proyecto, respetando el manejo correcto de la información.

Toda la información a que tenga acceso el personal que SCITUM, en caso de resultar adjudicado, designe para el cumplimiento del contrato, es considerada de carácter confidencial.

RESPONSABILIDAD LABORAL
SCITUM se constituye como único patrón del personal que ocupe para llevar a cabo las acciones derivadas del presente procedimiento de contratación y será el único responsable de las obligaciones que en virtud de disposiciones legales y demás ordenamientos en materia de trabajo y seguridad social, les deriven frente a dicho personal, liberando a **EL CONALEP** de cualquier responsabilidad laboral al respecto.

COTIZACIÓN
SCITUM, cotiza por precios unitarios sin incluir el I.V.A. y en moneda nacional (pesos mexicanos), conforme al presente anexo técnico y a los formatos que se acompañan.

Las cotizaciones se presentan por precios unitarios considerando los costos por periodos mensuales de acuerdo con las tablas del anexo técnico de las presentes bases

VIGENCIA DE LA CONTRATACIÓN
A partir del día siguiente hábil de la notificación del fallo al 31 de diciembre de 2025

ATENTAMENTE

Edgar Hernández Soto
Apoderado Legal de Scitum, S.A. de C.V.

REFERENCIAS TÉCNICAS

CIUDAD DE MÉXICO, A 8 DE JULIO DE 2025

COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA
PRESENTE.

CON RELACIÓN A LA **INVITACIÓN A CUANDO MENOS TRES PERSONAS NACIONAL ELECTRÓNICA No. IA-11-L5X-011L5X001-N-25-2025 "SERVICIO DE SEGURIDAD PERIMETRAL PARA LA RED LOCAL DE OFICINAS NACIONALES"**

EDGAR HERNÁNDEZ SOTO, ME PERMITO SOMETER A SU CONSIDERACIÓN LAS SIGUINETES REFERENCIAS TÉCNICAS:

FUNCIONALIDADES Y/O CARACTERÍSTICAS REQUERIDAS	NOMBRE DEL ARCHIVO	TITULO INTERNO DEL DOCUMENTO	TRADUCCIÓN SIMPLE TITULO INTERNO DEL DOCUMENTO	PAGINA DEL ARCHIVO	PARRAFO DE REFERENCIA	TRADUCCIÓN SIMPLE AL ESPAÑOL
Firewall tipo 1						
SCITUM considera el siguiente equipamiento: Modelo USG6635F de la Marca HUAWEI						
El equipamiento deberá incluir como mínimo los elementos de hardware, software y funcionalidades requeridas en el presente anexo técnico. Para garantizar la operación de seguridad de red, el proveedor deberá ofertar en su propuesta, soluciones en las que el fabricante esté ubicado y reconocido dentro de los cuadrantes de Gartner más reciente divulgado a la fecha de inicio del procedimiento de contratación, o en algún otro reporte reconocido por la industria a nivel internacional.	GartnerReprint.pdf		Cuadrante Mágico para Firewalls de Red	12, 13	Huawei Huawei is a Challenger in this Magic Quadrant. A large product portfolio makes Huawei a desirable vendor for customers who want to consolidate. Huawei has different fi rewalls for different use cases. It often wins deals based on its price/performance. Huawei is a large infrastructure vendor with a diverse product portfolio. Its fi rewalls, which include the USG series for enterprise and the Eudemon series for carriers, are part of its network security product portfolio. Major updates in 2022 relating to Huawei's firewalls have included enhancements to routing, SD-WAN and sandboxing capabilities.	Huawei Huawei es un retador en este Cuadrante Mágico. Una amplia cartera de productos convierte a Huawei en un proveedor deseable para los clientes que desean consolidarse. Huawei tiene diferentes firewalls para diferentes casos de uso. A menudo consigue acuerdos en función de su precio/rendimiento. Huawei es un gran proveedor de infraestructura con una cartera de productos diversa. Sus cortafuegos, que incluyen la serie USG para empresas y la serie Eudemon para operadores, forman parte de su cartera de productos de seguridad de red. Las principales actualizaciones en 2022 relacionadas con los firewalls de Huawei incluyeron mejoras en las capacidades de enrutamiento, SD-WAN y sandboxing.
Funcionalidades de los equipos Firewall	N/A	N/A	N/A	N/A	N/A	N/A

I. Control de políticas	N/A	N/A	N/A	N/A	N/A	N/A
Permite a los usuarios configurar políticas de seguridad en función del tiempo, grupo de usuarios/grupo de seguridad, protocolo de capa de aplicación, ubicación geográfica, dirección IP, puerto, grupo de nombre de dominio, categoría de URL, tipo de acceso, tipo de terminal y grupo de dispositivos.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Security policy management Supports traffic management and control based on the VLAN ID, 5-tuple, security zone, region, application, and time range, and implements integrated content security inspection. Provides predefined templates for common attack defense scenarios to facilitate security policy deployment. Supports interworking with third-party policy management software (FireMon and Algosec) to facilitate security O&M.	Gestión de políticas de seguridad Admite la gestión y el control del tráfico según el ID de VLAN, 5-tuplas, zona de seguridad, región, aplicación y rango de tiempo, e implementa una inspección de seguridad de contenido integrada. Proporciona plantillas predefinidas para escenarios comunes de defensa contra ataques, lo que facilita la implementación de políticas de seguridad. Admite la interconexión con software de gestión de políticas de terceros (FireMon y Algosec) para facilitar las operaciones y el mantenimiento de la seguridad.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Application identification and control Application identification based on signatures, correlation, and behaviors instead of ports; 6000+ preset applications, which can be further classified; support for user-defined applications; 50+ categories and 20+ risk labels for access control based on categories and labels; automatic update of the application identification signature database	Identificación y control de aplicaciones Identificación de aplicaciones basada en firmas, correlación y comportamientos en lugar de puertos; más de 6000 aplicaciones predefinidas con clasificación adicional; compatibilidad con aplicaciones definidas por el usuario; más de 50 categorías y más de 20 etiquetas de riesgo para el control de acceso basadas en categorías y etiquetas; actualización automática de la base de datos de firmas de identificación de aplicaciones.

	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	WEB Security The URL category database on the cloud contains 500 million URLs in over 130 categories, such as news, games, gambling, drugs, and malicious web pages. URLs cover over 100 languages, and key categories of URLs cover over 20 languages. The URL category query servers are deployed in multiple countries/regions to provide high-speed and low-latency category query services. User-defined URL/host whitelist and blacklist are supported. HTTPS traffic can be filtered without decryption. TLS/SSL traffic can be decrypted before filtering. HTTP/2 and QUIC traffic can be filtered, and URL categories can be imported in batches. URL access can be controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors.	Seguridad WEB La base de datos de categorías de URL en la nube contiene 500 millones de URL en más de 130 categorías, como noticias, juegos, apuestas, drogas y páginas web maliciosas. Las URL abarcan más de 100 idiomas, y las categorías clave de URL abarcan más de 20. Los servidores de consulta de categorías de URL están implementados en varios países y regiones para ofrecer servicios de consulta de categorías de alta velocidad y baja latencia. Se admiten listas blancas y negras de URL/host definidas por el usuario. El tráfico HTTPS se puede filtrar sin descifrar. El tráfico TLS/SSL se puede descifrar antes del filtrado. El tráfico HTTP/2 y QUIC se puede filtrar, y las categorías de URL se pueden importar por lotes. El acceso a las URL se puede controlar en función de usuarios/grupos de usuarios, intervalos de tiempo y zonas de seguridad para gestionar con precisión el comportamiento en línea de los usuarios.
Deben de ser capaces de manejar protocolos tales como RADIUS o KERBEROS.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	10	USER authentication Supports multiple authentication modes for Internet access users, including local Portal authentication and single sign-on (SSO). In local Portal authentication, the built-in Portal page of the device can be pushed to users, and the account and password entered on the Portal page by a user can be sent to the local database or RADIUS, HWTACACS, AD, or LDAP authentication server for authentication. SSO includes RADIUS SSO and Agile Controller (NCE-Campus) SSO.	Autenticación de USUARIO Admite múltiples modos de autenticación para usuarios con acceso a Internet, incluyendo la autenticación local del Portal y el inicio de sesión único (SSO). En la autenticación local del Portal, se puede enviar a los usuarios la página del Portal integrada del dispositivo, y la cuenta y la contraseña introducidas en ella se pueden enviar a la base de datos local o al servidor de autenticación RADIUS, HWTACACS, AD o LDAP para su autenticación. El SSO incluye RADIUS SSO y Agile Controller (NCE-Campus).
II. Enrutamiento	N/A	N/A	N/A	N/A	N/A	N/A
Admite rutas estáticas protocolos de enrutamiento dinámicos como RIP, OSPF, BGP e IS-IS en sus últimas versiones estables.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	4	Provides dynamic and static intelligent traffic steering based on multi-egress links, selects the outbound interface based on the specified link bandwidth, weight, or priority, forwards traffic to each link based on the specified traffic steering mode, and dynamically tunes the link selection result in real time to maximize the usage of link resources and improve user experience.	Proporciona direccionamiento inteligente de tráfico dinámico y estático basado en enlaces multisalida, selecciona la interfaz de salida según el ancho de banda, el peso o la prioridad del enlace especificados, reenvía el tráfico a cada enlace según el modo de direccionamiento de tráfico especificado y ajusta dinámicamente el resultado de la selección de enlace en tiempo real para maximizar el uso de los recursos del

						enlace y mejorar la experiencia del usuario.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	Routing Supports multiple types of IPv4/IPv6 routing protocols, such as RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.	Enrutamiento Compatible con múltiples tipos de protocolos de enrutamiento IPv4/IPv6, como RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+ e IPv6 IS-IS.
El enrutamiento basado en políticas admite las siguientes condiciones coincidentes: dirección IP de origen, dirección IP de destino, tipo de servicio, tipo de aplicación, usuario/grupo de usuarios/grupo de seguridad, interfaz de entrada y prioridad DSCP.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	Intelligent uplink selection Supports service-specific PBR and intelligently selects the optimal link based on multiple types of load balancing criteria (such as the bandwidth ratio and link health status) in multi-ISP scenarios.	Selección inteligente de enlace ascendente Compatible con PBR específico del servicio y selecciona inteligentemente el enlace óptimo según diversos criterios de balanceo de carga (como la relación de ancho de banda y el estado del enlace) en escenarios con múltiples ISP.
	DSCP_Ingles.pdf	Creating a Customized Application	Creación de una aplicación personalizada	1	Advance Rule FPI based on advanced ACL rules: Rules are created based on 5-tuple and DSCP information. The 5-tuple information includes the protocol type, source IP address, destination IP address, source port number, and destination port number of a packet. If you know the 5-tuple and DSCP information of service packets, you can configure rules based on 5-tuple and DSCP information to identify these packets. When you use this method to configure a customized application rule, at least one of the source IP address, destination IP address, source port, destination port, and DSCP information must be configured.	Regla avanzada FPI basada en reglas ACL avanzadas: Las reglas se crean con base en información de 5-tuplas y DSCP. Esta información incluye el tipo de protocolo, la dirección IP de origen, la dirección IP de destino, el número de puerto de origen y el número de puerto de destino de un paquete. Si conoce la información de 5-tuplas y DSCP de los paquetes de servicio, puede configurar reglas basadas en dicha información para identificar estos paquetes. Al utilizar este método para configurar una regla de aplicación personalizada, se debe configurar al menos la dirección IP de origen, la dirección IP de destino, el puerto de origen, el puerto de destino y la información DSCP.

Deberá de soportar la encapsulación de tráfico IPv4 e IP6.	HiSecEngine USG6600F_Ingles.pdf	HiSecEngine USG6600F Series AI Firewalls	Cortafuegos con IA de la serie USG6600F de HiSecEngine	2	HiSecEngine USG6600F Series AI Firewalls Huawei HiSecEngine USG6600F Series Artificial Intelligence (AI) Firewalls are designed for next generation data centers at the network edge. Based on new software and hardware platforms, the series provides Internet Protocol version 4 (IPv4)/IPv6 dual-stack capabilities, greatly improving service performance, with intelligent technologies further helping to effectively defend against today's advanced threats.	Cortafuegos con IA HiSecEngine serie USG6600F Los cortafuegos con IA (IA) Huawei HiSecEngine serie USG6600F están diseñados para centros de datos de última generación en el borde de la red. Basados en nuevas plataformas de software y hardware, estos cortafuegos ofrecen capacidades de doble pila IPv4/IPv6, lo que mejora considerablemente el rendimiento del servicio. Además, las tecnologías inteligentes contribuyen a una defensa eficaz contra las amenazas avanzadas actuales.
Protocolos Avanzados de VPN	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	3	A wide range of network features Huawei HiSecEngine USG6000F series also provides various network features such as VPN, IPv6, and intelligent traffic steering. Provides various VPN features such as IPsec VPN and SSL VPN, and supports multiple encryption algorithms, such as DES, 3DES, AES, and SHA, ensuring secure and reliable data transmission.	Amplia gama de funciones de red La serie Huawei HiSecEngine USG6000F también ofrece diversas funciones de red como VPN, IPv6 y direccionamiento inteligente del tráfico. Ofrece diversas funciones de VPN, como VPN IPsec y VPN SSL, y admite múltiples algoritmos de cifrado, como DES, 3DES, AES y SHA, lo que garantiza una transmisión de datos segura y fiable.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	VPN encryption Supports various highly reliable VPN features, such as IPsec VPN, SSL VPN, and GRE, and multiple encryption algorithms, such as DES, 3DES, AES, SHA, SM2, SM3, and SM4.	Cifrado VPN Admite diversas funciones VPN de alta fiabilidad, como IPsec VPN, SSL VPN y GRE, y múltiples algoritmos de cifrado, como DES, 3DES, AES, SHA, SM2, SM3 y SM4.
III. Especificaciones IKE Versión 1, Versión 2	N/A	N/A	N/A	N/A	N/A	N/A

Modo de Negociación: automático, Main, Aggressive (soportado unicamente en topología hub and spoke star)	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	10	Secure SD-WAN Provides a built-in secure SD-WAN solution for low-cost and business-level Internet links. Supports zero-touch provisioning (ZTP) through email to complete device provisioning in minutes without requiring technical skills. Supports forward error correction (FEC) to prevent pixelated display and video freezing at a 30% packet loss rate; supports real-time link switching based on link quality ensure key application experience. Supports multi-link routing and dual-CPE flexible networking to ensure uninterrupted connections for site services; supports E2E IPsec encryption to ensure secure service transmission. Note: The USG6600F series can function as a hub or spoke.	SD-WAN segura Proporciona una solución SD-WAN segura integrada para enlaces de Internet de bajo coste y a nivel empresarial. Admite aprovisionamiento sin intervención (ZTP) a través de correo electrónico para completar el aprovisionamiento de dispositivos en minutos sin necesidad de conocimientos técnicos. Admite corrección de errores de reenvío (FEC) para evitar la visualización pixelada y el congelamiento de vídeo con una tasa de pérdida de paquetes del 30 %; admite conmutación de enlaces en tiempo real basada en la calidad del enlace para garantizar una experiencia de aplicación clave. Admite enrutamiento multienlace y redes flexibles de doble CPE para garantizar conexiones ininterrumpidas para los servicios del sitio; admite cifrado IPsec de extremo a extremo para garantizar la transmisión segura del servicio. Nota: La serie USG6600F puede funcionar como concentrador o radio.
	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	36	Negotiation Mode This parameter is only available when Version is set to v1. You can set Negotiation Mode to Main or Aggressive. The default mode is Main.	Modo de negociación Este parámetro solo está disponible cuando la versión está configurada en v1. Puede configurar el modo de negociación como Principal o Agresivo. El modo predeterminado es Principal.
	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	61	Negotiation Mode This parameter is available only when Version is v1. • Main • Aggressive	Modo de negociación: Este parámetro solo está disponible si la versión es v1. • Principal • Agresivo

Encriptación: AES-256, AES-192, AES-128, 3DES, DES	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual, Guía del usuario	61	Encryption Algorithm Encryption algorithm. The following options are available: • 3DES(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-256(Insecure. Not recommended.) • AES-128-GCM-16 • AES-256-GCM-16 When this encryption algorithm is used, the IKE version can only be v2. The default value is AES-128.	Algoritmo de cifrado: Algoritmo de cifrado. Están disponibles las siguientes opciones: • 3DES (Inseguro. No recomendado) • AES-128 (Inseguro. No recomendado) • AES-192 (Inseguro. No recomendado) • AES-256 (Inseguro. No recomendado) • AES-128-GCM-16 • AES-256-GCM-16 Cuando se utiliza este algoritmo de cifrado, la versión de IKE solo puede ser v2. El valor predeterminado es AES-128
Autenticación: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	61	Authentication Algorithm Hash algorithm used for authentication. The following options are available: • SHA1(Insecure. Not recommended.) • MD5(Insecure. Not recommended.) • SHA2-256 • SHA2-384 • SHA2-512 The default value is SHA2-256.	Algoritmo de autenticación: Algoritmo hash utilizado para la autenticación. Están disponibles las siguientes opciones: • SHA1 (Inseguro. No recomendado) • MD5 (Inseguro. No recomendado) • SHA2-256 • SHA2-384 • SHA2-512 El valor predeterminado es SHA2-256.
Integridad Hash: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5, AES	Config IPSEC	Configuring Point-to-Point Ipsec	Configuración de IPsec punto a punto	9	The 3DES, AES-128, AES-128-GCM-128, AES-128-GMAC, AES-192, AES-192-GCM-128, AES-192-GMAC, AES-256, AES-256-GCM-128, AES- 256-GMAC, AES-GCM-128, AES-GCM-192, AES-GCM-256, AES-XCBC-128, AES-XCBC-96, DES, GROUP1, GROUP14, GROUP15, GROUP16, GROUP18, GROUP19, GROUP2, GROUP20, GROUP21, GROUP24, GROUP5, HMAC-MD5, HMAC-MD5-96, HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, MD5, PKCS1, PSS, SHA1, SHA2-256, SHA2-384, SHA2-512, SM3 and SM4 security algorithms can be configured only after the weak security algorithm and protocol software package WEAKEA is installed.	El 3DES, AES-128, AES-128-GCM-128, AES-128-GMAC, AES-192, AES-192-GCM-128, AES-192-GMAC, AES-256, AES-256-GCM-128, AES-256-GMAC, AES-GCM-128, AES-GCM-192, AES-GCM-256, AES-XCBC-128, AES-XCBC-96, DES, GRUPO1, GRUPO14, GRUPO15, GRUPO16, GRUPO18, GRUPO19, GRUPO2, GRUPO20, GRUPO21, GRUPO24, GRUPO5, HMAC-MD5, HMAC-MD5-96, HMAC-SHA1, Los algoritmos de seguridad HMAC-SHA1-96, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, MD5, PKCS1, PSS, SHA1, SHA2-256, SHA2-384, SHA2-512, SM3 y SM4 se pueden configurar solo después de instalar el paquete de software de protocolo y algoritmo de seguridad débil WEAKEA.

PRF: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5, AES-128	PRF.pdf	PRF	PRF	1	prf Function The prf command configures the pseudo-random function (PRF) algorithm used in IKEv2 negotiation. The undo prf command restores the default configuration. By default, the HMAC-SHA2-256 PRF algorithm is used in IKEv2 negotiation. aes-xcbc-128 Indicates the AES-XCBC-128 authentication algorithm. This algorithm applies only to IKEv2 negotiation. hmac-md5 Indicates the HMAC-MD5 authentication algorithm. hmac-sha1 Indicates the HMAC-SHA1 authentication algorithm. hmac-sha2-256 Indicates the HMAC-SHA2-256 authentication algorithm. hmac-sha2-384 Indicates the HMAC-SHA2-384 authentication algorithm. hmac-sha2-512 Indicates the HMAC-SHA2-512 authentication algorithm.	prf Función El comando prf configura el algoritmo de función pseudoaleatoria (PRF) utilizado en la negociación IKEv2. El comando undo prf restaura la configuración predeterminada. De forma predeterminada, se utiliza el algoritmo PRF HMAC-SHA2-256 en la negociación IKEv2. aes-xcbc-128 Indica el algoritmo de autenticación AES-XCBC-128. Este algoritmo solo se aplica a la negociación IKEv2. hmac-md5 Indica el algoritmo de autenticación HMAC-MD5. hmac-sha1 Indica el algoritmo de autenticación HMAC-SHA1. hmac-sha2-256 Indica el algoritmo de autenticación HMAC-SHA2-256. hmac-sha2-384 Indica el algoritmo de autenticación HMAC-SHA2-384. hmac-sha2-512 Indica el algoritmo de autenticación HMAC-SHA2-512.
Grupo DH: 1,2,5,14,15,16,18,19,20,21	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	62	DH Algorithm The following algorithms are supported: • Group 1(Insecure. Not recommended.) • Group 2(Insecure. Not recommended.) • Group 5(Insecure. Not recommended.) • Group 14(Insecure. Not recommended.) • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 The default value is Group 15.	Algoritmo DH: Se admiten los siguientes algoritmos: • Grupo 1 (Inseguro. No recomendado) • Grupo 2 (Inseguro. No recomendado) • Grupo 5 (Inseguro. No recomendado) • Grupo 14 (Inseguro. No recomendado) • Grupo 15 • Grupo 16 • Grupo 19 • Grupo 20 • Grupo 21 El valor predeterminado es el Grupo 15.
IV. Especificaciones IPSec	N/A	N/A	N/A	N/A	N/A	N/A

I. Cuenta con Modo de encapsulación: Automático, Transport, Tunnel	encapsulation mode	encapsulation-mode	modo de encapsulación	1	encapsulation-mode Function The encapsulation-mode command sets the IPsec encapsulation mode. The undo encapsulation-mode command restores the default IPsec encapsulation mode. By default, the tunnel mode is used. Format encapsulation-mode { transport | tunnel | auto } undo encapsulation-mode Parameters transport Encapsulates IP packets in transport mode. tunnel Encapsulates IP packets in tunnel mode. auto Indicates the auto-sensing mode. The tunnel mode is used if the device serves as the IKE negotiation initiator. If the device serves as the responder, both the tunnel mode and transport mode can be used.	encapsulation-mode Función El comando encapsulation-mode establece el modo de encapsulación de IPsec. El comando undo encapsulation-mode restaura el modo de encapsulación de IPsec predeterminado. De forma predeterminada, se utiliza el modo túnel. Formato encapsulation-mode { transport | tunnel | auto } undo encapsulation-mode Parámetros transport Encapsula los paquetes IP en modo transporte. tunnel Encapsula los paquetes IP en modo túnel. auto Indica el modo de detección automática. El modo túnel se utiliza si el dispositivo actúa como iniciador de la negociación IKE. Si el dispositivo actúa como respondedor, se pueden utilizar tanto el modo túnel como el modo transporte.
II. Protocolo de seguridad: ESP, AH, AH-ESP	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	37	Transfer Protocol Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • AH • ESP • AH-ESP The default protocol is ESP.	Protocolo de transferencia Protocolo de seguridad utilizado en IPsec para transmitir y encapsular datos de usuario. Se admiten los siguientes protocolos: • AH • ESP • AH-ESP El protocolo predeterminado es ESP.

ESP Encriptación: GCM256, GCM192, GCM128, GMAC256, GMAC192, GMAC128, AES-256, AES-192, AES-128, 3DES y DES	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	11	Encryption Algorithm The following encryption algorithms are supported: • AES-256-GCM-16 • AES-128-GCM-16 • AES-256(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • 3DES(Insecure. Not recommended.) By default, the AES-128 algorithm is used.	Algoritmo de cifrado: Se admiten los siguientes algoritmos de cifrado: • AES-256-GCM-16 • AES-128-GCM-16 • AES-256 (Inseguro. No recomendado) • AES-192 (Inseguro. No recomendado) • AES-128 (Inseguro. No recomendado) • 3DES (Inseguro. No recomendado) De forma predeterminada, se utiliza el algoritmo AES-128.
	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	36	Encryption Algorithm Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is AES-128.	Algoritmo de cifrado: Se admiten los siguientes algoritmos: • AES-128 • AES-192 • AES-256 • 3DES (Este algoritmo no es seguro. Tenga cuidado al usarlo). El algoritmo predeterminado es AES-128.
IV. ESP Autenticación: SHA2-512, SHA2-384, SHA2-256, SHA1, MD5	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	36	Authentication Algorithm Hash algorithm used for authentication. The following algorithms are supported: • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512	Algoritmo de autenticación: Algoritmo hash utilizado para la autenticación. Se admiten los siguientes algoritmos: • SHA1 (este algoritmo no es seguro. Tenga cuidado al usarlo). • MD5 (este algoritmo no es seguro. Tenga cuidado al usarlo). • SHA2-256 • SHA2-384 • SHA2-512

	PFS: 1,2,5,14,15,16,18,19,20 y 21	Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	12	PFS Perfect Forward Secrecy (PFS) ensures that the compromise of the keys of an IPsec tunnel does not affect the security of other tunnels by leveraging that the keys of these tunnels are irrelevant to each other. By default, the PFS function is enabled for S2C VPN. Each IPsec VPN connection consists of at least one IPsec tunnel, each of which uses an independent set of keys to protect user traffic. S2C VPN supports the following algorithms: • DH group 1 (This algorithm is insecure. Exercise caution when using it.) • DH group 2 (This algorithm is insecure. Exercise caution when using it.) • DH group 5 (This algorithm is insecure. Exercise caution when using it.) • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21	PFS Perfect Forward Secrecy (PFS) garantiza que la vulneración de las claves de un túnel IPsec no afecte la seguridad de otros túneles, aprovechando que las claves de estos túneles son irrelevantes entre sí. De forma predeterminada, la función PFS está habilitada para S2C VPN. Cada conexión VPN IPsec consta de al menos un túnel IPsec, cada uno de los cuales utiliza un conjunto independiente de claves para proteger el tráfico del usuario. S2C VPN admite los siguientes algoritmos: • Grupo DH 1 (Este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 2 (Este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 5 (Este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 14 • Grupo DH 15 • Grupo DH 16 • Grupo DH 19 • Grupo DH 20 • Grupo DH 21"

		Virtual Private Network.pdf	Virtual Private Network User Guide	Red privada virtual Guía del usuario	37	PFS Perfect Forward Secrecy (PFS) ensures that the compromise of the keys of an IPsec tunnel does not affect the security of other tunnels by leveraging that the keys of these tunnels are irrelevant to each other. By default, the PFS function is enabled for S2C VPN. Each IPsec VPN connection consists of at least one IPsec tunnel, each of which uses an independent set of keys to protect user traffic. S2C VPN supports the following algorithms: • DH group 1 (This algorithm is insecure. Exercise caution when using it.) • DH group 2 (This algorithm is insecure. Exercise caution when using it.) • DH group 5 (This algorithm is insecure. Exercise caution when using it.) • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21	PFS Perfect Forward Secrecy (PFS) garantiza que la vulneración de las claves de un túnel IPsec no afecte la seguridad de otros túneles, aprovechando que las claves de estos túneles son irrelevantes entre sí. De forma predeterminada, la función PFS está habilitada para S2C VPN. Cada conexión VPN IPsec consta de al menos un túnel IPsec, cada uno de los cuales utiliza un conjunto independiente de claves para proteger el tráfico del usuario. S2C VPN admite los siguientes algoritmos: • Grupo DH 1 (Este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 2 (Este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 5 (Este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 14 • Grupo DH 15 • Grupo DH 16 • Grupo DH 19 • Grupo DH 20 • Grupo DH 21"
DPD modos: Periodic, On-oemand	dpd type	dpd type	tipo dpd	1	dpd type Function The dpd type command configures the DPD mode on an IKE peer. The undo dpd type command deletes the DPD mode on an IKE peer. By default, the DPD mode is not configured on an IKE peer. Format dpd type { on-demand | periodic } undo dpd type	"dpd type Función El comando dpd type configura el modo DPD en un par IKE. El comando undo dpd type elimina el modo DPD en un par IKE. De forma predeterminada, el modo DPD no está configurado en un par IKE. Formato dpd type { on-demand | periodic } undo dpd type"	

L2TP	L2TP	HUAWEI Firewall Interoperability Configuration Guide for VPN	Guía de configuración de interoperabilidad del firewall de HUAWEI para VPN	1	Web: Example for Configuring L2TP over IPSec to Allow Users to Acces the Headquarters Using Windows 7 Terminals The LAC client directly initiates a connection request to the LNS. The LAC client and LNS negotiate an IPSec tunnel, and perform L2TP negotiation to authenticate the user's identity and establish an L2TP over IPSec tunnel. The data between the LAC client and the LNS is transmitted through the tunnel. Layer-2 data is encapsulated using L2TP and then the data is encrypted using IPSec. Figure 2-6 Networking diagram for configuring L2TP over IPSec for users to access the headquarters using the Windows L2TP client	"Web: Ejemplo de configuración de L2TP sobre IPSec para permitir el acceso de los usuarios a la sede central mediante terminales Windows 7 El cliente LAC inicia directamente una solicitud de conexión al LNS. El cliente LAC y el LNS negocian un túnel IPSec y realizan la negociación L2TP para autenticar la identidad del usuario y establecer un túnel L2TP sobre IPSec. Los datos entre el cliente LAC y el LNS se transmiten a través del túnel. Los datos de capa 2 se encapsulan mediante L2TP y luego se cifran mediante IPSec. Figura 2-6 Diagrama de red para configurar L2TP sobre IPSec para que los usuarios accedan a la sede central mediante Cliente L2TP de Windows"
L2TP OVER IPSEC	L2TP	HUAWEI Firewall Interoperability Configuration Guide for VPN	Guía de configuración de interoperabilidad del firewall de HUAWEI para VPN	1	Web: Example for Configuring L2TP over IPSec to Allow Users to Acces the Headquarters Using Windows 7 Terminals The LAC client directly initiates a connection request to the LNS. The LAC client and LNS negotiate an IPSec tunnel, and perform L2TP negotiation to authenticate the user's identity and establish an L2TP over IPSec tunnel. The data between the LAC client and the LNS is transmitted through the tunnel. Layer-2 data is encapsulated using L2TP and then the data is encrypted using IPSec. Figure 2-6 Networking diagram for configuring L2TP over IPSec for users to access the headquarters using the Windows L2TP client	"Web: Ejemplo de configuración de L2TP sobre IPSec para permitir el acceso de los usuarios a la sede central mediante terminales Windows 7 El cliente LAC inicia directamente una solicitud de conexión al LNS. El cliente LAC y el LNS negocian un túnel IPSec y realizan la negociación L2TP para autenticar la identidad del usuario y establecer un túnel L2TP sobre IPSec. Los datos entre el cliente LAC y el LNS se transmiten a través del túnel. Los datos de capa 2 se encapsulan mediante L2TP y, posteriormente, se cifran mediante IPSec. Figura 2-6 Diagrama de red para configurar L2TP sobre IPSec para que los usuarios accedan a la sede central mediante el cliente L2TP de Windows"
GRE	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	VPN encryption Supports various highly reliable VPN features, such as IPsec VPN, SSL VPN, and GRE, and multiple encryption algorithms, such as DES, 3DES, AES, SHA, SM2, SM3, and SM4.	"Cifrado VPN Admite diversas funciones VPN de alta fiabilidad, como VPN IPsec, VPN SSL y GRE, y múltiples algoritmos de cifrado, como DES, 3DES, AES, SHA, SM2, SM3 y SM4."

	MULTIPOINT GRE	DSVPN.pdf	What Is DSVPN	¿Qué es DSVPN?	1	Dynamic Smart Virtual Private Network (DSVPN), which Cisco calls DMVPN, works in conjunction with Multipoint Generic Routing Encapsulation (mGRE) and Next Hop Resolution Protocol (NHRP)to establish dynamic full-mesh VPNs between branches andbetween branches and the headquarters (HQ). Compared withtraditional VPN technologies, DSVPN simplifies the HQ'sconfiguration and O&M when new branches join the network,making network expansion easy. It helps realize directcommunication between branches, improving transmissionefficiency by avoiding delays caused by HQ pass-through.Additionally, DSVPN supports dynamic public addresses atbranches, eliminating the need to purchase static public addressesand thereby reducing network construction costs	La Red Privada Virtual Inteligente Dinámica (DSVPN), que Cisco denomina DMVPN, funciona en conjunto con la Encapsulación de Enrutamiento Genérico Multipunto (mGRE) y el Protocolo de Resolución de Próximo Salto (NHRP) para establecer VPN dinámicas de malla completa entre sucursales y entre estas y la sede central (HQ). En comparación con las tecnologías VPN tradicionales, DSVPN simplifica la configuración, la operación y el mantenimiento de la sede central cuando nuevas sucursales se incorporan a la red, lo que facilita su expansión. Facilita la comunicación directa entre sucursales, mejorando la eficiencia de la transmisión al evitar los retrasos causados por el paso a la sede central. Además, DSVPN admite direcciones públicas dinámicas en las sucursales, lo que elimina la necesidad de adquirir direcciones públicas estáticas y, por lo tanto, reduce los costos de construcción de la red.
	V. Identificación de aplicaciones	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Bandwidth management Manages per-IP bandwidth based on service application identification to guarantee the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.	Gestión del ancho de banda Gestiona el ancho de banda por IP basándose en la identificación de la aplicación de servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y modificando la prioridad de reenvío de aplicaciones.
		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Application identification and control Application identification based on signatures, correlation, and behaviors instead of ports; 6000+ preset applications, which can be further classified; support for user-defined applications; 50+ categories and 20+ risk labels for access control based on categories and labels; automatic update of the application identification signature database	Identificación y control de aplicaciones Identificación de aplicaciones basada en firmas, correlación y comportamientos en lugar de puertos; más de 6000 aplicaciones predefinidas con clasificación adicional; compatibilidad con aplicaciones definidas por el usuario; más de 50 categorías y más de 20 etiquetas de riesgo para el control de acceso basadas en categorías y etiquetas; actualización automática de la base de datos de firmas de identificación de aplicaciones.
	V. Identificación de aplicaciones IPV6	N/A	N/A	N/A	N/A	N/A	N/A

Soportar el protocolo IPv6.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	3	A wide range of network features Huawei HiSecEngine USG6000F series also provides various network features such as VPN, IPv6, and intelligent traffic steering.	Amplia gama de funciones de red La serie Huawei HiSecEngine USG6000F también ofrece diversas funciones de red como VPN, IPv6 y direccionamiento inteligente de tráfico.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	4	Provides secure and rich IPv6 network switchover, policy control, security protection, and service visualization capabilities, helping government, media, carrier, Internet, and finance sectors implement IPv6 reconstruction.	Proporciona conmutación de red IPv6 segura y completa, control de políticas, protección de seguridad y capacidades de visualización de servicios, lo que ayuda a los sectores gubernamentales, de medios de comunicación, operadores, Internet y financiero a implementar la reconstrucción de IPv6.
Compatible con IPv6 sobre túneles GRE de IPv4 y túneles 6R.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	VPN encryption Supports various highly reliable VPN features, such as IPsec VPN, SSL VPN, and GRE, and multiple encryption algorithms, such as DES, 3DES, AES, SHA, SM2, SM3, and SM4.	Cifrado VPN Admite diversas funciones VPN de alta fiabilidad, como VPN IPsec, VPN SSL y GRE, y múltiples algoritmos de cifrado, como DES, 3DES, AES, SHA, SM2, SM3 y SM4.
	IPv6 GRE Tunnel.pdf	NetEngine 8000 M1A V800R023C10SPC500 Configuration Guide	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	1	Configuring an IPv6 GRE Tunnel IPv6 Generic Routing Encapsulation (GRE) provides a mechanism of encapsulating packets of a protocol into packets of another protocol. This allows packets to be transmitted over heterogeneous networks. The channel for transmitting heterogeneous packets is called a tunnel.	Configuración de un túnel GRE IPv6 La encapsulación de enrutamiento genérico (GRE) IPv6 proporciona un mecanismo para encapsular paquetes de un protocolo en paquetes de otro protocolo. Esto permite la transmisión de paquetes a través de redes heterogéneas. El canal para transmitir paquetes heterogéneos se denomina túnel.

		IPv6 IPv4 Tunnel.pf	NE40E V800R022C00SPC600 Configuration Guide	Guía de configuración del NE40E V800R022C00SPC600	1	IPv6 over IPv4 Tunnel Configuration The IPv6 over IPv4 tunneling technology provides a solution for the transition from IPv4 to IPv6. Overview of IPv6 over IPv4 Tunnel Configuration Precautions for IPv6 over IPv4 Tunnel Configuring a Manual IPv6 over IPv4 Tunnel Configuring a 6to4 Tunnel Configuring a 6RD Tunnel Configuration Examples for IPv6 over IPv4 Tunnel Example for Configuring a Manual IPv6 over IPv4 Tunnel Example for Configuring a 6to4 Tunnel Example for Configuring 6to4 Relay Example for Configuring a 6RD Tunnel Example for Configuring a 6RD Relay	Configuración del túnel IPv6 sobre IPv4 La tecnología de tunelización IPv6 sobre IPv4 ofrece una solución para la transición de IPv4 a IPv6. Descripción general del túnel IPv6 sobre IPv4 Precauciones de configuración para el túnel IPv6 sobre IPv4 Configuración manual de un túnel IPv6 sobre IPv4 Configuración de un túnel 6 a 4 Configuración de un túnel 6RD Ejemplos de configuración para el túnel IPv6 sobre IPv4 Ejemplo de configuración manual de un túnel IPv6 sobre IPv4 Ejemplo de configuración de un túnel 6 a 4 Ejemplo de configuración de un relé 6 a 4 Ejemplo de configuración de un túnel 6RD Ejemplo de configuración de un relé 6RD
VI. Control de trafico		N/A	N/A	N/A	N/A	N/A	N/A
Admite políticas de control de tráfico basadas en el protocolo de la capa de aplicación, incluida la configuración del ancho de banda máximo, el ancho de banda garantizado y la prioridad del tráfico del protocolo.		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	Intelligent uplink selection Supports service-specific PBR and intelligently selects the optimal link based on multiple types of load balancing criteria (such as the bandwidth ratio and link health status) in multi-ISP scenarios.	Selección inteligente de enlace ascendente Compatible con PBR específico del servicio y selecciona inteligentemente el enlace óptimo según diversos criterios de equilibrio de carga (como la relación de ancho de banda y el estado del enlace) en escenarios con múltiples ISP.
		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	4	Provides dynamic and static intelligent traffic steering based on multi-egress links, selects the outbound interface based on the specified link bandwidth, weight, or priority, forwards traffic to each link based on the specified traffic steering mode, and dynamically tunes the link selection result in real time to maximize the usage of link resources and improve user experience.	Proporciona direccionamiento inteligente de tráfico, tanto dinámico como estático, basado en enlaces de salida múltiple. Selecciona la interfaz de salida según el ancho de banda, el peso o la prioridad del enlace especificados. Reenvía el tráfico a cada enlace según el modo de direccionamiento de tráfico especificado y ajusta dinámicamente el resultado de la selección de enlace en tiempo real para maximizar el uso de los recursos del enlace y mejorar la experiencia del usuario.

	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Bandwidth Manages per-IP bandwidth based on service application identification to guarantee the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.	Ancho de banda Administra el ancho de banda por IP según la identificación de la aplicación de servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y modificando la prioridad de reenvío de la aplicación.
Admite garantía de ancho de banda basada en usuarios y direcciones IP.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Bandwidth Manages per-IP bandwidth based on service application identification to guarantee the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.	Ancho de banda Administra el ancho de banda por IP según la identificación de la aplicación de servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y modificando la prioridad de reenvío de la aplicación.
Admite el numero máximo de conexiones por dirección IP o usuario.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Bandwidth Manages per-IP bandwidth based on service application identification to guarantee the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.	Ancho de banda Administra el ancho de banda por IP según la identificación de la aplicación de servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y modificando la prioridad de reenvío de la aplicación.
Admite el tráfico basado en la ubicación geográfica y el análisis de amenazas.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Advanced malware prevention The heuristic antivirus engine uses detection technologies such as AI, semantic analysis, and Emulator, coupled with threat and reputation information, to detect packed malware, script morphing, and malware embedded in compound documents. It can detect billions of malware variants and supports automatic update of the signature database. In addition, it can send suspicious files to the local or cloud sandbox for further inspection to detect zero-day malware.	Prevención avanzada de malware El motor antivirus heurístico utiliza tecnologías de detección como IA, análisis semántico y emulador, junto con información sobre amenazas y reputación, para detectar malware empaquetado, mutación de scripts y malware incrustado en documentos compuestos. Puede detectar miles de millones de variantes de malware y admite la actualización automática de la base de datos de firmas. Además, puede enviar archivos sospechosos al entorno de pruebas local o en la nube para una inspección más exhaustiva y detectar malware de día cero.

	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	8	Threat information Huawei Intelligent Security Center leverages multiple AI algorithms and expert analysis to generate massive threat information about IP addresses, domain names, URLs, and files on a daily basis. The threat information is automatically synchronized to devices for threat detection to quickly block emerging attacks. In addition, it can interconnect with third-party threat information sources to enrich inspection rules.	Información sobre amenazas Huawei Intelligent Security Center aprovecha múltiples algoritmos de IA y análisis de expertos para generar diariamente información masiva sobre amenazas: direcciones IP, nombres de dominio, URL y archivos. Esta información se sincroniza automáticamente con los dispositivos para su detección y bloquear rápidamente los ataques emergentes. Además, puede interconectarse con fuentes de información de amenazas de terceros para enriquecer las reglas de inspección.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Bandwidth management Manages per-IP bandwidth based on service application identification to guarantee the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.	Ancho de banda Administra el ancho de banda por IP según la identificación de la aplicación de servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y modificando la prioridad de reenvío de la aplicación.

		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	2	Intelligent defense HiSecEngine USG6000F series AI firewalls provide content security functions, such as application identification, IPS, antivirus, and URL filtering to protect intranet servers and users against threats. HiSecEngine USG6000F series also support to detect unknown threats by interworking with sandbox. Huawei innovatively enables the IPS signature production on the intelligent cloud by adopting intelligence technologies and utilizing expert experience. Such an intelligent mode helps increase the signature productivity by 30 times compared with manual production, reduce errors caused by manual analysis, and continuously improve the accuracy of intrusion detection. The built-in antivirus content-based detection engine (CDE) powered by intelligence technologies can detect unknown threats and provide in-depth data analysis. With these capabilities, the CDE-boosted firewall is able to gain insight into threat activities and quickly detect malicious files, effectively improving the threat detection rate. NGFW USG supports to detect and defend malware spreading and network attacks, like Worm, Virus, Trojan-horse, Spyware, etc. malware spreading and botnet, DoS/DDoS, SQL injection, cross site attack,ransomware,etc.	Defensa inteligente Los firewalls con IA de la serie HiSecEngine USG6000F ofrecen funciones de seguridad de contenido, como identificación de aplicaciones, IPS, antivirus y filtrado de URL, para proteger a los servidores y usuarios de la intranet contra amenazas. La serie HiSecEngine USG6000F también permite detectar amenazas desconocidas mediante la interconexión con entornos seguros. Huawei permite de forma innovadora la generación de firmas IPS en la nube inteligente mediante la adopción de tecnologías de inteligencia artificial y la experiencia de expertos. Este modo inteligente ayuda a aumentar la productividad de las firmas 30 veces en comparación con la generación manual, reduce los errores causados por el análisis manual y mejora continuamente la precisión de la detección de intrusiones. El motor de detección basado en contenido (CDE) antivirus integrado, impulsado por tecnologías de inteligencia artificial, puede detectar amenazas desconocidas y proporcionar un análisis de datos exhaustivo. Con estas capacidades, el firewall con CDE puede obtener información sobre las actividades de las amenazas y detectar rápidamente archivos maliciosos, mejorando eficazmente la tasa de detección de amenazas. El NGFW USG permite detectar y defenderse de la propagación de malware y los ataques de red, como gusanos, virus, troyanos, spyware, etc. Botnets, DoS/DDoS, inyección SQL, ataques entre sitios, ransomware, etc.

		Referencing Regions	Huawei Firewall Security Policy Essentials	Fundamentos de la política de seguridad del firewall de Huawei	1	Referencing Regions and Region Groups in Security Policies A region maps a public IP address to a geographical location, and a region group is a set of regions. Therefore, a region and a region group. You can use regions and region groups to configure security policies based on geographical locations. For example, an enterprise provides denies access from country A for security purposes. In this case, you can configure a security policy with the source address set to country A prevent users in country A from accessing the web service. To simplify user operations, Huawei firewalls provide the geolocation database (pre-defined regions). Pre-defined regions in China can be s pre-defined regions outside China can be set at the country level. The geolocation database is an IP address group divided by country and region. It is collected and maintained by Huawei and can be updat the upgrade center. The geolocation database is not updated in time. Therefore, three user-defined configuration methods are available for defined region is higher than that of a pre-defined region. User-defined region: You can manually create a region and add IP addresses that meet the requirements to it. Adding an IP address to a pre-defined region: If an IP address is missing in a pre-defined region, you can add it to the pre-defined region Excluding an IP address from a pre-defined region: If an IP address is incorrectly classified into a region, you can add the IP address to t region.	Referencia a regiones y grupos de regiones en políticas de seguridad Una región asigna una dirección IP pública a una ubicación geográfica, y un grupo de regiones es un conjunto de regiones. Por lo tanto, se pueden usar regiones y grupos de regiones para configurar políticas de seguridad basadas en ubicaciones geográficas. Por ejemplo, una empresa deniega el acceso desde el país A por motivos de seguridad. En este caso, se puede configurar una política de seguridad con la dirección de origen establecida en el país A para impedir que los usuarios del país A accedan al servicio web. Para simplificar las operaciones del usuario, los firewalls de Huawei proporcionan una base de datos de geolocalización (regiones predefinidas). Las regiones predefinidas en China se pueden configurar a nivel de país. Las regiones predefinidas fuera de China se pueden configurar a nivel de país. La base de datos de geolocalización es un grupo de direcciones IP dividido por país y región. Huawei la recopila y mantiene, y puede actualizarse en el centro de actualizaciones. La base de datos de geolocalización no se actualiza periódicamente. Por lo tanto, hay tres métodos de configuración definidos por el usuario disponibles para una región definida con un nivel superior al de una región predefinida. Región definida por el usuario: Se puede crear manualmente una región y agregar direcciones IP que cumplan los requisitos. Agregar una dirección IP a una región predefinida: Si falta una dirección IP en una región predefinida, puede agregarla. Excluir una dirección IP de una región predefinida: Si una dirección IP se clasifica incorrectamente en una región, puede agregarla a la región predefinida.

		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Bandwidth management Manages per-IP bandwidth based on service application identification to guarantee the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.	Ancho de banda Administra el ancho de banda por IP según la identificación de la aplicación de servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y modificando la prioridad de reenvío de la aplicación.
Soporta la gestión de cuotas de tráfico de usuarios.		QUOTA.pdf	Configuring a Quota Control Policy	Configuración de una política de control decuotas	1	Configuring a Quota Control Policy The quota control policy defines users whose quota needs to be managed, assigns the quota to them, and specify the management and control actions after the quota is exceeded. Prerequisites Users whose quota statistics need to be collected, managed, and controlled have been specified. The quota allocation mode and quota data planning have been clarified based on bandwidth requirements of the enterprise. The quota control policy differs from other policies (such as the security policy and traffic policy) in that if the parameter user of a policy is set to any, this policy applies to all users. Therefore, use this setting with caution to prevent complaints about such network problems as slow or failed to access the Internet at a large scope. Procedure Choose Policy > Quota Control Policy > Quota Control Policy. Click Add. Configure basic information of the quota control policy, including the name, description, tag, user, and time range	Configuración de una política de control de cuotas La política de control de cuotas define los usuarios cuya cuota debe administrarse, les asigna la cuota y especifica las acciones de administración y control una vez excedida. Requisitos Se han especificado los usuarios cuyas estadísticas de cuotas deben recopilarse, administrarse y controlarse. El modo de asignación de cuotas y la planificación de datos de cuotas se han aclarado según los requisitos de ancho de banda de la empresa. La política de control de cuotas se diferencia de otras políticas (como la política de seguridad y la política de tráfico) en que si el parámetro "usuario" de una política se establece en "cualquiera", esta política se aplica a todos los usuarios. Por lo tanto, utilice esta configuración con precaución para evitar quejas sobre problemas de red como acceso lento o fallos de acceso a Internet a gran escala. Procedimiento Seleccione Política > Política de control de cuotas > Política de control de cuotas. Haga clic en Agregar. Configure la información básica de la política de control de cuotas, incluyendo el nombre, la descripción, la etiqueta, el usuario y el intervalo de tiempo.
Soporta traffic shaping.		Traffic Shaping.pdf	Traffic Shaping	Modelado del tráfico	1	Traffic Shaping Traffic shaping adjusts the rate of outgoing traffic to reduce traffic bursts so that outgoing packets can be transmitted at a stable rate. Traffic shaping uses a buffer and token buckets to control the traffic rate. When packets are sent at a high rate, the system buffers packets and then sends them evenly under	Configuración de tráfico La configuración de tráfico ajusta la velocidad del tráfico saliente para reducir las ráfagas de tráfico, de modo que... Los paquetes se pueden transmitir a una velocidad estable. El modelado de tráfico utiliza un búfer y contenedores de tokens para controlar la velocidad del tráfico. Cuando los paquetes se envían a alta velocidad, el

						the control of the token buckets.	sistema los almacena en el búfer y luego los envía uniformemente bajo el control de los contenedores de tokens.
Proporcionar protección y soporte al menos a las siguientes tecnologías de Voz sobre IP: SIP, H.323, H.460, ICE/STUN para tráfico cifrado y calidad de servicio.	Understanding SIP	Understanding SIP ASPF/ALG	Entendiendo SIP ASPF/ALG	1	Understanding SIP ASPF/ALG The Session Initiation Protocol (SIP) is an IETF standard protocol used to create, modify, and release sessions of one or more participants. These sessions can be interactive user sessions that involve multimedia elements such as voice calls, multimedia conferences, and virtual reality. SIP is a multi-channel protocol. In addition to establishing signaling channels for transmitting signaling, the calling and called parties also establish data channels for transmitting media data such as voice and video data. Therefore, SIP traffic is classified into signaling streams and media streams. Signaling streams are transmitted through UDP or TCP, including requests and responses from both parties. Media streams are transmitted through RTP and RTCP, including media (such as voice and video) data packets.	Entendiendo SIP ASPF/ALG El Protocolo de Iniciación de Sesión (SIP) es un protocolo estándar del IETF que se utiliza para crear, modificar y liberar sesiones de uno o más participantes. Estas sesiones pueden ser sesiones de usuario interactivas que incluyen elementos multimedia, como llamadas de voz, conferencias multimedia y realidad virtual. SIP es un protocolo multicanal. Además de establecer canales de señalización para la transmisión de la señalización, las partes llamante y llamada también establecen canales de datos para transmitir datos multimedia, como voz y vídeo. Por lo tanto, el tráfico SIP se clasifica en flujos de señalización y flujos multimedia. Los flujos de señalización se transmiten a través de UDP o TCP, incluyendo solicitudes y respuestas de ambas partes. Los flujos multimedia se transmiten a través de RTP y RTCP, incluyendo paquetes de datos multimedia (como voz y vídeo).

		H323.pdf	Overview of ASPF/ALG	Descripción general de ASPF/ALG	1	Overview of ASPF/ALG ASPF Definition Application specific packet filter (ASPF) is a packet filtering technology applied to the application layer, which is also called state-based packet filtering. ASPF Purpose ASPF enables the device to automatically detect the application layer information of certain packets and create the corresponding access rules (server map) based on the application layer information. The server map is used to permit subsequent packets in the data channel, which is equivalent to creating a refined security policy. For example, for multi-channel protocols (such as FTP, H.323, and SIP), the address and port of a data channel need to be negotiated in a control channel, and then the data channel can be established based on the negotiation result. The administrator cannot predict the address and port of the data channel, in that they are dynamically negotiated. Therefore, it is impossible for the administrator to configure full-fledged and accurate security policies. To ensure the proper establishment of the data channel, all ports need to be opened, which brings the risk of being attacked to the server or client. In this case, you can enable ASPF to prevent this risk.	Descripción general de ASPF/ALG Definición de ASPF El filtro de paquetes específico de la aplicación (ASPF) es una tecnología de filtrado de paquetes aplicada a la capa de aplicación, también denominada filtrado de paquetes basado en el estado. Propósito de ASPF ASPF permite que el dispositivo detecte automáticamente la información de la capa de aplicación de ciertos paquetes y cree las reglas de acceso correspondientes (mapa de servidor) basándose en dicha información. El mapa de servidor se utiliza para permitir paquetes posteriores en el canal de datos, lo que equivale a crear una política de seguridad refinada. Por ejemplo, para protocolos multicanal (como FTP, H.323 y SIP), la dirección y el puerto de un canal de datos deben negociarse en un canal de control, y luego el canal de datos puede establecerse según el resultado de la negociación. El administrador no puede predecir la dirección y el puerto del canal de datos, ya que se negocian dinámicamente. Por lo tanto, le resulta imposible configurar políticas de seguridad completas y precisas. Para garantizar el correcto establecimiento del canal de datos, todos los puertos deben estar abiertos, lo que conlleva el riesgo de ataques al servidor o al cliente. En este caso, puede habilitar ASPF para evitar este riesgo".

		Understanding SIP	Understanding SIP ASPF/ALG	Entendiendo SIP ASPF/ALG	1	In this case, the SIP ASPF/ALG function needs to be enabled on the Device for detecting and translating the IP address and port carried in the application layer information and recording the information in the server map. The media data packets match the server map when passing through the Device and are permitted, which are no longer controlled by security policies. As shown in Figure 1, client A is located on the intranet, and client B and the SIP proxy are located on the Internet in the source NAT scenario. This section describes the key interaction process among client A, client B, and the SIP proxy and the processing of packets after the ASPF/ALG function is enabled on the Device.	En este caso, es necesario habilitar la función SIP ASPF/ALG en el dispositivo para detectar y traducir la dirección IP y el puerto incluidos en la información de la capa de aplicación y registrar dicha información en el mapa del servidor. Los paquetes de datos multimedia coinciden con el mapa del servidor al pasar por el dispositivo y se permiten, lo que ya no está controlado por las políticas de seguridad. Como se muestra en la Figura 1, el cliente A se encuentra en la intranet, y el cliente B y el proxy SIP se encuentran en Internet en el escenario NAT de origen. Esta sección describe el proceso de interacción clave entre el cliente A, el cliente B y el proxy SIP, así como el procesamiento de paquetes tras habilitar la función ASPF/ALG en el dispositivo.
		H460Network.pdf	H.460 Network	Red H.460	1	H.460 is a protocol issued by the International Telecommunications Union (ITU) to deal with the firewall/NAT traversal. This protocol can implement traversal between public and private networks.	H.460 es un protocolo emitido por la Unión Internacional de Telecomunicaciones (UIT) para abordar el cruce de firewall/NAT. Este protocolo puede implementar el cruce entre redes públicas y privadas.
		NATALG.pdf	Conoce la función de NAT ALG en los firewalls de Huawei	N/A	3	Paquetes de protocolo definidos por el usuario QQ/MSN/que atraviesan dispositivos NAT También mencionamos QQ y MSN, y protocolos definidos por el usuario en "Security Policy". Firewalls clasifica estos protocolos en un tipo: "STUN". STUN es corto para Simple Traversal of UDP Through Network Address Translators que es un modo de transversal NAT. A diferencia de ALG NAT, el STUN no necesita ningún procesamiento en dispositivos NAT. En cambio, el cliente STUN en una intranet obtiene su dirección pública a través de intercambios de información entre el cliente STUN y el servidor. Luego, el cliente agrega la dirección pública en la carga útil y envía el paquete. De esta manera, el servidor en Internet obtiene la dirección pública del cliente desde la carga útil e inicia una solicitud de conexión al cliente.	N/A

	Limiting the ASPFALG	Limiting the ASPF/ALG Processing Range of Stun Protocol Traffic	Limitación del rango de procesamiento ASPF/ALG del tráfico del protocolo Stun	1	Limiting the ASPF/ALG Processing Range of Stun Protocol Traffic Context The device allows you to use the CLI to configure whether to permit packets matching the STUN server map table.	Limitación del rango de procesamiento ASPF/ALG del tráfico del protocolo STUN Contexto El dispositivo permite usar la CLI para configurar si se permiten paquetes que coincidan con la tabla de mapas del servidor STUN.
Permite la distribución por DHCP para IPv4 e IPv6 en sus interfaces LAN y subinterfaces (Vlans) en interfaces LAN.	DHCP.pdf	DHCP/6/DHCP_SERVER_DETECT	DHCP /6/ DETECCIÓN DEL SERVIDOR DHCP	1	DHCP/6/DHCP_SERVER_DETECT Message DHCP/6/DHCP_SERVER_DETECT: A new server was found. (IP Address=[ipaddress], MAC Address=[macaddress], Interface=[interface], PeVlan=[pevlan], CeVlan=[cevlan], BdID=[BdID]) Description A new DHCP server was discovered.	DHCP/6/DHCP_SERVER_DETECT Mensaje DHCP/6/DHCP_SERVER_DETECT: Se encontró un nuevo servidor. (Dirección IP=[direcciónIP], Dirección MAC=[direcciónMAC], Interfaz=[interfaz], PeVlan=[pevlan], CeVlan=[cevlan], BdID=[BdID]) Descripción Se descubrió un nuevo servidor DHCP.
VII. Gestión de políticas	N/A	N/A	N/A	N/A	N/A	N/A
Admite la prevención de fugas de datos para identificar y filtrar archivos y contenido (diferentes tipos de información, como tarjetas de identificación, tarjetas de crédito, tarjetas de débito y de seguridad social) en tránsito.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	8	DLP Supports identification of 100+ real file types, user-defined file name extensions, and file type-based upload/download control; supports keyword filtering for Office documents, web pages, code, and TXT files; supports user-defined keywords, regular expressions, and weight configuration.	DLP Admite la identificación de más de 100 tipos de archivos reales, extensiones de nombre de archivo definidas por el usuario y control de carga/descarga basado en el tipo de archivo; admite el filtrado de palabras clave para documentos de Office, páginas web, código y archivos TXT; admite palabras clave definidas por el usuario, expresiones regulares y configuración de peso.
Admite el filtrado de URL mediante la implementación de un servidor de URL local.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	2	HiSecEngine USG6000F series AI firewalls provide content security functions, such as application identification, IPS, antivirus, and URL filtering to protect intranet servers and users against threats. HiSecEngine USG6000F series also support to detect unknown threats by interworking with sandbox.	Los firewalls con IA de la serie HiSecEngine USG6000F ofrecen funciones de seguridad de contenido, como identificación de aplicaciones, IPS, antivirus y filtrado de URL para proteger a los servidores y usuarios de la intranet contra amenazas. La serie HiSecEngine USG6000F también permite detectar amenazas desconocidas mediante la interconexión con un entorno de pruebas
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Integrated protection Integrates firewall, VPN, intrusion prevention, antivirus, bandwidth management, Anti-DDoS, and URL filtering functions, and provides a global configuration view and integrated policy management.	Protección integrada Integra funciones de firewall, VPN, prevención de intrusiones, antivirus, gestión de ancho de banda, anti-DDoS y filtrado de URL, y proporciona una vista de configuración global y una gestión integrada de políticas.

		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Web security The URL category database on the cloud contains 500 million URLs in over 130 categories, such as news, games, gambling, drugs, and malicious web pages. URLs cover over 100 languages, and key categories of URLs cover over 20 languages. The URL category query servers are deployed in multiple countries/regions to provide high-speed and low-latency category query services. User-defined URL/host whitelist and blacklist are supported. HTTPS traffic can be filtered without decryption. TLS/SSL traffic can be decrypted before filtering. HTTP/2 and QUIC traffic can be filtered, and URL categories can be imported in batches. URL access can be controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors.	Seguridad web La base de datos de categorías de URL en la nube contiene 500 millones de URL en más de 130 categorías, como noticias, juegos, apuestas, drogas y páginas web maliciosas. Las URL abarcan más de 100 idiomas, y las categorías clave de URL abarcan más de 20. Los servidores de consulta de categorías de URL están implementados en varios países y regiones para ofrecer servicios de consulta de categorías de alta velocidad y baja latencia. Se admiten listas blancas y negras de URL/host definidas por el usuario. El tráfico HTTPS se puede filtrar sin descifrar. El tráfico TLS/SSL se puede descifrar antes del filtrado. El tráfico HTTP/2 y QUIC se puede filtrar, y las categorías de URL se pueden importar por lotes. El acceso a las URL se puede controlar en función de usuarios o grupos de usuarios, intervalos de tiempo y zonas de seguridad para gestionar con precisión el comportamiento en línea de los usuarios.
	Admite el filtrado de DNS para mejorar el rendimiento del filtrado de páginas web.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Web security The URL category database on the cloud contains 500 million URLs in over 130 categories, such as news, games, gambling, drugs, and malicious web pages. URLs cover over 100 languages, and key categories of URLs cover over 20 languages. The URL category query servers are deployed in multiple countries/regions to provide high-speed and low-latency category query services. User-defined URL/host whitelist and blacklist are supported. HTTPS traffic can be filtered without decryption. TLS/SSL traffic can be decrypted before filtering. HTTP/2 and QUIC traffic can be filtered, and URL categories can be imported in batches. URL access can be controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors.	Seguridad web La base de datos de categorías de URL en la nube contiene 500 millones de URL en más de 130 categorías, como noticias, juegos, apuestas, drogas y páginas web maliciosas. Las URL abarcan más de 100 idiomas, y las categorías clave de URL abarcan más de 20. Los servidores de consulta de categorías de URL están implementados en varios países y regiones para ofrecer servicios de consulta de categorías de alta velocidad y baja latencia. Se admiten listas blancas y negras de URL/host definidas por el usuario. El tráfico HTTPS se puede filtrar sin descifrar. El tráfico TLS/SSL se puede descifrar antes del filtrado. El tráfico HTTP/2 y QUIC se puede filtrar, y las categorías de URL se pueden importar por lotes. El acceso a las URL se puede controlar en función de usuarios o grupos de usuarios, intervalos de tiempo y zonas de seguridad para gestionar con precisión el comportamiento en línea de los usuarios.

	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	DNS security Based on massive threat information, technologies such as AI and knowledge graph are used to detect malicious DNS requests, including C&C domain names, DGA-generated domain names, compromised sites, and malicious domain names such as cryptojacking, ransomware, and phishing domain names. The local malicious domain name database supports a maximum of 2 million malicious domain names. DNS category-based filtering, DNS safe search, and DNS redirection (sinkholing) are also supported.	Seguridad DNS Con base en información masiva sobre amenazas, se utilizan tecnologías como IA y gráficos de conocimiento para detectar solicitudes DNS maliciosas, incluyendo nombres de dominio de C&C, nombres de dominio generados por DGA, sitios comprometidos y nombres de dominio maliciosos, como nombres de dominio de cryptojacking, ransomware y phishing. La base de datos local de nombres de dominio maliciosos admite un máximo de 2 millones de nombres de dominio maliciosos. También se admiten el filtrado por categorías de DNS, la búsqueda segura de DNS y la redirección de DNS (sinkholing).
Es compatible con SafeSearch para filtrar el contenido no saludable devuelto por los motores de búsqueda como Google, Yahoo, MSN	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	DNS security Based on massive threat information, technologies such as AI and knowledge graph are used to detect malicious DNS requests, including C&C domain names, DGA-generated domain names, compromised sites, and malicious domain names such as cryptojacking, ransomware, and phishing domain names. The local malicious domain name database supports a maximum of 2 million malicious domain names. DNS category-based filtering, DNS safe search, and DNS redirection (sinkholing) are also supported.	Seguridad DNS Con base en información masiva sobre amenazas, se utilizan tecnologías como IA y gráficos de conocimiento para detectar solicitudes DNS maliciosas, incluyendo nombres de dominio de C&C, nombres de dominio generados por DGA, sitios comprometidos y nombres de dominio maliciosos, como nombres de dominio de cryptojacking, ransomware y phishing. La base de datos local de nombres de dominio maliciosos admite un máximo de 2 millones de nombres de dominio maliciosos. También se admiten el filtrado por categorías de DNS, la búsqueda segura de DNS y la redirección de DNS (sinkholing).
	Understanding URL	Understanding URL Safe Search	Comprensión de la búsqueda segura de URL	1	Understanding URL Safe Search Safe search is a function of the search engine that automatically filters pornographic contents and potential attacks. To regulate Internet access behavior, you can enable URL safe search on the device, so as to enable safe search for all Internet access users. After the URL safe search function is enabled on the device, the device forcibly performs safe search on the search requests of Bing, Google, Yahoo, Yandex, and YouTube search engines to filter the search results of the five engines.	Entendiendo la Búsqueda Segura de URL La Búsqueda Segura es una función del motor de búsqueda que filtra automáticamente el contenido pornográfico y posibles ataques. Para controlar el comportamiento de acceso a Internet, puede habilitar la Búsqueda Segura de URL en el dispositivo para que todos los usuarios puedan acceder a ella. Una vez habilitada, el dispositivo realiza búsquedas seguras en las solicitudes de búsqueda de Bing, Google, Yahoo, Yandex y YouTube para filtrar los resultados de los cinco motores.

Las reglas de firewall deberán tener vigencia con base a fechas (incluyendo día, mes y año).	Config Secu Policy	Configuring the Session Aging Time of a Security Policy	Configuración del tiempo de caducidad de la sesión de una política de seguridad	1	Configuring the Session Aging Time of a Security Policy Context Session aging time Created session entries need to be matched by packets constantly. If no packet matches a session for a long time, the connection has been torn down, and the session is unnecessary. To save system resources, the system deletes the entry that is not matched for a continuous period of time; that is, the session entry ages. You can set the session aging time based on security policies as required. User-defined persistent connection Generally, the default aging time for different types of services on the device can meet the forwarding requirements. You can also fine-tune the aging time as needed. For some special services, however, the interval between two consecutive packets of a session can be very long.	Configuración del tiempo de caducidad de la sesión en un contexto de política de seguridad. Tiempo de caducidad de la sesión Las entradas de sesión creadas deben coincidir con los paquetes constantemente. Si ningún paquete coincide con una sesión durante un tiempo prolongado, la conexión se interrumpe y la sesión deja de ser necesaria. Para ahorrar recursos del sistema, este elimina la entrada que no coincide durante un período de tiempo continuo; es decir, la entrada de la sesión caduca. Puede configurar el tiempo de caducidad de la sesión según las políticas de seguridad según sea necesario. Conexión persistente definida por el usuario Generalmente, el tiempo de caducidad predeterminado para los diferentes tipos de servicios en el dispositivo puede cumplir con los requisitos de reenvío. También puede ajustar el tiempo de caducidad según sea necesario. Sin embargo, para algunos servicios especiales, el intervalo entre dos paquetes consecutivos de una sesión puede ser muy largo.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Web security URL access can be controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors.	Seguridad web El acceso a la URL se puede controlar según usuarios/grupos de usuarios, rangos de tiempo y zonas de seguridad para gestionar con precisión el comportamiento en línea de los usuarios. Gestión de políticas de seguridad
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Security policy management Supports traffic management and control based on the VLAN ID, 5-tuple, security zone, region, application, and time range, and implements integrated content security inspection.	Admite la gestión y el control del tráfico según el ID de VLAN, quintuplas, zona de seguridad, región, aplicación y rango de tiempo, e implementa una inspección integrada de seguridad de contenido.
VIII. Contar con soporte NAT	N/A	N/A	N/A	N/A	N/A	N/A
Admite funciones NAT completas y NAT ALG para múltiples protocolos de capa de aplicación, incluidos ILS, DNS, PPTP, SIP, FTP, ICQ, RTSP, QQ, MSN y MMS.	ASPFALG	ASPF/ALG Support for Known Protocols	Compatibilidad de ASPF/ALG con protocolosconocidos	1	ASPF/ALG Support for Known Protocols The FW can perform ASPF/ALG for the following known protocols. For scenario-based supportdetails, see Table 1 Table 1. ASPF/ALG support for known protocols: ILS, DNS, PPTP, SIP, FTP, ICQ, RTSP, QQ, MSN y MMS.	"ASPF/ALG Support for Known Protocols The FW can perform ASPF/ALG for the following known protocols. For scenario-based supportdetails, see Table 1 Table 1. ASPF/ALG support for known protocols: ILS, DNS, PPTP, SIP, FTP, ICQ, RTSP, QQ, MSN y MMS."

	NATALG.pdf	Conoce la función de NAT ALG en los firewalls de Huawei	N/A	3	Paquetes de protocolo definidos por el usuario QQ/MSN/que atraviesan dispositivos NAT También mencionamos QQ y MSN, y protocolos definidos por el usuario en "Security Policy". Firewalls clasifica estos protocolos en un tipo: "STUN". STUN es corto para Simple Traversal of UDP Through Network Address Translators que es un modo de transversal NAT. A diferencia de ALG NAT, el STUN no necesita ningún procesamiento en dispositivos NAT. En cambio, el cliente STUN en una intranet obtiene su dirección pública a través de intercambios de información entre el cliente STUN y el servidor. Luego, el cliente agrega la dirección pública en la carga útil y envía el paquete. De esta manera, el servidor en Internet obtiene la dirección pública del cliente desde la carga útil e inicia una solicitud de conexión al cliente.	"Paquetes de protocolo definidos por el usuario QQ/MSN/que atraviesan dispositivos NAT También mencionamos QQ y MSN, y protocolos definidos por el usuario en ""Security Policy"". Firewalls clasifica estos protocolos en un tipo: ""STUN"". STUN es corto para Simple Traversal of UDP Through Network Address Translators que es un modo de transversal NAT. A diferencia de ALG NAT, el STUN no necesita ningún procesamiento en dispositivos NAT. En cambio, el cliente STUN en una intranet obtiene su dirección pública a través de intercambios de información entre el cliente STUN y el servidor. Luego, el cliente agrega la dirección pública en la carga útil y envía el paquete. De esta manera, el servidor en Internet obtiene la dirección pública del cliente desde la carga útil e inicia una solicitud de conexión al cliente."
Admite la generación de una alarma si el uso del grupo de direcciones NAT de origen supera el umbral.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	10	Border protection and response service Automatic event analysis: Combines intelligent analysis and manual analysis by experts to analyze security events to ensure the accuracy of attack blocking and security alarms and optimize attack identification rules.	"Border protection and response service Automatic event analysis: Combines intelligent analysis and manual analysis by experts to analyze security events to ensure the accuracy of attack blocking and security alarms and optimize attack identification rules."
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	3	Simplified O&M The HiSecEngine USG6000F series provides a brand-new web UI, which intuitively visualizes threats as well as displays key information such as device status, alarms, traffic, and threat events. With multi-dimensional data drilling, the web UI offers optimal user experience, enhanced usability, and simplified O&M.	Operación y mantenimiento simplificados La serie HiSecEngine USG6000F ofrece una interfaz de usuario web completamente nueva que visualiza intuitivamente las amenazas y muestra información clave como el estado del dispositivo, las alarmas, el tráfico y los eventos de amenazas. Con análisis de datos multidimensionales, la interfaz de usuario web ofrece una experiencia de usuario óptima, mayor usabilidad y operaciones y mantenimiento simplificados.

		Config Secu Policy	Configuring the Session Aging Time of a Security Policy	Configuración del tiempo de caducidad de la sesión de una política de seguridad	1	Configuring the Session Aging Time of a Security Policy Context Session aging time Created session entries need to be matched by packets constantly. If no packet matches a session for a long time, the connection has been torn down, and the session is unnecessary. To save system resources, the system deletes the entry that is not matched for a continuous period of time; that is, the session entry ages. You can set the session aging time based on security policies as required. User-defined persistent connection Generally, the default aging time for different types of services on the device can meet the forwarding requirements. You can also fine-tune the aging time as needed. For some special services, however, the interval between two consecutive packets of a session can be very long.	Configuración del tiempo de caducidad de la sesión en un contexto de política de seguridad. Tiempo de caducidad de la sesión Las entradas de sesión creadas deben coincidir con los paquetes constantemente. Si ningún paquete coincide con una sesión durante un tiempo prolongado, la conexión se interrumpe y la sesión deja de ser necesaria. Para ahorrar recursos del sistema, este elimina la entrada que no coincide durante un período de tiempo continuo; es decir, la entrada de la sesión caduca. Puede configurar el tiempo de caducidad de la sesión según las políticas de seguridad según sea necesario. Conexión persistente definida por el usuario Generalmente, el tiempo de caducidad predeterminado para los diferentes tipos de servicios en el dispositivo puede cumplir con los requisitos de reenvío. También puede ajustar el tiempo de caducidad según sea necesario. Sin embargo, para algunos servicios especiales, el intervalo entre dos paquetes consecutivos de una sesión puede ser muy largo.
		Config NAT	Configuring NAT Alarm Functions	Configuración de las funciones de alarma NAT	1	Configuring NAT Alarm Functions Context After NAT is configured, you can configure the alarm and log functions in the system view to monitor the usage of IP addresses in an address pool and overall usage of the address pool.	Contexto de configuración de las funciones de alarma de NAT Después de configurar NAT, puede configurar las funciones de alarma y registro en la vista del sistema para supervisar el uso de las direcciones IP en un grupo de direcciones y el uso general de dicho grupo.

Hacer traslación de direcciones estático, uno a uno.	NAT Static	Example for Configuring Bidirectional NAT (Source NAT + Static Destination NAT) for Internet Users to Access Intranet Servers	Ejemplo de configuración de NAT bidireccional (NAT de origen + NAT de destino estático) para que los usuarios de Internet accedan a servidores de intranet	1	Networking Requirements An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 1.1.10.11 from the ISP, which are used by the intranet servers to provide services to Internet users. A source NAT policy is also required to enable intranet servers to send response packets to DeviceA, removing the need to configure return routes for intranet servers. Figure 1 shows the network diagram, in which the router is the access gateway provided by the ISP.	Requisitos de red Una empresa ha implementado el Dispositivo A como puerta de enlace de seguridad en el límite de la intranet. Es necesario configurar la NAT de destino en el Dispositivo A para que los servidores web y FTP de la red privada de la empresa puedan prestar servicios a los usuarios de Internet. Además de la dirección IP pública de la interfaz WAN del Dispositivo A, la empresa ha obtenido las direcciones IP públicas 1.1.10.10 y 1.1.10.11 del ISP, que utilizan los servidores de la intranet para prestar servicios a los usuarios de Internet. También se requiere una política de NAT de origen para que los servidores de la intranet puedan enviar paquetes de respuesta al Dispositivo A, eliminando así la necesidad de configurar rutas de retorno para los servidores de la intranet. La Figura 1 muestra el diagrama de red, en el que el enrutador es la puerta de enlace de acceso proporcionada por el ISP.
	Overview of NAT.pdf	Overview of NAT	Descripción general de NAT	1	Overview of NAT Definition Network Address Translation (NAT) translates IP addresses in the packet header into other IP addresses. Purpose As the Internet expands and becomes more accessible, an increasing number of private network users access the Internet using public IPv4 addresses. The rapid exhaustion of IPv4 address space causes a significant depletion of public addresses. Although IPv6 technology can be used to solve this problem, most contents and applications are still based on IPv4, and therefore they cannot be completely switched to IPv6 within a short period of time. NAT technology allows public IPv4 addresses to be reused, offering a short-term solution to IPv4 address exhaustion.	Descripción general de NAT Definición La Traducción de Direcciones de Red (NAT) traduce las direcciones IP del encabezado del paquete a otras direcciones IP. Propósito A medida que Internet se expande y se vuelve más accesible, un número cada vez mayor de usuarios de redes privadas acceden a Internet utilizando direcciones IPv4 públicas. El rápido agotamiento del espacio de direcciones IPv4 provoca una disminución significativa de las direcciones públicas. Si bien la tecnología IPv6 puede utilizarse para resolver este problema, la mayoría de los contenidos y aplicaciones aún se basan en IPv4 y, por lo tanto, no pueden migrarse completamente a IPv6 en un corto período de tiempo. La tecnología NAT permite la reutilización de direcciones IPv4 públicas, lo que ofrece una solución a corto plazo al agotamiento de direcciones IPv4.

	Hacer traslación de direcciones dinámico, muchos a uno.	NAT Dynamic	Example for Configuring Bidirectional NAT (Source NAT + Dynamic Destination NAT) for Internet Users to Access Intranet Servers	Ejemplo de configuración de NAT bidireccional (NAT de origen + NAT de destino dinámico) para que los usuarios de Internet accedan a servidores de intranet	1	Example for Configuring Bidirectional NAT (Source NAT + Dynamic Destination NAT) for Internet Users to Access Intranet Servers Networking Requirements An enterprise has deployed DeviceA as a security gateway at the intranet border. Dynamic destination NAT needs to be configured on DeviceA to prevent a large number of Internet users from accessing a specific server. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.10.10) from the ISP, which is used by intranet servers to provide services to Internet users. A source NAT policy is required so that intranet servers can send response packets to DeviceA, removing the need to configure return routes for intranet servers. Figure 1 shows the network diagram, in which the router is the access gateway provided by the ISP.	Ejemplo de configuración de NAT bidireccional (NAT de origen + NAT de destino dinámico) para que los usuarios de Internet accedan a los servidores de la intranet Requisitos de red Una empresa ha implementado el Dispositivo A como puerta de enlace de seguridad en el límite de la intranet. Es necesario configurar NAT de destino dinámico en el Dispositivo A para evitar que un gran número de usuarios de Internet accedan a un servidor específico. Además de la dirección IP pública de la interfaz WAN del Dispositivo A, la empresa ha obtenido otra dirección IP pública (1.1.10.10) del ISP, que los servidores de la intranet utilizan para prestar servicios a los usuarios de Internet. Se requiere una política de NAT de origen para que los servidores de la intranet puedan enviar paquetes de respuesta al Dispositivo A, eliminando así la necesidad de configurar rutas de retorno para los servidores de la intranet. La Figura 1 muestra el diagrama de red, en el que el enrutador es la puerta de enlace de acceso proporcionada por el ISP.
		Qverview of NAT.pdf	Overview of NAT	Descripción general de NAT	1	Overview of NAT Definition Network Address Translation (NAT) translates IP addresses in the packet header into other IP addresses. Purpose As the Internet expands and becomes more accessible, an increasing number of private network users access the Internet using public IPv4 addresses. The rapid exhaustion of IPv4 address space causes a significant depletion of public addresses. Although IPv6 technology can be used to solve this problem, most contents and applications are still based on IPv4, and therefore they cannot be completely switched to IPv6 within a short period of time. NAT technology allows public IPv4 addresses to be reused, offering a short-term solution to IPv4 address exhaustion.	Descripción general de NAT Definición La Traducción de Direcciones de Red (NAT) traduce las direcciones IP del encabezado del paquete a otras direcciones IP. Propósito A medida que Internet se expande y se vuelve más accesible, un número cada vez mayor de usuarios de redes privadas acceden a Internet utilizando direcciones IPv4 públicas. El rápido agotamiento del espacio de direcciones IPv4 provoca una disminución significativa de las direcciones públicas. Si bien la tecnología IPv6 puede utilizarse para resolver este problema, la mayoría de los contenidos y aplicaciones aún se basan en IPv4 y, por lo tanto, no pueden migrarse completamente a IPv6 en un corto período de tiempo. La tecnología NAT permite la reutilización de direcciones IPv4 públicas, lo que ofrece una solución a corto plazo al agotamiento de direcciones IPv4.
IX. Prevención de intrusiones y antivirus	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Admite la personalización de plantillas de políticas de prevención de intrusiones basadas en escenarios.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	5	The intrusion prevention capability effectively blocks a variety of malicious attacks and delivers differentiated defense based on virtual environment requirements to guarantee data security.	La función de prevención de intrusiones bloquea eficazmente diversos ataques maliciosos y ofrece una defensa diferenciada según los requisitos del entorno virtual para garantizar la seguridad de los datos.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Integrated protection Integrates firewall, VPN, intrusion prevention, antivirus, bandwidth management, Anti-DDoS, and URL filtering functions, and provides a global configuration view and integrated policy management.	Protección integrada Integra firewall, VPN, prevención de intrusiones, antivirus, gestión de ancho de banda, anti-DDoS y filtrado de URL, y proporciona una vista global de la configuración y una gestión integrada de políticas.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Intrusion Prevention Obtains the latest threat information in a timely manner and accurately detects and prevents vulnerability exploits; covers tens of thousands of CVE vulnerabilities; prevents the exploit of vulnerabilities (such as those in Windows and Unix/Linux operating systems, databases, Apache, IIS, and Tomcat as well as middleware), web attacks (such as SQL injection, XSS, and RCE), botnets, remote control, and Trojan horses; supports brute force cracking detection based on user behavior; provides 25,000+ predefined signatures and supports user-defined signatures and automatic signature database update; supports attack forensics collection, full-flow packet obtaining (including three-way handshake information), and attack fragment display to facilitate O&M; supports X-Forwarded-For (XFF) field extraction.	Prevención de intrusiones Obtiene la información más reciente sobre amenazas de forma oportuna y detecta y previene con precisión la explotación de vulnerabilidades; cubre decenas de miles de vulnerabilidades CVE; previene la explotación de vulnerabilidades (como las de sistemas operativos Windows y Unix/Linux, bases de datos, Apache, IIS y Tomcat, así como middleware), ataques web (como inyección SQL, XSS y RCE), botnets, control remoto y troyanos; admite la detección de ataques por fuerza bruta basados en el comportamiento del usuario; proporciona más de 25 000 firmas predefinidas y admite firmas definidas por el usuario y la actualización automática de la base de datos de firmas; admite la recopilación forense de ataques, la obtención de paquetes de flujo completo (incluida la información de protocolo de enlace de tres vías) y la visualización de fragmentos de ataque para facilitar las operaciones y el mantenimiento (O&M); admite la extracción de campos X-Forwarded-For (XFF).
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	10	Border protection and response service Intrusion detection and prevention: Leverages signatures to block application-layer attacks, terminates the transfer of phishing emails and malware (such as viruses and Trojan horses), detects compromised hosts on the internal network, and disconnects these hosts from the Internet to protect the security and stability of customer services.	Servicio de protección y respuesta fronteriza Detección y prevención de intrusiones: Utiliza firmas para bloquear ataques a la capa de aplicación, detiene la transferencia de correos electrónicos de phishing y malware (como virus y troyanos), detecta hosts comprometidos en la red interna y los desconecta de Internet para proteger la seguridad y la estabilidad de los servicios al cliente.

	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Security policy management Provides predefined templates for common attack defense scenarios to facilitate security policy deployment. Supports interworking with third-party policy management software (FireMon and Algosec) to facilitate security O&M.	Gestión de políticas de seguridad Proporciona plantillas predefinidas para escenarios comunes de defensa contra ataques, facilitando así la implementación de políticas de seguridad. Admite la interconexión con software de gestión de políticas de terceros (FireMon y Algosec) para facilitar las operaciones y el mantenimiento de la seguridad.
Admite la prevención de craqueo de fuerza bruta para servicios de aplicaciones comunes HTTP, FTP, SSH, SMTP e IMAP, VoIP, SIP) y software de base de datos (MySQL, Oracle y MSSQL)	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Intrusion Prevention Obtains the latest threat information in a timely manner and accurately detects and prevents vulnerability exploits; covers tens of thousands of CVE vulnerabilities; prevents the exploit of vulnerabilities (such as those in Windows and Unix/Linux operating systems, databases, Apache, IIS, and Tomcat as well as middleware), web attacks (such as SQL injection, XSS, and RCE), botnets, remote control, and Trojan horses; supports brute force cracking detection based on user behavior; provides 25,000+ predefined signatures and supports user-defined signatures and automatic signature database update; supports attack forensics collection, full-flow packet obtaining (including three-way handshake information), and attack fragment display to facilitate O&M; supports X-Forwarded-For (XFF) field extraction.	Prevención de intrusiones Obtiene la información más reciente sobre amenazas de forma oportuna y detecta y previene con precisión la explotación de vulnerabilidades; cubre decenas de miles de vulnerabilidades CVE; previene la explotación de vulnerabilidades (como las de sistemas operativos Windows y Unix/Linux, bases de datos, Apache, IIS y Tomcat, así como middleware), ataques web (como inyección SQL, XSS y RCE), botnets, control remoto y troyanos; admite la detección de ataques por fuerza bruta basados en el comportamiento del usuario; proporciona más de 25 000 firmas predefinidas y admite firmas definidas por el usuario y la actualización automática de la base de datos de firmas; admite la recopilación forense de ataques, la obtención de paquetes de flujo completo (incluida la información de protocolo de enlace de tres vías) y la visualización de fragmentos de ataque para facilitar las operaciones y el mantenimiento (O&M); admite la extracción de campos X-Forwarded-For (XFF).

		IPS Overview.pdf	Overview of Intrusion Prevention	Descripción general de la prevención de intrusiones	1	Overview of Intrusion Prevention Definition Intrusion prevention is a security mechanism that detects intrusions based on the attack signature database and takes certain response measures to terminate the intrusions in real time. Purpose Trojan horses, worms, botnets, spyware, overflow attacks, and injection attacks are on the rise, threatening network security. In addition, security vulnerabilities within operating systems and applications can be exploited by hackers to hack into systems. To address such problems, Huawei provides the intrusion prevention function to defend against various attacks and protect the network from being attacked. As shown in Figure 1, when an extranet user accesses the enterprise intranet, the device detects the access traffic. If an intrusion behavior is detected, the device blocks the access. Otherwise, the traffic is allowed. Similarly, when an intranet user accesses an external network, if the accessed web page or server contains malicious codes, the device blocks the access. Otherwise, the traffic is permitted.	Resumen de la Prevención de Intrusiones Definición La prevención de intrusiones es un mecanismo de seguridad que detecta intrusiones basándose en la base de datos de firmas de ataques y toma medidas de respuesta para eliminarlas en tiempo real. Objetivo Los troyanos, gusanos, botnets, spyware, ataques de desbordamiento e inyección están en aumento y amenazan la seguridad de la red. Además, los hackers pueden aprovechar las vulnerabilidades de seguridad de los sistemas operativos y las aplicaciones para acceder a los sistemas. Para abordar estos problemas, Huawei ofrece la función de prevención de intrusiones para defenderse de diversos ataques y proteger la red. Como se muestra en la Figura 1, cuando un usuario de la extranet accede a la intranet empresarial, el dispositivo detecta el tráfico de acceso. Si se detecta una intrusión, el dispositivo bloquea el acceso. De lo contrario, se permite el tráfico. De igual manera, cuando un usuario de la intranet accede a una red externa, si la página web o el servidor al que se accede contiene códigos maliciosos, el dispositivo bloquea el acceso. De lo contrario, se permite el tráfico.
		Config IPS	Configuring IPS	Configuración de IPS	1	By default, the device has multiple IPS profiles for different application scenarios, as shown in Table 1. The default IPS profiles can be viewed or directly referenced by security policies, but cannot be modified or deleted. Protocol DNS, HTTP, FTP, Telnet, SSH, RTSP, SSL, UDP, TCP, DNS, IMAP4, SMTP, POP3	De forma predeterminada, el dispositivo cuenta con múltiples perfiles IPS para diferentes escenarios de aplicación, como se muestra en la Tabla 1. Las políticas de seguridad pueden visualizar o hacer referencia directa a los perfiles IPS predeterminados, pero no pueden modificarse ni eliminarse. Protocolo DNS, HTTP, FTP, Telnet, SSH, RTSP, SSL, UDP, TCP, DNS, IMAP4, SMTP, POP3

	Understanding Attack	Understanding Attack Defense	Entendiendo la defensa contra ataques	7	Source IP address detection The device detects the source IP address of a request packet. If the source IP address is real, the packet is forwarded; otherwise, the packet is discarded. SYN flood, HTTP flood, HTTPS flood, DNS request flood, DNS reply flood, and SIP flood This defense technology requires the client to support source detection (that is, the client can properly process source detection reply packets). If the client does not support source detection, normal client requests will be discarded. In addition, this defense technology cannot mitigate flood attacks initiated using real IP addresses.	Detección de la dirección IP de origen El dispositivo detecta la dirección IP de origen de un paquete de solicitud. Si la dirección IP de origen es real, el paquete se reenvía; de lo contrario, se descarta. Inundación SYN, inundación HTTP, inundación HTTPS, inundación de solicitudes DNS, inundación de respuestas DNS e inundación SIP Esta tecnología de defensa requiere que el cliente admita la detección de origen (es decir, que pueda procesar correctamente los paquetes de respuesta a la detección de origen). Si el cliente no admite la detección de origen, se descartarán las solicitudes normales del cliente. Además, esta tecnología de defensa no puede mitigar los ataques de inundación iniciados con direcciones IP reales.
Admite el filtrado basado en nombres de dominio malintencionados para bloquear C&C.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	DNS security Based on massive threat information, technologies such as AI and knowledge graph are used to detect malicious DNS requests, including C&C domain names, DGA-generated domain names, compromised sites, and malicious domain names such as cryptojacking, ransomware, and phishing domain names. The local malicious domain name database supports a maximum of 2 million malicious domain names. DNS category-based filtering, DNS safe search, and DNS redirection (sinkholing) are also supported.	Seguridad DNS Con base en información masiva sobre amenazas, se utilizan tecnologías como IA y gráficos de conocimiento para detectar solicitudes DNS maliciosas, incluyendo nombres de dominio de C&C, nombres de dominio generados por DGA, sitios web comprometidos y nombres de dominio maliciosos, como nombres de dominio de cryptojacking, ransomware y phishing. La base de datos local de nombres de dominio maliciosos admite un máximo de 2 millones de nombres de dominio maliciosos. También se admiten el filtrado por categorías de DNS, la búsqueda segura de DNS y la redirección de DNS (sinkholing).

	Admite antivirus para protocolos como HTTP, FTP, SMTP, POP3, IMAP y NFS.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Antivirus Detects malware in files transmitted through protocols like HTTP, FTP, SMTP, POP3, IMAP4, NFS, and SMB; detects Trojan horses, worms, spyware, vulnerability exploits, adware, hacker tools, Rootkit, backdoors, grayware, botnet programs, ransomware, phishing software, cryptojacking software, and web shell programs; supports virus detection for Office files, executable files (Windows/Linux/MacOS), script files, flash files, PDF files, RTF files, web pages, and images; supports attack forensics collection; supports the inspection of archive files of up to 100 nested compression levels in multiple compression formats, such as tar, gzip, zip, rar, and 7z, and supports multiple actions, such as alert, block, add declaration, and attachment deletion.	Antivirus Detecta malware en archivos transmitidos a través de protocolos como HTTP, FTP, SMTP, POP3, IMAP4, NFS y SMB; detecta troyanos, gusanos, spyware, exploits de vulnerabilidades, adware, herramientas de hackers, rootkits, puertas traseras, grayware, programas de botnets, ransomware, software de phishing, software de cryptojacking y programas web shell; admite la detección de virus en archivos de Office, archivos ejecutables (Windows/Linux/MacOS), archivos de script, archivos flash, archivos PDF, archivos RTF, páginas web e imágenes; admite la recopilación de datos forenses de ataques; admite la inspección de archivos comprimidos de hasta 100 niveles de compresión anidados en múltiples formatos de compresión, como tar, gzip, zip, rar y 7z, y admite múltiples acciones, como alertar, bloquear, agregar declaración y eliminar archivos adjuntos.
	Soporte de detección y bloqueo de ataques.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Antivirus Detects malware in files transmitted through protocols like HTTP, FTP, SMTP, POP3, IMAP4, NFS, and SMB; detects Trojan horses, worms, spyware, vulnerability exploits, adware, hacker tools, Rootkit, backdoors, grayware, botnet programs, ransomware, phishing software, cryptojacking software, and web shell programs; supports virus detection for Office files, executable files (Windows/Linux/MacOS), script files, flash files, PDF files, RTF files, web pages, and images; supports attack forensics collection; supports the inspection of archive files of up to 100 nested compression levels in multiple compression formats, such as tar, gzip, zip, rar, and 7z, and supports multiple actions, such as alert, block, add declaration, and attachment deletion.	Antivirus Detecta malware en archivos transmitidos a través de protocolos como HTTP, FTP, SMTP, POP3, IMAP4, NFS y SMB; detecta troyanos, gusanos, spyware, exploits de vulnerabilidades, adware, herramientas de hackers, rootkits, puertas traseras, grayware, programas de botnets, ransomware, software de phishing, software de cryptojacking y programas web shell; admite la detección de virus en archivos de Office, archivos ejecutables (Windows/Linux/MacOS), archivos de script, archivos flash, archivos PDF, archivos RTF, páginas web e imágenes; admite la recopilación de datos forenses de ataques; admite la inspección de archivos comprimidos de hasta 100 niveles de compresión anidados en múltiples formatos de compresión, como tar, gzip, zip, rar y 7z, y admite múltiples acciones, como alertar, bloquear, agregar declaración y eliminar archivos adjuntos.

		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	8	Threat information Huawei Intelligent Security Center leverages multiple AI algorithms and expert analysis to generate massive threat information about IP addresses, domain names, URLs, and files on a daily basis. The threat information is automatically synchronized to devices for threat detection to quickly block emerging attacks. In addition, it can interconnect with third-party threat information sources to enrich inspection rules.	Información sobre amenazas El Centro de Seguridad Inteligente de Huawei aprovecha múltiples algoritmos de IA y análisis de expertos para generar diariamente información masiva sobre amenazas, como direcciones IP, nombres de dominio, URL y archivos. Esta información se sincroniza automáticamente con los dispositivos para su detección y bloquear rápidamente los ataques emergentes. Además, puede interconectarse con fuentes de información de amenazas de terceros para enriquecer las reglas de inspección.
		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	10	Intrusion detection and prevention: Leverages signatures to block application-layer attacks, terminates the transfer of phishing emails and malware (such as viruses and Trojan horses), detects compromised hosts on the internal network, and disconnects these hosts from the Internet to protect the security and stability of customer services.	Detección y prevención de intrusiones: Utiliza firmas para bloquear ataques a la capa de aplicación, detiene la transferencia de correos electrónicos de phishing y malware (como virus y troyanos), detecta hosts comprometidos en la red interna y los desconecta de Internet para proteger la seguridad y la estabilidad de los servicios al cliente.
X. Protección de seguridad de tráfico cifrado		N/A	N/A	N/A	N/A	N/A	N/A
Brinda protección de seguridad de tráfico cifrado		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	5	Enterprise border protection Firewalls are deployed at the network border. The built-in traffic probe can extract packets of encrypted traffic to monitor threats in encrypted traffic in real time. The policy control and data filtering functions of the firewalls are used to monitor social network applications to prevent data breach and protect enterprise networks.	Protección de fronteras empresariales Los firewalls se implementan en las fronteras de la red. La sonda de tráfico integrada puede extraer paquetes de tráfico cifrado para monitorear las amenazas en tiempo real. Las funciones de control de políticas y filtrado de datos de los firewalls se utilizan para monitorear las aplicaciones de redes sociales, prevenir filtraciones de datos y proteger las redes empresariales.
		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	SSL-encrypted traffic inspection Detects and defends against threats hidden in TLS/SSL-encrypted traffic, performs application-layer protection, such as intrusion prevention, antivirus, data filtering, and URL filtering, on decrypted TLS/SSL traffic, and supports URL category whitelist.	Inspección de tráfico cifrado con SSL Detecta y defiende contra amenazas ocultas en el tráfico cifrado con TLS/SSL, ofrece protección a nivel de aplicación, como prevención de intrusiones, antivirus, filtrado de datos y filtrado de URL, en el tráfico TLS/SSL descifrado, y admite la lista blanca de categorías de URL.

Descifra el tráfico HTTPS, POP3S, SMTPS e IMAPS y realiza filtrado de datos, auditoria y protección de seguridad en el tráfico descifrado.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Antivirus Detects malware in files transmitted through protocols like HTTP, FTP, SMTP, POP3, IMAP4, NFS, and SMB; detects Trojan horses, worms, spyware, vulnerability exploits, adware, hacker tools, Rootkit, backdoors, grayware, botnet programs, ransomware, phishing software, cryptojacking software, and web shell programs; supports virus detection for Office files, executable files (Windows/Linux/MacOS), script files, flash files, PDF files, RTF files, web pages, and images; supports attack forensics collection; supports the inspection of archive files of up to 100 nested compression levels in multiple compression formats, such as tar, gzip, zip, rar, and 7z, and supports multiple actions, such as alert, block, add declaration, and attachment deletion.	Antivirus Detecta malware en archivos transmitidos a través de protocolos como HTTP, FTP, SMTP, POP3, IMAP4, NFS y SMB; detecta troyanos, gusanos, spyware, exploits de vulnerabilidades, adware, herramientas de hackers, rootkits, puertas traseras, grayware, programas de botnets, ransomware, software de phishing, software de cryptojacking y programas web shell; admite la detección de virus en archivos de Office, archivos ejecutables (Windows/Linux/MacOS), archivos de script, archivos flash, archivos PDF, archivos RTF, páginas web e imágenes; admite la recopilación de datos forenses de ataques; admite la inspección de archivos comprimidos de hasta 100 niveles de compresión anidados en múltiples formatos de compresión, como tar, gzip, zip, rar y 7z, y admite múltiples acciones, como alertar, bloquear, agregar declaración y eliminar archivos adjuntos.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Web security The URL category database on the cloud contains 500 million URLs in over 130 categories, such as news, games, gambling, drugs, and malicious web pages. URLs cover over 100 languages, and key categories of URLs cover over 20 languages. The URL category query servers are deployed in multiple countries/regions to provide high-speed and low-latency category query services. User-defined URL/host whitelist and blacklist are supported. HTTPS traffic can be filtered without decryption. TLS/SSL traffic can be decrypted before filtering. HTTP/2 and QUIC traffic can be filtered, and URL categories can be imported in batches. URL access can be controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors.	Seguridad web La base de datos de categorías de URL en la nube contiene 500 millones de URL en más de 130 categorías, como noticias, juegos, apuestas, drogas y páginas web maliciosas. Las URL abarcan más de 100 idiomas, y las categorías clave de URL abarcan más de 20. Los servidores de consulta de categorías de URL están implementados en varios países y regiones para ofrecer servicios de consulta de categorías de alta velocidad y baja latencia. Se admiten listas blancas y negras de URL/host definidas por el usuario. El tráfico HTTPS se puede filtrar sin descifrar. El tráfico TLS/SSL se puede descifrar antes del filtrado. El tráfico HTTP/2 y QUIC se puede filtrar, y las categorías de URL se pueden importar por lotes. El acceso a las URL se puede controlar en función de usuarios o grupos de usuarios, intervalos de tiempo y zonas de seguridad para gestionar con precisión el comportamiento en línea de los usuarios.

	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	SSL-encrypted traffic inspection Detects and defends against threats hidden in TLS/SSL-encrypted traffic, performs application-layer protection, such as intrusion prevention, antivirus, data filtering, and URL filtering, on decrypted TLS/SSL traffic, and supports URL category whitelist.	Inspección de tráfico cifrado con SSL Detecta y defiende contra amenazas ocultas en el tráfico cifrado con TLS/SSL, ofrece protección a nivel de aplicación, como prevención de intrusiones, antivirus, filtrado de datos y filtrado de URL, en el tráfico TLS/SSL descifrado, y admite la lista blanca de categorías de URL.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	SSL offloading Replaces the server to implement SSL encryption and decryption, reducing the server load and implementing load balancing of HTTP traffic.	Descarga de SSL Reemplaza el servidor para implementar el cifrado y descifrado SSL, lo que reduce la carga del servidor y equilibra la carga del tráfico HTTP.
soporta descifrado refinado basado en categorías de URL para mejorar el rendimiento del descifrado.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	7	Web security The URL category database on the cloud contains 500 million URLs in over 130 categories, such as news, games, gambling, drugs, and malicious web pages. URLs cover over 100 languages, and key categories of URLs cover over 20 languages. The URL category query servers are deployed in multiple countries/regions to provide high-speed and low-latency category query services. User-defined URL/host whitelist and blacklist are supported. HTTPS traffic can be filtered without decryption. TLS/SSL traffic can be decrypted before filtering. HTTP/2 and QUIC traffic can be filtered, and URL categories can be imported in batches. URL access can be controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors.	Seguridad web La base de datos de categorías de URL en la nube contiene 500 millones de URL en más de 130 categorías, como noticias, juegos, apuestas, drogas y páginas web maliciosas. Las URL abarcan más de 100 idiomas, y las categorías clave de URL abarcan más de 20. Los servidores de consulta de categorías de URL están implementados en varios países y regiones para ofrecer servicios de consulta de categorías de alta velocidad y baja latencia. Se admiten listas blancas y negras de URL/host definidas por el usuario. El tráfico HTTPS se puede filtrar sin descifrar. El tráfico TLS/SSL se puede descifrar antes del filtrado. El tráfico HTTP/2 y QUIC se puede filtrar, y las categorías de URL se pueden importar por lotes. El acceso a las URL se puede controlar en función de usuarios o grupos de usuarios, intervalos de tiempo y zonas de seguridad para gestionar con precisión el comportamiento en línea de los usuarios.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	SSL-encrypted traffic inspection Detects and defends against threats hidden in TLS/SSL-encrypted traffic, performs application-layer protection, such as intrusion prevention, antivirus, data filtering, and URL filtering, on decrypted TLS/SSL traffic, and supports URL category whitelist.	Inspección de tráfico cifrado con SSL Detecta y defiende contra amenazas ocultas en el tráfico cifrado con TLS/SSL, ofrece protección a nivel de aplicación, como prevención de intrusiones, antivirus, filtrado de datos y filtrado de URL, en el tráfico TLS/SSL descifrado, y admite la lista blanca de categorías de URL.

	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	SSL offloading Replaces the server to implement SSL encryption and decryption, reducing the server load and implementing load balancing of HTTP traffic.	Descarga de SSL Reemplaza el servidor para implementar el cifrado y descifrado SSL, lo que reduce la carga del servidor y equilibra la carga del tráfico HTTP.
Descifra el tráfico y lo refleja en dispositivos de terceros para auditoria y detección de seguridad.	Config Mirroring	Configuring Mirroring of SSL-Decrypted Packets	Configuración de la duplicación de paquetesdescifrados con SSL	1	The scenario of decrypted packet mirroring is generally applied when the FW is deployed at the enterprise egress. After the mirroring interface for packet decryption is specified, the FW sends the decrypted plaintext data to the third-party detection device through the mirroring interface, and the third-party detection device performs security check on the mirrored data. The decrypted packet mirroring function enables multiple devices to perform security detection and audit on the decrypted content, extending the detection scope of the third-party device and maximizing the value of existing devices.	El escenario de duplicación de paquetes descifrados se aplica generalmente cuando el FW se implementa en la salida de la empresa. Una vez especificada la interfaz de duplicación para el descifrado de paquetes, el FW envía los datos de texto plano descifrados al dispositivo de detección de terceros a través de la interfaz de duplicación, y el dispositivo de detección de terceros realiza una verificación de seguridad de los datos reflejados. La función de duplicación de paquetes descifrados permite que múltiples dispositivos realicen detección y auditoría de seguridad en el contenido descifrado, ampliando el alcance de detección del dispositivo de terceros y maximizando el valor de los dispositivos existentes.
	Overview of Mirroring.pdf	Overview of Mirroring	Descripción general de la duplicación	1	Overview of Mirroring Definition Mirroring is a function used to copy (or mirror) traffic received or sent (or both) on a specified source (known as a mirrored source) to a destination port (known as an observing port) for analysis. Copied packets are known as mirrored packets. Purpose During network maintenance, you may need to obtain and analyze packets. For example, if you suspect that there are attack packets on the network, you need to be able to obtain and analyze the packets without affecting packet forwarding. The mirroring function is able to achieve such results. Mirroring copies packets on a mirrored port to an observing port for analysis by a monitoring device without affecting switching of packets on the mirrored port. This function facilitates network monitoring and troubleshooting.	Descripción general de la duplicación Definición La duplicación es una función que se utiliza para copiar (o reflejar) el tráfico recibido o enviado (o ambos) en un origen específico (conocido como origen reflejado) a un puerto de destino (conocido como puerto de observación) para su análisis. Los paquetes copiados se conocen como paquetes reflejados. Propósito Durante el mantenimiento de la red, es posible que necesite obtener y analizar paquetes. Por ejemplo, si sospecha que hay paquetes de ataque en la red, necesita poder obtenerlos y analizarlos sin afectar el reenvío de paquetes. La función de duplicación permite lograr estos resultados. La duplicación copia los paquetes de un puerto reflejado a un puerto de observación para que un dispositivo de monitoreo los analice sin afectar la conmutación de paquetes en el puerto reflejado. Esta función facilita la monitorización y la resolución de problemas de la red.

XI. Autenticación de usuario de acceso a la red	N/A	N/A	N/A	N/A	N/A	N/A
Compatible con AD (directorio activo), SSO (Single Sing-On), RADIUS SSO (Single Sing-On), autenticación NTLM, sin autenticación, autenticación MAC y autenticación SMS.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	10	User authentication Supports multiple authentication modes for Internet access users, including local Portal authentication and single sign-on (SSO). In local Portal authentication, the built-in Portal page of the device can be pushed to users, and the account and password entered on the Portal page by a user can be sent to the local database or RADIUS, HWTACACS, AD, or LDAP authentication server for authentication. SSO includes RADIUS SSO and Agile Controller (NCE-Campus) SSO.	Autenticación de usuario Admite múltiples modos de autenticación para usuarios con acceso a Internet, incluyendo la autenticación local del portal y el inicio de sesión único (SSO). En la autenticación local del portal, la página del portal integrada del dispositivo se puede enviar a los usuarios, y la cuenta y la contraseña introducidas en ella se pueden enviar a la base de datos local o al servidor de autenticación RADIUS, HWTACACS, AD o LDAP para su autenticación. El SSO incluye el SSO RADIUS y el SSO de Agile Controller (NCE-Campus).
	NTLM.pdf	Portal Authentication on Internet Access Users	Autenticación del portal en usuarios de acceso aInternet	5	NTLM Authentication If a user in the AD domain wants to access the Internet, the NTLM authentication proxy to trigger and forward NTLM authentication packets exchanged between the browser and AD server and obtain the user identity in the authentication process. NTLM authentication is a portal authentication mode in which the user is unaware of entering the user name and password. Figure 5 shows the detailed mechanism.	Autenticación NTLM Si un usuario del dominio AD desea acceder a Internet, el proxy de autenticación NTLM activa y reenvía los paquetes de autenticación NTLM intercambiados entre el navegador y el servidor AD, obteniendo la identidad del usuario durante el proceso de autenticación. La autenticación NTLM es un modo de autenticación del portal en el que el usuario no es consciente de haber introducido su nombre de usuario y contraseña. La Figura 5 muestra el mecanismo detallado.
	User Authentication	User Authentication Modes	Modos de autenticación de usuario	3	User Authentication Modes Anonymous authentication Guests access the network without using any accounts. The controller automatically displays the login accounts of the guests asanonymous accounts. SMS authentication A user enters a mobile number as the user name and clicks the button for obtaining a password.The SMS server then sends apassword to the user. The system automatically registers and authenticates the user name and password after the user enters thepassword.	Modos de autenticación de usuario Autenticación anónima Los invitados acceden a la red sin usar ninguna cuenta. El controlador muestra automáticamente las cuentas de inicio de sesión de los invitados como anónimas. Autenticación por SMS Un usuario introduce un número de teléfono móvil como nombre de usuario y pulsa el botón para obtener una contraseña. El servidor SMS envía una contraseña al usuario. El sistema registra y autentica automáticamente el nombre de usuario y la contraseña después de que el usuario la introduzca.

	User Authenticatio n	User Authentication Modes	Modos de autenticación de usuario	1	MAC address authentication enables terminals to be authenticated based on their MACaddresses. When a terminal attempts to access the network, an access control device obtainsthe MAC address of the terminal and uses the MAC address as the user name and passwordfor authentication. MAC addresses can be easily forged, so the MAC address authenticationmode is less secure. In addition, MAC addresses need to be registered on an authenticationserver, resulting in complex management. In some special cases, this authentication mode canbe used when end users do not want to or are unable to enter user account information forauthentication. For example, user account information cannot be entered on dumb terminalssuch as printers and IP phones.	La autenticación por dirección MAC permite autenticar los terminales según sus direcciones MAC. Cuando un terminal intenta acceder a la red, un dispositivo de control de acceso obtiene la dirección MAC del terminal y la utiliza como nombre de usuario y contraseña para la autenticación. Las direcciones MAC se pueden falsificar fácilmente, por lo que el modo de autenticación por dirección MAC es menos seguro. Además, las direcciones MAC deben registrarse en un servidor de autenticación, lo que resulta en una gestión compleja. En algunos casos especiales, este modo de autenticación se puede utilizar cuando los usuarios finales no desean o no pueden introducir la información de la cuenta de usuario para la autenticación. Por ejemplo, no se puede ingresar información de la cuenta de usuario en terminales tontas como impresoras y teléfonos IP.

Compatible con grupos de seguridad dinámicos para autorizar dinámicamente organizaciones horizontales.	User Organizational	User Organizational Structure	Estructura organizativa del usuario	1	A FW controls network behaviors and access permissions by the granularity of user. The user organizational structure on the FW is a reflection of real organizational structures in enterprises and is the basis of user-specific permission control. As shown in Figure 1, a user organizational structure can be a tree-shaped structure that divides users by department or divides users cross departments in the horizontal dimension. Security group: A security group is a cross-department group in the horizontal organizational structure. You can create cross-department security groups if you need to manage users in a dimension other than by department. For example, you can create a group between multiple departments. In addition, the server provides similar horizontal groups when enterprises use third-party authentication servers to store organizational structures. To configure policies based on cross-department security groups, you need to keep the security groups created on the FW consistent with the organizational structures on the servers.	Un firewall controla el comportamiento de la red y los permisos de acceso según la granularidad del usuario. La estructura organizativa de usuarios en el firewall refleja las estructuras organizativas reales de las empresas y constituye la base del control de permisos específicos para cada usuario. Como se muestra en la Figura 1, una estructura organizativa de usuarios puede tener forma de árbol, que divide a los usuarios por departamento o entre departamentos en la dimensión horizontal. Grupo de seguridad: Un grupo de seguridad es un grupo interdepartamental en la estructura organizativa horizontal. Puede crear grupos de seguridad interdepartamentales si necesita administrar usuarios en una dimensión distinta a la departamental. Por ejemplo, puede crear un grupo entre varios departamentos. Además, el servidor proporciona grupos horizontales similares cuando las empresas utilizan servidores de autenticación de terceros para almacenar las estructuras organizativas. Para configurar políticas basadas en grupos de seguridad interdepartamentales, debe mantener la coherencia entre los grupos de seguridad creados en el firewall y las estructuras organizativas de los servidores.

		User Organizational	User Organizational Structure	Estructura organizativa del usuario	3	Security Group-based Horizontal Organizational Structure User groups (departments) reflect the vertical organizational structure of users, whereas security groups reflect the horizontal organizational structure. You can add users from different departments to one security group for management. After you configure a policy for a security group, the policy takes effect on all users in this security group, which makes user management easier and more flexible. You can also configure security groups in the scenarios in which the FW functions with a third-party authentication server. When AD, AD LDAP, and Sun ONE LDAP servers are deployed on a network, the AD, AD LDAP, and Sun ONE LDAP servers have other types of organizational structures except organizational units (OU). For example, the AD and AD LDAP servers have security groups, and the Sun ONE LDAP server has static and dynamic groups. To enable the FW to manage users based on the security groups on the AD and AD LDAP servers and static and dynamic groups on the Sun ONE LDAP server, use the security groups on the FW.	Estructura organizativa horizontal basada en grupos de seguridad Los grupos de usuarios (departamentos) reflejan la estructura organizativa vertical de los usuarios, mientras que los grupos de seguridad reflejan la estructura organizativa horizontal. Puede agregar usuarios de diferentes departamentos a un grupo de seguridad para su administración. Tras configurar una política para un grupo de seguridad, esta se aplica a todos los usuarios de dicho grupo, lo que facilita y flexibiliza la administración de usuarios. También puede configurar grupos de seguridad en los casos en que el firewall funcione con un servidor de autenticación de terceros. Cuando se implementan servidores AD, AD LDAP y Sun ONE LDAP en una red, estos servidores tienen otros tipos de estructuras organizativas, excepto unidades organizativas (OU). Por ejemplo, los servidores AD y AD LDAP tienen grupos de seguridad, y el servidor Sun ONE LDAP tiene grupos estáticos y dinámicos. Para que el firewall administre usuarios según los grupos de seguridad de los servidores AD y AD LDAP, y los grupos estáticos y dinámicos del servidor Sun ONE LDAP, utilice los grupos de seguridad del firewall.

	Soporta múltiples dominios de autenticación para cumplir con los requisitos de administración independiente y autenticación de múltiples sucursales.	User Organizational	User Organizational Structure	Estructura organizativa del usuario	2	Tree-shaped Organizational Structure The top node of the tree-shaped organizational structure is "Authentication domain", which is also considered the root group. The subordinates of an authentication domain can be user groups or users. The default authentication domain equals the /default root group. In most cases, only the default authentication domain is used. If users have different authentication modes are used, or domain names must be consistent with those on servers, you need to plan other authentication domains. If new authentication domains are required, the FW provides the following modes for user organizational structure planning: Each authentication domain has independent user accounts. Each authentication domain is an independent tree-shaped organizational structure, similar to the domain structure on an AD or LDAP authentication server. Each authentication domain has independent user accounts. Different authentication domains can have the same account. All authentication domains share user accounts of the default authentication domain. There is only one tree-shaped organizational structure: default authentication domain. Other authentication domains share accounts with the default authentication domain. In this mode, a new authentication domain determines the authentication mode of its users, and the authentication domain is not the top node of the user organizational structure.	Estructura organizativa en forma de árbol El nodo superior de la estructura organizativa en forma de árbol es el "Dominio de autenticación", que también se considera el grupo raíz. Los subordinados de un dominio de autenticación pueden ser grupos de usuarios o usuarios. El dominio de autenticación predeterminado equivale al grupo raíz /default. En la mayoría de los casos, solo se utiliza el dominio de autenticación predeterminado. Si los usuarios utilizan diferentes modos de autenticación, o si los nombres de dominio deben ser coherentes con los de los servidores, es necesario planificar otros dominios de autenticación. Si se requieren nuevos dominios de autenticación, el firewall ofrece los siguientes modos para la planificación de la estructura organizativa de usuarios: Cada dominio de autenticación tiene cuentas de usuario independientes. Cada dominio de autenticación es una estructura organizativa independiente en forma de árbol, similar a la estructura de dominios de un servidor de autenticación AD o LDAP. Cada dominio de autenticación tiene cuentas de usuario independientes. Diferentes dominios de autenticación pueden tener la misma cuenta. Todos los dominios de autenticación comparten las cuentas de usuario del dominio de autenticación predeterminado. Solo existe una estructura organizativa en forma de árbol: el dominio de autenticación predeterminado. Otros dominios de autenticación comparten cuentas con el dominio de autenticación predeterminado. En este modo, un nuevo dominio de autenticación determina el modo de autenticación de su... usuarios, y el dominio de autenticación no es el nodo superior de la estructura organizativa del usuario".

Soporta la personalización de la página del portal y cuestionarios para promover el marketing.	Customizing Portal Page	Customizing Portal Page	Personalizar una página del portal	1	Customizing a Portal Page Context The layout of preset pages cannot be modified. As a result, preset pages cannot meet your requirements if you want to modify the Portal page layout or use a large number of multimedia elements and images on Portal pages. Application Scenarios The controller provides various page controls for you to design your own Portal pages. You can customize the content and style of page controls. If some controls cannot meet requirements, you can edit the controls using the HTML custom editing function provided on the controller. Feature Requirements If you need to customize controls beyond the control area (including common controls and page controls), contact Huawei engineers to customize them.	Personalización de una página del portal Contexto El diseño de las páginas predefinidas no se puede modificar. Por lo tanto, estas páginas no pueden satisfacer sus necesidades si desea modificar el diseño de la página del portal o usar una gran cantidad de elementos multimedia e imágenes en ellas. Escenarios de aplicación El controlador proporciona varios controles de página para que diseñe sus propias páginas del portal. Puede personalizar el contenido y el estilo de los controles de página. Si algunos controles no cumplen con los requisitos, puede editarlos mediante la función de edición personalizada de HTML del controlador. Requisitos de las funciones Si necesita personalizar controles más allá del área de control (incluidos los controles comunes y los controles de página), póngase en contacto con los ingenieros de Huawei para personalizarlos.
	Customizing Portal Page	Customizing Portal Page	Personalizar una página del portal	5	6. (Optional) When Email Auth Template is selected for System template, the mobile number, name, company, and application reason can be set as mandatory parameters. When you click Get Verification Code on the authentication page, the system checks whether the mobile number, name, company, and application reason are empty.	6. (Opcional) Al seleccionar la Plantilla de Autorización de Correo Electrónico como Plantilla del Sistema, se pueden configurar como parámetros obligatorios el número de teléfono móvil, el nombre, la empresa y el motivo de la solicitud. Al hacer clic en "Obtener Código de Verificación" en la página de autenticación, el sistema comprueba si el número de teléfono móvil, el nombre, la empresa y el motivo de la solicitud están vacíos.

	Customizing Portal Page	Customizing Portal Page	Personalizar una página del portal	9	Guest account policy Meaning: This parameter needs to be set when System template is set to Common self-registration template, SMS authentication template, One-click authentication template, QR Code Register Auth Template, or Email Auth Template. You can configure a guest account policy on the Admission Management > Admission Resource > Guest Management > Guest Account Policy page. Constraints: After a guest account policy is bound to a customized page, the password type, approval mode, and approver in the guest account policy cannot be modified.	Política de la cuenta de invitado: Significado: Este parámetro debe configurarse cuando la Plantilla del Sistema se configura como Plantilla de autorregistro común, Plantilla de autenticación por SMS, Plantilla de autenticación con un solo clic, Plantilla de Autorización de Registro por Código QR o Plantilla de Autorización de Correo Electrónico. Puede configurar una política de la cuenta de invitado en la página Administración de Admisiones > Recursos de Admisión > Administración de Invitados > Política de la Cuenta de Invitado. Restricciones: Una vez que una política de la cuenta de invitado se vincula a una página personalizada, no se pueden modificar el tipo de contraseña, el modo de aprobación ni el aprobador de la política de la cuenta de invitado.
	Customizing Portal Page	Customizing Portal Page	Personalizar una página del portal	11	Page Control Portal pages of the following types can be configured: authentication page, authentication success page, full-screen advertisement page, user notice page, registration page, registration success page, password change page, username and password verification page, password reset page, and questionnaire page. Due to function differences, each type of page has controls that are different from those on other pages.	Control de página Se pueden configurar páginas del portal de los siguientes tipos: página de autenticación, página de autenticación exitosa, página de publicidad a pantalla completa, página de avisos para el usuario, página de registro, página de registro exitoso, página de cambio de contraseña, página de verificación de nombre de usuario y contraseña, página de restablecimiento de contraseña y página de cuestionario. Debido a las diferencias de funcionalidad, cada tipo de página tiene controles diferentes a los de otras páginas.
XII. Gestión centralizada	N/A	N/A	N/A	N/A	N/A	N/A
Admite la actualización mediante una unidad flash USB para reducir los costos de O&M.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	1	The security O&M platform implements unified management and O&M of multiple types of security products, such as firewalls, anti-DDoS devices, reducing security O&M OPEX.	La plataforma de seguridad O&M implementa la gestión unificada de múltiples tipos de productos de seguridad, como firewalls y dispositivos anti-DDoS, lo que reduce los gastos operativos de O&M.

		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	3	Simplified O&M The HiSecEngine USG6000F series provides a brand-new web UI, which intuitively visualizes threats as well as displays key information such as device status, alarms, traffic, and threat events. With multi-dimensional data drilling, the web UI offers optimal user experience, enhanced usability, and simplified O&M. The HiSecEngine USG6000F series firewalls can be centrally managed by the security management platform SecoManager, implementing a shift from single-point defense to collaborative network protection. The SecoManager provides policy tuning and intelligent O&M capabilities. It can also manage security products, such as anti-DDoS devices to quickly eliminate network threats and improve security handling effectiveness. The HiSecEngine USG6000F series NGFW can also be managed by NCE-Campus, and NCE-Campus can also support to manage switch, AR, POL device at the same time, even third party devices.	Operación y mantenimiento simplificados La serie HiSecEngine USG6000F ofrece una interfaz web completamente nueva que visualiza intuitivamente las amenazas y muestra información clave como el estado del dispositivo, las alarmas, el tráfico y los eventos de amenazas. Con la exploración de datos multidimensional, la interfaz web ofrece una experiencia de usuario óptima, una usabilidad mejorada y una operación y mantenimiento simplificados. Los firewalls de la serie HiSecEngine USG6000F se pueden gestionar de forma centralizada mediante la plataforma de gestión de seguridad SecoManager, lo que permite pasar de la defensa de punto único a la protección colaborativa de la red. SecoManager ofrece ajuste de políticas y funciones inteligentes de operación y mantenimiento. También puede gestionar productos de seguridad, como dispositivos anti-DDoS, para eliminar rápidamente las amenazas de red y mejorar la eficacia de la gestión de la seguridad. El firewall de próxima generación (NGFW) de la serie HiSecEngine USG6000F también puede gestionarse mediante NCE-Campus, que también permite gestionar simultáneamente conmutadores, AR y dispositivos POL, e incluso dispositivos de terceros.
		HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	10	O&M capability Supports telemetry to automatically read information from hardware, such as fans, power modules, optical modules, Ethernet ports, temperature sensors, and drivers, and sends interface traffic statistics, CPU usage, and memory usage to the collector	Capacidad de operación y mantenimiento Admite telemetría para leer automáticamente información del hardware, como ventiladores, módulos de potencia, módulos ópticos, puertos Ethernet, sensores de temperatura y controladores, y envía estadísticas de tráfico de interfaz, uso de CPU y uso de memoria al recopilador.

	Config USB based Deploy	Example for Configuring USB-based Deployment (Configured Device Scenario)	Ejemplo de configuración de implementación basada en USB (escenario de dispositivo configurado)	1	Networking Requirements A new network needs to be deployed. DeviceA has been configured, and the customer requires that it automatically completes upgrade after it is powered on to reduce labor costs and deployment time. The system software software_file.cc is required for upgrading DeviceA. Configuration Roadmap The configuration roadmap is as follows: 1. Make the intermediate file usb.ini to enable the device to obtain its system software according to the intermediate file. 2. Save the intermediate file to the root directory of the USB flash drive and system software to the directory specified by the DIRECTORY field in the intermediate file. 3. Power on the device and enable USB-based deployment. 4. Insert the USB flash drive into the device to complete the deployment process.	Requisitos de red Se necesita implementar una nueva red. El Dispositivo A se ha configurado y el cliente requiere que complete la actualización automáticamente después de encenderlo para reducir los costos de mano de obra y el tiempo de implementación. Se requiere el software del sistema software_file.cc para actualizar el Dispositivo A. Guía de configuración La guía de configuración es la siguiente: 1. Cree el archivo intermedio usb.ini para que el dispositivo obtenga su software de sistema según el archivo intermedio. 2. Guarde el archivo intermedio en el directorio raíz de la unidad flash USB y el software del sistema en el directorio especificado en el campo DIRECTORIO del archivo intermedio. 3. Encienda el dispositivo y habilite la implementación basada en USB. 4. Inserte la unidad flash USB en el dispositivo para completar el proceso de implementación.
Proporciona interfaces API de integración hacia el norte, como RESTCONF y NETCONF para conectarse a plataformas de administración de terceros.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	12	Third-Party and Open-Source Ecosystem Open API for integration with third-party products, providing NETCONF interfaces Other third-party management software based on SNMP, SSH, and Syslog	Ecosistema de terceros y de código abierto API abierta para la integración con productos de terceros, que proporciona interfaces NETCONF Otro software de gestión de terceros basado en SNMP, SSH y Syslog

		Overview of RESTCONF.pdf	Overview of RESTCONF	Descripción general de RESTCONF	1	Overview of RESTCONF Definition RESTCONF, an HTTP-based protocol, provides RESTful programming interfaces and allows users to add, delete, modify, as well as query network device data. Purpose Increasing network scale and complexity are driving the growing demand for automated O&M. The Network Configuration Protocol (NETCONF) provides application programming interfaces (APIs) based on the remote procedure call (RPC) mechanism. However, networks are developing faster than NETCONF, necessitating standard programming interfaces that support web application access and network device operations. RESTCONF is developed based on both NETCONF and HTTP, and it provides core NETCONF functions using HTTP methods. The programming interface complies with the RESTful style of the IT industry and provides users with the capability of efficiently developing web O&M tools. Table 1 compares RESTCONF and NETCONF based on the YANG data model.	Descripción general de RESTCONF Definición RESTCONF, un protocolo basado en HTTP, proporciona interfaces de programación RESTful y permite a los usuarios agregar, eliminar, modificar y consultar datos de dispositivos de red. Propósito El aumento de la escala y la complejidad de la red impulsan la creciente demanda de operaciones y mantenimiento automatizados. El Protocolo de Configuración de Red (NETCONF) proporciona interfaces de programación de aplicaciones (API) basadas en el mecanismo de llamada a procedimiento remoto (RPC). Sin embargo, las redes se desarrollan a un ritmo más rápido que NETCONF, lo que requiere interfaces de programación estándar que admitan el acceso a aplicaciones web y las operaciones de dispositivos de red. RESTCONF se basa en NETCONF y HTTP, y proporciona las funciones principales de NETCONF mediante métodos HTTP. La interfaz de programación cumple con el estilo RESTful de la industria de TI y ofrece a los usuarios la capacidad de desarrollar de forma eficiente. Herramientas web de operación y mantenimiento. La Tabla 1 compara RESTCONF y NETCONF según el modelo de datos YANG.

Soportar los protocolos SNMP RFC 1157, SNMPv2c o SNMPv3	SNMP Version.pdf	SNMP Version	Versiones de SNMP	1	SNMP Versions SNMP versions include SNMPv1, SNMPv2c, and SNMPv3. Both SNMPv1 and SNMPv2c use community name-based authentication. The NMS uses the community name list to control the device access rights, but the agent does not check whether the community name used by a given sender is authorized. Additionally, SNMP messages are not encrypted for transmission, so secure authentication and privacy are not ensured. Compared with SNMPv1, SNMPv2c supports more operations, data types, error codes, and transport protocols. SNMPv3 provides all the functions of SNMPv1 and SNMPv2c and also includes authentication and encryption of SNMP packets. In terms of security, SNMPv3 emphasizes data security and access control.	Versiones de SNMP Las versiones de SNMP incluyen SNMPv1, SNMPv2c y SNMPv3. Tanto SNMPv1 como SNMPv2c utilizan autenticación basada en nombres de comunidad. El NMS utiliza la lista de nombres de comunidad para controlar los derechos de acceso del dispositivo, pero el agente no comprueba si el nombre de comunidad utilizado por un remitente determinado está autorizado. Además, los mensajes SNMP no se cifran para su transmisión, por lo que no se garantiza la autenticación segura ni la privacidad. En comparación con SNMPv1, SNMPv2c admite más operaciones, tipos de datos, códigos de error y protocolos de transporte. SNMPv3 proporciona todas las funciones de SNMPv1 y SNMPv2c, e incluye la autenticación y el cifrado de paquetes SNMP. En términos de seguridad, SNMPv3 prioriza la seguridad de los datos y el control de acceso.
XIII: Autenticación 802.1X	N/A	N/A	N/A	N/A	N/A	N/A

a) Admite el paso del proceso de autenticación 802.1X para garantizar la seguridad del acceso a la red Wi-Fi o en la LAN.	8021X.pdf	Overview of 802.1X Authentication	Descripción general de la autenticación 802.1X	1	Overview of 802.1X Authentication Definition 802.1X defines a port-based network access control protocol to authenticate users and control their access rights based on access ports of LAN access devices. Benefits 802.1X authentication provides high security: Authentication packets are encapsulated using EAP and multiple encryption algorithms are supported. You can select an authentication mode based on the actual scenario and obtain certificates to verify the client and server. For details about the supported authentication modes, see Authentication Mode Selection. Authentication packets and data packets are transmitted through different logical interfaces, strengthening network security. 802.1X is a Layer 2 protocol that does not require Layer 3 processing and can implement access control at the access layer.	Descripción general de la autenticación 802.1X Definición 802.1X define un protocolo de control de acceso a la red basado en puertos para autenticar a los usuarios y controlar sus derechos de acceso según los puertos de los dispositivos de acceso LAN. Beneficios La autenticación 802.1X proporciona alta seguridad: los paquetes de autenticación se encapsulan mediante EAP y se admiten múltiples algoritmos de cifrado. Puede seleccionar un modo de autenticación según la situación real y obtener certificados para verificar el cliente y el servidor. Para obtener más información sobre los modos de autenticación compatibles, consulte Selección del modo de autenticación. Los paquetes de autenticación y los paquetes de datos se transmiten a través de diferentes interfaces lógicas, lo que refuerza la seguridad de la red. 802.1X es un protocolo de capa 2 que no requiere procesamiento de capa 3 y puede implementar el control de acceso en la capa de acceso.
XIV. Selección de enlace ascendente inteligente	N/A	N/A	N/A	N/A	N/A	N/A
Selecciona de forma inteligente los enlaces del operador en función de las direcciones IP de destino, admite la configuración de la interfaz activa/en espera y el equilibrio de carga por porcentaje.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	9	Intelligent uplink selection Supports service-specific PBR and intelligently selects the optimal link based on multiple types of load balancing criteria (such as the bandwidth ratio and link health status) in multi-ISP scenarios.	Selección inteligente de enlace ascendente Admite PBR específico del servicio y selecciona inteligentemente el enlace óptimo según diversos criterios de balanceo de carga (como la relación de ancho de banda y el estado del enlace) en escenarios con múltiples ISP.
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	4	Provides dynamic and static intelligent traffic steering based on multi-egress links, selects the outbound interface based on the specified link bandwidth, weight, or priority, forwards traffic to each link based on the specified traffic steering mode, and dynamically tunes the link selection result in real time to maximize the usage of link resources and improve user experience.	Proporciona direccionamiento inteligente de tráfico, dinámico y estático, basado en enlaces de salida múltiple. Selecciona la interfaz de salida según el ancho de banda, el peso o la prioridad del enlace especificados. Reenvía el tráfico a cada enlace según el modo de direccionamiento de tráfico especificado y ajusta dinámicamente el resultado de la selección de enlace en tiempo real para maximizar el uso de los recursos del enlace y mejorar la experiencia del usuario.

	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	6	Bandwidth management Manages per-IP bandwidth based on service application identification to guarantee the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.	Gestión del ancho de banda Gestiona el ancho de banda por IP según la identificación de la aplicación del servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y modificando la prioridad de reenvío de la aplicación.
Soportar QoS basada en colas inteligentes.	Creating a QoS Policy	Creating a QoS Policy (Common Configuration)	Creación de una política de QoS (configuración común)	1	The WAN link bandwidth of an enterprise site is usually lower than that of the enterprise LAN. The egress of the enterprise site becomes the bandwidth bottleneck of outbound traffic and is prone to congestion. Therefore, QoS policies are required to ensure the experience of high-priority application traffic. To ensure the bandwidth of the local Internet access traffic of a site at the WAN egress, you can use common QoS policies to prioritize the traffic based on the traffic classifiers of different applications and schedule it accordingly. Traffic classifier: Data flows are classified based on information such as the Layer 3 ACL, application group, VLAN ID, 802.1p priority, source MAC address, destination MAC address, and Layer 2 protocol. Traffic behavior: Priorities are defined for traffic of different applications, and priority-based queue scheduling is then performed. In this case, the traffic of a high-priority application is preferentially forwarded when a congestion occurs.	El ancho de banda del enlace WAN de un sitio empresarial suele ser menor que el de la LAN empresarial. La salida del sitio empresarial se convierte en un cuello de botella del tráfico saliente y es propensa a congestionarse. Por lo tanto, se requieren políticas de QoS para garantizar la experiencia del tráfico de aplicaciones de alta prioridad.Para garantizar el ancho de banda del tráfico de acceso local a Internet de un sitio en la salida de la WAN, se pueden utilizar políticas de QoS comunes para priorizar el tráfico según los clasificadores de tráfico de las diferentes aplicaciones y programarlo en consecuencia. Clasificador de tráfico: Los flujos de datos se clasifican según información como la ACL de Capa 3, el grupo de aplicaciones, el ID de VLAN, la prioridad 802.1p, la dirección MAC de origen, la dirección MAC de destino y el protocolo de Capa 2. Comportamiento del tráfico: Se definen prioridades para el tráfico de las diferentes aplicaciones y, a continuación, se realiza una programación de colas basada en prioridades. En este caso, el tráfico de una aplicación de alta prioridad se reenvía preferentemente cuando se produce una congestión. Prioridad de cola (Los parámetros de Prioridad de cola solo deben configurarse cuando el Tipo se establece en WAN).

	Creating a QoS Policy	Creating a QoS Policy (Common Configuration)	Creación de una política de QoS (configuración común)	5	Queue priority (Parameters under Queue priority need to be set only when Type is set to WAN.) Queue priority You are advised to toggle on Queue priority for key applications that need to be preferentially guaranteed. When Queue priority is toggled on, a CPE automatically sends packets matching the traffic classifier to queues of different types based on the defined queue priorities. Priority level (This parameter needs to be set only when Queue priority is toggled on.) QoS priority. If network congestion occurs, the system preferentially transmits packets of higher-priority applications. For devices running V300, queues with the following priorities are supported:	Prioridad de cola Se recomienda activar la Prioridad de cola para las aplicaciones clave que deban garantizarse preferentemente. Cuando la Prioridad de cola está activada, un CPE envía automáticamente los paquetes que coinciden con el clasificador de tráfico a colas de diferentes tipos según las prioridades de cola definidas. Nivel de prioridad (Este parámetro solo debe configurarse cuando la Prioridad de cola está activada). Prioridad de QoS. Si se produce congestión de la red, el sistema transmite preferentemente los paquetes de las aplicaciones de mayor prioridad. Para dispositivos con V300, se admiten colas con las siguientes prioridades:
Las funcionalidades y características antes descritas apliçan para cada uno de los tipos de Firewall descritos en el presente anexo tecnico	N/A	N/A	N/A	N/A	N/A	N/A
CARACTERÍSTICAS TÉCNICAS DE LOS EQUIPOS	N/A	N/A	N/A	N/A	N/A	N/A
El equipo de seguridad FIREWALL y NAC debera apegarse a las características tecnicas que se describen a continuación:	N/A	N/A	N/A	N/A	N/A	N/A
FIREWALL TIPO 1	N/A	N/A	N/A	N/A	N/A	N/A
Requisitos de configuración física	N/A	N/A	N/A	N/A	N/A	N/A
≥2,000 Usuarios de VPN SSL simultáneos	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	USG6635F Concurrent SSL VPN Users *(Default/Maximum) 100/10000	USG6635F Usuarios VPN SSL simultáneos *(Predeterminado/Máximo) 100/10 000
≥5,000 Túneles de VPN IPSec	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	USG6635F Maximum IPsec VPN Tunnels 20,000	USG6635F Máximo de túneles VPN IPsec 20 000

≥Soporte de 10 Firewalls virtuales	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	USG6635F Virtual Firewalls: 2048	USG6635F Cortafuegos virtuales: 2048
Arquitectura de hardware	N/A	N/A	N/A	N/A	N/A	N/A
Capacidad de soportar Fuentes de poder redundantes interna o externa.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	14	Hardware Specifications USG6635F Power Supplies Optional dual AC power supplies Dual AC power supply	Especificaciones de hardware USG6635F Fuentes de alimentación: Fuentes de alimentación de CA duales opcionales
Requisitos de interfaces	N/A	N/A	N/A	N/A	N/A	N/A
≥32 Número máximo de puertos	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	5	Figure 4-2 HiSecEngine USG6635F/USG6655F/USG6685F	Figura 4-2 HiSecEngine USG6635F/USG6655F/USG6685F
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	14	Fixed Interface 8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+	"Interfaz fija 8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+
≥16 Puertos 10/100/1000 base-T GE.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	5	Figure 4-2 HiSecEngine USG6635F/USG6655F/USG6685F	Figura 4-2 HiSecEngine USG6635F/USG6655F/USG6685F
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	14	Fixed Interface 8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+	"Interfaz fija 8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+"
	01 11 Plugg Modules	SFP-1000BaseT (02314171)	SFP-1000BaseT (02314171)	1	SFP-1000BaseT Application standard 1000BASE-T Connector type RJ45	"FP-1000BaseT Estándar de aplicación 1000BASE-T Tipo de conector RJ45"

≥16 Puertos ópticos 1GE SFP	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	5	Figure 4-2 HiSecEngine USG6635F/USG6655F/USG6685F	Figura 4-2 HiSecEngine USG6635F/USG6655F/USG6685F
	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	14	Fixed Interface 8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+	"Interfaz fija 8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+"
Tarjetas de bypass de puertos eléctricos	N/A	N/A	N/A	N/A	N/A	N/A
Requisitos de desempeño	N/A	N/A	N/A	N/A	N/A	N/A
≥ 8Gbps Rendimiento IPv4 de Firewall (Throughput).	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	10	USG6635F IPv4Firewall Throughput1 (1518/512/64-byte, UDP) 35/35/35 Gbps	USG6635F Rendimiento de firewall IPv41 (1518/512/64 bytes, UDP) 35/35/35 Gbps
≥8Gbps Rendimiento IPv6 de Firewall (Throughput)	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	USG6635F IPv6 Firewall Throughput1 (1518/512/84-byte, UDP) 35/35/25 Gbps	USG6635F Rendimiento de firewall IPv61 (1518/512/84 bytes, UDP) 35/35/25 Gbps
≥3.5 Gbps Rendimiento Protección Real de Firewall (EMIX Throughput)	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	USG6635F NGFW Throughput (HTTP 100K) 16Gbps NGFW Throughput (Enterprise Mix) 8Gbps Threat Protection Throughput (Enterprise Mix) 7Gbps	USG6635F Rendimiento de NGFW (HTTP 100K) 16 Gbps Rendimiento de NGFW (Enterprise Mix) 8 Gbps Rendimiento de protección contra amenazas (Enterprise Mix) 7 Gbps
≥2.5 Gbps Rendimiento inspección SSL	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	SSL Inspection Throughput 4 Gbps SSL VPN Throughput 3Gbps	Rendimiento de inspección SSL 4 Gbps Rendimiento de VPN SSL 3 Gbps
≥4,000,000 Número de conexiones simultaneas.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	Concurrent Sessions (HTTP1.1) 20,000,000	Sesiones concurrentes (HTTP1.1) 20 000 000

≥5,000 Número de conexiones simultáneas SSL VPN(Throughput).	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	USG6635F Concurrent SSL VPN Users *(Default/Maximum) 100/10000	USG6635F Usuarios de VPN SSL concurrentes *(Predeterminado/Máximo) 100/10000"
≥5,000 Número de conexiones nuevas por segundo.	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	USG6635F New Sessions/Second 500,000	"USG6635F Nuevas sesiones/segundo: 500 000"
≥512 Mb IPsec VPN Throughput (AES-128+SHA1, 1420byte).	HUAWEI HiSecEngine	HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls	HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA	11	IPsec VPN Throughput1 (AES-256 + SHA256, 1420-byte) 30Gbps	"Rendimiento de VPN IPsec[1] (AES-256 + SHA256, 1420 bytes) 30 Gbps"

ATENTAMENTE

Edgar Hernández Soto
Apoderado Legal de Scitum, S.A. de C.V.

REFERENCIAS TECNICAS

INGLES

01 11 Plugg Modules

SFP-1000BaseT (02314171)

Table 1 SFP-1000BaseT specifications

Item	Value
Basic Information	
Module name	SFP-1000BaseT
Part Number	02314171
Model	SFP-1000BaseT
Form factor	SFP
Application standard	1000BASE-T
Connector type	RJ45
Optical fiber type	-
Working case temperature [°C(°F)]	0°C to 70°C
Transmission rate [bit/s]	10-1000M
Target transmission distance [km]	0.1 km
Transmitter Optical Characteristics	
Center wavelength [nm]	-
Maximum Tx optical power [dBm]	-
Minimum Tx optical power [dBm]	-
Minimum extinction ratio [dB]	-
Receiver Optical Characteristics	
Rx sensitivity (AVG) [dBm]	-
Overload power (AVG) [dBm]	-

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

01 11 Plugg Modules

SFP-1000BaseT (02314171)

Tabla 1 Especificaciones del SFP-1000BaseT

Artículo	Valor
Información básica	
Nombre del módulo	SFP-1000BaseT
Número de pieza	02314171
Modelo	SFP-1000BaseT
Factor de forma	SFP
Estándar de aplicación	1000BASE-T
Tipo de conector	RJ45
Tipo de fibra óptica	-
Temperatura de la caja de trabajo [°C(°F)]	0°C a 70°C
Velocidad de transmisión [bit/s]	10-1000M
Distancia de transmisión del objetivo [km]	0,1 kilómetros
Características ópticas del transmisor	
Longitud de onda central [nm]	-
Potencia óptica máxima de transmisión [dBm]	-
Potencia óptica mínima de transmisión [dBm]	-
Relación mínima de extinción [dB]	-
Características ópticas del receptor	
Sensibilidad Rx (AVG) [dBm]	-
Potencia de sobrecarga (AVG) [dBm]	-

REFERENCIAS TECNICAS

INGLES

8021X

Overview of 802.1X Authentication

Definition

802.1X defines a port-based network access control protocol to authenticate users and control their access rights based on access ports of LAN access devices.

Benefits

802.1X authentication provides high security:

- Authentication packets are encapsulated using EAP and multiple encryption algorithms are supported. You can select an authentication mode based on the actual scenario and obtain certificates to verify the client and server. For details about the supported authentication modes, see Authentication Mode Selection.
- Authentication packets and data packets are transmitted through different logical interfaces, strengthening network security.
- 802.1X is a Layer 2 protocol that does not require Layer 3 processing and can implement access control at the access layer.

802.1X Authentication System

In Figure 1, the 802.1X authentication system uses a typical client/server architecture, which consists of three types of entities: client, access device, and authentication server.

Figure 1 802.1X authentication system



- The client is usually a user terminal that initiates 802.1X authentication using the client software. The client must support Extensible Authentication Protocol over LAN (EAPoL).
- The access device is usually an 802.1X-capable network device that provides a physical or logical port for the client to access a LAN.
- The authentication server, typically a RADIUS server, performs user authentication, authorization, and accounting.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

8021X

Descripción general de la autenticación 802.1X

Definición

802.1X define un protocolo de control de acceso a red basado en puertos para autenticar usuarios y controlar sus derechos de acceso según los puertos de acceso de los dispositivos de acceso LAN.

Beneficios

La autenticación 802.1X proporciona alta seguridad:

- Los paquetes de autenticación se encapsulan mediante EAP y se admiten múltiples algoritmos de cifrado. Puede seleccionar un modo de autenticación según la situación real y obtener certificados para verificar el cliente y el servidor. Para obtener más información sobre los modos de autenticación compatibles, consulte Selección del modo de autenticación .
- Los paquetes de autenticación y los paquetes de datos se transmiten a través de diferentes interfaces lógicas, lo que fortalece la seguridad de la red.
- 802.1X es un protocolo de capa 2 que no requiere procesamiento de capa 3 y puede implementar control de acceso en la capa de acceso.

Sistema de autenticación 802.1X

En la Figura 1 , el sistema de autenticación 802.1X utiliza una arquitectura cliente/servidor típica, que consta de tres tipos de entidades: cliente, dispositivo de acceso y servidor de autenticación.

Figura 1 Sistema de autenticación 802.1X



- El cliente suele ser un terminal de usuario que inicia la autenticación 802.1X mediante el software cliente. El cliente debe ser compatible con el Protocolo de Autenticación Extensible sobre LAN (EAPoL).
- El dispositivo de acceso generalmente es un dispositivo de red compatible con 802.1X que proporciona un puerto físico o lógico para que el cliente acceda a una LAN.
- El servidor de autenticación, normalmente un servidor RADIUS, realiza la autenticación, autorización y contabilidad del usuario.

REFERENCIAS TECNICAS

INGLES

ASPFALG

ASPF/ALG Support for Known Protocols

The FW can perform ASPF/ALG for the following known protocols. For scenario-based support details, see Table 1.

Table 1 ASPF/ALG support for known protocols

Protocol	ASPF (IPv4)	ASPF (IPv6)	ALG (V4–V4)	NAT64 ALG (V4–V6/V6–V4)	DS-Lite ALG	NAT66 ALG (V6–V6)
DNS	Yes	No	Yes	Yes	No	No
FTP	Yes	Yes	Yes	Yes	Yes	Yes
H.323	Yes	No	Yes	Yes	Yes	No
ICQ	Yes	No	Yes	No	Yes	No
ILS	Yes	No	Yes	No	Yes	No
NETBIOS	Yes	No	Yes	No	Yes	No
MGCP	Yes	No	Yes	No	Yes	No
MMS	Yes	No	Yes	No	Yes	No
MSN	Yes	No	Yes	No	Yes	No
PPTP	Yes	No	Yes	No	Yes	No
QQ	Yes	No	Yes	No	Yes	No
RTSP	Yes	Yes	Yes	Yes	Yes	No
RSH	Yes	No	Yes	No	Yes	No
SCCP	Yes	No	Yes	No	Yes	No
SIP	Yes	Yes	Yes	Yes	Yes	No

Home

	(IPv4)	(IPv6)	(V4–V4)	V6/V6–V4)		V6)
SQLNET	Yes	No	Yes	No	Yes	No

Parent Topic: ASPF/ALG

Copyright © Huawei Technologies Co., Ltd.

Previous Next topic

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

ASPFALG

Compatibilidad de ASPF/ALG con protocolos conocidos

El FW puede ejecutar ASPF/ALG para los siguientes protocolos conocidos. Para obtener información detallada sobre la compatibilidad según el escenario, consulte la Tabla 1 .

Tabla 1 Compatibilidad de ASPF/ALG con protocolos conocidos

Protocolo	ASPF (IPv4)	ASPF (IPv6)	ALG (V4–V4)	NAT64 ALG (V4–V6/V6–V4)	DS-Lite ALG	ALG NAT66 (V6–V6)
DNS	Sí	No	Sí	Sí	No	No
FTP	Sí	Sí	Sí	Sí	Sí	Sí
H.323	Sí	No	Sí	Sí	Sí	No
ICQ	Sí	No	Sí	No	Sí	No
ILS	Sí	No	Sí	No	Sí	No
NETBIOS	Sí	No	Sí	No	Sí	No
MGCP	Sí	No	Sí	No	Sí	No
MMS	Sí	No	Sí	No	Sí	No
MSN	Sí	No	Sí	No	Sí	No
PPTP	Sí	No	Sí	No	Sí	No
QQ	Sí	No	Sí	No	Sí	No
RTSP	Sí	Sí	Sí	Sí	Sí	No
RSH	Sí	No	Sí	No	Sí	No
PCCC	Sí	No	Sí	No	Sí	No
SORBO	Sí	Sí	Sí	Sí	Sí	No

Inicio

o	(IPv4)	(IPv6)	(V4–V4)	V6/V6–V4)		V6)
SQLNET	Sí	No	Sí	No	Sí	No

Tema principal: **ASPF/ALG**

Derechos de autor © Huawei Technologies Co., Ltd.

Tema Siguiente

REFERENCIAS TECNICAS

INGLES

Config IPS

Configuring IPS

Context

By default, the device has multiple IPS profiles for different application scenarios, as shown in Table 1. The default IPS profiles can be viewed or directly referenced by security policies, but cannot be modified or deleted.

NOTE

When referencing a profile in a security policy, you can view the name of the default profile in the drop-down list.

Table 1 Default IPS profiles

Profile Name	Target	Severity	Operating System	Protocol	Category	Action	Application Scenario
video_surveillance	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	DNS, HTTP, FTP, Telnet, SSH, RTSP, SSL, UDP, TCP	All	Default	The intrusion prevention profile applies when the device is deployed in video security scenarios.
strict	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	Block	The intrusion prevention profile applies to the scenarios in which the device is required to block all matched packets.
web_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	DNS, HTTP, FTP	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a web server.
file_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	DNS, SMB, NetBIOS, NFS, Sun RPC, MSRPC, file, and Telnet	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a file server.
dns_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	DNS	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a DNS server.
mail_server	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	DNS, IMAP4, SMTP, POP3	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a mail server.
inside_firewall	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	Protocols other than Telnet and TFTP	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed behind a firewall.
dmz	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	Protocols other than NetBIOS, NFS, SMB, Telnet and TFTP	All	Default	The profile applies to the scenarios in which the device is deployed in front of the DMZ zone.
outside_firewall	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	Except **Scanner**	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in front of a firewall.
ids	All	Low, Medium, High	Unix-like, Windows, Android, iOS, Other	All	All	Alert	The intrusion prevention profile applies to the scenarios in which the device is deployed off-line as an IDS.
default	All	Low, Medium	Unix-like, Windows,	All	All	Default	The intrusion prevention profile applies to the scenarios in which the device is deployed in-

Profile Name	Target	Severity	Operating System	Protocol	Category	Action	Application Scenario
		m, High	Android, iOS, Other				line as an IPS.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Config IPS

Configuración de IPS

Contexto

De forma predeterminada, el dispositivo tiene varios perfiles IPS para diferentes escenarios de aplicación, como se muestra en la Tabla 1. Las políticas de seguridad pueden ver o hacer referencia directa a los perfiles IPS predeterminados, pero no pueden modificarse ni eliminarse.

NOTE

Al hacer referencia a un perfil en una política de seguridad, puede ver el nombre del perfil predeterminado en la lista desplegable.

Tabla 1 Perfiles IPS predeterminados

Nombre del perfil	Objetivo	Gravedad	Sistema operativo	Protocolo	Categoría	Acción	Escenario de aplicación
videovigilancia	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	DNS, HTTP, FTP, Telnet, SSH, RTSP, SSL, UDP, TCP	Todo	Por defecto	El perfil de prevención de intrusiones se aplica cuando el dispositivo se implementa en escenarios de seguridad de video.
estricto	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	Todo	Todo	Bloquear	El perfil de prevención de intrusiones se aplica a los escenarios en los que se requiere que el dispositivo bloquee todos los paquetes coincidentes.
servidor web	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	DNS, HTTP, FTP	Todo	Por defecto	El perfil de prevención de intrusiones se aplica a los escenarios en los que el dispositivo se implementa frente a un servidor web.
servidor de archivos	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	DNS, SMB, NetBIOS, NFS, Sun RPC, MSRPC, archivos y Telnet	Todo	Por defecto	El perfil de prevención de intrusiones se aplica a los escenarios en los que el dispositivo se implementa frente a un servidor de archivos.
servidor dns	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	DNS	Todo	Por defecto	El perfil de prevención de intrusiones se aplica a los escenarios en los que el dispositivo se implementa frente a un servidor DNS.
servidor de correo	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	DNS, IMAP4, SMTP, POP3	Todo	Por defecto	El perfil de prevención de intrusiones se aplica a los escenarios en los que el dispositivo se implementa frente a un servidor de correo.
cortafuegos interno	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	Protocolos distintos de Telnet y TFTP	Todo	Por defecto	El perfil de prevención de intrusiones se aplica a los escenarios en los que el dispositivo se implementa detrás de un firewall.
zona desmilitarizada	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	Protocolos distintos de NetBIOS, NFS, SMB, Telnet y TFTP	Todo	Por defecto	El perfil se aplica a los escenarios en los que el dispositivo se implementa frente a la zona DMZ.
cortafuegos externo	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	Todo	Excepto **escáner**	Por defecto	El perfil de prevención de intrusiones se aplica a los escenarios en los que el dispositivo se implementa frente a un firewall.
identificaciones	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	Todo	Todo	Alerta	El perfil de prevención de intrusiones se aplica a los escenarios en los que el dispositivo se implementa fuera de línea como un IDS.

Nombre del perfil	Objetivo	Gravedad	Sistema operativo	Protocolo	Categoría	Acción	Escenario de aplicación
por defecto	Todo	Bajo, Medio, Alto	Similar a Unix, Windows, Android, iOS, Otros	Todo	Todo	Por defecto	El perfil de prevención de intrusiones se aplica a los escenarios en los que el dispositivo se implementa en línea como IPS.

REFERENCIAS TECNICAS

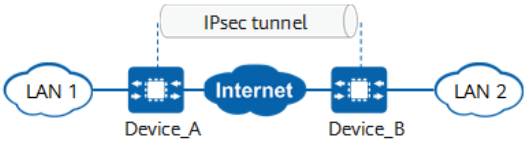
INGLES

Config IPSEC

Configuring Point-to-Point IPsec

Context

Internet Protocol Security (IPsec) is a suite of protocols for securing IP networks by allowing two devices to establish an IPsec encrypted tunnel. Data is forwarded through the IPsec encrypted tunnel, which effectively protects data.
IPsec is classified into point-to-point IPsec and point-to-multipoint IPsec based on networking requirements.
Point-to-point IPsec, also called LAN-to-LAN IPsec, is used to establish an IPsec tunnel between two devices to secure communication between LANs, as shown in the following figure.

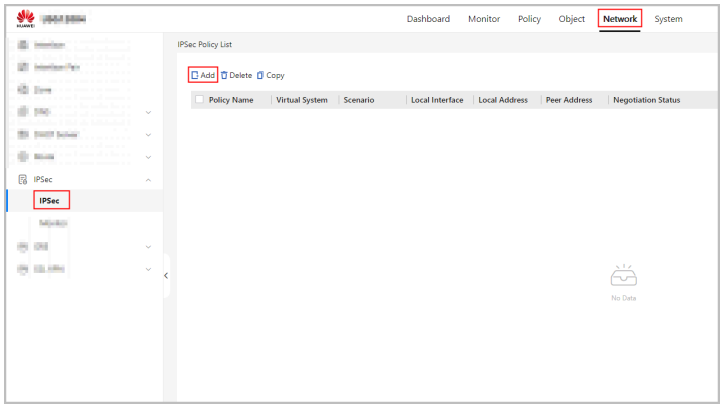


NOTE

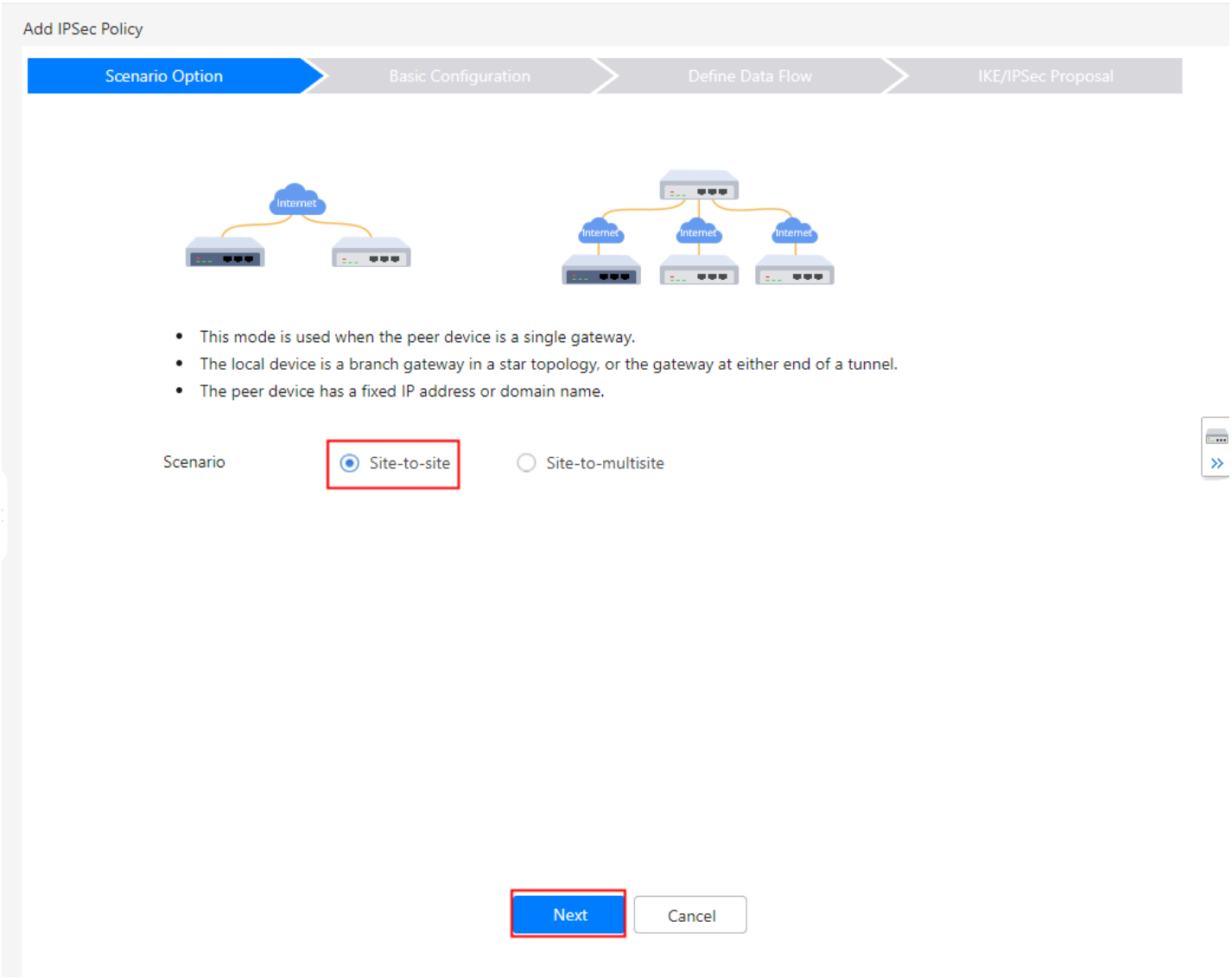
After an IPsec policy is deleted or modified (for example, the interface where the policy applies, data flows to be encrypted, local ID type, or authentication mode is changed), the IPsec policy group to which this policy belongs will become invalid, resulting in service interruption. To avoid this, you are advised to disable the IPsec policy before modifying it, and then either copy the policy or create a new one.

Procedure

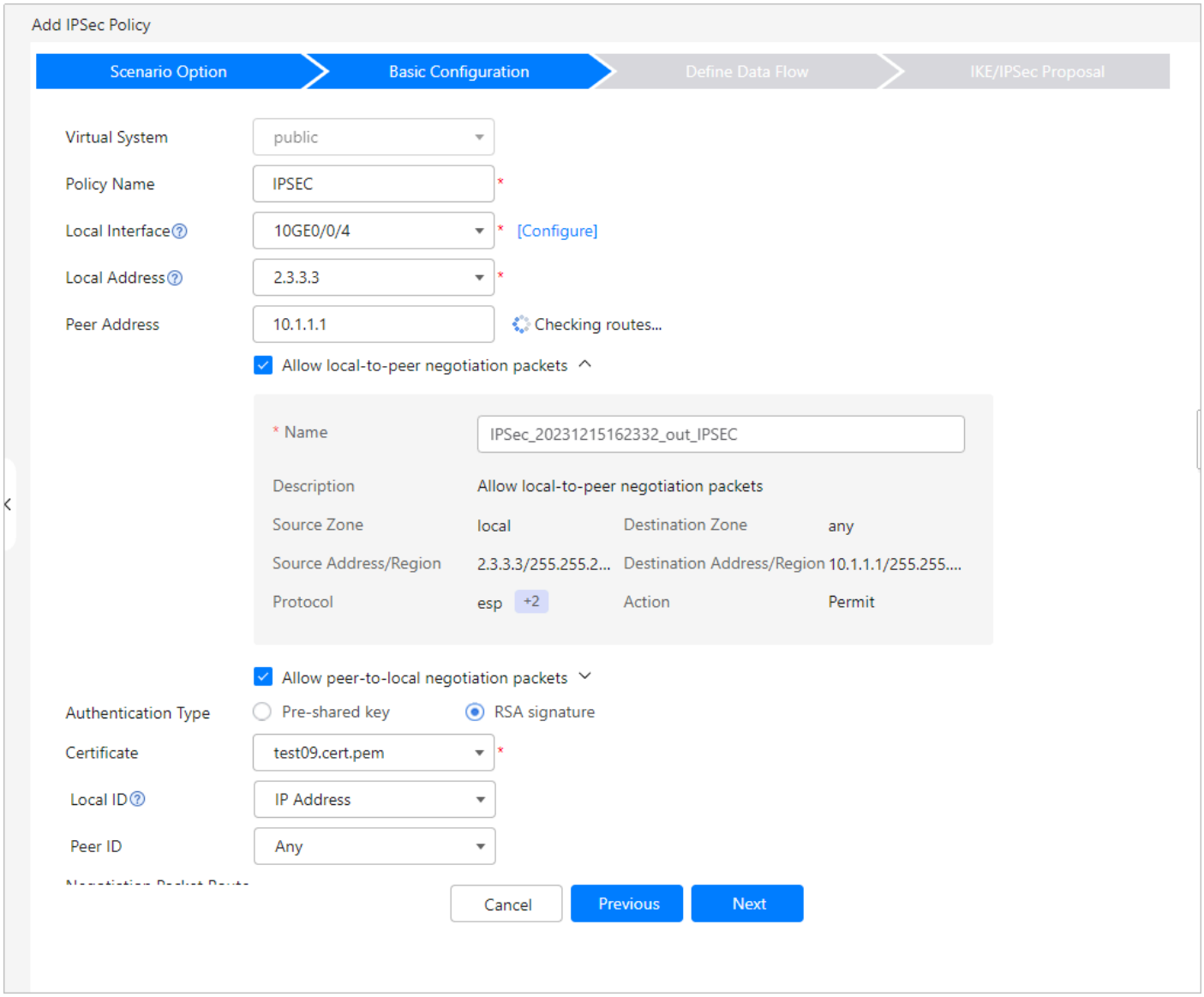
1. Choose **Network** > **IPSec** > **IPSec**.
2. Click **Add** to add an IPsec policy.



3. Select **Site-to-site** in **Scenario** and click **Next**.



4. On the **Basic Configuration** tab page, configure basic information about the IPsec policy and click **Next**.



- Configure the basic parameters of the IPsec policy.

Parameter	Description
Policy Name	Specify a name for the IPsec policy.
Local Interface	Select an interface from the drop-down list on which the IPsec policy is to be applied. This interface can be a physical interface or a tunnel interface. The physical interface must be the interface that connects the local end to the peer gateway, and it is usually the WAN interface of the device. The local end uses this interface to establish a tunnel to the peer gateway.
Local Address	Select an IP address for the local gateway to establish a tunnel to the peer gateway. If the **Local Interface** has several local IP addresses, select an IP address accessible from the peer gateway. In a hot standby network, select a virtual IP address for the local interface.
Peer Address	Specify the IP address or domain name of the peer gateway, for example, 1.1.1.1 or test1.com. In common practices, the IP address or domain name must be specified to restrict the access from other gateways. Leave this parameter unspecified if the peer gateway does not have a fixed IP address or domain name. In this case, the local gateway cannot initiate negotiations.
Allow local-to-peer negotiation packets	If Allow local-to-peer negotiation packets is selected, a security policy with **Action** set to **Permit** is created for negotiation packets from the local end to the peer end. The security policy name can be modified.

Parameter	Description
	Select this option to ensure that negotiation packets can be exchanged. If no security policy is configured to permit negotiation packets, choose **Policy** > **Security Policy** to create a security policy to permit negotiation packets from the local end to the peer end.
Allow peer-to-local negotiation packets	If **Allow peer-to-local negotiation packets** is selected, a security policy with **Action** set to **Permit** is created for negotiation packets from the peer end to the local end. The security policy name can be modified. Select this option to ensure that negotiation packets can be exchanged. If no security policy is configured to permit negotiation packets, choose **Policy** > **Security Policy** to create a security policy to permit negotiation packets from the peer end to the local end.

- Configure tunnel authentication.
  There are three IPsec tunnel authentication modes, and some of their parameter values are different.
  - Pre-shared key

Parameter	Description
Authentication Type	**Pre-shared key**
Pre-shared key	Enter the key negotiated between administrators of both sides.
Local ID	The local ID identifies the local gateway for authentication by the peer gateway. The type and value must be the same as those of the **Peer ID** of the peer device. ■ **IP Address**: Use the local IP address as the local ID. ■ **Name**: If this option is selected, the local gateway name is used as the default ID. You can specify another character string. ■ **User-FQDN**: If this option is selected, the local gateway name is used as the default ID. You can specify another character string. ■ **ESN**: If this option is selected, the local gateway ESN is used as the local ID. You can specify another character string.
Peer ID	The peer ID identifies the peer device. Obtain this parameter value from the administrator of the peer device. The type and value must be the same as those of the **Local ID** specified on the peer device. Select **Any** if no authentication is required. If only string match is required, select **Any Type**. **NOTE:** When the peer ID type is IP address, the device uses **Peer Address** configured in Configure the basic para... as the peer ID for consistency check with the local ID configured on the peer device.

  - RSA signature

Parameter	Description
Authentication Type	**RSA signature**
Certificate	Select the local certificate obtained from the CA when this parameter is available. Certain information in the certificate will be sent to the peer gateway for authentication. For details about certificate uploading, see Local Certificates.
Local ID	After the certificate is loaded, select the local ID type. The system automatically extracts the corresponding field value from the certificate as the local ID. The local ID can be one of the following items (corresponding to the specific fields in the certificate): ■ **IP Address**: The **IP Address** field value serves as the local ID. ■ **DN**: The **Subject** field value serves as the local ID. ■ **Name**: The **Commonname** field value serves as the local ID. ■ **User-FQDN**: The **Email** field value serves as the local ID.

Parameter	Description
Peer ID	The peer ID identifies the peer device. Obtain this parameter value from the administrator of the peer device. The type and value must be the same as those of the **Local ID** specified on the peer device. Select **Any** if no authentication is required. If only string match is required, select **Any Type**. **NOTE:** When the peer ID type is IP address, the device uses **Peer Address** configured in Configure the basic para... as the peer ID for consistency check with the local ID configured on the peer device.

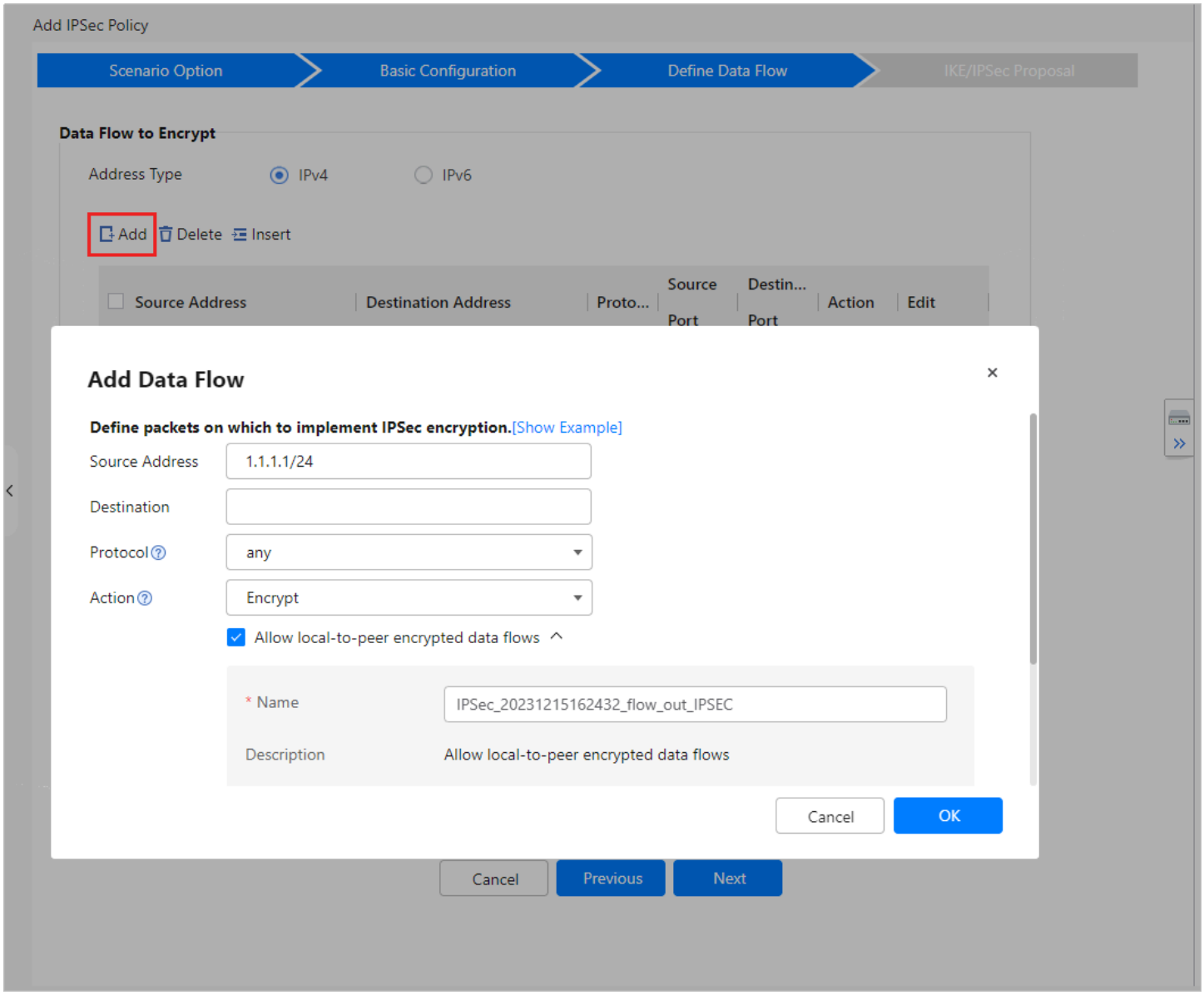
- SM2 digital envelope

NOTE

By default, the device does not support this parameter (the device does not support SA negotiation through IKEv1). To use this parameter, you need to load the IKEv1 feature package.

Parameter	Description
Authentication Type	**SM2 digital envelope**
Encryption Realm	Select the PKI realm of the encryption certificate requested and imported from the SM2 server.
Signature Realm	Select the PKI realm of the signature certificate requested and imported from the SM2 server. In addition, the CA certificates used by the devices at both ends need to be imported to this signature realm.

5. Configure the data flows to be encrypted through the IPsec tunnel.

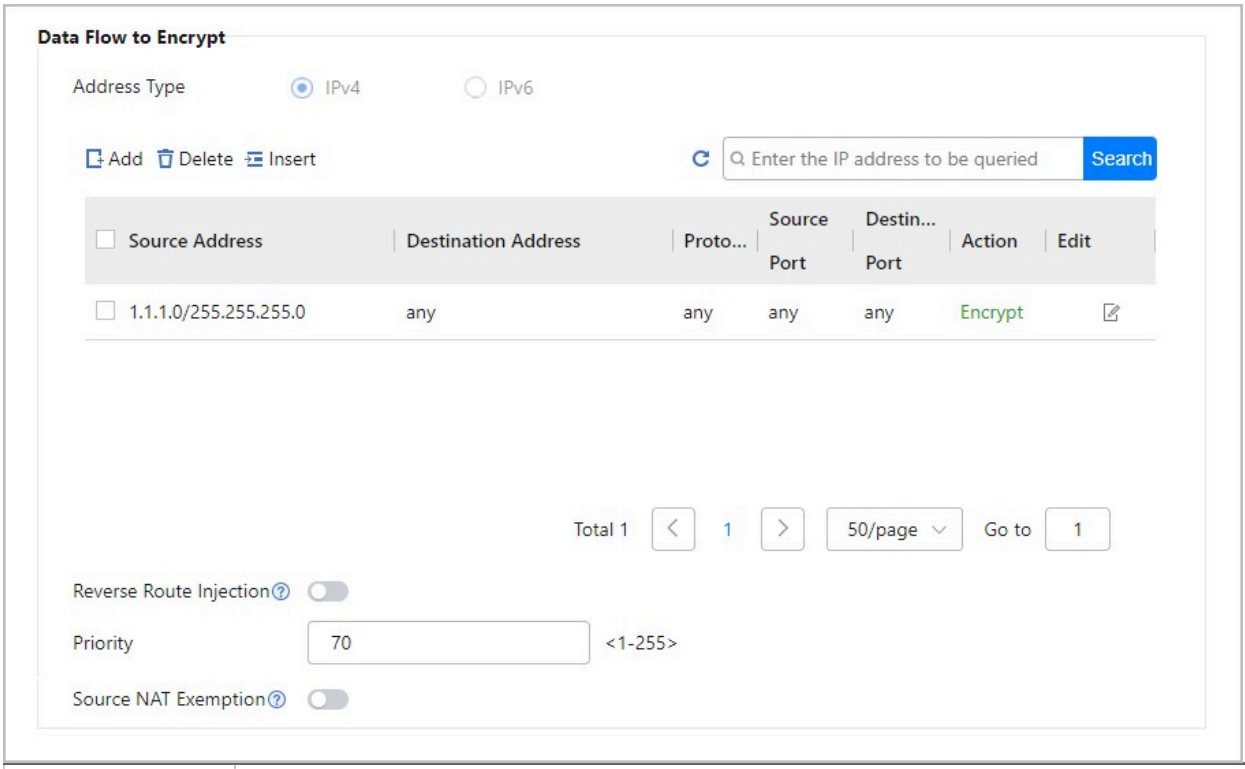


Generally, only some data flows need to be encrypted before they are sent to the peer, and some data flows are directly transmitted to the Internet. To avoid those data flows to be transmitted directly through the Internet entering the tunnel, you need to configure certain rules to restrict them.
You can configure multiple rules in a list. Data flows match the rules from top to bottom. If a match is found, data flows are processed according to the specified action, and the matching process ends.
Under **Data Flow to Encrypted**, select **IPv4** or **IPv6** for **Address Type** and click **Add**.

Parameter	Description
Source Address	Specify the source address of the data flows to be encrypted through the tunnel. In common practices, the source address is usually the address of the intranet subnet to be protected. Only the IP address/subnet mask format is supported. You can enter a single IP address (for example, 192.168.1.1/32 or 192.168.1.1/255.255.255.255) or a network segment (for example, 192.168.1.0/24 or 192.168.1.0/255.255.255.0). You can enter a single IP address.
Destination Address	Specify the destination address of the data flows to be encrypted through the tunnel. In common practices, the destination address is usually the address of the subnet to be accessed on the peer intranet. Only the IP address/subnet mask format is supported. You can enter a single IP address (for example, 192.168.1.1/32 or 192.168.1.1/255.255.255.255) or a network segment (for example, 192.168.1.0/24 or 192.168.1.0/255.255.255.0). You can enter a single IP address.
Protocol	Specify the protocol of the data flows to be encrypted through the tunnel. You can configure a TCP or UDP port to encrypt the traffic of a specified service. For example, you can configure TCP port 80 to encrypt HTTP traffic and UDP port 69 to encrypt TFTP traffic. If you do not know the protocol and port or there is no need to perform protocol-based restriction, leave this parameter unspecified or set it to **any**.

Parameter	Description
Source Port	This parameter is available when **Protocol** is set to **TCP** or **UDP**. Specify the source port number from which the data flows to be encrypted through the tunnel are originated.
Destination Port	This parameter is available when **Protocol** is set to **TCP** or **UDP**. Specify the destination port number for which the data flows to be encrypted through the tunnel are destined.
Action	Specify the action for data flows that match the preceding conditions. • **Encrypt** indicates that the data flows are allowed to be encrypted through the tunnel. • **Do Not Encrypt** indicates that the data flows are not allowed to be encrypted through the tunnel. The **Do Not Encrypt** action is used to exempt traffic of some clients from encryption. For example, to encrypt the traffic from all hosts on subnet 192.168.1.0/24 except a host at 192.168.1.2, configure a rule for exempting traffic of the host at 192.168.1.2 from encryption and a rule for encrypting traffic of hosts on subnet 192.168.1.0/24.
Allow local-to-peer encrypted data flows	If **Allow local-to-peer encrypted data flows** is selected, a security policy with **Action** set to **Permit** is created for encrypted data flows from the local end to the peer end. The security policy name can be modified. Select this option to ensure that encrypted data flows can be exchanged. If no security policy is configured to permit encrypted data flows, choose **Policy** > **Security Policy** to create a security policy to permit encrypted data flows from the local end to the peer end.
Allow peer-to-local encrypted data flows	If **Allow peer-to-local encrypted data flows** is selected, a security policy with **Action** set to **Permit** is created for encrypted data flows from the peer end to the local end. The security policy name can be modified. Select this option to ensure that encrypted data flows can be exchanged. If no security policy is configured to permit encrypted data flows, choose **Policy** > **Security Policy** to create a security policy to permit encrypted data flows from the peer end to the local end.

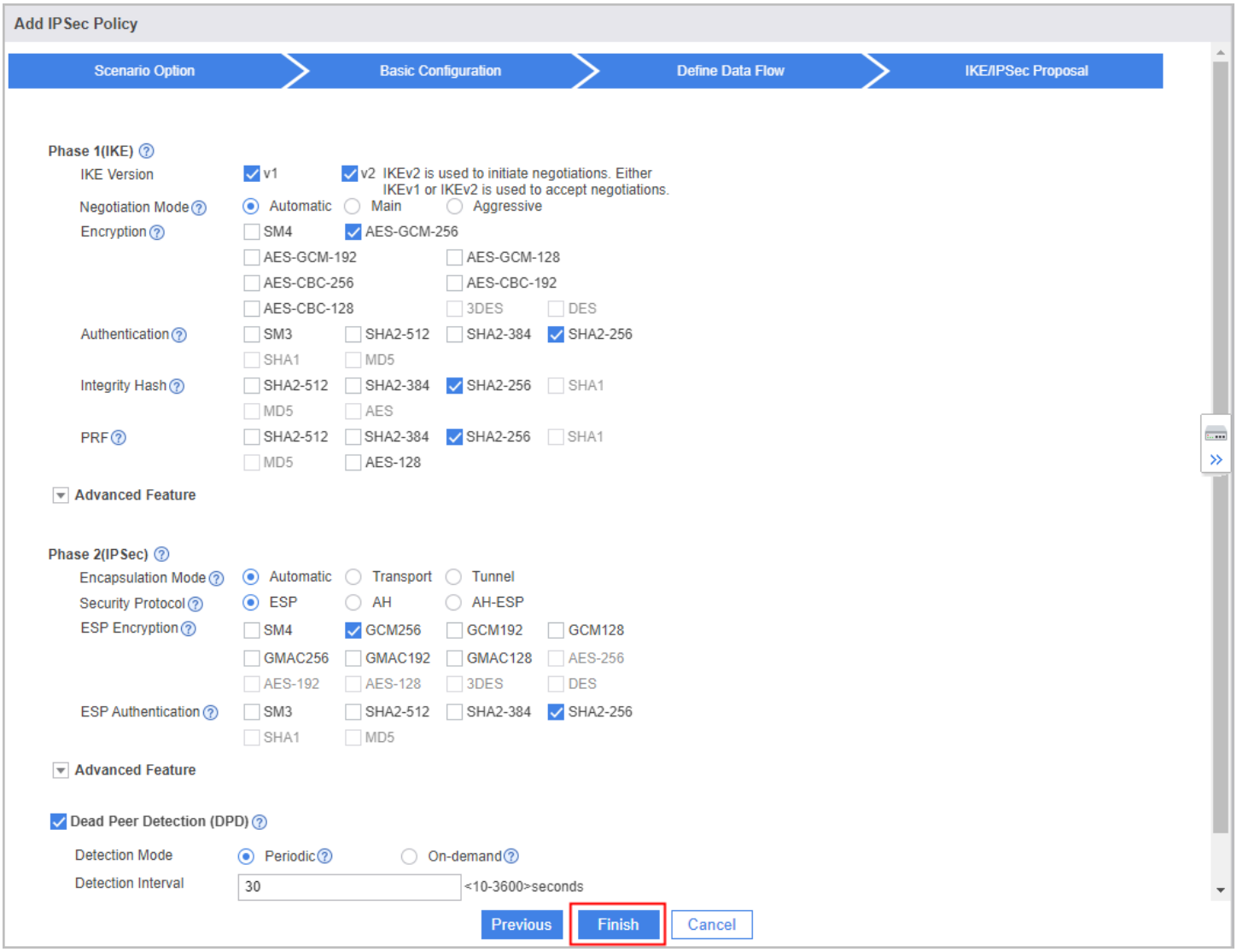
You can toggle on **Reverse Route Injection** if necessary.



Parameter	Description
Reverse Route Injection	If this function is enabled, the device automatically installs the routes destined for the peer network, eliminating the need for administrators to configure these routes manually. This function is usually configured on the HQ gateway connected to multiple branches.

Parameter	Description
Priority	This parameter is displayed after **Reverse Route Injection** is enabled. You can set **Priority** if necessary. For example, if the device has other routes to the same destination, you can specify the same priority for them to implement load balancing, or different priorities to implement route backup.
Source NAT Exemption	Assume that a branch gateway is a NAT gateway with source NAT configured that controls branch access to the HQ. When this NAT gateway receives a cleartext packet that matches a source NAT policy, it will translate the packet's source address. However, the translation makes the packet no longer match the ACL that defines the data flows protected by IPsec. Consequently, the packet cannot enter the IPsec tunnel for encrypted transmission and is discarded. To solve this problem, you can enable NAT exemption in the IPsec policy at the branch. After this function is enabled, data flows to be encrypted by IPsec are forwarded directly through IPsec tunnels, without being processed based on source NAT policies. **NOTE:** This parameter can be configured only when **Address Type** of the data flows to be encrypted is set to **IPv4**.

6. Set parameters on the **IKE/IPSec Proposal** tab page.



Multiple sets of default security proposal parameters are pre-defined in the system. If the default security proposal cannot meet the negotiation requirements, you can modify the parameter settings. All parameters except the SA timeout period must be set to the same values at both ends.
You can select multiple algorithms for the security proposal. Then the tunnel peers will preferentially use the algorithm with the highest security for the IKE negotiation. On the web UI, the algorithms are ranked in descending order of their priorities from left to right.

NOTE

- By default, the device does not support SA negotiation through IKEv1. To use IKEv1-related functions, you need to install the IKEv1 feature package. Log in to the Huawei technical support website, search for the corresponding product and version in the software download area, and download the **IKEv1_*Product_Version*.ccx**. For details about how to install the feature package, see "Configuring Module Loading" in CLI Configuration Guide > System Management Configuration > Upgrade Maintenance Configuration.
- By default, IPsec does not support weak security algorithms. If you select a weak security algorithm, an error message will be displayed.

  For security purposes, you are not advised to use the weak security algorithm or protocol provided by this feature. If you need to use the weak security algorithm or protocol, run the **install feature-software WEAKEA** command to install the weak security algorithm and protocol software package WEAKEA. By default, the device has the weak security algorithm and protocol software package WEAKEA. For details about how to install or uninstall the software package, see "Upgrade Maintenance Configuration" in *CLI Configuration Guide > System Management Configuration*.
- The AES-CBC-256, AES-CBC-192, and AES-CBC-128 security algorithms can be configured after the IKEv1 feature package or the weak security algorithm and protocol software package WEAKEA is installed.
- The 3DES, AES-128, AES-128-GCM-128, AES-128-GMAC, AES-192, AES-192-GCM-128, AES-192-GMAC, AES-256, AES-256-GCM-128, AES-256-GMAC, AES-GCM-128, AES-GCM-192, AES-GCM-256, AES-XCBC-128, AES-XCBC-96, DES, GROUP1, GROUP14, GROUP15, GROUP16, GROUP18, GROUP19, GROUP2, GROUP20, GROUP21, GROUP24, GROUP5, HMAC-MD5, HMAC-MD5-96, HMAC-SHA1, HMAC-SHA1-96, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, MD5, PKCS1, PSS, SHA1, SHA2-256, SHA2-384, SHA2-512, SM3 and SM4 security algorithms can be configured only after the weak security algorithm and protocol software package WEAKEA is installed.

Parameter	Description
Phase 1 (IKE) Parameters	
IKE Version	Select **v1** or **v2** to specify the version of the IKE protocol used in negotiations with the peer gateway. For details on IKE versions. If both versions are selected, the local end can respond to both IKEv1 and IKEv2 requests but initiate only IKEv2 requests.
Negotiation Mode	Select the IKEv1 negotiation mode. • Automatic: Both the main mode and aggressive mode are acceptable in the response to IKE requests, but only the main mode is acceptable in the initiation of IKE requests. • Main Mode: Only the main mode is acceptable in the negotiation. • Aggressive Mode: Only the aggressive mode is acceptable in the negotiation.
Encryption	Select an encryption algorithm as required. **NOTE:** SM4 can meet the high confidentiality and security requirements, but it takes a comparatively long time for processing. The 3DES, AES-CBC-256, AES-CBC-192, AES-CBC-128, and DES algorithms provide low security and so are not recommended. SM4 encryption algorithm is available only when **IKE Version** is set to **v1**. The AES-GCM-256, AES-GCM-192, and AES-GCM-128 encryption algorithms are available only when **IKE Version** is set to **v2**.
Authentication	This parameter is available only after you select **v1** in **IKE Version**. Select the algorithm used in data source authentication. **NOTE:** SM3 can meet the high confidentiality and security requirements, but it takes a comparatively long time for processing. The MD5 and SHA1 algorithms provide low security and so are not recommended.
Integrity Hash	This parameter is available only after you select **v2** in **IKE Version**. Specify the algorithm for data integrity checks if IKEv2 is used in the negotiation. **NOTE:** The AES, MD5, and SHA1 algorithms provide low security and so are not recommended.

Parameter	Description
PRF	This parameter is available only after you select **v2** in **IKE Version**. Select the algorithm used in data source authentication. **NOTE:** The MD5 and SHA1 algorithms provide low security and so are not recommended.
DH Group	This parameter is displayed when you click **Advanced Feature**. Select the key exchange methods.
SA Timeout	This parameter is displayed when you click **Advanced Feature**. Set the IKE SA lifetime. When the lifetime is about to expire, the device will negotiate a new SA. The new SA will immediately replace the old SA once it is established. Specify the timeout period, in seconds.
Phase 2 (IPSec) Parameters	
Encapsulation Mode	Select an IPsec encryption mode. • Automatic: Both the transport mode and tunnel mode can be used to respond to negotiation requests, but only the tunnel mode can be used to initiate negotiation requests. • Transport: It is used in establishing tunnels between mobile devices and the VPN gateway. • Tunnel: It is usually used in establishing tunnels between the VPN gateways.
Security Protocol	Select an IPsec protocol. • Encapsulating Security Payload (ESP): Encrypts and authenticates the packet payload. • Authentication Header (AH): Authenticates the entire packet, but does not encrypt the packet. • AH-ESP: Encrypts and authenticates the entire packet.
ESP Encryption	This parameter is available if you select **ESP** or **AH-ESP** in **Security Protocol**. Select the algorithm used in data encryption. **NOTE:** SM4 can meet the high confidentiality and security requirements, but it takes a comparatively long time for processing. The GCM256, GCM192, GCM128, GMAC256, GMAC192 and GMAC128 algorithms are recommended for security purposes. The AES-256, AES-192, AES-128, 3DES and DES algorithms are not recommended.
ESP Authentication	This parameter is available if you select **ESP** or **AH-ESP** in **Security Protocol**. Select the algorithm used in data source authentication. **NOTE:** SM3 can meet the high confidentiality and security requirements, but it takes a comparatively long time for processing. The SHA2-256, SHA2-384, and SHA2-512 algorithms are recommended for security purposes. The MD5 and SHA1 algorithms are not recommended.
AH Authentication	This parameter is available if you select **AH** or **AH-ESP** in **Security Protocol**. Select the algorithm used in data source authentication. **NOTE:** SM3 can meet the high confidentiality and security requirements, but it takes a comparatively long time for processing. The SHA2-256, SHA2-384, and SHA2-

Parameter	Description
	512 algorithms are recommended for security purpose. MD5 and SHA1 are not recommended.
PFS	This parameter is displayed when you click **Advanced Feature**. Select the key exchange methods. A greater group ID indicates a longer key and higher security. **NONE** indicates no extra key exchanges are to be performed.
SA Timeout	This parameter is displayed when you click **Advanced Feature**. The IPsec tunnel is renegotiated to ensure security when the establishment time or transmitted traffic volume reaches the specified threshold. Specify the idle period for SA renegotiation in **Based on Time**. Specify the traffic volume threshold in **Based on Traffic**. When either of the preceding conditions is met after an IPsec tunnel is established, IPsec SA renegotiates the tunnel. The renegotiation does not disconnect the currently available tunnel.
Dead Peer Detection (DPD)	
Detection Mode	After **Dead Peer Detection (DPD)** is enabled, the local end sends DPD packets to detect whether the peer gateway is still alive. Available detection methods are as follows: • Periodic: The local end resends DPD packets if no packet is received from the peer device within the period specified in **Detection Interval**. • On-demand: The local end sends DPD packets only when the communication is required and no packet is received from the peer device within the period specified in **Detection Interval**. Enable or disable this function on both ends at the same time. A detection failure is logged if no response is received within the period specified in **Retry Interval** after the local end sends a DPD packet. After five consecutive detection failures, the peer is regarded to be down and the tunnel is automatically removed.
Detection Interval	Specify a period in **Detection Interval**, in seconds.
Retry Interval	Specify a period in **Retry Interval**, in seconds. This parameter is applicable only when the tunnel uses IKEv1.

7. Click **Finish**. The newly configured IPsec policy is displayed in the policy list.

Follow-up Procedure

- **Cloning an IPsec Policy**
  Select an existing IPsec policy in **IPSec Policy List** and click **Copy** to create an IPsec policy using the selected policy as a template. On the configuration page of the newly created IPsec policy, some parameters (such as the scenario, authentication mode, and security proposal) have been configured. You only need to set the remaining parameters (such as policy name, pre-shared key, and data flow to be encrypted).
- **Viewing and Exporting Recommended Settings for the Peer Device**
  Consistent parameter settings on local and peer devices are important for IPsec negotiation to succeed. This helpful function allows you to export the recommended peer settings and send them to the administrator of the peer device for reference.

1. On the **Add IPSec Policy** or **Modify IPSec Policy** page, you can click the peer device for reference icon  to display the recommended peer settings.
2. The recommended brief settings are displayed on the right pane. Click **export** to export the detailed settings.

REFERENCIAS TECNICAS

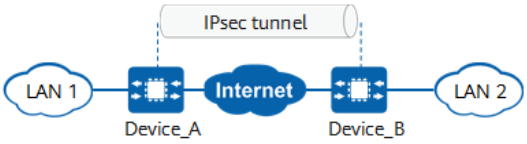
TRADUCCION SIMPLE

Config IPSEC

Configuración de IPsec punto a punto

Contexto

El Protocolo de Seguridad de Internet (IPsec) es un conjunto de protocolos para proteger las redes IP, permitiendo que dos dispositivos establezcan un túnel cifrado IPsec. Los datos se transmiten a través de este túnel, lo que los protege eficazmente.
IPsec se clasifica en IPsec punto a punto e IPsec punto a multipunto según los requisitos de la red.
IPsec punto a punto, también llamado IPsec LAN a LAN, se utiliza para establecer un túnel IPsec entre dos dispositivos para asegurar la comunicación entre LAN, como se muestra en la siguiente figura.

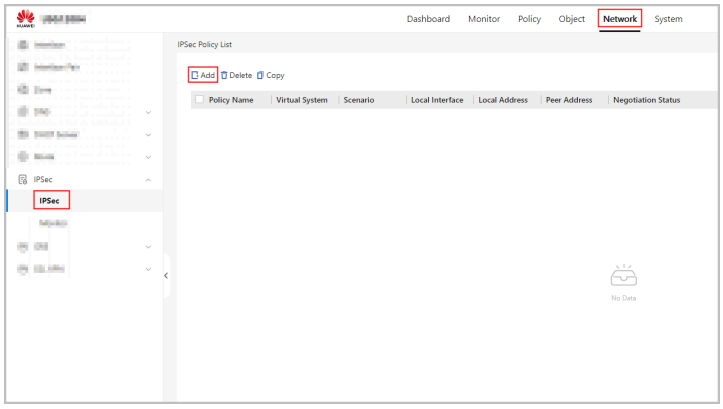


NOTE

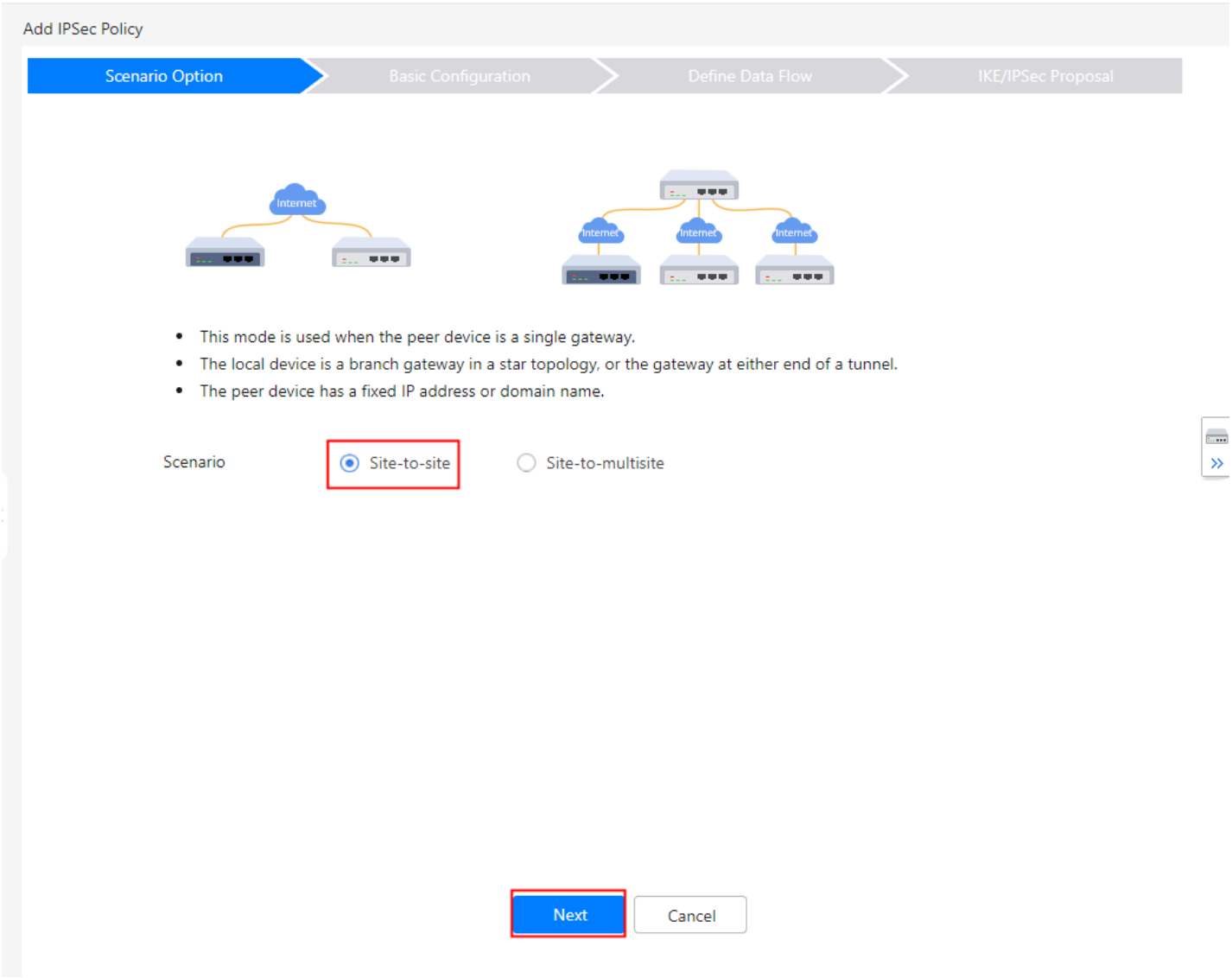
Tras eliminar o modificar una política IPsec (por ejemplo, si se modifica la interfaz donde se aplica, los flujos de datos que se cifrarán, el tipo de ID local o el modo de autenticación), el grupo de políticas IPsec al que pertenece dejará de ser válido, lo que provocará la interrupción del servicio. Para evitarlo, se recomienda deshabilitar la política IPsec antes de modificarla y, a continuación, copiarla o crear una nueva.

Procedimiento

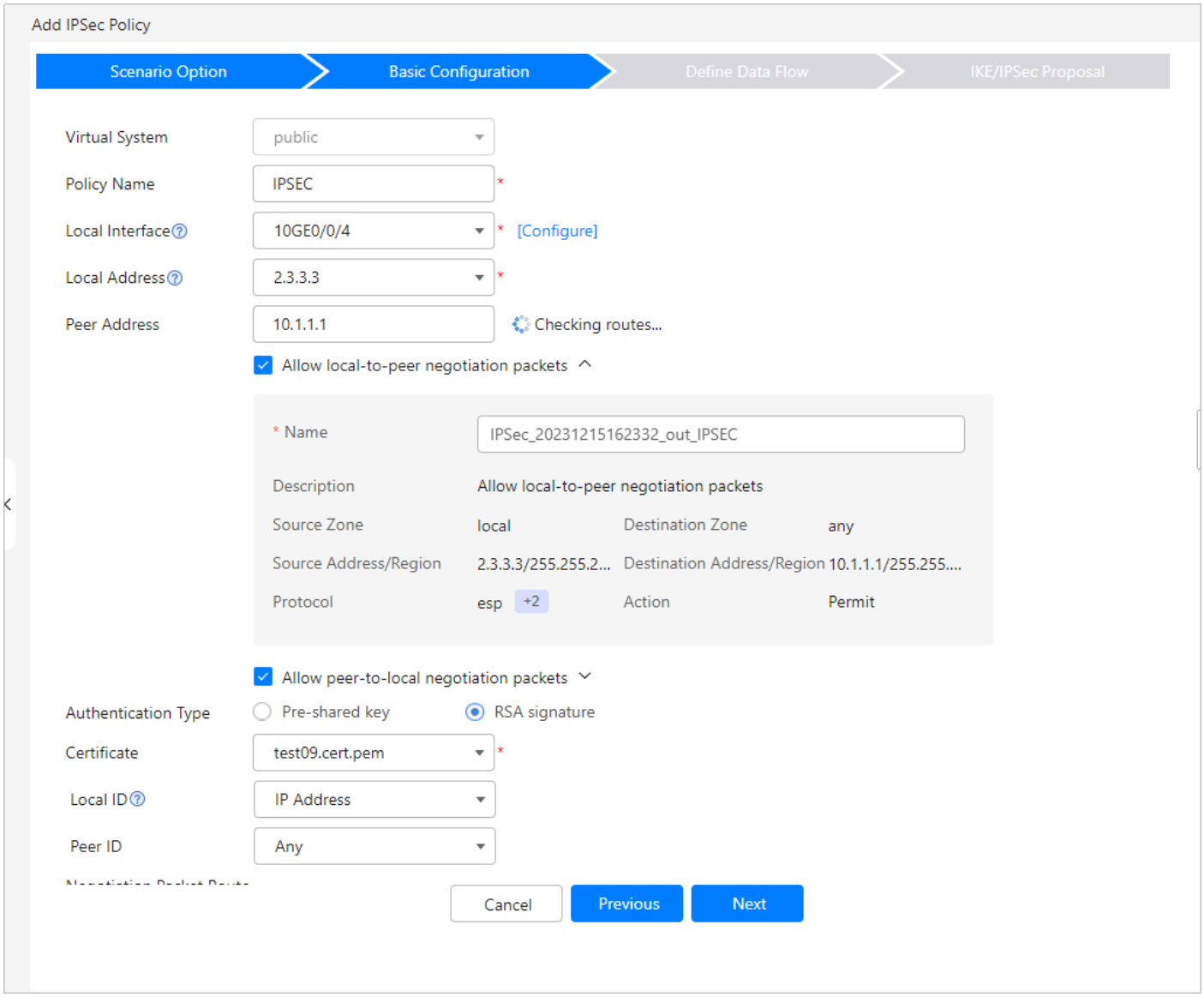
1. Seleccione **Red** > **IPSec** > **IPSec** .
2. Haga clic en **Agregar** para agregar una política IPsec.



3. Seleccione **Sitio a sitio** en **Escenario** y haga clic **en Siguiente** .



4. En la página de la pestaña **Configuración básica** , configure la información básica sobre la política IPsec y haga clic **en Siguiente** .



- Configurar los parámetros básicos de la política IPsec.

Parámetro	**Descripción**
Nombre de la póliza	Especifique un nombre para la política IPsec.
Interfaz local	Seleccione una interfaz de la lista desplegable donde se aplicará la política IPsec. Esta interfaz puede ser física o de túnel. La interfaz física debe ser la que conecta el extremo local con la puerta de enlace del par, y suele ser la interfaz WAN del dispositivo. El extremo local utiliza esta interfaz para establecer un túnel con la puerta de enlace del par.
Dirección local	Seleccione una dirección IP para la puerta de enlace local a fin de establecer un túnel con la puerta de enlace del par. Si la **interfaz local** tiene varias direcciones IP locales, seleccione una dirección IP accesible desde la puerta de enlace del par. En una red de espera activa, seleccione una dirección IP virtual para la interfaz local.
Dirección de pares	Especifique la dirección IP o el nombre de dominio de la puerta de enlace de pares, por ejemplo, 1.1.1.1 o test1.com. Generalmente, se debe especificar la dirección IP o el nombre de dominio para restringir el acceso desde otras puertas de enlace. Deje este parámetro sin especificar si la puerta de enlace del par no tiene una dirección IP o un nombre de dominio fijos. En este caso, la puerta de enlace local no puede iniciar negociaciones.
Permitir paquetes de negociación de local a par	Si se selecciona "Permitir paquetes de negociación local a par", se crea una política de seguridad con **la opción "Acción"** establecida en " **Permitir"** para los paquetes

Parámetro	Descripción
	de negociación del extremo local al extremo par. El nombre de la política de seguridad se puede modificar. Seleccione esta opción para garantizar el intercambio de paquetes de negociación. Si no hay una política de seguridad configurada para permitir paquetes de negociación, seleccione **Política** > **Política de seguridad** para crear una política de seguridad que permita el intercambio de paquetes de negociación desde el extremo local hasta el extremo del par.
Permitir paquetes de negociación de punto a punto local	Si se selecciona **Permitir paquetes de negociación entre pares (peer-to-local) , se crea una política de seguridad con la acción** establecida en **Permitir** para los paquetes de negociación entre pares (peer-to-local). El nombre de la política de seguridad se puede modificar. Seleccione esta opción para garantizar el intercambio de paquetes de negociación. Si no hay una política de seguridad configurada para permitir paquetes de negociación, seleccione **Política** > **Política de seguridad** para crear una política de seguridad que permita el intercambio de paquetes de negociación desde el extremo del par hasta el extremo local.

- Configurar la autenticación del túnel.
  Hay tres modos de autenticación de túnel IPsec y algunos de sus valores de parámetros son diferentes.
  - Clave precompartida

Parámetro	Descripción
Tipo de autenticación	**Clave precompartida**
Clave precompartida	Introduzca la clave negociada entre los administradores de ambos lados.
Identificación local	El ID local identifica la puerta de enlace local para la autenticación por parte de la puerta de enlace del par. El tipo y el valor deben ser iguales a los del **ID de par** del dispositivo par. ■ **Dirección IP** : utilice la dirección IP local como ID local. ■ **Nombre** : Si se selecciona esta opción, se utiliza el nombre de la puerta de enlace local como ID predeterminado. Puede especificar otra cadena de caracteres. ■ **FQDN de usuario** : Si se selecciona esta opción, se utiliza el nombre de la puerta de enlace local como ID predeterminado. Puede especificar otra cadena de caracteres. ■ **ESN** : Si se selecciona esta opción, se utiliza el ESN de la puerta de enlace local como ID local. Puede especificar otra cadena de caracteres.
Identificación de pares	El ID de par identifica el dispositivo par. Solicite este valor al administrador del dispositivo par. El tipo y el valor deben coincidir con el **ID local** especificado en el dispositivo par. Seleccione **Cualquiera** si no se requiere autenticación. Si solo se requiere coincidencia de cadenas, seleccione **Cualquier tipo** . **NOTA:** Cuando el tipo de ID de par es la dirección IP, el dispositivo utiliza **la dirección de par** configurada en Configurar los parámetros básicos... como ID de par para verificar la coherencia con la ID local configurada en el dispositivo par.

  - Firma RSA

Parámetro	Descripción
Tipo de autenticación	**Firma RSA**
Certificado	Seleccione el certificado local obtenido de la CA cuando este parámetro esté disponible. Cierta información del certificado se enviará a la puerta de enlace de pares para su autenticación. Para obtener más información sobre la carga de certificados, consulte Certificados locales .
Identificación local	Una vez cargado el certificado, seleccione el tipo de ID local. El sistema extrae automáticamente el valor del campo correspondiente del certificado como ID local. El ID local puede ser uno de los siguientes elementos (correspondientes a los campos específicos del certificado): ■ **Dirección IP** : el valor del campo **Dirección IP** sirve como ID local.

Parámetro	Descripción
	▪ **DN** : El valor del campo **Asunto** sirve como ID local. ▪ **Nombre** : El valor del campo **Nombre común** sirve como ID local. ▪ **FQDN del usuario** : el valor del campo **Correo electrónico** sirve como ID local.
Identificación de pares	El ID de par identifica el dispositivo par. Solicite este valor al administrador del dispositivo par. El tipo y el valor deben coincidir con el **ID local** especificado en el dispositivo par. Seleccione **Cualquiera** si no se requiere autenticación. Si solo se requiere coincidencia de cadenas, seleccione **Cualquier tipo** . **NOTA:** Cuando el tipo de ID de par es la dirección IP, el dispositivo utiliza **la dirección de par** configurada en Configurar los parámetros básicos... como ID de par para verificar la coherencia con la ID local configurada en el dispositivo par.

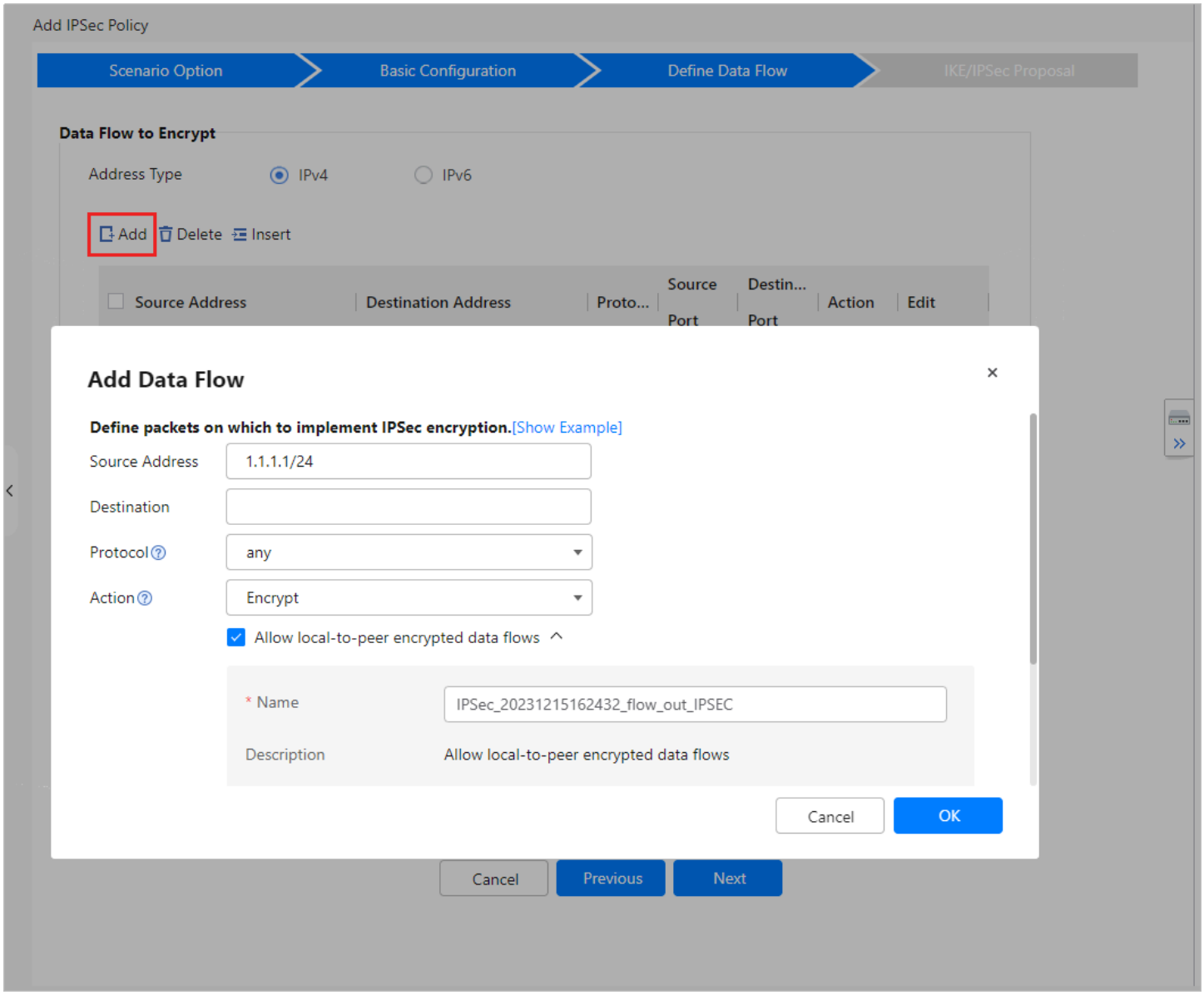
- Sobre digital SM2

NOTE

De forma predeterminada, el dispositivo no admite este parámetro (no admite la negociación de SA mediante IKEv1). Para usarlo, debe cargar el paquete de características de IKEv1.

Parámetro	Descripción
Tipo de autenticación	**Sobre digital SM2**
Reino de cifrado	Seleccione el ámbito PKI del certificado de cifrado solicitado e importado desde el servidor SM2.
Reino de la Firma	Seleccione el ámbito PKI del certificado de firma solicitado e importado desde el servidor SM2. Además, los certificados CA utilizados por los dispositivos en ambos extremos deben importarse a este ámbito de firma.

5. Configure los flujos de datos para que se cifren a través del túnel IPsec.

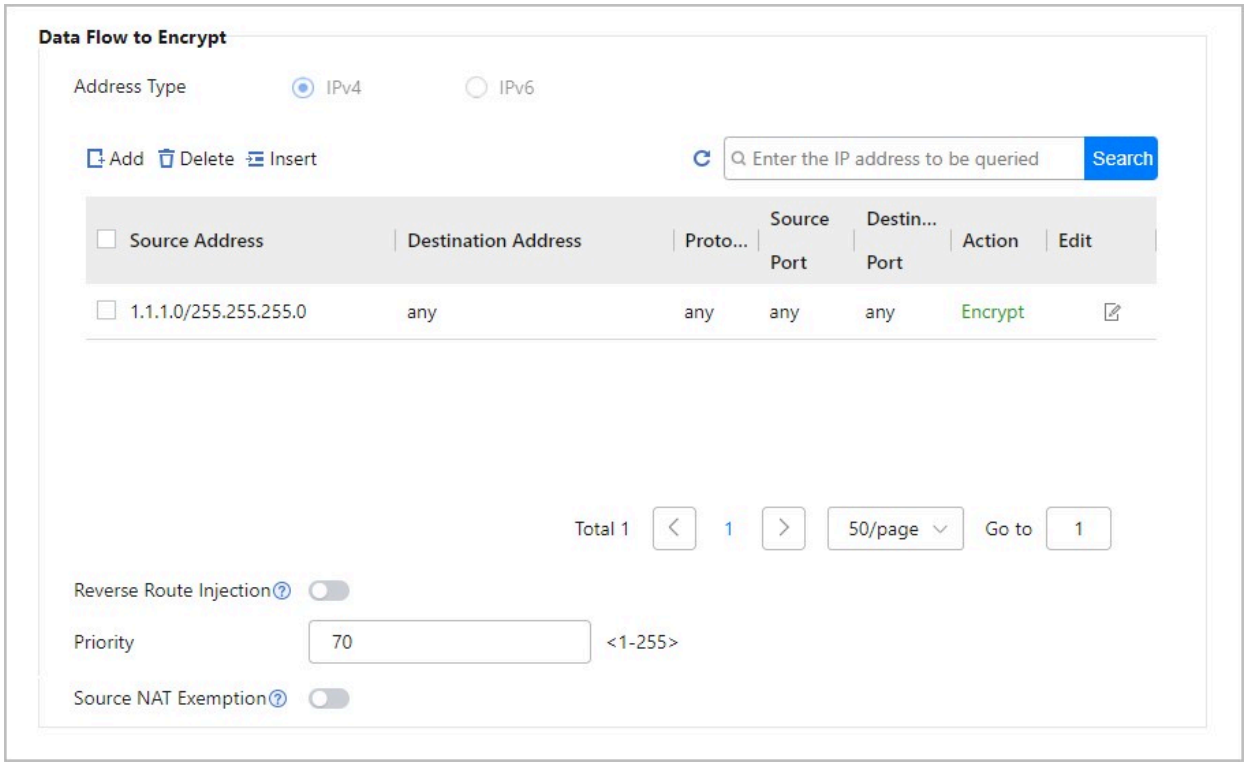


Generalmente, solo algunos flujos de datos necesitan cifrarse antes de enviarse al par, y otros se transmiten directamente a Internet. Para evitar que estos flujos se transmitan directamente a través de Internet y entren en el túnel, es necesario configurar ciertas reglas para restringirlos.
Puede configurar varias reglas en una lista. Los flujos de datos coinciden con las reglas de arriba a abajo. Si se encuentra una coincidencia, los flujos de datos se procesan según la acción especificada y el proceso de coincidencia finaliza.
En **Flujo de datos cifrados** , seleccione **IPv4** o **IPv6** para **Tipo de dirección** y haga clic en **Agregar** .

Parámetro	Descripción
Dirección de origen	Especifique la dirección de origen de los flujos de datos que se cifrarán a través del túnel. Normalmente, la dirección de origen suele ser la dirección de la subred de la intranet que se protegerá. Solo se admite el formato de dirección IP/máscara de subred. Puede introducir una sola dirección IP (por ejemplo, 192.168.1.1/32 o 192.168.1.1/255.255.255.255) o un segmento de red (por ejemplo, 192.168.1.0/24 o 192.168.1.0/255.255.255.0). Puede introducir una única dirección IP.
Dirección de destino	Especifique la dirección de destino de los flujos de datos que se cifrarán a través del túnel. Normalmente, la dirección de destino suele ser la dirección de la subred a la que se accede en la intranet del par. Solo se admite el formato de dirección IP/máscara de subred. Puede introducir una sola dirección IP (por ejemplo, 192.168.1.1/32 o 192.168.1.1/255.255.255.255) o un segmento de red (por ejemplo, 192.168.1.0/24 o 192.168.1.0/255.255.255.0). Puede introducir una única dirección IP.
Protocolo	Especifique el protocolo de los flujos de datos que se cifrarán a través del túnel. Puede configurar un puerto TCP o UDP para cifrar el tráfico de un servicio específico. Por ejemplo, puede configurar el puerto TCP 80 para cifrar el tráfico HTTP y el puerto UDP 69 para cifrar el tráfico TFTP.

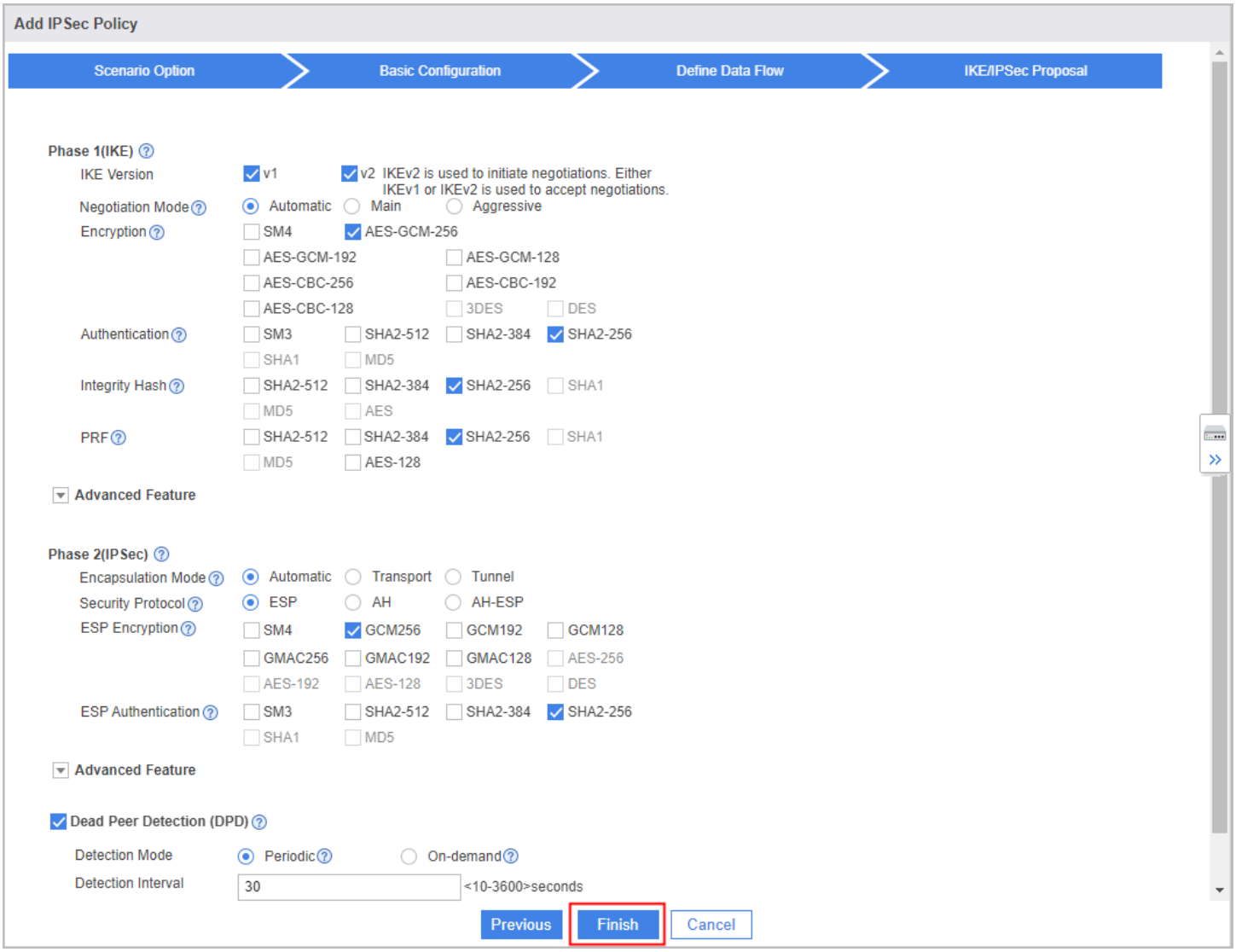
Parámetro	Descripción
	Si no conoce el protocolo y el puerto o no es necesario realizar una restricción basada en protocolo, deje este parámetro sin especificar o configúrelo en **cualquier valor** .
Puerto de origen	Este parámetro está disponible cuando **el Protocolo** está configurado como **TCP** o **UDP** . Especifique el número de puerto de origen desde donde se originan los flujos de datos que se cifrarán a través del túnel.
Puerto de destino	Este parámetro está disponible cuando **el Protocolo** está configurado como **TCP** o **UDP** . Especifique el número de puerto de destino al que se destinan los flujos de datos que se cifrarán a través del túnel.
Acción	Especifique la acción para los flujos de datos que coincidan con las condiciones anteriores. • **Cifrar** indica que se permite cifrar los flujos de datos a través del túnel. • **No cifrar** indica que no se permite cifrar los flujos de datos a través del túnel. La acción **"No cifrar"** se utiliza para eximir del cifrado el tráfico de algunos clientes. Por ejemplo, para cifrar el tráfico de todos los hosts de la subred 192.168.1.0/24, excepto el host en 192.168.1.2, configure una regla para eximir del cifrado el tráfico del host en 192.168.1.2 y una regla para cifrar el tráfico de los hosts de la subred 192.168.1.0/24.
Permitir flujos de datos cifrados de local a par	Si se selecciona **"Permitir flujos de datos cifrados de local a par"** , se crea una política de seguridad con **la opción "Acción"** establecida en " **Permitir"** para los flujos de datos cifrados del extremo local al par. El nombre de la política de seguridad se puede modificar. Seleccione esta opción para garantizar el intercambio de flujos de datos cifrados. Si no hay una política de seguridad configurada para permitir flujos de datos cifrados, seleccione **Política** > **Política de seguridad** para crear una que permita flujos de datos cifrados desde el extremo local hasta el extremo del par.
Permitir flujos de datos cifrados de punto a punto local	Si se selecciona **Permitir flujos de datos cifrados entre pares (peer-to-local) , se crea una política de seguridad con la acción** establecida en **Permitir** para los flujos de datos cifrados desde el punto de acceso al extremo local. El nombre de la política de seguridad se puede modificar. Seleccione esta opción para garantizar el intercambio de flujos de datos cifrados. Si no hay una política de seguridad configurada para permitir flujos de datos cifrados, seleccione **Política** > **Política de seguridad** para crear una que permita flujos de datos cifrados desde el punto de acceso al punto local.

Puede activar **la inyección de ruta inversa** si es necesario.



Parámetro	Descripción
Inyección por vía inversa	Si esta función está habilitada, el dispositivo instala automáticamente las rutas destinadas a la red de pares, eliminando la necesidad de que los administradores las configuren manualmente. Esta función suele configurarse en la puerta de enlace de la sede central conectada a varias sucursales.
Prioridad	Este parámetro se muestra después de habilitar **la inyección de ruta inversa** . Puede establecer **la prioridad** si es necesario. Por ejemplo, si el dispositivo tiene otras rutas al mismo destino, puede especificar la misma prioridad para que implementen el balanceo de carga, o prioridades diferentes para implementar la copia de seguridad de rutas.
Exención de NAT de origen	Supongamos que una puerta de enlace de sucursal es una puerta de enlace NAT con NAT de origen configurada que controla el acceso de la sucursal a la sede central. Cuando esta puerta de enlace NAT recibe un paquete de texto simple que coincide con una política NAT de origen, traduce la dirección de origen del paquete. Sin embargo, la traducción hace que el paquete ya no coincida con la ACL que define los flujos de datos protegidos por IPsec. En consecuencia, el paquete no puede entrar en el túnel IPsec para la transmisión cifrada y se descarta. Para solucionar este problema, puede habilitar la exención de NAT en la política IPsec de la sucursal. Una vez habilitada esta función, los flujos de datos que se cifrarán mediante IPsec se reenvían directamente a través de túneles IPsec, sin procesarse en función de las políticas NAT de origen. **NOTA:** Este parámetro solo se puede configurar cuando **el tipo de dirección** de los flujos de datos que se van a cifrar se establece en **IPv4** .

6. Establezca los parámetros en la página de la pestaña **Propuesta IKE/IPSec** .



El sistema predefine varios conjuntos de parámetros de propuesta de seguridad. Si la propuesta de seguridad predeterminada no cumple con los requisitos de negociación, puede modificar la configuración de los parámetros. Todos los parámetros, excepto el tiempo de espera de la SA, deben tener

los mismos valores en ambos extremos.
Puede seleccionar varios algoritmos para la propuesta de seguridad. Los pares del túnel utilizarán preferentemente el algoritmo con la mayor seguridad para la negociación de IKE. En la interfaz web, los algoritmos se clasifican en orden descendente de prioridad, de izquierda a derecha.

NOTE

- De forma predeterminada, el dispositivo no admite la negociación de SA mediante IKEv1. Para utilizar las funciones relacionadas con IKEv1, debe instalar el paquete de funciones IKEv1. Inicie sesión en el sitio web de soporte técnico de Huawei, busque el producto y la versión correspondientes en el área de descarga de software y descargue el archivo **IKEv1_Product_Version.ccx . Para obtener más información sobre cómo instalar el paquete *de*** funciones, consulte "Configuración de la carga de módulos" en la Guía de configuración de la CLI > Configuración de administración del sistema > Configuración de mantenimiento de actualizaciones.
- De forma predeterminada, IPsec no admite algoritmos de seguridad débiles. Si selecciona un algoritmo de seguridad débil, se mostrará un mensaje de error.

  Por motivos de seguridad, no se recomienda utilizar el algoritmo o protocolo de seguridad débil que ofrece esta función. Si necesita utilizarlo, ejecute el comando **install feature-software WEAKEA** para instalar el paquete de software WEAKEA. De forma predeterminada, el dispositivo tiene el paquete de software WEAKEA. Para obtener más información sobre cómo instalar o desinstalar el paquete de software, consulte "Actualizar la configuración de mantenimiento" en *la Guía de configuración de la CLI > Configuración de administración del sistema* .
- Los algoritmos de seguridad AES-CBC-256, AES-CBC-192 y AES-CBC-128 se pueden configurar después de instalar el paquete de características IKEv1 o el paquete de software de protocolo y algoritmo de seguridad débil WEAKEA.
- El 3DES, AES-128, AES-128-GCM-128, AES-128-GMAC, AES-192, AES-192-GCM-128, AES-192-GMAC, AES-256, AES-256-GCM-128, AES-256-GMAC, AES-GCM-128, AES-GCM-192, AES-GCM-256, AES-XCBC-128, AES-XCBC-96, DES, GRUPO1, GRUPO14, GRUPO15, GRUPO16, GRUPO18, GRUPO19, GRUPO2, GRUPO20, GRUPO21, GRUPO24, GRUPO5, HMAC-MD5, HMAC-MD5-96, HMAC-SHA1, Los algoritmos de seguridad HMAC-SHA1-96, HMAC-SHA2-256, HMAC-SHA2-384, HMAC-SHA2-512, MD5, PKCS1, PSS, SHA1, SHA2-256, SHA2-384, SHA2-512, SM3 y SM4 se pueden configurar solo después de instalar el paquete de software de protocolo y algoritmo de seguridad débil WEAKEA.

Parámetro	**Descripción**
Parámetros de la fase 1 (IKE)	
Versión IKE	Seleccione **v1** o **v2** para especificar la versión del protocolo IKE utilizada en las negociaciones con la puerta de enlace de pares. Para obtener más información sobre las versiones de IKE, consulte [enlace faltante]. Si se seleccionan ambas versiones, el extremo local puede responder a las solicitudes IKEv1 e IKEv2, pero solo iniciar solicitudes IKEv2.
Modo de negociación	Seleccione el modo de negociación IKEv1. • Automático: tanto el modo principal como el modo agresivo son aceptables en la respuesta a las solicitudes IKE, pero solo el modo principal es aceptable en el inicio de las solicitudes IKE. • Modo principal: solo el modo principal es aceptable en la negociación. • Modo agresivo: Sólo el modo agresivo es aceptable en la negociación.
Cifrado	Seleccione un algoritmo de cifrado según sea necesario. **NOTA:** SM4 cumple con los altos requisitos de confidencialidad y seguridad, pero su procesamiento requiere un tiempo de procesamiento relativamente largo. Los algoritmos 3DES, AES-CBC-256, AES-CBC-192, AES-CBC-128 y DES ofrecen baja seguridad, por lo que no se recomiendan. El algoritmo de cifrado SM4 solo está disponible cuando **la versión de IKE** está configurada en **v1** . Los algoritmos de cifrado AES-GCM-256, AES-GCM-192 y AES-GCM-128 solo están disponibles cuando **la versión de IKE** está configurada en **v2** .
Autenticación	Este parámetro solo está disponible después de seleccionar **v1** en **Versión IKE** . Seleccione el algoritmo utilizado en la autenticación de la fuente de datos. **NOTA:** SM3 puede cumplir con los altos requisitos de confidencialidad y seguridad, pero su procesamiento requiere un tiempo comparativamente largo. Los algoritmos MD5 y SHA1 ofrecen baja seguridad, por lo que no se recomiendan.

Parámetro	Descripción
Hash de integridad	Este parámetro solo está disponible después de seleccionar **v2** en **Versión IKE** . Especifique el algoritmo para las comprobaciones de integridad de los datos si se utiliza IKEv2 en la negociación. **NOTA:** Los algoritmos AES, MD5 y SHA1 proporcionan poca seguridad y, por lo tanto, no se recomiendan.
PRF	Este parámetro solo está disponible después de seleccionar **v2** en **Versión IKE** . Seleccione el algoritmo utilizado en la autenticación de la fuente de datos. **NOTA:** Los algoritmos MD5 y SHA1 proporcionan poca seguridad y, por lo tanto, no se recomiendan.
Grupo DH	Este parámetro se muestra al hacer clic en **Función avanzada** . Seleccione los métodos de intercambio de claves.
Tiempo de espera de AT	Este parámetro se muestra al hacer clic en **Función avanzada** . Establezca la duración de la SA de IKE. Cuando esté a punto de expirar, el dispositivo negociará una nueva SA. Esta reemplazará inmediatamente a la anterior una vez establecida. Especifique el período de tiempo de espera, en segundos.
Parámetros de la fase 2 (IPSec)	
Modo de encapsulación	Seleccione un modo de cifrado IPsec. • Automático: tanto el modo de transporte como el modo túnel se pueden utilizar para responder a solicitudes de negociación, pero solo el modo túnel se puede utilizar para iniciar solicitudes de negociación. • Transporte: Se utiliza para establecer túneles entre los dispositivos móviles y la puerta de enlace VPN. • Túnel: Generalmente se utiliza para establecer túneles entre las puertas de enlace VPN.
Protocolo de seguridad	Seleccione un protocolo IPsec. • Carga útil de seguridad encapsulante (ESP): cifra y autentica la carga útil del paquete. • Encabezado de autenticación (AH): autentica todo el paquete, pero no lo cifra. • AH-ESP: Cifra y autentica todo el paquete.
Cifrado ESP	Este parámetro está disponible si selecciona **ESP** o **AH-ESP** en **Protocolo de seguridad** . Seleccione el algoritmo utilizado en el cifrado de datos. **NOTA:** SM4 cumple con los altos requisitos de confidencialidad y seguridad, pero su procesamiento requiere un tiempo de procesamiento relativamente largo. Se recomiendan los algoritmos GCM256, GCM192, GCM128, GMAC256, GMAC192 y GMAC128 por motivos de seguridad. No se recomiendan los algoritmos AES-256, AES-192, AES-128, 3DES ni DES.
Autenticación ESP	Este parámetro está disponible si selecciona **ESP** o **AH-ESP** en **Protocolo de seguridad** . Seleccione el algoritmo utilizado en la autenticación de la fuente de datos. **NOTA:**

Parámetro	Descripción
	SM3 cumple con los altos requisitos de confidencialidad y seguridad, pero su procesamiento requiere un tiempo de procesamiento relativamente largo. Se recomiendan los algoritmos SHA2-256, SHA2-384 y SHA2-512 por motivos de seguridad. No se recomiendan los algoritmos MD5 ni SHA1.
Autenticación AH	Este parámetro está disponible si selecciona **AH** o **AH-ESP** en **Protocolo de seguridad** . Seleccione el algoritmo utilizado en la autenticación de la fuente de datos. **NOTA:** SM3 cumple con los altos requisitos de confidencialidad y seguridad, pero su procesamiento requiere un tiempo relativamente largo. Se recomiendan los algoritmos SHA2-256, SHA2-384 y SHA2-512 por motivos de seguridad. No se recomiendan MD5 ni SHA1.
PFS	Este parámetro se muestra al hacer clic en **Función avanzada** . Seleccione los métodos de intercambio de claves. Un ID de grupo mayor indica una clave más larga y mayor seguridad. **NINGUNO** indica que no se realizarán intercambios de claves adicionales.
Tiempo de espera de AT	Este parámetro se muestra al hacer clic en **Función avanzada** . El túnel IPsec se renegocia para garantizar la seguridad cuando el tiempo de establecimiento o el volumen de tráfico transmitido alcanza el umbral especificado. Especifique el periodo de inactividad para la renegociación de SA en **"Basado en el tiempo"** . Especifique el umbral de volumen de tráfico en **"Basado en el tráfico"** . Cuando se cumple alguna de las condiciones anteriores tras establecer un túnel IPsec, la SA IPsec renegocia el túnel. La renegociación no desconecta el túnel disponible.
Detección de pares muertos (DPD)	
Modo de detección	Una vez habilitada **la detección de pares inactivos (DPD) , el extremo local envía paquetes DPD para detectar si el gateway de pares aún está activo.** Los métodos de detección disponibles son los siguientes: • Periódico: el extremo local reenvía paquetes DPD si no se recibe ningún paquete del dispositivo par dentro del período especificado en **Intervalo de detección** . • A pedido: el extremo local envía paquetes DPD solo cuando se requiere la comunicación y no se recibe ningún paquete del dispositivo par dentro del período especificado en **Intervalo de detección** . Habilite o deshabilite esta función en ambos extremos simultáneamente. Se registra un fallo de detección si no se recibe respuesta dentro del período especificado en el **Intervalo de Reintento** después de que el extremo local envíe un paquete DPD. Tras cinco fallos de detección consecutivos, se considera que el par está inactivo y el túnel se elimina automáticamente.
Intervalo de detección	Especifique un período en **Intervalo de detección** , en segundos.
Intervalo de reintento	Especifique un periodo en **el intervalo de reintento** , en segundos. Este parámetro solo es aplicable cuando el túnel utiliza IKEv1.

7. Haga clic en **Finalizar** . La política IPsec recién configurada se mostrará en la lista de políticas.

Procedimiento de seguimiento

- **Clonación de una política IPsec**
  Seleccione una política IPsec existente en **la Lista de Políticas IPSec** y haga clic en **Copiar** para crear una política IPsec usando la política seleccionada como plantilla. En la página de configuración de la política IPsec recién creada, se han configurado algunos parámetros (como el escenario, el modo de autenticación y la propuesta de seguridad). Solo necesita configurar los parámetros restantes (como el nombre de la política, la clave precompartida y el flujo de datos que se cifrará).
- **Visualización y exportación de la configuración recomendada para el dispositivo par**
  La configuración de parámetros consistente en los dispositivos locales y de pares es fundamental para el éxito de la negociación de IPsec. Esta práctica función permite exportar la configuración recomendada de pares y enviarla al administrador del dispositivo de pares como referencia.

1. En la página **Agregar política IPSec** o **Modificar política IPSec** , puede hacer clic en el ícono del dispositivo par como referencia  para mostrar la configuración de par recomendada.
2. La configuración breve recomendada se muestra en el panel derecho. Haga clic en **"Exportar"** para exportar la configuración detallada.

REFERENCIAS TECNICAS

INGLES

Config Mirroring

Configuring Mirroring of SSL-Decrypted Packets

This section describes mirroring of SSL-decrypted packets and how to configure this function.

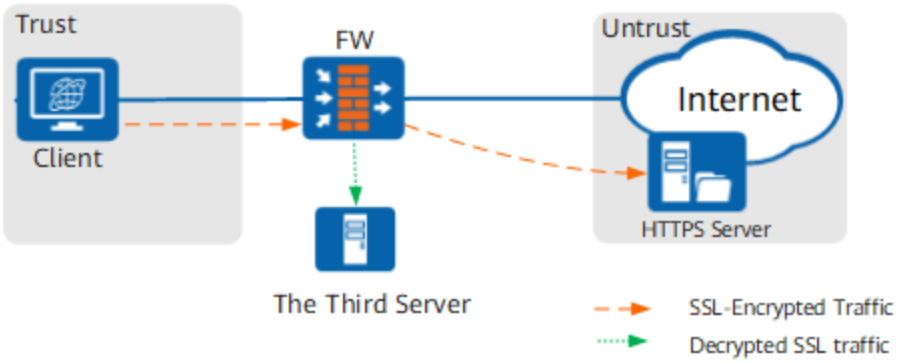
Application Scenario

The scenario of decrypted packet mirroring is generally applied when the FW is deployed at the enterprise egress. After the mirroring interface for packet decryption is specified, the FW sends the decrypted plaintext data to the third-party detection device through the mirroring interface, and the third-party detection device performs security check on the mirrored data. The decrypted packet mirroring function enables multiple devices to perform security detection and audit on the decrypted content, extending the detection scope of the third-party device and maximizing the value of existing devices.

The decrypted packets are sent to the third-party device through the mirroring interface for detection, and the packets detected by the third-party device are not sent to the FW.

The decrypted packet mirroring function can be used in both the protection server and client protection scenarios. The following figure shows the server protection scenario where the SSL-decrypted packet mirroring function is enabled.

Figure 1 Mirroring of SSL-Decrypted Packets application scenario



Configuring Mirroring of SSL-Decrypted Packets Using the Web UI

1. Choose **Policy** > **Encrypted Traffic Detection** > **Detection Profile**. Click **Add** to configure a detection profile.
2. Set **Type** to **Inbound** or **Outbound** to configure a mirroring interface.
   If you select a mirroring interface, the decrypted traffic is sent to a third-party device through the mirroring interface. Currently, the mirroring interface supports only Layer 3 Ethernet

interface.

This section describes only the operations related to decrypted packet mirroring. If this function is used in server protection and client protection scenarios, you also need to configure certificates, detection policies, and detection profiles. For details, see the corresponding sections.

Configuring Mirroring of SSL-Decrypted Packets Using the CLI

The following uses the configuration of mirroring interface GigabitEthernet 0/0/2 for SSL-encrypted traffic as an example.

```
<sysname> system-view
[sysname] profile type decryption name profile1
[sysname-profile-decryption-profile1] detect type outbound
[sysname-profile-decryption-profile1] mirror-interface GigabitEthernet 0/0/2
```

Parent Topic: **SSL-Encrypted Traffic Detection**

Copyright © Huawei Technologies Co., Ltd.

Previous Next topic

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Config Mirroring

Configuración de la duplicación de paquetes descifrados con SSL

Esta sección describe la duplicación de paquetes descifrados SSL y cómo configurar esta función.

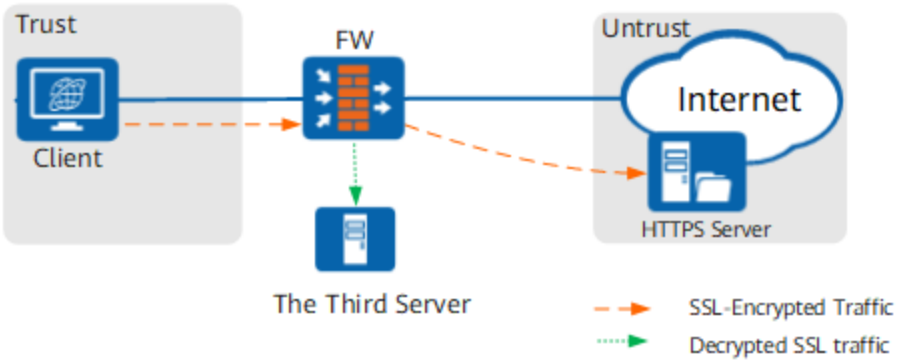
Escenario de aplicación

El escenario de duplicación de paquetes descifrados se aplica generalmente cuando el firewall se implementa en la salida de la empresa. Una vez especificada la interfaz de duplicación para el descifrado de paquetes, el firewall envía los datos de texto plano descifrados al dispositivo de detección de terceros a través de la interfaz de duplicación, y este realiza una comprobación de seguridad de los datos reflejados. La función de duplicación de paquetes descifrados permite que varios dispositivos realicen la detección y auditoría de seguridad del contenido descifrado, ampliando el alcance de detección del dispositivo de terceros y maximizando el valor de los dispositivos existentes.

Los paquetes descifrados se envían al dispositivo de terceros a través de la interfaz de duplicación para su detección, y los paquetes detectados por el dispositivo de terceros no se envían al FW .

La función de duplicación de paquetes descifrados se puede utilizar tanto en el servidor de protección como en el cliente. La siguiente figura muestra el escenario de protección del servidor donde está habilitada la función de duplicación de paquetes descifrados SSL.

Figura 1 Escenario de aplicación de duplicación de paquetes descifrados con SSL



Configuración de la duplicación de paquetes descifrados con SSL mediante la interfaz web

1. Seleccione **Política** > **Detección de tráfico cifrado** > **Perfil de detección** . Haga clic en **Agregar** para configurar un perfil de detección.
2. Establezca **el tipo** en **Entrante** o **Saliente** para configurar una interfaz de duplicación.

Inicio

externo a través de ella. Actualmente, la interfaz de duplicación solo admite la interfaz Ethernet de capa 3, la interfaz Ethernet de capa 2, la subinterfaz Ethernet, la interfaz Eth-Trunk y la interfaz de túnel.

Esta sección describe únicamente las operaciones relacionadas con la duplicación de paquetes descifrados. Si esta función se utiliza en escenarios de protección de servidores y clientes, también deberá configurar certificados, políticas de detección y perfiles de detección. Para obtener más información, consulte las secciones correspondientes.

Configuración de la duplicación de paquetes descifrados SSL mediante la CLI

A continuación se utiliza la configuración de la interfaz de duplicación GigabitEthernet 0/0/2 para el tráfico cifrado con SSL como ejemplo.

```
<sysname> vista-sistema
[sysname] tipo-perfil descifrado nombre perfil1
[sysname-profile-decryption-profile1] tipo-de-detección saliente
[sysname-profile-decryption-profile1] interfaz-espejo GigabitEthernet 0/0/2
```

Tema principal: **Detección de tráfico cifrado con SSL**

Tema **Siguiente**

Derechos de autor © Huawei Technologies Co., Ltd.

REFERENCIAS TECNICAS

INGLES

Config NAT

Enterprise Support

Size: 264.12MB

Enter keywords 0 / 256

HiSecEngine USG6000F Product Documentation ...

NAT and IPv6 Transition Technologies Configuration 3923 /23582

NAT Configuration Maintaining NAT

Configuring NAT Alarm Functions

Context

After NAT is configured, you can configure the alarm and log functions in the system view to monitor the usage of IP addresses in an address pool and overall usage of the address pool.

Procedure

- Configure the function of generating an alarm when the maximum number of translated private addresses for a public address is reached.
  1. Enable the function of sending logs and alarms when the maximum number of translated private addresses for a public address is reached.

     `nat srcip-car used-up alarm enable`

     By default, this function is enabled.
  2. Set the alarm threshold for the percentage of translated private addresses to the maximum supported for a public address.

     `nat srcip-car used-up alarm threshold threshold`

     By default, the alarm threshold is 80%.
- Configure alarm functions for the port usage in a 3-tuple NAT scenario.

We use cookies on this site, in order for the site to work properly and to analyse traffic, offer enhanced functionality and personalise content.Learn more

cookie settings

Accept Cookies

Reject Cookies

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Config NAT

Soporte empresarial

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Configuración de las funciones de alarma NAT

Contexto

Una vez configurado NAT, puede configurar las funciones de alarma y registro en la vista del sistema para monitorear el uso de direcciones IP en un grupo de direcciones y el uso general del grupo de direcciones.

Procedimiento

- Configure la función de generar una alarma cuando se alcanza el número máximo de direcciones privadas traducidas para una dirección pública.

  1. Habilite la función de envío de registros y alarmas cuando se alcanza el número máximo de direcciones privadas traducidas para una dirección pública.

     ```
     Activación de alarma de nat srcip-car agotado
     ```

     De forma predeterminada, esta función está habilitada.
  2. Establezca el umbral de alarma para el porcentaje de direcciones privadas traducidas en el máximo admitido para una dirección pública.

     ```
     Umbral de alarma de nat srcip-car agotado
     ```

     De forma predeterminada, el umbral de alarma es del 80%.

Utilizamos cookies en este sitio para su correcto funcionamiento, analizar el tráfico, ofrecer una mejor funcionalidad y personalizar el contenido. Más información

configuración de cookies

Aceptar cookies

Rechazar cookies

REFERENCIAS TECNICAS

INGLES

Config Secu Policy

Size: 264.12MB

Enter keywords 0 / 256

HiSecEngine USG6000F Product Documentation ...

CLI Configuration Guide Security Protection

4116 /23582

Configuration Security Policy Configuration

Configuring the Session Aging Time of a Security Policy

Context

Session aging time

Created session entries need to be matched by packets constantly. If no packet matches a session for a long time, the connection has been torn down, and the session is unnecessary. To save system resources, the system deletes the entry that is not matched for a continuous period of time; that is, the session entry ages. You can set the session aging time based on security policies as required.

User-defined persistent connection

Generally, the default aging time for different types of services on the device can meet the forwarding requirements. You can also fine-tune the aging time as needed. For some special services, however, the interval between two consecutive packets of a session can be very long. For example:

- When a user downloads large files through FTP, the interval between control packets along the control channel can be very long.
- A user may query the data on a database server now and then, and the time between query operations may be far greater than the aging time of the TCP session.

If you set the aging time for a service to a large value, the aging time applies to all sessions of the service, resulting in performance deterioration. Therefore, the aging time settings must be more specific. The persistent connection function resolves this issue. The persistent connection function allows you to set an ultra-long aging time for the special traffic so that the session information of the special traffic does not age for a long time, ensuring the normal running of the related service. The persistent connection function takes effect only on TCP packets that match policies.

The priorities of session aging time configurations are as follows: policy-based user-defined persistent connection aging time (**long-link aging-time**) > policy-based session aging time

Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Config Secu Policy

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Configuración del tiempo de caducidad de la sesión de una política de seguridad

Contexto

Tiempo de envejecimiento de la sesión

Las entradas de sesión creadas deben coincidir con paquetes constantemente. Si ningún paquete coincide con una sesión durante un tiempo prolongado, la conexión se interrumpe y la sesión deja de ser necesaria. Para ahorrar recursos del sistema, este elimina la entrada que no coincide durante un periodo continuo; es decir, la entrada de sesión envejece. Puede configurar el tiempo de envejecimiento de la sesión según las políticas de seguridad, según sea necesario.

Conexión persistente definida por el usuario

Generalmente, el tiempo de envejecimiento predeterminado para los diferentes tipos de servicios en el dispositivo puede cumplir con los requisitos de reenvío. También puede ajustar el tiempo de envejecimiento según sea necesario. Sin embargo, para algunos servicios especiales, el intervalo entre dos paquetes consecutivos de una sesión puede ser muy largo. Por ejemplo:

- Cuando un usuario descarga archivos grandes a través de FTP, el intervalo entre paquetes de control a lo largo del canal de control puede ser muy largo.
- Un usuario puede consultar datos en un servidor de base de datos de vez en cuando, y el tiempo entre operaciones de consulta puede ser mucho mayor que el tiempo de envejecimiento de la sesión TCP.

Si se establece un tiempo de caducidad para un servicio con un valor elevado, este se aplica a todas las sesiones del servicio, lo que provoca un deterioro del rendimiento. Por lo tanto, la configuración del tiempo de caducidad debe ser más específica. La función de conexión persistente resuelve este problema. Esta función permite establecer un tiempo de caducidad muy largo para el tráfico especial, de modo que la información de la sesión no caduque durante mucho tiempo, garantizando así el correcto funcionamiento del servicio. La función de conexión

Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

REFERENCIAS TECNICAS

INGLES

Config USB based Deploy

Example for Configuring USB-based Deployment (Configured Device Scenario)

Networking Requirements

A new network needs to be deployed. DeviceA has been configured, and the customer requires that it automatically completes upgrade after it is powered on to reduce labor costs and deployment time. The system software **software_file.cc** is required for upgrading DeviceA.

Configuration Roadmap

The configuration roadmap is as follows:

1. Make the intermediate file **usb.ini** to enable the device to obtain its system software according to the intermediate file.
2. Save the intermediate file to the root directory of the USB flash drive and system software to the directory specified by the **DIRECTORY** field in the intermediate file.
3. Power on the device and enable USB-based deployment.
4. Insert the USB flash drive into the device to complete the deployment process.

Procedure

1. Make the intermediate file **usb.ini** according to the file format requirements in Intermediate File in the INI Format. The file format is as follows:

```
;BEGIN USB
[GLOBAL CONFIG]
*TIME_SN=20200526120159
*DEVICE_TYPE_NUM=1

[DEVICE_TYPE_1 DESCRIPTION]
DEVICE_TYPE=
ESN=
MAC=
UNAME=
VRPVER=
SPACE_CLEAR=
DIRECTORY=
ACTIVE_DELAYTIME=
ACTIVE_INTIME=
*FILETYPENUM=1
*FILENAME_1=software_file.cc
*TYPE_1=SOFTWARE
*EFFECTIVE_MODE_1=0
ISBATCHPROCESS_1=
SHA256_1=
HMAC_1=
COMPRESS_ENCRYTION_1=
;END USB CONFIG
```

2. Save the intermediate file and system software to the root directory of the USB flash drive.

3. Power on the device and enable USB-based deployment.

```
<HUAWEI> system-view
[HUAWEI] sysname DeviceA
[DeviceA] ztp usb-deployment enable
```

4. Insert the USB flash drive into DeviceA.
5. Observe the USB indicator on the device to determine the USB-based deployment progress.
   - Blinking green: USB-based deployment is in progress.
   - Steady green: USB-based deployment succeeds. If there is no deployment configuration file, deployment will be repeatedly performed. In this case, the indicator is also steady green.
   - Steady red: USB-based deployment fails.
   - Off: No USB flash drive is connected, or the indicator fails.
6. If the USB indicator on DeviceA is steady green, the deployment is complete.
7. You are advised to disable the USB-based deployment function after the deployment is complete. Otherwise, an unnecessary upgrade will be triggered if a USB flash drive is inserted into the device by mistake, causing service interruption.

```
[DeviceA] undo ztp usb-deployment enable
```

Verifying the Configuration

A device completes the USB-based deployment process in about 15 minutes after it is powered on. You can then log in to the device and run the **display startup** command to check whether the current system software is the required one.

```
<DeviceA> display startup
MainBoard:
  Configured startup system software:        flash:/software_file.cc
  Startup system software:                   flash:/software_file.cc
  Next startup system software:              flash:/software_file.cc
  Startup saved-configuration file:          flash:/conf_file1.cfg
  Next startup saved-configuration file:     flash:/conf_file1.cfg
  Startup paf file:                          default
  Next startup paf file:                     default
  Startup patch package:                     NULL
  Next startup patch package:                NULL
  Startup feature software:                  NULL
  Next startup feature software:             NULL
```

Configuration Scripts

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Config USB based Deploy

Ejemplo de configuración de implementación basada en USB (escenario de dispositivo configurado)

Requisitos de red

Se necesita implementar una nueva red. El Dispositivo A ya está configurado y el cliente requiere que la actualización se complete automáticamente tras el encendido para reducir los costos de mano de obra y el tiempo de implementación. Se requiere el software del sistema **software_file.cc** para actualizar el Dispositivo A.

Hoja de ruta de configuración

La hoja de ruta de configuración es la siguiente:

1. Cree el archivo intermedio **usb.ini** para permitir que el dispositivo obtenga su software de sistema de acuerdo con el archivo intermedio.
2. Guarde el archivo intermedio en el directorio raíz de la unidad flash USB y el software del sistema en el directorio especificado por el campo **DIRECTORIO** en el archivo intermedio.
3. Encienda el dispositivo y habilite la implementación basada en USB.
4. Inserte la unidad flash USB en el dispositivo para completar el proceso de implementación.

Procedimiento

1. Cree el archivo intermedio **usb.ini** según los requisitos de formato de archivo de la sección Archivo intermedio en formato INI . El formato de archivo es el siguiente:

```
;INICIO USB
[CONFIGURACIÓN GLOBAL]
*TIEMPO_SN=20200526120159
*NÚMERO_DE_TIPO_DE_DISPOSITIVO=1

[DESCRIPCIÓN DEL TIPO DE DISPOSITIVO 1]
TIPO_DE_DISPOSITIVO=
ESN=
MAC=
UNNAME=
VRPVER=
ESPACIO_DESPEJADO=
DIRECTORIO=
TIEMPO_DE_RETRASO_ACTIVO=
TIEMPO_INTERNA_ACTIVO=
*NÚMERO DE TIPO DE ARCHIVO=1
*NOMBRE_DE_ARCHIVO_1=archivo_de_software.cc
*TIPO_1=SOFTWARE
*MODO EFECTIVO_1=0
ISBATCHPROCESS_1=
SHA256_1=
HMAC_1=
COMPRESS_ENCRYTION_1=
;FIN DE LA CONFIGURACIÓN USB
```

2. Guarde el archivo intermedio y el software del sistema en el directorio raíz de la unidad flash USB.

3. Encienda el dispositivo y habilite la implementación basada en USB.

```
< HUAWEI > vista del sistema
[ HUAWEI ] nombre_sistema DispositivoA
[DispositivoA] ztp usb-deployment enable
```

4. Inserte la unidad flash USB en el DispositivoA.
5. Observe el indicador USB en el dispositivo para determinar el progreso de la implementación basada en USB.
   - Verde intermitente: la implementación basada en USB está en progreso.
   - Verde fijo: La implementación basada en USB se realizó correctamente. Si no hay un archivo de configuración de implementación, la implementación se repetirá. En este caso, el indicador también permanece verde fijo.
   - Rojo fijo: falla la implementación basada en USB.
   - Apagado: No hay ninguna unidad flash USB conectada o el indicador falla.
6. Si el indicador USB en el DispositivoA está verde fijo, la implementación está completa.
7. Se recomienda desactivar la función de implementación basada en USB una vez finalizada la implementación. De lo contrario, se activará una actualización innecesaria si se inserta una unidad USB en el dispositivo por error, lo que provocará una interrupción del servicio.

```
[DispositivoA] Deshacer la habilitación de implementación USB de ZTP
```

Verificación de la configuración

El proceso de implementación basado en USB se completa en aproximadamente 15 minutos después de encenderse. A continuación, puede iniciar sesión en el dispositivo y ejecutar el comando **de inicio de pantalla** para comprobar si el software del sistema actual es el requerido.

```
Inicio de pantalla de <DeviceA>
Placa base:
  Software del sistema de inicio configurado: flash:/software_file.cc
  Software del sistema de inicio: flash:/software_file.cc
  Próximo software de inicio del sistema: flash:/software_file.cc
  Archivo de configuración guardada de inicio: flash:/conf_file1.cfg
  Próximo archivo de configuración guardada del inicio: flash:/conf_file1.cfg
  Archivo paf de inicio: predeterminado
  Próximo archivo paf de inicio: predeterminado
  Paquete de parche de inicio: NULL
  Próximo paquete de parche de inicio: NULL
  Software de función de inicio: NULL
  Próxima función de software de inicio: NULL
```

Scripts de configuración

REFERENCIAS TECNICAS

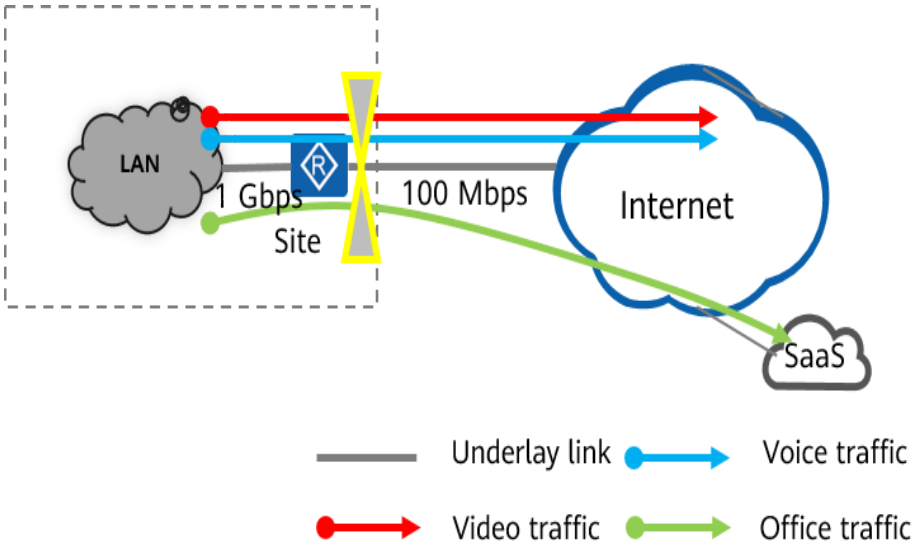
INGLES

Creating QoS Policy

Creating a QoS Policy (Common Configuration)

Context

The WAN link bandwidth of an enterprise site is usually lower than that of the enterprise LAN. The egress of the enterprise site becomes the bandwidth bottleneck of outbound traffic and is prone to congestion. Therefore, QoS policies are required to ensure the experience of high-priority application traffic.
To ensure the bandwidth of the local Internet access traffic of a site at the WAN egress, you can use common QoS policies to prioritize the traffic based on the traffic classifiers of different applications and schedule it accordingly.



As shown in the preceding figure, the LAN-side bandwidth is 1 Gbit/s, and the egress bandwidth of the site is 100 Mbit/s. You can configure a common QoS policy to control and schedule traffic to prevent congestion at the egress.

A common QoS policy needs to be configured with traffic classifiers and traffic behaviors.

- Traffic classifier: Data flows are classified based on information such as the Layer 3 ACL, application group, VLAN ID, 802.1p priority, source MAC address, destination MAC address, and Layer 2 protocol.
- Traffic behavior: Priorities are defined for traffic of different applications, and priority-based queue scheduling is then performed. In this case, the traffic of a high-priority application is preferentially forwarded when a congestion occurs.

Feature Requirements

- For firewall gateways, common QoS policies apply to the single uplink scenario instead of the multi-egress link scenario.
- V600 devices support common QoS policies in the inbound direction since V600R024C00 and support these policies in the outbound direction since V600R021C10.
- For V300 devices, if sub-interfaces are configured for an Eth-Trunk, common QoS policies cannot be configured for the sub-interfaces.
- Common QoS policies do not support traffic classifier templates that match traffic based on TCP flags.

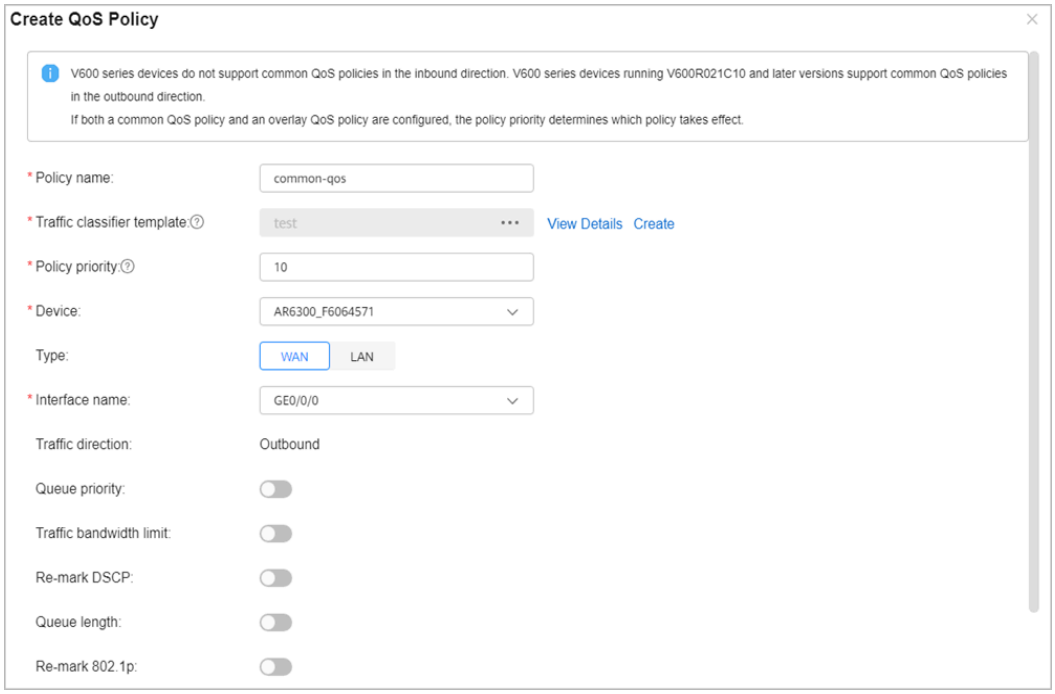
- If you want to configure both common QoS and overlay QoS policies for a V600 device, you cannot apply a traffic classifier template that matches traffic based on IPv6 ACLs to the common QoS policy.
- If common QoS and overlay QoS policies are both configured, the policy with a higher priority takes effect.
- Common QoS policies cannot be configured when multiple sub-interfaces are enabled for WAN links and overlay tunnels are enabled.
- The number of applications that can be specified in a QoS policy varies according to the model of the device to which the policy is to be applied.
- Firewall gateways support common QoS policies since V600R024C00.
- Firewall gateways do not support common QoS policies on LTE links and PPPoE links.
- The following firewall models do not support common QoS policies on Eth-Trunk interfaces and their sub-interfaces:
  USG6303F, USG6306F, USG6308F, USG6315F, USG6307F-D, USG6311F-D, USG6510F-D, USG6510F-DK, USG6510F-DL, USG6510F-DPL, USG6530F-D, USG6530F-DL, USG6530F-DPL, USG6520F-K, USG6525F, USG6555F, USG6560F-K, USG6565F, USG6585F, USG6590F-K
- In the scenario where the AR6700V-L is deployed through a cloud site, common QoS policies cannot be configured for LAN interfaces.

Prerequisites

1. A site has been added. For details, see Creating a Site.
2. A site has been activated. For details, see Configuring ZTP.
3. A traffic policy template has been configured. For details, see Creating a Traffic Classifier Template (Common).

Procedure

1. Choose **Network Configuration** > **SD-WAN** > **Policy Management** from the main menu and click the **Traffic Policy** tab.
2. Click the **Common** tab. The **QoS** tab page is displayed by default.
3. Select a site, click **Create**, and configure a QoS policy.



a. Enter a QoS policy name in the **Policy name** text box.

b. Set **Traffic classifier template** to specify a traffic matching rule.

c. Set **Policy priority** to specify a priority for the policy.

d. Select the device to which the QoS policy applies from the **Device** drop-down list box.

e. Select the type of the interface for which the QoS policy needs to be configured from the **Type** drop-down list box.

f. Select the interface to which the QoS policy applies from the **Interface name** drop-down list box.

g. Configure related information based on the selected interface type.

h. If you want the policy to take effect within a specific time period, select an effective time template from the **Effective time template** drop-down list box. If you want the policy to always take effect, skip this step.

4. Click **OK**.
   After the configuration is complete, the system automatically delivers the QoS policy to the device at the desired site.

Follow-up Procedure

Table 1 Follow-up procedure of configuring a QoS policy

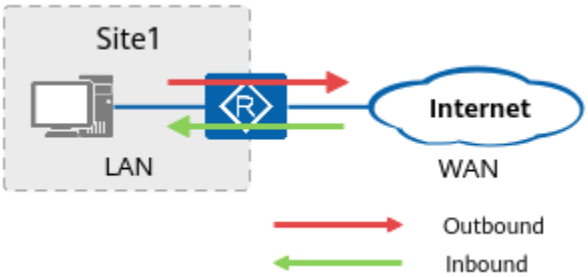
Function	Operation Scenario and Constraint	Procedure
Deleting a QoS policy	You can delete any policy that has been delivered to sites.	On the **QoS** tab page, select the QoS policy to be deleted and click **Delete**.

Function	Operation Scenario and Constraint	Procedure
Modifying a QoS policy	You can modify any policy that has been delivered to sites.	1. On the **QoS** tab page, click in the **Operation** column of the QoS policy to be modified. 2. Modify the policy as required. 3. Click **OK**.

Parameter Description

Table 2 Parameters for configuring a common QoS policy

Parameter	Description	Data Plan Required or Not
Policy name	Name of a QoS policy.	Y
Traffic classifier template	Traffic classifier template that matches the traffic to which the QoS policy applies. Firewall gateways do not support domain groups. If a firewall traffic classifier template containing a domain group is selected, the domain group configuration is not delivered.	Y
Policy priority	Priority of the QoS policy. The value ranges from 1 to 5000. A smaller value indicates a higher priority. When a flow matches multiple traffic policies, the policy with the highest priority takes effect.	Y
Device	Device for which the QoS policy needs to be configured.	Y
Type	WAN and LAN interfaces are supported. • **WAN**: When service packets are directly sent from the LAN side to the WAN side through the underlay network, the common QoS policy of the WAN type is recommended. • **LAN**: When the DSCP priority of packets needs to be modified, the common QoS policy of the LAN	Y

Parameter		Description	Data Plan Required or Not
		type is recommended.	
Interface name		Interface to which the QoS policy is to be applied.	Y
Traffic direction		This parameter is set automatically. The following figure shows the inbound and outbound traffic directions. When service flows pass through a CPE, **Outbound** refers to the direction from the LAN side to the WAN side while **Inbound** refers to the direction from the WAN side to the LAN side.  • When **Type** is set to **WAN**, this parameter is automatically set to **Outbound**. • When **Type** is set to **LAN**, this parameter is automatically set to **Inbound**.	Y
Queue priority (Parameters under **Queue priority** need to be set only when **Type** is set to **WAN**.)	Queue priority	You are advised to toggle on **Queue priority** for key applications that need to be preferentially guaranteed. When **Queue priority** is toggled on, a CPE automatically sends packets matching the traffic classifier to queues of different types based on the defined queue priorities.	Y
	Priority level (This parameter needs to be set only when **Queue priority** is toggled on.)	QoS priority. If network congestion occurs, the system preferentially transmits packets of higher-priority applications. For devices running V300, queues with the following priorities are supported: • **Medium**: Assured Forwarding (AF) is used to ensure a low drop probability of packets when the rate of outgoing service traffic does not exceed the minimum guaranteed bandwidth.	Y

Parameter		Description	Data Plan Required or Not
		• **High**: The matching traffic is sent to an Expedited Forwarding (EF) queue. After packets enter an EF queue, they are scheduled in the Strict Priority (SP) mode. Packets in other queues are scheduled only after all the packets in the EF queue are scheduled. In addition, EF queues can use the available bandwidth in AF or BE queues. • **Highest**: The matching traffic is sent to a Low Latency Queuing (LLQ) queue. The LLQ queue is a special EF queue that uses the SP mode. Compared with the EF queue, the LLQ queue has a shorter delay and provides QoS guarantee for delay-sensitive applications such as the VoIP service. The LLQ queue, however, does not preempt the available bandwidth of other queues. • **Medium**: Weighted Deficit Round Robin (WDRR) is used to schedule packets in medium-priority queues. By considering the length of packets during scheduling, WDRR ensures that packets are scheduled equally. When **Queue priority** is set to **Medium**, the guaranteed bandwidth needs to be configured (in percentage), which is the weight of the medium-priority queue. • **Highest**: Priority Queuing (PQ) is used to schedule packets in queues with the highest priority. The PQ algorithm schedules packets following a priority-based model. Packets are scheduled from the head of a given queue only if all queues of higher priority are empty. The device places core services into high-priority queues and non-core services (such as email services) into low-priority queues, ensuring that core services are processed preferentially. In this case, non-core services are processed only when all core services are processed. **NOTE:** For V600 devices, **Queue Priority** is toggled on by default and the priority level is	

Parameter		Description	Data Plan Required or Not
		mandatory and can be set only to **Highest** or **Medium**.	
	Guaranteed bandwidth (This parameter needs to be set only when **Queue priority** is toggled on.)	For medium- and high-priority queues, the guaranteed bandwidth is the minimum bandwidth that can be guaranteed. When the traffic exceeds the guaranteed bandwidth, the remaining bandwidth can be used. For queues with the highest priority, the guaranteed bandwidth is the maximum bandwidth that can be guaranteed because LLQ queues do not preempt the available bandwidth of other queues. When the traffic exceeds the guaranteed bandwidth, the excess traffic is discarded. The guaranteed bandwidth can be set to an absolute number or a percentage. The value range of the parameter is subject to the description on the web UI. If this parameter is set to a percentage, it is calculated by dividing the bandwidth to be guaranteed by the total available bandwidth of a department (VN). If this parameter is set to an absolute number, it cannot exceed the total available bandwidth. Assume that the bandwidth of a WAN interface is 100 Mbit/s and the bandwidth allocated to VN1 is 50 Mbit/s. If this parameter is set to 20%, packets matching the traffic classifier can occupy 10 Mbit/s bandwidth (50 Mbit/s x 20%). **NOTE:** For V600 devices, **Guaranteed bandwidth** can be set only when **Queue Priority** is set to **Medium**. In addition, the guaranteed bandwidth can be configured only in percentage.	Y
Traffic bandwidth limit	Traffic bandwidth limit	Whether to limit the traffic bandwidth. After **Traffic bandwidth limit** is toggled on, packets matching a certain rule are forwarded at a low delay.	Y

Parameter		Description	Data Plan Required or Not
(Parameters under **Traffic bandwidth limit** need to be set only when **Type** is set to **WAN**.)	Limit type (This parameter needs to be set only when **Traffic bandwidth limit** is toggled on.)	• **Shaping**: Traffic shaping is a measure to adjust the traffic rate sent from an interface. When the rate of an inbound interface on a downstream device is lower than that of an outbound interface on an upstream device or burst traffic occurs, traffic congestion may occur on the inbound interface of the downstream device. Traffic shaping can be configured on the outbound interface of the upstream device so that outgoing traffic is sent at even rates and congestion is avoided. • **Policing**: Traffic policing discards excess traffic to limit traffic within a proper range and to protect network resources and enterprise users' interests. **NOTE:** If **Queue priority** is toggled on and **Priority level** is set to **Highest** or **High** in a policy that applies to a V300 device, this parameter can be set only to **Policing**.	Y
	Bandwidth limit (This parameter needs to be set only when **Traffic bandwidth limit** is toggled on.)	Upper limit of the traffic rate. When traffic exceeds the limit specified by this parameter, the excess traffic is cached and sent later (if traffic shaping is configured) or directly discarded (if traffic policing is configured). This parameter can be set to an absolute number or a percentage. If this parameter is set to a percentage, it is calculated by dividing the bandwidth to be limited by the total available bandwidth of a department (VN). If this parameter is set to an absolute number, it cannot exceed the total available bandwidth. • If **Value** is selected for **Bandwidth limit**, the value ranges of this parameter on V300 and V600 devices are different, and the value range of this parameter on V600 devices varies according to **Limit type**. For details about the value range of this parameter, see the description on the web UI.	Y

Parameter		Description	Data Plan Required or Not
		• If **Percentage** is selected for **Bandwidth limit**, set this parameter to the percentage of the limited bandwidth to the total available bandwidth of a department (VN) on the interface. For details about the value range of this parameter, see the description on the web UI. Theoretically, the limited bandwidth must be greater than the guaranteed bandwidth so that the traffic within the guaranteed bandwidth is not limited.	
Re-mark DSCP		DSCP priority of IP packets. When a packet arrives at a CPE, the CPE sets the DSCP field in the outer IP header of the packet to the value of this parameter. The value is in the range from 0 to 63. A larger value indicates a higher priority. The DSCP value in the following packets is listed in descending order of priority: voice packets, video packets, and data packets.	Y
Queue length (This parameter needs to be set only when **Type** is set to **WAN**.)		Maximum length of a queue. You can specify the maximum number of bytes that can be stored in a queue, the maximum number of packets that can be stored in a queue, or both of them. If both of them are specified, when the total number of packets or bytes in a queue reaches the upper limit, the queue does not accept new packets. The queue length ranges from 2048 to 2097152 in the unit of bytes and ranges from 1 to 1024 in the unit of packets. **NOTE:** • For V300 devices, the queue length can be configured only when **Queue priority** is toggled on and the priority is set to **High** or **Medium**. • AR8140, AR6710-H4T4X2Y7, AR6710-L14T2X4, and AR6700V-L devices support only queues with a length of 512 or 1024	Y

Parameter	Description	Data Plan Required or Not
	packets. If this parameter is set to a value in the range from 1 to 512, the value 512 takes effect; if the parameter is set to a value in the range from 513 to 1024, the value 1024 takes effect. • For AR6700 series (excluding the AR6710-H4T4X2Y7 and AR6710-L14T2X4) and AR8700 series devices, the queue length can be set only in bytes.	
Re-mark 802.1p (This parameter needs to be set only when **Type** is set to **WAN**.)	Re-marked 802.1p priority of VLAN packets. A larger value indicates a higher priority. If a traffic policy is applied to the outbound direction on an interface, the CPE still processes outgoing packets based on the original priority but the downstream Layer 2 device processes the packets based on the re-marked priority.	Y

Statistics collection	Whether to enable the traffic statistics collection function. After this function is enabled, you can view traffic statistics on the CPE.
	V600 devices: You can run the following command to view traffic statistics:
	`display traffic-policy statistic`
	V300 devices: You can run the following command to view traffic statistics:
	`display traffic policy statistics`
		Y

Effective time template	Template that defines the time period during which the QoS policy takes effect.	

REFERENCIAS TECNICAS

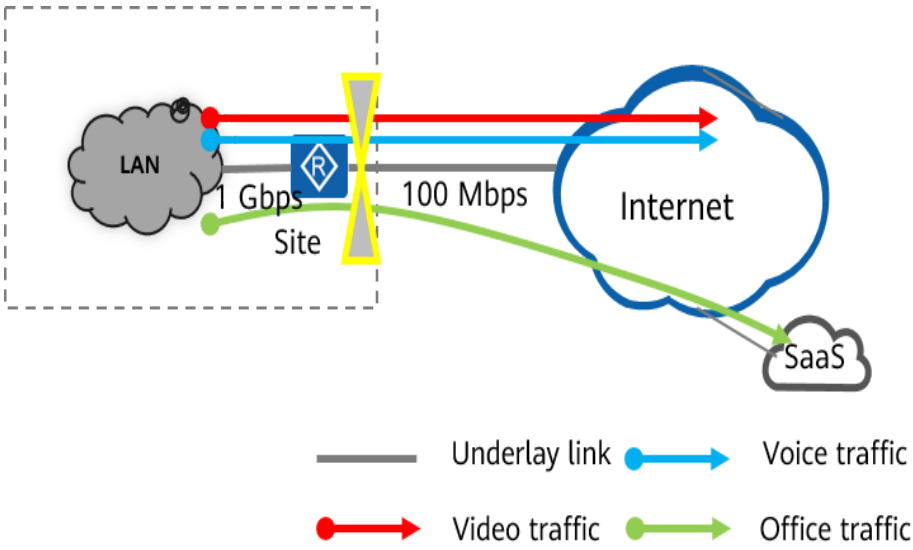
TRADUCCION SIMPLE

Creating QoS Policy

Creación de una política de QoS (configuración común)

Contexto

El ancho de banda del enlace WAN de una sede empresarial suele ser menor que el de la LAN empresarial. La salida de la sede empresarial se convierte en un cuello de botella del ancho de banda del tráfico saliente y es propensa a congestionarse. Por lo tanto, se requieren políticas de QoS para garantizar la experiencia del tráfico de aplicaciones de alta prioridad.
Para garantizar el ancho de banda del tráfico de acceso a Internet local de un sitio en la salida de la WAN, puede utilizar políticas QoS comunes para priorizar el tráfico en función de los clasificadores de tráfico de diferentes aplicaciones y programarlo en consecuencia.



Como se muestra en la figura anterior, el ancho de banda de la LAN es de 1 Gbit/s y el de salida del sitio es de 100 Mbit/s. Puede configurar una política de QoS común para controlar y programar el tráfico y evitar la congestión en la salida.

Es necesario configurar una política QoS común con clasificadores de tráfico y comportamientos de tráfico.

- Clasificador de tráfico: los flujos de datos se clasifican en función de información como la ACL de capa 3, el grupo de aplicaciones, el ID de VLAN, la prioridad 802.1p, la dirección MAC de origen, la dirección MAC de destino y el protocolo de capa 2.
- Comportamiento del tráfico: Se definen prioridades para el tráfico de las diferentes aplicaciones y, a continuación, se realiza una programación de colas basada en ellas. En este caso, el tráfico de una aplicación de alta prioridad se reenvía preferentemente cuando se produce una congestión.

Requisitos de las funciones

- Para las puertas de enlace de firewall, las políticas de QoS comunes se aplican al escenario de enlace ascendente único en lugar del escenario de enlace de egreso múltiple.
- Los dispositivos V600 admiten políticas QoS comunes en la dirección de entrada desde V600R024C00 y admiten estas políticas en la dirección de salida desde V600R021C10.

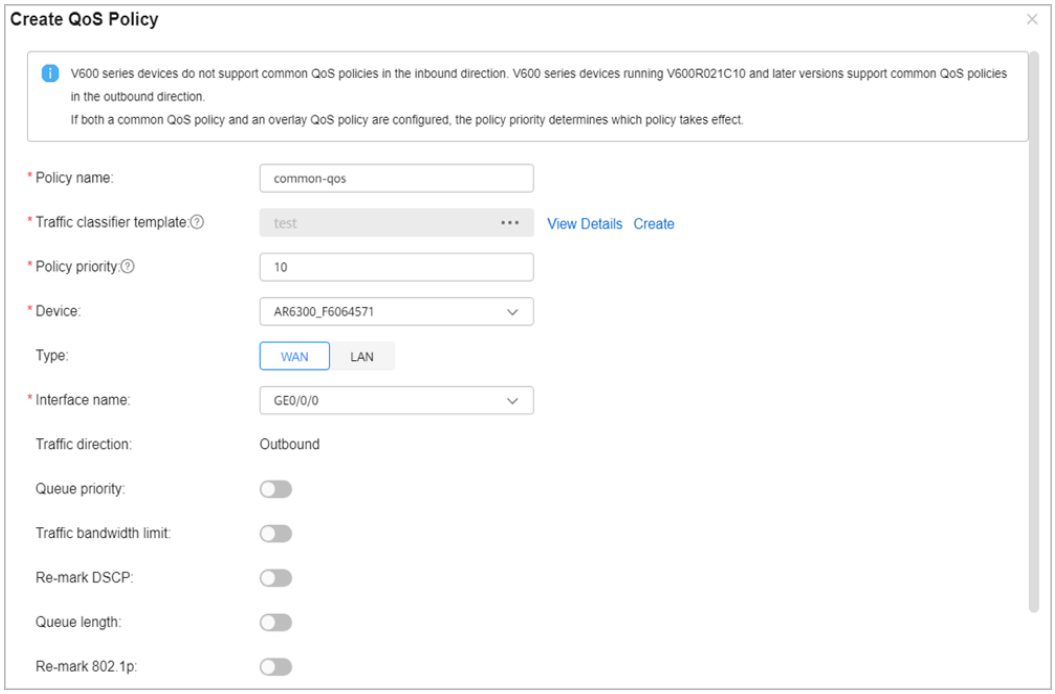
- Para los dispositivos V300, si se configuran subinterfaces para un Eth-Trunk, no se pueden configurar políticas QoS comunes para las subinterfaces.
- Las políticas de QoS comunes no admiten plantillas de clasificador de tráfico que coincidan con el tráfico en función de los indicadores TCP.
- Si desea configurar políticas de QoS comunes y de QoS superpuestas para un dispositivo V600 , no puede aplicar una plantilla de clasificador de tráfico que coincida con el tráfico basado en ACL de IPv6 con la política de QoS común.
- Si se configuran políticas de QoS comunes y de QoS superpuestas, tendrá efecto la política con mayor prioridad.
- No se pueden configurar políticas QoS comunes cuando se habilitan múltiples subinterfaces para enlaces WAN y se habilitan túneles superpuestos.
- La cantidad de aplicaciones que se pueden especificar en una política de QoS varía según el modelo del dispositivo al que se aplicará la política.
- Las puertas de enlace de firewall admiten políticas QoS comunes desde V600R024C00.
- Las puertas de enlace de firewall no admiten políticas QoS comunes en enlaces LTE y enlaces PPPoE.
- Los siguientes modelos de firewall no admiten políticas QoS comunes en las interfaces Eth-Trunk y sus subinterfaces:
  USG6303F, USG6306F, USG6308F, USG6315F, USG6307F-D, USG6311F-D, USG6510F-D, USG6510F-DK, USG6510F-DL, USG6510F-DPL, USG6530F-D, USG6530F-DL, USG6530F-DPL, USG6520F-K, USG6525F, USG6555F, USG6560F-K, USG6565F, USG6585F, USG6590F-K
- En el escenario donde el AR6700V-L se implementa a través de un sitio en la nube, no se pueden configurar políticas de QoS comunes para las interfaces LAN.

Prerrequisitos

1. Se ha añadido un sitio. Para más información, consulte "Crear un sitio" .
2. Se ha activado un sitio. Para más información, consulte Configuración de ZTP .
3. Se ha configurado una plantilla de política de tráfico. Para obtener más información, consulte " Creación de una plantilla de clasificador de tráfico (común)" .

Procedimiento

1. Seleccione **Configuración de red** > **SD-WAN** > **Administración de políticas** en el menú principal y haga clic en la pestaña **Política de tráfico** .
2. Haga clic en la pestaña **Común . La página de la pestaña QoS** se muestra de forma predeterminada.
3. Seleccione un sitio, haga clic **en Crear** y configure una política de QoS.



a. Introduzca un nombre de política de QoS en el cuadro de texto **Nombre de política** .

b. Establezca **la plantilla de clasificador de tráfico** para especificar una regla de coincidencia de tráfico.

c. Establecer **prioridad de política** para especificar una prioridad para la política.

d. Seleccione el dispositivo al que se aplica la política QoS en el cuadro de lista desplegable **Dispositivo .**

e. Seleccione el tipo de interfaz para la que se debe configurar la política QoS en el cuadro de lista desplegable **Tipo .**

f. Seleccione la interfaz a la que se aplica la política QoS en el cuadro de lista desplegable **Nombre de interfaz .**

g. Configure la información relacionada según el tipo de interfaz seleccionado.

h. Si desea que la política entre en vigor dentro de un plazo específico, seleccione una plantilla de vigencia en el cuadro desplegable **"Plantilla de vigencia ". Si desea que la política tenga vigencia siempre, omita este paso.**

4. Haga clic en **Aceptar** .
   Una vez completada la configuración, el sistema envía automáticamente la política de QoS al dispositivo en el sitio deseado.

Procedimiento de seguimiento

Tabla 1 Procedimiento de seguimiento de la configuración de una política de QoS

Función	Escenario de operación y restricción	Procedimiento

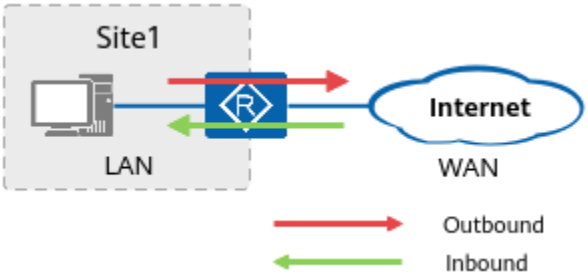
Función	Escenario de operación y restricción	Procedimiento
Eliminar una política de QoS	Puede eliminar cualquier política que se haya entregado a los sitios.	En la página de la pestaña **QoS** , seleccione la política de QoS que desea eliminar y haga clic en **Eliminar** .
Modificar una política de QoS	Puede modificar cualquier política que se haya entregado a los sitios.	1. En la página de la pestaña **QoS** , haga clic en la columna **Operación** de la política de QoS que desea modificar. 2. Modifique la política según sea necesario. 3. Haga clic en **Aceptar** .

Descripción del parámetro

Tabla 2 Parámetros para configurar una política de QoS común

Parámetro	Descripción	¿Se requiere o no un plan de datos?
Nombre de la póliza	Nombre de una política de QoS.	Y
Plantilla de clasificador de tráfico	Plantilla de clasificador de tráfico que coincide con el tráfico al que se aplica la política QoS. Las puertas de enlace de firewall no admiten grupos de dominios. Si se selecciona una plantilla de clasificador de tráfico de firewall que contenga un grupo de dominios, no se entregará la configuración del grupo de dominios.	Y
Prioridad política	Prioridad de la política de QoS. El valor varía de 1 a 5000. Un valor menor indica una prioridad mayor.	Y

Parámetro	Descripción	¿Se requiere o no un plan de datos?
	Cuando un flujo coincide con varias políticas de tráfico, se aplica la política con mayor prioridad.	
Dispositivo	Dispositivo para el cual se debe configurar la política de QoS.	Y
Tipo	Se admiten interfaces WAN y LAN. • **WAN** : cuando los paquetes de servicio se envían directamente desde el lado LAN al lado WAN a través de la red subyacente, se recomienda la política QoS común del tipo WAN. • **LAN** : cuando es necesario modificar la prioridad DSCP de los paquetes, se recomienda la política QoS común del tipo LAN.	Y
Nombre de la interfaz	Interfaz a la que se aplicará la política QoS.	Y

Parámetro		Descripción	¿Se requiere o no un plan de datos?
Dirección del tráfico		Este parámetro se establece automáticamente. La siguiente figura muestra las direcciones del tráfico entrante y saliente. Cuando los flujos de servicio pasan por un CPE, el **tráfico saliente** se refiere a la dirección de la LAN a la WAN, mientras que **el tráfico entrante** se refiere a la dirección de la WAN a la LAN.  • Cuando **Tipo** se establece en **WAN** , este parámetro se establece automáticamente en **Saliente** . • Cuando **Tipo** se establece en **LAN** , este parámetro se establece automáticamente en **Entrante** .	Y
Prioridad de cola (los parámetros bajo **Prioridad de cola** deben configurarse solo cuando **el Tipo** e	Prioridad de cola	Se recomienda activar **la prioridad de cola** para las aplicaciones clave que requieren una garantía preferencial. Al **activarla** , un CPE envía automáticamente los paquetes que coinciden con el clasificador de tráfico a colas de diferentes tipos según las prioridades de cola definidas.	Y
	Nivel de prioridad (este parámetro debe configurarse solo cuando **la prioridad de la**	Prioridad de QoS. Si se produce congestión en la red, el sistema transmite preferentemente los paquetes de aplicaciones de mayor prioridad. Para los dispositivos que ejecutan V300 , se admiten colas con las siguientes prioridades: • **Medio** : El reenvío asegurado (AF) se utiliza para garantizar una baja probabilidad de pérdida de paquetes cuando la tasa de tráfico del servicio saliente no excede el ancho de banda mínimo garantizado.	Y

Parámetro		Descripción	¿Se requiere o no un plan de datos?
stá config urado en **WA N**).	**cola** está activada).	• **Alta** : El tráfico coincidente se envía a una cola de reenvío acelerado (EF). Una vez que los paquetes entran en una cola EF, se programan en modo de prioridad estricta (SP). Los paquetes en otras colas se programan solo después de que todos los paquetes en la cola EF estén programados. Además, las colas EF pueden usar el ancho de banda disponible en las colas AF o BE. • **Máximo** : El tráfico coincidente se envía a una cola de baja latencia (LLQ). La cola LLQ es una cola EF especial que utiliza el modo SP. En comparación con la cola EF, la cola LLQ tiene un retardo menor y ofrece garantía de calidad de servicio (QoS) para aplicaciones sensibles al retardo, como el servicio VoIP. Sin embargo, la cola LLQ no ocupa el ancho de banda disponible de otras colas. • **Medio** : El algoritmo Round Robin de Déficit Ponderado (WDRR) se utiliza para programar paquetes en colas de prioridad media. Al considerar la longitud de los paquetes durante la programación, WDRR garantiza que se programen equitativamente. Cuando **la prioridad de la cola** se establece en **Media** , es necesario configurar el ancho de banda garantizado (en porcentaje), que es el peso de la cola de prioridad media. • **Máxima** prioridad: La cola de prioridad (PQ) se utiliza para programar paquetes en colas de máxima prioridad. El algoritmo PQ programa paquetes siguiendo un modelo basado en prioridades. Los paquetes se programan desde la cabecera de una cola solo si todas las colas de mayor prioridad están vacías. El dispositivo coloca los servicios principales en colas de alta prioridad y los servicios secundarios (como el correo electrónico) en colas de baja prioridad, garantizando así que los servicios	

Parámetro		Descripción	¿Se requiere o no un plan de datos?
		principales se procesen preferentemente. En este caso, los servicios secundarios se procesan solo cuando todos los servicios principales se procesan. **NOTA:** Para los dispositivos V600 , **la Prioridad de cola** está activada de manera predeterminada y el nivel de prioridad es obligatorio y solo se puede configurar como **Más alto** o **Medio** .	
	Ancho de banda garantizado (este parámetro debe configurarse solo cuando **la prioridad de cola** está activada).	Para colas de prioridad media y alta, el ancho de banda garantizado es el mínimo. Cuando el tráfico excede el ancho de banda garantizado, se puede utilizar el ancho de banda restante. Para las colas con la máxima prioridad, el ancho de banda garantizado es el máximo que se puede garantizar, ya que las colas LLQ no interrumpen el ancho de banda disponible de otras colas. Cuando el tráfico excede el ancho de banda garantizado, se descarta el exceso. El ancho de banda garantizado puede configurarse como un número absoluto o un porcentaje. El rango de valores del parámetro se describe en la interfaz web. Si este parámetro se configura como un porcentaje, se calcula dividiendo el ancho de banda a garantizar entre el ancho de banda total disponible de un departamento (VN). Si este parámetro se configura como un número absoluto, no puede superar el ancho de banda total disponible. Supongamos que el ancho de banda de una interfaz WAN es de 100 Mbit/s y el ancho de banda asignado a VN1 es de 50 Mbit/s. Si este parámetro se establece en 20%, los paquetes que coinciden con el clasificador de tráfico pueden ocupar 10 Mbit/s de ancho de banda (50 Mbit/s x 20%).	Y

Parámetro		Descripción	¿Se requiere o no un plan de datos?
		NOTA: En los dispositivos V600 , **el ancho de banda garantizado** solo se puede configurar cuando **la prioridad de cola** es **Media** . Además, el ancho de banda garantizado solo se puede configurar en porcentaje.	
Límite de ancho de banda del tráfico (Los parámetros bajo **Límite de ancho de banda de tráfico** deben configurarse solo cuando o **el Tipo** está config	Límite de ancho de banda del tráfico	Si se debe limitar el ancho de banda del tráfico. Al activar **la limitación del ancho de banda del tráfico , los paquetes que cumplen una regla determinada se reenvían con un retardo bajo.**	Y
	Tipo de límite (este parámetro debe configurarse solo cuando **el límite de ancho de banda de tráfico** está activado).	• **Modelado** : El modelado de tráfico es una medida para ajustar la velocidad del tráfico enviado desde una interfaz. Cuando la velocidad de una interfaz de entrada en un dispositivo descendente es menor que la de una interfaz de salida en un dispositivo ascendente, o se produce una ráfaga de tráfico, puede producirse congestión de tráfico en la interfaz de entrada del dispositivo descendente. El modelado de tráfico se puede configurar en la interfaz de salida del dispositivo ascendente para que el tráfico saliente se envíe a velocidades uniformes y se evite la congestión. • **Policía** : la policía de tráfico descarta el exceso de tráfico para limitar el tráfico dentro de un rango adecuado y proteger los recursos de la red y los intereses de los usuarios empresariales. **NOTA:** Si **la prioridad de la cola** está activada y **el nivel de prioridad** está configurado en **Más alto** o **Alto** en una política que se aplica a un	Y

Parámetro		Descripción	¿Se requiere o no un plan de datos?
urado en **WAN**).		dispositivo V300 , este parámetro solo se puede configurar en **Política** .	
	Límite de ancho de banda (este parámetro debe configurarse solo cuando **el límite de ancho de banda de tráfico** está activado).	Límite superior de la velocidad de tráfico. Cuando el tráfico supera el límite especificado por este parámetro, el exceso se almacena en caché y se envía posteriormente (si se configura la modelación de tráfico) o se descarta directamente (si se configura la vigilancia de tráfico). Este parámetro puede configurarse como un número absoluto o un porcentaje. Si se configura como un porcentaje, se calcula dividiendo el ancho de banda que se va a limitar entre el ancho de banda total disponible de un departamento (VN). Si se configura como un número absoluto, no puede superar el ancho de banda total disponible. • Si se selecciona **Valor para Límite de ancho de banda** , los rangos de valores de este parámetro en los dispositivos V300 y V600 son diferentes, y en los dispositivos V600 varía según el **tipo de límite** . Para obtener más información sobre el rango de valores de este parámetro, consulte la descripción en la interfaz web. • Si se selecciona **"Porcentaje" para el límite de ancho de banda** , configure este parámetro como el porcentaje del ancho de banda limitado respecto al ancho de banda total disponible de un departamento (VN) en la interfaz. Para obtener más información sobre el rango de valores de este parámetro, consulte la descripción en la interfaz web. En teoría, el ancho de banda limitado debe ser mayor que el ancho de banda garantizado para que el tráfico	Y

Parámetro	Descripción	¿Se requiere o no un plan de datos?
	dentro del ancho de banda garantizado no esté limitado.	
Remarcar DSCP	Prioridad DSCP de los paquetes IP. Cuando un paquete llega a un CPE, este configura el campo DSCP en el encabezado IP externo del paquete con el valor de este parámetro. El valor varía de 0 a 63. Un valor mayor indica una mayor prioridad. El valor DSCP en los siguientes paquetes aparece en orden descendente de prioridad: paquetes de voz, paquetes de vídeo y paquetes de datos.	Y
Longitud de la cola (Este parámetro debe configurarse solo cuando **el Tipo** está configurado en **WAN**).	Longitud máxima de una cola. Puede especificar el número máximo de bytes que se pueden almacenar en una cola, el número máximo de paquetes que se pueden almacenar en una cola, o ambos. Si se especifican ambos, cuando el número total de paquetes o bytes en una cola alcanza el límite superior, esta no acepta nuevos paquetes. La longitud de la cola varía de 2048 a 2097152 en la unidad de bytes y de 1 a 1024 en la unidad de paquetes. **NOTA:** • Para los dispositivos V300 , la longitud de la cola se puede configurar solo cuando **la prioridad de la cola** está activada y la prioridad está establecida en **Alta** o **Media** . • Los dispositivos AR8140, AR6710-H4T4X2Y7, AR6710-L14T2X4 y AR6700V-L solo admiten colas con una longitud de 512 o 1024 paquetes. Si este parámetro se configura con un valor entre 1 y 512, se aplica el valor 512; si se configura con un valor entre 513 y 1024, se aplica el valor 1024.	Y

Parámetro	Descripción	¿Se requiere o no un plan de datos?
	• Para los dispositivos de la serie AR6700 (excluidos los AR6710-H4T4X2Y7 y AR6710-L14T2X4) y de la serie AR8700, la longitud de la cola solo se puede configurar en bytes.	
Revisar 802.1p (Este parámetro debe configurarse solo cuando **el Tipo** está configurado en **WAN**).	Prioridad 802.1p remarcada de los paquetes VLAN. Un valor mayor indica una prioridad más alta. Si se aplica una política de tráfico a la dirección de salida en una interfaz, el CPE sigue procesando los paquetes salientes según la prioridad original, pero el dispositivo de capa 2 descendente los procesa según la prioridad remarcada.	Y

Recopilación de estadísticas	Si se activa la función de recopilación de estadísticas de tráfico. Una vez activada, podrá consultar las estadísticas de tráfico en el CPE.
	Dispositivos V600 : puede ejecutar el siguiente comando para ver las estadísticas de tráfico:
	`mostrar estadísticas de política de tráfico`
	Dispositivos V300 : puede ejecutar el siguiente comando para ver las estadísticas de tráfico:
	`mostrar estadísticas de políticas de tráfico`
		Y

Plantilla de tiempo efectivo	Plantilla que define el período de tiempo durante el cual la política de QoS tiene efecto.	Y

REFERENCIAS TECNICAS

INGLES

Customizing Portal Page

Customizing a Portal Page

Context

The layout of preset pages cannot be modified. As a result, preset pages cannot meet your requirements if you want to modify the Portal page layout or use a large number of multimedia elements and images on Portal pages.

Application Scenarios

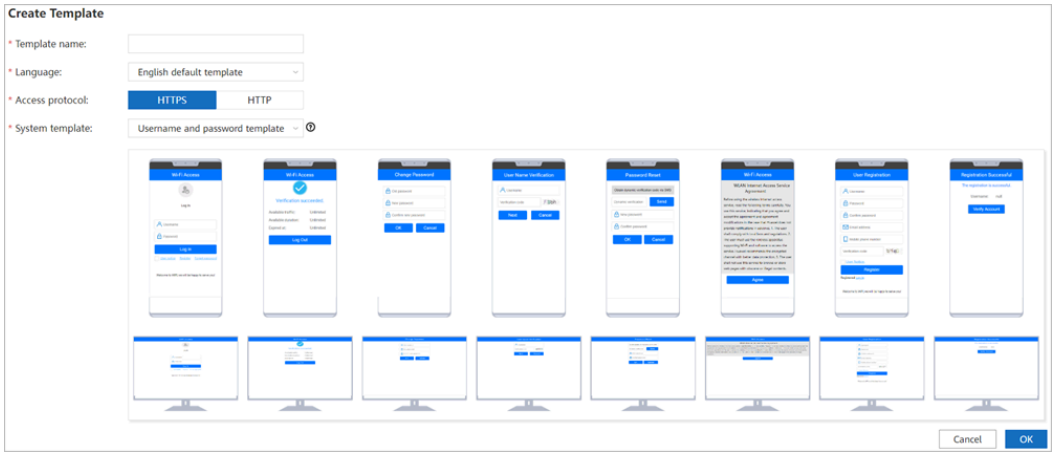
The controller provides various page controls for you to design your own Portal pages. You can customize the content and style of page controls. If some controls cannot meet requirements, you can edit the controls using the HTML custom editing function provided on the controller.

Feature Requirements

If you need to customize controls beyond the control area (including common controls and page controls), contact Huawei engineers to customize them.

Procedure

1. Choose **Admission Management** > **Admission Policy** > **Page Management** > **Page Customization** from the main menu.
2. On the **Page Customization** tab page, click ⊕ to create a custom Portal page template.



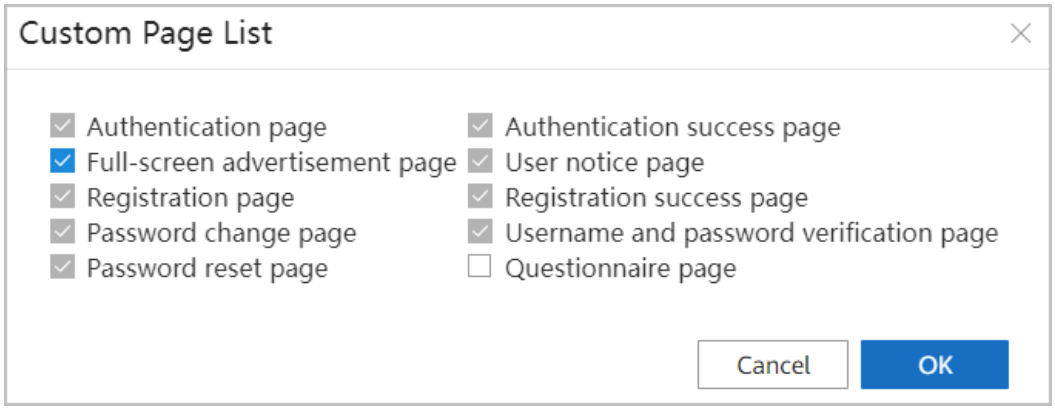
NOTE

Customized pages are generated based on the language template, access protocol, system template, and guest account policy. After a template is customized, these parameters cannot be modified.

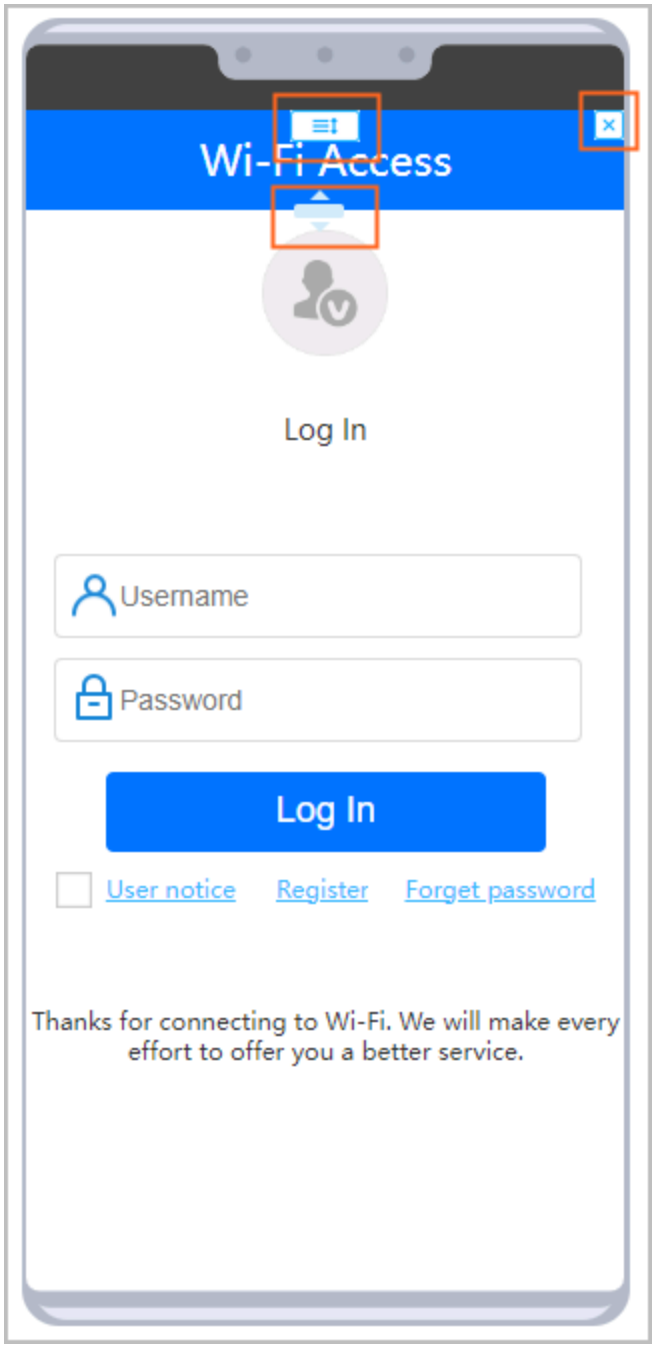
NOTICE

HTTPS is recommended, because it is more secure than HTTP. Exercise caution when using HTTP.

3. (Optional) After the template is created, click next to the template name and select the page to be customized in the **Custom Page List** window.



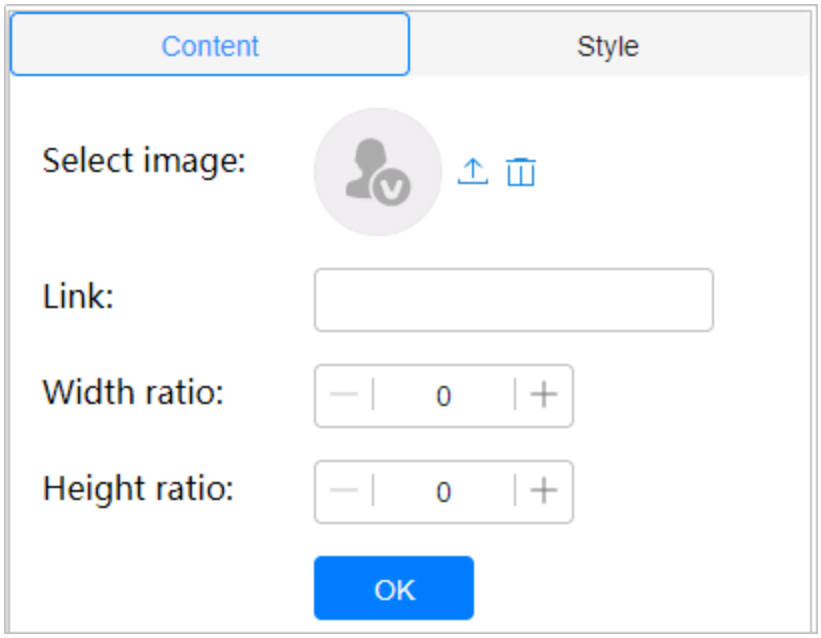
4. On the editing page, you can add or delete controls as needed, drag and drop controls to change their locations on the page, and set the height of a single control.

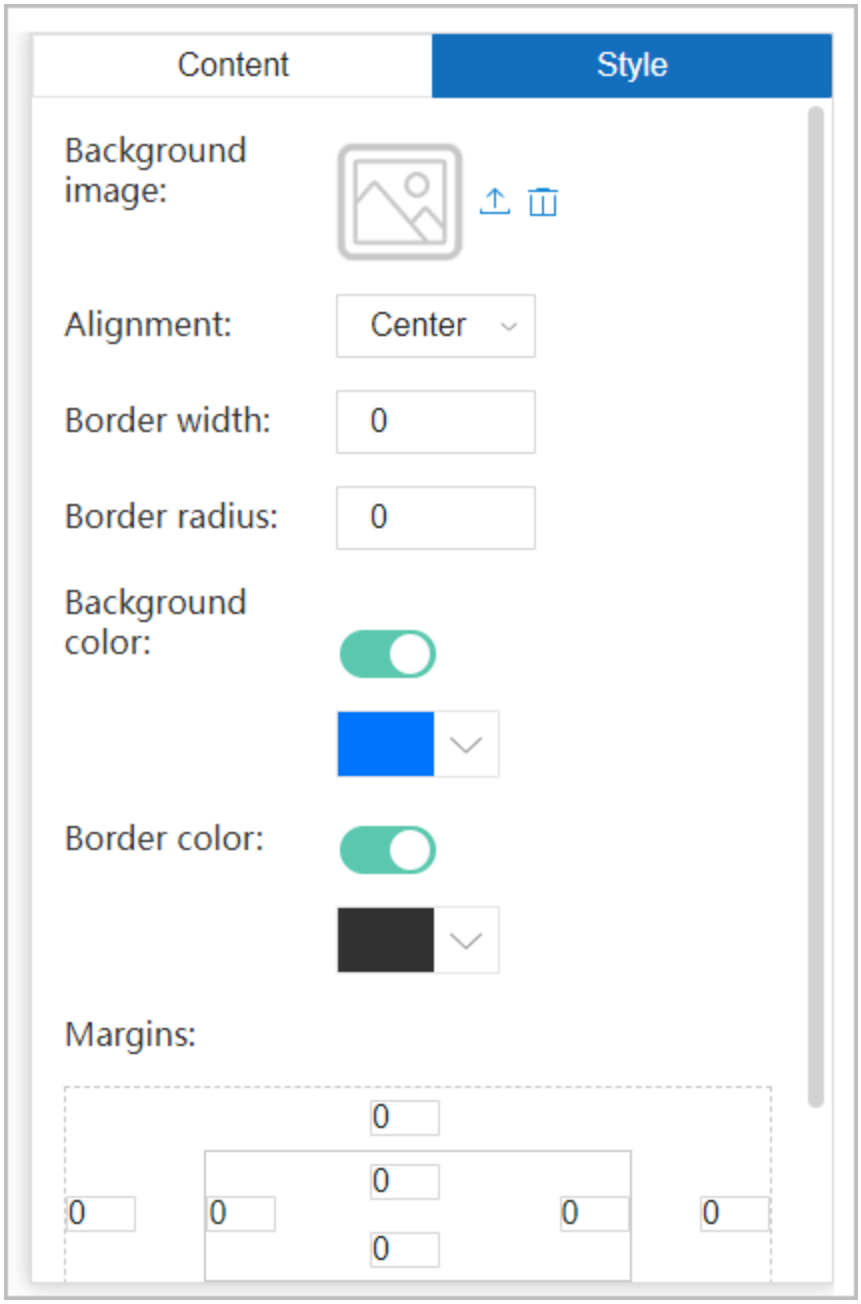


5. Configure the control style. For each control, you can set the background image, background color, text alignment mode, border thickness, border radius, border color, and margins (padding and margin).

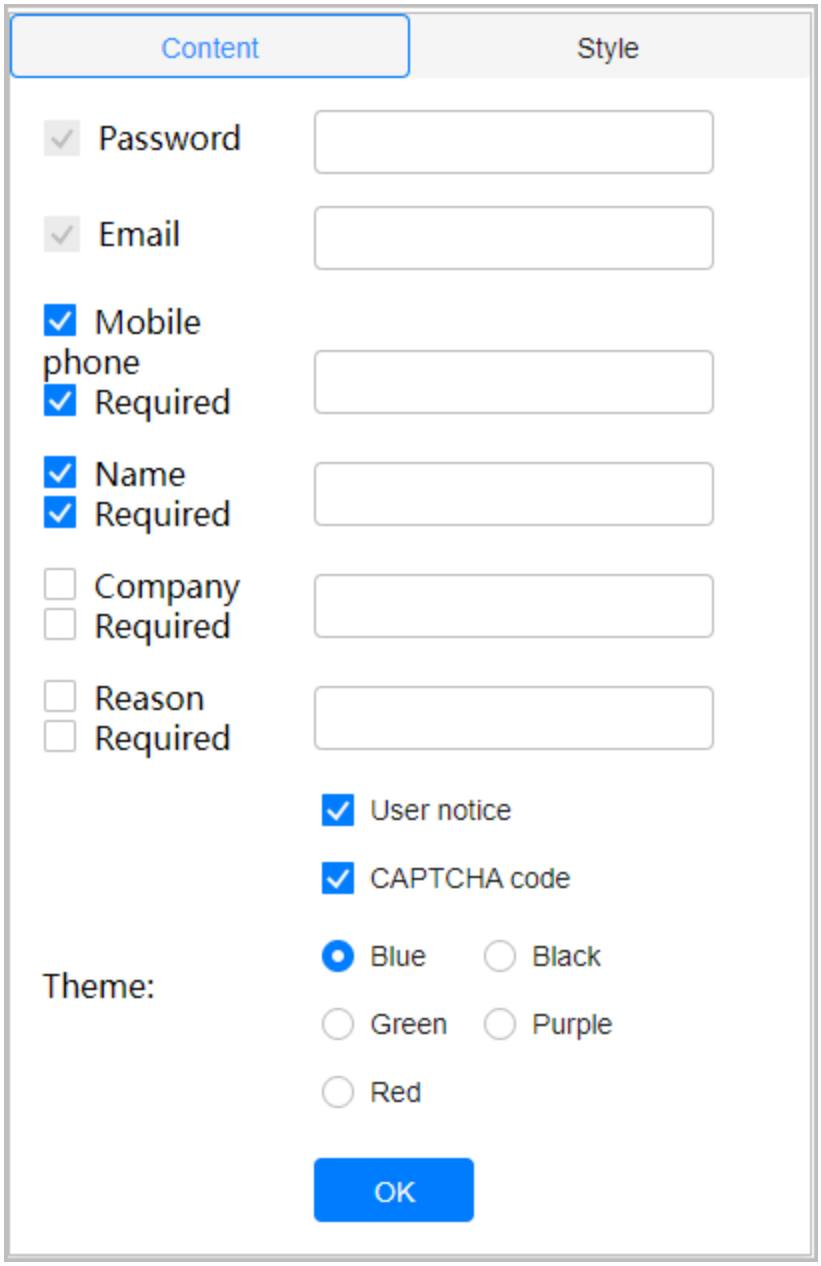
NOTE

If the width ratio and height ratio of an image are both set to 0, the image is automatically adapted based on the image ratio.


Content
Style
Select image:
Link:
Width ratio:
0
Height ratio:
0
OK


Content
Style
Background image:
Alignment:
Center
Border width:
0
Border radius:
0
Background color:
Border color:
Margins:
0
0
0
0
0
0

6. (Optional) When **Email Auth Template** is selected for **System template**, the mobile number, name, company, and application reason can be set as mandatory parameters. When you click **Get Verification Code** on the authentication page, the system checks whether the mobile number, name, company, and application reason are empty.



7. Edit controls using HTML. Table 1 lists the supported tags and attributes.

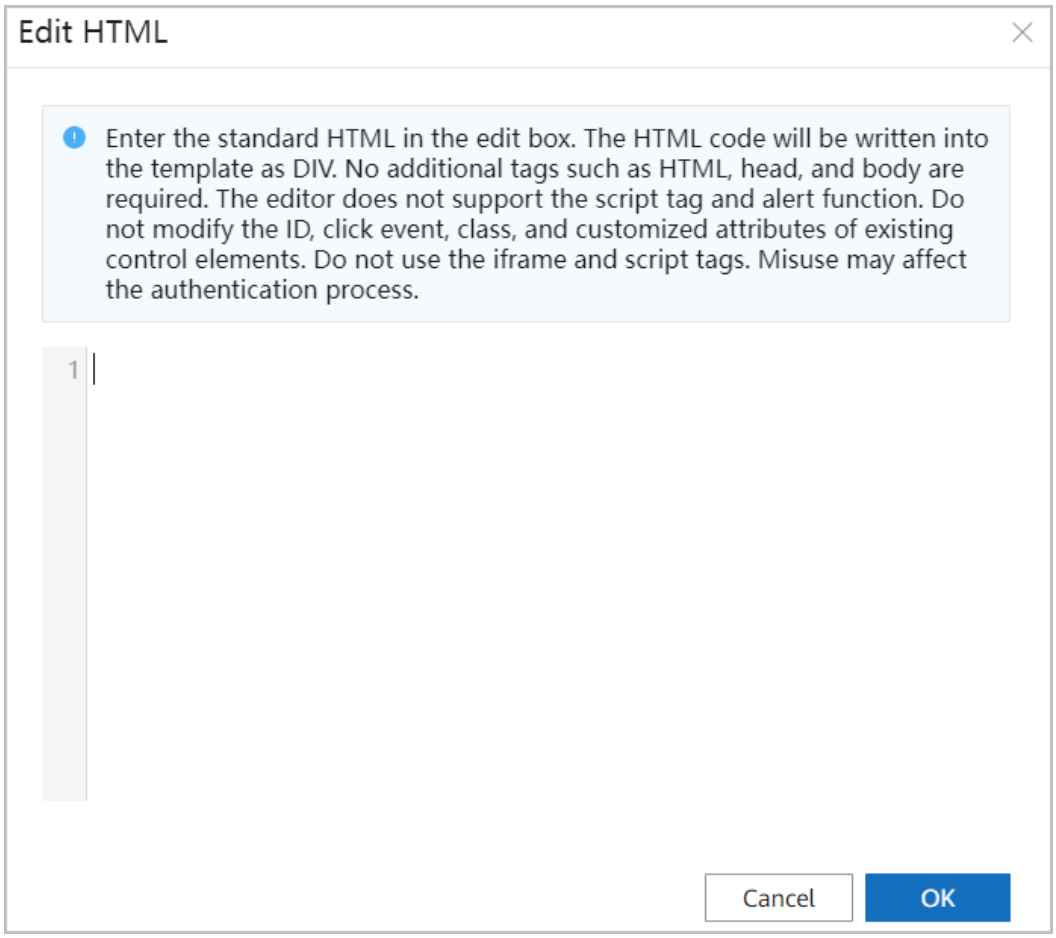


Table 1 Tags and attributes supported during HTML editing

Tag	Attributes Used in the Template
General risk-free attribute	class, style, id, width, height, title, typenum, custom-required, linkLabel, selectlabel, selectid, selectValue, lang, align, and border
<html>	-
<head>	-
<meta>	name, http-equiv, and content
<link>	rel, href, and type
<script>	type and src
<title>	-
<body>	-
	setheight, setwidth, authpluginarray, modelnum, logoutpluginarray, padarr, countdown, intervals, interval, data-

Tag	Attributes Used in the Template
	placeholder, subnum, loginothers, langnum, authchecks, firstcheck, langnum, style, typenum, id, and class
<p>	data-background, data-backgroundcolor, data-checked, and link
	link
<a>	title, download, location, lang, authtype, rel, target, name, id, and class
<img>	src, heightdata, widthdata, data-cursor, style, id, and class
<u>	-
<label>	-
<input >	type, value, placeholder, data-type, disabled, autocomplete, mdmregisterurl, isnewtab, pollingtime, disabled, name, maxlength, required, id, and class
<table>	cellspacing and cellpadding
<tbody>	-
<tr>	-
<td>	colspan, valign, and nowrap
<select>	-
<option>	value and selected
 	-
<i>	-
	-
	-
<dl>	-
<dt>	-
<dd>	-
<h3>	link

Tag	Attributes Used in the Template
<video>	autoplay, controls, and src

8. After a page is customized, click **Save** and then **Release**.

Parameter Description

Table 2 Creating a custom template

Parameter	Description
Template name	Meaning: Name of a customized page.
Language	Meaning: By using a language template, you can set the title, button labels, and text boxes on a Portal page as needed. You can customize Portal pages in different languages by using different language templates. Value range: • Chinese default template • English default template • German default template • Spanish default template
Access protocol	Value range: • HTTPS • HTTP **NOTICE:** HTTPS is recommended, because it is more secure than HTTP. Exercise caution when using HTTP.
System template	Meaning: A system template defines the pages that you can customize by default. Value range: • Username and password template • Common self-registration template • Anonymous authentication template • SMS authentication template • Social media authentication template

Parameter	Description
	• Passcode authentication template • One-click authentication template • URL-based WeChat authentication template • Public QR Code Auth Template • WeCom Authentication Template • QR Code Register Auth Template • Email Auth Template Constraints: The username and password template cannot be bound to a guest account policy and uses the approval-free mode by default. If you want to bind a guest account policy, select **Common self-registration template**.
Guest account policy	Meaning: This parameter needs to be set when **System template** is set to **Common self-registration template**, **SMS authentication template**, **One-click authentication template**, **QR Code Register Auth Template**, or **Email Auth Template**. You can configure a guest account policy on the **Admission Management > Admission Resource > Guest Management > Guest Account Policy** page. Constraints: After a guest account policy is bound to a customized page, the password type, approval mode, and approver in the guest account policy cannot be modified.

Common Control

After a Portal page template is created, you can adjust the controls displayed on Portal pages, for example, add, modify, or delete a page control, to adjust the page style.
iMaster NCE-Campus provides common controls and page controls based on application scenarios. Common controls can be used on all Portal pages, and there is no limit on the number of common controls used on each page. Page controls can only be used on the page where each page control applies.

NOTE

Generally, each time you select a control in the control area, the control is automatically displayed in the page preview, locating at the bottom of the previously configured controls. The control will not appear in the page preview if the page does not support the selected control, or another control of the same type has been added on the page (for example, the page background control).

- Title control
  Generally, a page title is located at the top of the page, and describes the page function. It is defined by a title control. The text content, font, font size, font weight, italic or not, background, and alignment

mode can be customized. A title can contain a maximum of 65535 characters.

- Image control
  An image control is used to add an image on the page. You can upload new images and use the images that have been uploaded. A maximum of 20 images can be added to a single Portal page. The size of an image cannot exceed 5 MB and the size of all images in total cannot exceed 30 MB. Images in JPG, PNG, JPEG, BMP, and GIF formats can be uploaded. You can set image links, set the width and height of an image in percentage, and delete an image that has been uploaded.

  NOTE

  If the width ratio and height ratio of an image are both set to 0, the image is automatically adapted based on the image ratio.

- Text control
  A text control is used to provide operation guides. This control can be edited in a similar way as a title control.
- Carousel control
  A carousel control is used to add scrolling images to pages. A maximum of five images can be added. You can set the play time of each image and play multiple images in cyclic mode. In addition, you can configure a redirect link for each image, so that users can be redirected to a certain link after clicking an image.
- Dial-up control
  A dial-up control is used to add phone numbers to pages. Customized prompt information, icons, and phone numbers are supported. A phone number can be a string of 10 to 24 characters, including digits, plus signs (+), minus signs (-), and spaces.
- Video control
  A video control is used to add videos to pages by specifying URLs.

  NOTE

  - If the certificate trusted by the browser is not loaded to the video playback source, the video may fail to be played. You are advised to use the playback source whose security certificate has been loaded.
  - In a customized template with **Access protocol** set to **HTTPS**, you can configure only HTTPS URLs for videos. In a customized template with **Access protocol** set to **HTTP**, you can configure HTTPS and HTTP URLs for videos.
  - Videos with HTTP URLs cannot be previewed on the editing page.

- Background control
  A background control is used to set the background of a Portal page. You can set a background color or background image. If both a background image and color are configured, the background image applies. The background style cannot be customized through a background control.
- Language control
  A language control is used to change the language in which a Portal page is displayed. Using this control, you can customize the language link text, and the Portal page to be redirected. You can set a

maximum of five language links using one language control.

> **NOTE**
>
> The language links specified in a language control must be the Portal pages that have been launched. For details about how to customize and release a Portal page, see Example for Customizing a Portal Page.

- Boarding control
  A boarding control is used to implement the boarding function on a Portal page. It allows users to click the link available on the page to download the boarding client.

Page Control

Portal pages of the following types can be configured: authentication page, authentication success page, full-screen advertisement page, user notice page, registration page, registration success page, password change page, username and password verification page, password reset page, and questionnaire page. Due to function differences, each type of page has controls that are different from those on other pages. Currently, the following controls are supported:

- Authentication page
  A user enters information on the authentication page and sends an authentication request to the authentication server.
  - Username and password authentication control: You can determine whether to add user notice, user registration, and password retrieval links on the user authentication page. Texts visible on buttons, placeholders to appear in text boxes, and control styles can be customized as well.
  - SMS authentication control: You can select whether to display the user notice link and the text box for entering a verification code on the user authentication page. Texts visible on buttons and placeholders to appear in text boxes can be customized as well.
  - URL-based WeChat authentication control: You can select whether to display the verification code text box, set the validity period of a mobile number, and customize the style, text, or image of the authentication button.
  - WeChat Work authentication control: You can specify the text to be displayed in the text box and select an authentication mode.
  - Anonymous authentication control: You can select whether to display the user notice link on the user authentication page, and customize the text, style, and image of the authentication button.
  - Social media authentication control: You can configure the default authentication mode, select whether to display the user notice link on the authentication page, and specify which social media accounts can be used for authentication, such as QQ and Twitter accounts.
  - Passcode authentication control: You can select whether to display the user notice link on the authentication page, and customize the text, style, and image of the authentication button.
  - Multi-mode authentication control: You can configure multiple authentication methods together using this control. For example, the username and password authentication, SMS authentication, passcode authentication, WeChat authentication, social media authentication, and anonymous authentication. Social media authentication supports only the HTTPS protocol and WeChat authentication supports only the HTTP protocol. When configuring multi-mode authentication,

check whether the protocol of the Portal page can be supported by social media authentication or WeChat authentication. The placeholders to appear in text boxes and button style can be customized. Before using anonymous authentication, you need to choose **Admission Management > Admission Policy > Admission Settings**, click the **Advanced Parameters** tab, and toggle on **Enable anonymous authentication**.

- Username and SMS authentication control: You can select whether to display user notice and user registration links on the authentication page. Texts visible on buttons, placeholders to appear in text boxes, and the style of each page control can be customized as well.
- Two-factor authentication (SMS) control: You can select whether to display user notice, user registration, and password retrieval links on the authentication page. Texts visible on buttons, placeholders to appear in text boxes, and the style of the login button can be customized as well.
- Two-factor authentication (RADIUS Token) control: You can select whether to display user notice, user registration, and password retrieval links on the authentication page. Texts visible on buttons, placeholders to appear in text boxes, and the style of the login button can be customized as well.
- Public QR code-based authentication control: You can customize the texts visible on buttons, as well as the theme.
- QR code scanning-based approval control: The QR code scanning-based authentication page and employee login page can be customized. On the QR code scanning-based authentication page, you can edit prompt messages and texts visible on buttons, and determine whether to display the user notice link. On the employee login page, you can edit account placeholders, password placeholders, and texts visible on buttons, and determine whether to display the user notice link and verification code text box.
- Email address authentication control: You can determine whether to display the user notice and verification code controls on the authentication page, and customize the placeholders to appear in text boxes and subjects.

- Authentication success page
  Users will be redirected to an authentication success page after successful authentication. The page displays the authentication result and allows users to log out or change their passwords.
  - Authentication success information: On an authentication success page, you can select whether to display the username, remaining data allowance, remaining online duration allowance, and expiration time. In addition, you can select whether to display mobile number association, password change, logout, and self-service buttons.
  - Authentication success message: This control defines a message indicating that user authentication succeeds.
  - Portal list 1: This control provides the function of editing the portal information page.
  - Portal list 2: This control provides the function of editing the portal information page.
  - Portal list 3: This control provides the function of editing the portal information page.
  - Portal in a single line: This control provides the function of editing the portal information page.
  - Portal double column: This control provides the function of editing the portal information page.

NOTE

Customized HTML pages can be uploaded. After a user is successfully authenticated, the user can be redirected to a customized Portal page from the authentication success page. To support this function, the administrator needs to upload a customized Portal page and add page

controls of a specific style as needed on the **Admission Management > Admission Policy > Page Management > Portal Management** page.

NOTICE

Tenant administrators have the permission to upload portal information pages and release customized pages. If such pages are uploaded, the application scenarios of customized pages need to be specified, uploaded files need to be scanned for viruses, and file validity needs to be verified (such as file names, suffixes, sizes, and whether files contain XSS attacks and phishing attacks).

- Full-screen advertisement page
  Only the banner countdown or video countdown can be set on the full-screen advertisement page. For banner countdown, you can specify the countdown time, countdown prompt information, merchant prompt information, and play time of a single image. A maximum of five images can be selected. For video countdown, you can set the countdown time and the video URL.

  NOTE

  - If the certificate trusted by the browser is not loaded to the video playback source, the video may fail to be played. You are advised to use the playback source whose security certificate has been loaded.
  - In a customized template with **Access protocol** set to **HTTPS**, you can configure only HTTPS URLs for videos. In a customized template with **Access protocol** set to **HTTP**, you can configure HTTPS and HTTP URLs for videos.
  - Videos with HTTP URLs cannot be previewed on the editing page.

- User notice page
  On the user notice page, rules and information that users need to be aware of when they attempt to connect to the Wi-Fi network are displayed.
  - User notice control: This control allows you to edit a user notice.
  - Agree control: After a user clicks the agree button, the login page is displayed. The button and control styles can be customized.
  - MDM registration control: prompts the user to register terminals with an MDM server. The button and control styles can be customized.
- Registration page
  On a user registration page, a user can register an account for authentication.
  - User registration control: The button labels, control styles, and placeholders of text boxes can be customized.
  - If user-defined parameters have been configured for the guest account policy in a self-registration template, you can set user-defined fields on the registration page as mandatory.
- Registration success page

- Registration success control: You can customize the style of the buttons and controls that are used to redirect users to the user authentication page.
- QR code scanning-based approval control: You can customize the text prompt, as well as the styles of the button and control for redirecting users to authentication pages.

> **NOTE**
>
> The QR code scanning-based approval control is supported only in common self-registration templates.

- Password change page
  - Password change control: The button labels, control styles, and placeholders of text boxes can be customized.

> **NOTE**
>
> Only passwords of local accounts and AD accounts can be changed.

- Username and password verification page
  - User name verification control: The button labels, control styles, and placeholders of text boxes can be customized.
- Password reset page
  - Password reset control: The button labels, control styles, and placeholders of text boxes can be customized.

> **NOTE**
>
> Only passwords of local accounts can be reset.

- Questionnaire page
  - Questionnaire control: The question descriptions, answer types, answer options, button labels, and control styles can be customized.

> **NOTE**
>
> - Before customizing a questionnaire page using a template, click  next to the template name and select **Questionnaire page** in the **Custom Page List** window.
> - Administrators can view questionnaire records on the **Questionnaire Records** tab page under **Admission Management** > **Admission Resource** > **Guest Management** > **Guest Logs**.
> - Tenant administrators can add a text control on a questionnaire page to declare the nature and terms of use of the questionnaire. If personal data is involved, tenant administrators

need to clearly inform end users of the questionnaire purpose and data collection scope.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Customizing Portal Page

Personalizar una página del portal

Contexto

El diseño de las páginas predefinidas no se puede modificar. Por lo tanto, no se ajustarán a sus necesidades si desea modificar el diseño de la página del Portal o usar una gran cantidad de elementos multimedia e imágenes en las páginas del Portal.

Escenarios de aplicación

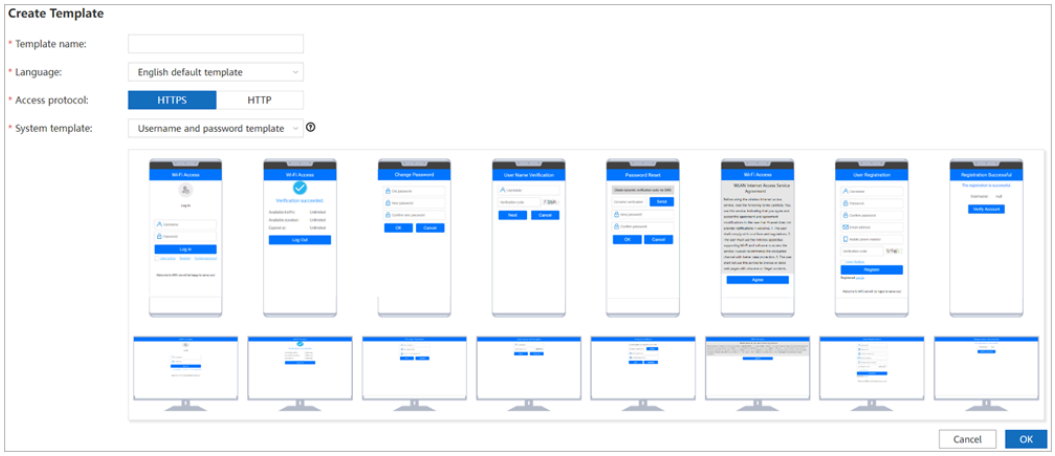
El controlador proporciona varios controles de página para que diseñes tus propias páginas del Portal. Puedes personalizar el contenido y el estilo de los controles. Si algunos controles no cumplen con los requisitos, puedes editarlos mediante la función de edición personalizada de HTML del controlador.

Requisitos de las funciones

Si necesita personalizar controles más allá del área de control (incluidos controles comunes y controles de página), comuníquese con los ingenieros de Huawei para personalizarlos.

Procedimiento

1. Seleccione **Gestión de admisiones** > **Política de admisiones** > **Gestión de páginas** > **Personalización de páginas** en el menú principal.
2. En la pestaña **Personalización de página**, haga clic para crear una plantilla de página de Portal personalizada.



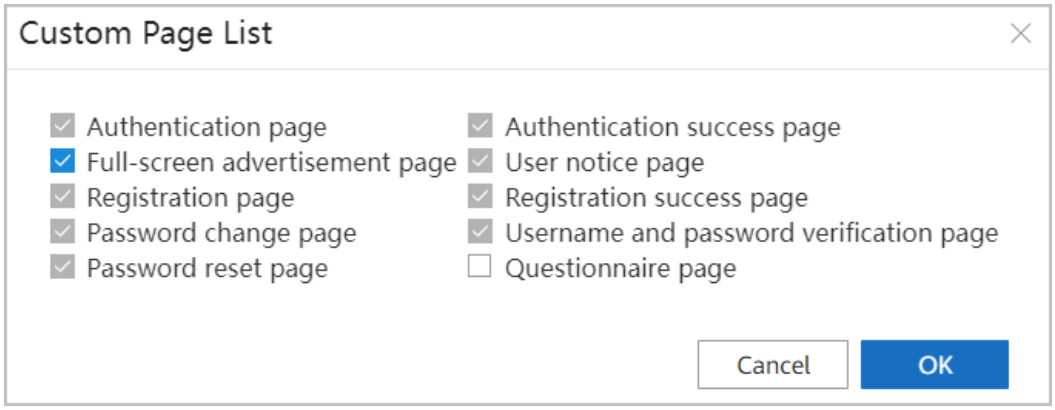
NOTE

Las páginas personalizadas se generan según la plantilla de idioma, el protocolo de acceso, la plantilla del sistema y la política de cuentas de invitado. Una vez personalizada una plantilla, estos parámetros no se pueden modificar.

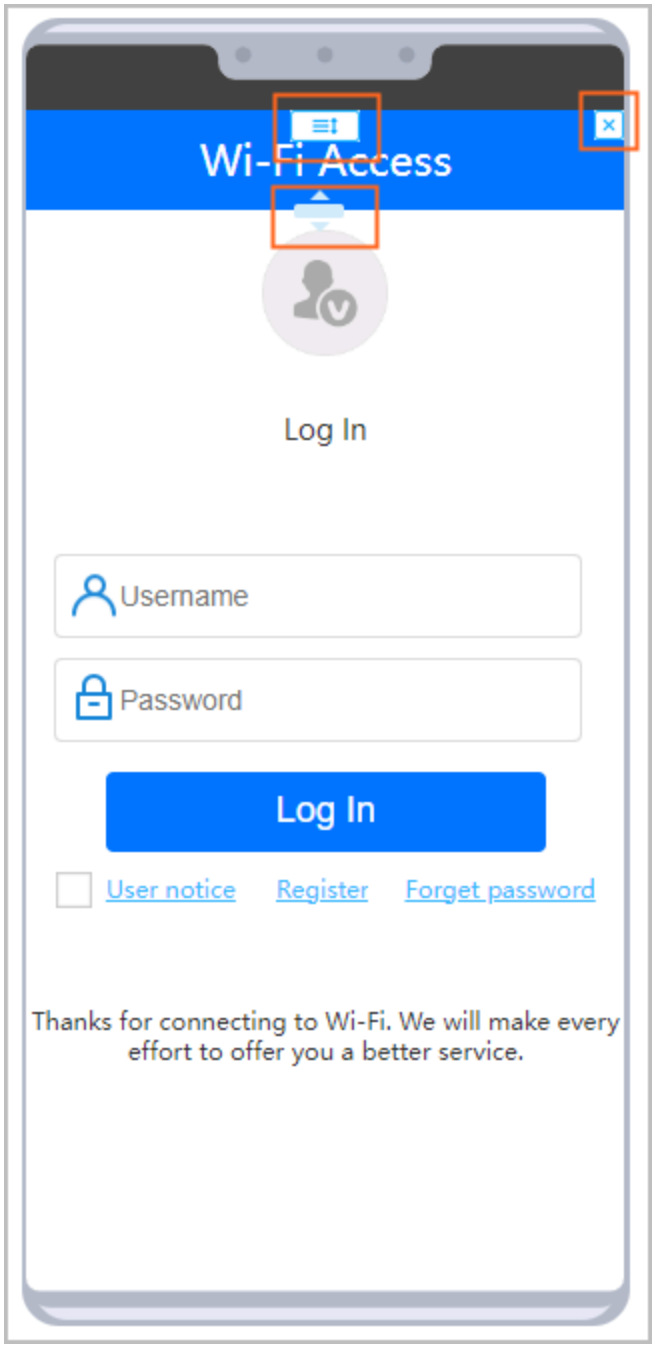
NOTICE

Se recomienda usar HTTPS, ya que es más seguro que HTTP. Tenga cuidado al usar HTTP.

3. (Opcional) Después de crear la plantilla, haga clic junto al nombre de la plantilla y seleccione la página que desea personalizar en la ventana **Lista de páginas personalizadas** .



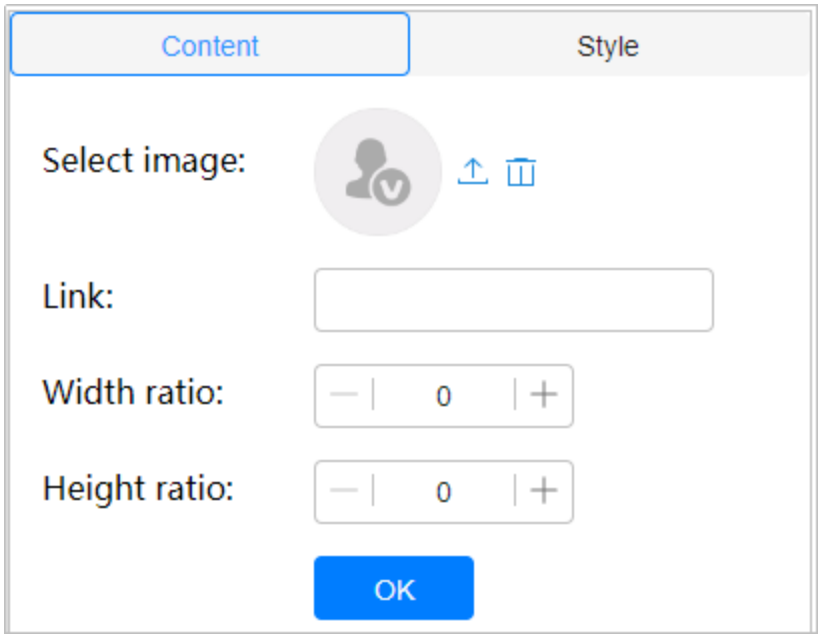
4. En la página de edición, puede agregar o eliminar controles según sea necesario, arrastrar y soltar controles para cambiar sus ubicaciones en la página y establecer la altura de un solo control.

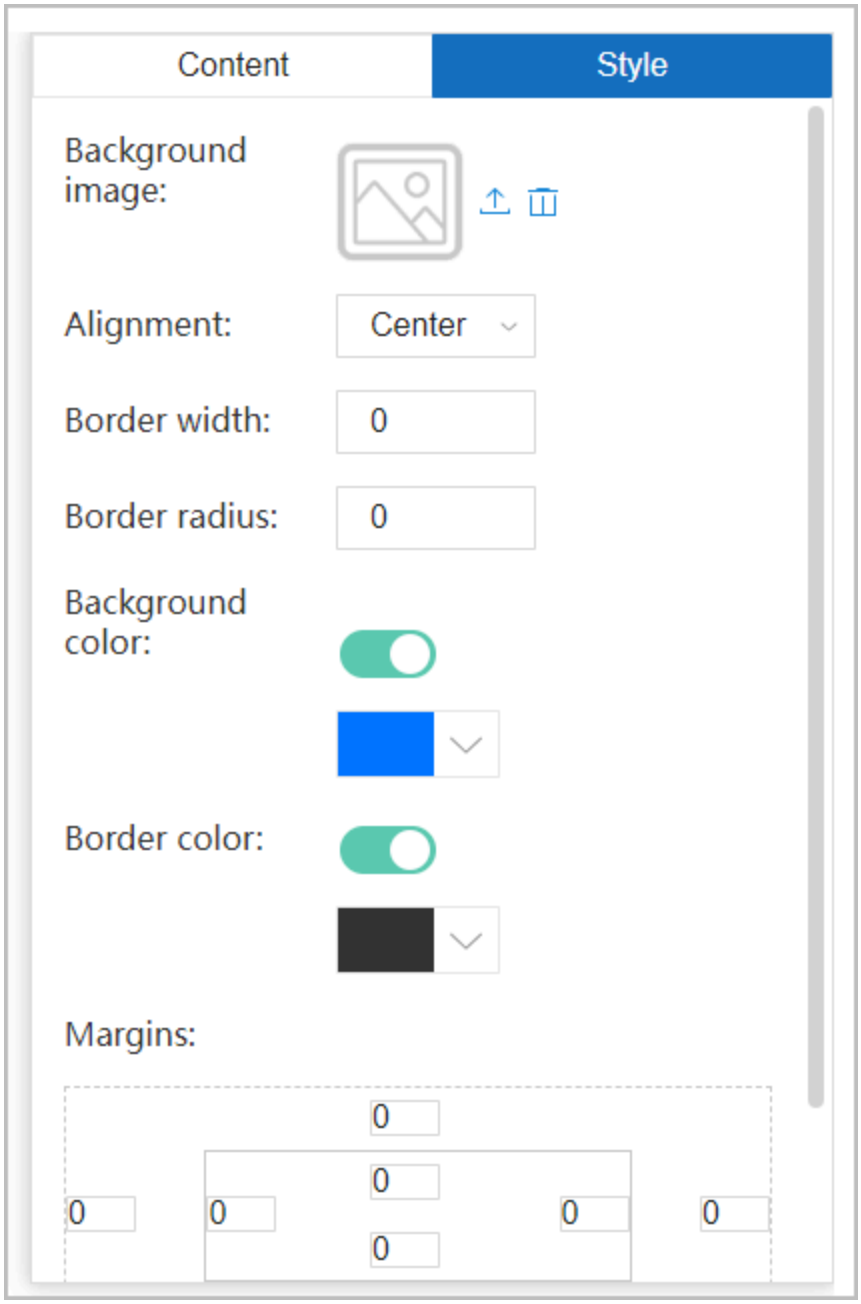


5. Configura el estilo del control. Para cada control, puedes configurar la imagen de fondo, el color de fondo, el modo de alineación del texto, el grosor, el radio y el color del borde, y los márgenes (relleno y margen).

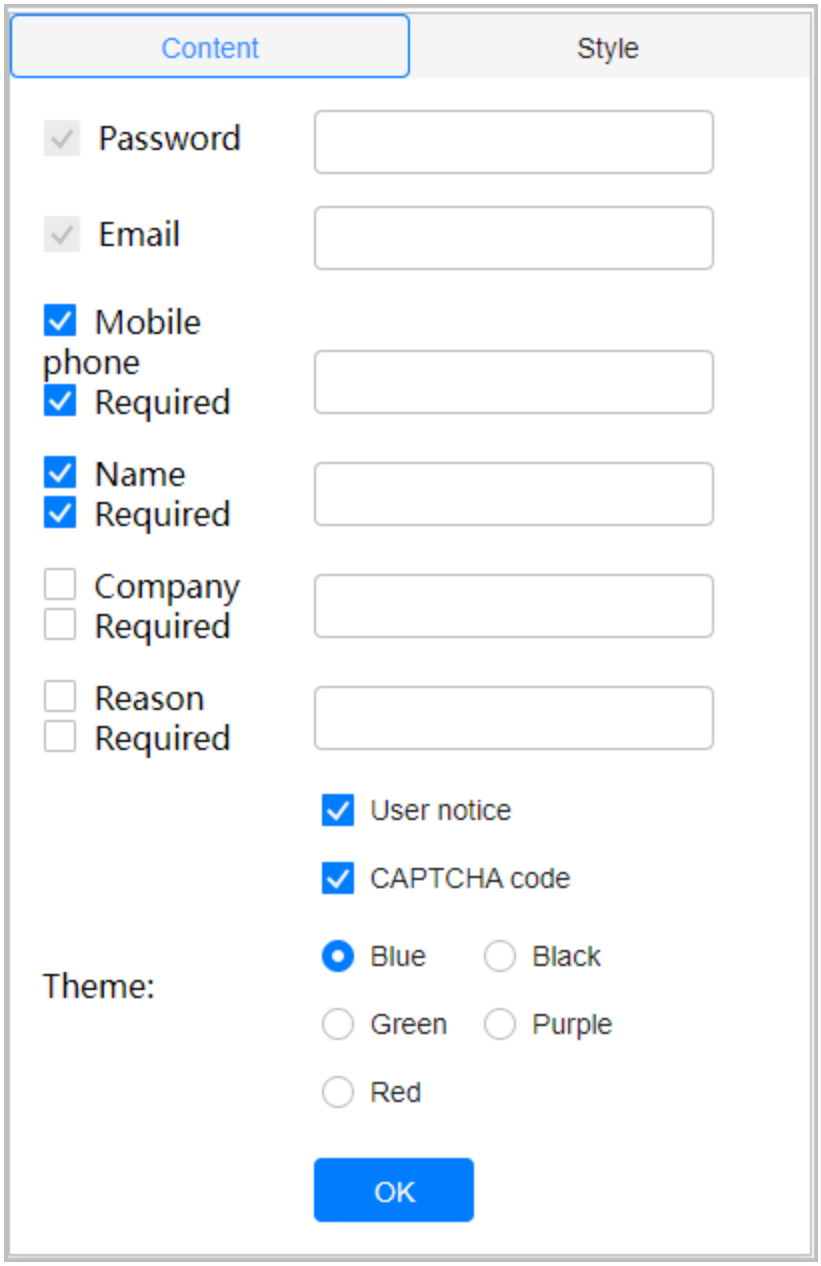
NOTE

Si la relación de ancho y la relación de alto de una imagen se establecen en 0, la imagen se adapta automáticamente en función de la relación de imagen.


Content
Style
Select image:
Link:
Width ratio:
0
Height ratio:
0
OK


Content
Style
Background image:
Alignment:
Center
Border width:
0
Border radius:
0
Background color:
Border color:
Margins:
0
0
0
0
0
0

6. (Opcional) Al seleccionar **la Plantilla de autenticación de correo electrónico como Plantilla del sistema** , se pueden configurar como parámetros obligatorios el número de teléfono móvil, el nombre, la empresa y el motivo de la solicitud. Al hacer clic en " **Obtener código de verificación"** en la página de autenticación, el sistema comprueba si los campos de número de teléfono móvil, nombre, empresa y motivo de la solicitud están vacíos.



7. Edite controles mediante HTML. La Tabla 1 enumera las etiquetas y atributos compatibles.

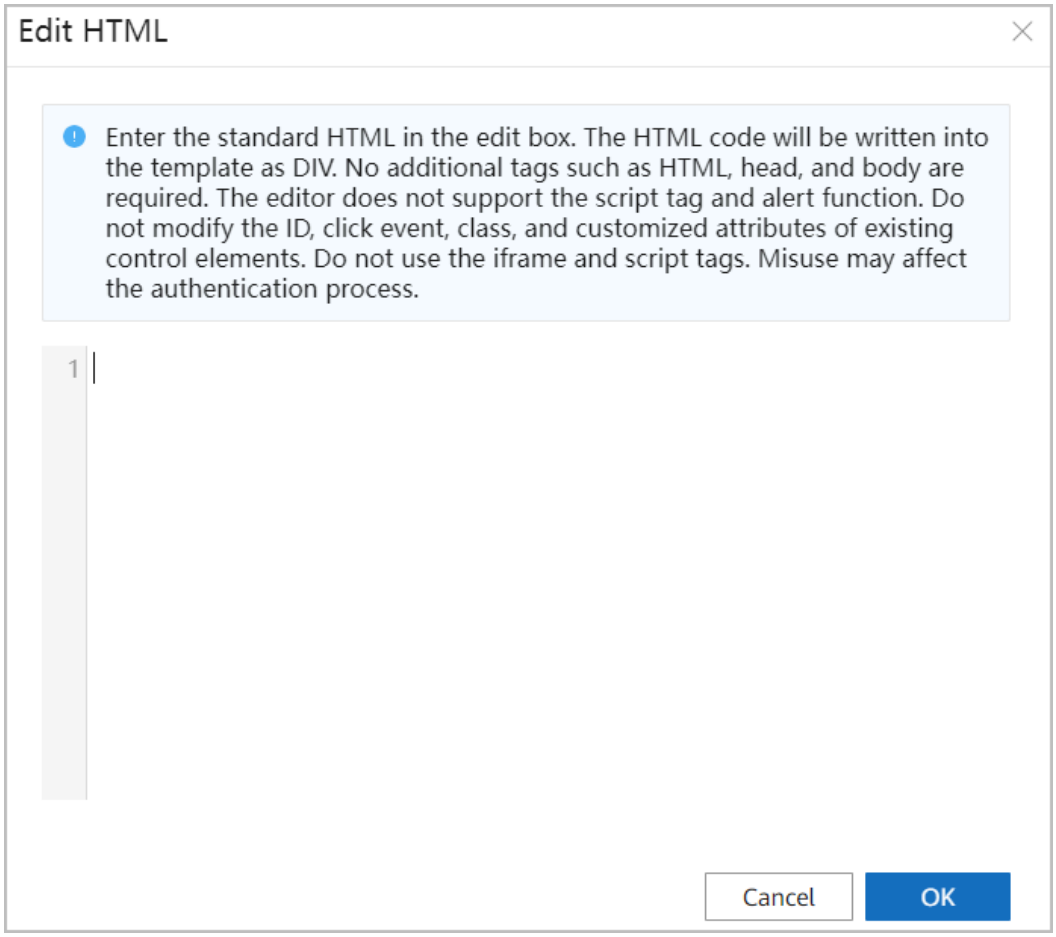


Tabla 1 Etiquetas y atributos admitidos durante la edición HTML

Etiqueta	**Atributos utilizados en la plantilla**
Atributo general libre de riesgos	clase, estilo, id, ancho, alto, título, typenum, personalizado-requerido, linkLabel, selectlabel, selectid, selectValue, lang, align y border
<html>	-
<cabeza>	-
<meta>	nombre, equivalente http y contenido
<enlace>	rel, href y tipo
<guión>	tipo y origen
<título>	-
<cuerpo>	-
	setheight, setwidth, authpluginarray, modelnum, logoutpluginarray, padarr, cuenta regresiva, intervalos, intervalo,

Etiqueta	Atributos utilizados en la plantilla
	marcador de posición de datos, subnum, loginothers, langnum, authchecks, firstcheck, langnum, estilo, typenum, id y clase
<p>	datos de fondo, color de fondo de datos, datos comprobados y enlace
	enlace
<a>	título, descarga, ubicación, idioma, tipo de autorización, rel, destino, nombre, id y clase
<img>	src, heightdata, widthdata, cursor de datos, estilo, id y clase
<u>	-
<etiqueta>	-
<entrada>	tipo, valor, marcador de posición, tipo de dato, deshabilitado, autocompletar, mdmregisterurl, isnewtab, pollingtime, deshabilitado, nombre, longitud máxima, obligatorio, id y clase
<tabla>	espaciado y relleno de celdas
<cuerpo>	-
<tr>	-
<td>	colspan, valign y nowrap
<seleccionar>	-
<opción>	valor y seleccionado
 	-
<i>	-
	-
	-
<dl>	-
<dt>	-
<dd>	-

Etiqueta	Atributos utilizados en la plantilla
<h3>	enlace
<vídeo>	reproducción automática, controles y fuente

8. Después de personalizar una página, haga clic en **Guardar** y luego **en Liberar** .

Descripción del parámetro

Tabla 2 Creación de una plantilla personalizada

Parámetro	Descripción
Nombre de la plantilla	Significado: Nombre de una página personalizada.
Idioma	Significado: Al usar una plantilla de idioma, puede configurar el título, las etiquetas de los botones y los cuadros de texto de una página del Portal según sus necesidades. Puede personalizar las páginas del Portal en diferentes idiomas usando diferentes plantillas. Rango de valores: • Plantilla predeterminada en chino • Plantilla predeterminada en inglés • Plantilla predeterminada en alemán • Plantilla predeterminada en español
Protocolo de acceso	Rango de valores: • HTTPS • HTTP **AVISO:** Se recomienda usar HTTPS, ya que es más seguro que HTTP. Tenga cuidado al usar HTTP.
Plantilla del sistema	Significado: Una plantilla de sistema define las páginas que puedes personalizar de forma predeterminada. Rango de valores: • Plantilla de nombre de usuario y contraseña • Plantilla común de autorregistro

Parámetro	Descripción
	• Plantilla de autenticación anónima • Plantilla de autenticación por SMS • Plantilla de autenticación de redes sociales • Plantilla de autenticación con código de acceso • Plantilla de autenticación con un solo clic • Plantilla de autenticación de WeChat basada en URL • Plantilla de autorización de código QR público • Plantilla de autenticación de WeCom • Plantilla de autorización de registro de código QR • Plantilla de autorización de correo electrónico Restricciones: La plantilla de nombre de usuario y contraseña no se puede vincular a una política de cuenta de invitado y utiliza el modo sin aprobación de forma predeterminada. Si desea vincular una política de cuenta de invitado, seleccione **Plantilla de autorregistro común** .
Política de cuentas de invitados	Significado: Este parámetro debe configurarse cuando **la plantilla del sistema** se configura como **Plantilla de autorregistro común** , **Plantilla de autenticación por SMS** , **Plantilla de autenticación con un solo clic** , **Plantilla de autenticación de registro de código QR** o **Plantilla de autenticación por correo electrónico** . Puede configurar una política de cuenta de invitado en la página **Gestión de Admisiones > Recursos de Admisión > Gestión de Invitados > Política de Cuenta de Invitado .** Restricciones: después de que una política de cuenta de invitado esté vinculada a una página personalizada, el tipo de contraseña, el modo de aprobación y el aprobador en la política de cuenta de invitado no se pueden modificar.

Control común

Después de crear una plantilla de página de Portal, puede ajustar los controles que se muestran en las páginas de Portal, por ejemplo, agregar, modificar o eliminar un control de página para ajustar el estilo de la página.
iMaster NCE-Campus ofrece controles comunes y controles de página según los escenarios de aplicación. Los controles comunes se pueden usar en todas las páginas del portal y no hay límite en el número de controles comunes que se pueden usar en cada página. Los controles de página solo se pueden usar en la página donde se aplica cada control.

NOTE

Generalmente, cada vez que se selecciona un control en el área de controles, este se muestra automáticamente en la vista previa de la página, ubicándose en la parte inferior de los controles previamente configurados. El control no aparecerá en la vista previa si la página no lo admite o si se ha añadido otro control del mismo tipo (por ejemplo, el control de fondo de página).

- Control de títulos
  Generalmente, el título de una página se ubica en la parte superior y describe su función. Se define mediante un control de título. Se pueden personalizar el contenido del texto, la fuente, el tamaño y el grosor de la fuente, si está en cursiva o no, el fondo y el modo de alineación. Un título puede contener un máximo de 65 535 caracteres.
- Control de imagen
  Se utiliza un control de imagen para añadir una imagen a la página. Puede subir nuevas imágenes y usar las que ya ha subido. Se puede añadir un máximo de 20 imágenes a una sola página del Portal. El tamaño de una imagen no puede superar los 5 MB y el de todas las imágenes no puede superar los 30 MB. Se pueden subir imágenes en formato JPG, PNG, JPEG, BMP y GIF. Puede configurar enlaces de imágenes, ajustar el ancho y la altura de una imagen en porcentaje y eliminar una imagen subida.

NOTE

Si la relación de ancho y la relación de alto de una imagen se establecen en 0, la imagen se adapta automáticamente en función de la relación de imagen.

- Control de texto
  Un control de texto se utiliza para proporcionar guías de operación. Este control se puede editar de forma similar a un control de título.
- Control del carrusel
  Se utiliza un control de carrusel para añadir imágenes desplazables a las páginas. Se puede añadir un máximo de cinco imágenes. Se puede configurar el tiempo de reproducción de cada imagen y reproducir varias imágenes en modo cíclico. Además, se puede configurar un enlace de redirección para cada imagen, de modo que los usuarios sean redirigidos a un enlace específico tras hacer clic en ella.
- Control de acceso telefónico
  Se utiliza un control de acceso telefónico para añadir números de teléfono a las páginas. Se admiten información de aviso, iconos y números de teléfono personalizados. Un número de teléfono puede ser una cadena de 10 a 24 caracteres, incluyendo dígitos, signos más (+), signos menos (-) y espacios.
- Control de vídeo
  Se utiliza un control de video para agregar videos a las páginas especificando URL.

NOTE

  - Si el certificado de confianza del navegador no está cargado en la fuente de reproducción de vídeo, es posible que no se reproduzca. Se recomienda usar la fuente de reproducción cuyo certificado de seguridad esté cargado.

  - En una plantilla personalizada con el protocolo **de acceso** HTTPS , puedes configurar solo URL HTTPS para vídeos. En una plantilla personalizada con el protocolo **de acceso** HTTP , puedes configurar URL HTTPS y HTTP para vídeos.
  - No es posible previsualizar los vídeos con URL HTTP en la página de edición.

- Control de fondo
  Un control de fondo se utiliza para configurar el fondo de una página del Portal. Puede configurar un color o una imagen de fondo. Si se configuran tanto una imagen como un color de fondo, se aplicará la imagen de fondo. El estilo de fondo no se puede personalizar mediante un control de fondo.
- Control del lenguaje
  Un control de idioma permite cambiar el idioma de visualización de una página del Portal. Con este control, puede personalizar el texto del enlace y la página del Portal a la que se redirigirá. Puede configurar un máximo de cinco enlaces de idioma con un solo control.

> **NOTE**
>
> Los enlaces de idioma especificados en un control de idioma deben ser las páginas del portal iniciadas. Para obtener más información sobre cómo personalizar y publicar una página del portal, consulte Ejemplo de personalización de una página del portal .

- Control de embarque
  Se utiliza un control de embarque para implementar la función de embarque en una página del portal. Permite a los usuarios hacer clic en el enlace disponible en la página para descargar el cliente de embarque.

Control de página

Se pueden configurar los siguientes tipos de páginas del portal: página de autenticación, página de autenticación correcta, página de publicidad a pantalla completa, página de avisos para el usuario, página de registro, página de registro correcto, página de cambio de contraseña, página de verificación de nombre de usuario y contraseña, página de restablecimiento de contraseña y página de cuestionario. Debido a las diferencias funcionales, cada tipo de página tiene controles diferentes a los de otras páginas. Actualmente, se admiten los siguientes controles:

- Página de autenticación
  Un usuario ingresa información en la página de autenticación y envía una solicitud de autenticación al servidor de autenticación.
  - Control de autenticación de usuario y contraseña: Puede determinar si desea añadir avisos de usuario, registro de usuario y enlaces para recuperar contraseña en la página de autenticación de usuario. También puede personalizar los textos visibles en los botones, los marcadores de posición que aparecen en los cuadros de texto y los estilos de control.
  - Control de autenticación por SMS: Puede seleccionar si desea mostrar el enlace de notificación al usuario y el cuadro de texto para introducir un código de verificación en la página de autenticación. También puede personalizar los textos visibles en los botones y los marcadores de posición que aparecen en los cuadros de texto.
  - Control de autenticación de WeChat basado en URL: puede seleccionar si desea mostrar el cuadro de texto del código de verificación, establecer el período de validez de un número de teléfono

móvil y personalizar el estilo, el texto o la imagen del botón de autenticación.

- Control de autenticación de WeChat Work: puede especificar el texto que se mostrará en el cuadro de texto y seleccionar un modo de autenticación.
- Control de autenticación anónima: puede seleccionar si desea mostrar el enlace de aviso al usuario en la página de autenticación del usuario y personalizar el texto, el estilo y la imagen del botón de autenticación.
- Control de autenticación de redes sociales: puede configurar el modo de autenticación predeterminado, seleccionar si desea mostrar el enlace de aviso al usuario en la página de autenticación y especificar qué cuentas de redes sociales se pueden usar para la autenticación, como las cuentas de QQ y Twitter.
- Control de autenticación con contraseña: puede seleccionar si desea mostrar el enlace de aviso al usuario en la página de autenticación y personalizar el texto, el estilo y la imagen del botón de autenticación.
- Control de autenticación multimodo: Puede configurar varios métodos de autenticación simultáneamente con este control. Por ejemplo, autenticación con nombre de usuario y contraseña, autenticación por SMS, autenticación con código de acceso, autenticación por WeChat, autenticación por redes sociales y autenticación anónima. La autenticación por redes sociales solo admite el protocolo HTTPS, mientras que la autenticación por WeChat solo admite el protocolo HTTP. Al configurar la autenticación multimodo, compruebe si el protocolo de la página del portal es compatible con la autenticación por redes sociales o por WeChat. Los marcadores de posición que aparecen en los cuadros de texto y el estilo de los botones se pueden personalizar. Antes de usar la autenticación anónima, debe seleccionar **Administración de Admisiones > Política de Admisiones > Configuración de Admisiones** , hacer clic en la pestaña **Parámetros Avanzados** y activar la opción **Habilitar autenticación anónima** .
- Control de autenticación por nombre de usuario y SMS: Puede seleccionar si desea mostrar avisos y enlaces de registro en la página de autenticación. También puede personalizar los textos visibles en los botones, los marcadores de posición en los cuadros de texto y el estilo de cada control de página.
- Control de autenticación de dos factores (SMS): Puede seleccionar si desea mostrar avisos de usuario, el registro de usuario y enlaces para recuperar contraseña en la página de autenticación. También puede personalizar los textos visibles en los botones, los marcadores de posición que aparecen en los cuadros de texto y el estilo del botón de inicio de sesión.
- Control de autenticación de dos factores (token RADIUS): Puede seleccionar si desea mostrar avisos de usuario, registro de usuario y enlaces para recuperar contraseña en la página de autenticación. También puede personalizar los textos visibles en los botones, los marcadores de posición que aparecen en los cuadros de texto y el estilo del botón de inicio de sesión.
- Control de autenticación público basado en código QR: puedes personalizar los textos visibles en los botones, así como el tema.
- Control de aprobación mediante escaneo de códigos QR: La página de autenticación mediante escaneo de códigos QR y la página de inicio de sesión de empleados se pueden personalizar. En la página de autenticación mediante escaneo de códigos QR, puede editar los mensajes de aviso y los textos visibles en los botones, y determinar si se muestra el enlace de aviso al usuario. En la página de inicio de sesión de empleados, puede editar los marcadores de posición de la cuenta, los marcadores de posición de la contraseña y los textos visibles en los botones, y determinar si se muestra el enlace de aviso al usuario y el cuadro de texto del código de verificación.
- Control de autenticación de direcciones de correo electrónico: puede determinar si desea mostrar los controles de aviso de usuario y código de verificación en la página de autenticación, y

personalizar los marcadores de posición para que aparezcan en cuadros de texto y asuntos.

- Página de éxito de autenticación
  Tras la autenticación, los usuarios serán redirigidos a una página de autenticación exitosa. Esta página muestra el resultado y permite cerrar sesión o cambiar su contraseña.
  - Información de autenticación exitosa: En la página de autenticación exitosa, puede seleccionar si desea mostrar el nombre de usuario, la asignación de datos restante, el tiempo restante de conexión y la fecha de vencimiento. Además, puede seleccionar si desea mostrar los botones de asociación de número de teléfono móvil, cambio de contraseña, cierre de sesión y autoservicio.
  - Mensaje de éxito de autenticación: este control define un mensaje que indica que la autenticación del usuario se realizó correctamente.
  - Lista del portal 1: este control proporciona la función de editar la página de información del portal.
  - Lista del portal 2: este control proporciona la función de editar la página de información del portal.
  - Lista del portal 3: este control proporciona la función de editar la página de información del portal.
  - Portal en una sola línea: Este control proporciona la función de editar la página de información del portal.
  - Portal de doble columna: Este control proporciona la función de editar la página de información del portal.

NOTE

Se pueden subir páginas HTML personalizadas. Tras la autenticación correcta de un usuario, se le puede redirigir a una página personalizada del Portal desde la página de autenticación correcta. Para habilitar esta función, el administrador debe subir una página personalizada del Portal y agregar controles de página con un estilo específico, según sea necesario, en la página **Gestión de Admisiones > Política de Admisiones > Gestión de Páginas > Gestión del Portal** .

NOTICE

Los administradores de inquilinos tienen permiso para cargar páginas de información del portal y publicar páginas personalizadas. Si se cargan estas páginas, es necesario especificar los escenarios de aplicación, analizar los archivos cargados en busca de virus y verificar su validez (como nombres de archivo, sufijos, tamaños y si contienen ataques XSS y phishing).

- Página de anuncios en pantalla completa
  Solo se puede configurar la cuenta regresiva del banner o del video en la página de anuncios a pantalla completa. Para la cuenta regresiva del banner, puede especificar el tiempo de la cuenta regresiva, la información del aviso de la cuenta regresiva, la información del aviso del comerciante y el tiempo de reproducción de una sola imagen. Se puede seleccionar un máximo de cinco imágenes. Para la cuenta regresiva del video, puede configurar el tiempo de la cuenta regresiva y la URL del video.

NOTE

  - Si el certificado de confianza del navegador no está cargado en la fuente de reproducción de vídeo, es posible que no se reproduzca. Se recomienda usar la fuente de reproducción cuyo certificado de seguridad esté cargado.
  - En una plantilla personalizada con el protocolo **de acceso** HTTPS , puedes configurar solo URL HTTPS para vídeos. En una plantilla personalizada con el protocolo **de acceso** HTTP , puedes configurar URL HTTPS y HTTP para vídeos.
  - No es posible previsualizar los vídeos con URL HTTP en la página de edición.

- Página de aviso al usuario
  En la página de aviso al usuario, se muestran las reglas y la información que los usuarios deben tener en cuenta cuando intentan conectarse a la red Wi-Fi.
  - Control de aviso de usuario: este control le permite editar un aviso de usuario.
  - Control de aceptación: Tras hacer clic en el botón de aceptación, se muestra la página de inicio de sesión. Los estilos del botón y del control se pueden personalizar.
  - Control de registro MDM: solicita al usuario que registre los terminales con un servidor MDM. Los estilos de los botones y controles son personalizables.
- Página de registro
  En una página de registro de usuario, un usuario puede registrar una cuenta para la autenticación.
  - Control de registro de usuario: Se pueden personalizar las etiquetas de los botones, los estilos de control y los marcadores de posición de los cuadros de texto.
  - Si se han configurado parámetros definidos por el usuario para la política de cuenta de invitado en una plantilla de registro automático, puede establecer los campos definidos por el usuario en la página de registro como obligatorios.
- Página de registro exitoso
  - Control de éxito de registro: puede personalizar el estilo de los botones y controles que se utilizan para redirigir a los usuarios a la página de autenticación de usuarios.
  - Control de aprobación basado en escaneo de código QR: puede personalizar el mensaje de texto, así como los estilos del botón y el control para redirigir a los usuarios a las páginas de autenticación.

NOTE

El control de aprobación basado en el escaneo de código QR solo se admite en plantillas de autorregistro comunes.

- Página de cambio de contraseña
  - Control de cambio de contraseña: Se pueden personalizar las etiquetas de los botones, los estilos de control y los marcadores de posición de los cuadros de texto.

NOTE

Sólo se pueden cambiar las contraseñas de las cuentas locales y de las cuentas AD.

- Página de verificación de nombre de usuario y contraseña
  - Control de verificación de nombre de usuario: Se pueden personalizar las etiquetas de los botones, los estilos de control y los marcadores de posición de los cuadros de texto.
- Página de restablecimiento de contraseña
  - Control de restablecimiento de contraseña: las etiquetas de los botones, los estilos de control y los marcadores de posición de los cuadros de texto se pueden personalizar.

NOTE

Sólo se pueden restablecer las contraseñas de las cuentas locales.

- Página del cuestionario
  - Control del cuestionario: Se pueden personalizar las descripciones de las preguntas, los tipos de respuestas, las opciones de respuesta, las etiquetas de los botones y los estilos de control.

NOTE

- Antes de personalizar una página de cuestionario utilizando una plantilla, haga clic junto al nombre de la plantilla y seleccione **Página de cuestionario** en la ventana **Lista de páginas personalizadas** .
- Los administradores pueden ver los registros de cuestionarios en la página de la pestaña **Registros de cuestionarios en Gestión de admisiones > Recurso de admisión > Gestión de invitados > Registros de invitados** .
- Los administradores de inquilinos pueden añadir un control de texto en la página del cuestionario para especificar la naturaleza y las condiciones de uso del mismo. Si se trata de datos personales, deben informar claramente a los usuarios finales sobre la finalidad del cuestionario y el alcance de la recopilación de datos.

REFERENCIAS TECNICAS

INGLES

DHCP

Contents

Collapse All

DHCP/5/DHCPV6_PD
DHCP/5/DHCPV6_PD
DHCP/5/DHCPV6_PD
DHCP/5/GW_RENEW
DHCP/5/RELEASE
DHCP/5/RENEW
DHCP/5/REQIP
DHCP/5/RT_RENEW
DHCP/5/WAITOFFER
DHCP/6/DHCP_BIND
DHCP/6/DHCP_SERV
DHCP/6/DHCPSNP_F
DHCP/6/DHCPSNP_U
DLP Log
DNS Log
DNSF Log
DOPHI Log
DPLM Log
DRIVER Log
EAP Log
ENTEXT Log
ERROR-DOWN Log
EUM Log

DHCP/6/DHCP_SERVER_DETECT

Message

DHCP/6/DHCP_SERVER_DETECT: A new server was found. (IP Address=[ipaddress], MAC Address=[macaddress], Interface=[interface], PeVlan=[pevlan], CeVlan=[cevlan], BdID=[BdID])

Description

A new DHCP server was discovered.

Parameters

Parameter Name	Parameter Meaning
ipaddress	IP address of a server.
macaddress	MAC address of the server.
interface	Name of the interface that receives packets from the new server.
pevlan	Outer VLAN ID.
cevlan	Inner VLAN ID.
BdID	Indicates a BD ID.

Possible Causes

The device receives packets from the new DHCP server.

Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

DHCP

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Contenido

Contraer todo

DHCP/5/DHCPV6_PD

RENOVACIÓN DE CL

DHCP/5/DHCPV6_PD

DHCP/5/GW_RENEW

DHCP/5/LIBERACIÓN

DHCP/5/RENOVE

DHCP/5/REQIP

DHCP/5/RT_RENEW

DHCP/5/TIEMPO DE

DHCP/6/DHCP_BIND

DHCP/6/DETECCIÓN

DHCP/6/LÍMITE DE T

DHCP/6/DHCPSNP_U

Registro DLP

Registro DNS

Registro DNSF

Registro DOPHI

Registro DPLM

Registro del CONDUCTO

Registro EAP

Registro de ENTEXT

Registro de ERROR-DO

DHCP /6/ DETECCIÓN DEL SERVIDOR DHCP

Mensaje

DHCP /6/ DHCP _SERVER_DETECT: Se encontró un nuevo servidor. (Dirección IP=[direcciónIP], Dirección MAC=[direcciónMAC], Interfaz=[interfaz], PeVlan=[pevlan], CeVlan=[cevlan], BdID=[BdID])

Descripción

Se descubrió un nuevo servidor DHCP .

Parámetros

Nombre del parámetro	Significado del parámetro
dirección IP	Dirección IP de un servidor.
dirección macaddress	Dirección MAC del servidor.
interfaz	Nombre de la interfaz que recibe paquetes del nuevo servidor.
pevlan	ID de VLAN externa.
cevlan	ID de VLAN interna.
BdID	Indica un ID de BD.

Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

REFERENCIAS TECNICAS

INGLES

dpd type

Home

dpd type

Function

The **dpd type** command configures the DPD mode on an IKE peer.
The **undo dpd type** command deletes the DPD mode on an IKE peer.
By default, the DPD mode is not configured on an IKE peer.

Format

dpd type { **on-demand** | **periodic** }
undo dpd type

Parameters

Parameter	Description	Value
on-demand	Configures on-demand DPD.	-
periodic	Configures periodic DPD.	-

Views

IKE peer view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario
When peers implement IPSec communication, the heartbeat mechanism can detect peer faults to avoid traffic loss. However, the periodic heartbeat message exchanges consume CPU resources on the two ends. The DPD mechanism enables a device to send DPD messages for peer detection only when the device does not receive IPSec packets from the peer within a period. This mechanism can detect peer faults and save CPU resources.

Home

Two DPD modes are available:

- On-demand DPD
  When the local end needs to send IPSec packets to the remote end, the local end sends a DPD request packet to the remote end for DPD detection.
- Periodic DPD
  If the local end does not receive IPSec packets or a DPD request packet from the remote end after the DPD idle time expires, it periodically sends a DPD request packet to the remote end.

The local end retransmits DPD request packets if it does not receive any DPD response packet from the remote end within the retransmission interval. If the local end still does not receive any DPD response packet within the retransmission interval after the maximum number of retransmissions is reached, the local end considers that the remote end is offline and deletes the involved IKE SA and IPSec SA.

Precautions

The sequence of the payload in DPD packets configured on IKE peers using the **dpd msg** command must be the same. Otherwise, DPD does not take effect.

When multiple branches are connected to the headquarters, you are advised not to set the DPD mode of the headquarters to periodic detection. This is because an IPSec tunnel will frequently flap, causing high CPU usage, if the network is unstable. You are advised to set the DPD mode of the headquarters to on-demand detection or not to configure the DPD mode.

Example

Configure on-demand DPD.

```
<Huawei> system-view
[Huawei] ike peer huawei
[Huawei-ike-peer-huawei] dpd type on-demand
```

Parent Topic: **IPSec Configuration Commands**

Copyright © Huawei Technologies Co., Ltd.

Previous Next topic

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

dpd type

tipo dpd

Función

El comando **de tipo dpd** configura el modo DPD en un par IKE.
El comando **undo dpd type** elimina el modo DPD en un par IKE.
De forma predeterminada, el modo DPD no está configurado en un par IKE.

Formato

tipo dpd { **bajo demanda** | **periódico** }
deshacer tipo dpd

Parámetros

Parámetro	Descripción	Valor
Bajo demanda	Configura DPD bajo demanda.	-
periódico	Configura DPD periódico.	-

Vistas

Vista de pares de IKE

Nivel predeterminado

2: Nivel de configuración

Instrucciones de uso

Escenario de uso
Cuando los pares implementan la comunicación IPSec, el mecanismo de latido puede detectar fallos de par para evitar la pérdida de tráfico. Sin embargo, el intercambio periódico de mensajes de latido consume recursos de CPU en ambos extremos. El mecanismo DPD permite que un dispositivo envíe mensajes DPD para la detección de pares solo cuando no recibe paquetes IPSec

recursos de CPU.

El dispositivo configura el modo DPD y habilita la función DPD según el comando **de tipo dpd** . Hay dos modos DPD disponibles:

- DPD bajo demanda
  Cuando el extremo local necesita enviar paquetes IPSec al extremo remoto, el extremo local envía un paquete de solicitud DPD al extremo remoto para la detección de DPD.
- DPD periódico
  Si el extremo local no recibe paquetes IPSec o un paquete de solicitud DPD del extremo remoto una vez que expira el tiempo de inactividad de DPD, envía periódicamente un paquete de solicitud DPD al extremo remoto.

El extremo local retransmite los paquetes de solicitud DPD si no recibe ningún paquete de respuesta DPD del extremo remoto dentro del intervalo de retransmisión. Si, una vez alcanzado el número máximo de retransmisiones, el extremo local sigue sin recibir ningún paquete de respuesta DPD dentro del intervalo de retransmisión, considera que el extremo remoto está desconectado y elimina las SA IKE e IPSec involucradas.

Precauciones

La secuencia de la carga útil en los paquetes DPD configurados en pares IKE mediante el comando **dpd msg** debe ser la misma. De lo contrario, el DPD no se aplica.

Cuando varias sucursales estén conectadas a la sede central, se recomienda no configurar el modo DPD de la sede central en detección periódica. Esto se debe a que, si la red es inestable, un túnel IPSec puede presentar fluctuaciones frecuentes, lo que provoca un alto consumo de CPU. Se recomienda configurar el modo DPD de la sede central en detección bajo demanda o no configurarlo.

Ejemplo

Configurar DPD bajo demanda.

```
< Huawei > vista del sistema
[ Huawei ] ike peer huawei
[ Huawei -ike-peer-huawei] tipo dpd a pedido
```

Tema principal: **Comandos de configuración de IPSec**

Tema **Siguiente**

Derechos de autor © Huawei Technologies Co., Ltd.

REFERENCIAS TECNICAS

INGLES

DSCP

Creating a Customized Application

Context

iMaster NCE-Campus can identify common applications using the built-in application signature database. When predefined applications cannot meet your requirements, you can customize a new application according to its characteristics.
Currently, the following types of customized applications are supported: **SA**, **Domain Name**, and **Advance Rule**. Table 1 lists the methods of identifying customized applications of each type.

Table 1 Methods of identifying a customized application

Customized Application Type	Application Identification Method
SA	Rules can be created through 3-tuple information, keywords, or both 3-tuple information and keywords. The 3-tuple information consists of the server address, protocol type, and port number. The keyword is the feature of the data packet or data flow of the corresponding application. The keyword uniquely identifies the application. If you create a customized application rule based on the 3-tuple information, the rule must contain at least one IP address or port number.
Domain Name	FPI through association with the DNS function: Rules are created by specifying DNS domain names. If users access applications using domain names, you can configure DNS domain name rules to identify these application packets. For devices running V300, this function applies only to UDP packets, DNS packets cannot be truncated (**Truncated** cannot be set to **1**), and a maximum of 10 IP addresses can be resolved in a packet.
Advance Rule	FPI based on advanced ACL rules: Rules are created based on 5-tuple and DSCP information. The 5-tuple information includes the protocol type, source IP address, destination IP address, source port number, and destination port number of a packet. If you know the 5-tuple and DSCP information of service packets, you can configure rules based on 5-tuple and DSCP information to identify these packets. When you use this method to configure a customized application rule, at least one of the source IP address, destination IP address, source port, destination port, and DSCP information must be configured.

For different models of ARs, refer to Table 2 to view the application specifications of the SA type and refer to Table 4 and Table 5 to view application specifications of the FPI types (**Domain Name** and **Advance Rule**).
For different models of firewall gateways, refer to Table 3 to view the application specifications of the SA type and refer to Table 6 to view the application specifications of the **Advance Rule** type.

NOTE

The following tables describe the maximum specifications supported by the controller for applications of different types, and list device models whose application specifications are lower than the maximum specifications supported by the controller. If application specifications of a device model exceed those supported by the controller, the specifications supported by the controller take effect.

Table 2 SA application specifications

Device Model	Maximum Number of Customized Applications	Maximum Number of Rules for a Single Application	Maximum Number of Rules
Device models are not distinguished.	256	8	512

Table 3 SA specifications (firewall gateway)

Device Type	Maximum Number of Customized Applications	Maximum Number of Rules for a Single Application	Maximum Number of Rules
USG6510F-DK, USG6510F-DL, USG6000F-E06-DL, USG6510F-DPL, USG6530F-D, USG6000F-E12-D, USG6530F-DL, USG6560F-D, USG6530F-DPL, USG6510F-D, USG6000F-E06-D	128	8	256
Other models	256	8	512

Table 4 Specifications for applications of the **Domain Name** type

Device Model	Maximum Number of Customized Applications	Maximum Number of Rules for a Single Application	Maximum Number of Rules
AR611, AR611-S, AR611W, AR611W-S, AR611W-LTE4CN, AR611W-LTE6EA	128	128	128
AR617, AR617-LTE4EA, AR617VW, AR617VW-LTE4, AR617VW-LTE4EA			
AR631I-LTE4EA, AR631I-LTE4CN			
AR651C and AR651F-Lite			
Other models	256		256

Table 5 Application specifications of the **Advance Rule** type (AR)

Device Model	Maximum Number of Customized Applications	Maximum Number of Rules for a Single Application	Maximum Number of Rules
AR611, AR611-LTE4EA, AR611-S AR611W, AR611W-S, AR611W-LTE4CN, AR611W-LTE6EA	128	8	256
AR617, AR617-LTE4EA, AR617VW,			

Device Model	Maximum Number of Customized Applications	Maximum Number of Rules for a Single Application	Maximum Number of Rules
AR617VW-LTE4, AR617VW-LTE4EA			
AR631I-LTE4EA, AR631I-LTE4CN			
AR651C and AR651F-Lite			
AR6280/AR6300 series	Common application: 256 Extended application: 1792	Common application: 8 Extended application: 1024	Common application: 1024 Extended application: 15360
Other models	256	8	1024

Table 6 Application specifications of the **Advance Rule** type (firewall gateway)

Device Type	Maximum Number of Customized Applications	Maximum Number of Rules for a Single Application	Maximum Number of Rules
USG6510F-DK, USG6510F-DL, USG6000F-E06-DL, USG6510F-DPL, USG6530F-D, USG6000F-E12-D, USG6530F-DL, USG6560F-D, USG6530F-DPL, USG6510F-D, USG6000F-E06-D	128	8	256
USG6520F-K, USG6525F, USG6555F, USG6560F-K, USG6565F, USG6585F, USG6590F-K, USG6585F-B	256	8	512
USG6600F series, USG6700F series	256	8	1024

Table 7 lists the specifications of customized applications supported by iMaster NCE-Campus.

Table 7 Specifications of customized applications

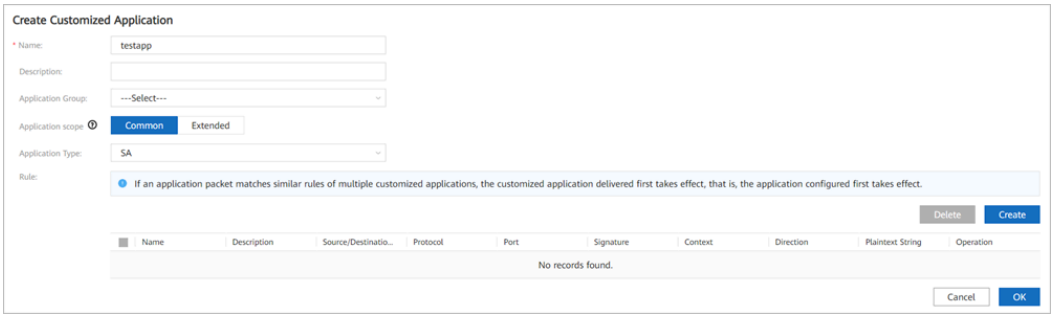
Application Type	Maximum Number of Customized Applications	Maximum Number of Rules for a Single Application	Maximum Number of Rules
SA	256	8	512
Domain Name	256 (total number of applications of the **Domain Name** and **Advance Rule** types)	128	256
Advance Rule (for common applications)		8	1024
Advance Rule (for extended applications)	1792	1024	15360

NOTE

- The port number range in a rule that defines a customized application of the **Advance Rule** type is saved on devices as multiple segments, each of which occupies an ACL resource. In this case, the number of rules that can be configured to define customized applications of the **Advance Rule** type are smaller than the specifications listed in the preceding table.
- The application signature database does not include applications of enterprises' self-built servers, such as Outlook and Office365 deployed on enterprise self-built servers, as predefined applications. If such applications need to be identified, customized applications need to be configured.

Procedure

1. Choose **Network Configuration** > **Global Settings** > **Template Management** from the main menu and expand **Policy** in the navigation pane.
2. Click the **WAN Customized Application** tab.
3. Click **Create** to create a customized application.



4. Set **Name** to a customized application name.
5. (Optional) Select an application group to which the customized application needs to be added, or add an application to an application group after customizing it. For details about related operations of application groups, see Creating an Application Group.
6. Select the application scope of the customized application. The application scopes include **Common** and **Extended**. **Extended** is applicable to the scenario where the specifications of applications of the **Advance Rule** type need to be expanded. Currently, only AR6280 and AR6300 series devices support this function. If **Common** is selected, the created customized application is delivered to all devices. If **Extended** is selected, the application is delivered only to AR6280 and AR6300 series devices.
7. Select an application type to define different rules. There are three application types: **SA**, **Domain Name**, and **Advance Rule**. If **Application scope** is set to **Extended**, you can only create customized applications of the **Advance Rule** type.

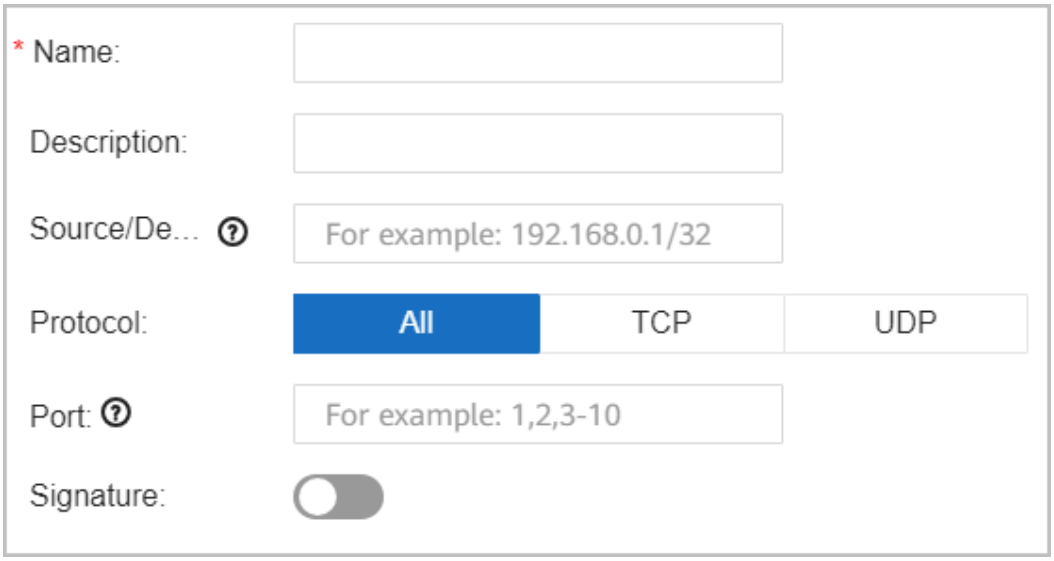
> **NOTE**
>
> Configuring extended configurations at sites where AR6280 or AR6300 series devices are deployed has the following restrictions:
>
> - If extended applications have been configured, the number of deployed sites that contain AR6280 or AR6300 series devices cannot exceed 200.
> - If the number of deployed sites that contain AR6280 or AR6300 series devices exceeds 200, no extended applications can be created.

8. Configure rules for the customized application.

> **NOTE**
>
> - The network segments configured for different customized applications cannot overlap.
> - For traffic that matches rules of both a customized application and a predefined application, devices preferentially match the traffic with the rule of the

customized application.

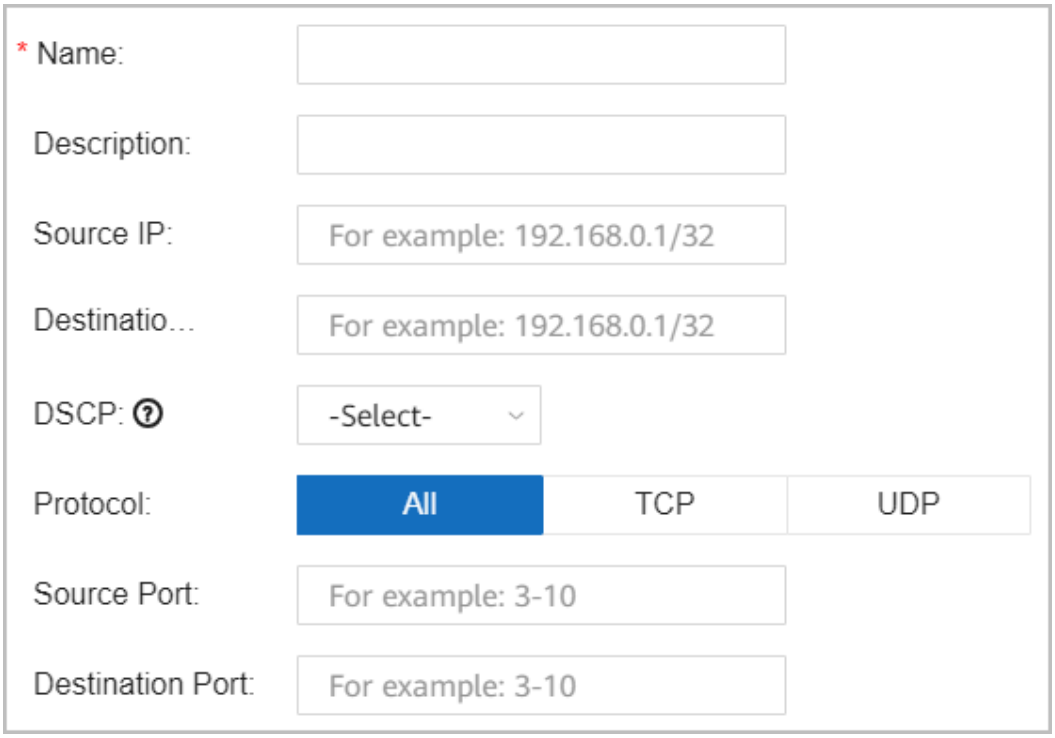
- Set **Application Type** to **SA**, click **Create**, create an SA application rule, and click **OK**.
  The AR6700V-L supports this function starting from V600R023C10.



- Set **Application Type** to **Domain Name**, click **Create**, create a rule for applications of the selected type, and click **OK**.
  Customized applications of the **Domain Name** type are supported by devices running V600 since V600R023C00, and supported by AR6700V-L devices since V600R023C10.



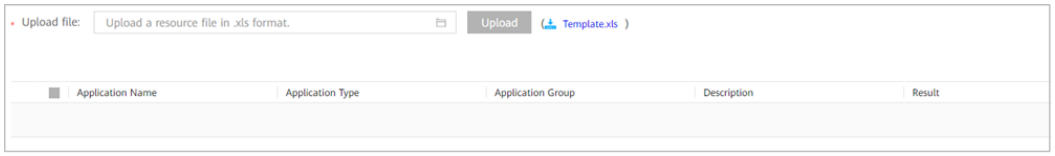
- Set **Application Type** to **Advance Rule**, click **Create**, create a rule for applications of the selected type, and click **OK**.
  Customized applications of the **Advance Rule** type are supported by devices running V600 since V600R022C00 and are supported by AR6700V-L devices since V600R023C10.



9. Click **OK**. The customized application is configured.
   After a customized application is created, iMaster NCE-Campus delivers the customized application rule to its managed devices. If multiple customized applications are created, the corresponding rules are delivered based on their configuration sequence. That is, the rule of a customized application that is configured first is delivered first to devices. If an application packet matches rules of multiple customized applications, the rule of the customized application that is delivered first takes effect. Once devices find the matching application for traffic, they stop matching the traffic with other applications.
   For example, application traffic traffic1 matches rules of both the customized applications APP1 and APP2. If the rule of APP1 is delivered to a device earlier than that of APP2, the device preferentially matches traffic1 with APP1 and does not continue to match the traffic with APP2.

Related Operations

- Import customized applications in batches.
  On the **Customized Application** tab page, click **Import**. Download the template for importing customized applications, set parameters about the applications to be imported, and upload the template.



Follow-up Procedure

Table 8 Follow-up procedure of customized applications

Function	Operation Scenario and Constraint	Procedure
Viewing details about a customized application	You can view detailed information about a customized application.	1. On the **Customized Application** tab page, click in the row where you want to view details about a customized application. 2. In the expanded area, view details about the customized application.
Modifying a customized application	You cannot modify **Application Name** of a customized application that has been referenced by an application group.	1. On the **Customized Application** tab page, click in the **Operation** column of the customized application to be modified. 2. On the page that is displayed, modify the customized application. You cannot change the application scope (**Common** or **Extended**) when modifying a customized application. 3. Click **OK**.
Cloning a customized application	You can quickly create a customized application by simply modifying an existing customized application.	1. On the **Customized Application** tab page, click in the **Operation** column of the customized application to be cloned. 2. Modify the cloned customized application. 3. Click **OK**.
Deleting a customized application	You cannot delete a customized application that has been referenced by an application group.	1. On the **Customized Application** tab page, click in the **Operation** column of the customized application to be deleted. 2. Click **Yes**.

Parameter Description

Table 9 Parameters on the **Customized Application** page

Parameter			Description	Data Plan Required or Not
Name			Name of a customized application. The value can contain only digits, letters, and underscores (_). The name of a customized application of the SA type can contain 1 to 29 characters, and that of a customized application of a non-SA type can contain 1 to 28 characters.	Y
Description			Description of a customized application's function.	-
Application Group			Application group to which the application is to be added. It must be an existing application group. You can also add an application to an application group after customizing it.	Y
Application scope			The value can be **Common** or **Extended**. **Extended** is applicable to the scenario where the specifications of applications of the **Advance Rule** type need to be expanded. Currently, only AR6280 and AR6300 series devices support this function.	Y
Application Type			You can select an application type to define a rule for identifying application packets. The application types include **SA**, **Domain Name**, and **Advance Rule**. The configurable rule parameters vary according to the application type. If **Application scope** is set to **Extended**, you can only create customized applications of the **Advance Rule** type.	Y
Rule	Name		Name of a rule defined for identifying application packets. A rule contains the protocol number and port number used by an application, and other basic attributes.	Y
	Description		Description of a rule.	-
	When **Application**	IP/Port	IP address and port number of application packets matching the rule. The system does not distinguish source and destination IP addresses of SA application packets, as well as source and destination port	Y

Parameter			Description	Data Plan Required or Not
	Type is set to **SA**		numbers. If an IP address and a port number are specified together in a rule, the relationship between **IP** and **Port** is **And**, that is, application packets only with the specified IP address and port number match this rule. For details about the value ranges of the IP address and port number, see the prompt message on the web UI. **NOTE:** When configuring a rule for V600 devices, you need to set this parameter to the destination IP address and destination port number of application packets. Otherwise, application packets cannot be matched.	
		Protocol	Transport layer protocol of a customized application rule. The options include **All**, **TCP**, and **UDP**.	Y
		Signature	Signature	Signature information. Data packets of some applications contain the same character string, which is regarded as a signature.	-
			Context	You can select the packet- or flow-based mode for signature identification: In the packet-based mode, the system checks every packet of applications. In flow-based mode, the system only checks the first packet in the application data flow and does not check the subsequent packets if the system detects that the subsequent packets belong to the same data flow based on the 5-tuple information.	-
			Direction	Direction of packets to be identified. You can configure a rule to identify the signatures only in request or response packets, or in both of them.	-

Parameter				Description	Data Plan Required or Not
			Plain-text String	Signature string, which is case-sensitive.	-
	When **Application Type** is set to **Domain Name**	Domain Name		Domain name of a customized application.	Y
	When **Application Type** is set to **Advance Rule**	Source IP/Source Port		Source IP address and port number of application packets matching the rule. If the source IP address and source port number are specified together in a rule, the relationship between **Source IP** and **Source Port** is **And**, that is, application packets only with the specified source IP address and source port number match this rule. For details about the value ranges of the IP address and port number, see the prompt message on the web UI.	Y
		Destination IP/Destination Port		Destination IP address and destination port number of application packets matching the rule. If the destination IP address and destination port number are specified together in a rule, the relationship between **Destination IP** and **Destination Port** is **And**, that is, application packets only with the specified destination IP address and destination port number match this rule. In most cases, the IP address of an application server is a fixed public IP address. This allows the system to identify application packets based on the destination IP address.	Y

Parameter			Description	Data Plan Required or Not
		DSCP	You can set the packet priority by specifying a DSCP value. The options include **Default** (which is 0), **CS** (low priority), **AF** (medium priority), **EF** (high priority), and **User Defined**. V600 devices do not support this function.	Y
		Protocol	Transport layer protocol of a customized application rule. The options include **All**, **TCP**, and **UDP**.	Y

Parent Topic: **Configuring Applications and Application Groups**

Copyright © Huawei Technologies Co., Ltd.

Previous Next topic

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

DSCP

Creación de una aplicación personalizada

Contexto

iMaster NCE-Campus puede identificar aplicaciones comunes mediante la base de datos de firmas de aplicaciones integrada. Si las aplicaciones predefinidas no cumplen con sus requisitos, puede personalizar una nueva aplicación según sus características.
Actualmente, se admiten los siguientes tipos de aplicaciones personalizadas: **SA** , **Nombre de dominio** y **Regla avanzada** . La Tabla 1 enumera los métodos para identificar aplicaciones personalizadas de cada tipo.

Tabla 1 Métodos para identificar una aplicación personalizada

Tipo de aplicación personalizada	**Método de identificación de la aplicación**
SA	Las reglas se pueden crear mediante información de 3-tuplas, palabras clave o ambas. La información de 3-tuplas consta de la dirección del servidor, el tipo de protocolo y el número de puerto. La palabra clave es la característica del paquete o flujo de datos de la aplicación correspondiente. La palabra clave identifica de forma única la aplicación. Si crea una regla de aplicación personalizada basada en la información de 3 tuplas, la regla debe contener al menos una dirección IP o un número de puerto.
Nombre de dominio	FPI mediante la asociación con la función DNS: Las reglas se crean especificando nombres de dominio DNS. Si los usuarios acceden a aplicaciones mediante nombres de dominio, puede configurar reglas de nombres de dominio DNS para identificar estos paquetes de aplicación. En dispositivos con V300, esta función solo se aplica a paquetes UDP; los paquetes DNS no se pueden truncar (el valor de **"Truncated"** no se puede establecer en **1**) y se puede resolver un máximo de 10 direcciones IP en un paquete.
Regla anticipada	FPI basado en reglas ACL avanzadas: Las reglas se crean a partir de información de 5-tuplas y DSCP. Esta información incluye el tipo de protocolo, la dirección IP de origen, la dirección IP de destino, el número de puerto de origen y el número de puerto de destino de un paquete. Si conoce la información de 5-tuplas y DSCP de los paquetes de servicio, puede configurar reglas basadas en dicha información para identificarlos. Al utilizar este método para configurar una regla de aplicación personalizada, se debe configurar al menos la dirección IP de

Tipo de aplicación personalizada	Método de identificación de la aplicación
	origen, la dirección IP de destino, el puerto de origen, el puerto de destino y la información DSCP.

Para conocer los diferentes modelos de AR, consulte la Tabla 2 para ver las especificaciones de aplicación del tipo SA y consulte la Tabla 4 y la Tabla 5 para ver las especificaciones de aplicación de los tipos de FPI (**nombre de dominio** y **regla avanzada**).
Para conocer los diferentes modelos de puertas de enlace de firewall, consulte la Tabla 3 para ver las especificaciones de la aplicación del tipo SA y consulte la Tabla 6 para ver las especificaciones de la aplicación del tipo **de regla avanzada** .

NOTE

Las siguientes tablas describen las especificaciones máximas admitidas por el controlador para diferentes tipos de aplicaciones y enumeran los modelos de dispositivo cuyas especificaciones de aplicación son inferiores a las admitidas por el controlador. Si las especificaciones de aplicación de un modelo de dispositivo superan las admitidas por el controlador, se aplicarán las especificaciones admitidas por este .

Tabla 2 Especificaciones de la aplicación SA

Modelo del dispositivo	Número máximo de aplicaciones personalizadas	Número máximo de reglas para una sola aplicación	Número máximo de reglas
Los modelos de dispositivos no se distinguen.	256	8	512

Tabla 3 Especificaciones de SA (puerta de enlace de firewall)

Tipo de dispositivo	Número máximo de aplicaciones personalizadas	Número máximo de reglas para una sola aplicación	Número máximo de reglas

Tipo de dispositivo	Número máximo de aplicaciones personalizadas	Número máximo de reglas para una sola aplicación	Número máximo de reglas
USG6510F-DK, USG6510F-DL, USG6000F-E06-DL, USG6510F-DPL, USG6530F-D, USG6000F-E12-D, USG6530F-DL, USG6560F-D, USG6530F-DPL, USG6510F-D, USG6000F-E06-D	128	8	256
Otros modelos	256	8	512

Tabla 4 Especificaciones para aplicaciones del tipo **Nombre de Dominio**

Modelo del dispositivo	Número máximo de aplicaciones personalizadas	Número máximo de reglas para una sola aplicación	Número máximo de reglas
AR611, AR611-S, AR611W, AR611W-S, AR611W-LTE4CN, AR611W-LTE6EA	128	128	128
AR617, AR617-LTE4EA, AR617VW, AR617VW-LTE4, AR617VW-LTE4EA			
AR631I-LTE4EA, AR631I-LTE4CN			
AR651C y AR651F-Lite			
Otros modelos	256		256

Tabla 5 Especificaciones de la aplicación del tipo **Regla Avanzada** (RA)

Modelo del dispositivo	**Número máximo de aplicaciones personalizadas**	**Número máximo de reglas para una sola aplicación**	**Número máximo de reglas**
AR611, AR611-LTE4EA, AR611-S AR611W, AR611W-S, AR611W-LTE4CN, AR611W-LTE6EA	128	8	256
AR617, AR617-LTE4EA, AR617VW, AR617VW-LTE4, AR617VW-LTE4EA			
AR631I-LTE4EA, AR631I-LTE4CN			
AR651C y AR651F-Lite			
Serie AR6280/AR6300	Aplicación común: 256 Aplicación extendida: 1792	Aplicación común: 8 Aplicación extendida: 1024	Aplicación común: 1024 Aplicación extendida: 15360
Otros modelos	256	8	1024

Tabla 6 Especificaciones de la aplicación del tipo **Regla avanzada** (puerta de enlace de firewall)

Tipo de dispositivo	**Número máximo de aplicaciones personalizadas**	**Número máximo de reglas para una sola aplicación**	**Número máximo de reglas**
USG6510F-DK, USG6510F-DL, USG6000F-E06-DL, USG6510F-DPL, USG6530F-D, USG6000F-E12-D, USG6530F-DL, USG6560F-D,	128	8	256

Tipo de dispositivo	Número máximo de aplicaciones personalizadas	Número máximo de reglas para una sola aplicación	Número máximo de reglas
USG6530F-DPL, USG6510F-D, USG6000F-E06-D			
USG6520F-K, USG6525F, USG6555F, USG6560F-K, USG6565F, USG6585F, USG6590F-K, USG6585F-B	256	8	512
Serie USG6600F, serie USG6700F	256	8	1024

En la Tabla 7 se enumeran las especificaciones de las aplicaciones personalizadas compatibles con iMaster NCE-Campus .

Tabla 7 Especificaciones de aplicaciones personalizadas

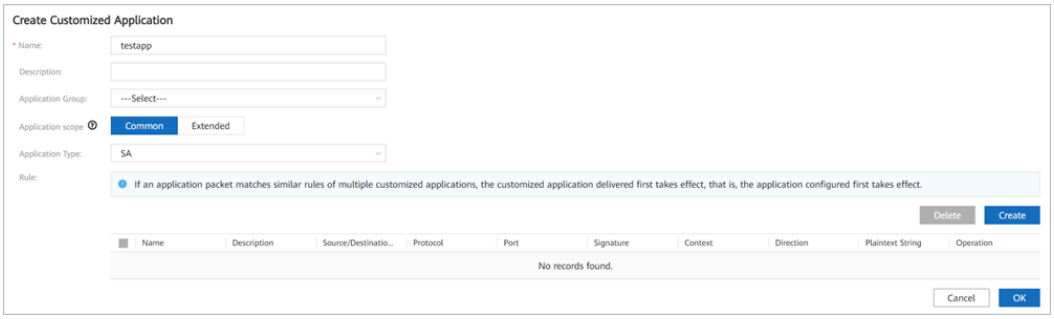
Tipo de aplicación	Número máximo de aplicaciones personalizadas	Número máximo de reglas para una sola aplicación	Número máximo de reglas
SA	256	8	512
Nombre de dominio	256 (número total de solicitudes de los tipos **Nombre de Dominio** y **Regla Avanzada**)	128	256
Regla anticipada (para aplicaciones comunes)		8	1024
Regla anticipada (para aplicaciones extendidas)	1792	1024	15360

NOTE

- El rango de números de puerto de una regla que define una aplicación personalizada de tipo **Regla Avanzada** se guarda en los dispositivos como varios segmentos, cada uno de los cuales ocupa un recurso de ACL. En este caso, el número de reglas que se pueden configurar para definir aplicaciones personalizadas de tipo **Regla Avanzada** es menor que las especificaciones de la tabla anterior.
- La base de datos de firmas de aplicaciones no incluye las aplicaciones de servidores de desarrollo propio de las empresas, como Outlook y Office 365 implementados en servidores de desarrollo propio de la empresa, como aplicaciones predefinidas. Si es necesario identificar dichas aplicaciones, se deben configurar aplicaciones personalizadas.

Procedimiento

1. Seleccione **Configuración de red** > **Configuración global** > **Administración de plantillas** en el menú principal y expanda **Política** en el panel de navegación.
2. Haga clic en la pestaña **Aplicación personalizada WAN** .
3. Haga clic en **Crear** para crear una aplicación personalizada.



4. Establezca **Nombre** en un nombre de aplicación personalizado.
5. (Opcional) Seleccione el grupo de aplicaciones al que desea añadir la aplicación personalizada, o añada una aplicación a un grupo de aplicaciones después de personalizarla. Para obtener más información sobre las operaciones relacionadas con los grupos de aplicaciones, consulte " Crear un grupo de aplicaciones" .
6. Seleccione el ámbito de aplicación de la aplicación personalizada. Los ámbitos de aplicación incluyen **Común** y **Extendido** . **Extendido** es aplicable cuando es necesario ampliar las especificaciones de las aplicaciones de tipo **Regla Avanzada** . Actualmente, solo los dispositivos de las series AR6280 y AR6300 admiten esta función. Si se selecciona **Común , la aplicación personalizada creada se distribuye a todos los dispositivos. Si se selecciona Extendido** , la aplicación se distribuye solo a los dispositivos de las series AR6280 y AR6300.
7. Seleccione un tipo de aplicación para definir diferentes reglas. Hay tres tipos de aplicación: **SA** , **Nombre de dominio** y **Regla avanzada** . Si **el ámbito de la aplicación** se establece en **Extendido** , solo podrá crear aplicaciones personalizadas del tipo **Regla avanzada** .

NOTE

La configuración de configuraciones extendidas en sitios donde se implementan dispositivos de la serie AR6280 o AR6300 tiene las siguientes restricciones:

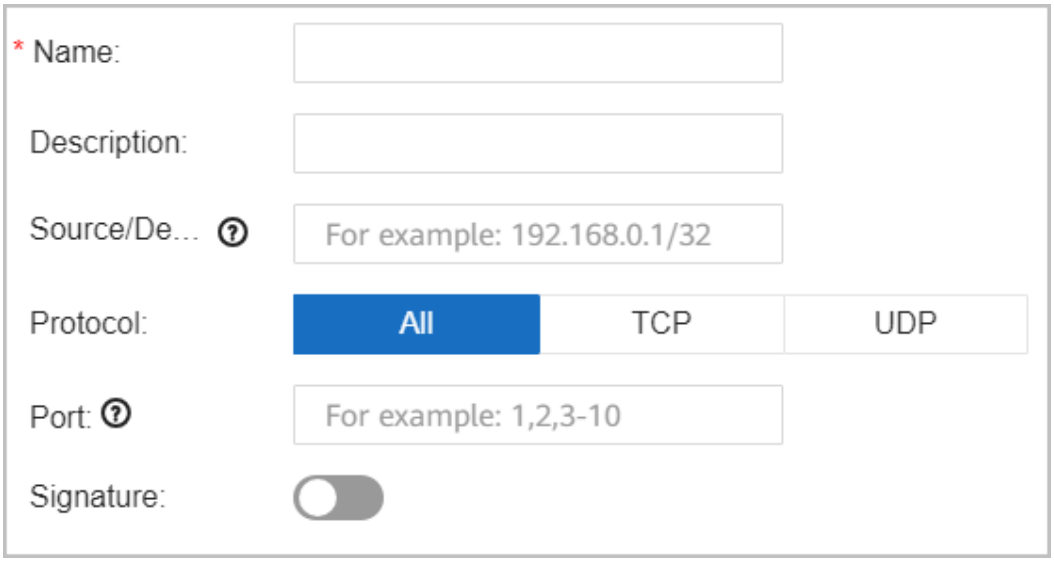
- Si se han configurado aplicaciones extendidas, la cantidad de sitios implementados que contienen dispositivos de la serie AR6280 o AR6300 no puede superar los 200.
- Si la cantidad de sitios implementados que contienen dispositivos de la serie AR6280 o AR6300 supera los 200, no se podrán crear aplicaciones extendidas.

8. Configurar reglas para la aplicación personalizada.

NOTE

- Los segmentos de red configurados para diferentes aplicaciones personalizadas no pueden superponerse.
- Para el tráfico que coincide con las reglas de una aplicación personalizada y de una aplicación predefinida, los dispositivos preferentemente hacen coincidir el tráfico con la regla de la aplicación personalizada.

- Establezca **el Tipo de aplicación** en **SA** , haga clic **en Crear** , cree una regla de aplicación SA y haga clic en **Aceptar** .
  El AR6700V-L admite esta función a partir de V600R023C10.

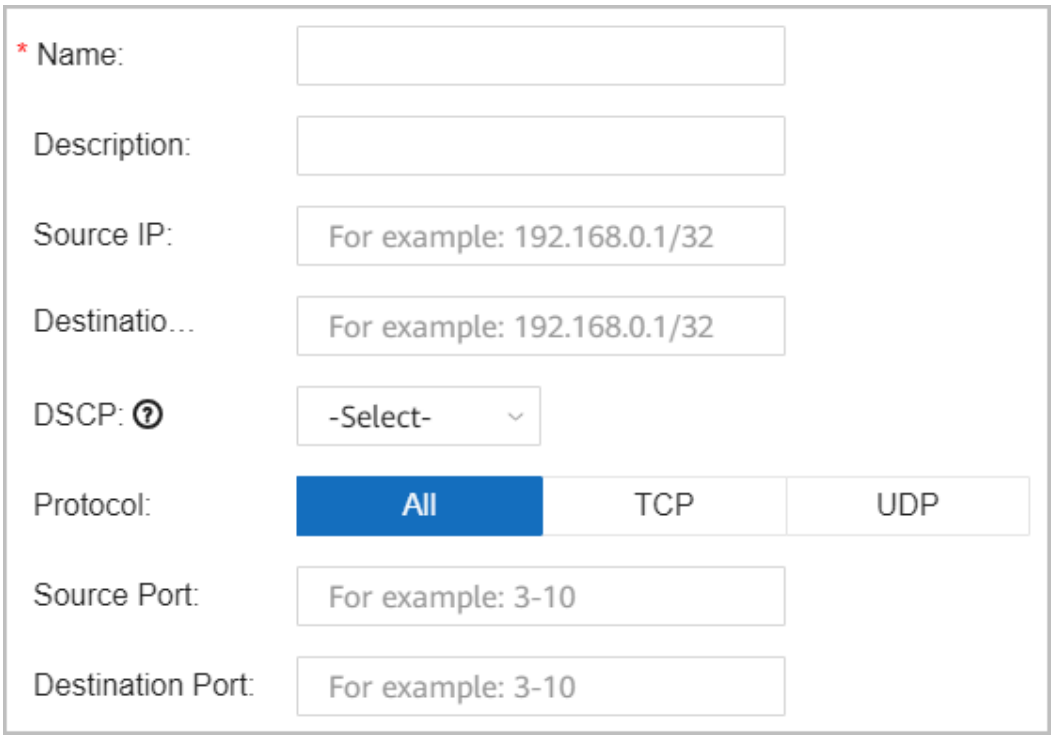


- Establezca **el Tipo de aplicación** en **Nombre de dominio** , haga clic **en Crear** , cree una regla para las aplicaciones del tipo seleccionado y haga clic en **Aceptar** .

Las aplicaciones personalizadas del tipo **Nombre de dominio** son compatibles con dispositivos que ejecutan V600 desde V600R023C00, y con dispositivos AR6700V-L desde V600R023C10.



- Establezca **el Tipo de aplicación** en **Regla avanzada** , haga clic **en Crear** , cree una regla para las aplicaciones del tipo seleccionado y haga clic en **Aceptar** .
  Las aplicaciones personalizadas del tipo **Regla avanzada** son compatibles con dispositivos que ejecutan V600 desde V600R022C00 y son compatibles con dispositivos AR6700V-L desde V600R023C10.

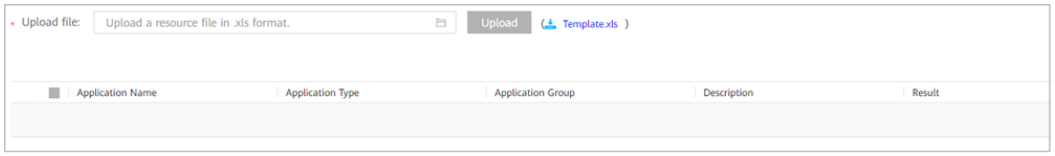


9. Haga clic en **Aceptar** . La aplicación personalizada está configurada.
   Tras crear una aplicación personalizada, iMaster NCE-Campus envía la regla a sus dispositivos administrados. Si se crean varias aplicaciones personalizadas, las reglas correspondientes se envían según su secuencia de configuración. Es decir, la regla de la aplicación personalizada que se configura primero se envía primero a los dispositivos. Si un paquete de aplicación coincide con las reglas de varias aplicaciones personalizadas, se aplica la regla de la aplicación personalizada que se envía primero. Una vez que los dispositivos encuentran la aplicación que coincide con el tráfico, dejan de enviar el tráfico a otras aplicaciones.
   Por ejemplo, el tráfico de la aplicación «traffic1» coincide con las reglas de las aplicaciones personalizadas «APP1» y «APP2». Si la regla de «APP1» se entrega a un dispositivo antes que

la de «APP2», este último prioriza la coincidencia de «traffic1» con «APP1» y deja de hacerlo con «APP2».

Operaciones relacionadas

- Importar aplicaciones personalizadas en lotes.
  En la pestaña **Aplicación personalizada , haga clic en Importar** . Descargue la plantilla para importar aplicaciones personalizadas, configure los parámetros de las aplicaciones que se importarán y cargue la plantilla.



Procedimiento de seguimiento

Tabla 8 Procedimiento de seguimiento de solicitudes personalizadas

Función	Escenario de operación y restricción	Procedimiento
Ver detalles sobre una aplicación personalizada	Puede ver información detallada sobre una aplicación personalizada.	1. En la página de la pestaña **Aplicación personalizada** , haga clic en la fila donde desea ver detalles sobre una aplicación personalizada. 2. En el área expandida, vea detalles sobre la aplicación personalizada.
Modificar una aplicación personalizada	No se puede modificar **el nombre de la aplicación** de una aplicación personalizada que haya sido referenciada por un grupo de aplicaciones.	1. En la página de la pestaña **Aplicación personalizada** , haga clic en la columna **Operación** de la aplicación personalizada que desea modificar. 2. En la página que se muestra, modifique la aplicación personalizada. No se puede cambiar el alcance de la aplicación (**Común** o **Extendido**) al modificar una aplicación personalizada. 3. Haga clic en **Aceptar** .
Clonación de una aplicación	Puede crear rápidamente una aplicación	1. En la página de la pestaña **Aplicación personalizada** , haga clic en la columna **Operación** de la aplicación

Función	Escenario de operación y restricción	Procedimiento
personalizada	personalizada simplemente modificando una aplicación personalizada existente.	personalizada que se clonará. 2. Modificar la aplicación personalizada clonada. 3. Haga clic en **Aceptar** .
Eliminar una aplicación personalizada	No se puede eliminar una aplicación personalizada a la que haya hecho referencia un grupo de aplicaciones.	1. En la página de la pestaña **Aplicación personalizada** , haga clic en la columna **Operación** de la aplicación personalizada que desea eliminar. 2. Haga clic **en Sí** .

Descripción del parámetro

Tabla 9 Parámetros en la página **de Aplicación personalizada**

Parámetro	Descripción	¿Se requiere o no un plan de datos?
Nombre	Nombre de una aplicación personalizada. El valor solo puede contener dígitos, letras y guiones bajos (_). El nombre de una aplicación personalizada del tipo SA puede contener de 1 a 29 caracteres, y el de una aplicación personalizada de un tipo no SA puede contener de 1 a 28 caracteres.	Y

Descripción			Descripción de la función de una aplicación personalizada.	-
Grupo de aplicaciones			Grupo de aplicaciones al que se añadirá la aplicación. Debe ser un grupo existente. También puede añadir una aplicación a un grupo de aplicaciones después de personalizarlo.	Y
Ámbito de aplicación			El valor puede ser **Común** o **Extendido** . **Extendido** es aplicable cuando es necesario ampliar las especificaciones de las aplicaciones de tipo **Regla Avanzada . Actualmente, solo los dispositivos de las series AR6280 y AR6300 admiten esta función.**	Y
Tipo de aplicación			Puede seleccionar un tipo de aplicación para definir una regla que identifique los paquetes de la aplicación. Los tipos de aplicación incluyen **SA** , **Nombre de dominio** y **Regla avanzada** . Los parámetros de regla configurables varían según el tipo de aplicación. Si **el ámbito de la aplicación** se establece en **Extendido** , solo podrá crear aplicaciones personalizadas del tipo **Regla avanzada** .	Y
Regla	Nombre		Nombre de una regla definida para identificar paquetes de aplicación. Una regla contiene el número de protocolo y el número de puerto utilizados por una aplicación, así como otros atributos básicos.	Y
	Descripción		Descripción de una regla.	-
	Cuando **el tipo de aplicación** se establece en **SA**	IP/Puerto	Dirección IP y número de puerto de los paquetes de aplicación que coinciden con la regla. El sistema no distingue entre las direcciones IP de origen y destino de los paquetes de aplicación de SA, ni entre los números de puerto de origen y destino. Si se especifican una dirección IP y un número de puerto juntos en una regla, la relación entre **IP** y **Puerto** es **"Y"** , es decir, solo los paquetes de aplicación con la dirección IP y el número de puerto especificados coinciden con esta regla. Para obtener más información sobre los rangos de valores de la dirección IP y el número de puerto, consulte el mensaje de solicitud en la interfaz web. **NOTA:** Al configurar una regla para dispositivos V600 , debe configurar este parámetro con la dirección IP y el número de puerto de destino de los paquetes de la aplicación. De lo	Y

			contrario, no se podrán vincular los paquetes de la aplicación.	
		Protocolo	Protocolo de capa de transporte de una regla de aplicación personalizada. Las opciones incluyen **All** , **TCP** y **UDP** .	Y
		Firma — Firma	Información de firma. Los paquetes de datos de algunas aplicaciones contienen la misma cadena de caracteres, que se considera una firma.	-
		Firma — Contexto	Puede seleccionar el modo basado en paquetes o flujo para la identificación de firma: En el modo basado en paquetes, el sistema verifica cada paquete de las aplicaciones. En el modo basado en flujo, el sistema solo verifica el primer paquete del flujo de datos de la aplicación y no verifica los paquetes subsiguientes si, según la información de la quintupla, detecta que pertenecen al mismo flujo de datos.	-
		Firma — Dirección	Dirección de los paquetes a identificar. Puede configurar una regla para identificar las firmas solo en los paquetes de solicitud o respuesta, o en ambos.	-
		Firma — Cadena de texto sin formato	Cadena de firma que distingue entre mayúsculas y minúsculas.	-
	Cuando **el tipo de aplicación** se establece en **Nombre de**	Nombre de dominio	Nombre de dominio de una aplicación personalizada.	Y

dominio			
Cuando **el tipo de aplicación** se establece en **Regla avanzada**	IP de origen/ Puerto de origen	Dirección IP de origen y número de puerto de los paquetes de la aplicación que coinciden con la regla. Si la dirección IP de origen y el número de puerto de origen se especifican juntos en una regla, la relación entre **la IP de origen** y **el puerto de origen** es **"Y"** , es decir, solo los paquetes de la aplicación con la dirección IP de origen y el número de puerto de origen especificados coinciden con esta regla. Para obtener más información sobre los rangos de valores de la dirección IP y el número de puerto, consulte el mensaje de solicitud en la interfaz web.	Y
	IP de destino/ Puerto de destino	Dirección IP de destino y número de puerto de destino de los paquetes de aplicación que coinciden con la regla. Si la dirección IP de destino y el número de puerto de destino se especifican juntos en una regla, la relación entre **la IP de destino** y **el puerto de destino** es " **Y"** , es decir, solo los paquetes de aplicación con la dirección IP de destino y el número de puerto de destino especificados coinciden con esta regla. En la mayoría de los casos, la dirección IP de un servidor de aplicaciones es una dirección IP pública fija. Esto permite al sistema identificar los paquetes de la aplicación según la dirección IP de destino.	Y
	DSCP	Puede configurar la prioridad de los paquetes especificando un valor DSCP. Las opciones incluyen **Predeterminado** (0), **CS** (prioridad baja), **AF** (prioridad media), **EF** (prioridad alta) y **Definido por el usuario** . Los dispositivos V600 no admiten esta función.	Y
	Protocolo	Protocolo de capa de transporte de una regla de aplicación personalizada. Las opciones incluyen **All** , **TCP** y **UDP** .	Y

Tema principal: **Configuración de aplicaciones y grupos de aplicacio**

〈 **Tema** **Siguiente**

Derechos de autor © Huawei Technologies Co., Ltd.

REFERENCIAS TECNICAS

INGLES

DSVPN

What Is DSVPN?

Dynamic Smart Virtual Private Network (DSVPN), which Cisco calls DMVPN, works in conjunction with Multipoint Generic Routing Encapsulation (mGRE) and Next Hop Resolution Protocol (NHRP) to establish dynamic full-mesh VPNs between branches and between branches and the headquarters (HQ). Compared with traditional VPN technologies, DSVPN simplifies the HQ's configuration and O&M when new branches join the network, making network expansion easy. It helps realize direct communication between branches, improving transmission efficiency by avoiding delays caused by HQ pass-through. Additionally, DSVPN supports dynamic public addresses at branches, eliminating the need to purchase static public addresses and thereby reducing network construction costs.

Related Topics

IPsec

VPN

About This Topic

Author: Bai Hehui

Updated on: 2024-11-21

Views: 2513

Average rating: 0

Contents

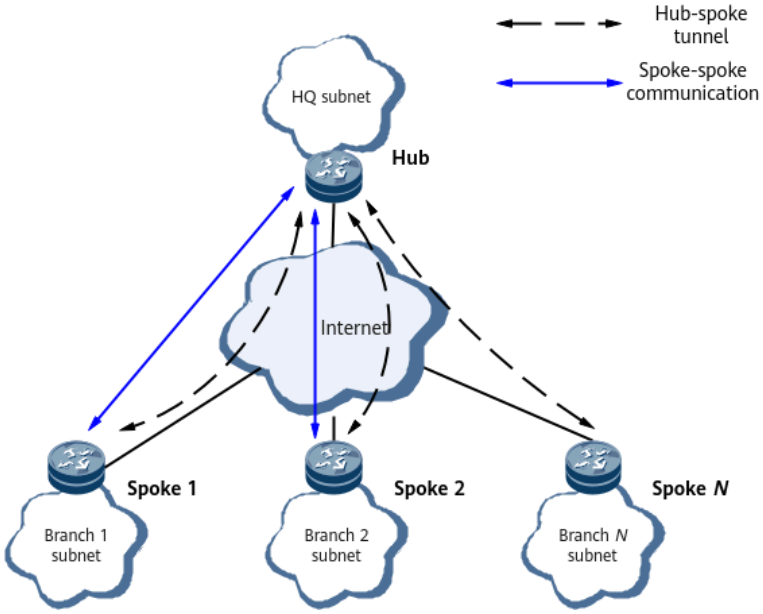
Why Do We Need …
What Are the Advan…
How Does DSVPN …
Application Scenari…

Why Do We Need DSVPN?

Currently, more and more enterprises want to connect branches (spokes) to the HQ (hub) and to each other through VPNs over a public network. They also require service traffic encryption and guaranteed quality of voice and video services. When realizing enterprise branch interconnection, traditional VPN technologies have the following problems:

- Complex configuration: When a new spoke joins the network, the hub needs to create and maintain the VPN configuration for this spoke. In this case, having a large number of spokes on a network complicates the configuration at the hub and makes network expansion difficult.

- Delayed traffic forwarding: Since traffic between branches has to traverse the hub, this traffic consumes bandwidth resources of the hub and results in an additional delay (especially when the hub needs to decrypt and encrypt the traffic). This may interrupt delay-sensitive services such as audio and video conferencing.
- Failure to use dynamic public addresses: When spokes want direct communication with each other and their egresses use dynamic IP addresses, they cannot obtain the peer end's address in advance. As a result, they cannot set up a tunnel between them. In this situation, purchasing static public addresses can solve the problem, but increases costs.



Typical networking for enterprise branch interconnection (without DSVPN deployed)

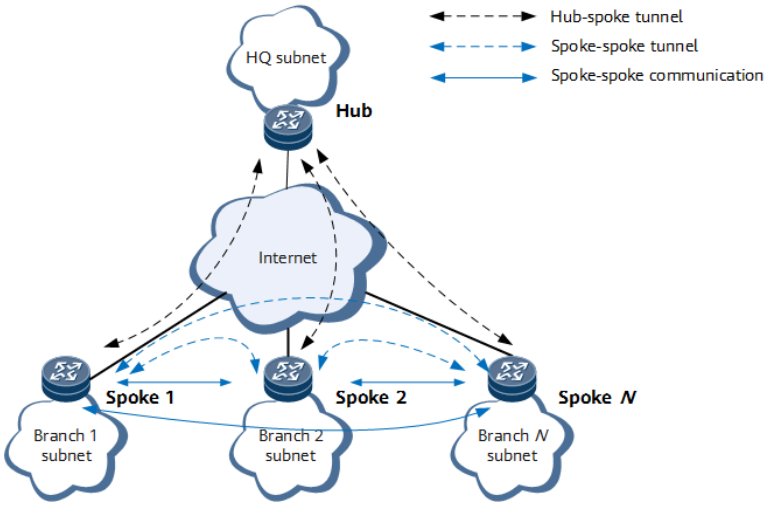
To solve the preceding problems, Huawei launches the dynamic smart VPN technology, that is, DSVPN.

What Are the Advantages of DSVPN?

In terms of enterprise interconnection, DSVPN offers the following advantages over traditional VPN technologies:

- Dynamic: Spokes set up a dynamic tunnel between each other when they have traffic to exchange, eliminating the need for spoke-spoke traffic to traverse the hub.
- Intelligent: Spoke devices use dynamic public addresses, eliminating the need for static address configuration and reducing network construction costs.
- Simplified: Each device only needs one tunnel interface to communicate with all other devices, and adding a new spoke to the network does not require any configuration changes at the hub. These simplify the hub's VPN configuration and O&M, making network expansion easy.

- Secure: DSVPN can work in conjunction with Internet Protocol Security (IPsec) to protect enterprise services.



Typical enterprise branch interconnection networking (with DSVPN deployed)

How Does DSVPN Work?

DSVPN relies on the following four technologies:

- mGRE
- NHRP
- Routing (RIP, OSPF, BGP, or other protocols)
- IPsec

mGRE

mGRE is a point-to-multipoint GRE technology that defines logical mGRE tunnel interfaces to help implement DSVPN. It allows a single GRE interface to support multiple GRE tunnels, simplifying the size and complexity of the configuration. With mGRE, the hub can use only one mGRE tunnel interface with a source specified to help every two spokes set up tunnels. Additionally, adding spokes to a DSVPN network requires no configuration changes at the hub or existing spokes. Only the new spokes need to be configured, after which they automatically register with the hub.

An mGRE tunnel interface has the following attributes:

- Tunnel source address: is used by the transport protocol to identify the packet source.
- Tunnel destination address: is used by the transport protocol to identify the packet destination.
- Tunnel interface IP address: Similar to an IP address of a physical interface, it is used for communication between devices, for example, obtaining routing information. The destination address of a GRE tunnel interface needs to be manually configured, whereas that of an mGRE tunnel interface

is determined by NHRP. An mGRE tunnel interface can have multiple peer ends because it supports multiple GRE tunnels.

NHRP

NHRP helps a spoke obtain the dynamic public address of another spoke on a public network. When a spoke comes online on a DSVPN network, it sends an NHRP Registration Request message to the hub, with the public address of the outbound interface as the source. The hub then creates or updates the corresponding NHRP mapping entry based on the message received. Two spokes also exchange NHRP Resolution Request and Reply messages to create or update NHRP mapping entries. DSVPN works in conjunction with NHRP to collect and maintain site information, such as dynamic public addresses. On a DSVPN network, branches use dynamic addresses for public network access and establish dynamic spoke-spoke tunnels between each other for direct communication. If a spoke-spoke tunnel has no traffic to forward within a certain period, the tunnel is automatically torn down. With NHRP, there is no need for spokes to purchase static public addresses, reducing network construction costs.

Routing

During DSVPN deployment, routing needs to be considered to ensure proper forwarding of mGRE-encapsulated packets. DSVPN supports the following route learning modes:

- Route learning between spokes (non-shortcut mode)
  In this mode, the next-hop address of the route from one spoke to another is the tunnel address of the destination spoke. Each spoke needs to learn routes to all other spokes. This consumes many CPU and memory resources and requires large routing tables and high performance on spokes. In practice, spokes have relatively low performance and can store a limited number of routes. As such, this route learning mode applies only to small and midsize networks where there are a few network nodes and a small number of routes.

  On such a DSVPN network, mGRE tunnels between spokes are set up in non-shortcut mode.

- Route summarization on the hub (shortcut mode)

  In this mode, the next-hop address of the route from one spoke to another is the tunnel address of the hub, and spokes only save routes destined for the hub. This mode reduces the number of routes on spokes, which makes it suitable for large networks with many spokes.

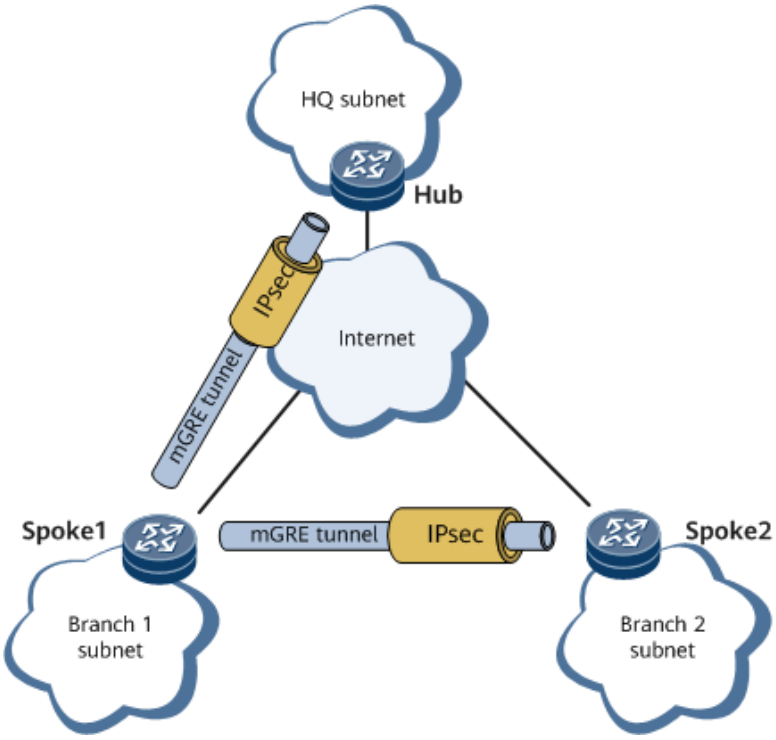
  On such a DSVPN network, mGRE tunnels between spokes are set up in shortcut mode.

On a DSVPN network, route learning in either mode can be achieved through static route configuration or a dynamic routing protocol (OSPF or BGP).

IPsec

Data transmitted between the hub and spokes, as well as between spokes, needs to be encrypted to increase data security. To meet this requirement, during DSVPN deployment, IPsec profiles can be applied to mGRE tunnel interfaces so that mGRE and IPsec tunnels are dynamically established between spokes.

- The establishment of an mGRE tunnel immediately triggers that of an IPsec tunnel.
- Typical IPsec technology uses ACLs to identify unicast traffic to be encrypted. An IPsec policy requires a large number of ACLs to be defined, which is difficult to implement. DSVPN combines NHRP and mGRE with IPsec to provide ease of device configurations, while ensuring data transmission security and facilitating network deployment.
- Because IPsec tunnels are dynamically established between spokes, IPsec data exchanged between spokes does not need to be decrypted or encrypted by the hub. This minimizes data transmission delay.



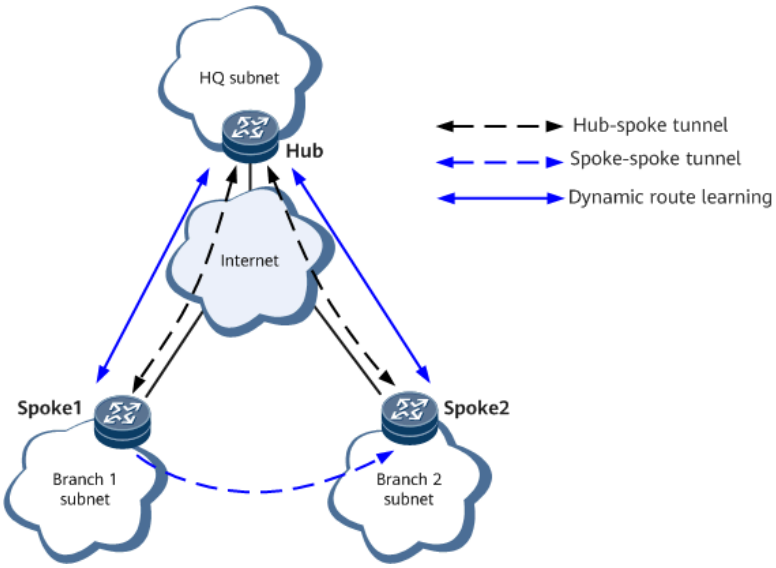
DSVPN over IPsec

Application Scenarios of DSVPN

DSVPN helps branches dynamically establish VPN tunnels in two scenarios: non-shortcut scenario for small and midsize networks and shortcut scenario for large networks.

DSVPN on Small and Midsize Networks

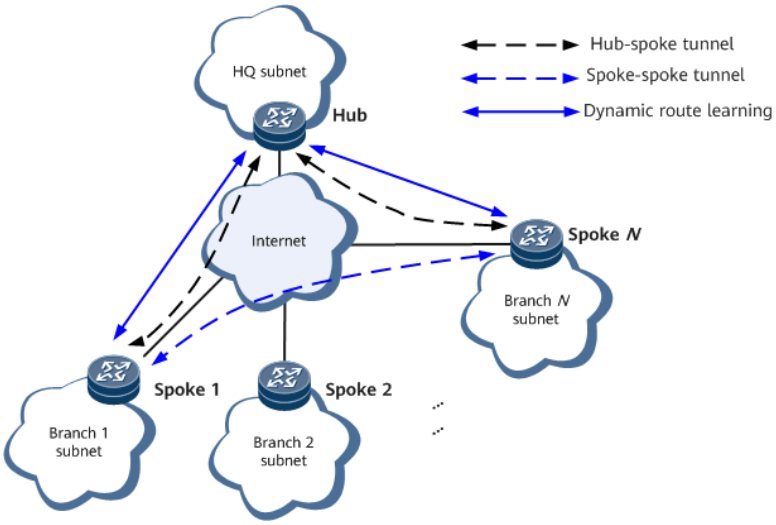
A small or midsize network has only a few branches. They can dynamically establish VPNs with each other by using DSVPN in a non-shortcut scenario for direct communication. As shown in the following figure, two branches (Spoke1 and Spoke2) connect to the HQ (Hub) through the Internet. Spoke1 and Spoke2 are configured to learn routes from each other. They can communicate with each other directly because they are each other's next hop.



DSVPN on small and midsize networks

DSVPN on Large Networks

A large network involves a large number of branches. Deploying DSVPN in a non-shortcut scenario on such networks requires spokes to support large routing tables and offer high forwarding performance. If upgrading spokes is not considered, DSVPN in a shortcut scenario can be a better solution. It reduces routing entries on spokes, lowering the requirements on their routing table sizes and forwarding performance. As shown in the following figure, all spokes have routes only to the hub. When two spokes need to communicate, the originating spoke sends the first packet to the hub. After that, a tunnel is established between the spokes, through which they can directly exchange data.



DSVPN on large networks

References

1 DSVPN Configuration Guide (AR Series Routers)

2 DSVPN Configuration Guide (NE40E Routers)

Follow Us

About Huawei

How to Buy

Partner

Resources

Others

Copyright © 2023 Huawei Technologies Co., Ltd. All rights reserved.

Privacy Policy | Cookie Settings | Terms of use | RSS Subscribe | Sitemap |

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

DSVPN

Enciclopedia IP > DSVPN

¿Qué es DSVPN?

La Red Privada Virtual Inteligente Dinámica (DSVPN), denominada DMVPN por Cisco, funciona en conjunto con la Encapsulación de Enrutamiento Genérico Multipunto (mGRE) y el Protocolo de Resolución de Próximo Salto (NHRP) para establecer VPN dinámicas de malla completa entre sucursales y entre las sucursales y la sede central. En comparación con las tecnologías VPN tradicionales , DSVPN simplifica la configuración, las operaciones y el mantenimiento de la sede central cuando se incorporan nuevas sucursales a la red, lo que facilita su expansión. Facilita la comunicación directa entre sucursales, mejorando la eficiencia de la transmisión al evitar los retrasos causados por la transferencia a la sede central. Además, DSVPN admite direcciones públicas dinámicas en las sucursales, lo que elimina la necesidad de adquirir direcciones públicas estáticas y, por lo tanto, reduce los costos de construcción de la red.

Contenido

¿Por qué necesitam…
¿Cuáles son las ven…
¿Cómo funciona DS…
Escenarios de aplica…

¿Por qué necesitamos DSVPN?

Actualmente, cada vez más empresas desean conectar sus sucursales (radios) con la sede central (hub) y entre sí mediante VPN a través de una red pública. También requieren el cifrado del tráfico de servicios y una calidad garantizada de los servicios de voz y video. Al implementar la interconexión de sucursales empresariales, las tecnologías VPN tradicionales presentan los siguientes problemas:

- Configuración compleja: Cuando un nuevo radio se une a la red, el concentrador debe crear y mantener la configuración de VPN para este radio. En este caso, tener un gran número de radios en

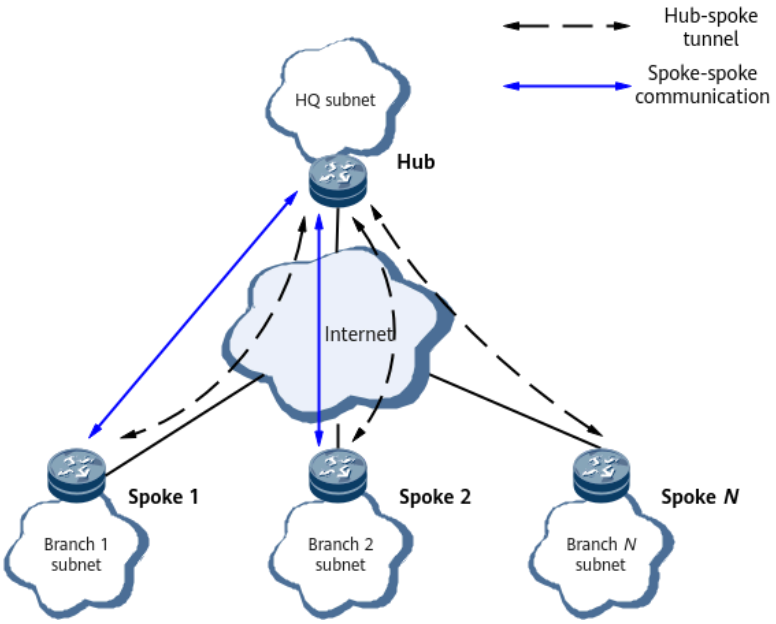
Temas relacionados
IPsec
VPN

Acerca de este tema
Autor: Bai Hehui
Actualizado el: 21/11/2024
Vistas: 2513
Puntuación media: 0

Contenido
¿Por qué necesitamos DSVPN?
¿Cuáles son las ventajas de DSVPN?
¿Cómo funciona DSVPN?
Escenarios de aplicación de DSVPN

una red complica la configuración en el concentrador y dificulta la expansión de la red.

- Reenvío de tráfico retrasado: Dado que el tráfico entre sucursales debe atravesar el concentrador, este consume recursos de ancho de banda del concentrador y genera un retraso adicional (especialmente cuando el concentrador necesita descifrar y cifrar el tráfico). Esto puede interrumpir servicios sensibles a los retrasos, como las conferencias de audio y video.
- Error en el uso de direcciones públicas dinámicas: Cuando los radios desean comunicarse directamente entre sí y sus salidas utilizan direcciones IP dinámicas , no pueden obtener la dirección del otro extremo con antelación. Por lo tanto, no pueden establecer un túnel entre ellos. En esta situación, la compra de direcciones públicas estáticas puede solucionar el problema, pero aumenta los costos.



Redes típicas para la interconexión de sucursales empresariales (sin DSVPN implementado)

Para resolver los problemas anteriores, Huawei lanza la tecnología VPN inteligente dinámica, es decir, DSVPN.

¿Cuáles son las ventajas de DSVPN?

En términos de interconexión empresarial, DSVPN ofrece las siguientes ventajas sobre las tecnologías VPN tradicionales :

- Dinámico: los radios establecen un túnel dinámico entre sí cuando tienen tráfico para intercambiar, lo que elimina la necesidad de que el tráfico entre radios atraviese el concentrador.
- Inteligente: los dispositivos Spoke utilizan direcciones públicas dinámicas, lo que elimina la necesidad de configurar direcciones estáticas y reduce los costos de construcción de la red.
- Simplificado: Cada dispositivo solo necesita una interfaz de túnel para comunicarse con los demás, y añadir un nuevo radio a la red

Temas relacionados

IPsec

VPN

Acerca de este tema

Autor: Bai Hehui

Actualizado el: 21/11/2024

Vistas: 2513

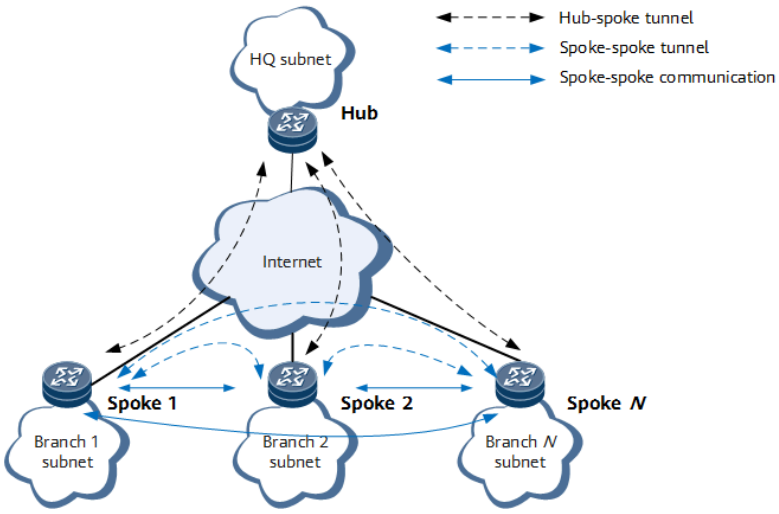
Puntuación media: 0

Contenido

¿Por qué necesitamos DSVPN?
¿Cuáles son las ventajas de DSVPN?
¿Cómo funciona DSVPN?
Escenarios de aplicación de DSVPN

no requiere cambios de configuración en el concentrador. Esto simplifica la configuración y las operaciones y el mantenimiento de la VPN del concentrador, facilitando la expansión de la red.

- Seguro: DSVPN puede funcionar junto con el Protocolo de Seguridad de Internet (IPsec) para proteger los servicios empresariales.



Red de interconexión de sucursales empresariales típica (con DSVPN implementado)

¿Cómo funciona DSVPN?

DSVPN se basa en las siguientes cuatro tecnologías:

- mGRE
- NHRP
- Enrutamiento (RIP, OSPF , BGP u otros protocolos)
- IPsec

mGRE

mGRE es una tecnología GRE punto a multipunto que define interfaces lógicas de túnel mGRE para facilitar la implementación de DSVPN. Permite que una sola interfaz GRE admita múltiples túneles GRE, lo que simplifica el tamaño y la complejidad de la configuración. Con mGRE, el concentrador puede usar solo una interfaz de túnel mGRE con una fuente especificada para facilitar la configuración de túneles por cada dos radios. Además, añadir radios a una red DSVPN no requiere cambios de configuración en el concentrador ni en los radios existentes. Solo es necesario configurar los nuevos radios, tras lo cual se registran automáticamente en el concentrador.

Una interfaz de túnel mGRE tiene los siguientes atributos:

- Dirección de origen del túnel: la utiliza el protocolo de transporte para identificar el origen del paquete.

Temas relacionados

IPsec

VPN

Acerca de este tema

Autor: Bai Hehui

Actualizado el: 21/11/2024

Vistas: 2513

Puntuación media: 0

Contenido

¿Por qué necesitamos DSVPN?
¿Cuáles son las ventajas de DSVPN?
¿Cómo funciona DSVPN?
Escenarios de aplicación de DSVPN

- Dirección de destino del túnel: la utiliza el protocolo de transporte para identificar el destino del paquete.
- Dirección IP de la interfaz de túnel : Similar a la dirección IP de una interfaz física, se utiliza para la comunicación entre dispositivos, por ejemplo, para obtener información de enrutamiento. La dirección de destino de una interfaz de túnel GRE debe configurarse manualmente, mientras que la de una interfaz de túnel mGRE la determina NHRP. Una interfaz de túnel mGRE puede tener múltiples extremos pares, ya que admite múltiples túneles GRE.

NHRP

NHRP ayuda a un radio a obtener la dirección pública dinámica de otro radio en una red pública. Cuando un radio se conecta a una red DSVPN, envía un mensaje de solicitud de registro NHRP al concentrador, con la dirección pública de la interfaz de salida como origen. El concentrador crea o actualiza la entrada de mapeo NHRP correspondiente según el mensaje recibido. Dos radios también intercambian mensajes de solicitud y respuesta de resolución NHRP para crear o actualizar las entradas de mapeo NHRP. DSVPN trabaja en conjunto con NHRP para recopilar y mantener información del sitio, como las direcciones públicas dinámicas. En una red DSVPN, las sucursales utilizan direcciones dinámicas para el acceso a la red pública y establecen túneles dinámicos entre radios para la comunicación directa. Si un túnel entre radios no tiene tráfico que reenviar dentro de un período determinado, se desactiva automáticamente. Con NHRP, los radios no necesitan adquirir direcciones públicas estáticas, lo que reduce los costos de construcción de la red.

Enrutamiento

Durante la implementación de DSVPN, es necesario considerar el enrutamiento para garantizar el reenvío correcto de los paquetes encapsulados en mGRE. DSVPN admite los siguientes modos de aprendizaje de rutas:

- Aprendizaje de ruta entre radios (modo sin atajo)
  En este modo, la dirección del siguiente salto de la ruta de un radio a otro es la dirección del túnel del radio de destino. Cada radio necesita aprender rutas a todos los demás. Esto consume muchos recursos de CPU y memoria, y requiere tablas de enrutamiento grandes y un alto rendimiento en los radios. En la práctica, los radios tienen un rendimiento relativamente bajo y pueden almacenar un número limitado de rutas. Por lo tanto, este modo de aprendizaje de rutas solo se aplica a redes pequeñas y medianas con pocos nodos de red y un número reducido de rutas.

  En una red DSVPN de este tipo, los túneles mGRE entre radios se configuran en modo sin acceso directo.
- Resumen de ruta en el concentrador (modo de acceso directo)

Temas relacionados

IPsec

VPN

Acerca de este tema

Autor: Bai Hehui

Actualizado el: 21/11/2024

Vistas: 2513

Puntuación media: 0

Contenido

¿Por qué necesitamos DSVPN?
¿Cuáles son las ventajas de DSVPN?
¿Cómo funciona DSVPN?
Escenarios de aplicación de DSVPN

En este modo, la dirección del siguiente salto de la ruta de un radio a otro es la dirección del túnel del concentrador, y los radios solo guardan las rutas destinadas al concentrador. Este modo reduce el número de rutas en los radios, lo que lo hace ideal para redes grandes con muchos radios.

En una red DSVPN de este tipo, los túneles mGRE entre radios se configuran en modo de acceso directo.

En una red DSVPN, el aprendizaje de ruta en cualquier modo se puede lograr a través de la configuración de ruta estática o un protocolo de enrutamiento dinámico (OSPF o BGP).

IPsec

Para cumplir con este requisito, durante la implementación de DSVPN, se pueden aplicar perfiles IPsec a las interfaces de túnel mGRE para que los túneles mGRE e IPsec se establezcan dinámicamente entre los radios.

- El establecimiento de un túnel mGRE activa inmediatamente el de un túnel IPsec.
- La tecnología IPsec típica utiliza ACL para identificar el tráfico unidifusión que se va a cifrar. Una política IPsec requiere la definición de un gran número de ACL, lo cual es difícil de implementar. DSVPN combina NHRP y mGRE con IPsec para facilitar la configuración de dispositivos, a la vez que garantiza la seguridad de la transmisión de datos y facilita la implementación de la red.
- Dado que los túneles IPsec se establecen dinámicamente entre radios, el concentrador no necesita descifrar ni cifrar los datos IPsec intercambiados entre ellos. Esto minimiza el retraso en la transmisión de datos.

Temas relacionados

IPsec

VPN

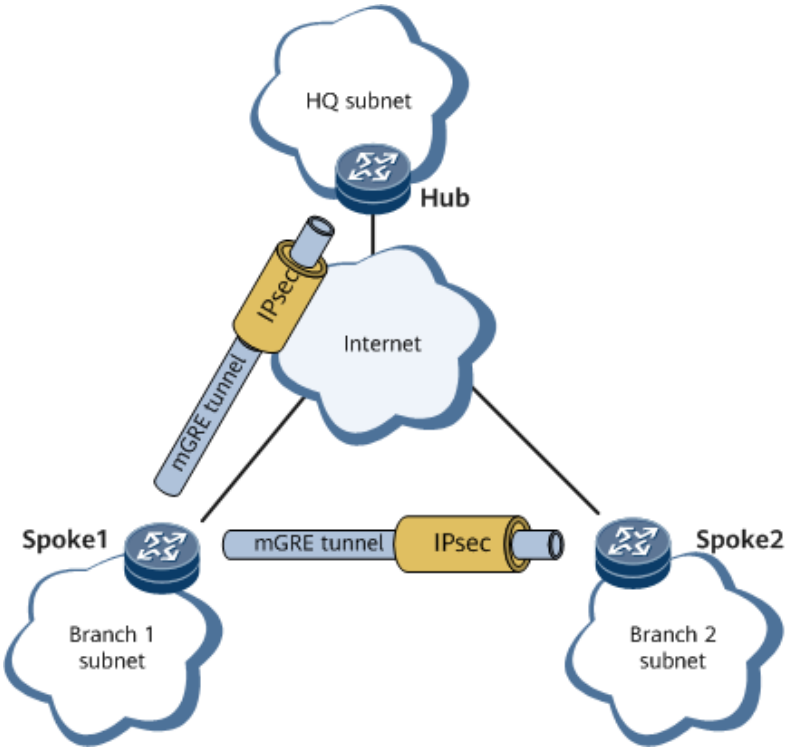
Acerca de este tema

Autor: Bai Hehui

Actualizado el: 21/11/2024

Contenido

¿Por qué necesitamos DSVPN?
¿Cuáles son las ventajas de DSVPN?
¿Cómo funciona DSVPN?
Escenarios de aplicación de DSVPN



DSVPN sobre IPsec

Escenarios de aplicación de DSVPN

DSVPN ayuda a las sucursales a establecer dinámicamente túneles VPN en dos escenarios: un escenario sin acceso directo para redes pequeñas y medianas y un escenario con acceso directo para redes grandes.

DSVPN en redes pequeñas y medianas

Una red pequeña o mediana tiene solo unas pocas sucursales. Estas pueden establecer VPN dinámicamente entre sí mediante DSVPN en un escenario sin acceso directo para la comunicación directa. Como se muestra en la siguiente figura, dos sucursales (Spoke1 y Spoke2) se conectan al concentrador (HQ) a través de Internet. Spoke1 y Spoke2 están configuradas para aprender rutas mutuamente. Pueden comunicarse directamente entre sí porque son el siguiente salto de cada una.

Temas relacionados

IPsec

VPN

Acerca de este tema

Autor: Bai Hehui

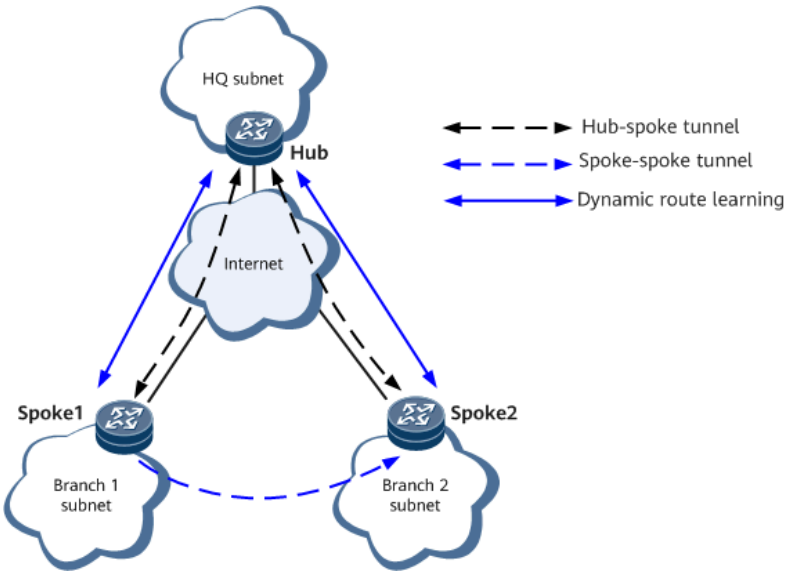
Actualizado el: 21/11/2024

Vistas: 2513

Puntuación media: 0

Contenido

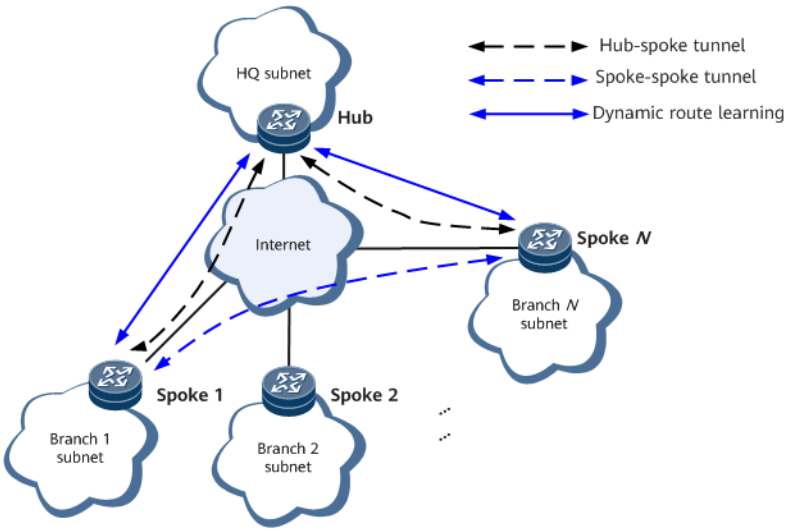
¿Por qué necesitamos DSVPN?
¿Cuáles son las ventajas de DSVPN?
¿Cómo funciona DSVPN?
Escenarios de aplicación de DSVPN



DSVPN en redes pequeñas y medianas

DSVPN en redes grandes

Una red grande implica una gran cantidad de sucursales. Implementar DSVPN en un escenario sin acceso directo en dichas redes requiere que los radios admitan tablas de enrutamiento grandes y ofrezcan un alto rendimiento de reenvío. Si no se considera la actualización de los radios, DSVPN en un escenario con acceso directo puede ser una mejor solución. Reduce las entradas de enrutamiento en los radios, lo que disminuye los requisitos de tamaño de sus tablas de enrutamiento y rendimiento de reenvío. Como se muestra en la siguiente figura, todos los radios tienen rutas solo al concentrador. Cuando dos radios necesitan comunicarse, el radio de origen envía el primer paquete al concentrador. Posteriormente, se establece un túnel entre los radios, a través del cual pueden intercambiar datos directamente.



DSVPN en redes grandes

Referencias

1 Guía de configuración de DSVPN (enrutadores de la serie AR)

Temas relacionados

IPsec

VPN

Acerca de este tema

Autor: Bai Hehui

Actualizado el: 21/11/2024

Vistas: 2513

Puntuación media: 0

Contenido

¿Por qué necesitamos DSVPN?
¿Cuáles son las ventajas de DSVPN?
¿Cómo funciona DSVPN?
Escenarios de aplicación de DSVPN

2 Guía de configuración de DSVPN (enrutadores NE40E)

Síganos

Acerca de Huawei

Cómo comprar

Pareja

Recursos

Otros

Copyright © 2023 Huawei Technologies Co., Ltd. Todos los derechos reservados.

política de privacidad | Configuración de cookies | Condiciones de uso | Suscribirse a RSS | Mapa del sitio |

¿Por qué necesitamos DSVPN?
¿Cuáles son las ventajas de DSVPN?
¿Cómo funciona DSVPN?
Escenarios de aplicación de DSVPN

REFERENCIAS TECNICAS

INGLES

encapsulation mode

encapsulation-mode

Function

The **encapsulation-mode** command sets the IPsec encapsulation mode.
The **undo encapsulation-mode** command restores the default IPsec encapsulation mode.
By default, the tunnel mode is used.

Format

encapsulation-mode { **transport** | **tunnel** | **auto** }
undo encapsulation-mode

Parameters

Parameter	Description	Value
transport	Encapsulates IP packets in transport mode.	-
tunnel	Encapsulates IP packets in tunnel mode.	-
auto	Indicates the auto-sensing mode. The tunnel mode is used if the device serves as the IKE negotiation initiator. If the device serves as the responder, both the tunnel mode and transport mode can be used.	-

Views

IPsec proposal view, IPsec proposal view of the virtual system

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario
IPsec encapsulates IP packets by adding an AH or ESP header and ESP tail to original IP packets for authentication and encryption. The following two IPsec encapsulation modes are available:

- Tunnel mode: In tunnel mode, IPsec adds a new IP header to an IP packet. The source and destination addresses of the new IP header are the IP addresses of two ends of a tunnel. The tunnel mode is more secure than the transport mode. In terms of performance, the tunnel mode consumes more bandwidth than the transport mode. The tunnel mode is often used between two security gateways. The packets encrypted by one security gateway can only be decrypted by the other security gateway.
- Transport mode: In transport mode, IPsec does not add a new header to an IP packet. The source and destination addresses of the original packet are the IP addresses of two ends of a tunnel. In transport mode, the two devices that encrypt and decrypt packets must be the original packet sender and final receiver

respectively. Since most data traffic between two security gateways is not communication traffic of the two gateways, the transport mode is not used between security gateways. The transport mode is suited for the communication between two hosts or between a host and a security gateway; however, the transport mode is not recommended because it provides low security.

- Auto-sensing mode: The auto-sensing mode enables IKE peers to negotiate the IPsec encapsulation mode. The receiver supports both the transport mode and tunnel mode, which improves the success rate of IKE negotiation.

Precautions

- The two IPsec tunnel ends must use the same encapsulation mode.
- When IKEv2 is used, the encapsulation mode in all the IPsec proposals configured on the IKE negotiation initiator must be the same; otherwise, IKE negotiation fails.
- When IKEv2 is used, after the **encapsulation-mode auto** command is run on the responder, the default duration and traffic for IPsec SA aging are 604800 seconds and 0 (indicating that the traffic timeout function is disabled on the responder), respectively. As a result, the responder cannot proactively initiate IPsec SA re-negotiation.
- If both ends use an IPsec policy in ISAKMP mode or an IPsec profile, IKE negotiation initiator DeviceA uses the transport mode to establish an IPsec tunnel with the responder DeviceB using the auto-sensing mode. When the SA of DeviceB is aged out, DeviceB functions as the IKE negotiation initiator (using the tunnel mode) to perform IPsec tunnel re-negotiation with DeviceA. As a result, encapsulation modes on both ends are inconsistent, causing a failure to establish an IPsec tunnel. Therefore, ensure that DeviceB using the auto-sensing mode functions only as the IKE negotiation responder. Otherwise, the auto-sensing mode does not apply to this scenario.

Example

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

encapsulation mode

modo de encapsulación

Función

El comando **encapsulation-mode** establece el modo de encapsulación de IPsec.
El comando **undo encapsulation-mode** restaura el modo de encapsulación IPsec predeterminado.
De forma predeterminada, se utiliza el modo túnel.

Formato

modo de encapsulación { **transporte** | **túnel** | **automático** }
deshacer el modo de encapsulación

Parámetros

Parámetro	Descripción	Valor
transporte	Encapsula paquetes IP en modo de transporte.	-
túnel	Encapsula paquetes IP en modo túnel.	-
auto	Indica el modo de detección automática. El modo túnel se utiliza si el dispositivo actúa como iniciador de la negociación IKE. Si el dispositivo actúa como respondedor, se pueden utilizar tanto el modo túnel como el modo transporte.	-

Vistas

Vista de propuesta de IPsec, vista de propuesta de IPsec del sistema virtual

Nivel predeterminado

2: Nivel de configuración

Instrucciones de uso

Escenario de uso
IPsec encapsula los paquetes IP añadiendo un encabezado AH o ESP y una cola ESP a los paquetes IP originales para su autenticación y cifrado. Están disponibles los dos modos de encapsulación IPsec siguientes:

- Modo túnel: En el modo túnel, IPsec añade un nuevo encabezado IP a un paquete IP. Las direcciones de origen y destino del nuevo encabezado IP son las direcciones IP de los dos extremos del túnel. El modo túnel es más seguro que el modo transporte. En términos de rendimiento, el modo túnel consume más

ancho de banda que el modo transporte. El modo túnel se utiliza a menudo entre dos puertas de enlace de seguridad. Los paquetes cifrados por una puerta de enlace de seguridad solo pueden ser descifrados por la otra.

- Modo de transporte: En el modo de transporte, IPsec no añade un nuevo encabezado a un paquete IP. Las direcciones de origen y destino del paquete original son las direcciones IP de los dos extremos de un túnel. En el modo de transporte, los dos dispositivos que cifran y descifran los paquetes deben ser el emisor y el receptor del paquete original, respectivamente. Dado que la mayor parte del tráfico de datos entre dos puertas de enlace de seguridad no es tráfico de comunicación entre ellas, el modo de transporte no se utiliza entre ellas. El modo de transporte es adecuado para la comunicación entre dos hosts o entre un host y una puerta de enlace de seguridad; sin embargo, no se recomienda debido a su baja seguridad.
- Modo de detección automática: Este modo permite que los pares IKE negocien el modo de encapsulación IPsec. El receptor admite tanto el modo de transporte como el modo túnel, lo que mejora la tasa de éxito de la negociación IKE.

Precauciones

- Los dos extremos del túnel IPsec deben utilizar el mismo modo de encapsulación.
- Cuando se utiliza IKEv2, el modo de encapsulación en todas las propuestas IPsec configuradas en el iniciador de negociación IKE debe ser el mismo; de lo contrario, la negociación IKE falla.
- Cuando se utiliza IKEv2, tras ejecutar el comando **"encapsulation-mode auto"** en el respondedor, la duración y el tráfico predeterminados para el envejecimiento de la SA de IPsec son 604800 segundos y 0 (lo que indica que la función de tiempo de espera de tráfico está deshabilitada en el respondedor), respectivamente. Por lo tanto, el respondedor no puede iniciar proactivamente la renegociación de la SA de IPsec.
- Si ambos extremos utilizan una política IPsec en modo ISAKMP o un perfil IPsec, el Dispositivo A, que inicia la negociación IKE, utiliza el modo de transporte para establecer un túnel IPsec con el Dispositivo B, que responde mediante el modo de detección automática. Cuando la SA del Dispositivo B alcanza la caducidad, este actúa como iniciador de la negociación IKE (utilizando el modo de túnel) para renegociar el túnel IPsec con el Dispositivo A. Como resultado, los modos de encapsulación en ambos extremos son inconsistentes, lo que provoca un fallo en el establecimiento de un túnel IPsec. Por lo tanto, asegúrese de que el Dispositivo B, que utiliza el modo de detección automática, funcione únicamente como respondedor de la negociación IKE. De lo contrario, el modo de detección automática no es aplicable a este escenario.

REFERENCIAS TECNICAS

INGLES

GartnerReprint

Magic Quadrant for Network Firewalls

19 December 2022 - ID G00761497 - 55 min read

By Rajpreet Kaur, Adam Hils, **and 1 more**

As network firewalls evolve into hybrid mesh firewalls with the emergence of cloud firewalls and firewall-as-a-service offerings, selecting the most suitable vendor is a challenge. Gartner assesses 17 vendors to help security and risk management leaders make the right choice for their organization.

Strategic Planning Assumptions

By 2026, more than 60% of organizations will have more than one type of firewall deployment, which will prompt adoption of hybrid mesh firewalls.

By 2026, over 30% of the new deployments of distributed branch-office firewalls will be of firewall-as-a-service offerings, up from less than 10% in 2022.

Market Definition/Description

Gartner defines the network firewall market as the market for firewalls that use bidirectional stateful traffic inspection (for both egress and ingress) to secure networks. Network firewalls are enforced through hardware, virtual appliances and cloud-native controls.

Network firewalls are used to secure networks. These can be on-premises, hybrid (on-premises and cloud), public cloud or private cloud networks. Network firewall products support different deployment use cases, such as for perimeters, midsize enterprises, data centers, clouds, cloud-native and distributed offices.

Network firewalls' capabilities include advanced networking, threat inspection and detection, and web filtering.

Core capabilities:

- **Networking:** This includes support for routing tables with destination network address translation (DNAT) and static network address translation (SNAT) capability.
- **Stateful inspection:** This enables inspection of traffic based on stateful firewall rules.

- **Threat detection and inspection:** This includes intrusion prevention system (IPS) and malware inspection capabilities.
- **Web filtering:** This includes filtering of outbound traffic for HTTP and HTTPS and applications.
- **Advanced logging and reporting:** All actions of firewall administrators can be logged, and reports can be customized and run based on different object types and traffic types. Threat-based and web-filtering-based granular reports can be generated.

Optional capabilities:

- **Internet of Things (IoT) security:** This is achieved either using a module built into threat detection controls or via a dedicated subscription integrated within network firewall offerings. Specific features may include discovery of IoT devices, risk analysis and dedicated rules to block attacks related to these devices. Also, IoT signatures as a part of IPS signature base.
- **Network sandboxing:** Network sandboxing monitors network traffic for suspicious objects and automatically submits them to the sandbox environment, where they are analyzed and assigned malware probability scores and severity ratings.
- **Zero trust network access (ZTNA):** Zero trust network access (ZTNA) makes possible an identity- and context-based access boundary between any user and device to applications.
- **Operational technology (OT) security:** This includes integrated or dedicated features related to protecting an OT environment. Stand-alone OT security offerings are not considered here. Features may include dedicated OT-related threat intelligence, dedicated IPS signatures for OT devices, support for supervisory control and data acquisition (SCADA) applications and threat inspection.
- **Domain Name System (DNS) security:** This secures traffic to DNS by offering monitoring, detection and prevention capabilities against DNS layer attacks.
- **Software-defined wide-area network (SD-WAN):** This provides dynamic path selection, based on business or application policy, centralized policy and management of appliances, virtual private network (VPN), and zero-touch configuration.

Magic Quadrant

Figure 1: Magic Quadrant for Network Firewalls



Source: Gartner (December 2022)

Vendor Strengths and Cautions

Alibaba Cloud

Alibaba Cloud is a Challenger in this Magic Quadrant. Its Alibaba Cloud Firewall is a more mature cloud firewall offering than those of its direct cloud service providers (CSP) competitors, with features such as application control, URL filtering and advanced threat prevention. It also offers firewalls for emerging cloud use cases, such as container firewalls, and microsegmentation exclusively inside its offerings.

Alibaba Cloud is a cloud service provider with an extensive product portfolio. It offers a strong set of security controls. Alibaba Cloud Firewall is its cloud-native firewall offering.

Alibaba Cloud has made major updates in relation to its firewall traffic visualization capability and introduction of a DNS firewall. It has also expanded its points of presence (POPs) to more regions outside China.

Strengths

- **Support for emerging cloud firewall use cases:** Alibaba Cloud offers a mature container firewall module, the Alibaba Security Center-Container Firewall, that offers image security and runtime application security features. Additionally, the Alibaba Cloud Firewall offers mature microsegmentation capabilities as a part of its advanced licensing tier.

- **Product portfolio and market responsiveness:** Alibaba Cloud is a large CSP with an extensive product portfolio. It has a strong focus on expanding its security offerings and scores highly for market responsiveness, compared with its direct CSP competitors.

- **Unified endpoint client:** Alibaba Cloud offers a single client for its firewall VPN, secure access service edge (SASE) and endpoint detection and response (EDR) products, which makes management and vendor consolidation easier. Both cloud firewall and EDR products can be managed centrally from the Alibaba Security Center.

- **Advanced threat detection:** Alibaba Cloud Firewall offers network detection and response (NDR) capabilities, with integration between Alibaba EDR and the Alibaba Cloud Security Center, its extended detection and response (XDR) platform. Clients also have the option to purchase a direct managed security service. Alibaba Cloud also offers a dedicated DNS firewall for DNS security.

Cautions

- **Application control:** Although Alibaba Cloud offers strong support for regional applications, along with data loss prevention (DLP) capability, its firewalls lack support for applications such as Microsoft Office 365 that are widely used outside China. Hence, customers outside China must compare Alibaba Cloud's application control with the applications they use, before finalizing a purchasing decision.

- **Geographic presence:** Alibaba Cloud has a major presence in China, but rarely appears on the shortlists of customers outside China. As a result, its product strategy focuses on Chinese requirements.

- **Third-party partnerships:** Alibaba Cloud's strategy is to create its own native offerings. It therefore has only limited regional partnerships. It does not offer any firewall integration with third-party EDR, XDR and identity and access management (IAM) solutions.

- **Features:** Alibaba Cloud Firewall lacks support for Transport Layer Security (TLS) decryption. It also lacks fully qualified domain name (FQDN)-based traffic routing and redirection and IoT security features.

Amazon Web Services

Amazon Web Services (AWS) is a Niche Player in this Magic Quadrant. AWS Network Firewall, a native cloud firewall, offers basic features, compared with those of other network firewall vendors. There are also third-party firewall as a service (FWaaS) offerings that customers can purchase, including partner-managed firewall rules, via the AWS Marketplace.

AWS is a CSP. AWS Network Firewall is offered as a fully managed service on AWS's cloud platform. Other AWS security product families include IAM, network and application protection, data protection, incident response and compliance.

Significant recent features developed for AWS Network Firewall include enhanced east-west protection (traffic inspection between subnets in the same virtual private cloud), default deny/drop rules, strict rule-ordering configuration options, and AWS Firewall Manager support for centralized deployment.

Strengths

- **Customer experience:** AWS Network Firewall scores highly for high availability and automated scaling. Additionally, clients like the customization feature using AWS's managed rules. They identify the ease of use of these integral features as a primary reason for selecting AWS Network Firewall.
- **Pricing:** Clients value the simplicity of AWS Network Firewall's pricing model. Customers pay for the number of firewalls deployed and the amount of traffic processed. All customers receive Basic support free of charge.
- **Scalability:** AWS Network Firewall's performance, high availability and scalability provide distinct advantages over other firewall vendors' offerings. It offers built-in high availability to ensure all traffic is inspected and monitored consistently.
- **Ease of deployment:** Ease of deployment is achieved through many different features in AWS's firewall manager, such as automatic firewall provisioning, the ability to automatically deploy firewalls across accounts and zero-touch deployment.

Cautions

- **Product strategy:** AWS Network Firewall lags behind in terms of features, compared with competing offerings. As a result, AWS relies on partnerships with other vendors, such as Palo Alto Networks, that offer native AWS instances of partner vendor firewalls for customers who see limitations in AWS's firewall.
- **Consolidation:** Gartner clients generally do not consider AWS a desirable vendor for consolidation toward zero trust architecture. AWS lacks a native ZTNA offering. It has a complicated deployment scheme using AWS Virtual Private Cloud (VPC) to achieve microsegmentation, which limits its appeal to shortlists for emerging firewall use cases.
- **Feature gaps:** AWS Network Firewall does not support native network address translation (NAT) features and has no IPv6 support. It also has no ability to detect client-based applications and lacks granular application control.
- **Advanced threat detection:** AWS Network Firewall offers fewer vendor-researched proprietary signatures than other firewalls. Additionally, AWS lacks TLS decryption in its firewall.

Barracuda

Barracuda is a Visionary in this Magic Quadrant. It offers a range of firewall appliances focused on distributed offices and virtual appliances for public clouds within the CloudGen Firewall product line. Branch connectivity is a key market for Barracuda.

Barracuda's security offerings include firewalls, web application and API protection (WAAP) offerings, secure web gateways, ZTNA (for remote access to private applications) and secure email gateways.

Recent updates to Barracuda's firewall line include IoT, OT and cloud security features. Barracuda has, for example, added IPS, URL, content, antivirus and Secure Sockets Layer (SSL) inspection features to its CloudGen WAN product.

Strengths

- **Cloud and branch-office features:** Barracuda's CloudGen Firewall product line offers mature integration with native AWS and Microsoft Azure controls. Barracuda has added a FWaaS product, CloudGen WAN, to address the work-from-home and remote-office use cases. Barracuda has also introduced Secure Connector for IoT connectivity to Microsoft Azure, which is fully manageable via CloudGen WAN.
- **Firewall deployment modes:** Barracuda has delivered products for all major firewall modes — CloudGen Firewall for hardware and virtual; CloudGen WAN for FWaaS; Secure Connector for containerized firewall; and CloudGen Firewall (rugged) for industrial firewall requirements.
- **Pricing:** Barracuda's low-end appliances provide a very good total cost of ownership (TCO). The vendor's pool-based licensing enables administrators to assign software licenses across platforms as needed.
- **IoT features:** Barracuda has increased its ability to secure IoT environments by developing partnerships with Crosser, Nozomi Networks and SCADAfence. Barracuda also has a partnership with Crosser to run edge compute logic on some firewall devices.

Cautions

- **Virtualization:** Barracuda's hardware appliances do not isolate some features, such as VPN, Dynamic Host Configuration Protocol (DHCP), DNS cache and DNS interception, when running multiple virtual instances on the same appliance.
- **Multiple management portals:** Separate management consoles are exclusive to their environments. The FWaaS product, CloudGen WAN, must be managed through Barracuda's cloud management platform. CloudGen physical and virtual appliances must be managed with an on-premises firewall manager called Barracuda Firewall Admin.
- **Product strategy:** Barracuda lacks native EDR and offers only limited third-party integration with endpoint and network security vendors. IPS capability is provided, but it uses technology from Trend Micro on an OEM basis. All IPS signatures are developed via the third party, and the quantity of signatures is inferior to that of competitors.
- **Customer feedback:** Client feedback indicates that Barracuda offers limited reporting on content-filtering modules and that product management is a complex task.

Check Point Software Technologies

Check Point Software Technologies is a Leader in this Magic Quadrant. It is shortlisted for stand-alone firewall use cases by enterprise clients. In addition to firewalls, Check Point offers a broad array of security functionality with mature cloud-based centralized management. This makes it a strong candidate for organizations seeking a security platform solution.

Check Point offers a comprehensive security portfolio that features Quantum-branded hardware appliances and the Maestro hyperscale product line. Check Point packages its FWaaS as part of its Harmony Connect offering.

During the evaluation period for this Magic Quadrant, Check Point released new Quantum Lightspeed appliances, management appliances, midsize/branch firewalls and its "Titan" software release. It also enhanced CloudGuard Workload support to support OpenShift and Docker, while adding microsegmentation.

Strengths

- **Platform strategy:** Check Point offers complementary product lines, which help customers avoid operational complexities and threat coordination gaps that result from managing too many security vendors. All its products can be managed through its cloud-based centralized manager, Infinity Portal.
- **Data center use case:** Check Point has particular traction with large organizations that have large data centers and that appreciate the licensing flexibility and scalability inherent to the Maestro hyperscale line.
- **Pricing:** Check Point's pricing models are favorable for both large- and midsize-enterprise customers. Check Point offers subscription-based pricing to enable large enterprises to avoid major capital expenditure. A single SKU offering for midsize enterprises provides a wide range of security products in one bundle.
- **Advanced threat detection:** Check Point ThreatCloud coordinates malware discovery and intelligence across Check Point's various products and services. Check Point has one of the largest libraries of IPS signatures. It also has a large signature-based database to detect client-side applications.

Cautions

- **Sales and marketing execution:** Check Point is lacking in proactive presales teams, compared with its direct competitors. It also lacks awareness marketing, which results in potential customers looking elsewhere because they are unaware of Check Point's product strategy and updated product portfolio.
- **Product execution:** Check Point's cloud security posture management (CSPM) is not integrated with its on-premises firewall central management offerings.
- **Advanced networking:** Check Point's firewalls lack built-in SD-WAN capabilities. The vendor partners with SD-WAN providers for its FWaaS offering.
- **Product features:** Although Check Point has a large database of malicious URL threat intelligence, it does not support dynamic classification of uncategorized websites. This shortcoming creates operational complexity.

Cisco

Cisco is a Challenger in this Magic Quadrant. Cisco has a large product portfolio and its firewalls are often sold as a part of large deals.

Cisco is an infrastructure vendor. It has different firewall product lines for different deployment use cases: the Cisco Secure Firewall, Cisco Adaptive Security Appliance (ASA), Cisco Secure Workload and Cisco Meraki series. In addition, Cisco offers the Umbrella Secure Internet Gateway (SIG) for FWaaS, and industrial firewalls (the Secure Firewall Industrial Security Appliance [ISA] series).

Major updates in 2021 and 2022 have included native support for TLS 1.3 decryption; support for Cisco Secure Firewall Threat Defense in Alibaba Cloud and Alkira; and the cloud-delivered Secure Firewall Management Center. Cisco also added a managed subscription service for VPN, which enables Cisco to manage scale and change for users, with options including Umbrella SIG support.

Strengths

- **IoT/industrial control system (ICS) security:** Cisco offers IoT security, having formed a partnership with Rockwell to secure ICSs. Cisco has a dedicated IoT research team within the Cisco Talos Intelligence Group. Cisco Secure Firewalls receive building management and medical asset information from Cisco Digital Network Architecture's (DNA's) endpoint analytics.
- **Licensing:** Cisco has a diverse, flexible collection of licensing agreements that allow organizations to deploy whichever Cisco security solutions make sense for their use cases, in deals with favorable commercial terms.
- **Customer feedback:** Clients consider the SecureX cloud-based threat correlation solution platform included with Cisco products a strength. They praise Cisco for continuing to deliver above-average technical support.
- **Distributed-office use case:** Cisco offers Meraki firewalls to connect remote offices. These firewalls benefit from tight integration with Cisco Umbrella for SASE use cases. Ease of deployment is enabled by zero-touch provisioning, which also provides connectivity assurance with VPN monitoring. Cisco also offers a dedicated FWaaS offering through Cisco Umbrella.

Cautions

- **Multiple firewall product lines:** Cisco's firewall portfolio is confusing, with overlapping product capabilities. This can result in deployment of products with different operating systems, which increases learning curves and slows effectiveness.
- **Container firewall:** Cisco lacks a dedicated containerized firewall offering to protect containers. It offers the Cisco Secure Workload microsegmentation product line for container security.
- **Sales execution:** Cisco Secure Firewalls are generally sold as a part of bigger Cisco enterprise license agreement (ELA) deals and lack visibility in pure firewall deals. Although Cisco Meraki MX firewalls are popular for the distributed-office use case, Gartner does not see Cisco firewalls preferred on clients' shortlists for other use cases, such as cloud firewalls and data centers.
- **Customer feedback:** We hear feedback from Gartner clients that Cisco's reseller partners are not recommending Cisco Secure Firewalls because of legacy instability issues and buggy firmware. The firewall management GUI is a work in progress, and some Cisco clients report that the firewall management is comparatively weak. Additionally, clients find Cisco Secure Firewalls expensive when purchased outside an ELA deal.

Forcepoint

Forcepoint is a Niche Player in this Magic Quadrant. It offers firewalls focused on the distributed-office use case but missing features such as FWaaS and cloud-based management. It is mainly considered by distributed enterprises that are looking for appliance-based SD-WAN-enabled firewalls for their sites.

Forcepoint offers Forcepoint ONE (a security service edge [SSE] platform) and network security and data security products. Forcepoint Next-Gen Firewall (NGFW) is the name of its firewall product line.

Major feature updates during the past year related to Forcepoint's firewalls have included support for more public cloud platforms, improved application inspection performance, and the addition of remote browser isolation (RBI) capabilities and subscriptions, and content disarm and reconstruction (CDR) capabilities. Forcepoint has also introduced new firewall models for remote and branch offices.

Strengths

- **Distributed-office use case:** Forcepoint firewalls have built-in advanced SD-WAN capabilities with full IPv6 support, advanced dynamic routing and mature VPN management controls, and active-active clustering. These make them attractive for distributed offices.
- **Integration with Forcepoint ONE:** Forcepoint offers cloud-based service-chaining-based integration through an EasyConnect feature between Forcepoint firewalls and Forcepoint ONE. Features such as RBI and CDR integration strengthen its firewalls' advanced threat detection and prevention capabilities.
- **Mature application control:** Forcepoint offers mature application control, DLP and URL filtering features. Along with support for dynamic categorization of uncategorized sites, service chaining with Forcepoint ONE CASB (a cloud access security broker) makes application control more granular.
- **Customer feedback:** Forcepoint's on-premises firewall manager, the NGFW Security Management Center (SMC), is frequently praised by customers. It is a strong firewall management platform with granular management, zero-touch provisioning, VPN management and logging capabilities.

Cautions

- **Features:** Forcepoint lacks FWaaS features desirable for branch offices and roaming users. Its firewalls have limited IoT protocol support. It does not offer support for 5G on appliances.
- **Visibility:** Forcepoint is not highly visible on the pure-firewall shortlists seen by Gartner, including those for distributed offices, at a time when more vendors are supporting this use case. Forcepoint also lacks visibility for cloud firewall use cases. Additionally, it lacks a dedicated container firewall.
- **Different endpoint agents:** Forcepoint offers two separate endpoint agents, namely the Endpoint Context Agent (ECA) for Forcepoint NGFW and the Forcepoint ONE Endpoint for its SSE solution. This makes it a less attractive vendor for customers looking for ease of management and consolidation.
- **Pricing strategy:** Despite having a large product portfolio, Forcepoint does not offer ELA contracts that cover its firewall product line and other products. The resulting licensing complexity and lack of ELA-based discounting discourages customers from consolidating on Forcepoint.

Fortinet

Fortinet is a Leader in this Magic Quadrant. It leads for appliance-based distributed-office use cases, thanks to its offer of mature SD-WAN and firewall capabilities in a single box.

Fortinet is a network security vendor with a large product portfolio. In addition to FortiGate, its firewall product, Fortinet offers SASE, networking and security operations products.

Major firewall-related updates in 2022 have included the introduction of ZTNA, an in-line sandbox and an in-line CASB. Fortinet has also enabled further integration between FortiGate and its network access control (FortiNAC), and introduced a security operations center (SOC) as a service, offered as a bundle with a FortiGate license.

Strengths

- **Integrated SD-WAN:** Fortinet offers built-in advanced SD-WAN and routing capabilities in FortiGate firewall appliances. Fortinet offers a complete SD-WAN package, with features including forward error correction, packet duplication, and intelligent and dynamic app routing.
- **Hybrid ZTNA deployment:** Fortinet offers flexible ZTNA deployment modes. ZTNA enforcement is part of the FortiGate operating system (FortiOS) and can be deployed on-premises or as a service as part of FortiSASE (a stand-alone offering). The vendor has also introduced an in-line CASB integrated with ZTNA capabilities.
- **Product portfolio:** Fortinet has a large product portfolio. It offers products for networking, network security and security operations. The majority of its products can be managed through a single management interface and offer integration through the Fortinet Security Fabric.
- **Centralized management:** Fortinet offers mature on-premises and cloud-based centralized management through FortiManager and FortiCloud, respectively. These offerings have feature parity and support centralized management of the majority of Fortinet's devices. FortiGate customers like the ease of management and configuration of Fortinet's firewalls.

Cautions

- **Customer feedback:** Feedback from some Gartner clients indicates that FortiGate firewalls do not lead in terms of price/performance. Clients that shortlist Fortinet for midsize-enterprise and data center use cases find its offerings to be more expensive than those of competitors.
- **Dedicated container firewall:** FortiGate lacks a native containerized firewall to protect container workloads. It offers container security through its FortiGate-VM firewalls and Calico integration.
- **Integrated FWaaS offering:** Fortinet lacks an integrated FWaaS offering. It offers FWaaS through FortiSASE as a dedicated product line, without any integration with FortiGate firewalls. FortiSASE comes with a dedicated management interface. Integration of FortiGate's built-in SD-WAN capability with FortiSASE is also lacking.
- **Visibility:** Fortinet appears less frequently on shortlists for cloud firewall and FWaaS use cases than its direct competitors. Fortinet is still considered primarily for its hardware firewall offering.

H3C

H3C is a Niche Player in this Magic Quadrant. It offers a full range of hardware firewalls, known as the SecPath series, for small, midsize and large environments. HC3 focuses on the Chinese market. It offers limited support

for cloud providers outside China.

H3C has a diverse portfolio of security products, which includes offerings for the XDR, EDR, distributed denial of service (DDoS) and web application firewall (WAF) market segments. H3C CloudSecPath Firewall Service is its FWaaS offering. H3C is a good choice for enterprises looking for a security stack focused on the Chinese market.

Major updates in the past year have included new appliances in the F100, F1000, F5000 and M9000 lines. H3C has also enhanced its advanced threat detection and prevention features by adding support for dynamic authorization, encrypted transmission and sensitive data protection.

Strengths

- **Scalability:** H3C's firewalls enable highly scalable deployments. Up to 4,096 virtual instances are supported on H3C's hardware appliances. H3C CloudSecPath Firewall Service offers high capacity, with H3C claiming that it supports 200GB of throughput for 200,000 users.
- **Product portfolio:** H3C has a large security portfolio, which is chosen by many enterprises seeking consolidation. H3C offers products such as SecCenter CSAP for endpoint protection and CSAP Threat Discovery for XDR, which make it a desirable vendor for consolidation in China.
- **Firewall deployment modes:** H3C offers a complete firewall product line, including hardware firewall, virtual firewall, FWaaS, containerized firewall and industrial firewall. As a result, it is a good choice for enterprises seeking to consolidate on a single vendor for different firewall deployment modes.
- **Pricing:** H3C's pricing gives it a good five-year TCO, compared with many other vendors. Support is priced reasonably at only 10% of the list price. Some features, such as DLP, are included at no extra cost.

Cautions

- **Cloud-firewall-supported platforms:** H3C offers a cloud firewall for VMware and H3C cloud environments but lacks support for regional cloud providers like Alibaba and Huawei. It also lacks support for AWS, Microsoft Azure and Google Cloud Platform (GCP). H3C offers a container firewall, but it requires NGINX for enforcement.
- **Regional support:** H3C's firewalls rely on partnerships with regional vendors for VPN authentication and EDR integration. H3C offers granular social media controls for mainly local apps, such as WeChat and QQ, and limited support for applications such as Microsoft Office 365.
- **Centralized management:** The firewall central manager can scale to manage only a limited number of devices, as compared with H3C's direct competitors. The platform lacks support for zero-touch provisioning of branch firewalls.
- **Geographic presence:** The majority of H3C's sales are to the Chinese market and a few parts of Southeast Asia. It lacks presence in other regions.

Hillstone Networks

Hillstone Networks is a Visionary in this Magic Quadrant. It is well-suited to fulfill midsize-enterprise use cases in Asia/Pacific and to some Latin American customers, especially cloud-first organizations.

Hillstone's network firewall products are part of its edge protection product family. Hillstone's main offering is a network firewall, but it also offers microsegmentation, endpoint and server security, a WAF, an application delivery controller (ADC), XDR and DLP.

Hillstone has recently released several new hardware and virtual firewalls, as well as a virtual firewall that integrates with VMware NSX-T. New features include DNS security and a cloud data lake.

Strengths

- **Cloud-focused product strategy:** Hillstone has a cloud-first strategy that supports AWS, Microsoft Azure, GCP and Alibaba Cloud, as well as multiple China-based public clouds. Hillstone offers a microsegmentation solution and CloudArmour, a container firewall that can work in Kubernetes environments.
- **Advanced features:** Hillstone's ZTNA capabilities are integrated into all its network firewalls. A Hillstone NGFW acts as the ZTNA gateway, while a Hillstone SSL VPN client can be upgraded to a ZTNA endpoint. An additional subscription license is required to activate the ZTNA feature. Hillstone does ZTNA enforcement on the firewall.
- **IoT security:** Hillstone's IoT security can proactively detect IoT devices such as webcams, multimedia players and game consoles. It can provide risk analysis and control, and threat detection for traffic associated with these IoT assets, as inclusive features.
- **Geographic strategy:** Hillstone is using its strength in China to fund targeted sales opportunities in other regions. The number of Hillstone customers in Latin America and North America is small but growing.

Cautions

- **Cloud security:** Hillstone integrates with several public clouds using Hillstone virtual appliances, but does not offer CSPM to manage cloud-native firewall policies. Nor does it manage native security controls in SDN infrastructures such as VMware NSX and Cisco Application Centric Infrastructure (ACI).
- **Product strategy:** Hillstone's IPS capabilities are undifferentiated. Hillstone has a relatively small threat research team to develop custom rules for "in the wild" threats. Relative to most competitors, Hillstone has a small client-based application database, which limits the breadth of its Layer 7 awareness.
- **Price/performance:** Although Hillstone's firewall appliance prices may seem low, they are not low compared with those of many competitors. Throughput on the lowest-end firewalls is very low, and data center firewall prices are relatively high, considering the volume of traffic they can process.
- **Customer feedback:** Hillstone clients identify a lack of high-throughput and high-performing hardware devices as a weakness, compared with other Chinese regional vendors within the Chinese market.

Huawei

Huawei is a Challenger in this Magic Quadrant. A large product portfolio makes Huawei a desirable vendor for customers who want to consolidate. Huawei has different firewalls for different use cases. It often wins deals based on its price/performance.

Huawei is a large infrastructure vendor with a diverse product portfolio. Its firewalls, which include the USG series for enterprise and the Eudemon series for carriers, are part of its network security product portfolio.

Major updates in 2022 relating to Huawei's firewalls have included enhancements to routing, SD-WAN and sandboxing capabilities.

Strengths

- **Scalability:** Huawei has a large base of carrier and data center customers. As a result, it offers highly scalable appliances. Of all the vendors evaluated in this Magic Quadrant, Huawei offers support for the most virtual firewall instances in its dedicated hardware appliance models and scalable management console.
- **Cloud-native firewall:** Huawei offers a cloud-native firewall service for Huawei Cloud, as well as a container firewall service called the Container Guard Service (only for Huawei Cloud). The container firewall offers features such as container runtime security and image security with vulnerability management. It can be managed from a centralized console within Huawei Cloud.
- **Advanced threat detection:** Huawei offers threat correlation capabilities between its firewall, native EDR and XDR platforms. Clients can also utilize managed detection and response (MDR) services offered directly by Huawei, which are sold as Qiankun Border Protection and Response.
- **Pricing:** Huawei's firewalls have a competitive price/performance ratio. Their TCO is one of the lowest in the market. Huawei often wins deals on this basis.

Cautions

- **Regional partnerships:** Huawei's partners are mostly limited to Chinese companies. For example, its ZTNA offering can integrate with Bamboo Cloud's IAM solution, while, for EDR, Huawei has partnered with Jiangmin and Leagsoft.
- **Offerings outside Huawei Cloud:** Although Huawei offers virtual cloud firewall, container firewall and microsegmentation products, these are primarily for Huawei Cloud. Only recently has Huawei partnered with Microsoft Azure for a cloud firewall.
- **IoT security:** Huawei firewalls offer only basic IoT-related security. They lack features such as IoT discovery. Huawei only offers limited signature-based protection of regular IoT vulnerabilities through the IPS signature database in its firewalls.
- **ELA:** Despite having a large product portfolio, Huawei does not offer ELA-based deals. An ELA would make deals involving multiple years and multiple products easier for customers to understand and accept.

Juniper

Juniper is a Challenger in this Magic Quadrant. It has a broad firewall line covering many use cases and deployment types, including FWaaS and container firewalls. We typically see Juniper firewalls shortlisted along with Juniper networking products, which limits their market penetration.

Juniper offers a broad range of products, including networking and security products. It offers appliance-based firewalls in the SRX, vSRX and cSRX product lines. It also has a FWaaS offering. Other products provide security information and event management, DDoS mitigation and threat intelligence.

Recent updates have included the introduction of Security Director Cloud, Secure Edge (an SSE product) and Cloud Workload Protection. Juniper has also gained a cloud-based network access control product with the acquisition of WiteSand.

Strengths

- **Firewall deployment use cases:** Juniper's firewall product line, the SRX series, includes hardware appliances and virtual appliances (vSRX) with native mature SD-WAN support. A FWaaS is provided with the Secure Edge product, and a full-featured containerized firewall is included in the cSRX line.
- **Platform approach:** Juniper offers a single console to manage all its security products through its Security Director and Security Director Cloud. Juniper also offers Advanced Threat Prevention and SecIntel as shared threat intelligence offerings between its networking and firewall product lines.
- **IoT and OT security:** Juniper has demonstrated a focus on IoT security by enhancing its automated device fingerprinting and control. Partnership with Dragos and SEL provide threat detection and response capabilities for industrial applications within OT and SCADA environments.
- **Scalability:** Juniper offers high-throughput firewalls that maintain good throughput even while decrypting traffic. The Junos Space Security Director and Juniper Security Director Cloud, a centralized manager, can manage up to 25,000 Juniper devices, including firewalls, switches and routers.

Cautions

- **Visibility:** Despite having firewall offerings for all deployment use cases, Juniper is not as visible as its direct competitors on customer shortlists seen by Gartner. Juniper firewalls are shortlisted primarily by telecom carriers or for consolidation with Juniper's other network product lines.
- **Market responsiveness:** The network security market is highly competitive, with aggressive competition between vendors to identify key emerging use cases, such as FWaaS, ZTNA, cloud security, SSE and security operations. Despite being a large network vendor, Juniper has been slow to identify such use cases and to introduce products for them.
- **Product strategy:** Juniper lacks a strong in-house security product portfolio, compared with direct competitors that are expanding their security product offerings aggressively. As a result, Gartner clients do not consider it a desirable candidate for security vendor consolidation.
- **Customer feedback:** Gartner clients identify slow responsiveness and a lack of innovation for emerging security use cases as reasons not to shortlist Juniper. They also find its prices high, relative to those of

competitors. SD-WAN and DLP features are available, but at added cost.

Microsoft

Microsoft is a Niche Player in this Magic Quadrant. Its Azure Firewall is considered mainly by existing Microsoft clients seeking consolidation. Application teams looking for native firewalls for seamless integration with Azure workloads also prefer the Microsoft Azure Firewall.

The Microsoft Azure Firewall is available via two subscriptions: Standard and Premium. It can be centrally managed by Azure Firewall Manager and monitored using Azure Monitor and Microsoft Sentinel.

Microsoft continues to invest in security, as shown by the addition of DDoS management to Azure Firewall Manager and of WAF policies to Azure Firewall Manager. Additionally, Microsoft has added an IPS to its Premium subscription.

Strengths

- **Vendor consolidation:** Microsoft firewalls are widely considered by existing Microsoft customers who want to consolidate on a single vendor. Microsoft offers a range of security services, including Azure Firewall, Azure Web Application Firewall and Azure Active Directory, which can be deployed together.
- **Ease of use:** Microsoft Azure Firewall integrates seamlessly with other Azure-hosted services. It is less complex than third-party firewalls to deploy, as it is an in-line offering with inbuilt sizing and scaling.
- **Sales execution:** Microsoft has capitalized on customers' shifting of workloads to Azure by offering a simple firewall that meets basic needs. Gartner is seeing clients consider Azure Firewall for Azure workloads, and this Microsoft offering frequently competes with products from dedicated firewall vendors.
- **Customer experience:** Users identify ease of deployment as the leading reason to use Microsoft Azure Firewall. A strong secondary reason is its tight integration with the Azure ecosystem, which assists DevOps. Customers also appreciate Microsoft's credibility as a vendor and its support for the product.

Cautions

- **Innovation:** Microsoft is focused on integrating Azure Firewall with native Azure offerings, and lags behind in terms of introducing features to support emerging cloud firewall use cases. It lacks a dedicated container firewall offering. Microsegmentation is handled via security tags, rather than a firewall product.
- **Feature gaps:** Microsoft Azure Firewall lacks multiple features that are desirable in a cloud firewall and that are offered by competitors. There is no support for IPv6, no sandbox and no signature-based application control.
- **Performance:** Network traffic throughput drops by 90% when an IPS with TLS is enabled. Microsoft does, however, provide an option to add sites manually to the list in order to bypass TLS decryption.
- **Customer feedback:** Customers indicate that the Premium firewall subscription is expensive, documentation is subpar, with a lack of training material, and logging lacks support for debugging issues.

Palo Alto Networks

Palo Alto Networks is a Leader in this Magic Quadrant. It has the most visible firewall for different firewall use cases, judging from Gartner client inquiries. With the recent introduction of the PA-400 series, Palo Alto Networks' firewalls have become good candidates for use by midsize enterprises.

Palo Alto Networks is a security vendor with a large product portfolio. In addition to its most popular firewall product line, the PA-Series, the vendor has SSE, cloud security and security operations product lines.

Major firewall-related updates over the past year have included the release of two major firmware releases with enhancements to URL filtering, DNS security, IoT security and threat prevention. The vendor has also introduced AIOps and enhanced the DLP features of its firewalls.

Strengths

- **Product portfolio:** Palo Alto Networks has a large product portfolio. Gartner often sees contracts from this vendor for multiple product lines, in addition to firewalls. Prisma Access (SASE) and Cortex Data Lake (XDR) are frequently shortlisted along with firewalls.
- **Deployment modes:** Palo Alto Networks supports multiple forms of firewall deployment, with its PA-Series (hardware firewalls), VM-Series (virtual firewalls), Prisma Access (FWaaS), Cloud NGFW (a cloud-native firewall for AWS) and CN-Series (containerized firewalls). This makes it a good choice for hybrid environments, where clients want a single firewall provider.
- **Advanced security features:** Palo Alto Networks' firewalls score highly for advanced security features. The vendor offers strong threat detection and prevention capabilities. Its IoT Security subscription offers autodiscovery of IoT devices. Palo Alto Networks also offers advanced DNS security and 5G security features.
- **FWaaS:** Palo Alto Networks' FWaaS offering, Prisma Access, continues to mature and supports full SSE capabilities, including a secure web gateway (SWG), a CASB and ZTNA. It can be managed as a plug-in for Panorama (an on-premises centralized manager) or as a stand-alone cloud-based management offering.

Cautions

- **Technical support:** Gartner has received consistent feedback from Palo Alto Networks customers indicating a decline in the quality of its technical support, with especially long escalation cycles being associated with Level 1 support. As a result, customers often feel the need to upgrade their support to a higher tier that offers a faster SLA but is more expensive.
- **Cloud-based manager:** Palo Alto Networks' cloud-based firewall manager, used for distributed-office and centralized-management use cases, is not on a par with on-premises management. Its cloud-based manager is used primarily for the Prisma Access product line and "generation 4" models of hardware.
- **Customer feedback:** A few Gartner clients have reported connectivity and routing issues with Prisma Access services. This feedback comes particularly from users of its FWaaS and of the GlobalProtect service of Prisma Access (as it relates to firewall clients).

- **Opacity of ELA contracts:** Palo Alto Networks offers multiple types of license, such as an ELA and credit-based licenses, but its quotations often lack transparency. They mostly include bulk pricing and lack clarity in terms of itemized part numbers with itemized costs.

Sangfor Technologies

Sangfor Technologies is a Visionary in this Magic Quadrant. This China-based vendor appeals to enterprises in Asia/Pacific and EMEA (especially the Middle East) that want to consolidate their security products by using a single vendor.

Sangfor's network firewall products are all part of the Next Generation Application Firewall (NGAF) product line, which also includes WAF functionality. In addition to network firewalls, Sangfor has a broad range of security offerings for WAAP, SASE, ZTNA, IAM, endpoint security, microsegmentation and cloud workload protection.

Sangfor has recently released several new hardware firewall appliances. New features include a cloud deception subscription to improve attack detection. Sangfor also offers a fully integrated network firewall with its ZTNA and SASE products.

Strengths

- **Platform approach:** Sangfor builds products that can be managed together. Its Platform-X cloud management platform can manage Sangfor's network firewall, Endpoint Secure and microsegmentation solutions, together with Sangfor's SWG and SD-WAN capabilities.
- **IoT security:** As part of its Essential License Suite, Sangfor offers differentiated IoT signatures, including support for IP camera protocols. Sangfor supports IoT asset classification, access control, protocol identification and control, weak-password detection and IoT vulnerability detection on surveillance networks.
- **Scalability:** Sangfor Central Manager, the vendor's on-premises central management appliance, is highly scalable. A large number of devices can be administered from a single console.
- **Pricing strategy:** As a vendor with many large customers, Sangfor uses its ELA as a strategic product packaging tool. It typically offers heavy discounts, flexible terms on virtual firewall deployments, and new product additions during the ELA term, with a true-up at renewal time.

Cautions

- **Advanced networking:** Sangfor's firewalls lack 5G support. This is a significant shortcoming for customers in China, several other Asia/Pacific countries and parts of the Middle East, where 5G infrastructure is mainly found.
- **Public cloud integration:** Sangfor lacks integration with the Microsoft Azure and GCP public clouds that are popular in many regions.
- **Threat detection:** Sangfor has fewer IPS signatures than other firewall vendors evaluated in this Magic Quadrant, and no machine learning analysis is performed in conjunction with the IPS to improve detection efficacy. In addition, Sangfor lacks integration with third-party tools to improve malware detection.

- **Geographic strategy:** Sangfor has very little presence outside Asia and the Middle East. Other regional competitors evaluated in this Magic Quadrant are more often considered and deployed in Latin America.

SonicWall

SonicWall is a Niche Player in this Magic Quadrant. It is a strong candidate for selection by midsize enterprises, for which it offers strong security and represents good value. Its native SD-WAN capabilities with a FWaaS make it a good choice for distributed-office and remote access use cases.

SonicWall offers three hardware appliance firewall product lines — the TZ, NSa and NSsp series — and a virtual appliance firewall product line, the NSv series. In addition to firewalls, SonicWall sells integrated EDR, secure email gateway, ZTNA and CASB capabilities.

Recent updates include enhancements to the centralized manager, including rule optimization and SD-WAN workflow to simplify provisioning of branch-office firewalls. SonicWall has also introduced centralized management for SonicWall Switch, SonicWave Wireless Access Points and SonicWall Capture Client.

Strengths

- **Distributed-office use case:** SonicWall offers native SD-WAN capabilities in all its firewall models and the SonicWall Network Security Manager. It also offers Cloud Edge Secure Access, a SASE offering with FWaaS, ZTNA, network access control and CASB features desirable for the distributed-office use case.
- **Pricing:** SonicWall offers competitive pricing, which makes it a good choice for midsize enterprises. SD-WAN functionality is included in all its appliances at no additional cost. DLP functionality is part of the base package, also with no additional cost.
- **Customer feedback:** Customers have praised SonicWall's single management interface for managing different SonicWall products. Additionally, they have identified low TCO as a reason to choose SonicWall firewalls.
- **Centralized management:** SonicWall's Capture Security Center (CSC) is a "single pane of glass" management portal for SonicWall products, including its firewalls and Cloud Edge Secure Access offering. It simplifies administration.

Cautions

- **Visibility:** Gartner sees SonicWall primarily on the firewall shortlists of midsize enterprises. It lacks visibility for other use cases, especially the distributed-office use case (despite having native SD-WAN capabilities and an FWaaS offering) and the data center use case.
- **Product features:** SonicWall supports only limited virtual instances — desirable for data center use cases — on its hardware appliances. It supports fewer categories of web application than other vendors evaluated in this Magic Quadrant. SonicWall lacks a native XDR offering; instead, it offers integration with third-party XDR platforms.
- **Cloud firewall:** SonicWall's support for public clouds lags behind that of other vendors in this Magic Quadrant, with support for only AWS and Microsoft Azure; there is no support for GCP. A pay-as-you-go option is not

available for Azure. SonicWall lacks a container firewall and a microsegmentation offering.
- **Customer feedback:** SonicWall clients have indicated that the firewall product's reporting capabilities are limited and lack granularity. They have also experienced long delays after contacting technical support.

Sophos

Sophos is a Niche Player in this Magic Quadrant. Its product strategy and platform-based approach, focused on the needs of midsize enterprises, offer strong integration between its firewalls and EDR. Sophos is gradually expanding its cloud security product lines.

Sophos has network security, endpoint security, cloud security and MDR offerings. Its firewall offerings come under different product lines. Sophos' firewalls and Intercept X endpoint security offering are its most popular products.

Major firewall-related updates over the past year have included the introduction of the Sophos XGS series of hardware firewalls, and the launch of a Sophos ZTNA offering and new software subscriptions. Sophos has also improved XGS performance and enhanced SD-WAN orchestration.

Strengths
- **Platform approach:** Sophos offers its firewall, EDR and XDR as a unified platform with strong integration, centralized management and correlation capabilities. It offers a single cloud console with a single endpoint agent to manage both products.
- **Midsize-enterprise use case:** Sophos' strategy and sales execution focuses on midsize enterprises. In addition to consolidating its firewall and EDR functionality, Sophos has introduced managed threat response and rapid response services for clients looking to outsource MDR services.
- **Cloud-based centralized manager:** Sophos offers a single, cloud-based centralized manager to manage all its products. This makes management easier.
- **Customer feedback:** Customers often identify Sophos' customer support and mature product documentation as key strengths. Sophos has introduced context-sensitive help, guided tutorials and embedded how-to videos to further improve the product administration experience.

Cautions
- **Visibility:** Sophos is generally visible to midsize enterprises, but is less commonly used for other firewall use cases. This is despite Sophos having a separate offering for ZTNA and a cloud firewall that includes a container firewall.
- **ELA:** Despite having a broad product portfolio, Sophos does not offer ELA pricing, even though this is desired by clients aiming to consolidate products with the same vendor. Instead, Sophos offers a simpler multiyear consumption model.
- **Features:** Sophos does not offer a FWaaS, even though one is desirable for use cases involving branch offices and roaming users. It also lacks support for 5G in its firewalls, which are SD-WAN-enabled.

287

- **Customer feedback:** As competition between vendors grows in the midsize-enterprise market, some Gartner clients find Sophos expensive, compared with other vendors that sell to midsize enterprises.

WatchGuard

WatchGuard is a Niche Player in this Magic Quadrant. It delivers firewalls for midsize-enterprise and distributed-enterprise use cases. In addition to the Firebox firewall, WatchGuard has a virtual appliance (FireboxV) and a virtual appliance designed specifically for public cloud environments (Firebox Cloud).

WatchGuard Dimension is this vendor's on-premises firewall management solution. All WatchGuard security products can be managed by WatchGuard Cloud, its cloud-based console. Other products in WatchGuard's security portfolio offer multifactor authentication (MFA), secure Wi-Fi and endpoint security.

WatchGuard has recently released several new firewall hardware appliances. Examples of new features include Firebox integration with WatchGuard's MFA and secure Wi-Fi products, and load-sharing capabilities for the vendor's on-firewall SD-WAN functionality.

Strengths

- **Product strategy:** In the past few years, WatchGuard has switched from a traditional value-added reseller (VAR)-based go-to-market strategy to a managed service provider (MSP)-focused strategy. This refocus has led the vendor to make WatchGuard Cloud service-provider-friendly and easy to use, while also being scalable across multiple end-user customers per service provider.
- **Endpoint integration:** WatchGuard's Firebox firewall is managed in conjunction with its endpoint security products. The vendor has a process called ThreatSync that collects event data from WatchGuard firewalls, endpoint sensors and threat intelligence feeds, analyzes the collective data, and assigns threat scores.
- **OT security:** WatchGuard has a ruggedized network firewall that is sometimes used in certain manufacturing and utility environments. The vendor also includes SCADA signatures in its Basic Security Suite and Total Security Suite feature bundles.
- **Pricing strategy:** Under the FlexPay licensing model, WatchGuard offers the choice to purchase its firewalls using upfront payments, WatchGuard Points or WatchGuard pay-as-you-go, which is unique in the traditional capital-expenditure-based firewall appliance market.

Cautions

- **IaaS security:** WatchGuard has public-cloud-friendly firewalls only for AWS and Microsoft Azure. In this regard it lags behind most competitors, which usually support three or more infrastructure as a service (IaaS) providers. The lack of GCP support limits WatchGuard's opportunities to serve "born in the cloud" midsize enterprises, which sometimes choose Google as their infrastructure provider.
- **FWaaS and ZTNA:** Many small and midsize Gartner clients inquire about FWaaS as an alternative to traditional branch-office firewalls. WatchGuard, however, does not offer a FWaaS. It also lacks a ZTNA offering.

- **Product strategy:** WatchGuard lacks offerings for emerging cloud security use cases, such as containerized firewall and microsegmentation. As a result, it lacks visibility in shortlists seen by Gartner, beyond those of midsize organizations looking for hardware firewalls.
- **Advanced networking:** At the time of this analysis, WatchGuard has not delivered any 5G-supporting firewalls. This limits its uptake in many regions that have built extensive 5G infrastructure.

Vendors Added and Dropped

We review and adjust our inclusion criteria for Magic Quadrants as markets change. As a result of these adjustments, the mix of vendors in any Magic Quadrant may change over time. A vendor's appearance in a Magic Quadrant one year and not the next does not necessarily indicate that we have changed our opinion of that vendor. It may be a reflection of a change in the market and, therefore, changed evaluation criteria, or of a change of focus by that vendor.

Added

None.

Dropped

- Cato Networks
- Versa Networks

Inclusion and Exclusion Criteria

The inclusion criteria represent the specific attributes that Gartner analysts thought it necessary for vendors to have in order to be included in this Magic Quadrant.

Vendors of network firewall functions covered by the Market Definition/Description section were considered for evaluation in this Magic Quadrant under the following conditions:

- Vendors must have hardware/virtual appliances or cloud-native firewalls as their primary firewall products.
- Vendors must have presence at least in three of the following regions, including their home region: Asia/Pacific, North America, Latin America, Europe, Middle East.
- Vendors offering a hardware appliance/virtual appliance as their primary firewall product offering must have generated at least $70 million in hardware appliance/virtual appliance firewall-only revenue in 2021.
- Vendors must have a track record of meeting the needs of public cloud use cases.
- Gartner analysts must have assessed that the vendors can effectively compete in the network firewall market.
- Gartner analysts must have determined that the vendors are significant players in the network firewall market, due to their market presence, competitive visibility or technological innovation.

- Vendors must have the ability to meet more than one network firewall deployment use case mentioned in the Market Definition/Description section.
- Public cloud vendors must have a dedicated firewall offering.

Exclusion criterion:

- Gartner considered vendors that offer FWaaS as their primary firewall product line to be ineligible for inclusion in this Magic Quadrant.

Evaluation Criteria

Ability to Execute

Gartner analysts evaluate vendors on the quality and efficacy of the processes, systems, methods or procedures that enable their performance to be competitive, efficient and effective, and to positively impact revenue, retention and reputation. The following criteria are used to evaluate vendors' Ability to Execute.

Product or Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Subcriteria:

- Ability of product to meet the needs of, and specialize in, different network firewall use cases.
- Platform approach.
- Support is evaluated by the quality, breadth and value of an offering (or offerings) specifically in relation to enterprise and cloud use cases.

Overall Viability:

Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness of the sales channel.

Subcriteria:

- Customer feedback on pricing.

290

- Transparency of contracts.
- Bundled-pricing models that are clear and easy to understand.
- Competitive TCO.
- Strong presale and postsale support and services.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Subcriteria:

- Timely introduction of new features to meet customers' requirements.
- Ability to support emerging use cases, such as SASE, cloud security and IoT security.
- Timely partner integrations to support customers' demands.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Subcriteria:

- Visibility of the vendor on clients' shortlists.
- Extent to which end users are migrating away from the vendor.
- Extent to which the vendor's marketing faces direct competition.
- End users' awareness of the vendor's brand.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

The most important factor is customer satisfaction throughout the sales and product life cycle. Also important are ease of use, platform approach, centralized management and protection against the latest attacks. Trending feedback — positive or negative — on a vendor's product(s) or support — is weighted highly as well.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Table 1: Ability to Execute Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Product or Service	High
Overall Viability	Medium
Sales Execution/Pricing	Medium
Market Responsiveness/Record	High
Marketing Execution	Medium
Customer Experience	High
Operations	Medium

Source: Gartner (December 2022)

Completeness of Vision

Gartner analysts evaluate vendors on their ability to convincingly articulate logical statements about a market's current and future direction, innovation, customer needs and competitive forces. They assess how well these statements correspond to Gartner's view of the market.

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Subcriteria:

- Ability to understand and add features in response to customers' requirements for different use cases.
- Ability to understand and respond to customers' product- and market-related requirements.
- Ability to meet timelines imposed by customers' requirements.
- Support for hybrid environments and different firewall deployment use cases, platform approach, centralized management and visibility, cloud security, cloud workload protection, and automation.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Subcriteria:

- Ability to provide clear messaging that resonates with customers' use cases and requirements.
- Ability to communicate effectively with sales and distribution channels, end users and different kinds of buyers on features, product firmware, vision and focus on evolving use cases, in order to build a brand.
- Strong, clear messaging on evolving use cases.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates to extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Subcriteria:

- Effective sales and pricing models to meet the requirements of clients for different deployment use cases.
- Clear and transparent pricing models.
- A comprehensive channel and partner strategy to sell to multiple deployment use cases.
- Approach to the network security and/or cloud workload buying center.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Subcriteria:

- Development of strong features to enhance threat prevention.
- Integrated features and automation, rather than a broad product portfolio with overlapping products.
- Strong features and enforcements to support all the network firewall use cases.

- Mature product integrations with partners to enhance network firewall capabilities for environments featuring, for example, OT, branches/campuses, cloud security and work-from-home users.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Subcriteria:

- Platform approach.
- Strong vision and exceptional features for particular firewall deployment use cases.
- Feature maturity.
- Integration with overlapping products.
- Use of technology to detect and prevent threats.
- Exceptional, differentiating features and innovation to support one or more network firewall use cases.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Table 2: Completeness of Vision Evaluation Criteria

Evaluation Criteria ↓	*Weighting* ↓
Market Understanding	High
Marketing Strategy	Medium
Sales Strategy	Medium
Offering (Product) Strategy	High

Evaluation Criteria ↓	Weighting ↓
Business Model	Medium
Vertical/Industry Strategy	NotRated
Innovation	High
Geographic Strategy	Medium

Source: Gartner (December 2022)

Quadrant Descriptions

Leaders

The Leaders quadrant contains vendors that can shape the market by being the first to introduce additional capabilities and raise awareness of the importance of those capabilities. Leaders have the potential to meet enterprises' requirements for multiple firewall use cases in a single platform solution.

Leaders offer new features that protect customers from emerging threats. They meet the requirements of evolving hybrid networks, including public and private clouds. They provide expert capabilities, rather than treating firewalls as commodities. They have a good track record of avoiding vulnerabilities in their security products.

Leaders offer innovative features to simplify configuration and management of firewall policies across hybrid environments. They commonly have the ability to handle the highest throughputs with minimal performance loss. Additionally, they often offer options for hardware acceleration, support for private and public cloud platforms, and form factors that protect enterprises as they move to new infrastructure form factors. Leaders offer the first features and capabilities to support emerging firewall use cases in depth. They take an integrated platform approach, instead of having multiple different product lines for different use cases with a lack of integration.

In addition to providing technology that is a good match for customers' current requirements, Leaders exhibit superior vision and execution with regard to likely future requirements and the evolution of hybrid networks.

Challengers

Challengers have sound reseller channels and customers, but do not consistently lead with differentiated next-generation capabilities. Many Challengers have not fully matured their firewall capabilities. They may have other security products that are successful in the enterprise sector and may be counting on their existing relationships with customers, rather than their firewall products, to win deals.

Challengers' products are often well-priced and, because of strong execution, these vendors can offer economical security product bundles that many others cannot.

Many Challengers hold themselves back from becoming Leaders by giving their security or firewall products a lower priority within their overall product sets.

Challengers often have significant market shares, but may trail those with smaller market shares when it comes to releasing new features.

Visionaries

Visionaries lead in terms of innovation, but are limited to one or two firewall deployment use cases. They have the right designs and features, but lack the sales base, strategy or financial means to compete consistently with Leaders and Challengers. Sometimes, Visionaries have made a conscious decision to focus on a limited number of firewall use cases. Most Visionaries' products have good next-generation firewall capabilities, but are lacking in terms of performance and support networks.

Visionaries show strong vision and market-leading innovation in relation to, among other things, securing work-from-home users, ensuring the security of workloads, enabling east-west segmentation in public cloud and software-defined networking environments, and automating threat detection.

Niche Players

Most Niche Players have a primary installed base for, or prominence in, a particular use case, such as those involving data centers, telcos, distributed enterprises, midsize enterprises and public IaaS. Some Niche Players that offer a firewall as a module, along with other services or components, focus on a particular use case.

Niche Players are lacking in terms of Ability to Execute because of their limited client bases, and they tend not to show much innovation. Some are confined to particular regions.

Context

As networks evolve, network firewall vendors continue to expand their product portfolios to cover overlapping security markets and attract buyers seeking consolidation. However, buying from the same vendor does not necessarily guarantee simplicity and centralized management.

Appliance-based firewalls remain relevant for multiple firewall use cases. Hardware appliance renewals continue to be pretty stable. There is demand for high-throughput hardware firewalls, especially for data center and enterprise perimeter use cases.

296

FWaaS is in growing demand for remote use cases, whether they involve branch offices or homes. Consolidation is also apparent in this regard, with SSE, which combines CASB, ZTNA and SWG functionality, becoming more of a requirement. Branches with high throughput requirements or compliance limitations continue to choose hardware appliances for the branch-office use case. (Stand-alone FWaaS vendors do not appear in this year's Magic Quadrant, as demand for their products is insufficient to warrant inclusion.)

Vendors innovating for cloud security use cases are gaining traction, as there is a strong demand for cloud firewalls (both cloud-native firewalls and container firewalls). Hence we include cloud service providers in this Magic Quadrant.

The sales execution/pricing criterion is weighted significantly because of consistent feedback from clients about its importance and frequent increases in the prices of network firewalls. More complex contracts, higher renewal costs and higher TCO are causing dissatisfaction among clients.

Market Overview

The network firewall market remains one of the largest security markets, and has been evolving along with the broader security market. As a result, multiple factors now drive the network firewall market.

The rise of hybrid environments is the key factor behind vendors' introduction of multiple firewall deployment types, such as FWaaS and cloud-native. There is growing demand to secure on-premises environments, multiple cloud environments and remote users with firewalls.

Interest in zero trust is favoring the selection of single firewall vendors that can help enterprises achieve a ZTNA, so that they do not have to use multiple vendors. Clients expect mature integration capabilities when purchasing overlapping technologies from the same vendor.

There is huge interest in visibility and control of east-west segmentation policies and enhanced security operation integrations.

Advanced security capabilities remain a key driving factor, as threat vectors are using more sophisticated means of attacking hybrid workforces and cloud networks. Most vendors are trying to develop or acquire products that offer these capabilities, but they face strong competition from best-of-breed vendors that offer granular capabilities for this specific use case.

The network firewall market has evolved to include the following segments, each of which has a specific set of features:

- **Cloud firewalls:** These firewalls from cloud infrastructure vendors are designed for cloud-native deployment as separate virtual instances or in containers. Container firewalls can also secure connections between containers.
- **Hybrid mesh firewalls:** These are platforms that help secure hybrid environments by extending modern network firewall controls to multiple enforcement points, including FWaaS and cloud firewalls, with centralized management via a single cloud-based manager.

- **Firewall as a service (FWaaS):** A FWaaS is a multifunction security gateway delivered as a cloud-based service, often to protect small branch offices and mobile users.

Other key observations about this market:

- Customers continue to give negative feedback about the increasing price of network firewall offerings. Only regional vendors seem to be offering simple and competitive pricing. Other vendors continue to increase their prices regularly.
- Advanced threat detection and prevention remains an important shortlisting criterion. Network firewall vendors have been enhancing their features in this area, with key enhancements relating to IoT security and DNS security.
- More vendors have introduced cloud firewall offerings, although these have differing levels of maturity. Container firewalls are still offered by only a limited number of vendors.
- Vendors may identify the introduction of FWaaS offerings as a priority, but more are introducing ZTNA and/or SWGs first.
- Although vendors claim strong integration between their network firewalls and other overlapping product lines, Gartner finds these integrations to be very basic.
- Data center network firewall vendors continue to introduce higher-performing boxes.
- All the firewall vendors evaluated in this Magic Quadrant offer native SD-WAN capabilities in their firewall appliances.
- As midsize enterprises are becoming hybrid-environment organizations, their need for mature security is prompting a rise in security budgets. As a result, midsize-enterprise firewall use cases seem to be growing, with more vendors introducing appliances and bundled licensing to attract these enterprises. There is now strong competition to win their business.

Evaluation Criteria Definitions

Ability to Execute

Product/Service: Core goods and services offered by the vendor for the defined market. This includes current product/service capabilities, quality, feature sets, skills and so on, whether offered natively or through OEM agreements/partnerships as defined in the market definition and detailed in the subcriteria.

Overall Viability: Viability includes an assessment of the overall organization's financial health, the financial and practical success of the business unit, and the likelihood that the individual business unit will continue investing in the product, will continue offering the product and will advance the state of the art within the organization's portfolio of products.

Sales Execution/Pricing: The vendor's capabilities in all presales activities and the structure that supports them. This includes deal management, pricing and negotiation, presales support, and the overall effectiveness

of the sales channel.

Market Responsiveness/Record: Ability to respond, change direction, be flexible and achieve competitive success as opportunities develop, competitors act, customer needs evolve and market dynamics change. This criterion also considers the vendor's history of responsiveness.

Marketing Execution: The clarity, quality, creativity and efficacy of programs designed to deliver the organization's message to influence the market, promote the brand and business, increase awareness of the products, and establish a positive identification with the product/brand and organization in the minds of buyers. This "mind share" can be driven by a combination of publicity, promotional initiatives, thought leadership, word of mouth and sales activities.

Customer Experience: Relationships, products and services/programs that enable clients to be successful with the products evaluated. Specifically, this includes the ways customers receive technical support or account support. This can also include ancillary tools, customer support programs (and the quality thereof), availability of user groups, service-level agreements and so on.

Operations: The ability of the organization to meet its goals and commitments. Factors include the quality of the organizational structure, including skills, experiences, programs, systems and other vehicles that enable the organization to operate effectively and efficiently on an ongoing basis.

Completeness of Vision

Market Understanding: Ability of the vendor to understand buyers' wants and needs and to translate those into products and services. Vendors that show the highest degree of vision listen to and understand buyers' wants and needs, and can shape or enhance those with their added vision.

Marketing Strategy: A clear, differentiated set of messages consistently communicated throughout the organization and externalized through the website, advertising, customer programs and positioning statements.

Sales Strategy: The strategy for selling products that uses the appropriate network of direct and indirect sales, marketing, service, and communication affiliates that extend the scope and depth of market reach, skills, expertise, technologies, services and the customer base.

Offering (Product) Strategy: The vendor's approach to product development and delivery that emphasizes differentiation, functionality, methodology and feature sets as they map to current and future requirements.

Business Model: The soundness and logic of the vendor's underlying business proposition.

Vertical/Industry Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of individual market segments, including vertical markets.

Innovation: Direct, related, complementary and synergistic layouts of resources, expertise or capital for investment, consolidation, defensive or pre-emptive purposes.

Geographic Strategy: The vendor's strategy to direct resources, skills and offerings to meet the specific needs of geographies outside the "home" or native geography, either directly or through partners, channels and subsidiaries as appropriate for that geography and market.

Learn how Gartner can help you succeed

Become a Client

© 2024 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by **Gartner's Usage Policy**. Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "**Guiding Principles on Independence and Objectivity**." Gartner research may not be used as input into or for the training or development of generative artificial intelligence, machine learning, algorithms, software, or related technologies.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

GartnerReprint

Traducido del inglés al español - www.onlinedoctranslator.com

Cuadrante mágico para firewalls de red

19 de diciembre de 2022 - ID G00761497 - 55 min de lectura

Por Rajpreet Kaur, Adam Hils,**y 1 más**

A medida que los firewalls de red evolucionan hacia firewalls de malla híbridos con la aparición de firewalls en la nube y ofertas de firewall como servicio, seleccionar el proveedor más adecuado se convierte en un desafío. Gartner evalúa a 17 proveedores para ayudar a los líderes en seguridad y gestión de riesgos a tomar la decisión correcta para su organización.

Supuestos de planificación estratégica

Para 2026, más del 60% de las organizaciones tendrán más de un tipo de implementación de firewall, lo que impulsará la adopción de firewalls de malla híbridos.

Para 2026, más del 30 % de las nuevas implementaciones de firewalls distribuidos en sucursales serán ofertas de firewall como servicio, frente a menos del 10 % en 2022.

Definición/Descripción del mercado

Gartner define el mercado de firewalls de red como el mercado de firewalls que utilizan inspección bidireccional de tráfico con estado (tanto de entrada como de salida) para proteger las redes. Los firewalls de red se implementan mediante hardware, dispositivos virtuales y controles nativos de la nube.

Los firewalls de red se utilizan para proteger las redes. Estas pueden ser locales, híbridas (locales y en la nube), de nube pública o privada. Los firewalls de red son compatibles con diferentes casos de implementación, como perímetros, medianas empresas, centros de datos, nubes, oficinas nativas de la nube y distribuidas.

Las capacidades de los firewalls de red incluyen redes avanzadas, inspección y detección de amenazas y filtrado web.

Capacidades principales:

- Redes:Esto incluye soporte para tablas de enrutamiento con capacidad de traducción de direcciones de red de destino (DNAT) y traducción de direcciones de red estática (SNAT).
- Inspección de estado:Esto permite la inspección del tráfico basándose en reglas de firewall con estado.

- Detección e inspección de amenazas:Esto incluye un sistema de prevención de intrusiones (IPS) y capacidades de inspección de malware.
- Filtrado web:Esto incluye el filtrado del tráfico saliente para HTTP y HTTPS y aplicaciones.
- Registro e informes avanzados:Se pueden registrar todas las acciones de los administradores de firewall, y se pueden personalizar y generar informes según diferentes tipos de objetos y tipos de tráfico. Se pueden generar informes granulares basados en amenazas y filtrado web.

Capacidades opcionales:

- Seguridad del Internet de las cosas (IoT):Esto se logra mediante un módulo integrado en los controles de detección de amenazas o mediante una suscripción dedicada integrada en las ofertas de firewall de red. Las funciones específicas pueden incluir la detección de dispositivos IoT, el análisis de riesgos y reglas específicas para bloquear ataques relacionados con estos dispositivos. Además, las firmas IoT forman parte de la base de firmas IPS.
- Sandbox de red:El sandbox de red monitorea el tráfico de red en busca de objetos sospechosos y los envía automáticamente al entorno sandbox, donde se analizan y se les asignan puntajes de probabilidad de malware y clasificaciones de gravedad.
- Acceso a la red de confianza cero (ZTNA):El acceso a la red de confianza cero (ZTNA) posibilita un límite de acceso basado en la identidad y el contexto entre cualquier usuario y dispositivo y las aplicaciones.
- Seguridad de la tecnología operativa (OT):Esto incluye funciones integradas o dedicadas a la protección de un entorno OT. No se consideran aquí las soluciones de seguridad OT independientes. Las funciones pueden incluir inteligencia de amenazas específica para OT, firmas IPS específicas para dispositivos OT, compatibilidad con aplicaciones de control de supervisión y adquisición de datos (SCADA) e inspección de amenazas.
- Seguridad del sistema de nombres de dominio (DNS):Esto protege el tráfico al DNS al ofrecer capacidades de monitoreo, detección y prevención contra ataques a la capa DNS.
- Red de área amplia definida por software (SD-WAN):Esto proporciona una selección de ruta dinámica, basada en políticas comerciales o de aplicaciones, políticas centralizadas y administración de dispositivos, red privada virtual (VPN) y configuración sin intervención.

Cuadrante mágico

Figura 1: Cuadrante mágico para firewalls de red



Fuente: Gartner (diciembre de 2022)

Fortalezas y precauciones de los proveedores

Nube de Alibaba

Alibaba Cloud es un competidor en este Cuadrante Mágico. Su firewall de Alibaba Cloud es una solución de firewall en la nube más consolidada que la de sus competidores, proveedores directos de servicios en la nube (CSP), con funciones como control de aplicaciones, filtrado de URL y prevención avanzada de amenazas. También ofrece firewalls para casos de uso emergentes en la nube, como firewalls de contenedores y microsegmentación, exclusivamente dentro de sus servicios.

Alibaba Cloud es un proveedor de servicios en la nube con una amplia cartera de productos. Ofrece un sólido conjunto de controles de seguridad. Alibaba Cloud Firewall es su solución de firewall nativo en la nube.

Alibaba Cloud ha implementado importantes actualizaciones en la capacidad de visualización del tráfico de su firewall y la introducción de un firewall DNS. También ha ampliado sus puntos de presencia (POP) a más regiones fuera de China.

Strengths
Fortalezas

- Compatibilidad con casos de uso emergentes de firewall en la nube:Alibaba Cloud ofrece un módulo de firewall de contenedores avanzado, Alibaba Security Center-Container Firewall, que ofrece seguridad de imágenes y de aplicaciones en tiempo de ejecución. Además, Alibaba Cloud Firewall ofrece capacidades de microsegmentación avanzadas como parte de su licencia avanzada.

- Cartera de productos y capacidad de respuesta al mercado:Alibaba Cloud es un gran proveedor de servicios de comunicaciones (CSP) con una amplia cartera de productos. Está fuertemente enfocado en expandir su oferta de seguridad y destaca por su alta capacidad de respuesta al mercado, en comparación con sus competidores directos de CSP.

- Cliente de punto final unificado:Alibaba Cloud ofrece un único cliente para sus productos de firewall, VPN, acceso seguro al borde del servicio (SASE) y detección y respuesta de endpoints (EDR), lo que facilita la gestión y la consolidación de proveedores. Tanto los productos de firewall en la nube como los de EDR se pueden gestionar de forma centralizada desde el Centro de Seguridad de Alibaba.

- Detección avanzada de amenazas:Alibaba Cloud Firewall ofrece funciones de detección y respuesta de red (NDR), con integración entre Alibaba EDR y Alibaba Cloud Security Center, su plataforma de detección y respuesta extendida (XDR). Los clientes también pueden contratar un servicio de seguridad gestionado directamente. Alibaba Cloud también ofrece un firewall DNS dedicado para la seguridad DNS.

Cautions

- Control de aplicaciones:Si bien Alibaba Cloud ofrece un sólido soporte para aplicaciones regionales, además de la capacidad de prevención de pérdida de datos (DLP), sus firewalls no son compatibles con aplicaciones como Microsoft Office 365, ampliamente utilizadas fuera de China. Por lo tanto, los clientes fuera de China deben comparar el control de aplicaciones de Alibaba Cloud con las aplicaciones que utilizan antes de tomar una decisión de compra.

- Presencia geográfica:Alibaba Cloud tiene una importante presencia en China, pero rara vez figura en las listas de clientes de otros países. Por ello, su estrategia de producto se centra en las necesidades chinas.

- Asociaciones con terceros:La estrategia de Alibaba Cloud consiste en crear sus propias ofertas nativas. Por lo tanto, solo cuenta con asociaciones regionales limitadas. No ofrece integración de firewall con soluciones de EDR, XDR ni de gestión de identidades y acceso (IAM) de terceros.

- Características:Alibaba Cloud Firewall no es compatible con el descifrado de Seguridad de la Capa de Transporte (TLS). Tampoco cuenta con enrutamiento y redirección de tráfico basados en nombres de dominio completos (FQDN) ni con funciones de seguridad para IoT.

Servicios web de Amazon

Amazon Web Services (AWS) es un actor de nicho en este Cuadrante Mágico. AWS Network Firewall, un firewall nativo en la nube, ofrece funciones básicas, en comparación con las de otros proveedores de firewalls de red. También existen servicios de firewall como servicio (FWaaS) de terceros que los clientes pueden adquirir a través de AWS Marketplace, incluyendo reglas de firewall gestionadas por socios.

AWS es un proveedor de servicios de comunicaciones (CSP). AWS Network Firewall se ofrece como un servicio totalmente gestionado en la plataforma de nube de AWS. Otras familias de productos de seguridad de AWS incluyen IAM, protección de redes y aplicaciones, protección de datos, respuesta a incidentes y cumplimiento normativo.

Entre las características recientes más importantes desarrolladas para AWS Network Firewall se incluyen una protección este-oeste mejorada (inspección de tráfico entre subredes en la misma nube privada virtual), reglas de denegación/eliminación predeterminadas, opciones de configuración de ordenamiento de reglas estrictas y compatibilidad con AWS Firewall Manager para una implementación centralizada.

Strengths

- Experiencia del cliente:AWS Network Firewall destaca por su alta disponibilidad y escalado automatizado. Además, a los clientes les gusta la función de personalización mediante las reglas administradas de AWS. Consideran la facilidad de uso de estas funciones integrales como la principal razón para elegir AWS Network Firewall.
- Precios:Los clientes valoran la simplicidad del modelo de precios de AWS Network Firewall. Pagan por la cantidad de firewalls implementados y el volumen de tráfico procesado. Todos los clientes reciben soporte básico gratuito.
- Escalabilidad:El rendimiento, la alta disponibilidad y la escalabilidad de AWS Network Firewall ofrecen ventajas distintivas con respecto a las ofertas de otros proveedores de firewalls. Ofrece alta disponibilidad integrada para garantizar que todo el tráfico se inspeccione y monitorice de forma consistente.
- Facilidad de implementación:La facilidad de implementación se logra a través de muchas características diferentes en el administrador de firewall de AWS, como el aprovisionamiento automático de firewall, la capacidad de implementar firewalls automáticamente en todas las cuentas y la implementación sin intervención.

Cautions

- Estrategia de producto:El firewall de red de AWS se queda atrás en cuanto a funcionalidades en comparación con la competencia. Por ello, AWS recurre a alianzas con otros proveedores, como Palo Alto Networks, que ofrecen instancias nativas de AWS de firewalls de proveedores asociados para clientes que detectan limitaciones en el firewall de AWS.
- Consolidación:Los clientes de Gartner generalmente no consideran a AWS un proveedor atractivo para la consolidación hacia una arquitectura de confianza cero. AWS carece de una oferta nativa de ZTNA. Su complejo esquema de implementación utiliza AWS Virtual Private Cloud (VPC) para lograr la microsegmentación, lo que limita su atractivo para casos de uso de firewalls emergentes.
- Brechas de características:AWS Network Firewall no admite funciones nativas de traducción de direcciones de red (NAT) ni IPv6. Tampoco detecta aplicaciones basadas en cliente y carece de control granular de aplicaciones.
- Detección avanzada de amenazas:El firewall de red de AWS ofrece menos firmas propietarias investigadas por el proveedor que otros firewalls. Además, AWS carece de descifrado TLS en su firewall.

Barracuda

Barracuda es un visionario en este Cuadrante Mágico. Ofrece una gama de dispositivos de firewall enfocados en oficinas distribuidas y dispositivos virtuales para nubes públicas dentro de la línea de productos CloudGen Firewall. La conectividad de sucursales es un mercado clave para Barracuda.

Las ofertas de seguridad de Barracuda incluyen firewalls, protección de aplicaciones web y API (WAAP), puertas de enlace web seguras, ZTNA (para acceso remoto a aplicaciones privadas) y puertas de enlace de correo electrónico seguras.

Las actualizaciones recientes de la línea de firewalls de Barracuda incluyen funciones de seguridad para IoT, OT y la nube. Barracuda, por ejemplo, ha añadido funciones de inspección de IPS, URL, contenido, antivirus y SSL (Secure Sockets Layer) a su producto CloudGen WAN.

Strengths

- Características de la nube y de las sucursales:La línea de productos CloudGen Firewall de Barracuda ofrece una integración sólida con los controles nativos de AWS y Microsoft Azure. Barracuda ha añadido CloudGen WAN, un producto FWaaS, para abordar los casos de teletrabajo y teletrabajo. Barracuda también ha introducido el Conector Seguro para la conectividad IoT con Microsoft Azure, totalmente gestionable a través de CloudGen WAN.

- Modos de implementación de firewall:Barracuda ha entregado productos para todos los modos de firewall principales: CloudGen Firewall para hardware y virtual; CloudGen WAN para FWaaS; Secure Connector para firewall en contenedores; y CloudGen Firewall (resistente) para requisitos de firewall industrial.

- Precios:Los dispositivos de gama baja de Barracuda ofrecen un excelente coste total de propiedad (TCO). El sistema de licencias basado en pools del proveedor permite a los administradores asignar licencias de software entre plataformas según sea necesario.

- Características de IoT:Barracuda ha aumentado su capacidad para proteger entornos IoT mediante alianzas con Crosser, Nozomi Networks y SCADAfence. Barracuda también colabora con Crosser para ejecutar lógica de computación en el borde de la red en algunos dispositivos de firewall.

Cautions

- Virtualización:Los dispositivos de hardware de Barracuda no aíslan algunas funciones, como VPN, Protocolo de configuración dinámica de host (DHCP), caché DNS e intercepción DNS, cuando se ejecutan múltiples instancias virtuales en el mismo dispositivo.

- Múltiples portales de gestión:Las consolas de administración independientes son exclusivas de sus entornos. El producto FWaaS, CloudGen WAN, debe administrarse a través de la plataforma de administración en la nube de Barracuda. Los dispositivos físicos y virtuales de CloudGen deben administrarse con un administrador de firewall local llamado Barracuda Firewall Admin.

- Estrategia de producto:Barracuda carece de EDR nativo y ofrece una integración limitada con proveedores de seguridad de endpoints y redes. Si bien ofrece capacidad IPS, utiliza tecnología de Trend Micro como OEM. Todas las firmas IPS son desarrolladas por terceros, y la cantidad de firmas es inferior a la de la competencia.

- Comentarios de los clientes:Los comentarios de los clientes indican que Barracuda ofrece informes limitados sobre los módulos de filtrado de contenido y que la gestión de productos es una tarea compleja.

Tecnologías de software Check Point

Check Point Software Technologies es líder en este Cuadrante Mágico. Ha sido seleccionado para casos de uso de firewalls independientes por clientes empresariales. Además de firewalls, Check Point ofrece una amplia gama de funciones de seguridad con una gestión centralizada basada en la nube. Esto lo convierte en un candidato ideal para organizaciones que buscan una solución de plataforma de seguridad.

Check Point ofrece una cartera completa de seguridad que incluye dispositivos de hardware de la marca Quantum y la línea de productos de hiperescala Maestro. Check Point integra su FWaaS en su oferta Harmony Connect.

Durante el período de evaluación de este Cuadrante Mágico, Check Point lanzó nuevos dispositivos Quantum Lightspeed, dispositivos de gestión, firewalls para sucursales y medianas empresas, y su versión de software "Titan". También mejoró la compatibilidad con CloudGuard Workload para OpenShift y Docker, e incorporó la microsegmentación.

Strengths

- Estrategia de plataforma:Check Point ofrece líneas de productos complementarias que ayudan a los clientes a evitar las complejidades operativas y las brechas de coordinación de amenazas que resultan de gestionar demasiados proveedores de seguridad. Todos sus productos se pueden gestionar a través de su gestor centralizado en la nube, Infinity Portal.
- Caso de uso del centro de datos:Check Point tiene una tracción particular entre las grandes organizaciones que tienen grandes centros de datos y que aprecian la flexibilidad de licencias y la escalabilidad inherentes a la línea de hiperescala Maestro.
- Precios:Los modelos de precios de Check Point son favorables tanto para grandes como para medianas empresas. Check Point ofrece precios por suscripción para que las grandes empresas eviten grandes gastos de capital. Una única oferta de SKU para medianas empresas ofrece una amplia gama de productos de seguridad en un solo paquete.
- Detección avanzada de amenazas:Check Point ThreatCloud coordina la detección de malware y la inteligencia en los diversos productos y servicios de Check Point. Check Point cuenta con una de las bibliotecas de firmas IPS más grandes del mundo. También cuenta con una extensa base de datos de firmas para detectar aplicaciones del lado del cliente.

Cautions

- Ejecución de ventas y marketing:Check Point carece de equipos de preventa proactivos, en comparación con sus competidores directos. También carece de marketing de concienciación, lo que provoca que los clientes potenciales busquen en otra parte por desconocimiento de la estrategia de productos de Check Point y su portafolio actualizado.
- Ejecución del producto:La gestión de la postura de seguridad en la nube (CSPM) de Check Point no está integrada con sus ofertas de gestión centralizada de firewall local.
- Redes avanzadas:Los firewalls de Check Point carecen de capacidades SD-WAN integradas. El proveedor colabora con proveedores de SD-WAN para su oferta FWaaS.
- Características del producto:Aunque Check Point cuenta con una extensa base de datos de inteligencia sobre amenazas de URL maliciosas, no admite la clasificación dinámica de sitios web sin categorizar. Esta deficiencia genera complejidad operativa.

Cisco

Cisco es un competidor en este Cuadrante Mágico. Cisco cuenta con una amplia cartera de productos y sus firewalls suelen venderse como parte de grandes acuerdos.

Cisco es un proveedor de infraestructura. Ofrece diferentes líneas de firewalls para distintos casos de uso: Cisco Secure Firewall, Cisco Adaptive Security Appliance (ASA), Cisco Secure Workload y la serie Cisco Meraki. Además, Cisco ofrece Umbrella Secure Internet Gateway (SIG) para FWaaS y firewalls industriales (la serie Secure Firewall Industrial Security Appliance [ISA]).

Las principales actualizaciones de 2021 y 2022 incluyen compatibilidad nativa con el descifrado TLS 1.3; compatibilidad con Cisco Secure Firewall Threat Defense en Alibaba Cloud y Alkira; y el Secure Firewall Management Center en la nube. Cisco también añadió un servicio de suscripción gestionada para VPN, que permite a Cisco gestionar la escalabilidad y los cambios para los usuarios, con opciones que incluyen compatibilidad con Umbrella SIG.

Strengths
Fortalezas

- Seguridad del sistema de control industrial (ICS)/IoT:Cisco ofrece seguridad para IoT, tras haber establecido una alianza con Rockwell para proteger los ICS. Cisco cuenta con un equipo de investigación dedicado a IoT dentro del Grupo de Inteligencia Cisco Talos. Los firewalls seguros de Cisco reciben información sobre la gestión de edificios y los activos médicos del análisis de endpoints de la Arquitectura de Red Digital (DNA) de Cisco.

- Licencia:Cisco tiene una colección diversa y flexible de acuerdos de licencia que permiten a las organizaciones implementar cualquier solución de seguridad de Cisco que tenga sentido para sus casos de uso, en acuerdos con términos comerciales favorables.

- Comentarios de los clientes:Los clientes consideran la plataforma de correlación de amenazas basada en la nube SecureX, incluida en los productos de Cisco, como una fortaleza. Elogian a Cisco por seguir ofreciendo un soporte técnico excepcional.

- Caso de uso de oficina distribuida:Cisco ofrece firewalls Meraki para conectar oficinas remotas. Estos firewalls se benefician de una estrecha integración con Cisco Umbrella para casos de uso SASE. La implementación es sencilla gracias al aprovisionamiento automático, que también garantiza la conectividad con la monitorización de VPN. Cisco también ofrece una solución FWaaS dedicada a través de Cisco Umbrella.

Cautions
Cautions

- Varias líneas de productos de firewall:La cartera de firewalls de Cisco es confusa, con capacidades de producto superpuestas. Esto puede resultar en la implementación de productos con diferentes sistemas operativos, lo que aumenta la curva de aprendizaje y reduce la eficacia.

- Firewall de contenedores:Cisco no cuenta con un firewall contenedorizado dedicado para proteger los contenedores. Ofrece la línea de productos de microsegmentación Cisco Secure Workload para la seguridad de los contenedores.

- Ejecución de ventas:Los firewalls seguros de Cisco se suelen vender como parte de acuerdos de licencia empresarial (ELA) más amplios de Cisco y carecen de visibilidad en acuerdos de firewalls puros. Si bien los firewalls Cisco Meraki MX son populares para oficinas distribuidas, Gartner no considera que los firewalls Cisco sean una opción preferida por los clientes para otros casos de uso, como firewalls en la nube y centros de datos.

- Comentarios de los clientes:Hemos recibido comentarios de clientes de Gartner que indican que los socios distribuidores de Cisco no recomiendan los firewalls seguros de Cisco debido a problemas de inestabilidad heredados y firmware defectuoso. La interfaz gráfica de usuario (GUI) de administración del firewall está en desarrollo, y algunos clientes de Cisco informan que su administración es comparativamente deficiente. Además, los clientes consideran que los firewalls seguros de Cisco son caros cuando se adquieren fuera de un acuerdo ELA.

Punto de fuerza

Forcepoint es un actor de nicho en este Cuadrante Mágico. Ofrece firewalls enfocados en el caso de uso de oficinas distribuidas, pero carece de funciones como FWaaS y administración en la nube. Es considerado principalmente por empresas distribuidas que buscan firewalls basados en dispositivos y compatibles con SD-WAN para sus sitios.

Forcepoint ofrece Forcepoint ONE (una plataforma de seguridad perimetral [SSE]) y productos de seguridad de red y de datos. Su línea de firewalls se denomina Forcepoint Next-Gen Firewall (NGFW).

Las principales actualizaciones de funciones de los firewalls de Forcepoint realizadas el año pasado incluyen compatibilidad con más plataformas de nube pública, un mejor rendimiento de la inspección de aplicaciones y la incorporación de funciones y suscripciones de aislamiento remoto de navegador (RBI), así como funciones de desarmado y reconstrucción de contenido (CDR). Forcepoint también ha introducido nuevos modelos de firewall para oficinas remotas y sucursales.

Strengths
Fortalezas

- Caso de uso de oficina distribuida:Los firewalls Forcepoint incorporan funciones SD-WAN avanzadas con compatibilidad total con IPv6, enrutamiento dinámico avanzado, controles de gestión de VPN consolidados y agrupación en clústeres activo-activo. Esto los hace atractivos para oficinas distribuidas.

- Integración con Forcepoint ONE:Forcepoint ofrece integración en la nube mediante encadenamiento de servicios mediante la función EasyConnect entre los firewalls Forcepoint y Forcepoint ONE. Funciones como la integración con RBI y CDR refuerzan las capacidades avanzadas de detección y prevención de amenazas de sus firewalls.

- Control de aplicaciones maduras:Forcepoint ofrece funciones avanzadas de control de aplicaciones, DLP y filtrado de URL. Además de la compatibilidad con la categorización dinámica de sitios web no categorizados, el encadenamiento de servicios con Forcepoint ONE CASB (un agente de seguridad de acceso a la nube) permite un control de aplicaciones más granular.

- Comentarios de los clientes:El administrador de firewall local de Forcepoint, el Centro de Gestión de Seguridad (SMC) de NGFW, recibe frecuentes elogios de los clientes. Es una sólida plataforma de gestión de firewall con gestión granular, aprovisionamiento automático, gestión de VPN y capacidades de registro.

Cautions
Cautions

- Características:Forcepoint carece de las funciones FWaaS deseables para sucursales y usuarios itinerantes. Sus firewalls tienen una compatibilidad limitada con el protocolo IoT. No ofrece compatibilidad con 5G en sus dispositivos.

- Visibilidad:Forcepoint no tiene una alta visibilidad en las listas de firewalls puros que Gartner ha analizado, incluyendo las de oficinas distribuidas, en un momento en que más proveedores están apoyando este caso de uso. Forcepoint también carece de visibilidad para los casos de uso de firewall en la nube. Además, carece de un firewall dedicado para contenedores.

- Diferentes agentes de punto final:Forcepoint ofrece dos agentes de endpoint independientes: el Endpoint Context Agent (ECA) para Forcepoint NGFW y Forcepoint ONE Endpoint para su solución SSE. Esto lo convierte en un proveedor menos atractivo para los clientes que buscan facilidad de gestión y consolidación.

- Estrategia de precios:A pesar de contar con una amplia cartera de productos, Forcepoint no ofrece contratos ELA que cubran su línea de firewalls y otros productos. La complejidad resultante de las licencias y la falta de descuentos basados en ELA desalientan a los clientes a consolidarse en Forcepoint.

Fortinet

Fortinet es líder en este Cuadrante Mágico. Es líder en casos de uso de oficinas distribuidas basadas en dispositivos, gracias a su oferta de capacidades de SD-WAN y firewall consolidadas en un solo dispositivo.

Fortinet es un proveedor de seguridad de redes con una amplia cartera de productos. Además de FortiGate, su firewall, Fortinet ofrece productos SASE, de redes y de operaciones de seguridad.

Las principales actualizaciones de firewall en 2022 incluyeron la introducción de ZTNA, un sandbox en línea y un CASB en línea. Fortinet también ha facilitado una mayor integración entre FortiGate y su sistema de control de acceso a la red (FortiNAC), e introdujo un centro de operaciones de seguridad (SOC) como servicio, que se ofrece como paquete con una licencia de FortiGate.

Strengths Fortalezas

- SD-WAN integrada:Fortinet ofrece funciones avanzadas de SD-WAN y enrutamiento integradas en los firewalls FortiGate. Fortinet ofrece un paquete completo de SD-WAN, con funciones como corrección de errores de reenvío, duplicación de paquetes y enrutamiento inteligente y dinámico de aplicaciones.
- Implementación híbrida de ZTNA:Fortinet ofrece modos flexibles de implementación de ZTNA. La implementación de ZTNA forma parte del sistema operativo FortiGate (FortiOS) y puede implementarse localmente o como servicio dentro de FortiSASE (una oferta independiente). El proveedor también ha presentado un CASB en línea integrado con las capacidades de ZTNA.
- Portafolio de productos:Fortinet cuenta con una amplia cartera de productos. Ofrece productos para redes, seguridad de red y operaciones de seguridad. La mayoría de sus productos se pueden gestionar mediante una única interfaz de administración y ofrecen integración a través de Fortinet Security Fabric.
- Gestión centralizada:Fortinet ofrece una gestión centralizada sólida, tanto local como en la nube, a través de FortiManager y FortiCloud, respectivamente. Estas soluciones ofrecen paridad de funciones y permiten la gestión centralizada de la mayoría de los dispositivos Fortinet. Los clientes de FortiGate valoran la facilidad de gestión y configuración de los firewalls de Fortinet.

Cautions Precauciones

- Comentarios de los clientes:Los comentarios de algunos clientes de Gartner indican que los firewalls FortiGate no son líderes en relación precio/rendimiento. Los clientes que seleccionan Fortinet para medianas empresas y centros de datos consideran que sus ofertas son más caras que las de la competencia.
- Firewall de contenedores dedicado:FortiGate no cuenta con un firewall contenedorizado nativo para proteger las cargas de trabajo en contenedores. Ofrece seguridad para contenedores mediante sus firewalls FortiGate-VM y la integración con Calico.
- Oferta FWaaS integrada:Fortinet carece de una oferta integrada de FWaaS. Ofrece FWaaS a través de FortiSASE como una línea de productos dedicada, sin integración con los firewalls FortiGate. FortiSASE incluye una interfaz de gestión dedicada. La integración de la capacidad SD-WAN integrada de FortiGate con FortiSASE también es deficiente.
- Visibilidad:Fortinet aparece con menos frecuencia en las listas de candidatos para casos de uso de firewall en la nube y FWaaS que sus competidores directos. Fortinet sigue siendo considerado principalmente por su oferta de firewall de hardware.

H3C

H3C es un actor de nicho en este Cuadrante Mágico. Ofrece una gama completa de firewalls de hardware, conocidos como la serie SecPath, para entornos pequeños, medianos y grandes. HC3 se centra en el mercado chino. Ofrece soporte limitado.

para proveedores de nube fuera de China.

H3C cuenta con una cartera diversa de productos de seguridad, que incluye soluciones para los segmentos de mercado XDR, EDR, denegación de servicio distribuido (DDoS) y firewall de aplicaciones web (WAF). El servicio de firewall H3C CloudSecPath es su oferta FWaaS. H3C es una excelente opción para empresas que buscan una solución de seguridad enfocada en el mercado chino.

Las principales actualizaciones del último año han incluido nuevos dispositivos en las líneas F100, F1000, F5000 y M9000. H3C también ha mejorado sus funciones avanzadas de detección y prevención de amenazas, añadiendo compatibilidad con autorización dinámica, transmisión cifrada y protección de datos confidenciales.

Strengths Fortalezas

- Escalabilidad:Los firewalls de H3C permiten implementaciones altamente escalables. Los dispositivos de hardware de H3C admiten hasta 4096 instancias virtuales. El servicio de firewall CloudSecPath de H3C ofrece alta capacidad; H3C afirma que admite 200 GB de rendimiento para 200 000 usuarios.
- Portafolio de productos:H3C cuenta con una amplia cartera de seguridad, elegida por muchas empresas que buscan consolidación. Ofrece productos como SecCenter CSAP para la protección de endpoints y CSAP Threat Discovery para XDR, lo que la convierte en un proveedor atractivo para la consolidación en China.
- Modos de implementación de firewall:H3C ofrece una línea completa de firewalls, que incluye firewalls de hardware, firewalls virtuales, FWaaS, firewalls en contenedores y firewalls industriales. Por ello, es una excelente opción para empresas que buscan consolidar sus servicios en un único proveedor para diferentes modos de implementación de firewalls.
- Precios:El precio de H3C le ofrece un buen TCO a cinco años, en comparación con muchos otros proveedores. El soporte tiene un precio razonable, tan solo el 10 % del precio de lista. Algunas funciones, como DLP, se incluyen sin coste adicional.

Cautions Precauciones

- Plataformas compatibles con firewall en la nube:H3C ofrece un firewall en la nube para entornos de nube de VMware y H3C, pero no es compatible con proveedores regionales de nube como Alibaba y Huawei. Tampoco es compatible con AWS, Microsoft Azure y Google Cloud Platform (GCP). H3C ofrece un firewall para contenedores, pero requiere NGINX para su implementación.
- Soporte regional:Los firewalls de H3C se basan en alianzas con proveedores regionales para la autenticación VPN y la integración de EDR. H3C ofrece controles granulares de redes sociales principalmente para aplicaciones locales, como WeChat y QQ, y compatibilidad limitada con aplicaciones como Microsoft Office 365.
- Gestión centralizada:El administrador central de firewalls puede escalar para gestionar solo un número limitado de dispositivos, a diferencia de los competidores directos de H3C. La plataforma no admite el aprovisionamiento automático de firewalls de sucursales.
- Presencia geográfica:La mayoría de las ventas de H3C se destinan al mercado chino y a algunas zonas del Sudeste Asiático. Carece de presencia en otras regiones.

312

Hillstone Networks es una empresa visionaria en este Cuadrante Mágico. Es ideal para atender casos de uso de empresas medianas en Asia/Pacífico y para algunos clientes latinoamericanos, especialmente organizaciones que priorizan la nube.

Los firewalls de red de Hillstone forman parte de su familia de productos de protección perimetral. Su oferta principal es un firewall de red, pero también ofrece microsegmentación, seguridad de endpoints y servidores, un WAF, un controlador de entrega de aplicaciones (ADC), XDR y DLP.

Hillstone ha lanzado recientemente varios nuevos firewalls de hardware y virtuales, así como un firewall virtual que se integra con VMware NSX-T. Entre las nuevas funciones se incluyen seguridad DNS y un lago de datos en la nube.

Strengths
Fortalezas

- Estrategia de producto centrada en la nube:Hillstone cuenta con una estrategia centrada en la nube, compatible con AWS, Microsoft Azure, GCP y Alibaba Cloud, así como con múltiples nubes públicas con sede en China. Hillstone ofrece una solución de microsegmentación y CloudArmour, un firewall de contenedores compatible con entornos Kubernetes.

- Funciones avanzadas:Las capacidades ZTNA de Hillstone están integradas en todos sus firewalls de red. Un NGFW de Hillstone actúa como puerta de enlace ZTNA, mientras que un cliente SSL VPN de Hillstone puede actualizarse a un punto final ZTNA. Se requiere una licencia de suscripción adicional para activar la función ZTNA. Hillstone implementa la ZTNA en el firewall.

- Seguridad del IoT:La seguridad IoT de Hillstone detecta proactivamente dispositivos IoT como cámaras web, reproductores multimedia y consolas de videojuegos. Ofrece análisis y control de riesgos, así como detección de amenazas para el tráfico asociado a estos activos IoT, como funciones integradas.

- Estrategia geográfica:Hillstone está aprovechando su fortaleza en China para financiar oportunidades de venta específicas en otras regiones. El número de clientes de Hillstone en Latinoamérica y Norteamérica es pequeño, pero está creciendo.

Cautions
Cautions

- Seguridad en la nube:Hillstone se integra con varias nubes públicas mediante dispositivos virtuales de Hillstone, pero no ofrece CSPM para gestionar políticas de firewall nativas de la nube. Tampoco gestiona controles de seguridad nativos en infraestructuras SDN como VMware NSX y Cisco Application Centric Infrastructure (ACI).

- Estrategia de producto:Las capacidades IPS de Hillstone no están diferenciadas. Hillstone cuenta con un equipo de investigación de amenazas relativamente pequeño para desarrollar reglas personalizadas para amenazas "en la naturaleza". En comparación con la mayoría de sus competidores, Hillstone cuenta con una pequeña base de datos de aplicaciones basadas en clientes, lo que limita el alcance de su conocimiento de Capa 7.

- Precio/rendimiento:Aunque los precios de los firewalls de Hillstone puedan parecer bajos, no lo son en comparación con los de muchos competidores. El rendimiento de los firewalls de gama baja es muy bajo, y los precios de los firewalls para centros de datos son relativamente altos, considerando el volumen de tráfico que pueden procesar.

- Comentarios de los clientes:Los clientes de Hillstone identifican la falta de dispositivos de hardware de alto rendimiento y rendimiento como una debilidad, en comparación con otros proveedores regionales chinos dentro del mercado chino.

Huawei

Huawei es un competidor en este Cuadrante Mágico. Su amplia cartera de productos la convierte en un proveedor atractivo para los clientes que buscan consolidarse. Huawei cuenta con diferentes firewalls para distintos casos de uso. Suele conseguir contratos gracias a su relación calidad-precio.

Huawei es un importante proveedor de infraestructura con una cartera de productos diversa. Sus firewalls, que incluyen la serie USG para empresas y la serie Eudemon para operadores, forman parte de su cartera de productos de seguridad de red.

Las principales actualizaciones en 2022 relacionadas con los firewalls de Huawei incluyeron mejoras en las capacidades de enrutamiento, SD-WAN y sandbox.

Strengths
Fortalezas

- Escalabilidad:Huawei cuenta con una amplia base de clientes, entre operadores y centros de datos. Como resultado, ofrece dispositivos altamente escalables. De todos los proveedores evaluados en este Cuadrante Mágico, Huawei ofrece compatibilidad con la mayor cantidad de instancias de firewall virtuales en sus modelos de dispositivos de hardware dedicados y su consola de administración escalable.

- Firewall nativo de la nube:Huawei ofrece un servicio de firewall nativo en la nube para Huawei Cloud, así como un servicio de firewall para contenedores llamado Container Guard Service (solo para Huawei Cloud). Este firewall para contenedores ofrece funciones como seguridad en tiempo de ejecución de contenedores y seguridad de imágenes con gestión de vulnerabilidades. Se puede gestionar desde una consola centralizada dentro de Huawei Cloud.

- Detección avanzada de amenazas:Huawei ofrece capacidades de correlación de amenazas entre su firewall, plataformas nativas EDR y XDR. Los clientes también pueden utilizar los servicios de detección y respuesta gestionadas (MDR) ofrecidos directamente por Huawei, comercializados como Qiankun Border Protection and Response.

- Precios:Los firewalls de Huawei ofrecen una relación precio-rendimiento competitiva. Su TCO es uno de los más bajos del mercado. Huawei suele conseguir contratos gracias a esto.

Cautions
Cautelas

- Asociaciones regionales:Los socios de Huawei se limitan principalmente a empresas chinas. Por ejemplo, su oferta ZTNA puede integrarse con la solución IAM de Bamboo Cloud, mientras que, para EDR, Huawei se ha asociado con Jiangmin y Leagsoft.

- Ofertas fuera de Huawei Cloud:Aunque Huawei ofrece firewalls virtuales en la nube, firewalls de contenedores y productos de microsegmentación, estos están destinados principalmente a Huawei Cloud. Recientemente, Huawei se asoció con Microsoft Azure para desarrollar un firewall en la nube.

- Seguridad del IoT:Los firewalls de Huawei solo ofrecen seguridad básica para IoT. Carecen de funciones como el descubrimiento de IoT. Huawei solo ofrece protección limitada basada en firmas contra vulnerabilidades comunes de IoT a través de la base de datos de firmas IPS de sus firewalls.

- Lenguaje de señas:A pesar de contar con una amplia cartera de productos, Huawei no ofrece acuerdos basados en ELA. Un ELA facilitaría a los clientes la comprensión y aceptación de acuerdos con varios años de vigencia y múltiples productos.

Enebro

Juniper es un competidor en este Cuadrante Mágico. Cuenta con una amplia gama de firewalls que abarca diversos casos de uso y tipos de implementación, incluyendo FWaaS y firewalls de contenedores. Normalmente, los firewalls de Juniper se incluyen en la lista junto con sus productos de red, lo que limita su penetración en el mercado.

Juniper ofrece una amplia gama de productos, incluyendo productos de redes y seguridad. Ofrece firewalls basados en dispositivos en las líneas de productos SRX, vSRX y cSRX. También cuenta con una oferta de FWaaS. Otros productos ofrecen gestión de información y eventos de seguridad, mitigación de DDoS e inteligencia de amenazas.

Las actualizaciones recientes incluyen la introducción de Security Director Cloud, Secure Edge (un producto de SSE) y Cloud Workload Protection. Juniper también ha adquirido un producto de control de acceso a la red basado en la nube con la adquisición de WiteSand.

Strengths
Fortalezas

- Casos de uso de implementación de firewall:La línea de firewalls de Juniper, la serie SRX, incluye dispositivos de hardware y dispositivos virtuales (vSRX) con compatibilidad nativa con SD-WAN. El producto Secure Edge incluye FWaaS, y la línea cSRX incluye un firewall contenedorizado con todas las funciones.

- Enfoque de plataforma:Juniper ofrece una única consola para gestionar todos sus productos de seguridad a través de Security Director y Security Director Cloud. Juniper también ofrece Prevención Avanzada de Amenazas y SecIntel como soluciones de inteligencia de amenazas compartidas entre sus líneas de productos de redes y firewalls.

- Seguridad de IoT y OT:Juniper ha demostrado su enfoque en la seguridad del IoT al mejorar la identificación y el control automatizados de dispositivos. La colaboración con Dragos y SEL proporciona capacidades de detección y respuesta ante amenazas para aplicaciones industriales en entornos OT y SCADA.

- Escalabilidad:Juniper ofrece firewalls de alto rendimiento que mantienen un buen rendimiento incluso al descifrar el tráfico. Junos Space Security Director y Juniper Security Director Cloud, un gestor centralizado, pueden gestionar hasta 25 000 dispositivos Juniper, incluyendo firewalls, switches y routers.

Cautions
Precauciones

- Visibilidad:A pesar de ofrecer firewalls para todos los casos de implementación, Juniper no tiene la misma visibilidad que sus competidores directos en las listas de clientes consultadas por Gartner. Los firewalls de Juniper son seleccionados principalmente por operadores de telecomunicaciones o para su integración con otras líneas de productos de red de Juniper.

- Capacidad de respuesta del mercado:El mercado de seguridad de red es altamente competitivo, con una intensa competencia entre proveedores para identificar casos de uso emergentes clave, como FWaaS, ZTNA, seguridad en la nube, SSE y operaciones de seguridad. A pesar de ser un importante proveedor de redes, Juniper ha tardado en identificar estos casos de uso y en lanzar productos para ellos.

- Estrategia de producto:Juniper carece de una sólida cartera de productos de seguridad interna, en comparación con sus competidores directos, que están expandiendo su oferta de productos de seguridad de forma agresiva. Por ello, los clientes de Gartner no la consideran una candidata atractiva para la consolidación de proveedores de seguridad.

- Comentarios de los clientes:Los clientes de Gartner identifican la lentitud de respuesta y la falta de innovación para casos de uso de seguridad emergentes como razones para no seleccionar a Juniper. También consideran que sus precios son elevados en comparación con los de...

competidores. Las funciones SD-WAN y DLP están disponibles, pero con un costo adicional.

Microsoft

Microsoft es un actor de nicho en este Cuadrante Mágico. Su Firewall de Azure es considerado principalmente por los clientes actuales de Microsoft que buscan consolidación. Los equipos de aplicaciones que buscan firewalls nativos para una integración fluida con las cargas de trabajo de Azure también prefieren el Firewall de Microsoft Azure.

El Firewall de Microsoft Azure está disponible mediante dos suscripciones: Estándar y Premium. Se puede administrar de forma centralizada con Azure Firewall Manager y supervisar con Azure Monitor y Microsoft Sentinel.

Microsoft sigue invirtiendo en seguridad, como lo demuestra la incorporación de la gestión de DDoS y de las políticas WAF a Azure Firewall Manager. Además, Microsoft ha añadido un IPS a su suscripción Premium.

Strengths

- Consolidación de proveedores:Los firewalls de Microsoft son ampliamente considerados por los clientes actuales de Microsoft que desean consolidar sus servicios en un solo proveedor. Microsoft ofrece una gama de servicios de seguridad, como Azure Firewall, Azure Web Application Firewall y Azure Active Directory, que pueden implementarse conjuntamente.
- Facilidad de uso:El Firewall de Microsoft Azure se integra a la perfección con otros servicios alojados en Azure. Su implementación es más sencilla que la de los firewalls de terceros, ya que se trata de una solución en línea con dimensionamiento y escalado integrados.
- Ejecución de ventas:Microsoft ha aprovechado la migración de cargas de trabajo de sus clientes a Azure al ofrecer un firewall sencillo que satisface las necesidades básicas. Gartner observa que los clientes consideran Azure Firewall para sus cargas de trabajo, y esta oferta de Microsoft compite frecuentemente con productos de proveedores de firewalls dedicados.
- Experiencia del cliente:Los usuarios identifican la facilidad de implementación como la principal razón para usar Microsoft Azure Firewall. Una segunda razón importante es su estrecha integración con el ecosistema de Azure, que facilita DevOps. Los clientes también valoran la credibilidad de Microsoft como proveedor y su soporte al producto.

Cautions

- Innovación:Microsoft se centra en la integración de Azure Firewall con las ofertas nativas de Azure, pero se queda atrás en la introducción de funciones compatibles con los nuevos casos de uso de firewall en la nube. Carece de una oferta de firewall de contenedores dedicada. La microsegmentación se gestiona mediante etiquetas de seguridad, en lugar de un producto de firewall.
- Brechas de características:El firewall de Microsoft Azure carece de varias funciones deseables en un firewall en la nube, y que ofrecen la competencia. No es compatible con IPv6, no tiene espacio aislado ni control de aplicaciones basado en firmas.
- Actuación:El rendimiento del tráfico de red se reduce en un 90 % al habilitar un IPS con TLS. Sin embargo, Microsoft ofrece una opción para agregar sitios manualmente a la lista y así evitar el descifrado TLS.
- Comentarios de los clientes:Los clientes indican que la suscripción al firewall Premium es costosa, la documentación es deficiente, falta material de capacitación y el registro no admite problemas de depuración.

Redes de Palo Alto

Palo Alto Networks es líder en este Cuadrante Mágico. Cuenta con el firewall más visible para diferentes casos de uso, según las consultas de clientes de Gartner. Con la reciente introducción de la serie PA-400, los firewalls de Palo Alto Networks se han convertido en excelentes candidatos para las medianas empresas.

Palo Alto Networks es un proveedor de seguridad con una amplia cartera de productos. Además de su línea de firewalls más popular, la Serie PA, el proveedor cuenta con líneas de productos de seguridad de seguridad (SSE), seguridad en la nube y operaciones de seguridad.

Las principales actualizaciones relacionadas con los firewalls del último año incluyen el lanzamiento de dos versiones principales de firmware con mejoras en el filtrado de URL, la seguridad de DNS, la seguridad de IoT y la prevención de amenazas. El proveedor también ha introducido AIOps y mejorado las funciones de DLP de sus firewalls.

Strengths
Strengths

- Portafolio de productos:Palo Alto Networks cuenta con una amplia cartera de productos. Gartner suele ver contratos de este proveedor para diversas líneas de productos, además de firewalls. Prisma Access (SASE) y Cortex Data Lake (XDR) suelen ser preseleccionados junto con los firewalls.

- Modos de implementación:Palo Alto Networks admite múltiples formas de implementación de firewalls, con sus series PA (firewalls de hardware), VM (firewalls virtuales), Prisma Access (FWaaS), Cloud NGFW (un firewall nativo de la nube para AWS) y CN (firewalls en contenedores). Esto lo convierte en una excelente opción para entornos híbridos, donde los clientes buscan un único proveedor de firewall.

- Funciones de seguridad avanzadas:Los firewalls de Palo Alto Networks destacan por sus funciones de seguridad avanzadas. El proveedor ofrece sólidas capacidades de detección y prevención de amenazas. Su suscripción a IoT Security ofrece detección automática de dispositivos IoT. Palo Alto Networks también ofrece seguridad DNS avanzada y funciones de seguridad 5G.

- FWaaS:La oferta FWaaS de Palo Alto Networks, Prisma Access, continúa evolucionando y es compatible con todas las funciones de SSE, incluyendo una puerta de enlace web segura (SWG), un CASB y ZTNA. Puede gestionarse como complemento para Panorama (un gestor centralizado local) o como una solución de gestión independiente en la nube.

Cautions
Cautions

- Apoyo técnico:Gartner ha recibido comentarios constantes de los clientes de Palo Alto Networks que indican una disminución en la calidad de su soporte técnico, con ciclos de escalamiento especialmente largos asociados con el soporte de Nivel 1. Como resultado, los clientes a menudo sienten la necesidad de actualizar su soporte a un nivel superior que ofrece un SLA más rápido, pero es más costoso.

- Gestor basado en la nube:El administrador de firewall en la nube de Palo Alto Networks, utilizado para oficinas distribuidas y administración centralizada, no es comparable con la administración local. Su administrador en la nube se utiliza principalmente para la línea de productos Prisma Access y los modelos de hardware de cuarta generación.

- Comentarios de los clientes:Algunos clientes de Gartner han reportado problemas de conectividad y enrutamiento con los servicios de Prisma Access. Estos comentarios provienen principalmente de usuarios de su FWaaS y del servicio GlobalProtect de Prisma Access (en lo que respecta a los clientes de firewall).

- Opacidad de los contratos ELA:Palo Alto Networks ofrece varios tipos de licencia, como licencias ELA y licencias basadas en créditos, pero sus presupuestos suelen ser poco transparentes. Generalmente incluyen precios al por mayor y carecen de claridad en cuanto a los números de pieza y los costos detallados.

Tecnologías Sangfor

Sangfor Technologies es un visionario en este Cuadrante Mágico. Este proveedor con sede en China es atractivo para empresas de Asia/Pacífico y EMEA (especialmente Oriente Medio) que desean consolidar sus productos de seguridad con un único proveedor.

Los productos de firewall de red de Sangfor forman parte de la línea de firewalls de aplicaciones de próxima generación (NGAF), que también incluye la funcionalidad WAF. Además de los firewalls de red, Sangfor ofrece una amplia gama de soluciones de seguridad para WAAP, SASE, ZTNA, IAM, seguridad de endpoints, microsegmentación y protección de cargas de trabajo en la nube.

Sangfor ha lanzado recientemente varios firewalls de hardware nuevos. Entre las nuevas funciones se incluye una suscripción a Cloud Deception para mejorar la detección de ataques. Sangfor también ofrece un firewall de red totalmente integrado con sus productos ZTNA y SASE.

Strengths Fortalezas

- Enfoque de plataforma:Sangfor desarrolla productos que pueden gestionarse conjuntamente. Su plataforma de gestión de la nube Platform-X puede gestionar el firewall de red, Endpoint Secure y las soluciones de microsegmentación de Sangfor, junto con las capacidades SWG y SD-WAN de Sangfor.

- Seguridad del IoT:Como parte de su Suite de Licencias Esenciales, Sangfor ofrece firmas IoT diferenciadas, incluyendo compatibilidad con protocolos de cámaras IP. Sangfor admite la clasificación de activos IoT, el control de acceso, la identificación y el control de protocolos, la detección de contraseñas débiles y la detección de vulnerabilidades IoT en redes de vigilancia.

- Escalabilidad:Sangfor Central Manager, el dispositivo de gestión centralizada local del proveedor, es altamente escalable. Permite administrar una gran cantidad de dispositivos desde una única consola.

- Estrategia de precios:Como proveedor con una gran cantidad de clientes importantes, Sangfor utiliza su ELA como herramienta estratégica para el empaquetado de productos. Suele ofrecer importantes descuentos, condiciones flexibles para la implementación de firewalls virtuales y la incorporación de nuevos productos durante la vigencia del ELA, con un ajuste al momento de la renovación.

Cautions Precauciones

- Redes avanzadas:Los firewalls de Sangfor carecen de compatibilidad con 5G. Esta es una deficiencia importante para los clientes en China, varios otros países de Asia/Pacífico y partes de Oriente Medio, donde se encuentra principalmente la infraestructura 5G.

- Integración de la nube pública:Sangfor carece de integración con las nubes públicas Microsoft Azure y GCP que son populares en muchas regiones.

- Detección de amenazas:Sangfor tiene menos firmas IPS que otros proveedores de firewall evaluados en este Cuadrante Mágico, y no se realiza ningún análisis de aprendizaje automático junto con el IPS para mejorar la eficacia de la detección. Además, Sangfor carece de integración con herramientas de terceros para mejorar la detección de malware.

318

- Estrategia geográfica:Sangfor tiene muy poca presencia fuera de Asia y Oriente Medio. Otros competidores regionales evaluados en este Cuadrante Mágico se consideran y se implementan con mayor frecuencia en Latinoamérica.

SonicWall

SonicWall es un actor de nicho en este Cuadrante Mágico. Es un candidato sólido para las empresas medianas, ya que ofrece una seguridad sólida y una excelente relación calidad-precio. Sus capacidades nativas de SD-WAN con FWaaS lo convierten en una excelente opción para oficinas distribuidas y casos de uso de acceso remoto.

SonicWall ofrece tres líneas de firewalls de dispositivos de hardware: las series TZ, NSa y NSsp, y una línea de firewalls de dispositivos virtuales, la serie NSv. Además de firewalls, SonicWall comercializa funciones integradas de EDR, gateway de correo electrónico seguro, ZTNA y CASB.

Las actualizaciones recientes incluyen mejoras en el administrador centralizado, como la optimización de reglas y el flujo de trabajo SD-WAN para simplificar el aprovisionamiento de firewalls en sucursales. SonicWall también ha introducido la gestión centralizada para los conmutadores SonicWall, los puntos de acceso inalámbricos SonicWave y el cliente de captura SonicWall.

Strengths

- Caso de uso de oficina distribuida:SonicWall ofrece capacidades SD-WAN nativas en todos sus modelos de firewall y en SonicWall Network Security Manager. También ofrece Cloud Edge Secure Access, una solución SASE con FWaaS, ZTNA, control de acceso a la red y funciones CASB, ideal para oficinas distribuidas.

- Precios:SonicWall ofrece precios competitivos, lo que lo convierte en una excelente opción para empresas medianas. La funcionalidad SD-WAN está incluida en todos sus dispositivos sin coste adicional. La funcionalidad DLP forma parte del paquete básico, también sin coste adicional.

- Comentarios de los clientes:Los clientes han elogiado la interfaz de gestión única de SonicWall para gestionar diferentes productos. Además, consideran que su bajo coste total de propiedad (TCO) es una razón para elegir los firewalls de SonicWall.

- Gestión centralizada:El Centro de Seguridad de Captura (CSC) de SonicWall es un portal de gestión integral para los productos de SonicWall, incluyendo sus firewalls y la solución Cloud Edge Secure Access. Simplifica la administración.

Cautions

- Visibilidad:Gartner considera a SonicWall principalmente como una opción de firewall para empresas medianas. Carece de visibilidad para otros casos de uso, especialmente el de oficinas distribuidas (a pesar de contar con capacidades SD-WAN nativas y una oferta FWaaS) y el de centros de datos.

- Características del producto:SonicWall solo admite instancias virtuales limitadas (ideales para centros de datos) en sus dispositivos de hardware. Admite menos categorías de aplicaciones web que otros proveedores evaluados en este Cuadrante Mágico. SonicWall carece de una solución XDR nativa; en su lugar, ofrece integración con plataformas XDR de terceros.

- Cortafuegos en la nube:El soporte de SonicWall para nubes públicas está por detrás del de otros proveedores en este Magic Quadr1a8 Compatible únicamente con AWS y Microsoft Azure; no con GCP. No existe una opción de pago por uso.

Disponible para Azure. SonicWall no cuenta con firewall de contenedores ni microsegmentación. Comentarios de los clientes:Los

- clientes de SonicWall han indicado que las capacidades de generación de informes del firewall son limitadas y carecen de granularidad. También han experimentado largas demoras tras contactar con el soporte técnico.

Sophos

Sophos es un actor de nicho en este Cuadrante Mágico. Su estrategia de producto y su enfoque basado en plataformas, centrado en las necesidades de las medianas empresas, ofrecen una sólida integración entre sus firewalls y EDR. Sophos está ampliando gradualmente sus líneas de productos de seguridad en la nube.

Sophos ofrece soluciones de seguridad de red, seguridad de endpoints, seguridad en la nube y MDR. Sus firewalls se dividen en diferentes líneas de productos. Los firewalls de Sophos y la solución de seguridad de endpoints Intercept X son sus productos más populares.

Las principales actualizaciones relacionadas con los firewalls del último año incluyen la introducción de la serie Sophos XGS de firewalls de hardware, el lanzamiento de Sophos ZTNA y nuevas suscripciones de software. Sophos también ha mejorado el rendimiento de XGS y la orquestación de SD-WAN.

Strengths Fortalezas

- Enfoque de plataforma:Sophos ofrece su firewall, EDR y XDR como una plataforma unificada con sólida integración, gestión centralizada y funciones de correlación. Ofrece una única consola en la nube con un único agente de endpoint para gestionar ambos productos.
- Caso de uso de empresa mediana:La estrategia y la ejecución de ventas de Sophos se centran en las medianas empresas. Además de consolidar su firewall y la funcionalidad EDR, Sophos ha introducido servicios de respuesta gestionada ante amenazas y respuesta rápida para clientes que buscan externalizar servicios de MDR.
- Gestor centralizado basado en la nube:Sophos ofrece un único gestor centralizado en la nube para gestionar todos sus productos. Esto facilita la gestión.
- Comentarios de los clientes:Los clientes suelen identificar la atención al cliente y la documentación completa del producto de Sophos como puntos fuertes. Sophos ha incorporado ayuda contextual, tutoriales guiados y vídeos instructivos integrados para mejorar aún más la experiencia de administración del producto.

Cautions Precauciones

- Visibilidad:Sophos suele ser visible para empresas medianas, pero se usa con menos frecuencia para otros casos de uso de firewall. Esto a pesar de que Sophos cuenta con una oferta independiente para ZTNA y un firewall en la nube que incluye un firewall para contenedores.
- Lenguaje de señas:A pesar de contar con una amplia cartera de productos, Sophos no ofrece precios ELA, a pesar de que los clientes que buscan consolidar productos con el mismo proveedor lo desean. En su lugar, Sophos ofrece un modelo de consumo multianual más sencillo.
- Características:Sophos no ofrece FWaaS, aunque es recomendable para casos de uso con sucursales y usuarios itinerantes. Además, sus firewalls, que están habilitados para SD-WAN, carecen de compatibilidad con 5G.

- Comentarios de los clientes:A medida que crece la competencia entre proveedores en el mercado de empresas medianas, algunos clientes de Gartner consideran que Sophos es caro, en comparación con otros proveedores que venden a empresas medianas.

WatchGuard

WatchGuard es un actor de nicho en este Cuadrante Mágico. Ofrece firewalls para casos de uso en empresas medianas y distribuidas. Además del firewall Firebox, WatchGuard cuenta con un dispositivo virtual (FireboxV) y un dispositivo virtual diseñado específicamente para entornos de nube pública (Firebox Cloud).

WatchGuard Dimension es la solución de gestión de firewalls locales de este proveedor. Todos los productos de seguridad de WatchGuard se pueden gestionar mediante WatchGuard Cloud, su consola en la nube. Otros productos de la cartera de seguridad de WatchGuard ofrecen autenticación multifactor (MFA), Wi-Fi seguro y seguridad de endpoints.

WatchGuard ha lanzado recientemente varios nuevos dispositivos de hardware de firewall. Entre las nuevas funciones se incluyen la integración de Firebox con los productos MFA y Wi-Fi seguro de WatchGuard, así como la capacidad de compartir carga para la funcionalidad SD-WAN integrada en el firewall del proveedor.

Strengths
Fortalezas

- Estrategia de producto:En los últimos años, WatchGuard ha pasado de una estrategia tradicional de comercialización basada en revendedores de valor añadido (VAR) a una estrategia centrada en proveedores de servicios gestionados (MSP). Este reenfoque ha llevado al proveedor a crear WatchGuard Cloud fácil de usar y fácil de usar para proveedores de servicios, a la vez que escalable para múltiples clientes finales por proveedor de servicios.

- Integración de puntos finales:El firewall Firebox de WatchGuard se gestiona en conjunto con sus productos de seguridad para endpoints. El proveedor cuenta con un proceso llamado ThreatSync que recopila datos de eventos de los firewalls de WatchGuard, sensores de endpoints y fuentes de inteligencia de amenazas, analiza los datos colectivos y asigna puntuaciones de amenaza.

- Seguridad OT:WatchGuard cuenta con un firewall de red robusto que se utiliza ocasionalmente en ciertos entornos de fabricación y servicios públicos. El proveedor también incluye firmas SCADA en sus paquetes de funciones Basic Security Suite y Total Security Suite.

- Estrategia de precios:Bajo el modelo de licencia FlexPay, WatchGuard ofrece la opción de comprar sus firewalls mediante pagos por adelantado, Puntos WatchGuard o pago por uso de WatchGuard, lo que es único en el mercado tradicional de dispositivos de firewall basados en gastos de capital.

Cautions
Cautions

- Seguridad de IaaS:WatchGuard solo ofrece firewalls compatibles con la nube pública para AWS y Microsoft Azure. En este sentido, se queda atrás de la mayoría de sus competidores, que suelen ofrecer soporte para tres o más proveedores de infraestructura como servicio (IaaS). La falta de compatibilidad con GCP limita las oportunidades de WatchGuard para prestar servicio a empresas medianas "nacidas en la nube", que en ocasiones eligen a Google como su proveedor de infraestructura.

- FWaaS y ZTNA:Muchos clientes pequeños y medianos de Gartner preguntan por FWaaS como alternativa a los firewalls tradicionales para sucursales. Sin embargo, WatchGuard no ofrece FWaaS. Tampoco ofrece ZTNA.

- Estrategia de producto:WatchGuard carece de soluciones para casos de uso emergentes de seguridad en la nube, como firewalls en contenedores y microsegmentación. Por lo tanto, no aparece en las listas de candidatos de Gartner, más allá de las de organizaciones medianas que buscan firewalls de hardware.
- Redes avanzadas:Al momento de este análisis, WatchGuard no ha entregado ningún firewall compatible con 5G. Esto limita su adopción en muchas regiones que han desarrollado una extensa infraestructura 5G.

Proveedores añadidos y eliminados

Revisamos y ajustamos nuestros criterios de inclusión en los Cuadrantes Mágicos a medida que cambian los mercados. Como resultado de estos ajustes, la composición de proveedores en cualquier Cuadrante Mágico puede variar con el tiempo. La aparición de un proveedor en un Cuadrante Mágico un año y no al siguiente no implica necesariamente un cambio de opinión sobre él. Puede ser reflejo de un cambio en el mercado y, por lo tanto, de una modificación en los criterios de evaluación, o de un cambio de enfoque por parte de ese proveedor.

Agregado

Ninguno.

Abandonó

- Redes Cato
- Redes Versa

Criterios de inclusión y exclusión

Los criterios de inclusión representan los atributos específicos que los analistas de Gartner consideraron necesario que los proveedores tuvieran para ser incluidos en este Cuadrante Mágico.

Los proveedores de funciones de firewall de red cubiertos por la sección Definición/Descripción del mercado fueron considerados para evaluación en este Cuadrante Mágico bajo las siguientes condiciones:

- Los proveedores deben tener dispositivos de hardware/virtuales o firewalls nativos de la nube como sus productos de firewall principales.
- Los proveedores deben tener presencia al menos en tres de las siguientes regiones, incluida su región de origen: Asia/Pacífico, América del Norte, América Latina, Europa y Medio Oriente.
- Los proveedores que ofrecen un dispositivo de hardware/dispositivo virtual como su oferta principal de productos de firewall deben haber generado al menos $70 millones en ingresos únicamente por dispositivos de hardware/dispositivos virtuales de firewall en 2021.
- Los proveedores deben tener un historial de satisfacción de las necesidades de los casos de uso de la nube pública.
- Los analistas de Gartner deben haber evaluado que los proveedores pueden competir eficazmente en el mercado de firewalls de red.
- Los analistas de Gartner deben haber determinado que los proveedores son actores importantes en el mercado de firewalls de red, debido a su presencia en el mercado, visibilidad competitiva o innovación tecnológica.

- Los proveedores deben tener la capacidad de satisfacer más de un caso de uso de implementación de firewall de red mencionado en la sección Definición/Descripción del mercado.
- Los proveedores de nube pública deben tener una oferta de firewall dedicada.

Criterio de exclusión:

- Gartner consideró que los proveedores que ofrecen FWaaS como su línea principal de productos de firewall no son elegibles para su inclusión en este Cuadrante Mágico.

Criterios de evaluación

Capacidad de ejecución

Los analistas de Gartner evalúan a los proveedores en función de la calidad y eficacia de los procesos, sistemas, métodos o procedimientos que les permiten ser competitivos, eficientes y eficaces, y que impactan positivamente en los ingresos, la retención y la reputación. Los siguientes criterios se utilizan para evaluar la capacidad de ejecución de los proveedores.

Producto o servicio:Bienes y servicios principales que ofrece el proveedor para el mercado definido. Esto incluye las capacidades actuales del producto/servicio, la calidad, las características, las habilidades, etc., ya sea que se ofrezcan de forma nativa o mediante acuerdos/colaboraciones con fabricantes de equipos originales (OEM), según se define en la definición del mercado y se detalla en los subcriterios.

Subcriterios:

- Capacidad del producto para satisfacer las necesidades de diferentes casos de uso de firewall de red y especializarse en ellos.
- Enfoque de plataforma.
- El soporte se evalúa por la calidad, amplitud y valor de una oferta (u ofertas) específicamente en relación con casos de uso empresariales y de la nube.

Viabilidad general:

La viabilidad incluye una evaluación de la salud financiera general de la organización, el éxito financiero y práctico de la unidad de negocios y la probabilidad de que la unidad de negocios individual continúe invirtiendo en el producto, continúe ofreciéndolo y avance en el estado del arte dentro de la cartera de productos de la organización.

Ejecución de ventas/Precios:Las capacidades del proveedor en todas las actividades de preventa y la estructura que las respalda. Esto incluye la gestión de acuerdos, la fijación de precios y la negociación, el soporte preventa y la eficacia general del canal de ventas.

Subcriterios:

- Comentarios de los clientes sobre los precios.

- Transparencia de los contratos.
- Modelos de precios agrupados que sean claros y fáciles de entender.
- TCO competitivo.
- Fuerte soporte y servicios de pre-venta y post-venta.

Capacidad de respuesta/historial del mercado:Capacidad de respuesta, cambio de dirección, flexibilidad y éxito competitivo a medida que surgen oportunidades, la competencia actúa, las necesidades de los clientes evolucionan y la dinámica del mercado cambia. Este criterio también considera el historial de capacidad de respuesta del proveedor.

Subcriterios:

- Introducción oportuna de nuevas funciones para satisfacer los requisitos de los clientes.
- Capacidad para soportar casos de uso emergentes, como SASE, seguridad en la nube y seguridad de IoT.
- Integraciones oportunas de socios para satisfacer las demandas de los clientes.

Ejecución de marketing:La claridad, calidad, creatividad y eficacia de los programas diseñados para transmitir el mensaje de la organización con el fin de influir en el mercado, promover la marca y el negocio, aumentar el conocimiento de los productos y establecer una identificación positiva con el producto/marca y la organización en la mente de los compradores. Esta "participación mental" puede impulsarse mediante una combinación de publicidad, iniciativas promocionales, liderazgo de pensamiento, boca a boca y actividades de ventas.

Subcriterios:

- Visibilidad del proveedor en las listas de candidatos seleccionados de los clientes.
- Grado en el cual los usuarios finales están migrando desde el proveedor.
- Medida en la que el marketing del proveedor se enfrenta a la competencia directa.
- Conocimiento de la marca del proveedor por parte de los usuarios finales.

Experiencia del cliente:Relaciones, productos y servicios/programas que permiten a los clientes tener éxito con los productos evaluados. Esto incluye, en concreto, la forma en que los clientes reciben soporte técnico o de cuenta. También puede incluir herramientas complementarias, programas de atención al cliente (y su calidad), disponibilidad de grupos de usuarios, acuerdos de nivel de servicio, etc.

El factor más importante es la satisfacción del cliente durante todo el ciclo de ventas y de vida del producto. También son importantes la facilidad de uso, el enfoque de plataforma, la gestión centralizada y la protección contra los ataques más recientes. Las opiniones de tendencia, tanto positivas como negativas, sobre los productos o el soporte de un proveedor también tienen una gran importancia.

Operaciones:La capacidad de la organización para cumplir sus objetivos y compromisos. Los factores incluyen la calidad de la estructura organizacional, incluyendo habilidades, experiencias, programas, sistemas y otros instrumentos que permiten a la organización operar de forma eficaz y eficiente de forma continua.

Tabla 1: Criterios de evaluación de la capacidad de ejecución

Criterios de evaluación	***Ponderación***
Producto o servicio	Alto
Viabilidad general	Medio
Ejecución de ventas/Precios	Medio
Capacidad de respuesta/registro del mercado	Alto
Ejecución de marketing	Medio
Experiencia del cliente	Alto
Operaciones	Medio

Fuente: Gartner (diciembre de 2022)

Integridad de la visión

Los analistas de Gartner evalúan a los proveedores según su capacidad para articular de forma convincente declaraciones lógicas sobre la dirección actual y futura del mercado, la innovación, las necesidades de los clientes y las fuerzas competitivas. Evaluan la correspondencia de estas declaraciones con la visión de Gartner sobre el mercado.

Comprensión del mercado:Capacidad del proveedor para comprender los deseos y necesidades de los compradores y traducirlos en productos y servicios. Los proveedores con mayor visión escuchan y comprenden los deseos y necesidades de los compradores, y pueden moldearlos o mejorarlos con su visión.

Subcriterios:

- Capacidad para comprender y agregar funciones en respuesta a los requisitos de los clientes para diferentes casos de uso.
- Capacidad para comprender y responder a los requisitos de los clientes relacionados con el producto y el mercado.
- Capacidad para cumplir con los plazos impuestos por los requisitos de los clientes.
- Compatibilidad con entornos híbridos y diferentes casos de uso de implementación de firewall, enfoque de plataforma, administración y visibilidad centralizadas, seguridad en la nube, protección de carga de trabajo en la nube y automatización.

Estrategia de comercialización:Un conjunto claro y diferenciado de mensajes comunicados consistentemente en toda la organización y externalizados a través del sitio web, la publicidad, los programas de clientes y las declaraciones de posicionamiento.

Subcriterios:

- Capacidad de proporcionar mensajes claros que resuenen con los casos de uso y requisitos de los clientes.
- Capacidad para comunicarse de manera efectiva con los canales de ventas y distribución, los usuarios finales y diferentes tipos de compradores sobre las características, el firmware del producto, la visión y el enfoque en la evolución de los casos de uso, con el fin de construir una marca.
- Mensajes fuertes y claros sobre casos de uso en evolución.

Estrategia de ventas:La estrategia de venta de productos que utiliza la red adecuada de afiliados de ventas directas e indirectas, marketing, servicios y comunicación para ampliar el alcance y la profundidad del alcance del mercado, las habilidades, la experiencia, las tecnologías, los servicios y la base de clientes.

Subcriterios:

- Modelos de ventas y precios efectivos para satisfacer los requisitos de los clientes para diferentes casos de uso de implementación.
- Modelos de precios claros y transparentes.
- Una estrategia integral de canales y socios para vender en múltiples casos de uso de implementación.
- Acercamiento al centro de compras de seguridad de red y/o carga de trabajo en la nube.

Estrategia de oferta (producto):El enfoque del proveedor hacia el desarrollo y la entrega de productos que enfatiza la diferenciación, la funcionalidad, la metodología y los conjuntos de características a medida que se adaptan a los requisitos actuales y futuros.

Subcriterios:

- Desarrollo de funciones potentes para mejorar la prevención de amenazas.
- Funciones integradas y automatización, en lugar de una amplia cartera de productos con productos superpuestos.
- Funciones y refuerzos potentes para soportar todos los casos de uso de firewall de red.

- Integraciones de productos maduros con socios para mejorar las capacidades del firewall de red para entornos que incluyen, por ejemplo, OT, sucursales/campus, seguridad en la nube y usuarios que trabajan desde casa.

Modelo de negocio:La solidez y la lógica de la propuesta comercial subyacente del proveedor.

Estrategia vertical/industrial:La estrategia del proveedor para dirigir recursos, habilidades y ofertas para satisfacer las necesidades específicas de segmentos de mercado individuales, incluidos los mercados verticales.

Innovación:Disposiciones directas, relacionadas, complementarias y sinérgicas de recursos, experiencia o capital con fines de inversión, consolidación, defensivos o preventivos.

Subcriterios:

- Enfoque de plataforma.
- Fuerte visión y características excepcionales para casos de uso particulares de implementación de firewall.
- Madurez de las características.
- Integración con productos superpuestos.
- Uso de tecnología para detectar y prevenir amenazas.
- Características excepcionales y diferenciadoras e innovación para respaldar uno o más casos de uso de firewall de red.

Estrategia geográfica:La estrategia del proveedor para dirigir recursos, habilidades y ofertas para satisfacer las necesidades específicas de geografías fuera de la geografía "de origen" o nativa, ya sea directamente o a través de socios, canales y subsidiarias según sea apropiado para esa geografía y mercado.

Tabla 2: Integridad de los criterios de evaluación de la visión

Criterios de evaluación	***Ponderación***
Comprensión del mercado	Alto
Estrategia de comercialización	Medio
Estrategia de ventas	Medio
Estrategia de oferta (producto)	Alto

Criterios de evaluación	*Ponderación*
Modelo de negocio	Medio
Estrategia vertical/industrial	Sin calificación
Innovación	Alto
Estrategia geográfica	Medio

Fuente: Gartner (diciembre de 2022)

Descripciones de cuadrantes

Líderes

El cuadrante de líderes incluye proveedores que pueden influir en el mercado al ser pioneros en introducir capacidades adicionales y concienciar sobre su importancia. Los líderes tienen el potencial de satisfacer las necesidades empresariales de múltiples casos de uso de firewall en una única plataforma.

Los líderes ofrecen nuevas funciones que protegen a los clientes de las amenazas emergentes. Cumplen con los requisitos de las redes híbridas en constante evolución, incluyendo las nubes públicas y privadas. Ofrecen capacidades especializadas, en lugar de tratar los firewalls como simples productos básicos. Cuentan con un excelente historial de prevención de vulnerabilidades en sus productos de seguridad.

Los líderes ofrecen funciones innovadoras para simplificar la configuración y la gestión de políticas de firewall en entornos híbridos. Suelen ser capaces de gestionar el máximo rendimiento con una mínima pérdida de rendimiento. Además, suelen ofrecer opciones de aceleración de hardware, compatibilidad con plataformas de nube pública y privada, y formatos que protegen a las empresas en su transición a nuevos formatos de infraestructura. Los líderes ofrecen las primeras funciones y capacidades para respaldar en profundidad los nuevos casos de uso de firewall. Adoptan un enfoque de plataforma integrada, en lugar de tener múltiples líneas de productos para distintos casos de uso sin integración.

Además de proporcionar tecnología que se adapta bien a los requisitos actuales de los clientes, los líderes muestran una visión y ejecución superiores con respecto a los posibles requisitos futuros y la evolución de las redes híbridas.

Retadores

Los retadores cuentan con canales de distribución y clientes sólidos, pero no lideran constantemente con capacidades diferenciadas de última generación. Muchos retadores no han desarrollado completamente sus capacidades de firewall. Es posible que cuenten con otros productos de seguridad que tienen éxito en el sector empresarial y que confíen en sus relaciones existentes con los clientes, en lugar de en sus productos de firewall, para cerrar contratos.

Los productos de los proveedores más competitivos suelen tener buenos precios y, gracias a su excelente ejecución, pueden ofrecer paquetes de productos de seguridad económicos que muchos otros no pueden ofrecer.

Muchos retadores se frenan a sí mismos para convertirse en líderes al darle a sus productos de seguridad o firewall una prioridad más baja dentro de su conjunto general de productos.

Los competidores suelen tener cuotas de mercado significativas, pero pueden quedar rezagados respecto a aquellos con cuotas de mercado más pequeñas cuando se trata de lanzar nuevas funciones.

Visionarios

Los visionarios lideran en innovación, pero se limitan a uno o dos casos de uso de implementación de firewalls. Cuentan con los diseños y las características adecuados, pero carecen de la base de ventas, la estrategia o los recursos financieros para competir de forma consistente con los líderes y los retadores. En ocasiones, los visionarios han tomado la decisión consciente de centrarse en un número limitado de casos de uso de firewalls. La mayoría de los productos de los visionarios cuentan con buenas capacidades de firewall de última generación, pero presentan deficiencias en términos de rendimiento y redes de soporte.

Los visionarios muestran una fuerte visión e innovación líder en el mercado en relación, entre otras cosas, con la protección de los usuarios que trabajan desde casa, la garantía de la seguridad de las cargas de trabajo, la habilitación de la segmentación este-oeste en entornos de redes definidas por software y de nube pública, y la automatización de la detección de amenazas.

Jugadores de nicho

La mayoría de los actores de nicho tienen una base instalada principal o prominencia en un caso de uso específico, como los que involucran centros de datos, telecomunicaciones, empresas distribuidas, medianas empresas e IaaS público. Algunos actores de nicho que ofrecen un firewall como módulo, junto con otros servicios o componentes, se centran en un caso de uso específico.

Los actores de nicho carecen de capacidad de ejecución debido a su limitada cartera de clientes y tienden a no mostrar mucha innovación. Algunos se limitan a regiones específicas.

Contexto

A medida que las redes evolucionan, los proveedores de firewalls de red continúan ampliando sus carteras de productos para cubrir mercados de seguridad que se solapan y atraer a compradores que buscan consolidarse. Sin embargo, comprar al mismo proveedor no garantiza necesariamente simplicidad ni una gestión centralizada.

Los firewalls basados en dispositivos siguen siendo relevantes para múltiples casos de uso. La renovación de dispositivos de hardware se mantiene bastante estable. Existe una demanda de firewalls de hardware de alto rendimiento, especialmente para centros de datos y perímetros empresariales.

La demanda de FWaaS para casos de uso remotos es cada vez mayor, ya sea en sucursales o en domicilios particulares. La consolidación también es evidente en este sentido, con SSE, que combina las funcionalidades CASB, ZTNA y SWG, convirtiéndose en un requisito cada vez más importante. Las sucursales con altos requisitos de rendimiento o limitaciones de cumplimiento normativo siguen optando por dispositivos de hardware para el caso de uso en sucursales. (Los proveedores de FWaaS independientes no aparecen en el Cuadrante Mágico de este año, ya que la demanda de sus productos es insuficiente para justificar su inclusión).

Los proveedores que innovan para casos de uso de seguridad en la nube están ganando terreno, debido a la fuerte demanda de firewalls en la nube (tanto nativos como para contenedores). Por ello, incluimos a los proveedores de servicios en la nube en este Cuadrante Mágico.

El criterio de ejecución de ventas/precio tiene una ponderación significativa debido a la retroalimentación constante de los clientes sobre su importancia y a los frecuentes aumentos en los precios de los firewalls de red. Contratos más complejos, mayores costos de renovación y un mayor TCO están generando insatisfacción entre los clientes.

Descripción general del mercado

El mercado de firewalls de red sigue siendo uno de los más grandes de la seguridad y ha evolucionado junto con el mercado general de la misma. Como resultado, múltiples factores impulsan el mercado de firewalls de red.

El auge de los entornos híbridos es el factor clave que impulsa a los proveedores a introducir múltiples tipos de implementación de firewalls, como FWaaS y nativos de la nube. Existe una creciente demanda de proteger entornos locales, múltiples entornos de nube y usuarios remotos con firewalls.

El interés en la confianza cero favorece la selección de proveedores de firewall únicos que puedan ayudar a las empresas a lograr una ZTNA, evitando así la necesidad de recurrir a múltiples proveedores. Los clientes esperan capacidades de integración consolidadas al adquirir tecnologías que se solapan con el mismo proveedor.

Existe un enorme interés en la visibilidad y el control de las políticas de segmentación este-oeste y en la integración mejorada de operaciones de seguridad.

Las capacidades de seguridad avanzadas siguen siendo un factor clave, ya que los vectores de amenaza utilizan métodos más sofisticados para atacar las fuerzas de trabajo híbridas y las redes en la nube. La mayoría de los proveedores intentan desarrollar o adquirir productos que ofrezcan estas capacidades, pero se enfrentan a una fuerte competencia de los mejores proveedores que ofrecen capacidades granulares para este caso de uso específico.

El mercado de firewalls de red ha evolucionado para incluir los siguientes segmentos, cada uno de los cuales tiene un conjunto específico de características:

- Cortafuegos en la nube:Estos firewalls de proveedores de infraestructura en la nube están diseñados para su implementación nativa en la nube como instancias virtuales independientes o en contenedores. Los firewalls de contenedores también pueden proteger las conexiones entre contenedores.

- Cortafuegos de malla híbridos:Se trata de plataformas que ayudan a proteger entornos híbridos al extender los controles de firewall de red modernos a múltiples puntos de aplicación, incluidos FWaaS y firewalls en la nube, con gestión centralizada a través de un único administrador basado en la nube.

- Firewall como servicio (FWaaS):Un FWaaS es una puerta de enlace de seguridad multifunción entregada como un servicio basado en la nube, a menudo para proteger pequeñas sucursales y usuarios móviles.

Otras observaciones clave sobre este mercado:

- Los clientes siguen dando opiniones negativas sobre el aumento de precio de los firewalls de red. Solo los proveedores regionales parecen ofrecer precios sencillos y competitivos. Otros proveedores siguen subiendo sus precios regularmente.
- La detección y prevención avanzada de amenazas sigue siendo un criterio de selección importante. Los proveedores de firewalls de red han mejorado sus funciones en este ámbito, con mejoras clave en la seguridad del IoT y la seguridad del DNS.
- Cada vez más proveedores han introducido soluciones de firewall en la nube, aunque con distintos niveles de madurez. Los firewalls de contenedores aún son ofrecidos por un número limitado de proveedores.
- Los proveedores pueden identificar la introducción de ofertas FWaaS como una prioridad, pero cada vez son más los que introducen ZTNA y/o SWG primero.
- Aunque los proveedores afirman que existe una fuerte integración entre sus firewalls de red y otras líneas de productos superpuestas, Gartner considera que estas integraciones son muy básicas.
- Los proveedores de firewalls de redes de centros de datos continúan presentando equipos de mayor rendimiento.
- Todos los proveedores de firewall evaluados en este Cuadrante Mágico ofrecen capacidades SD-WAN nativas en sus dispositivos de firewall.
- A medida que las empresas medianas se convierten en organizaciones de entornos híbridos, su necesidad de una seguridad madura está impulsando un aumento en los presupuestos de seguridad. Como resultado, el uso de firewalls en empresas medianas parece estar en aumento, con más proveedores introduciendo dispositivos y licencias en paquetes para atraer a estas empresas. Actualmente, existe una fuerte competencia para captar su clientela.

Definiciones de criterios de evaluación

Capacidad de ejecución

Producto/Servicio:Bienes y servicios principales que ofrece el proveedor para el mercado definido. Esto incluye las capacidades actuales del producto/servicio, la calidad, las características, las habilidades, etc., ya sea que se ofrezcan de forma nativa o mediante acuerdos/colaboraciones con fabricantes de equipos originales (OEM), según se define en la definición del mercado y se detalla en los subcriterios.

Viabilidad general:La viabilidad incluye una evaluación de la salud financiera general de la organización, el éxito financiero y práctico de la unidad de negocios y la probabilidad de que la unidad de negocios individual continúe invirtiendo en el producto, continúe ofreciéndolo y avance en el estado del arte dentro de la cartera de productos de la organización.

Ejecución de ventas/Precios:Las capacidades del proveedor en todas las actividades de preventa y la estructura que las respalda Esto incluye la gestión de acuerdos, la fijación de precios y la negociación, el soporte de preventa y la eficacia general.

del canal de ventas.

Capacidad de respuesta/historial del mercado:Capacidad de respuesta, cambio de dirección, flexibilidad y éxito competitivo a medida que surgen oportunidades, la competencia actúa, las necesidades de los clientes evolucionan y la dinámica del mercado cambia. Este criterio también considera el historial de capacidad de respuesta del proveedor.

Ejecución de marketing:La claridad, calidad, creatividad y eficacia de los programas diseñados para transmitir el mensaje de la organización con el fin de influir en el mercado, promover la marca y el negocio, aumentar el conocimiento de los productos y establecer una identificación positiva con el producto/marca y la organización en la mente de los compradores. Esta "participación mental" puede impulsarse mediante una combinación de publicidad, iniciativas promocionales, liderazgo de pensamiento, boca a boca y actividades de ventas.

Experiencia del cliente:Relaciones, productos y servicios/programas que permiten a los clientes tener éxito con los productos evaluados. Esto incluye, en concreto, la forma en que los clientes reciben soporte técnico o de cuenta. También puede incluir herramientas complementarias, programas de atención al cliente (y su calidad), disponibilidad de grupos de usuarios, acuerdos de nivel de servicio, etc.

Operaciones:La capacidad de la organización para cumplir sus objetivos y compromisos. Los factores incluyen la calidad de la estructura organizacional, incluyendo habilidades, experiencias, programas, sistemas y otros instrumentos que permiten a la organización operar de forma eficaz y eficiente de forma continua.

Integridad de la visión

Comprensión del mercado:Capacidad del proveedor para comprender los deseos y necesidades de los compradores y traducirlos en productos y servicios. Los proveedores con mayor visión escuchan y comprenden los deseos y necesidades de los compradores, y pueden moldearlos o mejorarlos con su visión.

Estrategia de comercialización:Un conjunto claro y diferenciado de mensajes comunicados consistentemente en toda la organización y externalizados a través del sitio web, la publicidad, los programas de clientes y las declaraciones de posicionamiento.

Estrategia de ventas:La estrategia de venta de productos que utiliza la red adecuada de afiliados de ventas directas e indirectas, marketing, servicios y comunicación que amplían el alcance y la profundidad del alcance del mercado, las habilidades, la experiencia, las tecnologías, los servicios y la base de clientes.

Estrategia de oferta (producto):El enfoque del proveedor hacia el desarrollo y la entrega de productos que enfatiza la diferenciación, la funcionalidad, la metodología y los conjuntos de características a medida que se adaptan a los requisitos actuales y futuros.

Modelo de negocio:La solidez y la lógica de la propuesta comercial subyacente del proveedor.

Estrategia vertical/industrial:La estrategia del proveedor para dirigir recursos, habilidades y ofertas para satisfacer las necesidades específicas de segmentos de mercado individuales, incluidos los mercados verticales.

Innovación:Disposiciones directas, relacionadas, complementarias y sinérgicas de recursos, experiencia o capital con fines de inversión, consolidación, defensivos o preventivos.

Estrategia geográfica:La estrategia del proveedor para dirigir recursos, habilidades y ofertas para satisfacer las necesidades específicas de geografías fuera de la geografía "de origen" o nativa, ya sea directamente o a través de socios, canales y subsidiarias según sea apropiado para esa geografía y mercado.

Learn how Gartner can help you succeed

Become a Client

© 2024 Gartner, Inc. y/o sus filiales. Todos los derechos reservados. Gartner es una marca registrada de Gartner, Inc. y sus filiales. Esta publicación no puede reproducirse ni distribuirse en ningún formato sin la autorización previa por escrito de Gartner. Consiste en las opiniones del equipo de investigación de Gartner, que no deben interpretarse como declaraciones de hechos. Si bien la información contenida en esta publicación se ha obtenido de fuentes consideradas fiables, Gartner no ofrece ninguna garantía en cuanto a la exactitud, integridad o idoneidad de dicha información. Si bien la investigación de Gartner puede abordar cuestiones legales y financieras, Gartner no proporciona asesoramiento legal ni de inversión, y su investigación no debe interpretarse ni utilizarse como tal. Su acceso y uso de esta publicación se rigen porPolítica de uso de Gartner Gartner se enorgullece de su reputación de independencia y objetividad. Su organización de investigación elabora sus investigaciones de forma independiente, sin la participación ni la influencia de terceros. Para más información, consulte "Principios rectores sobre independencia y objetividad."La investigación de Gartner no puede utilizarse como insumo ni para el entrenamiento o desarrollo de inteligencia artificial generativa, aprendizaje automático, algoritmos, software o tecnologías relacionadas.

© 2024 Gartner, Inc. y/o sus filiales. Todos los derechos reservados.

REFERENCIAS TECNICAS

INGLES

H323

Overview of ASPF/ALG

ASPF Definition

Application specific packet filter (ASPF) is a packet filtering technology applied to the application layer, which is also called state-based packet filtering.

ASPF Purpose

ASPF enables the device to automatically detect the application layer information of certain packets and create the corresponding access rules (server map) based on the application layer information. The server map is used to permit subsequent packets in the data channel, which is equivalent to creating a refined security policy.

For example, for multi-channel protocols (such as FTP, H.323, and SIP), the address and port of a data channel need to be negotiated in a control channel, and then the data channel can be established based on the negotiation result. The administrator cannot predict the address and port of the data channel, in that they are dynamically negotiated. Therefore, it is impossible for the administrator to configure full-fledged and accurate security policies. To ensure the proper establishment of the data channel, all ports need to be opened, which brings the risk of being attacked to the server or client. In this case, you can enable ASPF to prevent this risk.

ALG Definition

Application Level Gateway (ALG) is a NAT traversal technology.

ALG Purpose

In NAT scenarios, the Application Level Gateway (ALG) function can automatically detect application-layer information of certain packets, generate corresponding access rules based on the application-layer information (generate a server map), and automatically translate the IP address and port information in packet payloads. NAT translates only the IP address and port in

Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

H323

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Descripción general de ASPF/ALG

Definición de ASPF

El filtro de paquetes específico de aplicación (ASPF) es una tecnología de filtrado de paquetes aplicada a la capa de aplicación, también denominada filtrado de paquetes basado en estado.

Propósito de ASPF

ASPF permite que el dispositivo detecte automáticamente la información de la capa de aplicación de ciertos paquetes y cree las reglas de acceso correspondientes (mapa de servidor) basándose en dicha información. El mapa de servidor se utiliza para permitir paquetes subsiguientes en el canal de datos, lo que equivale a crear una política de seguridad refinada. Por ejemplo, para protocolos multicanal (como FTP, H.323 y SIP), la dirección y el puerto de un canal de datos deben negociarse en un canal de control, y luego el canal de datos puede establecerse según el resultado de la negociación. El administrador no puede predecir la dirección y el puerto del canal de datos, ya que se negocian dinámicamente. Por lo tanto, le resulta imposible configurar políticas de seguridad completas y precisas. Para garantizar el correcto establecimiento del canal de datos, todos los puertos deben estar abiertos, lo que conlleva el riesgo de ataques al servidor o cliente. En este caso, puede habilitar ASPF para evitar este riesgo.

Definición de ALG

Application Level Gateway (ALG) es una tecnología de travesía NAT.

Propósito de ALG

En escenarios NAT, la función de Puerta de Enlace a Nivel de Aplicación (ALG) puede detectar automáticamente la información de la capa de aplicación de ciertos paquetes, generar las reglas de acceso correspondientes basándose en dicha información (generar un mapa de servidores) y

Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

REFERENCIAS TECNICAS

INGLES

H460Network

H.460 Network

Created: Oct 7, 2020 13:04:12 Latest reply: Mar 2, 2021 03:38:27 285 10 4 0

View the author #1



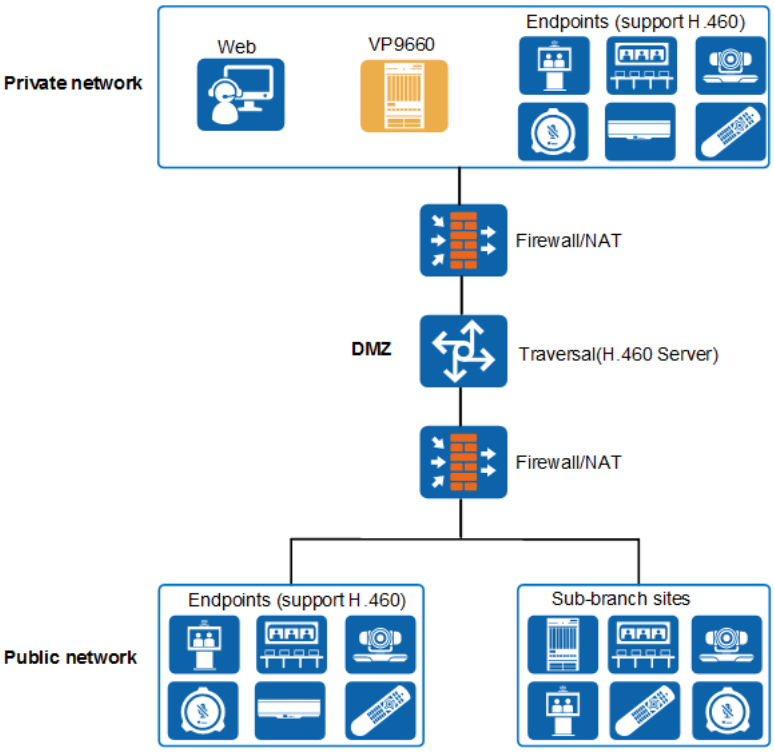
Mr.Jack L2 MVE

33 814

Follow

Post

H.460 is a protocol issued by the International Telecommunications Union (ITU) to deal with the firewall/NAT traversal. This protocol can implement traversal between public and private networks.



the VP9660 is deployed in a private network,and register the VP9660 with the traversal server. Traversal is implemented with the help of the traversal server.

- The H.460 protocol consists of two parts: H.460.18 and H.460.19. The former deals with H.323 call signaling's traversal while the latter deals with the media data's traversal.
- Firewall/NAT: indicates a firewall, NAT device, or a NAT-capable firewall.
- Traversal server: used to provide GK functions, forward calls and signaling from the public network, and assist media stream traversal and multiplexing.
- The network requires several communications ports in the firewall to be enabled. Apart from that, no other changes to an enterprise's existing network security solution are needed, which helps data control within and without the enterprise.
- All videoconferencing devices in the network must be H.460 capable.

RECOMMENDED

1 eSight installation problem

2 U2000 unable to sync the NE

3 VLAN

4 Imaster Campus NCE

5 NETWORK CUTOVER

Helpful (4) Favorite(0) Share Report

Previous: Fix Slowness Problem with SecureCRT

Next: MPLS forwarding plane and control plane

We use cookies on this site,including third party cookies,in order for the site to work properly and to analyse traffic,offer enhanced functionality,social media features and personalise content and ads.Learn more

cookie settings Accept Cookies

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

H460Network

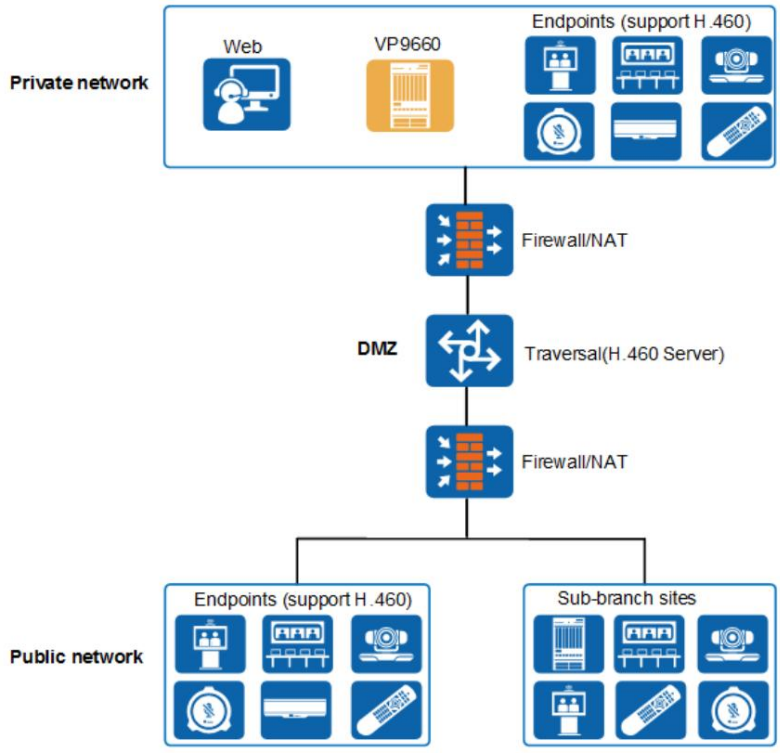
Machine Translated by Google

Red H.460

Creado: 7 oct. 2020 13:04:12 Última respuesta: 2 mar. 2021 03:38:27 285 10 4 0

Ver al autor #1

H.460 es un protocolo emitido por la Unión Internacional de Telecomunicaciones (UIT) para gestionar la travesía de firewalls/NAT. Este protocolo permite la travesía entre redes públicas y privadas.



El VP9660 se implementa en una red privada y se registra con el servidor transversal.
La travesía se implementa con la ayuda del servidor de travesía.

- El protocolo H.460 consta de dos partes: H.460.18 y H.460.19. La primera se ocupa de la señalización de llamadas H.323. recorrido, mientras que el último se ocupa del recorrido de los datos multimedia.
- Firewall/NAT: indica un firewall, un dispositivo NAT o un firewall con capacidad NAT.
- Servidor transversal: se utiliza para proporcionar funciones GK, reenviar llamadas y señalización desde la red pública y ayudar a la travesía y multiplexación de flujos de medios.
- La red requiere la habilitación de varios puertos de comunicación en el firewall. Además, no se requieren cambios adicionales en la solución de seguridad de red existente de la empresa, lo que facilita el control de datos dentro y fuera de la empresa.
- Todos los dispositivos de videoconferencia de la red deben ser compatibles con H.460.

Útil (4) Favorito(0) Compartir Informar



Señor Jack VE

33 814

Seguir Ch

Correo

RECOMENDADO

1 Problema de instalación de eSight

2 U2000 no puede sincronizar el NE

3 VLAN

4 Campus Imaster NCE

5 CORTE DE RED

Anterior: Solucione el problema de lentitud con SecureCRT

Siguiente: Plano de reenvío MPLS y plano de control

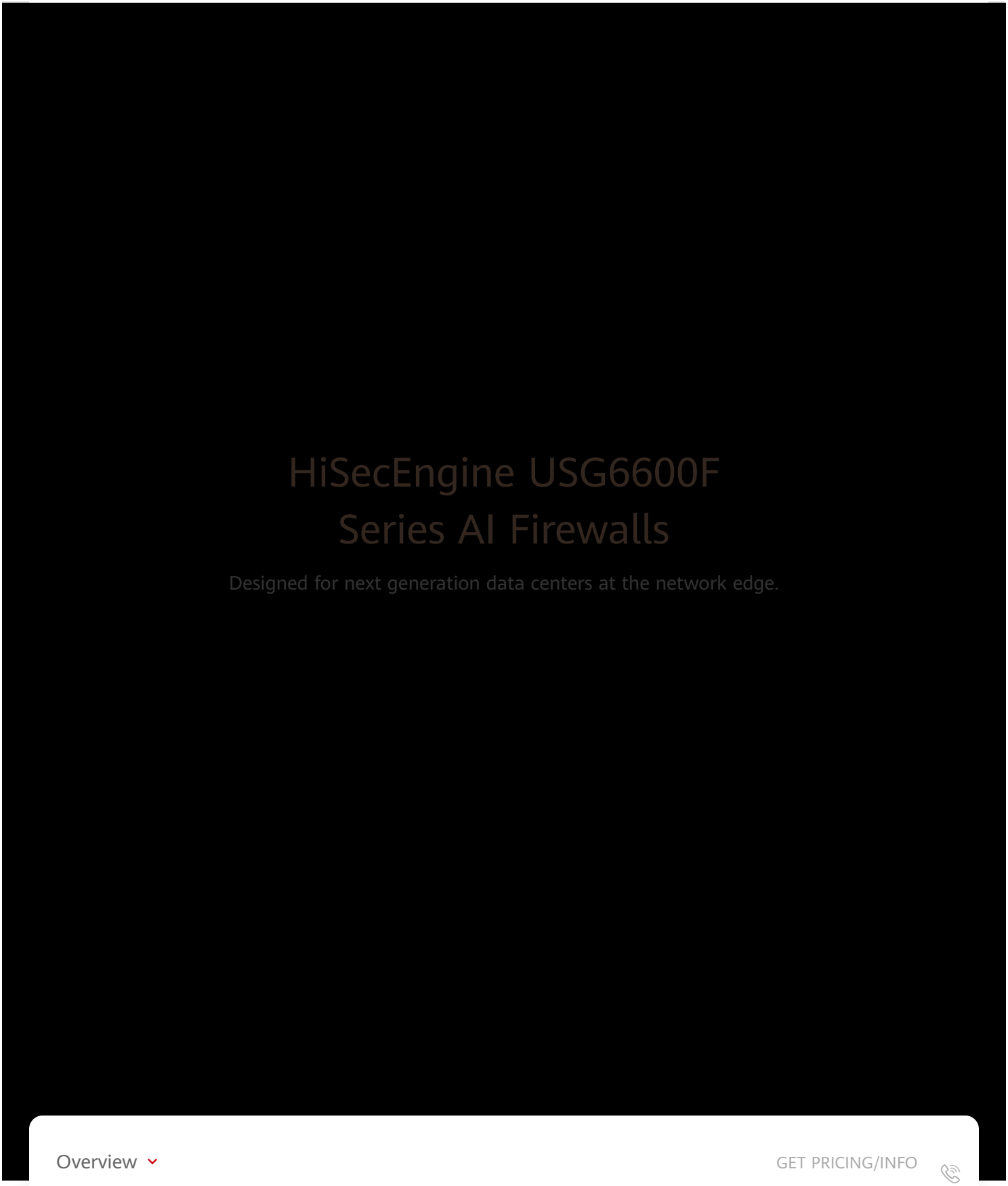
Utilizamos cookies en este sitio, incluidas cookies de terceros, para que el sitio funcione correctamente y para analizar el tráfico, ofrecer una mejor funcionalidad, funciones de redes sociales y personalizar el contenido y los anuncios. Más información

configuración de cookies Aceptar cookies

REFERENCIAS TECNICAS

INGLES

HiSecEngineUSG6600F



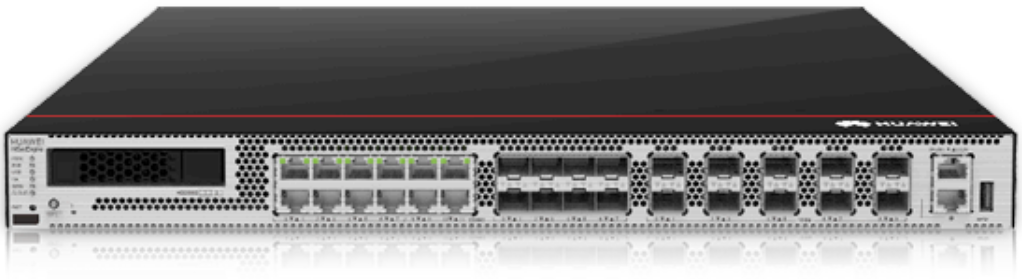
Overview

GET PRICING/INFO

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. Read our privacy policy>

HiSecEngine USG6600F Series AI Firewalls

Huawei HiSecEngine USG6600F Series Artificial Intelligence (AI) Firewalls are designed for next generation data centers at the network edge. Based on new software and hardware platforms, the series provides Internet Protocol version 4 (IPv4)/IPv6 dual-stack capabilities, greatly improving service performance, with intelligent technologies further helping to effectively defend against today's advanced threats.



Superb Performance

New software and hardware platforms greatly improve service performance.

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. Read our privacy policy>



Intelligent Defense

Real-time threat processing at the network edge, with an unknown threat detection accuracy of



Simplified O&M

Threat visualization defines the new security interface and greatly improves Operations and Maintenance (O&M).

Specifications

Parameters	USG6615F	USG6625F	USG6635F	USG6655F
Fixed Interfaces	8 x GE COMBO + 4 x GE (RJ45) + 4 x GE (SFP) + 6 x 10 GE (SFP+)	8 x GE COMBO + 4 x GE (RJ45) + 4 x GE (SFP) + 6 x 10 GE (SFP+)	8 x GE COMBO + 4 x GE (RJ45) + 10 x 10 GE (SFP+)	8 x GE COMBO + 4 x GE (RJ45) + 10 x 10 GE (SFP+)
Form Factor/Height	1U			

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. Read our privacy policy>

Integrated Protection	Provides firewall, VPN, intrusion prevention, antivirus, bandv
Application Identification and Control	Identifies over 6000 applications and supports the access co application identification with intrusion detection, antivirus,
Intrusion Prevention and Web Protection	Rapidly obtains the latest threat information for accurate de device can defend against web-specific attacks, including SC
DDoS Attack Mitigation	Uses technologies such as source IP address detection, finge over 10 common DDoS attacks and over 20 single-packet at HTTPS flood, DNS flood, and SIP flood attacks, and supports
Antivirus	Supports intelligent antivirus engine that can detect hundre
VPN encryption	Supports multiple highly available VPN features, such as IPs

Resources

Brochures

HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls (Fixed-Configuration) Datasheet

About Us

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. Read our privacy policy>

Partner

Resources

Quick Links

Huawei e+ App

HUAWEI eKit App

Huawei HiKnow App

HUAWEI eFly App

Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.
Privacy Terms of use

This site uses cookies. By continuing to browse the site you are agreeing to our use of cookies. Read our privacy policy>

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

HiSecEngineUSG6600F

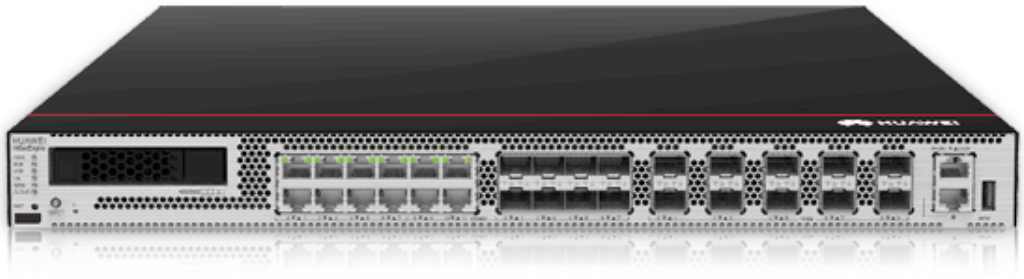


Este sitio utiliza cookies. Al continuar navegando, acepta nuestro uso de cookies. Lea nuestra política de privacidad.

Descripción general

OBTENGA PRECIOS/INFORMACIÓN

Los firewalls de Inteligencia Artificial (IA) Huawei HiSecEngine serie USG6600F están diseñados para centros de datos de última generación en el borde de la red. Basados en nuevas plataformas de software y hardware, estos firewalls ofrecen capacidades de doble pila IPv4/IPv6, lo que mejora significativamente el rendimiento del servicio, con tecnologías inteligentes que contribuyen a una defensa eficaz contra las amenazas avanzadas actuales.



Excelente rendimiento

Las nuevas plataformas de software y hardware mejoran enormemente el rendimiento del servicio.

Este sitio utiliza cookies. Al continuar navegando, acepta nuestro uso de cookies. Lea nuestra política de privacidad.

350

Defensa inteligente

Procesamiento de amenazas en tiempo real en el borde de la red, con una precisión de detección de amenazas desconocidas del 95%.



Operaciones y mantenimiento simplificados

La visualización de amenazas define la nueva interfaz de seguridad y mejora enormemente las operaciones y el mantenimiento (O&M).

Presupuesto

Este sitio utiliza cookies. Al continuar navegando, acepta nuestro uso de cookies. Lea nuestra política de privacidad.

Interfaces fijas	8 conectores GE COMBO + 4 conectores GE (RJ45) + 4 conectores GE (SFP) + 6 conectores 10 GE (SFP+)	8 conectores GE COMBO + 4 conectores GE (RJ45) + 4 conectores GE (SFP) + 6 conectores 10 GE (SFP+)	8 conectores GE COMBO + 4 conectores GE (RJ45) + 10 conectores 10 GE (SFP+)	8 conect GE COMB 4 conect GE (RJ + 10 conect 10 GE (SFP+)
Factor de forma/altura	1U			
Protección integrada	Proporciona firewall, VPN, prevención de intrusiones, anti más.			
Identificación y control de aplicaciones	Identifica más de 6000 aplicaciones y admite la granulari Combina la identificación de aplicaciones con la detecció rendimiento y la precisión de la detección.			
Prevención de intrusiones y protección web	Obtiene rápidamente la información más reciente sobre a basados en vulnerabilidades. El dispositivo puede defende			

Este sitio utiliza cookies. Al continuar navegando, acepta nuestro uso de cookies. Lea nuestra política de privacidad.

Mitigación de ataques DDoS	Utiliza tecnologías como detección de dirección IP de orig para defenderse contra más de 10 ataques DDoS comune inundación UDP, inundación ICMP, inundación HTTP, inun aprendizaje de línea de base de tráfico y filtrado basado e
Antivirus	Admite un motor antivirus inteligente que puede detectar
Cifrado VPN	Admite múltiples funciones VPN de alta disponibilidad, cc

Recursos

Folletos

Ficha técnica de los firewalls con IA HUAWEI HiSecEngine series USG6600F y USG6700F (configuración fija)

Este sitio utiliza cookies. Al continuar navegando, acepta nuestro uso de cookies. Lea nuestra política de privacidad.

Aplicación Huawei HiKnow

Aplicación HUAWEI eFly

Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.
Privacidad Condiciones de uso

Este sitio utiliza cookies. Al continuar navegando, acepta nuestro uso de cookies. Lea nuestra política de privacidad.

REFERENCIAS TECNICAS

INGLES

HUAWEI HiSecEngine

HUAWEI HiSecEngine USG6600F&USG6700F Series AI Firewalls

1 Overview

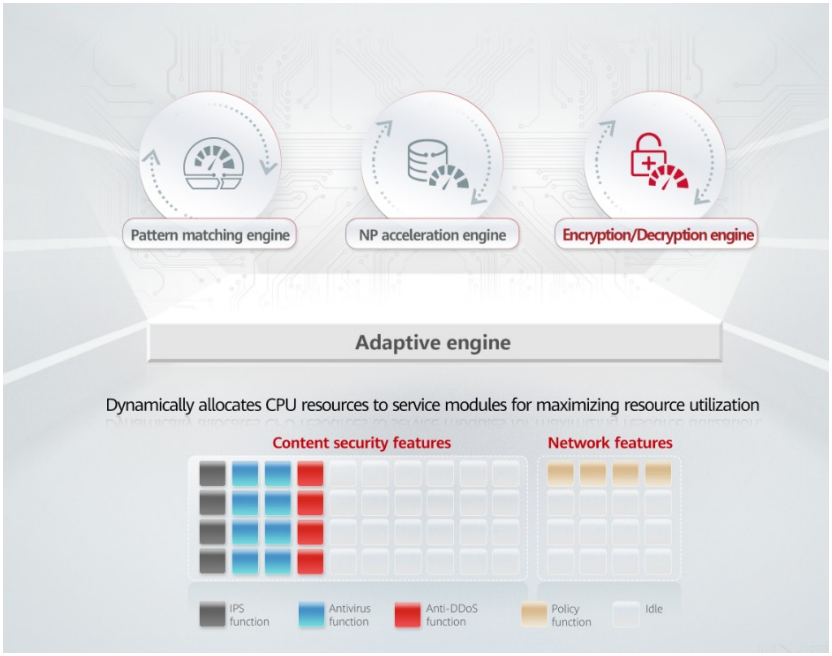
As digitalization is sweeping the world, extensive connections, explosive growth of data, and booming intelligent applications are profoundly changing the way we live and work. Enterprise services are going digital and moving to the cloud, which promotes the transformation of enterprise networks while bringing greater challenges to network security. As threats increase, unknown threats are ever-changing and highly covert. As users' requirements for security services increase, performance and latency become bottlenecks. With mass numbers of security policies and logs, threat handling and O&M are extremely time-consuming. As the "first gate" on network borders, firewalls are the first choice for enterprise security protection. However, traditional firewalls can only analyze and block threats based on signatures and therefore are unable to effectively handle unknown threats. In addition, the effectiveness of threats depends on the professional experience of O&M personnel. The single-point, reactive, and in-event defense method cannot effectively defend against unknown threat attacks, let alone threats hidden in encrypted traffic.

With new hardware and software architectures, Huawei HiSecEngine USG6000F series are next-generation AI firewalls that feature intelligent defense, outstanding performance, and simplified O&M, effectively addressing the preceding challenges. The USG6000F series uses intelligence technologies to enable border defense to accurately block known and unknown threats. Equipped with multiple built-in security-dedicated acceleration engines, the USG6000F series firewalls support enhanced forwarding, content security detection, and IPsec service processing acceleration. The security O&M platform implements unified management and O&M of multiple types of security products, such as firewalls, anti-DDoS devices, reducing security O&M OPEX.

2 Product Highlights

Excellent performance

By leveraging fresh-new hardware and software architectures of forwarding and control separation, HiSecEngine USG6000F series AI firewalls dynamically allocate resources to service modules through the adaptive security engine (ASE), maximizing resource utilization and improving overall service performance. For core services, the HiSecEngine USG6000F series also supports network processor (NP), pattern matching, and encryption/decryption engines. These engines greatly improve short-packet forwarding, reduce the forwarding latency, and enhance application identification, intrusion prevention detection, and IPsec service performance.



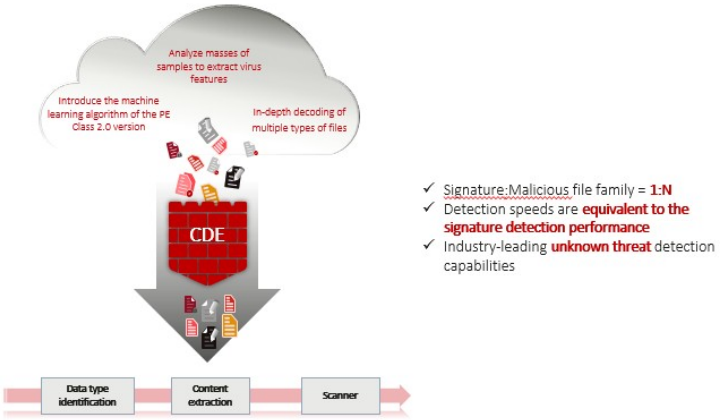
Intelligent defense

HiSecEngine USG6000F series AI firewalls provide content security functions, such as application identification, IPS, antivirus, and URL filtering to protect intranet servers and users against threats. HiSecEngine USG6000F series also support to detect unknown threats by interworking with sandbox.

Traditional IPS signatures are manually produced through analysis, resulting in low productivity. Also, the accuracy of the signatures depends heavily on expert experience. Huawei innovatively enables the IPS signature production on the intelligent cloud by adopting intelligence technologies and utilizing expert experience. Such an intelligent mode helps increase the signature productivity by 30 times compared with manual production, reduce errors caused by manual analysis, and continuously improve the accuracy of intrusion detection.

The built-in antivirus content-based detection engine (CDE) powered by intelligence technologies can detect unknown threats and provide in-depth data analysis. With these capabilities, the CDE-boosted firewall is able to gain insight into threat activities and quickly detect malicious files, effectively improving the threat detection rate.

NGFW USG supports to detect and defend malware spreading and network attacks, like Worm, Virus, Trojan-horse, Spyware, etc. malware spreading and botnet, DoS/DDoS, SQL injection, cross site attack,ransomware,etc.



Simplified O&M

The HiSecEngine USG6000F series provides a brand-new web UI, which intuitively visualizes threats as well as displays key information such as device status, alarms, traffic, and threat events. With multi-dimensional data drilling, the web UI offers optimal user experience, enhanced usability, and simplified O&M.

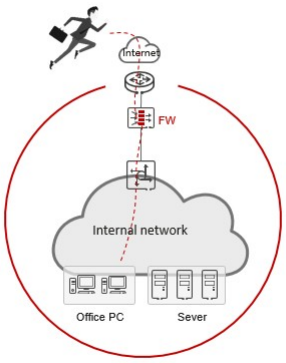
The HiSecEngine USG6000F series firewalls can be centrally managed by the security management platform SecoManager, implementing a shift from single-point defense to collaborative network protection. The SecoManager provides policy tuning and intelligent O&M capabilities. It can also manage security products, such as anti-DDoS devices to quickly eliminate network threats and improve security handling effectiveness.

The HiSecEngine USG6000F series NGFW can also be managed by NCE-Campus, and NCE-Campus can also support to manage switch, AR, POL device at the same time, even third party devices.

A wide range of network features

Huawei HiSecEngine USG6000F series also provides various network features such as VPN, IPv6, and intelligent traffic steering.

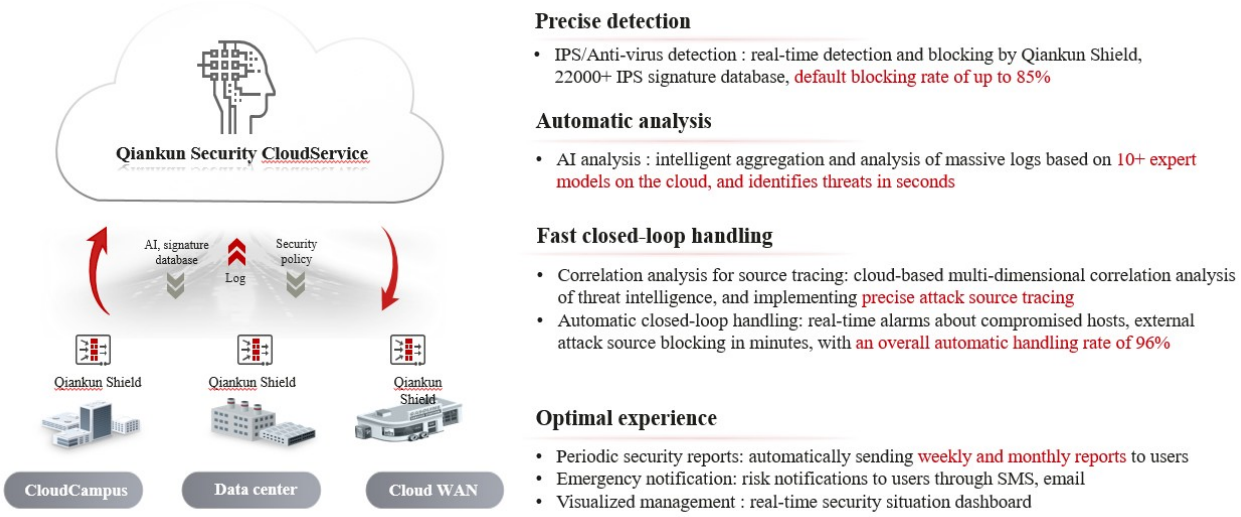
- Provides various VPN features such as IPsec VPN and SSL VPN, and supports multiple encryption algorithms, such as DES, 3DES, AES, and SHA, ensuring secure and reliable data transmission.



- Provides secure and rich IPv6 network switchover, policy control, security protection, and service visualization capabilities, helping government, media, carrier, Internet, and finance sectors implement IPv6 reconstruction.
- Provides dynamic and static intelligent traffic steering based on multi-egress links, selects the outbound interface based on the specified link bandwidth, weight, or priority, forwards traffic to each link based on the specified traffic steering mode, and dynamically tunes the link selection result in real time to maximize the usage of link resources and improve user experience.

Collaboration with Huawei Qiankun Security Cloud Service

- Most threats and attacks come from network traffic. Firewalls are deployed at the egress of the local network to interwork with Huawei Qiankun security cloud service to implement automatic threat analysis and handling. This ensures the interconnection between the intranet and extranet, effectively intercepts traffic attacks, and automatically handles external attack sources. Protects enterprise network resources.



- By associating with Huawei Qiankun security cloud service, the firewall can obtain security services such as border protection and response on demand. Lightweight deployment and unified cloud O&M effectively reduce hardware stacking and greatly reduce enterprise security investment and O&M difficulties.

3 Deployment

Small data center border protection

- Firewalls are deployed at egresses of data centers, and functions and system resources can be virtualized. The firewall has multiple types of interfaces, such as 100G,40G, 10G, and 1G interfaces. Services can be flexibly expanded without extra interface cards.
- The intrusion prevention capability effectively blocks a variety of malicious attacks and delivers differentiated defense based on virtual environment requirements to guarantee data security.
- VPN tunnels can be set up between firewalls and mobile workers and between firewalls and branch offices for secure and low-cost remote access and mobile working.

Enterprise border protection

- Firewalls are deployed at the network border. The built-in traffic probe can extract packets of encrypted traffic to monitor threats in encrypted traffic in real time.
- The policy control and data filtering functions of the firewalls are used to monitor social network applications to prevent data breach and protect enterprise networks.

4 Product Appearance

Figure 4-1 HiSecEngine USG6615F/USG6625F

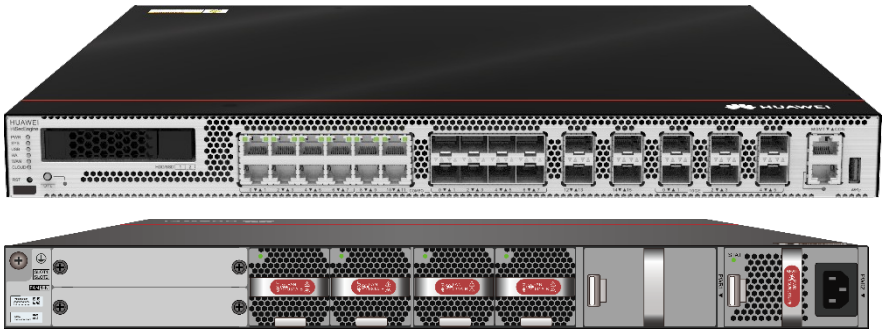
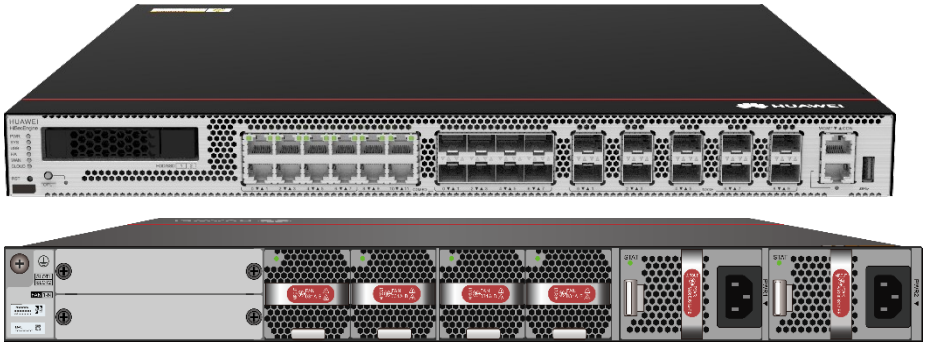


Figure 4-2 HiSecEngine USG6635F/USG6655F/USG6685F



360

Figure 4-3 HiSecEngine USG6710F/USG6715F

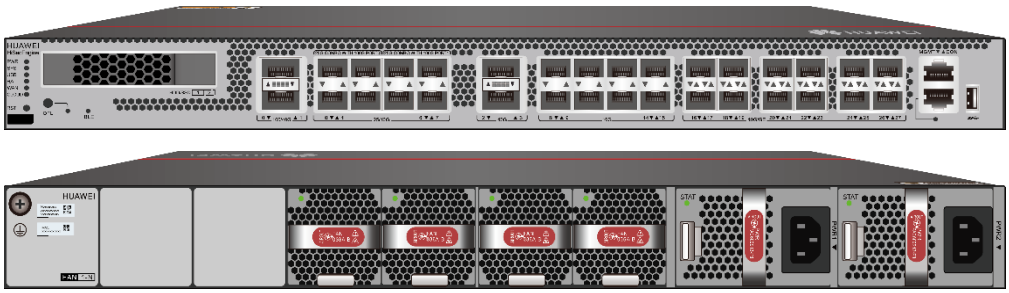
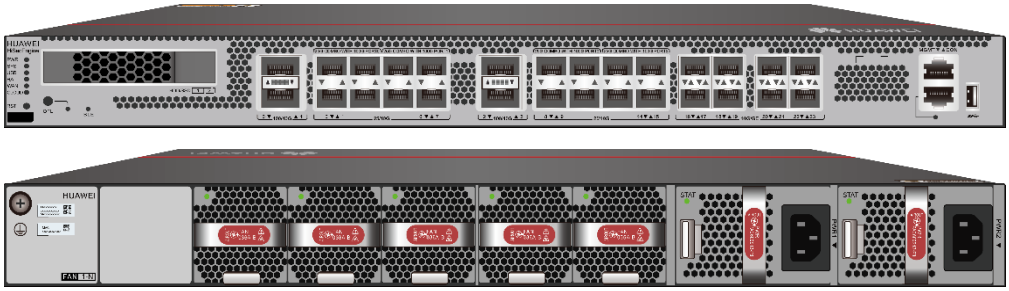


Figure 4-4 HiSecEngine USG6725F



5 Software Features

Feature	Description
Integrated protection	Integrates firewall, VPN, intrusion prevention, antivirus, bandwidth management, Anti-DDoS, and URL filtering functions, and provides a global configuration view and integrated policy management.
Application identification and control	Application identification based on signatures, correlation, and behaviors instead of ports; 6000+ preset applications, which can be further classified; support for user-defined applications; 50+ categories and 20+ risk labels for access control based on categories and labels; automatic update of the application identification signature database
Security policy management	Supports traffic management and control based on the VLAN ID, 5-tuple, security zone, region, application, and time range, and implements integrated content security inspection. Provides predefined templates for common attack defense scenarios to facilitate security policy deployment. Supports interworking with third-party policy management software (FireMon and Algosec) to facilitate security O&M.
Bandwidth management	Manages per-IP bandwidth based on service application identification to guarantee the network experience of key services and users. The management and control can be implemented by limiting the maximum bandwidth, guaranteeing the minimum bandwidth, and changing the application forwarding priority.
Intrusion	Obtains the latest threat information in a timely manner and accurately detects and

prevention	prevents vulnerability exploits; covers tens of thousands of CVE vulnerabilities; prevents the exploit of vulnerabilities (such as those in Windows and Unix/Linux operating systems, databases, Apache, IIS, and Tomcat as well as middleware), web attacks (such as SQL injection, XSS, and RCE), botnets, remote control, and Trojan horses; supports brute force cracking detection based on user behavior; provides 25,000+ predefined signatures and supports user-defined signatures and automatic signature database update; supports attack forensics collection, full-flow packet obtaining (including three-way handshake information), and attack fragment display to facilitate O&M; supports X-Forwarded-For (XFF) field extraction.
WAF	Uses signature, semantic analysis, and machine learning technologies to detect OWASP top 10 attacks, such as SQL injection, cross-site scripting, RCE, CSRF, and deserialization, and supports anti-leeching and web page anti-tampering; supports HTTP method and field length control.
Antivirus	Detects malware in files transmitted through protocols like HTTP, FTP, SMTP, POP3, IMAP4, NFS, and SMB; detects Trojan horses, worms, spyware, vulnerability exploits, adware, hacker tools, Rootkit, backdoors, grayware, botnet programs, ransomware, phishing software, cryptojacking software, and web shell programs; supports virus detection for Office files, executable files (Windows/Linux/MacOS), script files, flash files, PDF files, RTF files, web pages, and images; supports attack forensics collection; supports the inspection of archive files of up to 100 nested compression levels in multiple compression formats, such as tar, gzip, zip, rar, and 7z, and supports multiple actions, such as alert, block, add declaration, and attachment deletion.
Advanced malware prevention	The heuristic antivirus engine uses detection technologies such as AI, semantic analysis, and Emulator, coupled with threat and reputation information, to detect packed malware, script morphing, and malware embedded in compound documents. It can detect billions of malware variants and supports automatic update of the signature database. In addition, it can send suspicious files to the local or cloud sandbox for further inspection to detect zero-day malware.
Web security	The URL category database on the cloud contains 500 million URLs in over 130 categories, such as news, games, gambling, drugs, and malicious web pages. URLs cover over 100 languages, and key categories of URLs cover over 20 languages. The URL category query servers are deployed in multiple countries/regions to provide high-speed and low-latency category query services. User-defined URL/host whitelist and blacklist are supported. HTTPS traffic can be filtered without decryption. TLS/SSL traffic can be decrypted before filtering. HTTP/2 and QUIC traffic can be filtered, and URL categories can be imported in batches. URL access can be controlled based on users/user groups, time ranges, and security zones to precisely manage users' online behaviors.
DNS security	Based on massive threat information, technologies such as AI and knowledge graph are used to detect malicious DNS requests, including C&C domain names, DGA-generated domain names, compromised sites, and malicious domain names such as cryptojacking, ransomware, and phishing domain names. The local malicious domain name database supports a maximum of 2 million malicious domain names. DNS category-based filtering, DNS safe search, and DNS redirection (sinkholing) are also supported.

Anti-botnet/ spyware	Supports the detection and prevention of viruses and advanced malware, such as botnets, Trojan horses, worms, remote control tools, and spyware, and prevents the download of malware; quickly detects malicious traffic like C&C based on signatures, IP addresses, and domain reputation information; displays the roles of communication parties in botnet attack logs.
Threat information	Huawei Intelligent Security Center leverages multiple AI algorithms and expert analysis to generate massive threat information about IP addresses, domain names, URLs, and files on a daily basis. The threat information is automatically synchronized to devices for threat detection to quickly block emerging attacks. In addition, it can interconnect with third-party threat information sources to enrich inspection rules.
OT/IoT security	Supports common industrial control protocols such as Modbus, S7, Profinet, and OPC, identification and control of IoT devices such as cameras, and IoT asset risk assessment. Supports vulnerability detection for IoT devices like cameras and industrial control software and protocols like ICS/SCADA. The traffic probe function, coupled with HiSec Insight situational awareness system, can learn the traffic behavior baseline of IoT assets and detect and evaluate IoT asset risks. For details about the list of supported OT protocols, see https://isecurity.huawei.com/security/wiki/application (Business Systems > Industrial).
Flow probe	Collects and parses metadata and attack forensics information, including network-layer metadata (such as IP addresses, ports, and packet characteristics) and application-layer metadata (such as field information obtained after in-depth parsing of protocols like HTTP, DNS, TLS, and SSH), and sends the data to the HiSec Insight security situational awareness platform for further analysis by using algorithms, such as deep learning and machine learning algorithms, to detect potential, unknown, and advanced threats in network traffic.
Anti-DDoS	Uses technologies such as source IP address detection, fingerprint detection, and dynamic traffic limiting to defend against over 10 common DDoS attacks and over 20 single-packet attacks, such as SYN flood, UDP flood, ICMP flood, HTTP flood, HTTPS flood, DNS flood, and SIP flood attacks, and supports traffic baseline learning and IP reputation-based filtering.
Mail filtering	Supports mail address filtering (covering the sender and recipient addresses) and SMTP mail sending rate limiting.
DLP	Supports identification of 100+ real file types, user-defined file name extensions, and file type-based upload/download control; supports keyword filtering for Office documents, web pages, code, and TXT files; supports user-defined keywords, regular expressions, and weight configuration.
SaaS access control	Supports SaaS application identification and access control based on signatures, DNS, IP addresses (IP address database of the top 50 SaaS applications), and first packets, and supports traffic steering based on SaaS applications, ensuring good SaaS application experience.
Behavior audit	Audits and regulates common user online behaviors, including FTP operations (upload, download, and command), HTTP operations (posting, search, and browsing), DNS, Telnet, SNMP, and email sending and receiving operations.

Intelligent uplink selection	Supports service-specific PBR and intelligently selects the optimal link based on multiple types of load balancing criteria (such as the bandwidth ratio and link health status) in multi-ISP scenarios.
VPN encryption	Supports various highly reliable VPN features, such as IPsec VPN, SSL VPN, and GRE, and multiple encryption algorithms, such as DES, 3DES, AES, SHA, SM2, SM3, and SM4.
SSL-encrypted traffic inspection	Detects and defends against threats hidden in TLS/SSL-encrypted traffic, performs application-layer protection, such as intrusion prevention, antivirus, data filtering, and URL filtering, on decrypted TLS/SSL traffic, and supports URL category whitelist.
SSL offloading	Replaces the server to implement SSL encryption and decryption, reducing the server load and implementing load balancing of HTTP traffic.
Diversified reports	Provides visualized and multi-dimensional reports by IP address, application, time, traffic, or threat.
Security virtualization	Supports virtualization of multiple types of security services, including firewall, intrusion prevention, antivirus, and VPN services; allows users to separately conduct personalized management on the same physical device.
Routing	Supports multiple types of IPv4/IPv6 routing protocols, such as RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+, and IPv6 IS-IS.
IP multicast	Supports IPv4 Layer 3 multicast protocols, such as IGMP, MSDP, and PIM, and provides point-to-multipoint services to reduce bandwidth consumption.
Server load balancing	Supports IPv6, Layer 4/Layer 7 server load balancing, and multiple session persistence methods such as source IP address-based and HTTP cookie-based session persistence; supports SSL offloading and encryption; combines services and security policies to improve service security; supports health check based on multiple protocols such as TCP, RADIUS, DNS, and HTTP to detect server status changes promptly.
Deployment and reliability	Supports transparent (Layer 2), routing (Layer 3), tap, and hybrid working modes and high availability (HA), including the Active/Active and Active/Standby modes.
Security center	The built-in asset identification module can identify assets such as Windows, Linux, Android, and iOS assets and cameras, perform correlation analysis on threat logs and assets, and display asset risk assessment results and the entire kill chain.
SRv6	Supports IS-IS for SRv6, BGP for SRv6, SRv6 BE, SRv6 TE policy, SRv6 midpoint protection, SRv6 microloop avoidance, SRv6 OAM, SRv6 SRH compression, SRv6 TI-LFA FRR, and EVPN L3VPN.
Secure SD-WAN	Provides a built-in secure SD-WAN solution for low-cost and business-level Internet links. Supports zero-touch provisioning (ZTP) through email to complete device provisioning in minutes without requiring technical skills. Supports forward error correction (FEC) to prevent pixelated display and video freezing at a 30% packet loss rate; supports real-time link switching based on link quality ensure key application experience. Supports multi-link routing and dual-CPE flexible networking to ensure

	uninterrupted connections for site services; supports E2E IPsec encryption to ensure secure service transmission. Note: The USG6600F series can function as a hub or spoke. The USG6700F series does not support SD-WAN.
User authentication	Supports multiple authentication modes for Internet access users, including local Portal authentication and single sign-on (SSO). In local Portal authentication, the built-in Portal page of the device can be pushed to users, and the account and password entered on the Portal page by a user can be sent to the local database or RADIUS, HWTACACS, AD, or LDAP authentication server for authentication. SSO includes RADIUS SSO and Agile Controller (NCE-Campus) SSO.
O&M capability	Supports telemetry to automatically read information from hardware, such as fans, power modules, optical modules, Ethernet ports, temperature sensors, and drivers, and sends interface traffic statistics, CPU usage, and memory usage to the collector.
PPPoE	Functions as a PPPoE client to provide Internet access services, including user authentication and authorization and dynamic IP address allocation.
Firewall Interworking with Huawei Qiankun Security CloudService	
Service	**Description**
Border protection and response service	Intrusion detection and prevention: Leverages signatures to block application-layer attacks, terminates the transfer of phishing emails and malware (such as viruses and Trojan horses), detects compromised hosts on the internal network, and disconnects these hosts from the Internet to protect the security and stability of customer services.
	Automatic event analysis: Combines intelligent analysis and manual analysis by experts to analyze security events to ensure the accuracy of attack blocking and security alarms and optimize attack identification rules.
	Whitelist and blacklist: Supports whitelist and blacklist configuration on the Portal or app to protect services from threats.
	Periodic security reports: Generates weekly and monthly reports on security protection events and sends the reports to users by email.
	Emergency notification: Identifies emergencies from security events and sends notifications to users via SMS and email.

6 Specifications

System Performance and Capacity

Model	USG6615F	USG6625F	USG6635F	USG6655F
IPv4Firewall Throughput[1] (1518/512/64-byte, UDP)	15/15/15 Gbps	25 /25 /25 Gbps	35/35/35 Gbps	50/50/40 Gbps

Model	USG6615F	USG6625F	USG6635F	USG6655F
IPv6 Firewall Throughput1 (1518/512/84-byte, UDP)	15/15/15 Gbps	25 /25 /25 Gbps	35/35/25 Gbps	50/50/25 Gbps
Secure SD-WAN EVPN Throughput(1400/512 byte,UDP) [9]	15/15 Gbps	25 /25 Gbps	35/35 Gbps	50/40 Gbps
Secure SD-WAN EVPN tunnels	3,000	3,000	6,000	6,000
Firewall Latency (64-byte, UDP)	18 µs	18 µs	18 µs	18 µs
Firewall Latency[8] **(64-byte, UDP)**	7 µs	7 µs	7 µs	7 µs
Concurrent Sessions (HTTP1.1)[1]	10,000,000	10,000,000	20,000,000	20,000,000
New Sessions/Second (HTTP1.1)[1]	250,000	250,000	500,000	500,000
FW + SA* Throughput[2]	12Gbps	12Gbps	23Gbps	26.5Gbps
NGFW Throughput[3] **(HTTP 100K)**	6Gbps	10Gbps	16Gbps	25Gbps
NGFW Throughput (Enterprise Mix)[4]	4.6Gbps	5Gbps	8Gbps	8.5Gbps
Threat Protection Throughput (Enterprise Mix)[5]	4Gbps	4Gbps	7Gbps	8Gbps
IPsec VPN Throughput[1] **(AES-256 + SHA256, 1420-byte)**	15Gbps	25Gbps	30Gbps	30Gbps
Maximum IPsec VPN Tunnels	20,000	20,000	20,000	20,000
SSL Inspection Throughput[7]	2.5 Gbps	2.5 Gbps	4 Gbps	4 Gbps
SSL VPN Throughput [6]	1 Gbps	1.5 Gbps	3 Gbps	3 Gbps
Concurrent SSL VPN Users *(Default/Maximum)	100/4000	100/8000	100/10000	100/10000
Security Policies (Maximum)	50,000	50,000	150,000	150,000
Virtual Firewalls	2048	2048	2048	2048
URL Filtering: Categories	More than 130			
URL Filtering: URLs	A database of over 500 million URLs in the cloud			
Automated IPS Signature	Yes, an industry-leading security center from Huawei			

Model	USG6615F	USG6625F	USG6635F	USG6655F
Updates	(http://sec.huawei.com/sec/web/index.do)			
Third-Party and Open-Source Ecosystem	Open API for integration with third-party products, providing NETCONF interfaces Other third-party management software based on SNMP, SSH, and Syslog			
VLANs (Maximum)	4094			
VLANIF Interfaces (Maximum)	4094			

Model	USG6685F	USG6710F	USG6715F	USG6725F
IPv4Firewall Throughput[1] (1518/512/64-byte, UDP)	80/80/40 Gbps	100/100/60 Gbps	160/160/80 Gbps	240/240/120 Gbps
IPv6 Firewall Throughput1 (1518/512/84-byte, UDP)	80/80/25 Gbps	100/100/45 Gbps	160/160/50 Gbps	240/240/85 Gbps
Secure SD-WAN EVPN Throughput(1400/512 byte,UDP)[9]	50/40 Gbps	/	/	/
Secure SD-WAN EVPN tunnels	6000	/	/	/
Firewall Latency (64-byte, UDP)	18 µs	35 µs	35 µs	35 µs
Firewall Latency[8] (64-byte, UDP)	7µs	7 µs	7 µs	7 µs
Concurrent Sessions (HTTP1.1)[1]	25,000,000	50,000,000	50,000,000	75,000,000
New Sessions/Second (HTTP1.1)[1]	750,000	1,500,000	1,500,000	2,250,000
FW + SA* Throughput[2]	26.5Gbps	50Gbps	55Gbps	80Gbps
NGFWThroughput[3](HTTP 100K)	25Gbps	40Gbps	50Gbps	75Gbps
NGFW Throughput (Enterprise Mix)[4]	8.5Gbps	16Gbps	17Gbps	26Gbps
Threat Protection Throughput (Enterprise Mix)[5]	8Gbps	14Gbps	16Gbps	24Gbps
IPsec VPN Throughput[1] (AES-256 + SHA256, 1420-	30Gbps	40Gbps	45Gbps	65 Gbps

Model	USG6685F	USG6710F	USG6715F	USG6725F
byte)				
Maximum IPsec VPN Tunnels	20000	80000	80000	120000
SSL Inspection Throughput[7]	4 Gbps	8 Gbps	8 Gbps	12 Gbps
SSL VPN Throughput[6]	5 Gbps	10 Gbps	10 Gbps	12 Gbps
Concurrent SSL VPN Users *(Default/Maximum)	100/10000	100/20000	100/20000	100/30000
Security Policies (Maximum)	150,000	160,000	160,000	160,000
Virtual Firewalls	2048	2048	2048	2048
URL Filtering: Categories	More than 130			
URL Filtering: URLs	A database of over 500 million URLs in the cloud			
Automated IPS Signature Updates	Yes, an industry-leading security center from Huawei (http://sec.huawei.com/sec/web/index.do)			
Third-Party and Open-Source Ecosystem	Open API for integration with third-party products, providing NETCONF interfaces Other third-party management software based on SNMP, SSH, and Syslog			
VLANs (Maximum)	4094			
VLANIF Interfaces (Maximum)	4094			

1. Performance is tested under ideal conditions based on RFC2544, 3511. The actual result may vary with deployment environments.
2. SA performances are measured using 100 KB HTTP files.
3. NGFW throughput is measured with Firewall, SA, and IPS enabled; the performance is measured using 100 KB HTTP files.
4. NGFW throughput is measured with Firewall, SA, and IPS enabled; the performance is measured using the Enterprise Mix Traffic Model.
5. The threat protection throughput is measured with Firewall, SA, IPS, and AV enabled; the performance is measured using the Enterprise Mix Traffic Model.
6. SSL VPN throughput is measured using TLS v1.2 with AES128-SHA.
7. SSL inspection throughput is measured with IPS-enabled and HTTPS traffic using TLS v1.2 with TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256.
8. The data test condition is the interface pair mode .
9. The SD-WAN tunnel is packed with GRE over IPSec.

7 Hardware Specifications

Model	USG6615F	USG6625F	USG6635F	USG6655F
Chassis Height	1 U			
Dimensions (H x W x D) mm	43.6 x 442 x 420			
Fixed Interface	8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+		8*GE COMBO + 4*GE RJ45 + 10*10GE SFP+	
USB Port	1 x USB 3.0			
Weight	6.3 kg		7.3 kg	
Hardware	Optional, SATA (1 x 2.5 inch) supported, 240GB/480GB/960GB/1920GB, hot-swappable			
Power Supply(AC)	100 V to 240 V			
Maximum power consumption of the machine	222 W		242 W	
Power Supplies	Optional dual AC power supplies		Dual AC power supply	
Operating Environment (Temperature/Humidity)	Temperature: 0°C to 45°C Humidity: 5% to 95%, non-condensing			
Non-operating Environment	Temperature: –40°C to +70°C Humidity: 5% to 95%, non-condensing			
Installation Type	Rack			

Model	USG6685F	USG6710F	USG6715F	USG6725F
Chassis Height	1 U			
Dimensions (H x W x D) mm	43.6 x 442 x 420	43.6 x 442 x 600		
Fixed Interface	8*GE COMBO + 4*GE(RJ45)+ 10*10GE(SFP+)	2*100GE(QSFP28) + 2*40G(QSFP+)+ 8*25(ZSFP+) + 20*10GE(SFP+)[1]		4*100GE(QSFP28) + 16*25GE(ZSFP+) + 8*10GE(SFP+)[2]
USB Port	1 x USB 3.0			
Weight	7.3 kg	10.26 kg		10.6 kg
External Storage	Optional, SATA (1 x 2.5 inch) supported, 240GB/480GB/960GB /1920GB			
Power Supply	100 V to 240 V			

Model	USG6685F	USG6710F	USG6715F	USG6725F
Maximum power consumption of the machine	242 W	391 W		445 W
Power Supplies	Dual AC power supplies			
Operating Environment (Temperature/Humidity)	Temperature: 0°C to 45°C Humidity: 5% to 95%, non-condensing			
Non-operating Environment	Temperature: –40°C to +70°C Humidity: 5% to 95%, non-condensing			
Installation Type	Rack	Rack (19-inch standard cabinet)		

1. *Some 100GE interfaces and 25GE interfaces of USG6710F and USG6715F are mutually exclusive.*
2. *Some 100GE interfaces and 25GE interfaces of USG6715F are mutually exclusive.*

8 Ordering Information

Note:

1、The ordering information of USG6625F/USG6635F/USG6655F/USG6685F is the same as USG6615F

2、The ordering information of USG6710F/USG6715F is the same as USG6725F

3、The model USG6615F support Qiankun Security Cloud Service

Product	Model	Description
USG6615F	USG6615F-AC	USG6615F AC Host (8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+, 1 AC power supply)
USG6725F	USG6725F-AC	USG6725F AC Host (4*QSFP28 + 16*ZSFP+ + 8*SFP+,,2 AC power supplies)
Function License		
Virtual Firewall	LIC-USG6KF-VSYS-10	Quantity of Virtual Firewall (10 Vsys)
	LIC-USG6KF-VSYS-20	Quantity of Virtual Firewall (20 Vsys)
	LIC-USG6KF-VSYS-50	Quantity of Virtual Firewall (50 Vsys)
	LIC-USG6KF-VSYS-100	Quantity of Virtual Firewall (100 Vsys)
	LIC-USG6KF-VSYS-200	Quantity of Virtual Firewall (200 Vsys)
	LIC-USG6KF-VSYS-500	Quantity of Virtual Firewall (500 Vsys)
	LIC-USG6KF-VSYS-1000	Quantity of Virtual Firewall (1000 Vsys)
SSL VPN	LIC-USG6KF-SSLVPN-100	Quantity of SSL VPN Concurrent Users (100 Users)
	LIC-USG6KF-SSLVPN-200	Quantity of SSL VPN Concurrent Users (200 Users)
	LIC-USG6KF-SSLVPN-500	Quantity of SSL VPN Concurrent Users (500 Users)
	LIC-USG6KF-SSLVPN-1000	Quantity of SSL VPN Concurrent Users (1000 Users)

Product	Model	Description
	LIC-USG6KF-SSLVPN-2000	Quantity of SSL VPN Concurrent Users (2000 Users)
	LIC-USG6KF-SSLVPN-5000	Quantity of SSL VPN Concurrent Users (5000 Users)
NGFW License		
IPS Update Service	LIC-USG6615F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6615F)
	LIC-USG6725F-IPS-1Y	IPS Update Service Subscribe Per Year (Applies to USG6725F)
URL Filtering Update Service	LIC-USG6615F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6615F)
	LIC-USG6725F-URL-1Y	URL Update Service Subscribe Per Year (Applies to USG6725F)
Antivirus Update Service	LIC-USG6615F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6615F)
	LIC-USG6725F-AV-1Y	AV Update Service Subscribe Per Year (Applies to USG6725F)
Threat Protection Bundle (IPS, AV, URL)	LIC-USG6615F-TP -1Y-OVS	Threat Protection Subscription Per Year (Applies to USG6615F Overseas)
	LIC-USG6725F-TP-1Y-OVS	Threat Protection Subscription Per Year (Applies to USG6725F Overseas)
Industrial Control Security Service	LIC-USG6615F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6615F)
	LIC-USG6725F-ICS-1Y	Industrial Control Security Service Subscribe Per Year (Applies to USG6725F)
IPv6+	N1-AD-USG6600F-IPv6+-LIC	IPv6+ Feature (includes SRv6,channel subinterface, iFit) (Applies to USG6600F)
	N1-AD-USG6700F-IPv6+-LIC	IPv6+ Feature (includes SRv6,channel subinterface, iFit) (Applies to USG6700F)
Enhanced DDoS defense	LIC-USG6000F-AntiDDoS	Enhanced anti-DDoS function (applies to USG6000F)
N1 License		
USG6615F	N1-USG6615F-F-Lic	N1-USG6615F Foundation, Per Device
	N1-USG6615F-F-SnS1Y	N1-USG6615F Foundation, SnS, Per Device, Per Year
	N1-USG6615F-A-Lic	N1-USG6615F Advanced, Per Device

Product	Model	Description
	N1-USG6615F-A-SnS1Y	N1-USG6615F Advanced, SnS, Per Device, Per Year
USG6725F	N1-USG6725F-F-Lic	N1-USG6725F Foundation, Per Device
	N1-USG6725F-F-SnS1Y	N1-USG6725F Foundation, SnS, Per Device, Per Year
	N1-USG6725F-A-Lic	N1-USG6725F Advanced, Per Device
	N1-USG6725F-A-SnS1Y	N1-USG6725F Advanced, SnS, Per Device, Per Year
QianKun Cloud Deployment License		
USG6615F	N1-C-USG6615F-F-Lic	Cloud Deployment Model Foundation, Per Device,Per Year
	LIC-USG6615F-BA-1Y	Border Protection and Response - Threat automatic blocking (Applies to USG6615F), Per Device, Per Year
	LIC-USG6615F-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6510F-D), Per Device, Per Year
QianKun OP mode		
USG6615F	LIC-USG6615F-TPU-1Y	Threat Protection Database Upgrade Service (Applies to USG6510F-D), Per Device, Per Year
N1 SASE Branch Interconnection license		
USG6615F	N1-USG6615F-S-S-Lic	N1 SASE Branch Interconnection Standard Package(Package for USG6615F)
	N1-USG6615F-S-S-S1Y	N1 SASE Branch Interconnection Standard Package(Package for USG6615F),Per Device,1 Year

NOTE

Some parts of this table list the sales strategies in different regions. For more information, please contact your Huawei representative.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

HUAWEI HiSecEngine

Machine Translated by Google

HUAWEI HiSecEngine USG6600F y USG6700F Serie de cortafuegos con IA

1 Descripción general

A medida que la digitalización se extiende por todo el mundo, las extensas conexiones, el crecimiento explosivo de los datos y el auge de las aplicaciones inteligentes están transformando profundamente nuestra forma de vivir y trabajar. Los servicios empresariales se están digitalizando y migrando a la nube, lo que promueve la transformación de las redes empresariales y plantea mayores desafíos para la seguridad de la red. A medida que aumentan las amenazas, las amenazas desconocidas cambian constantemente y son altamente encubiertas. A medida que aumentan las necesidades de los usuarios en cuanto a servicios de seguridad, el rendimiento y la latencia se convierten en cuellos de botella.
Con grandes cantidades de políticas y registros de seguridad, el manejo de amenazas y las operaciones y el mantenimiento consumen muchísimo tiempo.
Como "primera puerta" en los límites de la red, los firewalls son la primera opción para la protección de la seguridad empresarial.
Sin embargo, los firewalls tradicionales solo pueden analizar y bloquear amenazas basándose en firmas y, por lo tanto, no pueden gestionar eficazmente las amenazas desconocidas. Además, la eficacia de las amenazas depende de la experiencia profesional del personal de operaciones y mantenimiento. El método de defensa de punto único, reactivo y en caso de evento no puede...
defenderse eficazmente contra ataques de amenazas desconocidas, y más aún contra amenazas ocultas en el tráfico cifrado.

Con nuevas arquitecturas de hardware y software, la serie Huawei HiSecEngine USG6000F es de próxima generación
Cortafuegos con IA que ofrecen defensa inteligente, rendimiento excepcional y operaciones y mantenimiento simplificados, abordando eficazmente los desafíos anteriores. La serie USG6000F utiliza tecnologías de inteligencia artificial para permitir que la defensa fronteriza bloquee con precisión las amenazas conocidas y desconocidas. Equipado con múltiples funciones integradas dedicadas a la seguridad.
Los firewalls de la serie USG6000F, con sus motores de aceleración, ofrecen reenvío mejorado, detección de seguridad de contenido y aceleración del procesamiento de servicios IPsec. La plataforma de operaciones y mantenimiento de seguridad implementa la gestión y el mantenimiento unificados de diversos tipos de productos de seguridad, como firewalls y dispositivos anti-DDoS, lo que reduce los gastos operativos de operaciones y mantenimiento de seguridad.

2 Aspectos destacados del producto

Excelente rendimiento

Al aprovechar las nuevas arquitecturas de hardware y software para la separación de control y reenvío, los firewalls con IA de la serie HiSecEngine USG6000F asignan recursos dinámicamente a los módulos de servicio mediante el motor de seguridad adaptativo (ASE), lo que maximiza la utilización de recursos y mejora el rendimiento general del servicio. Para los servicios principales, la serie HiSecEngine USG6000F también admite procesadores de red (NP), coincidencia de patrones y motores de cifrado/descifrado. Estos motores mejoran considerablemente el reenvío de paquetes cortos, reducen la latencia de reenvío y optimizan la identificación de aplicaciones, la detección de prevención de intrusiones y el rendimiento del servicio IPsec.

Machine Translated by Google

Defensa inteligente

Los firewalls de IA de la serie USG6000F de HiSecEngine brindan funciones de seguridad de contenido, como la protección de aplicaciones. Identificación, IPS, antivirus y filtrado de URL para proteger a los servidores y usuarios de la intranet contra amenazas.
La serie HiSecEngine USG6000F también permite detectar amenazas desconocidas mediante la interacción con sandbox.

Las firmas IPS tradicionales se generan manualmente mediante análisis, lo que resulta en una baja productividad. Además, la precisión de las firmas depende en gran medida de la experiencia de expertos. Huawei, de forma innovadora, permite la generación de firmas IPS en la nube inteligente mediante la adopción de tecnologías inteligentes y el uso de la experiencia de expertos. Este modo inteligente ayuda a aumentar la productividad de las firmas 30 veces en comparación con la generación manual, reduce los errores causados por el análisis manual y mejora continuamente la precisión de la detección de intrusiones.

El motor de detección basado en contenido (CDE) antivirus integrado, impulsado por tecnologías de inteligencia, puede detectar amenazas desconocidas y proporcionar un análisis exhaustivo de los datos. Con estas capacidades, el firewall potenciado por CDE puede comprender mejor las actividades de las amenazas y detectar rápidamente archivos maliciosos, lo que mejora eficazmente la seguridad.
la tasa de detección de amenazas.

NGFW USG ayuda a detectar y defender la propagación de malware y ataques de red, como gusanos, virus, troyanos, spyware, etc., propagación de malware y botnets, DoS/DDoS, inyección SQL, ataques entre sitios, ransomware, etc.

Machine Translated by Google

Operaciones y mantenimiento simplificados

La serie HiSecEngine USG6000F ofrece una nueva interfaz web que visualiza intuitivamente las amenazas y muestra información clave como el estado del dispositivo, las alarmas, el tráfico y los eventos de amenaza. Con análisis de datos multidimensionales, la interfaz web ofrece una experiencia de usuario óptima, mayor usabilidad y un funcionamiento y mantenimiento simplificados.

Los firewalls de la serie HiSecEngine USG6000F se pueden administrar de forma centralizada mediante la plataforma de gestión de seguridad SecoManager, implementando un cambio de la defensa de un solo punto a la protección de red colaborativa. SecoManager ofrece optimización de políticas y funciones inteligentes de operación y mantenimiento (O&M). También puede administrar productos de seguridad, como dispositivos anti-DDoS, para eliminar rápidamente las amenazas de red y mejorar la eficacia de la gestión de la seguridad.

El NGFW de la serie HiSecEngine USG6000F también puede ser administrado por NCE-Campus, y NCE-Campus también puede soportar la administración de conmutadores, AR, dispositivos POL al mismo tiempo, e incluso dispositivos de terceros.

Una amplia gama de funciones de red

La serie Huawei HiSecEngine USG6000F también proporciona varias funciones de red como VPN, IPv6 y dirección de tráfico inteligente.

- Proporciona varias funciones VPN como IPsec VPN y SSL VPN, y admite múltiples algoritmos de cifrado, como DES, 3DES, AES y SHA, lo que garantiza una transmisión de datos segura y confiable.

Machine Translated by Google

Proporciona conmutación de red IPv6 segura y enriquecida, control de políticas, protección de seguridad y servicio.
capacidades de visualización, ayudando a los sectores gubernamentales, de medios de comunicación, de operadores, de Internet y financieros a implementar la reconstrucción de IPv6.

Proporciona una dirección de tráfico inteligente, estática y dinámica basada en enlaces de múltiples salidas, selecciona
La interfaz de salida, basada en el ancho de banda, el peso o la prioridad del enlace especificado, reenvía el tráfico a cada enlace en función del modo de dirección de tráfico especificado y ajusta dinámicamente el resultado de la selección del enlace en tiempo real.
Es hora de maximizar el uso de los recursos de enlace y mejorar la experiencia del usuario.

Colaboración con el servicio de seguridad en la nube Huawei Qiankun

La mayoría de las amenazas y ataques provienen del tráfico de red. Se implementan firewalls en la salida de la red local para interactuar con el servicio de seguridad en la nube Huawei Qiankun e implementar el análisis y la gestión automáticos de amenazas. Esto garantiza la interconexión entre la intranet y la extranet, intercepta eficazmente los ataques de tráfico y gestiona automáticamente las fuentes de ataque externas. Protege los recursos de la red empresarial.

Al asociarse con el servicio de seguridad en la nube Huawei Qiankun, el firewall puede obtener servicios de seguridad como protección de fronteras y respuesta bajo demanda. La implementación ligera y la operación y el mantenimiento unificados en la nube reducen eficazmente la acumulación de hardware y reducen considerablemente la inversión en seguridad empresarial y las dificultades de operación y mantenimiento .

Machine Translated by Google

3 Despliegue

Protección de fronteras en centros de datos pequeños

Los firewalls se implementan en las salidas de los centros de datos, y las funciones y los recursos del sistema se pueden Virtualizado. El firewall tiene varios tipos de interfaces, como 100G, 40G, 10G y 1G.
Los servicios se pueden ampliar de forma flexible sin tarjetas de interfaz adicionales.

La capacidad de prevención de intrusiones bloquea eficazmente una variedad de ataques maliciosos y ofrece una defensa diferenciada según los requisitos del entorno virtual para garantizar la seguridad de los datos.

Se pueden configurar túneles VPN entre firewalls y trabajadores móviles y entre firewalls y sucursales. oficinas para acceso remoto seguro y de bajo costo y trabajo móvil.

Protección fronteriza empresarial

Se implementan firewalls en el borde de la red. La sonda de tráfico integrada puede extraer paquetes de tráfico cifrado para monitorear las amenazas en tiempo real.

Las funciones de control de políticas y filtrado de datos de los firewalls se utilizan para monitorear las redes sociales. Aplicaciones para prevenir la violación de datos y proteger las redes empresariales.

4 Apariencia del producto

Figura 4-1 HiSecEngine USG6615F/USG6625F

Figura 4-2 HiSecEngine USG6635F/USG6655F/USG6685F

Machine Translated by Google

Figura 4-3 HiSecEngine USG6710F/USG6715F

Figura 4-4 HiSecEngine USG6725F

5 características del software

Característica	Descripción
Protección integrada	Integra firewall, VPN, prevención de intrusiones, antivirus, administración de ancho de banda, Anti-DDoS y funciones de filtrado de URL, y proporciona una vista de configuración global. y gestión integrada de políticas.
Identificación de aplicaciones y control	Identificación de aplicaciones basada en firmas, correlación y comportamientos en lugar de puertos; más de 6000 aplicaciones predefinidas que pueden clasificarse aún más; compatibilidad con aplicaciones definidas por el usuario; más de 50 categorías y más de 20 etiquetas de riesgo para el control de acceso basadas en categorías y etiquetas; actualización automática de la base de datos de firmas de identificación de aplicaciones
Gestión de políticas de seguridad	Admite la gestión y el control del tráfico en función del ID de VLAN, tupla de 5, zona de seguridad, región, aplicación y rango de tiempo, e implementa una inspección de seguridad de contenido integrada. Proporciona plantillas predefinidas para escenarios comunes de defensa contra ataques para facilitar la implementación de políticas de seguridad. Admite la interoperabilidad con software de gestión de políticas de terceros (FireMon y Algosec) para facilitar la operación y el mantenimiento de seguridad.
Gestión del ancho de banda	Gestiona el ancho de banda por IP según la identificación de la aplicación de servicio para garantizar la experiencia de red de los servicios y usuarios clave. La gestión y el control se pueden implementar limitando el ancho de banda máximo, garantizando el ancho de banda mínimo y modificando la prioridad de reenvío de la aplicación.
Intrusión	Obtiene la información más reciente sobre amenazas de manera oportuna y detecta y ataca con precisión.

Machine Translated by Google

prevención	previene la explotación de vulnerabilidades; cubre decenas de miles de vulnerabilidades CVE; previene la explotación de vulnerabilidades (como las de los sistemas operativos Windows y Unix/Linux, bases de datos, Apache, IIS y Tomcat, así como middleware), ataques web (como inyección SQL, XSS y RCE), botnets, control remoto y caballos de Troya; admite la detección de craqueo por fuerza bruta según el comportamiento del usuario; proporciona más de 25 000 firmas predefinidas y admite firmas definidas por el usuario y actualización automática de la base de datos de firmas; admite la recopilación de análisis forense de ataques, la obtención de paquetes de flujo completo (incluida la información de protocolo de enlace de tres vías) y la visualización de fragmentos de ataque para facilitar las operaciones y el mantenimiento; admite la extracción del campo X-Forwarded-For (XFF).
WAF	Utiliza tecnologías de firma, análisis semántico y aprendizaje automático para detectar los 10 principales ataques de OWASP, como inyección SQL, secuencias de comandos entre sitios, RCE, CSRF y deserialización, y admite anti-leeching y anti-manipulación de páginas web; admite el método HTTP y el control de longitud de campo.
Antivirus	Detecta malware en archivos transmitidos a través de protocolos como HTTP, FTP, SMTP, POP3, IMAP4, NFS y SMB; detecta caballos de Troya, gusanos, spyware, vulnerabilidades, adware, herramientas de hackers, rootkits, puertas traseras, grayware, programas de botnet, ransomware, software de phishing, software de cryptojacking y programas web shell; admite la detección de virus para archivos de Office, archivos ejecutables (Windows/Linux/MacOS), archivos de script, archivos flash, archivos PDF, archivos RTF, páginas web, e imágenes; apoya la recopilación de datos forenses de ataques; apoya la inspección de archivos archivos de hasta 100 niveles de compresión anidados en múltiples formatos de compresión, como tar, gzip, zip, rar y 7z, y admite múltiples acciones, como alertar, bloquear, agregar Declaración y eliminación de archivos adjuntos.
Prevención avanzada de malware	El motor antivirus heurístico utiliza tecnologías de detección como IA, análisis semántico y emulador, junto con información sobre amenazas y reputación, para detectar malware empaquetado, mutación de scripts y malware incrustado en documentos compuestos. Puede detectar miles de millones de variantes de malware y actualiza automáticamente la base de datos de firmas. Además, puede enviar archivos sospechosos al entorno de pruebas local o en la nube para una inspección más exhaustiva y detectar malware de día cero.
Seguridad web	La base de datos de categorías de URL en la nube contiene 500 millones de URL en más de 130 categorías, como noticias, juegos, apuestas, drogas y páginas web maliciosas. URL cubre más de 100 idiomas y las categorías clave de URL cubren más de 20 idiomas. Los servidores de consulta de categorías de URL se implementan en varios países/regiones para proporcionar servicios de consulta de categorías de alta velocidad y baja latencia. Se admiten listas blancas y negras de URL/host definidas por el usuario. El tráfico HTTPS se puede filtrar sin descifrar. El tráfico TLS/SSL se puede descifrar antes del filtrado. HTTP/2 y Se puede filtrar el tráfico QUIC y se pueden importar categorías de URL en lotes. El acceso a la URL se puede controlar en función de usuarios/grupos de usuarios, rangos de tiempo y zonas de seguridad para administrar con precisión los comportamientos en línea de los usuarios.
Seguridad DNS	Basándose en información masiva sobre amenazas, se utilizan tecnologías como IA y gráficos de conocimiento para detectar solicitudes DNS maliciosas, incluyendo nombres de dominio de C&C, nombres de dominio generados por DGA, sitios web comprometidos y nombres de dominio maliciosos, como nombres de dominio de cryptojacking, ransomware y phishing. La base de datos local de nombres de dominio maliciosos admite un máximo de 2 millones. También se admiten el filtrado basado en categorías de DNS, la búsqueda segura de DNS y la redirección de DNS (sinkholing).

Machine Translated by Google

Anti-botnet/ software espía	Admite la detección y prevención de virus y malware avanzado, como botnets, troyanos, gusanos, herramientas de control remoto y spyware, y evita el descarga de malware; detecta rápidamente tráfico malicioso como C&C basado en firmas, direcciones IP e información de reputación del dominio; muestra los roles de las partes de comunicación en los registros de ataques de botnet.
Información sobre amenazas	El Centro de Seguridad Inteligente de Huawei aprovecha múltiples algoritmos de IA y análisis de expertos para generar diariamente información masiva sobre amenazas, como direcciones IP, nombres de dominio, URL y archivos. Esta información se sincroniza automáticamente con los dispositivos para su detección y bloqueo rápido de ataques emergentes. Además, puede interconectarse con fuentes de información de amenazas de terceros para enriquecer las reglas de inspección.
Seguridad OT/IoT	Compatible con protocolos comunes de control industrial como Modbus, S7, Profinet y OPC, así como con la identificación y el control de dispositivos IoT como cámaras, y la evaluación de riesgos de activos IoT. Admite la detección de vulnerabilidades para dispositivos IoT como cámaras, software de control industrial y protocolos como ICS/SCADA. La función de sonda de tráfico, junto con el sistema de conocimiento de la situación HiSec Insight, puede conocer la línea base del comportamiento del tráfico de los activos de IoT y detectar y evaluar Riesgos de los activos de IoT. Para obtener detalles sobre la lista de protocolos OT compatibles, consulte https://isecurity.huawei.com/security/wiki/application (Sistemas de Negocios > Industrial).
Sonda de flujo	Recopila y analiza metadatos e información forense de ataques, incluidos metadatos de la capa de red (como direcciones IP, puertos y características de paquetes) y metadatos de la capa de aplicación (como información de campo obtenida después de un análisis en profundidad de protocolos como HTTP, DNS, TLS y SSH), y envía los datos a la plataforma de conocimiento de la situación de seguridad HiSec Insight para un análisis posterior mediante el uso de algoritmos, como aprendizaje profundo y aprendizaje automático, para detectar amenazas potenciales, desconocidas y avanzadas en el tráfico de la red.
Anti-DDoS	Utiliza tecnologías como detección de dirección IP de origen, detección de huellas dactilares y limitación dinámica del tráfico para defenderse contra más de 10 ataques DDoS comunes y más de 20 ataques de paquete único, como inundación SYN, inundación UDP, inundación ICMP, inundación HTTP, inundación HTTPS, inundación DNS y ataques de inundación SIP, y admite aprendizaje de línea de base de tráfico y filtrado basado en reputación IP.
Filtrado de correo	Admite el filtrado de direcciones de correo (que cubre las direcciones del remitente y del destinatario) y la limitación de la velocidad de envío de correo SMTP.
DLP	Admite la identificación de más de 100 tipos de archivos reales, extensiones de nombre de archivo definidas por el usuario y control de carga/descarga basado en el tipo de archivo; admite filtrado de palabras clave para Office documentos, páginas web, código y archivos TXT; admite palabras clave definidas por el usuario, expresiones regulares y configuración de peso.
Control de acceso SaaS	Admite identificación de aplicaciones SaaS y control de acceso basado en firmas, DNS, direcciones IP (base de datos de direcciones IP de las 50 principales aplicaciones SaaS) y primeros paquetes, y admite la dirección de tráfico basada en aplicaciones SaaS, lo que garantiza una buena experiencia de aplicación SaaS.
Auditoría de comportamiento	Audita y regula los comportamientos comunes de los usuarios en línea, incluidas las operaciones FTP (carga, descarga y comandos), operaciones HTTP (publicación, búsqueda y navegación), DNS, Telnet, SNMP y operaciones de envío y recepción de correo electrónico.

Machine Translated by Google

Selección inteligente de enlace ascendente	Admite PBR específico del servicio y selecciona de forma inteligente el enlace óptimo en función de múltiples tipos de criterios de equilibrio de carga (como la relación de ancho de banda y el estado de salud del enlace) en escenarios de múltiples ISP.
Cifrado VPN	Admite varias funciones VPN altamente confiables, como IPsec VPN, SSL VPN y GRE, y múltiples algoritmos de cifrado, como DES, 3DES, AES, SHA, SM2, SM3 y SM4.
Inspección de tráfico encriptado con SSL	Detecta y defiende contra amenazas ocultas en el tráfico cifrado TLS/SSL, realiza protección de la capa de aplicación, como prevención de intrusiones, antivirus, filtrado de datos y filtrado de URL, en tráfico TLS/SSL descifrado y admite la lista blanca de categorías de URL.
Descarga de SSL	Reemplaza el servidor para implementar el cifrado y descifrado SSL, reduciendo la carga del servidor e implementando el equilibrio de carga del tráfico HTTP.
Informes diversificados	Proporciona informes visualizados y multidimensionales por dirección IP, aplicación, hora, tráfico o amenaza.
Virtualización de seguridad	Admite la virtualización de múltiples tipos de servicios de seguridad, incluidos firewall, prevención de intrusiones, antivirus y servicios VPN; permite a los usuarios realizar una gestión personalizada por separado en el mismo dispositivo físico.
Enrutamiento	Admite varios tipos de protocolos de enrutamiento IPv4/IPv6, como RIP, OSPF, BGP, IS-IS, RIPng, OSPFv3, BGP4+ e IPv6 IS-IS.
Multidifusión IP	Admite protocolos de multidifusión de capa 3 IPv4, como IGMP, MSDP y PIM, y proporciona servicios punto a multipunto para reducir el consumo de ancho de banda.
Equilibrio de carga del servidor	Admite IPv6, equilibrio de carga de servidor de capa 4/capa 7 y múltiples métodos de persistencia de sesión, como persistencia de sesión basada en dirección IP de origen y basada en cookies HTTP; admite la descarga y el cifrado SSL; combina servicios y políticas de seguridad para mejorar la seguridad del servicio; admite la verificación del estado basada en múltiples protocolos, como TCP, RADIUS, DNS y HTTP, para detectar rápidamente los cambios en el estado del servidor.
Implementación y confiabilidad	Admite modos de trabajo transparentes (capa 2), de enrutamiento (capa 3), de toque e híbridos y alta disponibilidad (HA), incluidos los modos Activo/Activo y Activo/En espera.
Centro de seguridad	El módulo de identificación de activos integrado puede identificar activos como dispositivos y cámaras de Windows, Linux, Android e iOS y realizar análisis de correlación sobre amenazas. registros y activos, y muestra los resultados de la evaluación de riesgos de los activos y toda la cadena de eliminación.
SRv6	Admite IS-IS para SRv6, BGP para SRv6, SRv6 BE, política SRv6 TE, protección de punto medio SRv6, prevención de microbucles SRv6, SRv6 OAM, compresión SRv6 SRH, SRv6 TI-LFA FRR y EVPN L3VPN.
SD-WAN segura	Proporciona una solución SD-WAN segura integrada para aplicaciones de bajo costo y de nivel empresarial. Enlaces de Internet. Admite aprovisionamiento sin intervención (ZTP) a través de correo electrónico para completar el aprovisionamiento del dispositivo en minutos sin necesidad de habilidades técnicas. Admite corrección de errores de avance (FEC) para evitar la visualización pixelada y el congelamiento de video a una tasa de pérdida de paquetes del 30 %; admite conmutación de enlace en tiempo real en función de la calidad del enlace para garantizar una experiencia de aplicación clave. Admite enrutamiento de múltiples enlaces y redes flexibles de CPE dual para garantizar

Machine Translated by Google

	Conexiones ininterrumpidas para servicios del sitio; admite encriptación IPsec E2E para garantizar la transmisión segura del servicio. Nota: La serie USG6600F puede funcionar como concentrador o radio. La serie USG6700F no es compatible con SD-WAN.
Autenticación de usuario	Admite múltiples modos de autenticación para usuarios con acceso a Internet, incluyendo la autenticación local del Portal y el inicio de sesión único (SSO). En la autenticación local del Portal, se puede enviar la página del Portal integrada del dispositivo a los usuarios, y la cuenta y la contraseña introducidas en ella se pueden enviar a la base de datos local o al servidor de autenticación RADIUS, HWTACACS, AD o LDAP para su autenticación. SSO incluye RADIUS SSO y Agile Controller (NCE-Campus) SSO.
Capacidad de operaciones y mantenimiento	Admite telemetría para leer automáticamente información del hardware, como ventiladores, módulos de potencia, módulos ópticos, puertos Ethernet, sensores de temperatura y controladores, y envía estadísticas de tráfico de interfaz, uso de CPU y uso de memoria al recopilador.
PPPoE	Funciona como un cliente PPPoE para proporcionar servicios de acceso a Internet, incluida la autenticación y autorización de usuarios y la asignación dinámica de direcciones IP.
Interfuncionamiento del firewall con Huawei Qiankun Security CloudService	
Servicio	Descripción
Protección fronteriza y servicio de respuesta	Detección y prevención de intrusiones: aprovecha las firmas para bloquear la capa de aplicación ataques, finaliza la transferencia de correos electrónicos de phishing y malware (como virus y caballos de Troya), detecta hosts comprometidos en la red interna y desconecta estos hosts de Internet para proteger la seguridad y la estabilidad de los servicios al cliente.
	Análisis automático de eventos: combina el análisis inteligente y el análisis manual realizado por expertos para analizar eventos de seguridad para garantizar la precisión del bloqueo de ataques y las alarmas de seguridad y optimizar las reglas de identificación de ataques.
	Lista blanca y lista negra: admite la configuración de listas blancas y listas negras en el Portal o la aplicación para proteger los servicios de amenazas.
	Informes de seguridad periódicos: genera informes semanales y mensuales sobre eventos de protección de seguridad y envía los informes a los usuarios por correo electrónico.
	Notificación de emergencia: identifica emergencias de eventos de seguridad y envía notificaciones a los usuarios mediante SMS y correo electrónico.

6 Especificaciones

Rendimiento y capacidad del sistema

Modelo	USG6615F USG6625F		USG6635F	USG6655F
Rendimiento de firewall IPv41 (1518/512/64 bytes, UDP)	15/15/15 Gbps	25/25/25 Gbps	35/35/35 Gbps	50/50/40 Gbps

Machine Translated by Google

Modelo	USG6615F USG6625F		USG6635F	USG6655F
Rendimiento del firewall IPv61 (1518/512/84 bytes, UDP)	15/15/15 Gbps	25/25/25 Gbps	35/35/25 Gbps	50/50/25 Gbps
EVPN SD-WAN segura Rendimiento (1400/512 byte,UDP) [9]	15/15 Gbps	25/25 Gbps	35/35 Gbps	50/40 Gbps
Túneles EVPN SD-WAN seguros	3.000	3.000	6.000	6.000
Latencia del firewall (64 bytes,	18 µs	18 µs	18 µs	18 µs
Latencia del firewall8 (64 bytes,	7 µs	7 µs	7 µs	7 µs
Sesiones concurrentes (HTTP1.1)1	10.000.000	10.000.000	20.000.000	20.000.000
Nuevas sesiones por segundo (HTTP1.1)1	250.000	250.000	500.000	500.000
Rendimiento de FW + SA*2	12 Gbps	12 Gbps	23 Gbps	26,5 Gbps
Rendimiento de NGFW3 (HTTP 100K)	6 Gbps	10 Gbps	16 Gbps	25 Gbps
Rendimiento de NGFW (Mezcla empresarial)4	4,6 Gbps	5 Gbps	8 Gbps	8,5 Gbps
Protección contra amenazas Rendimiento (Empresa) Mezcla)5	4 Gbps	4 Gbps	7 Gbps	8 Gbps
Rendimiento de VPN IPsec1 (AES-256 + SHA256, 1420-byte)	15 Gbps	25 Gbps	30 Gbps	30 Gbps
Túneles VPN IPsec máximos : 20 000		20.000	20.000	20.000
Rendimiento de inspección SSL7	2,5 Gbps	2,5 Gbps	4 Gbps	4 Gbps
Rendimiento de VPN SSL [6]	1 Gbps	1,5 Gbps	3 Gbps	3 Gbps
Usuarios simultáneos de VPN SSL *(Predeterminado/Máximo)	100/4000	100/8000	100/10000	100/10000
Políticas de seguridad (máximo) 50.000		50.000	150.000	150.000
Cortafuegos virtuales	2048	2048	2048	2048
Filtrado de URL: Categorías	Más de 130			
Filtrado de URL: URL	Una base de datos de más de 500 millones de URL en la nube			
Firma IPS automatizada	Sí, un centro de seguridad líder en la industria de Huawei			

Machine Translated by Google

Modelo	USG6615F USG6625F	USG6635F	USG6655F
Actualizaciones	(http://sec.huawei.com/sec/web/index.do)		
De terceros y abiertos Ecosistema fuente	API abierta para integración con productos de terceros, proporcionando Interfaces NETCONF Otro software de gestión de terceros basado en SNMP, SSH y Registro del sistema		
VLAN (máximo)	4094		
Interfaces VLANIF (Máximo)	4094		

Modelo	USG6685F USG6710F		USG6715F	USG6725F
Rendimiento de firewall IPv41 (1518/512/64 bytes, UDP)	80/80/40 Gbps	100/100/60 Gbps	160/160/80 Gbps	240/240/120 Gbps
Rendimiento del firewall IPv61 (1518/512/84 bytes, UDP)	80/80/25 Gbps	100/100/45 Gbps	160/160/50 Gbps	240/240/85 Gbps
EVPN SD-WAN segura Rendimiento (1400/512 byte,UDP) [9]	50/40 Gbps /		/	/
Túneles EVPN SD-WAN seguros	6000	/	/	/
Latencia del firewall (64 bytes, Unidad de procesamiento unificado (UCP)	18 µs	35 µs	35 µs	35 µs
Latencia del firewall8 (64 bytes, Unidad de procesamiento unificado (UCP)	7 µs	7 µs	7 µs	7 µs
Sesiones concurrentes (HTTP1.1)1	25.000.000	50.000.000	50.000.000	75.000.000
Nuevas sesiones por segundo (HTTP1.1)1	750.000	1.500.000	1.500.000	2.250.000
Rendimiento de FW + SA*2	26,5 Gbps	50 Gbps	55 Gbps	80 Gbps
Rendimiento de NGFW3 (HTTP 100 mil)	25 Gbps	40 Gbps	50 Gbps	75 Gbps
Rendimiento de NGFW (Mezcla empresarial)4	8,5 Gbps	16 Gbps	17 Gbps	26 Gbps
Protección contra amenazas Rendimiento (Empresa) Mezcla)5	8 Gbps	14 Gbps	16 Gbps	24 Gbps
Rendimiento de VPN IPsec1 (AES-256 + SHA256, 1420-	30 Gbps	40 Gbps	45 Gbps	65 Gbps

Machine Translated by Google

Modelo	USG6685F USG6710F		USG6715F	USG6725F
byte)				
Túneles VPN IPsec máximos : 20 000		80000	80000	120000
Rendimiento de inspección SSL: 7,4 Gbps		8 Gbps	8 Gbps	12 Gbps
Rendimiento de VPN SSL [6]	5 Gbps	10 Gbps	10 Gbps	12 Gbps
Usuarios simultáneos de VPN SSL *(Predeterminado/Máximo)	100/10000	100/20000	100/20000	100/30000
Políticas de seguridad (máximo) 150.000		160.000	160.000	160.000
Cortafuegos virtuales	2048	2048	2048	2048
Filtrado de URL: Categorías	Más de 130			
Filtrado de URL: URL	Una base de datos de más de 500 millones de URL en la nube			
Firma IPS automatizada Actualizaciones	Sí, un centro de seguridad líder en la industria de Huawei (http://sec.huawei.com/sec/web/index.do)			
De terceros y abiertos Ecosistema fuente	API abierta para integración con productos de terceros, proporcionando Interfaces NETCONF Otro software de gestión de terceros basado en SNMP, SSH y Registro del sistema			
VLAN (máximo)	4094			
Interfaces VLANIF (Máximo)	4094			

1. El rendimiento se prueba en condiciones ideales según RFC2544, 3511. El resultado real puede variar. con entornos de implementación.
2. El rendimiento de SA se mide utilizando archivos HTTP de 100 KB.
3. El rendimiento de NGFW se mide con Firewall, SA e IPS habilitados; el rendimiento se mide utilizando archivos HTTP de 100 KB.
4. El rendimiento de NGFW se mide con Firewall, SA e IPS habilitados; el rendimiento se mide utilizando el modelo de tráfico mixto empresarial.
5. El rendimiento de la protección contra amenazas se mide con Firewall, SA, IPS y AV habilitados; el rendimiento se mide utilizando el modelo de tráfico mixto empresarial.
6. El rendimiento de VPN SSL se mide utilizando TLS v1.2 con AES128-SHA.
7. El rendimiento de la inspección SSL se mide con IPS habilitado y tráfico HTTPS utilizando TLS v1.2 con TLS_ECDHE_RSA_CON_AES_128_GCM_SHA256.
8. La condición de prueba de datos es el modo de par de interfaces.·
9. El túnel SD-WAN está repleto de GRE sobre IPSec.

Machine Translated by Google

7 Especificaciones de hardware

Modelo	USG6615F	USG6625F	USG6635F USG6655F
Altura del chasis	1 U		
Dimensiones (alto x ancho x profundidad) mm	43,6 x 442 x 420		
Interfaz fija	8*GE COMBO + 4*GE RJ45 + 4*GE SFP + 6*10GE SFP+		COMBO DE 8 GE + 4 GE RJ45 + 10*10GE SFP+
Puerto USB	1 USB 3.0		
Peso	6,3 kilogramos		7,3 kilogramos
Hardware	Opcional, compatible con SATA (1 x 2,5 pulgadas), 240 GB/480 GB/960 GB/1920 GB, intercambiables en caliente		
Fuente de alimentación (CA)	100 V a 240 V		
Consumo máximo de energía de la máquina	222 Oeste		242 Oeste
Fuentes de alimentación	Fuentes de alimentación de CA duales opcionales		Fuente de alimentación de CA dual
Entorno operativo (Temperatura/Humedad)	Temperatura: 0°C a 45°C Humedad: 5% a 95%, sin condensación		
Entorno no operativo	Temperatura: –40°C a +70°C Humedad: 5% a 95%, sin condensación		
Tipo de instalación	Estante		

Modelo	USG6685F	USG6710F USG6715F USG6725F	
Altura del chasis	1 U		
Dimensiones (alto x ancho x profundidad) mm	43,6 x 442 x 420	43,6 x 442 x 600	
Interfaz fija	COMBO DE 8*GE + 4*GE(RJ45)+ 10*10GE(SFP+)	2*100GE(QSFP28) + 2*40G(QSFP+)+ 8*25(ZSFP+) + 20*10GE(SFP+)1	4*100GE (QSFP28)) + 16*25GE (ZSFP+) + 8*10GE(SFP+)2
Puerto USB	1 USB 3.0		
Peso	7,3 kilogramos	10,26 kilogramos	10,6 kilogramos
Almacenamiento externo	Opcional, compatible con SATA (1 x 2,5 pulgadas), 240 GB/480 GB/960 GB/1920 GB		
Fuente de alimentación	100 V a 240 V		

Machine Translated by Google

Modelo	USG6685F	USG6710F USG6715F USG6725F	
Consumo máximo de energía de la máquina	242 Oeste	391 Oeste	445 Oeste
Fuentes de alimentación	Fuentes de alimentación de CA duales		
Entorno operativo (Temperatura/Humedad)	Temperatura: 0°C a 45°C Humedad: 5% a 95%, sin condensación		
Entorno no operativo	Temperatura: –40°C a +70°C Humedad: 5% a 95%, sin condensación		
Tipo de instalación	Estante	Rack (gabinete estándar de 19 pulgadas)	

1. Algunas interfaces 100GE e interfaces 25GE de USG6710F y USG6715F son mutuamente excluyentes.
2. Algunas interfaces 100GE e interfaces 25GE de USG6715F son mutuamente excluyentes.

8 Información para pedidos

Nota:

1La información de pedido de USG6625F/USG6635F/USG6655F/USG6685F es la misma que la de USG6615F

2La información de pedido de USG6710F/USG6715F es la misma que la de USG6725F.

3El modelo USG6615F es compatible con el servicio de seguridad en la nube Qiankun

Producto	Modelo	Descripción
USG6615F USG6615F-AC		Host de CA USG6615F (8*GE COMBO + 4*GE RJ45) + 4*GE SFP + 6*10GE SFP+, 1 fuente de alimentación de CA)
USG6725F USG6725F-AC		Host de CA USG6725F (4*QSFP28 + 16*ZSFP+ + 8*SFP+,,2 fuentes de alimentación de CA)
Licencia de función		
Virtual Cortafuegos	LIC-USG6KF-VSYS-10	Cantidad de Firewall Virtual (10 Vsys)
	LIC-USG6KF-VSYS-20	Cantidad de Firewall Virtual (20 Vsys)
	LIC-USG6KF-VSYS-50	Cantidad de Firewall Virtual (50 Vsys)
	LIC-USG6KF-VSYS-100	Cantidad de Firewall Virtual (100 Vsys)
	LIC-USG6KF-VSYS-200	Cantidad de Firewall Virtual (200 Vsys)
	LIC-USG6KF-VSYS-500	Cantidad de Firewall Virtual (500 Vsys)
	LIC-USG6KF-VSYS-1000	Cantidad de Firewalls Virtuales (1000 Vsys)
VPN SSL LIC-USG6KF-SSLVPN-100		Cantidad de usuarios simultáneos de SSL VPN (100 usuarios)
	LIC-USG6KF-SSLVPN-200	Cantidad de usuarios simultáneos de SSL VPN (200 usuarios)
	LIC-USG6KF-SSLVPN-500	Cantidad de usuarios simultáneos de SSL VPN (500 usuarios)
	LIC-USG6KF-SSLVPN-1000	Cantidad de usuarios simultáneos de SSL VPN (1000 usuarios)

Machine Translated by Google

Producto	Modelo	Descripción
	LIC-USG6KF-SSLVPN-2000	Cantidad de usuarios simultáneos de SSL VPN (2000 usuarios)
	LIC-USG6KF-SSLVPN-5000	Cantidad de usuarios simultáneos de SSL VPN (5000 usuarios)
Licencia NGFW		
Actualización de IPS Servicio	LIC-USG6615F-IPS-1Y	Servicio de actualización de IPS Suscripción por año (aplica a USG6615F)
	LIC-USG6725F-IPS-1Y	Servicio de actualización de IPS Suscripción por año (aplica a USG6725F)
URL Filtración Actualizar Servicio	LIC-USG6615F-URL-1Y	Servicio de actualización de URL Suscripción por año (aplica a USG6615F)
	LIC-USG6725F-URL-1Y	Servicio de actualización de URL Suscripción por año (aplica a USG6725F)
Antivirus Actualizar Servicio	LIC-USG6615F-AV-1Y	Servicio de actualización de AV Suscripción por año (se aplica a USG6615F)
	LIC-USG6725F-AV-1Y	Servicio de actualización de AV Suscripción por año (se aplica a USG6725F)
Amenaza Protección Paquete (IPS, APAGADO, URL)	LIC-USG6615F-TP -1Y-OVS	Suscripción de protección contra amenazas por año (se aplica a USG6615F en el extranjero)
	LIC-USG6725F-TP-1Y-OVS	Suscripción de protección contra amenazas por año (se aplica a USG6725F en el extranjero)
Industrial Control Seguridad Servicio	LIC-USG6615F-ICS-1Y	Servicio de Seguridad de Control Industrial Suscribirse Por Año (se aplica a USG6615F)
	LIC-USG6725F-ICS-1Y	Servicio de Seguridad de Control Industrial Suscribirse Por Año (se aplica a USG6725F)
IPv6+	N1-AD-USG6600F-IPv6+-LIC	Función IPv6+ (incluye SRv6, subinterfaz de canal, iFit) (se aplica a USG6600F)
	N1-AD-USG6700F-IPv6+-LIC	Función IPv6+ (incluye SRv6, subinterfaz de canal, iFit) (se aplica a USG6700F)
Mejorado Defensa contra DDoS	LIC-USG6000F-AntiDDoS	Función anti-DDoS mejorada (se aplica a USG6000F)
Licencia N1		
USG6615F N1-USG6615F-F-Lic		Fundación N1-USG6615F, por dispositivo
	N1-USG6615F-F-SnS1Y	Fundación N1-USG6615F, SnS, por dispositivo, por Año
	N1-USG6615F-A-Lic	N1-USG6615F Avanzado, por dispositivo

Machine Translated by Google

Producto	Modelo	Descripción
	N1-USG6615F-A-SnS1Y	N1-USG6615F Advanced, SnS, por dispositivo, por año
USG6725F N1-USG6725F-F-Lic		Fundación N1-USG6725F, por dispositivo
	N1-USG6725F-F-SnS1Y	Fundación N1-USG6725F, SnS, por dispositivo, por Año
	N1-USG6725F-A-Lic	N1-USG6725F Avanzado, por dispositivo
	N1-USG6725F-A-SnS1Y	N1-USG6725F Advanced, SnS, por dispositivo, por año
Licencia de implementación en la nube de QianKun		
USG6615F	N1-C-USG6615F-F-Lic	Fundación del modelo de implementación en la nube, por dispositivo, por Año
	LIC-USG6615F-BA-1Y	Protección y respuesta fronteriza: bloqueo automático de amenazas (se aplica a USG6615F), por dispositivo, por año
	LIC-USG6615F-TPU-1Y	Servicio de actualización de la base de datos de protección contra amenazas (se aplica a USG6510F-D), por dispositivo, por año
Modo OP QianKun		
USG6615F	LIC-USG6615F-TPU-1Y	Servicio de actualización de la base de datos de protección contra amenazas (se aplica a USG6510F-D), por dispositivo, por año
Licencia de interconexión de sucursales N1 SASE		
USG6615F	N1-USG6615F-SS-Licencia	Estándar de interconexión de sucursales SASE N1 Paquete (paquete para USG6615F)
	N1-USG6615F-SS-S1Y	Estándar de interconexión de sucursales SASE N1 Paquete (paquete para USG6615F), por dispositivo, 1 año

Algunas secciones de esta tabla detallan las estrategias de ventas en diferentes regiones. Para más información, contacte con su representante de Huawei.

REFERENCIAS TECNICAS

INGLES

IPS Overview

Overview of Intrusion Prevention

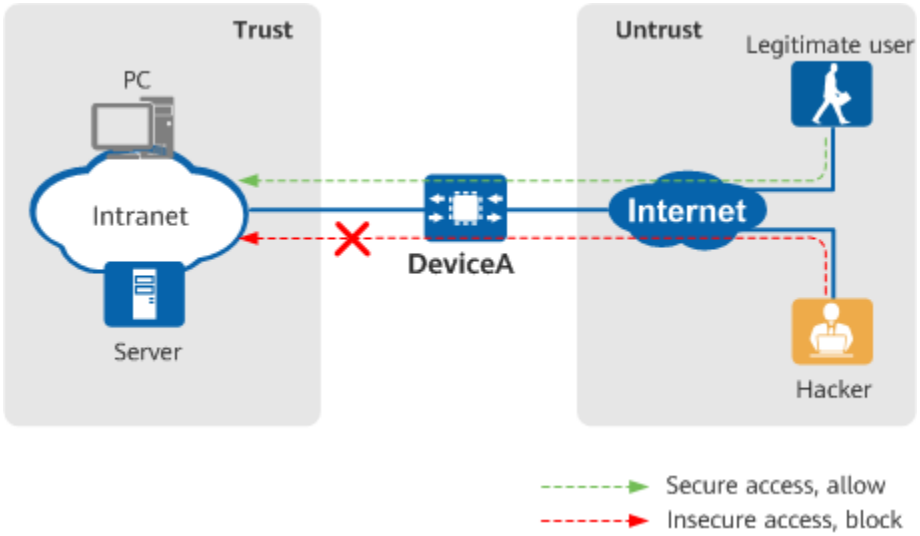
Definition

Intrusion prevention is a security mechanism that detects intrusions based on the attack signature database and takes certain response measures to terminate the intrusions in real time.

Purpose

Trojan horses, worms, botnets, spyware, overflow attacks, and injection attacks are on the rise, threatening network security. In addition, security vulnerabilities within operating systems and applications can be exploited by hackers to hack into systems. To address such problems, Huawei provides the intrusion prevention function to defend against various attacks and protect the network from being attacked.
As shown in Figure 1, when an extranet user accesses the enterprise intranet, the device detects the access traffic. If an intrusion behavior is detected, the device blocks the access. Otherwise, the traffic is allowed. Similarly, when an intranet user accesses an external network, if the accessed web page or server contains malicious codes, the device blocks the access. Otherwise, the traffic is permitted.

Figure 1 Networking diagram of intrusion prevention



Benefits

Intrusion prevention has the following advantages:

- Real-time attack blocking: A device is deployed on a network in in-path mode. When detecting an intrusion, the device blocks the intrusion and attack traffic in real time, minimizing intrusion impacts.
- In-depth protection: New attacks are hidden at the application layer of TCP/IP. Intrusion prevention can examine the content of application-layer packets, reassemble network data flows for protocol analysis and detection, and determine the traffic that must be blocked based on the attack type and policy.
- All-round protection: Intrusion prevention provides various protection measures against attacks such as worms, viruses, Trojan horses, botnets, spyware, adware, Common Gateway Interface (CGI) attacks, cross-site scripting attacks, injection attacks, directory traversal attacks, information leakage, remote file

inclusion (RFI) attacks, overflow attacks, code execution, DoS attacks, and scanning attacks, providing all-around protection for network security.

- All-scenario protection: Intrusion prevention not only protects traditional IT networks and assets, but also protects Internet of Things (IoT) assets such as cameras and printers as well as Operation Technology (OT) control systems such as the supervisory control and data acquisition (SCADA) system.
- Internal and external protection: Intrusion prevention can protect enterprises from both external and internal attacks. The intrusion prevention-capable device can detect the traffic passing through and protect servers and clients.
- Precise protection: The intrusion prevention system (IPS) signature database is continuously updated, enabling the device to deal with the latest threats. You can periodically update the IPS signature database of a device from the Huawei security center to ensure continuously effective intrusion prevention.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

IPS Overview

Descripción general de la prevención de intrusiones

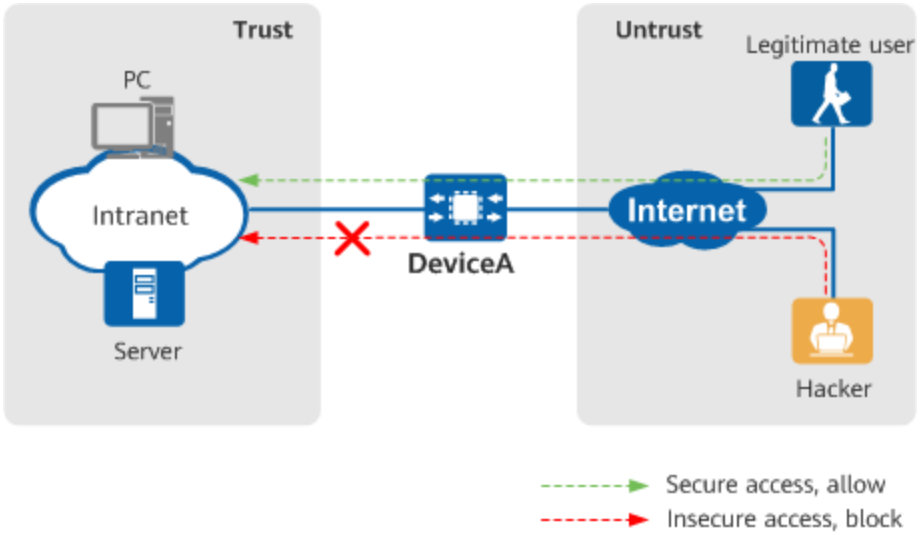
Definición

La prevención de intrusiones es un mecanismo de seguridad que detecta intrusiones basándose en la base de datos de firmas de ataques y toma determinadas medidas de respuesta para terminar las intrusiones en tiempo real.

Objetivo

Los troyanos, gusanos, botnets, spyware, ataques de desbordamiento e inyección están en aumento y amenazan la seguridad de la red. Además, los hackers pueden aprovechar las vulnerabilidades de seguridad de los sistemas operativos y las aplicaciones para acceder a los sistemas. Para abordar estos problemas, Huawei ofrece la función de prevención de intrusiones para defenderse de diversos ataques y proteger la red.
Como se muestra en la Figura 1 , cuando un usuario de la extranet accede a la intranet empresarial, el dispositivo detecta el tráfico de acceso. Si se detecta una intrusión, el dispositivo bloquea el acceso. De lo contrario, se permite el tráfico.
De igual forma, cuando un usuario de la intranet accede a una red externa, si la página web o el servidor al que accede contiene códigos maliciosos, el dispositivo bloquea el acceso. De lo contrario, se permite el tráfico.

Figura 1 Diagrama de red de prevención de intrusiones



Beneficios

La prevención de intrusiones tiene las siguientes ventajas:

- Bloqueo de ataques en tiempo real: Un dispositivo se implementa en una red en modo de ruta. Al detectar una intrusión, el dispositivo bloquea el tráfico de intrusión y ataque en tiempo real, minimizando así su impacto.
- Protección exhaustiva: Los nuevos ataques se ocultan en la capa de aplicación de TCP/IP. La prevención de intrusiones puede examinar el contenido de los paquetes de la capa de aplicación, reensamblar los

flujos de datos de red para el análisis y la detección de protocolos, y determinar el tráfico que debe bloquearse según el tipo de ataque y la política.

- Protección integral: la prevención de intrusiones proporciona varias medidas de protección contra ataques como gusanos, virus, troyanos, botnets, spyware, adware, ataques de interfaz de puerta de enlace común (CGI), ataques de secuencias de comandos entre sitios, ataques de inyección, ataques de recorrido de directorio, fuga de información, ataques de inclusión remota de archivos (RFI), ataques de desbordamiento, ejecución de código, ataques DoS y ataques de escaneo, proporcionando protección integral para la seguridad de la red.
- Protección para todo escenario: la prevención de intrusiones no solo protege las redes y los activos de TI tradicionales, sino que también protege los activos de Internet de las cosas (IoT), como cámaras e impresoras, así como los sistemas de control de tecnología operativa (OT), como el sistema de control de supervisión y adquisición de datos (SCADA).
- Protección interna y externa: La prevención de intrusiones puede proteger a las empresas de ataques tanto externos como internos. El dispositivo con capacidad de prevención de intrusiones puede detectar el tráfico que pasa y proteger servidores y clientes.
- Protección precisa: La base de datos de firmas del sistema de prevención de intrusiones (IPS) se actualiza constantemente, lo que permite al dispositivo hacer frente a las amenazas más recientes. Puede actualizar periódicamente la base de datos de firmas IPS de un dispositivo desde el centro de seguridad de Huawei para garantizar una prevención de intrusiones eficaz y continua.

REFERENCIAS TECNICAS

INGLES

IPv6 GRE Tunnel

NetEngine 8000 M1A V800R023C10SPC500 Configuration Guide

Search this document. 0 / 500

Please evaluate and leave your comments:

Configuring an IPv6 GRE Tunnel

IPv6 Generic Routing Encapsulation (GRE) provides a mechanism of encapsulating packets of a protocol into packets of another protocol. This allows packets to be transmitted over heterogeneous networks. The channel for transmitting heterogeneous packets is called a tunnel.

Usage Scenario

A single network protocol is used to transmit packets on a backbone network, whereas other protocols are used to transmit packets on non-backbone networks. Because the backbone and non-backbone networks use different protocols, packets cannot be transmitted between the non-backbone networks over the backbone network. IPv6 GRE resolves this issue. IPv6 GRE provides a mechanism of encapsulating packets of a protocol into packets of another protocol.

NOTE

For an IPv6 GRE tunnel:

- The packet transmission protocol is IPv6.
- Only IPv4 and IPv6 packets can be encapsulated and routed currently.

Pre-configuration Tasks

Before configuring an ordinary IPv6 GRE tunnel, configure reachable routes between the source and destination interfaces.

Configuring the Interface Bound to GRE

Configuring a Tunnel Interface

Configuring Tunnel Routes

Verifying the IPv6 GRE Tunnel Configuration

Configuring the Interface Bound to GRE

A GRE tunnel's source interface or the interface where the source address of a GRE tunnel resides must be bound to GRE. The GRE tunnel can use these interfaces to transmit GRE-encapsulated packets only after these interfaces are bound to GRE.

Context

Perform the following steps on the endpoint routers of a tunnel.

Procedure

Previous

2. Run **interface** interface-type interface-number

   The interface view is displayed.

3. Run **ip address** ip-address { mask | mask-length }

   An IP address is configured for the interface.

4. Run **binding tunnel gre**

   The interface is bound to GRE.

5. Run **quit**

   Exit the interface view.

6. Run **commit**

   The configuration is committed.

Configuring a Tunnel Interface

After creating a tunnel interface, specify IPv6 GRE as the encapsulation type, set the tunnel source address or source interface, and set the tunnel destination address. In addition, set the tunnel interface network address so that the tunnel can support route.

Context

An IPv6 GRE tunnel is established between two tunnel interfaces on two ends of a tunnel. Therefore, you need to configure tunnel interfaces of devices on both ends of the tunnel. Set the protocol type to IPv6 GRE, and specify a source address or interface and a destination address for the tunnel interface. Only tunnel interfaces with network addresses can support routes.

A tunnel interface is a logical interface, and its interface status changes to Down in the following cases:

- The destination address of the tunnel interface is unreachable or is the same as the address of this interface.
- The source interface status of the tunnel interface becomes Down.
- The IP address of the tunnel interface is invalid.

NOTE

After a tunnel interface is deleted, the interface configurations are also deleted.

Perform the following steps on the routers at the two ends of a tunnel.

Procedure

1. Run **system-view**

   The system view is displayed.

2. Run **interface tunnel** interface-number

   A tunnel interface is created, and the tunnel interface view is displayed.

   NOTE

   For centralized GRE in which a tunnel interface named in the format of slot ID/subcard ID/interface ID is used, the slot ID of the tunnel interface must be the same as the slot ID of the tunnel service board on which the tunnel's source interface resides. If the two slot IDs are inconsistent, the GRE tunnel cannot be established.

   ---

3. Run **tunnel-protocol gre ipv6**

   The tunnel is encapsulated with IPv6 GRE.

4. Run **source** { ipv6-address | ifName | ifTypeifNum }

   The source address or source interface of the tunnel is configured.

Previous

Run the **binding tunnel gre** command to bind GRE to the source interface or the interface where the source address resides. After the binding, a GRE tunnel can use the interface to forward packets encapsulated by GRE.

5. Run **destination** [**vpn-instance** vpn-instance-name] des-ipv6-address

   The destination address of the tunnel is configured.

6. Run **ipv6 address** { ipv6-address prefix-length | ipv6-address/prefix-length }

   The IPv6 address of the tunnel interface is configured. To support dynamic routing protocols on a tunnel, configure a network address for the tunnel interface. The network address of the tunnel interface may not be a public address, but should be in the same network segment on both ends of the tunnel.

7. Run **commit**

   The configuration is committed.

Configuring Tunnel Routes

Routes for a tunnel must be available on both the source and destination devices so that packets encapsulated with GRE can be forwarded correctly.

Context

Packets can be properly forwarded over an IPv6 GRE tunnel only if the local and remote devices both have routes that are advertised over the tunnel. Currently, only static routes can be advertised over an IPv6 GRE tunnel. A static route must be configured on both the source and destination devices. The destination address of the static route is neither the destination address of the tunnel nor the address of the destination tunnel interface. Instead, it is the destination address of the packet that is not encapsulated using IPv6 GRE. The outbound interface must be the tunnel interface at the local end.

Perform the following steps on the routers at both ends of the tunnel:

Procedure

1. Run **system-view**

   The system view is displayed.

2. Choose either of the following methods to configure static routes to be advertised over the IPv6 GRE tunnel:

   - If an IPv4 address is configured for the tunnel interface:

     Run the **ip route-static** dest-ip-address { mask | mask-length } **tunnel** interface-number [**description** text] command to configure an IPv4 static route.

   - If an IPv6 address is configured for the tunnel interface:

     Run the **ipv6 route-static** dest-ipv6-address prefix-length { interface-type interface-number [nexthop-ipv6-address] | **vpn-instance** vpn-instance-name nexthop-ipv6-address | nexthop-ipv6-address } [**description** text] command to configure an IPv6 static route.

3. Run **commit**

   The configuration is committed.

Verifying the IPv6 GRE Tunnel Configuration

After configuring an IPv6 GRE tunnel, you can check the status of the tunnel interface and routing information.

Prerequisites

An IPv6 GRE tunnel has been configured.

Procedure

- Run the **display ipv6 interface tunnel** command to check the status of a tunnel interface.
- Run either of the following commands to check related information:

Previous

If an IPv6 address is configured for the tunnel interface:

- Run the **display ipv6 routing-table** command to check the IPv6 routing table.
- Run the **ping ipv6 -a** source-ipv6-address dest-ipv6-address command to check tunnel connectivity.

About Us
How to Buy
Partner
Resources
Quick Links
Huawei e+ App
HUAWEI eKit App
Huawei HiKnow APP
HUAWEI eFly App
Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.
Privacy Terms of use Cookies Cookie Settings Report content

Previous

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

IPv6 GRE Tunnel

Guía de configuración de NetEngine 8000 M1A V800R023C10SPC500

Buscar este documento. 0 / 500

Por favor evalúa y deja tus comentarios:

Configuración de un túnel GRE IPv6

La encapsulación de enrutamiento genérico (GRE) de IPv6 proporciona un mecanismo para encapsular paquetes de un protocolo en paquetes de otro protocolo. Esto permite la transmisión de paquetes a través de redes heterogéneas. El canal para la transmisión de paquetes heterogéneos se denomina túnel.

Escenario de uso

Se utiliza un único protocolo de red para transmitir paquetes en una red troncal, mientras que se utilizan otros protocolos para transmitir paquetes en redes no troncales. Dado que las redes troncales y no troncales utilizan protocolos diferentes, no es posible transmitir paquetes entre estas últimas a través de la red troncal. IPv6 GRE resuelve este problema. IPv6 GRE proporciona un mecanismo para encapsular paquetes de un protocolo en paquetes de otro protocolo.

NOTE

Para un túnel GRE IPv6:

- El protocolo de transmisión de paquetes es IPv6.
- Actualmente sólo se pueden encapsular y enrutar paquetes IPv4 e IPv6.

Tareas de preconfiguración

Antes de configurar un túnel GRE IPv6 normal, configure rutas alcanzables entre las interfaces de origen y destino.

Configuración de la interfaz vinculada a GRE

Configuración de una interfaz de túnel

Configuración de rutas de túnel

Verificación de la configuración del túnel GRE IPv6

Configuración de la interfaz vinculada a GRE

La interfaz de origen de un túnel GRE, o la interfaz donde reside la dirección de origen de un túnel GRE, debe estar vinculada a GRE. El túnel GRE puede usar estas interfaces para transmitir paquetes encapsulados en GRE solo después de que estas interfaces estén vinculadas a GRE.

Contexto

Realice los siguientes pasos en los enrutadores de punto final de un túnel.

Pro Anterior

2. Ejecutar **interfaz** tipo-de-interfaz número-de-interfaz

   Se muestra la vista de la interfaz.

3. Ejecutar **dirección IP** dirección-IP { máscara | longitud-de-máscara }

   Se configura una dirección IP para la interfaz.

4. Ejecutar **túnel de enlace gre**

   La interfaz está vinculada a GRE.

5. Salir **corriendo**

   Salir de la vista de la interfaz.

6. Ejecutar **confirmación**

   La configuración está confirmada.

Configuración de una interfaz de túnel

Tras crear una interfaz de túnel, especifique IPv6 GRE como tipo de encapsulación, configure la dirección de origen o la interfaz de origen del túnel y la dirección de destino. Además, configure la dirección de red de la interfaz de túnel para que el túnel admita el enrutamiento.

Contexto

Un túnel GRE IPv6 se establece entre dos interfaces de túnel en ambos extremos del túnel. Por lo tanto, es necesario configurar las interfaces de túnel de los dispositivos en ambos extremos. Establezca el tipo de protocolo en GRE IPv6 y especifique una dirección o interfaz de origen y una dirección de destino para la interfaz de túnel. Solo las interfaces de túnel con direcciones de red admiten rutas.

Una interfaz de túnel es una interfaz lógica y su estado cambia a Inactivo en los siguientes casos:

- La dirección de destino de la interfaz del túnel es inalcanzable o es la misma que la dirección de esta interfaz.
- El estado de la interfaz de origen de la interfaz del túnel pasa a estar inactivo.
- La dirección IP de la interfaz del túnel no es válida.

NOTE

Después de eliminar una interfaz de túnel, también se eliminan las configuraciones de la interfaz.

Realice los siguientes pasos en los enrutadores en los dos extremos de un túnel.

Procedimiento

1. Ejecutar **system-view**

   Se muestra la vista del sistema.

2. Ejecutar **interfaz túnel** número de interfaz

   Se crea una interfaz de túnel y se muestra la vista de la interfaz de túnel.

   NOTE

   En el caso de GRE centralizado, donde se utiliza una interfaz de túnel cuyo nombre se define en el formato ID de ranura/ID de subtarjeta/ID de interfaz, el ID de ranura de la interfaz de túnel debe ser el mismo que el ID de ranura de la tarjeta de servicio de túnel donde reside la interfaz de origen del túnel. Si los dos ID de ranura son incoherentes, no se podrá establecer el túnel GRE.

   ---

3. Ejecutar **túnel-protocolo gre ipv6**

   El túnel está encapsulado con IPv6 GRE.

4. Ejecutar **source** { dirección-ipv6 | ifName | ifTypeifNum }

Anterior

Ejecute el comando **binding tunnel gre** para vincular GRE a la interfaz de origen o a la interfaz donde reside la dirección de origen. Tras la vinculación, un túnel GRE puede usar la interfaz para reenviar paquetes encapsulados por GRE.

5. Ejecutar **destino** [**instancia-vpn** nombre-instancia-vpn] dirección-ipv6-des

   Se configura la dirección de destino del túnel.

6. Ejecutar **dirección ipv6** { dirección-ipv6 longitud-prefijo | dirección-ipv6/longitud-prefijo }

   La dirección IPv6 de la interfaz del túnel está configurada. Para admitir protocolos de enrutamiento dinámico en un túnel, configure una dirección de red para la interfaz. Esta dirección de red no puede ser pública, pero debe estar en el mismo segmento de red en ambos extremos del túnel.

7. Ejecutar **confirmación**

   La configuración está confirmada.

Configuración de rutas de túnel

Las rutas para un túnel deben estar disponibles tanto en los dispositivos de origen como de destino para que los paquetes encapsulados con GRE puedan reenviarse correctamente.

Contexto

Los paquetes se pueden reenviar correctamente a través de un túnel GRE IPv6 solo si tanto los dispositivos locales como los remotos tienen rutas anunciadas a través del túnel. Actualmente, solo se pueden anunciar rutas estáticas a través de un túnel GRE IPv6. Se debe configurar una ruta estática tanto en el dispositivo de origen como en el de destino. La dirección de destino de la ruta estática no es la dirección de destino del túnel ni la dirección de la interfaz de destino del túnel. En cambio, es la dirección de destino del paquete que no está encapsulado mediante GRE IPv6. La interfaz de salida debe ser la interfaz del túnel en el extremo local.

Realice los siguientes pasos en los enrutadores en ambos extremos del túnel:

Procedimiento

1. Ejecutar **system-view**

   Se muestra la vista del sistema.

2. Elija uno de los siguientes métodos para configurar rutas estáticas que se anunciarán a través del túnel GRE IPv6:

   - Si se configura una dirección IPv4 para la interfaz del túnel:

     Ejecute el comando **ip route-static** dest-ip-address { mask | mask-length } **tunnel** interface-number [**description** text] para configurar una ruta estática IPv4.

   - Si se configura una dirección IPv6 para la interfaz del túnel:

     Ejecute el **comando ipv6 route-static** dest-ipv6-address prefix-length { interface-type interface-number [nexthop-ipv6-address] | **vpn-instance** vpn-instance-name nexthop-ipv6-address | nexthop-ipv6-address } [**description** text] para configurar una ruta estática IPv6.

3. Ejecutar **confirmación**

   La configuración está confirmada.

Verificación de la configuración del túnel GRE IPv6

Después de configurar un túnel GRE IPv6, puede verificar el estado de la interfaz del túnel y la información de enrutamiento.

Prerrequisitos

Se ha configurado un túnel GRE IPv6.

Procedimiento

- Ejecute el comando **display ipv6 interface tunnel** para comprobar el estado de una interfaz de túnel.
- E

Anterior

- Ejecute el comando **ping -a** source-ip-address dest-ip-address para verificar la conectividad del túnel.

Si se configura una dirección IPv6 para la interfaz del túnel:

- Ejecute el comando **display ipv6 route-table** para verificar la tabla de enrutamiento IPv6.
- Ejecute el comando **ping ipv6 -a** source-ipv6-address dest-ipv6-address para verificar la conectividad del túnel.

Sobre nosotros
Cómo comprar
Pareja
Recursos
Enlaces rápidos
Aplicación Huawei e+
Aplicación HUAWEI eKit
Aplicación Huawei HiKnow
Aplicación HUAWEI eFly
Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.
Privacidad Condiciones de uso Galletas Configuración de cookies Reportar contenido

Anterior

REFERENCIAS TECNICAS

INGLES

IPv6 IPv4 Tunnel

NE40E V800R022C00SPC600 Configuration Guide

Search this document. 0 / 500

Please evaluate and leave your comments:

IPv6 over IPv4 Tunnel Configuration

The IPv6 over IPv4 tunneling technology provides a solution for the transition from IPv4 to IPv6.

Overview of IPv6 over IPv4 Tunnel

Configuration Precautions for IPv6 over IPv4 Tunnel

Configuring a Manual IPv6 over IPv4 Tunnel

Configuring a 6to4 Tunnel

Configuring a 6RD Tunnel

Configuration Examples for IPv6 over IPv4 Tunnel

- Example for Configuring a Manual IPv6 over IPv4 Tunnel
- Example for Configuring a 6to4 Tunnel
- Example for Configuring 6to4 Relay
- Example for Configuring a 6RD Tunnel
- Example for Configuring a 6RD Relay

Overview of IPv6 over IPv4 Tunnel

The IPv6 over IPv4 tunnel technology enables communication between isolated IPv6 networks over existing IPv4 networks. IPv6 packets can be transparently transmitted over IPv4 networks after being encapsulated into IPv4 packets.

During the early transition from IPv4 to IPv6 networks, IPv4 networks have been widely deployed, whereas IPv6 networks are isolated islands scattered around the world. With the tunneling technology, IPv6 over IPv4 tunnels can be created on the IPv4 networks to connect the isolated IPv6 sites. To establish IPv6 over IPv4 tunnels, the IPv4/IPv6 dual stack must be enabled on the routers at the borders of the IPv4 and IPv6 networks.

Configuration Precautions for IPv6 over IPv4 Tunnel

Feature Requirements

Table 1-659 Feature requirements

Feature Requirements	Series	Models
The interface, source address, and destination address of an IPv6 over IPv4 tunnel do not support L3VPN.	NE40E	NE40E
IPv4 routes used by IPv6 over IPv4 tunnels and 6to4 tunnels can be used c	NE40E	NE40E

The 6to4, 6over4, and 6rd tunnels with the same source address cannot be controlled separately. If one of them is configured, the other two types of tunnels can forward packets normally.	NE40E	NE40E
After the source IP address of the 6to4 tunnel is changed, traffic from the original 6to4 address can still be forwarded. After smoothing, traffic is interrupted.	NE40E	NE40E

Configuring a Manual IPv6 over IPv4 Tunnel

A manual IPv6 over IPv4 tunnel is a P2P tunnel. The source address and destination address of a manual IPv6 over IPv4 tunnel are both manually assigned and must be unique on the same device. A manual IPv6 over IPv4 tunnel acts as a permanent link that connects two IPv6 networks across an IPv4 network. Border routers can communicate with each other securely and regularly through manual IPv6 over IPv4 tunnels.

Usage Scenario

To enable IPv6 networks to communicate with each other through an IPv4 network, configure IPv6 over IPv4 tunnels on the routers where IPv6 networks border an IPv4 network.

A manual IPv6 over IPv4 tunnel can be established between two border routers to provide a stable connection for separated IPv6 networks. It can also be established between a terminal system and a border router to provide a connection for the terminal system to access an IPv6 network. The devices at the two ends of an IPv6 over IPv4 tunnel must support the IPv4/IPv6 dual stack. The intermediate devices do not need to support the IPv4/IPv6 dual stack. You can configure multiple manual IPv6 over IPv4 tunnels on the border router to communicate with multiple IPv6 networks.

Pre-configuration Tasks

Before configuring a manual IPv6 over IPv4 tunnel, complete the following tasks:

- Connect interfaces and configure physical parameters for the interfaces to ensure that the physical status of the interfaces is Up.
- Configure link layer protocol parameters for the interfaces to ensure that the link layer protocol status of the interfaces is Up.
- Assign an IPv4 address to each border router.
- Configure IPv6 globally and on interfaces.
- Assign an IPv6 address to each border router.

Procedure

1. Run **system-view**

   The system view is displayed.

2. Run **interface tunnel** interface-number

   A tunnel interface is created.

3. Run **tunnel-protocol ipv6-ipv4**

   The tunnel mode is set to manual IPv6 over IPv4 tunnel mode.

4. Run **source** { ip-address | interface-type interface-number }

   The source address or source interface of the tunnel is specified.

5. Run **destination** ip-address

   The destination address of the tunnel is specified.

   > **NOTE**
   >
   > The destination address of an IPv6 over IPv4 tunnel can be a physical or loopback interface address.

6. Previous

An IPv6 address is configured for the tunnel interface.

8. Run **commit**

   The configuration is committed.

Verifying the Configurations

After configuring a manual IPv6 over IPv4 tunnel, verify the configurations.

- Run the **display ipv6 interface tunnel** interface-number command to check the IPv6 configuration of a tunnel interface.

Configuring a 6to4 Tunnel

A 6to4 tunnel can interconnect isolated IPv6 networks through an IPv4 network.

Usage Scenario

To enable IPv6 networks to communicate with each other through an IPv4 network, configure IPv6 over IPv4 tunnels on the routers where IPv6 networks border the IPv4 network.

6to4 tunnels use special 6to4 addresses that are in the format of 2002:a.b.c.d::/48, in which a.b.c.d represents the source address of the tunnel interface. During communication, the IPv4 address in a 6to4 address is used to encapsulate packets. The 6to4 tunnel does not need to be configured with a destination address.

Pre-configuration Tasks

Before configuring a 6to4 tunnel, complete the following tasks:

- Connect interfaces and configure physical parameters for the interfaces to ensure that the physical status of the interfaces is Up.
- Configure link layer protocol parameters for the interfaces to ensure that the link layer protocol status of the interfaces is Up.
- Configure the IPv4/IPv6 dual stack.

Procedure

1. Run **system-view**

   The system view is displayed.

2. Run **interface tunnel** interface-number

   A tunnel interface is created.

3. Run **tunnel-protocol ipv6-ipv4 6to4**

   The tunnel mode is set to 6to4 tunnel mode.

4. Run **source** { ip-address | interface-type interface-number }

   The source address or source interface of the tunnel is specified.

5. Run **ipv6 enable**

   IPv6 is configured on the interface.

6. Run **ipv6 address** { ipv6-address prefix-length | ipv6-address-mask }

   An IPv6 address is configured for the tunnel interface.

   NOTE

   The IPv6 address prefix specified in this command must be the same as the prefix of the address of the 6to4 network where the border router resides.

7. Run **commit**

   The configuration is committed.

Ch

Previous

Configuring a 6RD Tunnel

A 6RD tunnel is a point-to-multipoint (P2MP) tunnel that connects IPv6 sites through a carrier's IPv4 network. 6RD tunnels have been widely deployed on carriers' networks.

Usage Scenario

A 6RD tunnel is a P2MP tunnel and is an enhancement to the 6to4 solution. 6RD tunneling allows carriers to use one of their own IPv6 prefixes as the 6RD prefix, mitigating the IPv4 address shortage of the 6to4 solution.

6RD is used in the following scenarios:

- 6RD domain-6RD domain

  Connects different 6RD domains. 6RD CEs are deployed at either end of a tunnel, which enables hosts or devices in different 6RD domains to communicate with each other.

- 6RD domain-IPv6 network

  Connects a 6RD domain to a native IPv6 network. A 6RD CE and a 6RD BR are deployed at either end of a tunnel, which enables hosts or devices in the 6RD domain and on the IPv6 network to access each other.

Pre-configuration Tasks

Before configuring a 6RD tunnel, complete the following tasks:

- Connect interfaces and set their physical parameters to ensure that the physical status of the interfaces is Up.
- Configure link-layer protocol parameters for interfaces to go Up at the link layer.
- Ensure reachable routes between the source and destination interfaces.
- Enable IPv4/IPv6 dual stack on the interfaces.

Procedure

1. Run **system-view**

   The system view is displayed.

2. Run **interface tunnel** interface-number

   A tunnel interface is created, and the tunnel interface view is displayed.

3. Run **tunnel-protocol ipv6-ipv4 6rd**

   The tunnel encapsulation mode is set to 6RD.

4. Run **source** { ip-address | interface-type interface-number }

   The source address or source interface is specified for the 6RD tunnel interface.

5. Run **ipv6-prefix** { ipv6-address prefix-length | ipv6-prefix-mask }

   The 6RD prefix and 6RD prefix length are configured.

   A 6RD prefix is the IPv6 prefix assigned by a carrier for a 6RD address. The 6RD delegated prefix is calculated by combining the 6RD prefix and part or all bits of an IPv4 address. The 6RD delegated prefix is used to assign IPv6 address prefixes to devices or hosts in a 6RD domain.

   The 6RD prefix for each 6RD domain must be unique.

6. Run **ipv4-prefix length** ipv4-prefix-length

   The IPv4 prefix length of the 6RD tunnel is configured.

   The IPv4 prefix length indicates the number of high-order bits to be deleted from the source tunnel address (an IPv4 address). The remaining bits of the IPv4 address and the 6RD prefix together form the 6RD delegated prefix.

   You are advised to set ipv4-prefix-length to 0 when the carrier network is an IPv4 network. On an IPv4 carrier network, the source tunnel address is entirely embedded in the 6RD delegated prefix, which is used to search for the destination tunnel address.

   The IPv4 prefix length of the 6RD tunnel in each 6RD domain must be unique.

Previous

IPv6 is enabled on the interface.

8. Run **ipv6 address** { ipv6-address prefix-length | ipv6-address-mask }

   An IPv6 address is configured for the tunnel interface, and the address prefix is the 6RD delegated prefix.

9. (Optional) Run **border-relay address** br-ipv4-address The IPv4 address of the 6RD BR is configured.

   The IPv4 address of the 6RD BR needs to be configured on a 6RD CE only in a relay scenario where a 6RD domain interworks with a native IPv6 network.

Verify the configuration.

After configuring the 6RD tunnel, check the configurations.

Run the **display ipv6 interface tunnel** interface-number command to check the IPv6 attribute on the tunnel interface.

Configuration Examples for IPv6 over IPv4 Tunnel

This section provides configuration examples, which cover networking requirements, configuration precautions, and configuration roadmap.

Example for Configuring a Manual IPv6 over IPv4 Tunnel

This section provides an example for configuring a manual IPv6 over IPv4 tunnel.

Networking Requirements

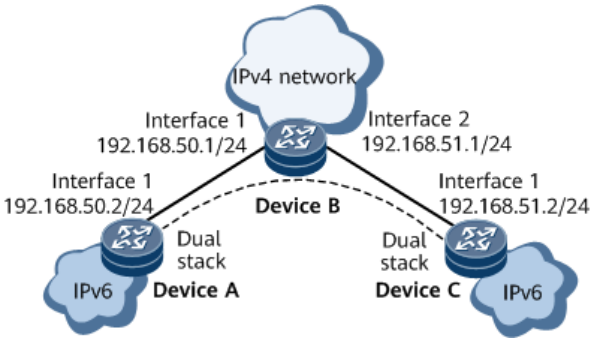
As shown in Figure 1-1994, two IPv6 networks are connected to DeviceB on the IPv4 backbone network through DeviceA and DeviceC. To interconnect the two IPv6 networks, configure a manual IPv6 over IPv4 tunnel between DeviceA and DeviceC.

Figure 1-1994 Networking diagram for configuring a manual IPv6 over IPv4 tunnel

---

NOTE

Interfaces 1 and 2 in this example represent GE 1/0/0 and GE 2/0/0, respectively.



Precautions

When configuring a manual IPv6 over IPv4 tunnel, note the following points:

- Create a tunnel interface and set parameters for the tunnel interface.
- Perform the following configuration on both DeviceA and DeviceC. The source IP address of the local end is the destination IP address of the remote end of the tunnel. Similarly, the destination IP address of the local end is the source IP address of the remote end.
- Configure an IPv6 address for the tunnel interface to support routing protocols.

Configuration Roadmap

The configuration roadmap is as follows:

Previous

3. Set the protocol type to IPv6-IPv4.

Data Preparation

To complete the configuration, you need the following data:

- IP addresses of interfaces
- IPv6 addresses of the tunnel interfaces, and source and destination IPv4 addresses of the tunnel

Procedure

1. Configure IPv6 addresses for interfaces on DeviceA, DeviceB, and DeviceC.

   # Configure DeviceA.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceA
   [*HUAWEI] commit
   [~DeviceA] interface gigabitethernet 1/0/0
   [~DeviceA-GigabitEthernet1/0/0] ip address 192.168.50.2 255.255.255.0
   [*DeviceA-GigabitEthernet1/0/0] undo shutdown
   [*DeviceA-GigabitEthernet1/0/0] quit
   ```

   # Configure DeviceB.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceB
   [*HUAWEI] commit
   [~DeviceB] interface gigabitethernet 1/0/0
   [~DeviceB-GigabitEthernet1/0/0] ip address 192.168.50.1 255.255.255.0
   [*DeviceB-GigabitEthernet1/0/0] undo shutdown
   [*DeviceB-GigabitEthernet1/0/0] quit
   [*DeviceB] interface gigabitethernet 2/0/0
   [*DeviceB-GigabitEthernet2/0/0] ip address 192.168.51.1 255.255.255.0
   [*DeviceB-GigabitEthernet2/0/0] undo shutdown
   [*DeviceB-GigabitEthernet2/0/0] commit
   [~DeviceB-GigabitEthernet2/0/0] quit
   ```

   # Configure DeviceC.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceC
   [*HUAWEI] commit
   [~DeviceC] interface gigabitethernet 1/0/0
   [~DeviceC-GigabitEthernet1/0/0] ip address 192.168.51.2 255.255.255.0
   [*DeviceC-GigabitEthernet1/0/0] undo shutdown
   [*DeviceC-GigabitEthernet1/0/0] quit
   ```

2. Create tunnel interfaces, and configure a tunnel mode, IPv6 addresses for the tunnel interfaces, and source and destination addresses for the tunnel.

   # Configure DeviceA.

   ```
   [*DeviceA] interface Tunnel 10
   [*DeviceA-Tunnel10] tunnel-protocol ipv6-ipv4
   [*DeviceA-Tunnel10] ipv6 enable
   [*DeviceA-Tunnel10] ipv6 address 2001:db8::1 64
   [*DeviceA-Tunnel10] source 192.168.50.2
   [*DeviceA-Tunnel10] destination 192.168.51.2
   [*DeviceA-Tunnel10] quit
   ```

Previous

```
[*DeviceC-Tunnel10] ipv6 enable
[*DeviceC-Tunnel10] ipv6 address 2001:db8::2 64
[*DeviceC-Tunnel10] source 192.168.51.2
[*DeviceC-Tunnel10] destination 192.168.50.2
[*DeviceC-Tunnel10] quit
```

3. Configure static routes to ensure that DeviceA and DeviceC are reachable.

   # Configure DeviceA.

```
[*DeviceA] ip route-static 192.168.51.0 255.255.255.0 192.168.50.1
[*DeviceA] commit
```

   # Configure DeviceC.

```
[*DeviceC] ip route-static 192.168.50.0 255.255.255.0 192.168.51.1
[*DeviceC] commit
```

4. Verify the configuration.

   # Ping the IPv4 address of GE 1/0/0 on DeviceA from DeviceC. The ping operation is successful.

```
[~DeviceC] ping 192.168.50.2
  PING 192.168.50.2: 56  data bytes, press CTRL_C to break
    Reply from 192.168.50.2: bytes=56 Sequence=1 ttl=254 time=84 ms
    Reply from 192.168.50.2: bytes=56 Sequence=2 ttl=254 time=27 ms
    Reply from 192.168.50.2: bytes=56 Sequence=3 ttl=254 time=25 ms
    Reply from 192.168.50.2: bytes=56 Sequence=4 ttl=254 time=3 ms
    Reply from 192.168.50.2: bytes=56 Sequence=5 ttl=254 time=24 ms

  --- 192.168.50.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/32/84 ms
```

   # Ping the IPv6 address of Tunnel 10 on DeviceA from Device C, and the ping operation is successful.

```
[~DeviceC] ping ipv6 2001:db8::1
  PING 2001:db8::1 : 56  data bytes, press CTRL_C to break
    Reply from 2001:db8::1
    bytes=56 Sequence=1 hop limit=64  time = 28 ms
    Reply from 2001:db8::1
    bytes=56 Sequence=2 hop limit=64  time = 27 ms
    Reply from 2001:db8::1
    bytes=56 Sequence=3 hop limit=64  time = 26 ms
    Reply from 2001:db8::1
    bytes=56 Sequence=4 hop limit=64  time = 27 ms
    Reply from 2001:db8::1
    bytes=56 Sequence=5 hop limit=64  time = 26 ms
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
  round-trip min/avg/max = 26/26/28 ms
```

Configuration Files

- DeviceA configuration file

```
#
```

Previous

```
#
interface Tunnel 10
 ipv6 enable
 ipv6 address 2001:db8::1/64
 tunnel-protocol ipv6-ipv4
 source 192.168.50.2
 destination 192.168.51.2
#
ip route-static 192.168.51.0 255.255.255.0 192.168.50.1
#
return
```

- DeviceB configuration file

```
#
 sysname DeviceB
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 192.168.50.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 undo shutdown
 ip address 192.168.51.1 255.255.255.0
#
return
```

- DeviceC configuration file

```
#
 sysname DeviceC
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 192.168.51.2 255.255.255.0
#
interface Tunnel 10
 ipv6 enable
 ipv6 address 2001:db8::2/64
 tunnel-protocol ipv6-ipv4
 source 192.168.51.2
 destination 192.168.50.2
#
ip route-static 192.168.50.0 255.255.255.0 192.168.51.1
#
return
```

Example for Configuring a 6to4 Tunnel

This section provides an example for configuring a 6to4 tunnel.

Networking Requirements

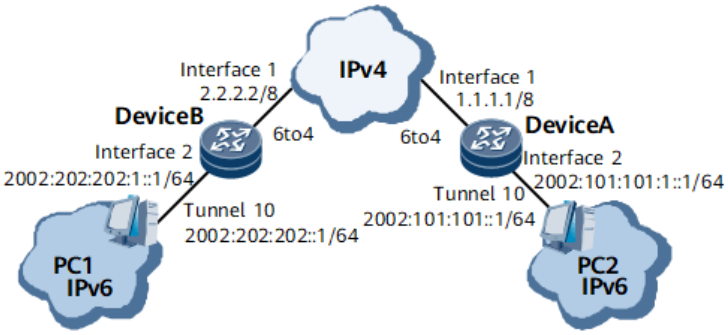
As shown in Figure 1-1995, two IPv6 networks are both 6to4 networks; both DeviceA and DeviceB connect to a 6to4 network and the IPv4 backbone network. To interconnect the two 6to4 networks, a 6to4 tunnel needs to be configured between DeviceA and DeviceB.

To allow interworking of 6to4 networks, a 6to4 address needs to be configured for the host, with the prefix of **2002:IPv4 address:** and prefix length of 48 bits. As shown in Figure 1-1995, the IPv4 address of the interface connecting DeviceA and the IPv4 network is 1.1.1.1. Then, the 6to4 address for the 6to4 network where DeviceA resides should have a prefix of 2002:101:101:: and a prefix length of 64 bits.

Figure 1-1995 Networking diagram for configuring a 6to4 tunnel

Previous

Interfaces 1 and 2 in this example represent GE 1/0/0 and GE 1/0/1, respectively.



Precautions

When configuring a 6to4 tunnel, note the following points:

- Create a tunnel interface and set parameters for the tunnel interface.
- Configure only the source IPv4 address of the tunnel. The destination IP address of the tunnel is the same as the destination IP address contained in the original IPv6 packet. The source IP address of a 6to4 tunnel must be unique.
- Assign a 6to4 address to the interface that connects a border router to a 6to4 network and an IPv4 address to the interface that connects a border router to an IPv4 network.
- Configure an IP address for the tunnel interface to support routing protocols.

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IPv4/IPv6 dual stack on the routers.
2. Configure a 6to4 tunnel on the routers.
3. Configure static routes on the routers.

Data Preparation

To complete the configuration, you need the following data:

- IPv4 and IPv6 addresses of the interfaces
- Source IP address of the tunnel interface

Procedure

1. Configure IP addresses for interfaces on DeviceA and DeviceB.

   # Configure DeviceA.

```
<HUAWEI> system-view
[~HUAWEI] sysname DeviceA
[*HUAWEI] commit
[~DeviceA] interface GigabitEthernet 1/0/0
[~DeviceA-GigabitEthernet1/0/0] ip address 1.1.1.1 8
[*DeviceA-GigabitEthernet1/0/0] undo shutdown
[*DeviceA-GigabitEthernet1/0/0] quit
[*DeviceA] interface gigabitethernet 1/0/1
[*DeviceA-GigabitEthernet1/0/1] ipv6 enable
[*DeviceA-GigabitEthernet1/0/1] ipv6 address 2002:101:101:1::1 64
```

Previous

```
<HUAWEI> system-view
[~HUAWEI] sysname DeviceB
[*HUAWEI] commit
[~DeviceB] interface GigabitEthernet 1/0/0
[~DeviceB-GigabitEthernet1/0/0] ip address 2.2.2.2 8
[*DeviceB-GigabitEthernet1/0/0] undo shutdown
[*DeviceB-GigabitEthernet1/0/0] quit
[*DeviceB] interface gigabitethernet 1/0/1
[*DeviceB-GigabitEthernet1/0/1] ipv6 enable
[*DeviceB-GigabitEthernet1/0/1] ipv6 address 2002:202:202:1::1 64
[*DeviceB-GigabitEthernet1/0/1] undo shutdown
[*DeviceB-GigabitEthernet1/0/1] quit
```

2. # Configure a 6to4 tunnel on DeviceA and DeviceB.

   # Configure DeviceA.

```
[*DeviceA] interface Tunnel 10
[*DeviceA-Tunnel10] tunnel-protocol ipv6-ipv4 6to4
[*DeviceA-Tunnel10] ipv6 enable
[*DeviceA-Tunnel10] ipv6 address 2002:101:101::1 64
[*DeviceA-Tunnel10] source 1.1.1.1
[*DeviceA-Tunnel10] quit
```

   # Configure DeviceB.

```
[*DeviceB] interface Tunnel 10
[*DeviceB-Tunnel10] tunnel-protocol ipv6-ipv4 6to4
[*DeviceB-Tunnel10] ipv6 enable
[*DeviceB-Tunnel10] ipv6 address 2002:202:202::1 64
[*DeviceB-Tunnel10] source 2.2.2.2
[*DeviceB-Tunnel10] quit
```

   NOTE

   Available routes are required between DeviceA and DeviceB. In this example, the two routers are directly connected. Therefore, no routing protocol is configured.

3. # Configure a route to the 6to4 network on DeviceA and DeviceB.

   # Configure DeviceA.

```
[*DeviceA] ipv6 route-static 2002:: 16 Tunnel 10
[*DeviceA] commit
```

   # Configure DeviceB.

```
[*DeviceB] ipv6 route-static 2002:: 16 Tunnel 10
[*DeviceB] commit
```

4. Verify the configuration.

   # Check the IPv6 status of Tunnel 10 on DeviceA. The command output shows that the tunnel is **UP**.

```
[~DeviceA] display ipv6 interface Tunnel 10
Tunnel10 current state : UP
IPv6 protocol current state : UP
link-local address is FE80::101:101
  Global unicast address(es):
    2002:101:101::1, subnet is 2002:101:101::/64
```

Previous

```
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1.
  ND reachable time is 1200000 milliseconds.
  ND retransmit interval is 1000 milliseconds.
  Hosts use stateless autoconfig for addresses.
```

Ping the 6to4 address of GE 2/0/0 on DeviceB from DeviceA. The command output shows the ping is successful.

```
[~DeviceA] ping ipv6 2002:202:202:1::1
  PING 2002:202:202:1::1 : 56  data bytes, press CTRL_C to break
    Reply from 2002:202:202:1::1
    bytes=56 Sequence=1 hop limit=64 time=37 ms
    Reply from 2002:202:202:1::1
    bytes=56 Sequence=2 hop limit=64 time=2 ms
    Reply from 2002:202:202:1::1
    bytes=56 Sequence=3 hop limit=64 time=8 ms
    Reply from 2002:202:202:1::1
    bytes=56 Sequence=4 hop limit=64 time=1 ms
    Reply from 2002:202:202:1::1
    bytes=56 Sequence=5 hop limit=64 time=2 ms

  ---2002:202:202:1::1 ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 4/9/25 ms
```

Configuration Files

- DeviceA configuration file

```
#
 sysname DeviceA
#
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 1.1.1.1 255.0.0.0
#
interface GigabitEthernet 1/0/1
 undo shutdown
 ipv6 enable
 ipv6 address 2002:101:101:1::1/64
#
interface Tunnel 10
 ipv6 enable
 ipv6 address 2002:101:101::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source 1.1.1.1
#
ipv6 route-static 2002:: 16 Tunnel 10
#
return
```

- DeviceB configuration file

```
#
```

Previous

```
 ip address 2.2.2.2 255.0.0.0
#
interface GigabitEthernet1/0/1
 undo shutdown
 ipv6 enable
 ipv6 address 2002:202:202:1::1/64
#
interface Tunnel 10
 ipv6 enable
 ipv6 address 2002:202:202::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source 2.2.2.2
#
ipv6 route-static 2002:: 16 Tunnel 10
#
return
```

Example for Configuring 6to4 Relay

This section provides an example for configuring 6to4 relay.

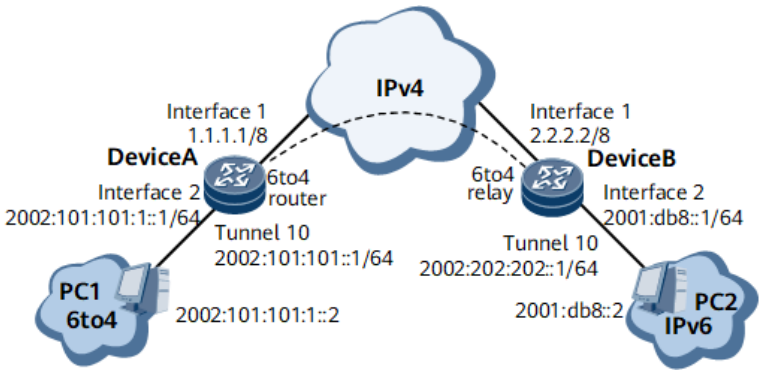
Networking Requirements

As shown in Figure 1-1996, DeviceA functions as a 6to4 router and connects to the 6to4 network; DeviceB is a 6to4 relay router and connects to the IPv6 network (2001:db8::/64); DeviceA connects to DeviceB through the IPv4 backbone network. To interconnect the hosts on the 6to4 and IPv6 networks, a 6to4 tunnel between DeviceA and DeviceB needs to be established.

The method of configuring a tunnel between a 6to4 relay router and a 6to4 router is the same as the method of configuring a tunnel between 6to4 routers. To interconnect a 6to4 network with an IPv6 network, configure a static route to the IPv6 network on each 6to4 router.

Figure 1-1996 Networking diagram for configuring 6to4 relay

> **NOTE**
>
> Interfaces 1 and 2 in this example represent GE 1/0/0 and GE 1/0/1, respectively.



Precautions

When configuring a 6to4 tunnel, note the following points:

- Create a tunnel interface and set parameters for the tunnel interface.
- Configure only the source IPv4 address of the tunnel. The destination IPv4 address of the tunnel is the same as the destination IPv4 address contained in the original IPv6 packet. The source address of a 6to4 tunnel must be unique.
- Assign a 6to4 address to the interface that connects a border router to a 6to4 network and an IPv4 address to the interface that

Previous

Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the IPv4/IPv6 dual stack on the routers.
2. Configure a 6to4 tunnel on the routers.
3. Configure static routes on the routers.

Data Preparation

To complete the configuration, you need the following data:

- IPv4 and IPv6 addresses of the interfaces
- Source IP address of the tunnel interface
- Static route to the indirectly connected router

Procedure

1. Configure IP addresses for interfaces on DeviceA and DeviceB.

   # Configure DeviceA.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceA
   [*HUAWEI] commit
   [~DeviceA] interface GigabitEthernet 1/0/0
   [~DeviceA-GigabitEthernet1/0/0] ip address 1.1.1.1 255.0.0.0
   [*DeviceA-GigabitEthernet1/0/0] undo shutdown
   [*DeviceA-GigabitEthernet1/0/0] quit
   [*DeviceA] interface gigabitethernet 1/0/1
   [*DeviceA-GigabitEthernet1/0/1] ipv6 enable
   [*DeviceA-GigabitEthernet1/0/1] ipv6 address 2002:101:101:1::1 64
   [*DeviceA-GigabitEthernet1/0/1] undo shutdown
   [*DeviceA-GigabitEthernet1/0/1] quit
   ```

   # Configure DeviceB.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceB
   [*HUAWEI] commit
   [~DeviceB] interface GigabitEthernet 1/0/0
   [~DeviceB-GigabitEthernet1/0/0] ip address 2.2.2.2 255.0.0.0
   [*DeviceB-GigabitEthernet1/0/0] undo shutdown
   [*DeviceB-GigabitEthernet1/0/0] quit
   [*DeviceB] interface gigabitethernet 1/0/1
   [*DeviceB-GigabitEthernet1/0/1] ipv6 enable
   [*DeviceB-GigabitEthernet1/0/1] ipv6 address 2001:db8::1 64
   [*DeviceB-GigabitEthernet1/0/1] undo shutdown
   [*DeviceB-GigabitEthernet1/0/1] quit
   ```

2. # Configure a 6to4 tunnel on DeviceA and DeviceB.

   # Configure DeviceA.

   ```
   [*DeviceA] interface Tunnel 10
   [*DeviceA-Tunnel10] tunnel-protocol ipv6-ipv4 6to4
   [*DeviceA-Tunnel10] ipv6 enable
   [*DeviceA-Tunnel10] ipv6 address 2002:101:101::1 64
   [*DeviceA-Tunnel10] source 1.1.1.1
   ```

Previous

```
[*DeviceB-Tunnel10] tunnel-protocol ipv6-ipv4 6to4
[*DeviceB-Tunnel10] ipv6 enable
[*DeviceB-Tunnel10] ipv6 address 2002:202:202::1 64
[*DeviceB-Tunnel10] source 2.2.2.2
[*DeviceB-Tunnel10] quit
```

3. Configure routes on DeviceA and DeviceB.

   # Configure a static route to 2002::/16 on DeviceA.

   ```
   [*DeviceA] ipv6 route-static 2002:: 16 Tunnel 10
   ```

   # Configure a default route to the IPv6 network on DeviceA.

   ```
   [*DeviceA] ipv6 route-static :: 0 2002:202:202::1
   [*DeviceA] commit
   ```

   # Configure a static route to 2002::/16 on DeviceB.

   ```
   [*DeviceB] ipv6 route-static 2002:: 16 Tunnel 10
   [*DeviceB] commit
   ```

4. Verify the configuration.

   # Ping the IPv6 address of GE 1/0/1 on DeviceB from DeviceA. The command output shows the ping is successful.

   ```
   [~DeviceA] ping ipv6 2001:db8::1
     PING 2001:db8::1 : 56  data bytes, press CTRL_C to break
       Reply from 2001:db8::1
       bytes=56 Sequence=1 hop limit=64 time=10 ms
       Reply from 2001:db8::1
       bytes=56 Sequence=2 hop limit=64 time=2 ms
       Reply from 2001:db8::1
       bytes=56 Sequence=3 hop limit=64 time=2 ms
       Reply from 2001:db8::1
       bytes=56 Sequence=4 hop limit=64 time=2 ms
       Reply from 2001:db8::1
       bytes=56 Sequence=5 hop limit=64 time=2 ms

     --- 2001:db8::1 ping statistics ---
       5 packet(s) transmitted
       5 packet(s) received
       0.00% packet loss
   round-trip min/avg/max = 5/14/29 ms
   ```

Configuration Files

- DeviceA configuration file

```
#
sysname DeviceA
#
admin
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 1.1.1.1 255.0.0.0
#
interface GigabitEthernet1/0/1
 undo shutdown
 ipv6 enable
 ipv6 address 2002:101:101:1::1/64
#
i
```

Previous

421

```
 source 1.1.1.1
#
ipv6 route-static :: 0 2002:202:202::1
#
ipv6 route-static 2002:: 16 Tunnel 10
#
return
```

- DeviceB configuration file

```
#
sysname DeviceB
#
admin
interface GigabitEthernet1/0/0
 undo shutdown
 ip address 2.2.2.2 255.0.0.0
#
interface GigabitEthernet1/0/1
 undo shutdown
 ipv6 enable
 ipv6 address 2001:db8::1/64
#
interface Tunnel 10
 ipv6 enable
 ipv6 address 2002:202:202::1/64
 tunnel-protocol ipv6-ipv4 6to4
 source 2.2.2.2
#
ipv6 route-static 2002:: 16 Tunnel 10
#
return
```

Example for Configuring a 6RD Tunnel

This section provides an example for configuring a 6RD tunnel to allow the clients or devices in different 6RD domains to communicate.

Networking Requirements

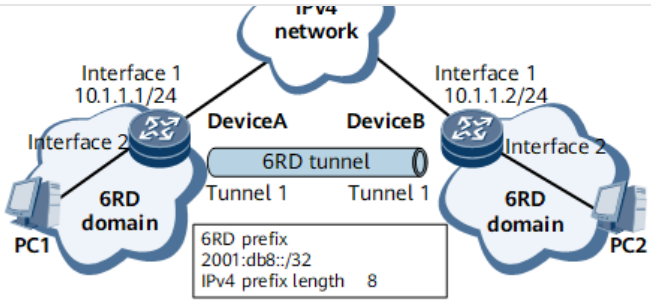
As shown in Figure 1-1997, both DeviceA and DeviceB support the IPv4/IPv6 dual stack, and they are connected to an IPv6 network and an IPv4 network. Both DeviceA and DeviceB are 6RD CEs. The IPv6 networks are 6RD networks. A 6RD tunnel needs to be established between DeviceA and DeviceB so that the hosts on the two IPv6 networks can communicate.

Figure 1-1997 Networking diagram for configuring a 6RD tunnel to allow the clients and devices in different 6RD domains to communicate

NOTE

Interfaces 1 and 2 in this example represent GE 1/0/1 and GE 1/0/2, respectively.

Previous



Configuration Roadmap

The configuration roadmap is as follows:

1. On DeviceA and DeviceB, configure IPv4 addresses for the physical interfaces connected to the IPv4 network and enable IPv6 packet forwarding.
2. On DeviceA and DeviceB, configure the source IPv4 address, 6RD prefix, IPv6 prefix length, and IPv4 prefix length for a 6RD tunnel so that the devices can calculate the 6RD delegated prefix based on a combination of these parameters.
3. On DeviceA and DeviceB, configure IPv6 addresses for the physical interfaces connected to the 6RD domains based on the 6RD delegated prefix.
4. Configure the IPv6 addresses on PC1 and PC2, with the IPv6 prefix set to a 64-bit address prefix that contains the 6RD prefix and subnet ID.
5. On DeviceA, configure a static route destined for the 6RD domain in which DeviceB resides. On DeviceB, configure a static route destined for the 6RD domain in which DeviceA resides.

Data Preparation

To complete the configuration, you need the following data:

- IPv4 addresses of interfaces
- Source IPv4 addresses of 6RD tunnel interfaces
- 6RD prefix of the 6RD tunnel
- IPv4 prefix length of the 6RD tunnel

Procedure

1. Configure IPv4 addresses for interfaces that connect devices to the IPv4 network.

   # Configure DeviceA.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceA
   [*HUAWEI] commit
   [~DeviceA] interface gigabitethernet 1/0/1
   [*DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
   [*DeviceA-GigabitEthernet1/0/1] commit
   [~DeviceA-GigabitEthernet1/0/1] quit
   ```

   # Configure DeviceB.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceB
   [*HUAWEI] commit
   [~DeviceB] interface gigabitethernet 1/0/1
   [*DeviceB-GigabitEthernet1/0/1] ip address 10.1.1.2 24
   [*DeviceB-GigabitEthernet1/0/1] commit
   [~DeviceB-GigabitEthernet1/0/1] quit
   ```

2. Previous

```
[*DeviceA-Tunnel1] tunnel-protocol ipv6-ipv4 6rd
[*DeviceA-Tunnel1] ipv6 enable
[*DeviceA-Tunnel1] source GigabitEthernet 1/0/1
[*DeviceA-Tunnel1] ipv6-prefix 2001:db8::/32
[*DeviceA-Tunnel1] ipv4-prefix length 8
[*DeviceA-Tunnel1] commit
```

Configure DeviceB.

```
[~DeviceB] interface Tunnel 1
[*DeviceB-Tunnel1] tunnel-protocol ipv6-ipv4 6rd
[*DeviceB-Tunnel1] ipv6 enable
[*DeviceB-Tunnel1] source GigabitEthernet 1/0/1
[*DeviceB-Tunnel1] ipv6-prefix 2001:db8::/32
[*DeviceB-Tunnel1] ipv4-prefix length 8
[*DeviceB-Tunnel1] commit
```

NOTE

The 6RD delegated prefix can be automatically calculated based on the configured source tunnel IPv4 address or source interface name, 6RD prefix, IPv6 prefix length, and IPv4 prefix length. You can run the **display this interface** command to view the 6RD delegated prefix and then configure an IPv6 address for the tunnel interface.

In this example, the IPv4 prefix length of the 6RD tunnel is set to 8 bits. To generate a 56-bit 6RD delegated prefix, the device removes the left-most 8 bits from the tunnel source address (IPv4 address of GE **1/0/1**) and adds the 6RD prefix 2001:db8::/32 before the remaining 24 bits (in hexadecimal notation) of the tunnel source address.

3. Query the calculated 6RD delegated prefix.

   # Query the calculated 6RD delegated prefix on DeviceA.

```
[~DeviceA-Tunnel1] display this interface
Tunnel1 current state : UP (ifindex: 9)
Line protocol current state : DOWN
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.1.1.1, destination unknown
Tunnel protocol/transport IPv6 over IPv4 (6rd)
ipv6 prefix 2001:DB8::/32
ipv4 prefix length 8
6RD Operational, Delegated Prefix is 2001:DB8:101:100::/56
Current system time: 2017-09-02 10:14:49
  300 seconds input rate 0 bits/sec, 0 packets/sec
  300 seconds output rate 0 bits/sec, 0 packets/sec
  0 seconds input rate 0 bits/sec, 0 packets/sec
  0 seconds output rate 0 bits/sec, 0 packets/sec
  0 packets input,  0 bytes
  0 input error
  0 packets output,  0 bytes
  0 output error
  Input:
    Unicast: 0 packets, Multicast: 0 packets
  Output:
    Unicast: 0 packets, Multicast: 0 packets
    Last 300 seconds input utility rate:  --
    Last 300 seconds output utility rate: --
# Query the calculated 6RD delegated prefix on DeviceB.
```

Previous

```
Line protocol current state : DOWN
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.1.1.2, destination unknown
Tunnel protocol/transport IPv6 over IPv4 (6rd)
ipv6 prefix 2001:DB8::/32
ipv4 prefix length 8
6RD Operational, Delegated Prefix is 2001:db8:101:200::/56
Current system time: 2017-09-02 10:22:13
  300 seconds input rate 0 bits/sec, 0 packets/sec
  300 seconds output rate 0 bits/sec, 0 packets/sec
  0 seconds input rate 0 bits/sec, 0 packets/sec
  0 seconds output rate 0 bits/sec, 0 packets/sec
  0 packets input,  0 bytes
  0 input error
  0 packets output,  0 bytes
  0 output error
  Input:
    Unicast: 0 packets, Multicast: 0 packets
  Output:
    Unicast: 0 packets, Multicast: 0 packets
    Last 300 seconds input utility rate:  --
    Last 300 seconds output utility rate: --
```

4. Configure IPv6 addresses for the tunnel interfaces based on the 6RD delegated prefix.

   # Configure DeviceA.

   ```
   [~DeviceA-Tunnel1] ipv6 address 2001:db8:101:100::1 56
   [*DeviceA-Tunnel1] commit
   [~DeviceA-Tunnel1] quit
   ```

   # Configure DeviceB.

   ```
   [~DeviceB-Tunnel1] ipv6 address 2001:db8:101:200::1 56
   [*DeviceB-Tunnel1] commit
   [~DeviceB-Tunnel1] quit
   ```

5. Configure an IPv6 address for GE 1/0/2.

   # Configure DeviceA.

   ```
   [~DeviceA] interface gigabitethernet 1/0/2
   [*DeviceA-GigabitEthernet1/0/2] ipv6 enable
   [*DeviceA-GigabitEthernet1/0/2] ipv6 address 2001:db8:101:101::1 64
   [*DeviceA-GigabitEthernet1/0/2] commit
   [~DeviceA-GigabitEthernet1/0/2] quit
   ```

   # Configure DeviceB.

   ```
   [~DeviceB] interface gigabitethernet 1/0/2
   [*DeviceB-GigabitEthernet1/0/2] ipv6 enable
   [*DeviceB-GigabitEthernet1/0/2] ipv6 address 2001:db8:101:201::1 64
   [*DeviceB-GigabitEthernet1/0/2] commit
   [~DeviceB-GigabitEthernet1/0/2] quit
   ```

6. Configure static routes destined for the 6RD domains connected to DeviceA and DeviceB.

   # Configure a static route destined for the 6RD domain connected to DeviceB.

   ```
   [~DeviceA] ipv6 route-static 2001:db8:: 32 Tunnel 1
   [*DeviceA] commit
   ```

   # Configure a static route destined for the 6RD domain connected to DeviceA.

Previous

NOTE

The leftmost 56 bits of the IPv6 address of GE **1/0/2** must be the same as the 6RD delegated prefix.

7. Configure IPv6 addresses for PC1 and PC2.

   # Configure PC1.

   Configure the IPv6 address 2001:db8:101:101::2/64 for PC1 based on the 6RD delegated prefix. This IPv6 address must be on the same network segment as that of GE 1/0/2 on DeviceA. Configure a static route from PC1 to DeviceA and set the destination address to 2001:db8:: 32. The method of configuring the IPv6 address and static route is related to the operating system running on PC1. The configuration details are not provided.

   # Configure PC2.

   Configure the IPv6 address 2001:db8:101:201::2/64 for PC2 based on the 6RD delegated prefix. This IPv6 address must be on the same network segment as that of GE 1/0/2 on DeviceB. Configure a static route from PC2 to DeviceB and set the destination address to 2001:db8:: 32. The method of configuring the IPv6 address and static route is related to the operating system running on PC2. The configuration details are not provided.

8. Verify the configuration.

   # After completing the configurations, run the **display interface Tunnel 1** command to check the status of Tunnel1 on DeviceA or DeviceB. The following command output shows that the status of Tunnel 1 is **UP**.

```
[~DeviceA] display interface Tunnel 1
Tunnel1 current state : UP (ifindex: 78)
Line protocol current state : DOWN
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 2.1.1.1, destination unknown
Tunnel protocol/transport IPv6 over IPv4 (6rd)
ipv6 prefix 2001:DB8::/32
ipv4 prefix length 8
6RD Operational, Delegated Prefix is 2001:db8:101:100::/56
Current system time: 2020-12-21 01:41:03
  300 seconds input rate 0 bits/sec, 0 packets/sec
  300 seconds output rate 0 bits/sec, 0 packets/sec
  0 seconds input rate 0 bits/sec, 0 packets/sec
  0 seconds output rate 0 bits/sec, 0 packets/sec
  0 packets input,  0 bytes
  0 input error
  0 packets output,  0 bytes
  0 output error
  Input:
    Unicast: 0 packets, Multicast: 0 packets
  Output:
    Unicast: 0 packets, Multicast: 0 packets
    Last 300 seconds input utility rate:  --
    Last 300 seconds output utility rate: --
```

   # On Device A, ping the IPv6 address of GE 1/0/2 on Device B. The following command output shows that the ping is successful.

```
[~DeviceA] ping ipv6 2001:db8:101:201::1
  PING 2001:db8:101:201::1 : 56  data bytes, press CTRL_C to break
    Reply from 2001:db8:101:201::1
    bytes=56 Sequence=1 hop limit=64  time = 4 ms
    Reply from 2001:db8:101:201::1
    bytes=56 Sequence=2 hop limit=64  time = 3 ms
    Reply from 2001:db8:101:201::1
    bytes=56 Sequence=3 hop limit=64  time = 2 ms
```

Previous

```
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 2/2/4 ms
```

On PC1, ping the IPv6 address of PC2. The following command output shows that the ping is successful.

```
C:\> ping 2001:db8:101:201::2
Pinging 2001:db8:101:201::2 with 32 bytes of data:
Reply from 2001:db8:101:201::2: time<1ms
Reply from 2001:db8:101:201::2: time<1ms
Reply from 2001:db8:101:201::2: time<1ms
Reply from 2001:db8:101:201::2: time<1ms
Ping statistics for 2001:db8:101:201::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Configuration Files

DeviceA configuration file

```
#
sysname DeviceA
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 undo shutdown
 ipv6 enable
 ipv6 address 2001:db8:101:101::1 64
#
interface Tunnel 1
 ipv6 enable
 ipv6 address 2001:db8:101:100::1 56
 tunnel-protocol ipv6-ipv4 6rd
 source GigabitEthernet1/0/1
 ipv6-prefix 2001:db8::/32
 ipv4-prefix length 8
#
ipv6 route-static 2001:db8:: 32 Tunnel1
#
return
```

Device B configuration file

```
#
sysname DeviceB
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.1.2 255.255.255.0
#
interface GigabitEthernet1/0/2
 undo shutdown
 ipv6 enable
 ipv6 address 2001:db8:101:201::1 64
#
interface Tunnel 1
 ip
 ip
```

Previous

```
 ipv4-prefix length 8
#
ipv6 route-static 2001:db8:: 32 Tunnel1
#
return
```

Example for Configuring a 6RD Relay

This section provides an example for configuring a 6RD relay to allow the hosts or devices on an isolated IPv6 network and in a 6RD domain to communicate with each other.

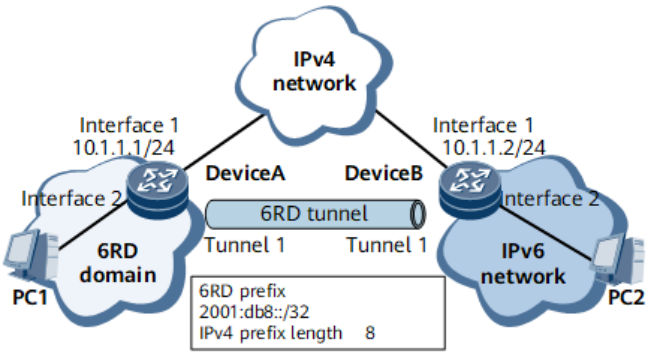
Networking Requirements

As shown in Figure 1-1998, both DeviceA and DeviceB support the IPv4/IPv6 dual stack and are connected to an IPv6 network and an IPv4 network. DeviceA functions as a 6RD CE and is connected to an IPv6 6RD network. DeviceB functions as a 6RD BR and is connected to a common IPv6 network outside the 6RD domain. A 6RD tunnel needs to be established between DeviceA and DeviceB so that the hosts on the two IPv6 networks can communicate with one another.

Figure 1-1998 Networking diagram for configuring a 6RD tunnel to enable a 6RD domain and a common IPv6 network to communicate

NOTE

Interfaces 1 and 2 in this example represent GE 1/0/1 and GE 1/0/2, respectively.



Configuration Roadmap

The configuration roadmap is as follows:

1. On DeviceA and DeviceB, configure IPv4 addresses for the physical interfaces connected to the IPv4 network and enable IPv6 packet forwarding.
2. On DeviceA and DeviceB, configure the source IPv4 address, 6RD prefix, IPv6 prefix length, and IPv4 prefix length for a 6RD tunnel. Then calculate the 6RD delegated prefix based on a combination of these parameters.
3. On DeviceA and DeviceB, configure IPv6 addresses for the physical interfaces connected to the 6RD domain and IPv6 network based on the 6RD delegated prefix.
4. Configure the IPv6 addresses on PC1 and PC2 and set the IPv6 prefix of PC1 to a 64-bit address prefix that contains the 6RD prefix and subnet ID and the IPv6 prefix of PC2 to a common IPv6 address prefix.
5. On DeviceA, configure a static route destined for the IPv6 network on which DeviceB resides. On DeviceB, configure a static route destined for the 6RD domain in which DeviceA resides.

Data Preparation

To complete the configuration, you need the following data:

- IPv4 addresses of interfaces
- S

Previous

Procedure

1. Configure IPv4 addresses for interfaces that connect devices to the IPv4 network.

   # Configure DeviceA.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceA
   [*HUAWEI] commit
   [~DeviceA] interface gigabitethernet 1/0/1
   [*DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
   [*DeviceA-GigabitEthernet1/0/1] commit
   [~DeviceA-GigabitEthernet1/0/1] quit
   ```

   # Configure DeviceB.

   ```
   <HUAWEI> system-view
   [~HUAWEI] sysname DeviceB
   [*HUAWEI] commit
   [~DeviceB] interface gigabitethernet 1/0/1
   [*DeviceB-GigabitEthernet1/0/1] ip address 10.1.1.2 24
   [*DeviceB-GigabitEthernet1/0/1] commit
   [~DeviceB-GigabitEthernet1/0/1] quit
   ```

2. Configure a 6RD tunnel.

   # Configure DeviceA.

   ```
   [~DeviceA] interface Tunnel 1
   [*DeviceA-Tunnel1] tunnel-protocol ipv6-ipv4 6rd
   [*DeviceA-Tunnel1] ipv6 enable
   [*DeviceA-Tunnel1] source GigabitEthernet 1/0/1
   [*DeviceA-Tunnel1] ipv6-prefix 2001:db8::/32
   [*DeviceA-Tunnel1] ipv4-prefix length 8
   [*DeviceA-Tunnel1] border-relay address 10.1.1.2
   [*DeviceA-Tunnel1] commit
   ```

   # Configure DeviceB.

   ```
   [~DeviceB] interface Tunnel 1
   [*DeviceB-Tunnel1] tunnel-protocol ipv6-ipv4 6rd
   [*DeviceB-Tunnel1] ipv6 enable
   [*DeviceB-Tunnel1] source GigabitEthernet 1/0/1
   [*DeviceB-Tunnel1] ipv6-prefix 2001:db8::/32
   [*DeviceB-Tunnel1] ipv4-prefix length 8
   [*DeviceB-Tunnel1] commit
   ```

   NOTE

   The 6RD delegated prefix can be automatically calculated based on the configured source tunnel address or source interface, 6RD prefix, IPv6 prefix length, and IPv4 prefix length. You can run the **display this interface** command to view the 6RD delegated prefix and then configure an IPv6 address for the tunnel interface.

3. Query the calculated 6RD delegated prefix.

   # Display the calculated 6RD delegated prefix on DeviceA.

   ```
   [~DeviceA-Tunnel1] display this interface
   Tunnel1 current state : UP (ifindex: 9)
   ```

Previous

```
Tunnel source 10.1.1.1, destination unknown
Tunnel protocol/transport IPv6 over IPv4 (6rd)
ipv6 prefix 2001:DB8::/32
ipv4 prefix length 8
6RD Operational, Delegated Prefix is 2001:DB8:101:100::/56
Current system time: 2017-09-02 10:14:49
  300 seconds input rate 0 bits/sec, 0 packets/sec
  300 seconds output rate 0 bits/sec, 0 packets/sec
  0 seconds input rate 0 bits/sec, 0 packets/sec
  0 seconds output rate 0 bits/sec, 0 packets/sec
  0 packets input,  0 bytes
  0 input error
  0 packets output,  0 bytes
  0 output error
  Input:
    Unicast: 0 packets, Multicast: 0 packets
  Output:
    Unicast: 0 packets, Multicast: 0 packets
    Last 300 seconds input utility rate:  --
    Last 300 seconds output utility rate: --
```

Display the calculated 6RD delegated prefix on DeviceB.

```
[DeviceB-Tunnel1] display this interface
Tunnel1 current state : UP (ifindex: 10)
Line protocol current state : DOWN
Description:
Route Port,The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Encapsulation is TUNNEL, loopback not set
Tunnel source 10.1.1.2, destination unknown
Tunnel protocol/transport IPv6 over IPv4 (6rd)
ipv6 prefix 2001:DB8::/32
ipv4 prefix length 8
6RD Operational, Delegated Prefix is 2001:db8:101:200::/56
Current system time: 2017-09-02 10:22:13
  300 seconds input rate 0 bits/sec, 0 packets/sec
  300 seconds output rate 0 bits/sec, 0 packets/sec
  0 seconds input rate 0 bits/sec, 0 packets/sec
  0 seconds output rate 0 bits/sec, 0 packets/sec
  0 packets input,  0 bytes
  0 input error
  0 packets output,  0 bytes
  0 output error
  Input:
    Unicast: 0 packets, Multicast: 0 packets
  Output:
    Unicast: 0 packets, Multicast: 0 packets
    Last 300 seconds input utility rate:  --
    Last 300 seconds output utility rate: --
```

4. Configure IPv6 addresses for the tunnel interfaces based on the 6RD delegated prefix.

   # Configure DeviceA.

   ```
   [~DeviceA-Tunnel1] ipv6 address 2001:db8:101:100::1 56
   [*DeviceA-Tunnel1] commit
   [~DeviceA-Tunnel1] quit
   ```

   # Configure DeviceB.

   ```
   [~DeviceB-Tunnel1] ipv6 address 2001:db8:101:200::1 56
   ```

Previous

Configure DeviceA.

```
[~DeviceA] interface gigabitethernet 1/0/2
[*DeviceA-GigabitEthernet1/0/2] ipv6 enable
[*DeviceA-GigabitEthernet1/0/2] ipv6 address 2001:db8:101:101::1 64
[*DeviceA-GigabitEthernet1/0/2] commit
[~DeviceA-GigabitEthernet1/0/2] quit
```

Configure DeviceB.

```
[~DeviceB] interface gigabitethernet 1/0/2
[*DeviceB-GigabitEthernet1/0/2] ipv6 enable
[*DeviceB-GigabitEthernet1/0/2] ipv6 address 2001:db8::1 64
[*DeviceB-GigabitEthernet1/0/2] commit
[~DeviceB-GigabitEthernet1/0/2] quit
```

6. Configure static routes.

   # Configure a static route destined for the IPv6 network connected to DeviceB.

   ```
   [~DeviceA] ipv6 route-static 2001:db8:: 32 Tunnel 1
   [*DeviceA] commit
   ```

   # Configure a static route destined for the 6RD domain connected to DeviceA.

   ```
   [~DeviceB] ipv6 route-static 2001:db8:: 32 Tunnel 1
   [*DeviceB] commit
   ```

7. Configure IPv6 addresses for PC1 and PC2.

   # Configure PC1.

   Configure the IPv6 address 2001:db8:101:101::2/64 for PC1 based on the 6RD delegated prefix. The PC1's IPv6 address must be on the same network segment as GE 1/0/2 of DeviceA. Configure a static route from PC1 to DeviceA and set the destination address to 2001:db8:: 32. The method of configuring the IPv6 address and static route is related to the operating system running on PC1. The configuration details are not provided.

   # Configure PC2.

   Configure the IPv6 address 2002:db8::2/64 for PC2 based on the 6RD delegated prefix. The PC2's IPv6 address must be on the same network segment as GE 1/0/2 of DeviceB. Configure a static route 2001:db8:: 32 from PC2 to DeviceB. The method of configuring the IPv6 address and static route is related to the operating system running on PC2. The configuration details are not provided.

8. Verify the configuration.

   # After completing the configuration, check the IPv6 status of Tunnel 1 on DeviceA or DeviceB. The following command output shows that the IPv6 status of Tunnel 1 is **UP**.

   ```
   [~DeviceA] display ipv6 interface Tunnel 1
   Tunnel1 current state : UP
   IPv6 protocol current state : UP
   IPv6 is enabled, link-local address is FE80::3ABA:9A00:9DC:D303
     Global unicast address(es):
       2001:DB8:101:100::1, subnet is 2001:DB8:101:100::/56
     Joined group address(es):
       FF02::1:FF00:1
       FF02::1:FFDC:D303
       FF02::2
       FF02::1
     MTU is 1500 bytes
     ND DAD is enabled, number of DAD attempts: 1
     ND reachable time is 1200000 milliseconds
     ND retransmit interval is 1000 milliseconds
     Hosts use stateless autoconfig for addresses
   ```

   # On DeviceA, ping the IPv6 address of GE 1/0/2 on DeviceB. The following command output shows that the ping is successful.

   ```
   [~DeviceA] ping ipv6 2001:db8::1
   ```

Previous

```
      Reply from 2001:db8::1
      bytes=56 Sequence=2 hop limit=64  time = 3 ms
      Reply from 2001:db8::1
      bytes=56 Sequence=3 hop limit=64  time = 2 ms
      Reply from 2001:db8::1
      bytes=56 Sequence=4 hop limit=64  time = 2 ms
      Reply from 2001:db8::1
      bytes=56 Sequence=5 hop limit=64  time = 2 ms
    --- 2001:db8::1 ping statistics ---
      5 packet(s) transmitted
      5 packet(s) received
      0.00% packet loss
      round-trip min/avg/max = 2/2/4 ms
```

On PC1, ping the IPv6 address of PC2. The following command output shows that the ping is successful.

```
C:\> ping 2001:db8::2
Pinging 2001:db8::2 with 32 bytes of data:
Reply from 2001:db8::2: time<1ms
Reply from 2001:db8::2: time<1ms
Reply from 2001:db8::2: time<1ms
Reply from 2001:db8::2: time<1ms
Ping statistics for 2001:db8::2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Configuration Files

DeviceA configuration file

```
#
sysname DeviceA
#
interface GigabitEthernet1/0/1
 undo shutdown
 ip address 10.1.1.1 255.255.255.0
#
interface GigabitEthernet1/0/2
 undo shutdown
 ipv6 enable
 ipv6 address 2001:db8:101:101::1 64
#
interface Tunnel 1
 ipv6 enable
 ipv6 address 2001:db8:101:100::1 56
 tunnel-protocol ipv6-ipv4 6rd
 source GigabitEthernet1/0/1
 ipv6-prefix 2001:db8::/32
 ipv4-prefix length 8
 border-relay address 10.1.1.2
#
ipv6 route-static 2001:db8:: 32 Tunnel1
#
return
```

DeviceB configuration file

```
#
sysname DeviceB
#
int
 un
```

Previous

HUAWEI

How to Buy

Partner

Resources

Quick Links

Huawei e+ App

HUAWEI eKit App

Huawei HiKnow APP

HUAWEI eFly App

Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

Privacy Terms of use Cookies Cookie Settings Report content

Previous

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

IPv6 IPv4 Tunnel

Guía de configuración del NE40E V800R022C00SPC600

Buscar este documento. 0 / 500

Por favor evalúa y deja tus comentarios:

Configuración del túnel IPv6 sobre IPv4

La tecnología de tunelización de IPv6 sobre IPv4 proporciona una solución para la transición de IPv4 a IPv6.

Descripción general del túnel IPv6 sobre IPv4

Precauciones de configuración para el túnel IPv6 sobre IPv4

Configuración de un túnel manual IPv6 sobre IPv4

Configuración de un túnel 6to4

Configuración de un túnel 6RD

Ejemplos de configuración para el túnel IPv6 sobre IPv4

- Ejemplo de configuración de un túnel manual IPv6 sobre IPv4
- Ejemplo de configuración de un túnel 6to4
- Ejemplo de configuración del relé 6to4
- Ejemplo de configuración de un túnel 6RD
- Ejemplo de configuración de un relé 6RD

Descripción general del túnel IPv6 sobre IPv4

La tecnología de túnel IPv6 sobre IPv4 permite la comunicación entre redes IPv6 aisladas a través de redes IPv4 existentes. Los paquetes IPv6 pueden transmitirse de forma transparente a través de redes IPv4 tras encapsularse en paquetes IPv4.

Durante la transición inicial de redes IPv4 a IPv6, estas se desplegaron ampliamente, mientras que las redes IPv6 eran islas aisladas dispersas por todo el mundo. Con la tecnología de tunelización, se pueden crear túneles IPv6 sobre IPv4 en las redes IPv4 para conectar los sitios IPv6 aislados. Para establecer túneles IPv6 sobre IPv4, se debe habilitar la doble pila IPv4/IPv6 en los enrutadores en los límites de las redes IPv4 e IPv6.

Precauciones de configuración para el túnel IPv6 sobre IPv4

Requisitos de las funciones

Tabla 1-659 Requisitos de funciones

Requisitos de las funciones	Serie	Modelos
La interfaz, la dirección de origen y la dirección de destino de un túnel IPv6 sobre IPv4 no admiten L3VPN.	NE40E	NE40E

Anterior

Las rutas IPv4 utilizadas por IPv6 sobre túneles IPv4 y túneles 6to4 solo se pueden usar para reenvío de IP.	NE40E	NE40E
Los túneles 6to4, 6sobre4 y 6rd con la misma dirección de origen no se pueden controlar por separado. Si uno de ellos está configurado, los otros dos tipos de túneles pueden reenviar paquetes con normalidad.	NE40E	NE40E
Tras cambiar la dirección IP de origen del túnel 6to4, el tráfico desde la dirección 6to4 original aún puede reenviarse. Tras la suavización, el tráfico se interrumpe.	NE40E	NE40E

Configuración de un túnel manual IPv6 sobre IPv4

Un túnel manual IPv6 sobre IPv4 es un túnel P2P. Tanto la dirección de origen como la de destino de un túnel manual IPv6 sobre IPv4 se asignan manualmente y deben ser únicas en el mismo dispositivo. Un túnel manual IPv6 sobre IPv4 actúa como un enlace permanente que conecta dos redes IPv6 a través de una red IPv4. Los enrutadores de borde pueden comunicarse entre sí de forma segura y regular mediante túneles manuales IPv6 sobre IPv4.

Escenario de uso

Para permitir que las redes IPv6 se comuniquen entre sí a través de una red IPv4, configure IPv6 sobre túneles IPv4 en los enrutadores donde las redes IPv6 bordean una red IPv4.

Se puede establecer un túnel manual IPv6 sobre IPv4 entre dos enrutadores de borde para proporcionar una conexión estable a redes IPv6 separadas. También se puede establecer entre un sistema terminal y un enrutador de borde para que el sistema terminal acceda a una red IPv6. Los dispositivos en ambos extremos de un túnel IPv6 sobre IPv4 deben ser compatibles con la doble pila IPv4/IPv6. Los dispositivos intermedios no necesitan ser compatibles con la doble pila IPv4/IPv6. Se pueden configurar varios túneles manuales IPv6 sobre IPv4 en el enrutador de borde para comunicarse con varias redes IPv6.

Tareas de preconfiguración

Antes de configurar un túnel manual IPv6 sobre IPv4, complete las siguientes tareas:

- Conecte interfaces y configure parámetros físicos para las interfaces para garantizar que el estado físico de las interfaces sea Activo.
- Configure los parámetros del protocolo de capa de enlace para las interfaces para garantizar que el estado del protocolo de capa de enlace de las interfaces sea Activo.
- Asignar una dirección IPv4 a cada enrutador de borde .
- Configurar IPv6 globalmente y en interfaces.
- Asignar una dirección IPv6 a cada enrutador de borde .

Procedimiento

1. Ejecutar **system-view**

   Se muestra la vista del sistema.

2. Ejecutar **interfaz túnel** número de interfaz

   Se crea una interfaz de túnel.

3. Ejecute **el protocolo de túnel ipv6-ipv4**

   El modo de túnel está configurado en modo de túnel manual IPv6 sobre IPv4.

4. Ejecutar **source** { dirección-ip | tipo-interfaz número-interfaz }

   Se especifica la dirección de origen o la interfaz de origen del túnel.

5. Ejecutar dirección IP **de destino**

   Se especifica la dirección de destino del túnel.

NOTE

Anterior

6. Ejecutar **ipv6 enable**

   IPv6 está configurado en la interfaz.

7. Ejecutar **dirección ipv6** { dirección-ipv6 longitud-prefijo | dirección-ipv6/longitud-prefijo }

   Se configura una dirección IPv6 para la interfaz del túnel.

8. Ejecutar **confirmación**

   La configuración está confirmada.

Verificación de las configuraciones

Después de configurar un túnel manual IPv6 sobre IPv4, verifique las configuraciones.

- Ejecute el comando **display ipv6 interface tunnel** interface-number para verificar la configuración IPv6 de una interfaz de túnel.

Configuración de un túnel 6to4

Un túnel 6to4 puede interconectar redes IPv6 aisladas a través de una red IPv4.

Escenario de uso

Para permitir que las redes IPv6 se comuniquen entre sí a través de una red IPv4, configure IPv6 sobre túneles IPv4 en los enrutadores donde las redes IPv6 bordean la red IPv4.

Los túneles 6to4 utilizan direcciones 6to4 especiales con el formato 2002:abcd::/48, donde abcd representa la dirección de origen de la interfaz del túnel. Durante la comunicación, la dirección IPv4 de una dirección 6to4 se utiliza para encapsular los paquetes. No es necesario configurar el túnel 6to4 con una dirección de destino.

Tareas de preconfiguración

Antes de configurar un túnel 6to4, complete las siguientes tareas:

- Conecte interfaces y configure parámetros físicos para las interfaces para garantizar que el estado físico de las interfaces sea Activo.
- Configure los parámetros del protocolo de capa de enlace para las interfaces para garantizar que el estado del protocolo de capa de enlace de las interfaces sea Activo.
- Configurar la pila dual IPv4/IPv6.

Procedimiento

1. Ejecutar **system-view**

   Se muestra la vista del sistema.

2. Ejecutar **interfaz túnel** número de interfaz

   Se crea una interfaz de túnel.

3. Ejecute **el protocolo de túnel ipv6-ipv4 6to4**

   El modo de túnel está establecido en modo de túnel 6to4.

4. Ejecutar **source** { dirección-ip | tipo-interfaz número-interfaz }

   Se especifica la dirección de origen o la interfaz de origen del túnel.

5. Ejecutar **ipv6 enable**

   IPv6 está configurado en la interfaz.

6. Ejecutar **dirección ipv6** { dirección-ipv6 longitud-prefijo | i dirección-ipv6 máscara }

   Se configura una dirección IPv6 para la interfaz del túnel.

NOTE

Anterior

7. Ejecutar **confirmación**

   La configuración está confirmada.

Comprobación de las configuraciones

Después de configurar un túnel 6to4, verifique las configuraciones.

- Ejecute el comando **display ipv6 interface tunnel** interface-number para verificar la configuración IPv6 de una interfaz de túnel.

Configuración de un túnel 6RD

Un túnel 6RD es un túnel punto a multipunto (P2MP) que conecta sitios IPv6 a través de la red IPv4 de un operador. Los túneles 6RD se han implementado ampliamente en las redes de los operadores.

Escenario de uso

Un túnel 6RD es un túnel P2MP y es una mejora de la solución 6to4. La tunelización 6RD permite a los operadores utilizar uno de sus propios prefijos IPv6 como prefijo 6RD, mitigando la escasez de direcciones IPv4 de la solución 6to4.

6RD se utiliza en los siguientes escenarios:

- Dominio 6RD-Dominio 6RD

  Conecta diferentes dominios 6RD. Los CE 6RD se implementan en cada extremo de un túnel, lo que permite que los hosts o dispositivos en diferentes dominios 6RD se comuniquen entre sí.

- Red IPv6 de dominio 6RD

  Conecta un dominio 6RD a una red IPv6 nativa. Se implementan un CE 6RD y un BR 6RD en cada extremo de un túnel, lo que permite que los hosts o dispositivos del dominio 6RD y de la red IPv6 se accedan entre sí.

Tareas de preconfiguración

Antes de configurar un túnel 6RD, complete las siguientes tareas:

- Conecte interfaces y configure sus parámetros físicos para garantizar que el estado físico de las interfaces sea Activo.
- Configure los parámetros del protocolo de capa de enlace para que las interfaces se activen en la capa de enlace.
- Asegúrese de que haya rutas accesibles entre las interfaces de origen y destino.
- Habilitar la pila dual IPv4/IPv6 en las interfaces.

Procedimiento

1. Ejecutar **system-view**

   Se muestra la vista del sistema.

2. Ejecutar **interfaz túnel** número de interfaz

   Se crea una interfaz de túnel y se muestra la vista de la interfaz de túnel.

3. Ejecute **el protocolo de túnel ipv6-ipv4 6.º**

   El modo de encapsulación del túnel está establecido en 6RD.

4. Ejecutar **source** { dirección-ip | tipo-interfaz número-interfaz }

   La dirección de origen o la interfaz de origen se especifica para la interfaz del túnel 6RD.

5. Ejecutar **ipv6-prefix** { dirección-ipv6 longitud-prefijo | i pv6-prefix-mask }

   Se configuran el prefijo 6RD y la longitud del prefijo 6RD.

   Un prefijo 6RD es el prefijo IPv6 asignado por un operador a una dirección 6RD. El prefijo delegado 6RD se calcula combinando el prefijo 6RD con parte o la totalidad de los bits de una dirección IPv4. El prefijo delegado 6RD se utiliza para asignar prefijos de direcciones IPv6 a dispositivos o hosts en un dominio 6RD.

   El prefijo 6RD para cada dominio 6RD debe ser único.

6. Anterior

dirección IPv4). Los bits restantes de la dirección IPv4 y el prefijo 6RD juntos forman el prefijo delegado 6RD.

Se recomienda establecer ipv4-prefix-length en 0 si la red del operador es IPv4. En una red IPv4, la dirección del túnel de origen está completamente integrada en el prefijo delegado 6RD, que se utiliza para buscar la dirección del túnel de destino.

La longitud del prefijo IPv4 del túnel 6RD en cada dominio 6RD debe ser única.

El prefijo delegado 6RD se puede calcular automáticamente en función de la dirección del túnel de origen o la interfaz de origen configurada, el prefijo 6RD, la longitud del prefijo IPv6 y la longitud del prefijo IPv4. Puede ejecutar el comando " **mostrar esta interfaz** " en la vista de la interfaz del túnel para comprobar el prefijo delegado 6RD calculado.

7. Ejecutar **ipv6 enable**

   IPv6 está habilitado en la interfaz.

8. Ejecutar **dirección ipv6** { dirección-ipv6 longitud-prefijo | i dirección-ipv6 máscara }

   Se configura una dirección IPv6 para la interfaz del túnel y el prefijo de la dirección es el prefijo delegado 6RD.

9. (Opcional) Ejecutar **la dirección border-relay** br-ipv4-address Se configura la dirección IPv4 del 6RD BR.

   La dirección IPv4 del BR 6RD debe configurarse en un CE 6RD solo en un escenario de retransmisión donde un dominio 6RD interactúa con una red IPv6 nativa.

Verificar la configuración.

Después de configurar el túnel 6RD, verifique las configuraciones.

Ejecute el comando **display ipv6 interface tunnel** interface-number para verificar el atributo IPv6 en la interfaz del túnel.

Ejemplos de configuración para el túnel IPv6 sobre IPv4

Esta sección proporciona ejemplos de configuración que cubren los requisitos de red, las precauciones de configuración y la hoja de ruta de configuración.

Ejemplo de configuración de un túnel manual IPv6 sobre IPv4

Esta sección proporciona un ejemplo para configurar un túnel manual de IPv6 sobre IPv4.

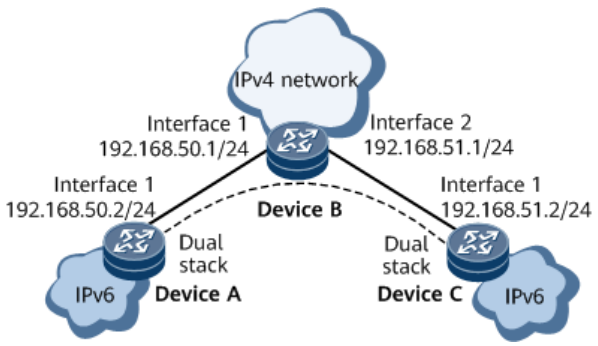
Requisitos de red

Como se muestra en la Figura 1-1994 , dos redes IPv6 están conectadas al Dispositivo B en la red troncal IPv4 a través del Dispositivo A y el Dispositivo C. Para interconectar las dos redes IPv6, configure un túnel manual IPv6 sobre IPv4 entre el Dispositivo A y el Dispositivo C.

Figura 1-1994 Diagrama de red para configurar un túnel manual IPv6 sobre IPv4

NOTE

Las interfaces 1 y 2 en este ejemplo representan GE 1/0/0 y GE 2/0/0 , respectivamente.



Precauciones

Al c

Anterior

dirección IP de destino del extremo remoto del túnel. De igual forma, la dirección IP de destino del extremo local es la dirección IP de origen del extremo remoto.

- Configure una dirección IPv6 para la interfaz del túnel para admitir protocolos de enrutamiento.

Hoja de ruta de configuración

La hoja de ruta de configuración es la siguiente:

1. Asignar una dirección IP a cada interfaz física.
2. Configure direcciones IPv6 para interfaces de túnel y direcciones IPv4 de origen y destino para el túnel involucrado.
3. Establezca el tipo de protocolo en IPv6-IPv4.

Preparación de datos

Para completar la configuración, necesitas los siguientes datos:

- Direcciones IP de interfaces
- Direcciones IPv6 de las interfaces del túnel y direcciones IPv4 de origen y destino del túnel

Procedimiento

1. Configure direcciones IPv6 para las interfaces en el dispositivo A, el dispositivo B y el dispositivo C.

   # Configurar el dispositivo A.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo A
   [ * HUAWEI ] confirmación
   [ ~ Dispositivo A] interfaz gigabitethernet 1/0/0
   [ ~ Dispositivo A-GigabitEthernet 1/0/0 ] dirección IP 192.168.50.2 255.255.255.0
   [ * Dispositivo A-GigabitEthernet 1/0/0 ] deshacer apagado
   [ * Dispositivo A-GigabitEthernet 1/0/0 ] salir
   ```

   # Configurar el dispositivo B.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo B
   [ * HUAWEI ] confirmación
   [ ~ Dispositivo B] interfaz gigabitethernet 1/0/0
   [ ~ Dispositivo B-GigabitEthernet 1/0/0 ] dirección IP 192.168.50.1 255.255.255.0
   [ * Dispositivo B-GigabitEthernet 1/0/0 ] deshacer apagado
   [ * Dispositivo B-GigabitEthernet 1/0/0 ] salir
   [ * Dispositivo B] interfaz gigabitethernet 2/0/0
   [ * Dispositivo B-GigabitEthernet 2/0/0 ] dirección IP 192.168.51.1 255.255.255.0
   [ * Dispositivo B-GigabitEthernet 2/0/0 ] deshacer apagado
   [ * Dispositivo B-GigabitEthernet 2/0/0 ] confirmación
   [ ~ Dispositivo B-GigabitEthernet 2/0/0 ] salir
   ```

   # Configurar el dispositivo C.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo C
   [ * HUAWEI ] confirmación
   [ ~ Dispositivo C] interfaz gigabitethernet 1/0/0
   [ ~ Dispositivo C-GigabitEthernet 1/0/0 ] dirección IP 192.168.51.2 255.255.255.0
   [ * Dispositivo C-GigabitEthernet 1/0/0 ] deshacer apagado
   [ * Dispositivo C-GigabitEthernet 1/0/0 ] salir
   ```

2. Cree interfaces de túnel y configure un modo de túnel, direcciones IPv6 para las interfaces de túnel y direcciones de origen y destino

Anterior

```
[ * Dispositivo A-Túnel10] protocolo de túnel ipv6-ipv4
[ * Dispositivo A-Tunnel10] Habilitar IPv6
[ * Dispositivo A-Tunnel10] dirección IPv6 2001:db8::1 64
[ * Dispositivo A-Tunnel10] fuente 192.168.50.2
[ * Dispositivo A-Túnel10] destino 192.168.51.2
[ * Dispositivo A-Tunnel10] salir
```

Configurar el dispositivo C.

```
[ * Dispositivo C] Interfaz Túnel 10
[ * Dispositivo C-Tunnel10] protocolo de túnel ipv6-ipv4
[ * Dispositivo C-Tunnel10] Habilitar IPv6
[ * Dispositivo C-Tunnel10] dirección ipv6 2001:db8::2 64
[ * Dispositivo C-Tunnel10] fuente 192.168.51.2
[ * Dispositivo C-Tunnel10] destino 192.168.50.2
[ * Dispositivo C-Tunnel10] salir
```

3. Configure rutas estáticas para garantizar que el Dispositivo A y el Dispositivo C sean accesibles.

Configurar el dispositivo A.

```
[ * Dispositivo A] ruta ip estática 192.168.51.0 255.255.255.0 192.168.50.1
[ * Dispositivo A] confirmación
```

Configurar el dispositivo C.

```
[ * Dispositivo C] ruta ip estática 192.168.50.0 255.255.255.0 192.168.51.1
[ * Dispositivo C] confirmación
```

4. Verificar la configuración.

Haga ping a la dirección IPv4 de GE 1/0/0 en el dispositivo A desde el dispositivo C. La operación de ping es exitosa.

```
[ ~ Dispositivo C] ping 192.168.50.2
  PING 192.168.50.2: 56 bytes de datos, presione CTRL_C para interrumpir
    Respuesta de 192.168.50.2: bytes=56 Secuencia=1 ttl=254 tiempo=84 ms
    Respuesta de 192.168.50.2: bytes=56 Secuencia=2 ttl=254 tiempo=27 ms
    Respuesta de 192.168.50.2: bytes=56 Secuencia=3 ttl=254 tiempo=25 ms
    Respuesta de 192.168.50.2: bytes=56 Secuencia=4 ttl=254 tiempo=3 ms
    Respuesta de 192.168.50.2: bytes=56 Secuencia=5 ttl=254 tiempo=24 ms

  --- Estadísticas de ping 192.168.50.2 ---
    5 paquete(s) transmitido(s)
    5 paquete(s) recibido(s)
    0,00% pérdida de paquetes
    viaje de ida y vuelta mín./promedio/máx. = 3/32/84 ms
```

Haga ping a la dirección IPv6 del túnel 10 en el dispositivo A desde el dispositivo C y la operación de ping será exitosa.

```
[ ~ Dispositivo C] ping ipv6 2001:db8::1
  PING 2001:db8::1 : 56 bytes de datos, presione CTRL_C para interrumpir
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=1 límite de salto=64 tiempo=28 ms
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=2 Límite de saltos=64 Tiempo=27 ms
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=3 Límite de saltos=64 Tiempo=26 ms
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=4 Límite de salto=64 Tiempo=27 ms
    Respuesta de 2001:db8::1
```

Anterior

```
    0,00% pérdida de paquetes
viaje de ida y vuelta mín./promedio/máx. = 26/26/28 ms
```

Archivos de configuración

- Archivo de configuración del dispositivo A

```
#
 sysname Dispositivo A
#
interfaz GigabitEthernet 1/0/0
 deshacer el apagado
 dirección IP 192.168.50.2 255.255.255.0
#
Interfaz Túnel 10
 Habilitar IPv6
 dirección IPv6 2001:db8::1/64
 protocolo de túnel ipv6-ipv4
 fuente 192.168.50.2
 destino 192.168.51.2
#
ruta ip estática 192.168.51.0 255.255.255.0 192.168.50.1
#
devolver
```

- Archivo de configuración del dispositivo B

```
#
 nombre del sistema Dispositivo B
#
interfaz GigabitEthernet 1/0/0
 deshacer el apagado
 dirección IP 192.168.50.1 255.255.255.0
#
interfaz GigabitEthernet 2/0/0
 deshacer el apagado
 dirección IP 192.168.51.1 255.255.255.0
#
devolver
```

- Archivo de configuración del dispositivo C

```
#
 nombre del sistema Dispositivo C
#
interfaz GigabitEthernet 1/0/0
 deshacer el apagado
 dirección IP 192.168.51.2 255.255.255.0
#
Interfaz Túnel 10
 Habilitar IPv6
 dirección IPv6 2001:db8::2/64
 protocolo de túnel ipv6-ipv4
 fuente 192.168.51.2
 destino 192.168.50.2
#
ruta ip estática 192.168.50.0 255.255.255.0 192.168.51.1
#
devolver
```

Ejemplo de configuración de un túnel 6to4

EstAnterior

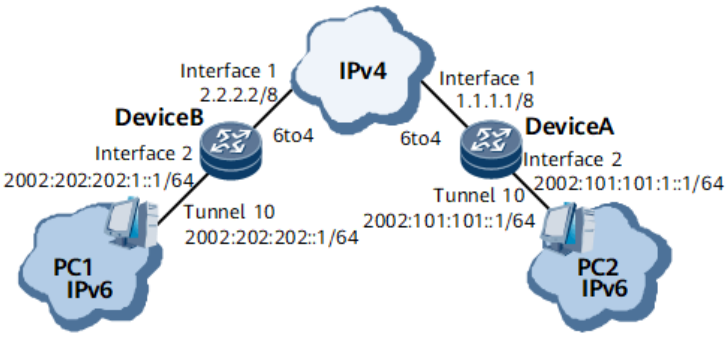
6to4 y a la red troncal IPv4. Para interconectar ambas redes 6to4, se debe configurar un túnel 6to4 entre los Dispositivos A y B.

Para permitir la interconexión de redes 6to4, se debe configurar una dirección 6to4 para el host con el prefijo **2002:Dirección IPv4:** y una longitud de prefijo de 48 bits. Como se muestra en la Figura 1-1995 , la dirección IPv4 de la interfaz que conecta el Dispositivo A con la red IPv4 es 1.1.1.1. Por lo tanto, la dirección 6to4 de la red 6to4 donde reside el Dispositivo A debe tener el prefijo 2002:101:101:: y una longitud de prefijo de 64 bits.

Figura 1-1995 Diagrama de red para configurar un túnel 6to4

NOTE

Las interfaces 1 y 2 en este ejemplo representan GE 1/0/0 y GE 1/0/1 , respectivamente.



Precauciones

Al configurar un túnel 6to4, tenga en cuenta los siguientes puntos:

- Cree una interfaz de túnel y establezca parámetros para la interfaz de túnel.
- Configure únicamente la dirección IPv4 de origen del túnel. La dirección IP de destino del túnel es la misma que la del paquete IPv6 original. La dirección IP de origen de un túnel 6to4 debe ser única.
- Asigne una dirección 6to4 a la interfaz que conecta un enrutador de borde a una red 6to4 y una dirección IPv4 a la interfaz que conecta un enrutador de borde a una red IPv4.
- Configure una dirección IP para la interfaz del túnel para admitir protocolos de enrutamiento.

Hoja de ruta de configuración

La hoja de ruta de configuración es la siguiente:

1. Configure la pila dual IPv4/IPv6 en los enrutadores .
2. Configurar un túnel 6to4 en el enrutador s.
3. Configurar rutas estáticas en los enrutadores .

Preparación de datos

Para completar la configuración, necesitas los siguientes datos:

- Direcciones IPv4 e IPv6 de las interfaces
- Dirección IP de origen de la interfaz del túnel

Procedimiento

1. Configurar direcciones IP para las interfaces en el dispositivo A y el dispositivo B.

   # Configurar el dispositivo A.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo A
   ```

Anterior

```
[ * Dispositivo A-GigabitEthernet 1/0/0 ] deshacer apagado
[ * Dispositivo A-GigabitEthernet 1/0/0 ] salir
[ * Dispositivo A] interfaz gigabitethernet 1/0/1
[ * Dispositivo A-GigabitEthernet 1/0/1 ] Habilitar IPv6
[ * Dispositivo A-GigabitEthernet 1/0/1 ] dirección IPv6 2002:101:101:1::1 64
[ * Dispositivo A-GigabitEthernet 1/0/1 ] deshacer apagado
[ * Dispositivo A-GigabitEthernet 1/0/1 ] salir
```

Configurar el dispositivo B.

```
Vista del sistema de HUAWEI
[ ~ HUAWEI ] nombre del sistema Dispositivo B
[ * HUAWEI ] confirmación
[ ~ Dispositivo B] Interfaz GigabitEthernet 1/0/0
[ ~ Dispositivo B-GigabitEthernet 1/0/0 ] dirección IP 2.2.2.2 8
[ * Dispositivo B-GigabitEthernet 1/0/0 ] deshacer apagado
[ * Dispositivo B-GigabitEthernet 1/0/0 ] salir
[ * Dispositivo B] interfaz gigabitethernet 1/0/1
[ * Dispositivo B-GigabitEthernet 1/0/1 ] Habilitar IPv6
[ * Dispositivo B-GigabitEthernet 1/0/1 ] dirección IPv6 2002:202:202:1::1 64
[ * Dispositivo B-GigabitEthernet 1/0/1 ] deshacer apagado
[ * Dispositivo B-GigabitEthernet 1/0/1 ] salir
```

2. # Configure un túnel 6to4 en el dispositivo A y el dispositivo B.

Configurar el dispositivo A.

```
Interfaz [ * Dispositivo A] Túnel 10
[ * Dispositivo A-Túnel10] protocolo de túnel ipv6-ipv4 6to4
[ * Dispositivo A-Tunnel10] Habilitar IPv6
[ * Dispositivo A-Tunnel10] dirección IPv6 2002:101:101::1 64
[ * Dispositivo A-Túnel10] fuente 1.1.1.1
[ * Dispositivo A-Tunnel10] salir
```

Configurar el dispositivo B.

```
[ * Dispositivo B] Interfaz Túnel 10
[ * Dispositivo B-Tunnel10] protocolo de túnel ipv6-ipv4 6to4
[ * Dispositivo B-Tunnel10] Habilitar IPv6
[ * Dispositivo B-Tunnel10] dirección IPv6 2002:202:202::1 64
[ * Dispositivo B-Tunnel10] fuente 2.2.2.2
[ * Dispositivo B-Tunnel10] salir
```

NOTE

Se requieren rutas disponibles entre el Dispositivo A y el Dispositivo B. En este ejemplo, ambos enrutadores están conectados directamente. Por lo tanto, no se configura ningún protocolo de enrutamiento.

---

3. # Configure una ruta a la red 6to4 en el dispositivo A y el dispositivo B.

Configurar el dispositivo A.

```
[ * Dispositivo A] ruta ipv6 estática 2002:: 16 Túnel 10
[ * Dispositivo A] confirmación
```

Configurar el dispositivo B.

```
[ * Dispositivo B] ruta ipv6 estática 2002:: 16 Túnel 10
[ * Dispositivo B] confirmación
```

4. Verificar la configuración

Anterior

```
Estado actual del protocolo IPv6: ACTIVO
La dirección del enlace local es FE80::101:101
  Direcciones de unidifusión global:
    2002:101:101::1, la subred es 2002:101:101::/64
  Direcciones del grupo al que se unió:
    FF02::1:FF01:101
    FF02::1:FF00:1
    FF02::2
    FF02::1
  La MTU es de 1500 bytes
  ND DAD está habilitado, número de intentos de DAD: 1.
  El tiempo alcanzable de ND es 1200000 milisegundos.
  El intervalo de retransmisión ND es de 1000 milisegundos.
  Los hosts utilizan una configuración automática sin estado para las direcciones.
```

Haga ping a la dirección 6to4 de GE 2/0/0 en el dispositivo B desde el dispositivo A. La salida del comando muestra que el ping es exitoso.

```
[ ~ Dispositivo A] ping ipv6 2002:202:202:1::1
  PING 2002:202:202:1::1 : 56 bytes de datos, presione CTRL_C para interrumpir
    Respuesta de 2002:202:202:1::1
    bytes=56 Secuencia=1 límite de salto=64 tiempo=37 ms
    Respuesta de 2002:202:202:1::1
    bytes=56 Secuencia=2 Límite de salto=64 Tiempo=2 ms
    Respuesta de 2002:202:202:1::1
    bytes=56 Secuencia=3 Límite de salto=64 Tiempo=8 ms
    Respuesta de 2002:202:202:1::1
    bytes=56 Secuencia=4 Límite de salto=64 Tiempo=1 ms
    Respuesta de 2002:202:202:1::1
    bytes=56 Secuencia=5 Límite de salto=64 Tiempo=2 ms

  ---2002:202:202:1::1 estadísticas de ping---
    5 paquete(s) transmitido(s)
    5 paquete(s) recibido(s)
    0,00% pérdida de paquetes
viaje de ida y vuelta mín./promedio/máx. = 4/9/25 ms
```

Archivos de configuración

- Archivo de configuración del dispositivo A

```
#
 sysname Dispositivo A
#
interfaz GigabitEthernet 1/0/0
 deshacer el apagado
 dirección IP 1.1.1.1 255.0.0.0
#
interfaz GigabitEthernet 1/0/1
 deshacer el apagado
 Habilitar IPv6
 dirección IPv6 2002:101:101:1::1/64
#
Interfaz Túnel 10
 Habilitar IPv6
 dirección IPv6 2002:101:101::1/64
```

Anterior

```
#
devolver
```

- Archivo de configuración del dispositivo B

```
#
 nombre del sistema Dispositivo B
#
interfaz GigabitEthernet 1/0/0
 deshacer el apagado
 dirección IP 2.2.2.2 255.0.0.0
#
interfaz GigabitEthernet 1/0/1
 deshacer el apagado
 Habilitar IPv6
 dirección IPv6 2002:202:202:1::1/64
#
Interfaz Túnel 10
 Habilitar IPv6
 dirección IPv6 2002:202:202::1/64
 protocolo-túnel ipv6-ipv4 6to4
 fuente 2.2.2.2
#
ruta ipv6 estática 2002:: 16 Túnel 10
#
devolver
```

Ejemplo de configuración del relé 6to4

Esta sección proporciona un ejemplo para configurar el relé 6to4.

Requisitos de red

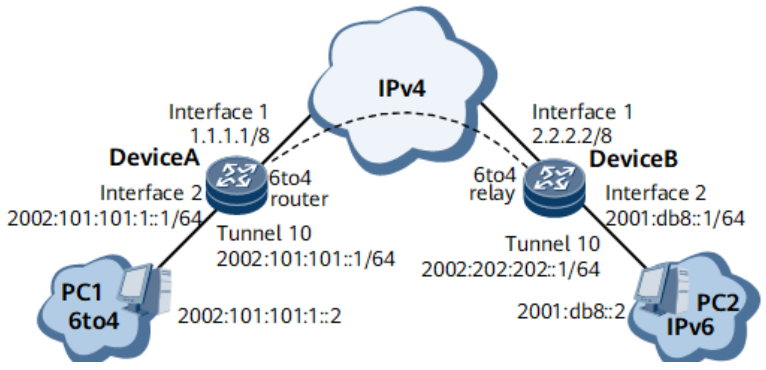
Como se muestra en la Figura 1-1996 , el Dispositivo A funciona como un enrutador 6to4 y se conecta a la red 6to4; el Dispositivo B es un enrutador de retransmisión 6to4 y se conecta a la red IPv6 (2001:db8::/64); el Dispositivo A se conecta al Dispositivo B a través de la red troncal IPv4. Para interconectar los hosts en las redes 6to4 e IPv6, se debe establecer un túnel 6to4 entre el Dispositivo A y el Dispositivo B.

El método para configurar un túnel entre un router de retransmisión 6to4 y un router 6to4 es el mismo que el método para configurar un túnel entre routers 6to4. Para interconectar una red 6to4 con una red IPv6, configure una ruta estática a la red IPv6 en cada router 6to4 .

Figura 1-1996 Diagrama de red para configurar el relé 6to4

NOTE

Las interfaces 1 y 2 en este ejemplo representan GE 1/0/0 y GE 1/0/1 , respectivamente.



Anterior

- Cree una interfaz de túnel y establezca parámetros para la interfaz de túnel.
- Configure únicamente la dirección IPv4 de origen del túnel. La dirección IPv4 de destino del túnel es la misma que la del paquete IPv6 original. La dirección de origen de un túnel 6to4 debe ser única.
- Asigne una dirección 6to4 a la interfaz que conecta un enrutador de borde a una red 6to4 y una dirección IPv4 a la interfaz que conecta un enrutador de borde a una red IPv4.
- Configure una dirección IP para la interfaz del túnel para admitir protocolos de enrutamiento.

Hoja de ruta de configuración

La hoja de ruta de configuración es la siguiente:

1. Configure la pila dual IPv4/IPv6 en los enrutadores .
2. Configurar un túnel 6to4 en el enrutador s.
3. Configurar rutas estáticas en los enrutadores .

Preparación de datos

Para completar la configuración, necesitas los siguientes datos:

- Direcciones IPv4 e IPv6 de las interfaces
- Dirección IP de origen de la interfaz del túnel
- Ruta estática al enrutador conectado indirectamente

Procedimiento

1. Configurar direcciones IP para las interfaces en el dispositivo A y el dispositivo B.

   # Configurar el dispositivo A.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo A
   [ * HUAWEI ] confirmación
   [ ~ Dispositivo A] Interfaz GigabitEthernet 1/0/0
   [ ~ Dispositivo A-GigabitEthernet 1/0/0 ] dirección IP 1.1.1.1 255.0.0.0
   [ * Dispositivo A-GigabitEthernet 1/0/0 ] deshacer apagado
   [ * Dispositivo A-GigabitEthernet 1/0/0 ] salir
   [ * Dispositivo A] interfaz gigabitethernet 1/0/1
   [ * Dispositivo A-GigabitEthernet 1/0/1 ] Habilitar IPv6
   [ * Dispositivo A-GigabitEthernet 1/0/1 ] dirección IPv6 2002:101:101:1::1 64
   [ * Dispositivo A-GigabitEthernet 1/0/1 ] deshacer apagado
   [ * Dispositivo A-GigabitEthernet 1/0/1 ] salir
   ```

   # Configurar el dispositivo B.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo B
   [ * HUAWEI ] confirmación
   [ ~ Dispositivo B] Interfaz GigabitEthernet 1/0/0
   [ ~ Dispositivo B-GigabitEthernet 1/0/0 ] dirección IP 2.2.2.2 255.0.0.0
   [ * Dispositivo B-GigabitEthernet 1/0/0 ] deshacer apagado
   [ * Dispositivo B-GigabitEthernet 1/0/0 ] salir
   [ * Dispositivo B] interfaz gigabitethernet 1/0/1
   [ * Dispositivo B-GigabitEthernet 1/0/1 ] Habilitar IPv6
   [ * Dispositivo B-GigabitEthernet 1/0/1 ] dirección IPv6 2001:db8::1 64
   [ * Dispositivo B-GigabitEthernet 1/0/1 ] deshacer apagado
   ```

Anterior

```
Interfaz [ * Dispositivo A] Túnel 10
[ * Dispositivo A-Túnel10] protocolo de túnel ipv6-ipv4 6to4
[ * Dispositivo A-Tunnel10] Habilitar IPv6
[ * Dispositivo A-Tunnel10] dirección IPv6 2002:101:101::1 64
[ * Dispositivo A-Túnel10] fuente 1.1.1.1
[ * Dispositivo A-Tunnel10] salir
```

Configurar el dispositivo B.

```
[ * Dispositivo B] Interfaz Túnel 10
[ * Dispositivo B-Tunnel10] protocolo de túnel ipv6-ipv4 6to4
[ * Dispositivo B-Tunnel10] Habilitar IPv6
[ * Dispositivo B-Tunnel10] dirección IPv6 2002:202:202::1 64
[ * Dispositivo B-Tunnel10] fuente 2.2.2.2
[ * Dispositivo B-Tunnel10] salir
```

3. Configurar rutas en el dispositivo A y el dispositivo B.

   # Configure una ruta estática a 2002::/16 en el dispositivo A.

   ```
   [ * Dispositivo A] ruta ipv6 estática 2002:: 16 Túnel 10
   ```

   # Configure una ruta predeterminada a la red IPv6 en el dispositivo A.

   ```
   [ * Dispositivo A] ruta ipv6 estática :: 0 2002:202:202::1
   [ * Dispositivo A] confirmación
   ```

   # Configure una ruta estática a 2002::/16 en el dispositivo B.

   ```
   [ * Dispositivo B] ruta ipv6 estática 2002:: 16 Túnel 10
   [ * Dispositivo B] confirmación
   ```

4. Verificar la configuración.

   # Haga ping a la dirección IPv6 de GE 1/0/1 en el dispositivo B desde el dispositivo A. La salida del comando muestra que el ping es exitoso.

   ```
   [ ~ Dispositivo A] ping ipv6 2001:db8::1
     PING 2001:db8::1 : 56 bytes de datos, presione CTRL_C para interrumpir
       Respuesta de 2001:db8::1
       bytes=56 Secuencia=1 salto límite=64 tiempo=10 ms
       Respuesta de 2001:db8::1
       bytes=56 Secuencia=2 Límite de salto=64 Tiempo=2 ms
       Respuesta de 2001:db8::1
       bytes=56 Secuencia=3 Límite de salto=64 Tiempo=2 ms
       Respuesta de 2001:db8::1
       bytes=56 Secuencia=4 Límite de salto=64 Tiempo=2 ms
       Respuesta de 2001:db8::1
       bytes=56 Secuencia=5 Límite de salto=64 Tiempo=2 ms

     --- Estadísticas de ping 2001:db8::1 ---
       5 paquete(s) transmitido(s)
       5 paquete(s) recibido(s)
       0,00% pérdida de paquetes
   viaje de ida y vuelta mín./promedio/máx. = 5/14/29 ms
   ```

Archivos de configuración

- Archivo de configuración del dispositivo A

  ```
  #
  sysname Dispositivo A
  ‡
  ```

Anterior

```
 dirección IP 1.1.1.1 255.0.0.0
#
interfaz GigabitEthernet 1/0/1
 deshacer el apagado
 Habilitar IPv6
 dirección IPv6 2002:101:101:1::1/64
#
Interfaz Túnel 10
 Habilitar IPv6
 dirección IPv6 2002:101:101::1/64
 protocolo-túnel ipv6-ipv4 6to4
 fuente 1.1.1.1
#
ruta ipv6 estática::0 2002:202:202::1
#
ruta ipv6 estática 2002:: 16 Túnel 10
#
devolver
```

- Archivo de configuración del dispositivo B

```
#
nombre del sistema Dispositivo B
#
administración
interfaz GigabitEthernet 1/0/0
 deshacer el apagado
 dirección IP 2.2.2.2 255.0.0.0
#
interfaz GigabitEthernet 1/0/1
 deshacer el apagado
 Habilitar IPv6
 dirección IPv6 2001:db8::1/64
#
Interfaz Túnel 10
 Habilitar IPv6
 dirección IPv6 2002:202:202::1/64
 protocolo-túnel ipv6-ipv4 6to4
 fuente 2.2.2.2
#
ruta ipv6 estática 2002:: 16 Túnel 10
#
devolver
```

Ejemplo de configuración de un túnel 6RD

Esta sección proporciona un ejemplo para configurar un túnel 6RD para permitir que los clientes o dispositivos en diferentes dominios 6RD se comuniquen.

Requisitos de red

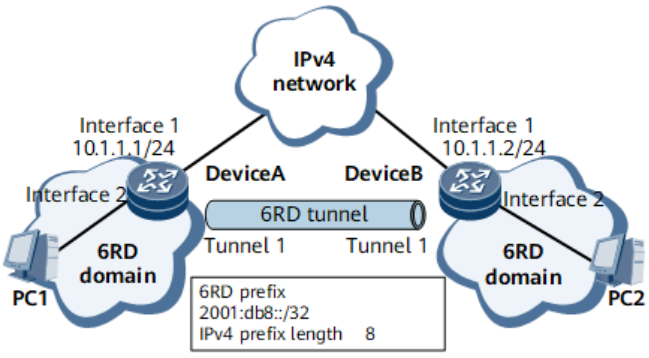
Como se muestra en la Figura 1-1997 , tanto el Dispositivo A como el Dispositivo B admiten la doble pila IPv4/IPv6 y están conectados a una red IPv6 y a una red IPv4. Tanto el Dispositivo A como el Dispositivo B son CE 6RD. Las redes IPv6 son redes 6RD. Es necesario establecer un túnel 6RD entre el Dispositivo A y el Dispositivo B para que los hosts de ambas redes IPv6 puedan comunicarse.

Figura 1-1997 Diagrama de red para configurar un túnel 6RD para permitir que los clientes y dispositivos en diferentes dominios 6RD se comuniquen

---

NOTE

Anterior



Hoja de ruta de configuración

La hoja de ruta de configuración es la siguiente:

1. En el dispositivo A y el dispositivo B, configure direcciones IPv4 para las interfaces físicas conectadas a la red IPv4 y habilite el reenvío de paquetes IPv6.
2. En el dispositivo A y el dispositivo B, configure la dirección IPv4 de origen, el prefijo 6RD, la longitud del prefijo IPv6 y la longitud del prefijo IPv4 para un túnel 6RD de modo que los dispositivos puedan calcular el prefijo delegado 6RD en función de una combinación de estos parámetros.
3. En el dispositivo A y el dispositivo B, configure direcciones IPv6 para las interfaces físicas conectadas a los dominios 6RD según el prefijo delegado 6RD.
4. Configure las direcciones IPv6 en PC1 y PC2, con el prefijo IPv6 establecido en un prefijo de dirección de 64 bits que contenga el prefijo 6RD y la identificación de subred.
5. En el dispositivo A, configure una ruta estática destinada al dominio 6RD donde reside el dispositivo B. En el dispositivo B, configure una ruta estática destinada al dominio 6RD donde reside el dispositivo A.

Preparación de datos

Para completar la configuración, necesitas los siguientes datos:

- Direcciones IPv4 de interfaces
- Direcciones IPv4 de origen de las interfaces del túnel 6RD
- Prefijo 6RD del túnel 6RD
- Longitud del prefijo IPv4 del túnel 6RD

Procedimiento

1. Configure direcciones IPv4 para las interfaces que conectan dispositivos a la red IPv4.

   # Configurar el dispositivo A.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo A
   [ * HUAWEI ] confirmación
   [ ~ Dispositivo A] interfaz gigabitethernet 1/0/1
   [ * Dispositivo A-GigabitEthernet 1/0/1 ] dirección IP 10.1.1.1 24
   [ * Dispositivo A-GigabitEthernet 1/0/1 ] confirmación
   [ ~ Dispositivo A-GigabitEthernet 1/0/1 ] salir
   ```

   # Configurar el dispositivo B.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo B
   [ * HUAWEI ] confirmación
   ```

Anterior

2. Configurar un túnel 6RD.

   # Configurar el dispositivo A.

```
Interfaz [ ~ Dispositivo A] Túnel 1
[ * Dispositivo A-Túnel1] protocolo de túnel ipv6-ipv4 6rd
[ * Dispositivo A-Túnel1] Habilitar IPv6
[ * Dispositivo A-Túnel1] fuente GigabitEthernet 1/0/1
[ * Dispositivo A-Túnel1] prefijo ipv6 2001:db8::/32
[ * Dispositivo A-Túnel1] longitud del prefijo IPv4 8
[ * Dispositivo A-Túnel1] confirmación
```

   # Configurar el dispositivo B.

```
[ ~ Dispositivo B] Interfaz Túnel 1
[ * Dispositivo B-Túnel1] protocolo de túnel ipv6-ipv4 6rd
[ * Dispositivo B-Tunnel1] Habilitar IPv6
[ * Dispositivo B-Tunnel1] fuente GigabitEthernet 1/0/1
[ * Dispositivo B-Tunnel1] prefijo ipv6 2001:db8::/32
[ * Dispositivo B-Tunnel1] longitud del prefijo IPv4 8
[ * Dispositivo B-Tunnel1] confirmación
```

   NOTE

   El prefijo delegado 6RD se puede calcular automáticamente en función de la dirección IPv4 del túnel de origen o el nombre de la interfaz de origen, el prefijo 6RD, la longitud del prefijo IPv6 y la longitud del prefijo IPv4. Puede ejecutar el comando **"display this interface"** para ver el prefijo delegado 6RD y, a continuación, configurar una dirección IPv6 para la interfaz del túnel.

   En este ejemplo, la longitud del prefijo IPv4 del túnel 6RD se establece en 8 bits. Para generar un prefijo delegado 6RD de 56 bits, el dispositivo elimina los 8 bits más a la izquierda de la dirección de origen del túnel (dirección IPv4 de GE **1/0/1**) y añade el prefijo 6RD 2001:db8::/32 antes de los 24 bits restantes (en notación hexadecimal) de la dirección de origen del túnel.

3. Consulta el prefijo delegado 6RD calculado.

   # Consulta el prefijo delegado 6RD calculado en el dispositivo A.

```
[ ~ Dispositivo A-Túnel1] muestra esta interfaz
Estado actual del túnel 1: ACTIVO (ifindex: 9)
Estado actual del protocolo de línea: INACTIVO
Descripción:
Puerto de ruta, la unidad máxima de transmisión es 1500
Procesamiento del protocolo de Internet: deshabilitado
La encapsulación es TÚNEL, bucle invertido no configurado
Origen del túnel 10.1.1.1, destino desconocido
Protocolo de túnel/transporte IPv6 sobre IPv4 (6º)
prefijo IPv6 2001:DB8::/32
longitud del prefijo IPv4 8
6RD Operacional, el prefijo delegado es 2001:DB8:101:100::/56
Hora actual del sistema: 2017-09-02 10:14:49
  300 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  Velocidad de salida de 300 segundos: 0 bits/seg, 0 paquetes/seg.
  0 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  0 segundos de velocidad de salida: 0 bits/seg, 0 paquetes/seg
  0 paquetes de entrada, 0 bytes
  0 errores de entrada
  0 paquetes de salida, 0 bytes
  0 errores de salida
  Aporte:
    Unicast: 0 paquetes, Multicast: 0 paquetes
```

Anterior

Consulta el prefijo delegado 6RD calculado en el dispositivo B.

```
[ ~ Dispositivo B-Tunnel1] muestra esta interfaz
Estado actual del túnel 1: ACTIVO (ifindex: 10)
Estado actual del protocolo de línea: INACTIVO
Descripción:
Puerto de ruta, la unidad máxima de transmisión es 1500
Procesamiento del protocolo de Internet: deshabilitado
La encapsulación es TÚNEL, bucle invertido no configurado
Origen del túnel 10.1.1.2, destino desconocido
Protocolo de túnel/transporte IPv6 sobre IPv4 (6º)
prefijo IPv6 2001:DB8::/32
longitud del prefijo IPv4 8
6RD Operacional, el prefijo delegado es 2001:db8:101:200::/56
Hora actual del sistema: 2017-09-02 10:22:13
  300 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  Velocidad de salida de 300 segundos: 0 bits/seg, 0 paquetes/seg.
  0 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  0 segundos de velocidad de salida: 0 bits/seg, 0 paquetes/seg
  0 paquetes de entrada, 0 bytes
  0 errores de entrada
  0 paquetes de salida, 0 bytes
  0 errores de salida
  Aporte:
    Unicast: 0 paquetes, Multicast: 0 paquetes
  Producción:
    Unicast: 0 paquetes, Multicast: 0 paquetes
    Tasa de utilidad de entrada de los últimos 300 segundos: --
    Tasa de utilidad de salida de los últimos 300 segundos: --
```

4. Configure direcciones IPv6 para las interfaces del túnel según el prefijo delegado 6RD.

   # Configurar el dispositivo A.

   ```
   [ ~ Dispositivo A-Túnel1] dirección IPv6 2001:db8:101:100::1 56
   [ * Dispositivo A-Túnel1] confirmación
   [ ~ Dispositivo A-Túnel1] salir
   ```

   # Configurar el dispositivo B.

   ```
   [ ~ Dispositivo B-Tunnel1] dirección IPv6 2001:db8:101:200::1 56
   [ * Dispositivo B-Tunnel1] confirmación
   [ ~ Dispositivo B-Tunnel1] salir
   ```

5. Configurar una dirección IPv6 para GE 1/0/2 .

   # Configurar el dispositivo A.

   ```
   [ ~ Dispositivo A] interfaz gigabitethernet 1/0/2
   [ * Dispositivo A-GigabitEthernet 1/0/2 ] Habilitar IPv6
   [ * Dispositivo A-GigabitEthernet 1/0/2 ] dirección IPv6 2001:db8:101:101::1 64
   [ * Dispositivo A-GigabitEthernet 1/0/2 ] confirmación
   [ ~ Dispositivo A-GigabitEthernet 1/0/2 ] salir
   ```

   # Configurar el dispositivo B.

   ```
   [ ~ Dispositivo B] interfaz gigabitethernet 1/0/2
   [ * Dispositivo B-GigabitEthernet 1/0/2 ] Habilitar IPv6
   [ * Dispositivo B-GigabitEthernet 1/0/2 ] dirección IPv6 2001:db8:101:201::1 64
   [ * Dispositivo B-GigabitEthernet 1/0/2 ] confirmación
   [ ~ Dispositivo B-GigabitEthernet 1/0/2 ] salir
   ```

6. Configure rutas estáticas destinadas a los dominios 6RD conectados al Dispositivo A y al Dispositivo B.

Anterior

Configure una ruta estática destinada al dominio 6RD conectado al dispositivo A.

```
[ ~ Dispositivo B] ruta ipv6 estática 2001:db8:: 32 Túnel 1
[ * Dispositivo B] confirmación
```

NOTE

Los 56 bits más a la izquierda de la dirección IPv6 de GE **1/0/2** deben ser los mismos que el prefijo delegado 6RD.

---

7. Configurar direcciones IPv6 para PC1 y PC2.

   # Configurar PC1.

   Configure la dirección IPv6 2001:db8:101:101::2/64 para la PC1 según el prefijo delegado 6RD. Esta dirección IPv6 debe estar en el mismo segmento de red que la de GE 1/0/2 en el Dispositivo A. Configure una ruta estática desde la PC1 al Dispositivo A y establezca la dirección de destino en 2001:db8::32. El método para configurar la dirección IPv6 y la ruta estática depende del sistema operativo que se esté ejecutando en la PC1. No se proporcionan los detalles de configuración.

   # Configurar PC2.

   Configure la dirección IPv6 2001:db8:101:201::2/64 para la PC2 según el prefijo delegado 6RD. Esta dirección IPv6 debe estar en el mismo segmento de red que la de GE 1/0/2 en el dispositivo B. Configure una ruta estática desde la PC2 al dispositivo B y establezca la dirección de destino en 2001:db8::32. El método para configurar la dirección IPv6 y la ruta estática depende del sistema operativo que se esté ejecutando en la PC2. No se proporcionan los detalles de configuración.

8. Verificar la configuración.

   # Después de completar las configuraciones, ejecute el comando **de interfaz de visualización Tunnel 1** para verificar el estado de Tunnel1 en el Dispositivo A o el Dispositivo B. La siguiente salida del comando muestra que el estado de Tunnel 1 es **UP** .

```
[ ~ Dispositivo A] Interfaz de pantalla Túnel 1
Estado actual del túnel 1: ACTIVO (ifindex: 78)
Estado actual del protocolo de línea: INACTIVO
Descripción:
Puerto de ruta, la unidad máxima de transmisión es 1500
Procesamiento del protocolo de Internet: deshabilitado
La encapsulación es TÚNEL, bucle invertido no configurado
Origen del túnel 2.1.1.1, destino desconocido
Protocolo de túnel/transporte IPv6 sobre IPv4 (6º)
prefijo IPv6 2001:DB8::/32
longitud del prefijo IPv4 8
6RD Operacional, el prefijo delegado es 2001:db8:101:100::/56
Hora actual del sistema: 2020-12-21 01:41:03
  300 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  Velocidad de salida de 300 segundos: 0 bits/seg, 0 paquetes/seg.
  0 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  0 segundos de velocidad de salida: 0 bits/seg, 0 paquetes/seg
  0 paquetes de entrada, 0 bytes
  0 errores de entrada
  0 paquetes de salida, 0 bytes
  0 errores de salida
  Aporte:
    Unicast: 0 paquetes, Multicast: 0 paquetes
  Producción:
    Unicast: 0 paquetes, Multicast: 0 paquetes
    Tasa de utilidad de entrada de los últimos 300 segundos: --
    Tasa de utilidad de salida de los últimos 300 segundos: --
```

   # En el dispositivo A, haga ping a la dirección IPv6 de GE 1/0/2 en el dispositivo B. La siguiente salida del comando muestra que el ping es exitoso.

```
[ ~ Dispositivo A] ping ipv6 2001:db8:101:201::1
  PING 2001:db8:101:201::1 : 56 bytes de datos, presione CTRL_C para interrumpir
    Respuesta de 2001:db8:101:201::1
```

Anterior

```
    bytes=56 Secuencia=3 Límite de salto=64 Tiempo=2 ms
    Respuesta de 2001:db8:101:201::1
    bytes=56 Secuencia=4 Límite de salto=64 Tiempo=2 ms
    Respuesta de 2001:db8:101:201::1
    bytes=56 Secuencia=5 Límite de saltos=64 Tiempo=2 ms
  --- 2001:db8:101:201::1 estadísticas de ping ---
    5 paquete(s) transmitido(s)
    5 paquete(s) recibido(s)
    0,00% pérdida de paquetes
    viaje de ida y vuelta mín./promedio/máx. = 2/2/4 ms
```

En la PC1, haga ping a la dirección IPv6 de la PC2. El siguiente comando muestra que el ping se realizó correctamente.

```
C:\> ping 2001:db8:101:201::2
Haciendo ping a 2001:db8:101:201::2 con 32 bytes de datos:
Respuesta de 2001:db8:101:201::2: tiempo<1ms
Respuesta de 2001:db8:101:201::2: tiempo<1ms
Respuesta de 2001:db8:101:201::2: tiempo<1ms
Respuesta de 2001:db8:101:201::2: tiempo<1ms
Estadísticas de ping para 2001:db8:101:201::2:
    Paquetes: Enviados = 4, Recibidos = 4, Perdidos = 0 (0% de pérdida),
Tiempos de ida y vuelta aproximados en milisegundos:
    Mínimo = 0 ms, Máximo = 0 ms, Promedio = 0 ms
```

Archivos de configuración

Archivo de configuración del dispositivo A

```
#
sysname Dispositivo A
#
interfaz GigabitEthernet 1/0/1
 deshacer el apagado
 dirección IP 10.1.1.1 255.255.255.0
#
interfaz GigabitEthernet 1/0/2
 deshacer el apagado
 Habilitar IPv6
 dirección IPv6 2001:db8:101:101::1 64
#
Interfaz Túnel 1
 Habilitar IPv6
 dirección IPv6 2001:db8:101:100::1 56
 protocolo de túnel ipv6-ipv4 6rd
 fuente GigabitEthernet 1/0/1
 prefijo ipv6 2001:db8::/32
 longitud del prefijo ipv4 8
#
ruta ipv6 estática 2001:db8:: 32 Túnel1
#
devolver
```

Archivo de configuración del dispositivo B

```
#
nombre del sistema Dispositivo B
#
interfaz GigabitEthernet 1/0/1
 deshacer el apagado
 dirección IP 10.1.1.2 255.255.255.0
#
int
 de
```

Anterior

```
Interfaz Túnel 1
 Habilitar IPv6
 dirección IPv6 2001:db8:101:200::1 56
 protocolo de túnel ipv6-ipv4 6rd
 fuente GigabitEthernet 1/0/1
 prefijo ipv6 2001:db8::/32
 longitud del prefijo ipv4 8
#
ruta ipv6 estática 2001:db8:: 32 Túnel1
#
devolver
```

Ejemplo de configuración de un relé 6RD

Esta sección proporciona un ejemplo para configurar un relé 6RD para permitir que los hosts o dispositivos en una red IPv6 aislada y en un dominio 6RD se comuniquen entre sí.

Requisitos de red

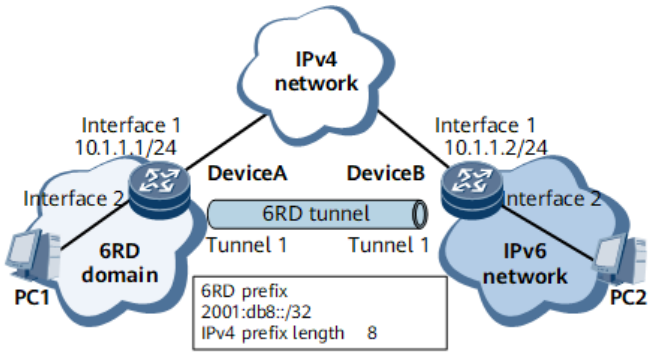
Como se muestra en la Figura 1-1998 , tanto el Dispositivo A como el Dispositivo B admiten la doble pila IPv4/IPv6 y están conectados a una red IPv6 y a una red IPv4. El Dispositivo A funciona como un CE 6RD y está conectado a una red IPv6 6RD. El Dispositivo B funciona como un BR 6RD y está conectado a una red IPv6 común fuera del dominio 6RD . Es necesario establecer un túnel 6RD entre los Dispositivos A y B para que los hosts de ambas redes IPv6 puedan comunicarse entre sí.

Figura 1-1998 Diagrama de red para configurar un túnel 6RD para permitir que un dominio 6RD y una red IPv6 común se comuniquen

---

NOTE

Las interfaces 1 y 2 en este ejemplo representan GE 1/0/1 y GE 1/0/2 , respectivamente.



Hoja de ruta de configuración

La hoja de ruta de configuración es la siguiente:

1. En el dispositivo A y el dispositivo B, configure direcciones IPv4 para las interfaces físicas conectadas a la red IPv4 y habilite el reenvío de paquetes IPv6.
2. En los dispositivos A y B , configure la dirección IPv4 de origen, el prefijo 6RD, la longitud del prefijo IPv6 y la longitud del prefijo IPv4 para un túnel 6RD. A continuación, calcule el prefijo delegado 6RD basándose en una combinación de estos parámetros.
3. En el dispositivo A y el dispositivo B, configure direcciones IPv6 para las interfaces físicas conectadas al dominio 6RD y a la red IPv6 según el prefijo delegado 6RD.
4. Configure las direcciones IPv6 en PC1 y PC2 y establezca el prefijo IPv6 de PC1 en un prefijo de dirección de 64 bits que contenga el prefijo 6RD y la ID de subred, y el prefijo IPv6 de PC2 en un prefijo de dirección IPv6 común.
5. En el dispositivo A, configure una ruta estática destinada a la red IPv6 donde reside el dispositivo B. En el dispositivo B, configure una

Anterior

- Direcciones IPv4 de interfaces
- Dirección IPv4 de origen de una interfaz de túnel 6RD
- Prefijo 6RD y longitud de un túnel 6RD
- Longitud del prefijo IPv4 de un túnel 6RD

Procedimiento

1. Configure direcciones IPv4 para las interfaces que conectan dispositivos a la red IPv4.

   # Configurar el dispositivo A.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo A
   [ * HUAWEI ] confirmación
   [ ~ Dispositivo A] interfaz gigabitethernet 1/0/1
   [ * Dispositivo A-GigabitEthernet 1/0/1 ] dirección IP 10.1.1.1 24
   [ * Dispositivo A-GigabitEthernet 1/0/1 ] confirmación
   [ ~ Dispositivo A-GigabitEthernet 1/0/1 ] salir
   ```

   # Configurar el dispositivo B.

   ```
   Vista del sistema de HUAWEI
   [ ~ HUAWEI ] nombre del sistema Dispositivo B
   [ * HUAWEI ] confirmación
   [ ~ Dispositivo B] interfaz gigabitethernet 1/0/1
   [ * Dispositivo B-GigabitEthernet 1/0/1 ] dirección IP 10.1.1.2 24
   [ * Dispositivo B-GigabitEthernet 1/0/1 ] confirmación
   [ ~ Dispositivo B-GigabitEthernet 1/0/1 ] salir
   ```

2. Configurar un túnel 6RD.

   # Configurar el dispositivo A.

   ```
   Interfaz [ ~ Dispositivo A] Túnel 1
   [ * Dispositivo A-Túnel1] protocolo de túnel ipv6-ipv4 6rd
   [ * Dispositivo A-Túnel1] Habilitar IPv6
   [ * Dispositivo A-Túnel1] fuente GigabitEthernet 1/0/1
   [ * Dispositivo A-Túnel1] prefijo ipv6 2001:db8::/32
   [ * Dispositivo A-Túnel1] longitud del prefijo IPv4 8
   [ * Dispositivo A-Túnel1] dirección de retransmisión de borde 10.1.1.2
   [ * Dispositivo A-Túnel1] confirmación
   ```

   # Configurar el dispositivo B.

   ```
   [ ~ Dispositivo B] Interfaz Túnel 1
   [ * Dispositivo B-Túnel1] protocolo de túnel ipv6-ipv4 6rd
   [ * Dispositivo B-Tunnel1] Habilitar IPv6
   [ * Dispositivo B-Tunnel1] fuente GigabitEthernet 1/0/1
   [ * Dispositivo B-Tunnel1] prefijo ipv6 2001:db8::/32
   [ * Dispositivo B-Tunnel1] longitud del prefijo IPv4 8
   [ * Dispositivo B-Tunnel1] confirmación
   ```

NOTE

El prefijo delegado 6RD se puede calcular automáticamente en función de la dirección del túnel de origen o la interfaz de origen configurada, el prefijo 6RD, la longitud del prefijo IPv6 y la longitud del prefijo IPv4. Puede ejecutar el comando **"display this interface"** para ver el prefijo delegado 6RD y, a continuación, configurar una dirección IPv6 para la interfaz del túnel.

Anterior

```
[ ~ Dispositivo A-Túnel1] muestra esta interfaz
Estado actual del túnel 1: ACTIVO (ifindex: 9)
Estado actual del protocolo de línea: INACTIVO
Descripción:
Puerto de ruta, la unidad máxima de transmisión es 1500
Procesamiento del protocolo de Internet: deshabilitado
La encapsulación es TÚNEL, bucle invertido no configurado
Origen del túnel 10.1.1.1, destino desconocido
Protocolo de túnel/transporte IPv6 sobre IPv4 (6º)
prefijo IPv6 2001:DB8::/32
longitud del prefijo IPv4 8
6RD Operacional, el prefijo delegado es 2001:DB8:101:100::/56
Hora actual del sistema: 2017-09-02 10:14:49
  300 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  Velocidad de salida de 300 segundos: 0 bits/seg, 0 paquetes/seg.
  0 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  0 segundos de velocidad de salida: 0 bits/seg, 0 paquetes/seg
  0 paquetes de entrada, 0 bytes
  0 errores de entrada
  0 paquetes de salida, 0 bytes
  0 errores de salida
  Aporte:
    Unicast: 0 paquetes, Multicast: 0 paquetes
  Producción:
    Unicast: 0 paquetes, Multicast: 0 paquetes
    Tasa de utilidad de entrada de los últimos 300 segundos: --
    Tasa de utilidad de salida de los últimos 300 segundos: --
```

Muestra el prefijo delegado 6RD calculado en el dispositivo B.

```
[ Dispositivo B-Tunnel1] muestra esta interfaz
Estado actual del túnel 1: ACTIVO (ifindex: 10)
Estado actual del protocolo de línea: INACTIVO
Descripción:
Puerto de ruta, la unidad máxima de transmisión es 1500
Procesamiento del protocolo de Internet: deshabilitado
La encapsulación es TÚNEL, bucle invertido no configurado
Origen del túnel 10.1.1.2, destino desconocido
Protocolo de túnel/transporte IPv6 sobre IPv4 (6º)
prefijo IPv6 2001:DB8::/32
longitud del prefijo IPv4 8
6RD Operacional, el prefijo delegado es 2001:db8:101:200::/56
Hora actual del sistema: 2017-09-02 10:22:13
  300 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  Velocidad de salida de 300 segundos: 0 bits/seg, 0 paquetes/seg.
  0 segundos de velocidad de entrada: 0 bits/seg, 0 paquetes/seg
  0 segundos de velocidad de salida: 0 bits/seg, 0 paquetes/seg
  0 paquetes de entrada, 0 bytes
  0 errores de entrada
  0 paquetes de salida, 0 bytes
  0 errores de salida
  Aporte:
    Unicast: 0 paquetes, Multicast: 0 paquetes
  Producción:
    Unicast: 0 paquetes, Multicast: 0 paquetes
    Tasa de utilidad de entrada de los últimos 300 segundos: --
    Tasa de utilidad de salida de los últimos 300 segundos: --
```

4. Configure direcciones IPv6 para las interfaces del túnel según el prefijo delegado 6RD.

Anterior

```
[ ~ Dispositivo A-Túnel1] salir
```

Configurar el dispositivo B.

```
[ ~ Dispositivo B-Tunnel1] dirección IPv6 2001:db8:101:200::1 56
[ * Dispositivo B-Tunnel1] confirmación
[ ~ Dispositivo B-Tunnel1] salir
```

5. Configure una dirección IPv6 para GE 1/0/2 en cada dispositivo .

   # Configurar el dispositivo A.

```
[ ~ Dispositivo A] interfaz gigabitethernet 1/0/2
[ * Dispositivo A-GigabitEthernet 1/0/2 ] Habilitar IPv6
[ * Dispositivo A-GigabitEthernet 1/0/2 ] dirección IPv6 2001:db8:101:101::1 64
[ * Dispositivo A-GigabitEthernet 1/0/2 ] confirmación
[ ~ Dispositivo A-GigabitEthernet 1/0/2 ] salir
```

   # Configurar el dispositivo B.

```
[ ~ Dispositivo B] interfaz gigabitethernet 1/0/2
[ * Dispositivo B-GigabitEthernet 1/0/2 ] Habilitar IPv6
[ * Dispositivo B-GigabitEthernet 1/0/2 ] dirección IPv6 2001:db8::1 64
[ * Dispositivo B-GigabitEthernet 1/0/2 ] confirmación
[ ~ Dispositivo B-GigabitEthernet 1/0/2 ] salir
```

6. Configurar rutas estáticas.

   # Configure una ruta estática destinada a la red IPv6 conectada al dispositivo B.

```
[ ~ Dispositivo A] ruta ipv6 estática 2001:db8:: 32 Túnel 1
[ * Dispositivo A] confirmación
```

   # Configure una ruta estática destinada al dominio 6RD conectado al dispositivo A.

```
[ ~ Dispositivo B] ruta ipv6 estática 2001:db8:: 32 Túnel 1
[ * Dispositivo B] confirmación
```

7. Configurar direcciones IPv6 para PC1 y PC2.

   # Configurar PC1.

   Configure la dirección IPv6 2001:db8:101:101::2/64 para la PC1 según el prefijo delegado 6RD. La dirección IPv6 de la PC1 debe estar en el mismo segmento de red que GE 1/0/2 del Dispositivo A. Configure una ruta estática desde la PC1 al Dispositivo A y establezca la dirección de destino en 2001:db8::32. El método para configurar la dirección IPv6 y la ruta estática depende del sistema operativo que se esté ejecutando en la PC1. No se proporcionan los detalles de configuración.

   # Configurar PC2.

   Configure la dirección IPv6 2002:db8::2/64 para la PC2 según el prefijo delegado 6RD. La dirección IPv6 de la PC2 debe estar en el mismo segmento de red que GE 1/0/2 del Dispositivo B. Configure una ruta estática 2001:db8::32 desde la PC2 al Dispositivo B. El método para configurar la dirección IPv6 y la ruta estática depende del sistema operativo que se esté ejecutando en la PC2. No se proporcionan los detalles de configuración.

8. Verificar la configuración.

   # Después de completar la configuración, verifique el estado de IPv6 del Túnel 1 en el Dispositivo A o el Dispositivo B. La siguiente salida del comando muestra que el estado de IPv6 del Túnel 1 es **ACTIVO** .

```
[ ~ Dispositivo A] muestra la interfaz IPv6 del túnel 1
Estado actual del túnel 1: ACTIVO
Estado actual del protocolo IPv6: ACTIVO
IPv6 está habilitado, la dirección de enlace local es FE80::3ABA:9A00:9DC:D303
  Direcciones de unidifusión global:
    2001:DB8:101:100::1, la subred es 2001:DB8:101:100::/56
  Direcciones del grupo al que se unió:
    FF02::1:FF00:1
    FF02::1:FFDC:D303
    FF02::2
```

Anterior

```
  Los hosts utilizan una configuración automática sin estado para las direcciones
```

En el dispositivo A, haga ping a la dirección IPv6 de GE 1/0/2 en el dispositivo B. La siguiente salida del comando muestra que el ping es exitoso.

```
[ ~ Dispositivo A] ping ipv6 2001:db8::1
  PING 2001:db8::1 : 56 bytes de datos, presione CTRL_C para interrumpir
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=1 límite de salto=64 tiempo=4 ms
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=2 Límite de saltos=64 Tiempo=3 ms
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=3 Límite de salto=64 Tiempo=2 ms
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=4 Límite de salto=64 Tiempo=2 ms
    Respuesta de 2001:db8::1
    bytes=56 Secuencia=5 Límite de saltos=64 Tiempo=2 ms
  --- Estadísticas de ping 2001:db8::1 ---
    5 paquete(s) transmitido(s)
    5 paquete(s) recibido(s)
    0,00% pérdida de paquetes
    viaje de ida y vuelta mín./promedio/máx. = 2/2/4 ms
```

En la PC1, haga ping a la dirección IPv6 de la PC2. El siguiente comando muestra que el ping se realizó correctamente.

```
C:\> ping 2001:db8::2
Haciendo ping a 2001:db8::2 con 32 bytes de datos:
Respuesta de 2001:db8::2: tiempo<1ms
Respuesta de 2001:db8::2: tiempo<1ms
Respuesta de 2001:db8::2: tiempo<1ms
Respuesta de 2001:db8::2: tiempo<1ms
Estadísticas de ping para 2001:db8::2:
    Paquetes: Enviados = 4, Recibidos = 4, Perdidos = 0 (0% de pérdida),
Tiempos de ida y vuelta aproximados en milisegundos:
    Mínimo = 0 ms, Máximo = 0 ms, Promedio = 0 ms
```

Archivos de configuración

Archivo de configuración del dispositivo A

```
#
sysname Dispositivo A
#
interfaz GigabitEthernet 1/0/1
 deshacer el apagado
 dirección IP 10.1.1.1 255.255.255.0
#
interfaz GigabitEthernet 1/0/2
 deshacer el apagado
 Habilitar IPv6
 dirección IPv6 2001:db8:101:101::1 64
#
Interfaz Túnel 1
 Habilitar IPv6
 dirección IPv6 2001:db8:101:100::1 56
 protocolo de túnel ipv6-ipv4 6rd
 fuente GigabitEthernet 1/0/1
 prefijo ipv6 2001:db8::/32
 longitud del prefijo ipv4 8
 dirección de retransmisión fronteriza 10.1.1.2
#
rut
```

Anterior

Archivo de configuración del dispositivo B

```
#
nombre del sistema Dispositivo B
#
interfaz GigabitEthernet 1/0/1
 deshacer el apagado
 dirección IP 10.1.1.2 255.255.255.0
#
interfaz GigabitEthernet 1/0/2
 deshacer el apagado
 Habilitar IPv6
 dirección IPv6 2001:db8::1 64
#
Interfaz Túnel 1
 Habilitar IPv6
 dirección IPv6 2001:db8:101:200::1 56
 protocolo de túnel ipv6-ipv4 6rd
```


Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

Privacidad Condiciones de uso Galletas Configuración de cookies Reportar contenido

REFERENCIAS TECNICAS

INGLES

L2TP

HUAWEI Firewall Interoperability Configuration Guide for VPN

This document provides the guide for configuring a Huawei firewall to use VPN to communicate with a non-Huawei device.

Search this document. 0 / 500

Please evaluate and leave your comments:

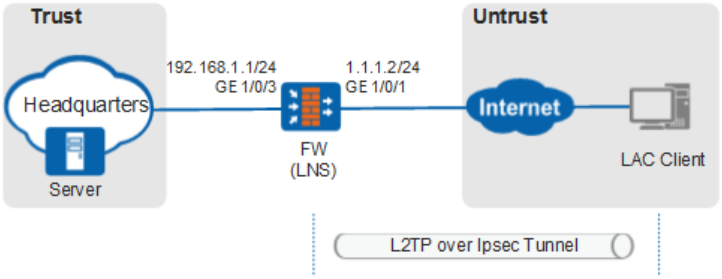
Web: Example for Configuring L2TP over IPSec to Allow Users to Acces the Headquarters Using Windows 7 Terminals

L2TP over IPSec VPN allows mobile employees to dial up to the headquarters (HQ) server using the Windows L2TP client.

Networking Requirements

The LAC client directly initiates a connection request to the LNS. The LAC client and LNS negotiate an IPSec tunnel, and perform L2TP negotiation to authenticate the user's identity and establish an L2TP over IPSec tunnel. The data between the LAC client and the LNS is transmitted through the tunnel. Layer-2 data is encapsulated using L2TP and then the data is encrypted using IPSec.

Figure 2-6 Networking diagram for configuring L2TP over IPSec for users to access the headquarters using the Windows L2TP client



Data Planning

Item	Data
LNS	Interface: GigabitEthernet 1/0/1 IP address: 1.1.1.2/24 Security zone: Untrust
	Interface: GigabitEthernet 1/0/3 IP address: 192.168.1.1/24 Security zone: Trust
	IP address and user for L2TP

Previous

	User name: vpdnuser User authentication password: Hello123
	IPSec configuration Security protocol: ESP IKE authentication algorithm: sha1 IKE encryption algorithm: 3des ESP authentication algorithm: sha1 ESP encryption algorithm: AES128 Pre-Shared Key: Admin@123 Local ID: IP Address Peer ID: Any Type IKE version: IKEv1
LAC	Internet address: 1.1.1.2 User name: vpdnuser Password: Hello123 Pre-Shared Key: Admin@123

Configuration Roadmap

1. Complete basic configurations, including the configurations of interfaces, security policies, and routes.
2. Complete the L2TP over IPSec configuration on FW.
3. On mobile employee's PC, complete the configurations. The parameters on the PC must match those on the FW.

Procedure

1. Configure the LNS.

   a. Set an IP address for each interface and assign the interfaces to security zones.

   a. Choose **Network** > **Interface**.

   b. Click of GE1/0/1 and set the following parameters:

Zone	untrust
IPv4	
IP Address	1.1.1.2/24

   c. Click **OK**.

   d. Repeat the preceding steps to set the parameters of the GE1/0/3 interface.

Zone	trust
IPv4	
IP Address	192.168.1.1/24

   b. Configure security policies to allow specific subnets to communicate.

Previous

Name	policy_ipsec_1
Source Zone	trust
Destination Zone	untrust
Source Address/Region	192.168.1.0/24
Destination Address/Region	10.1.1.2-10.1.1.100
Action	Permit

c. Click **OK**.

d. Repeat preceding steps to configure security policies for the Untrust -> Trust, Untrust -> Local, and Local -> Untrust interzones.

The parameters of the security policy for the Untrust -> Trust interzone are as follows:

Name	policy_ipsec_2
Source Zone	untrust
Destination Zone	trust
Source Address/Region	10.1.1.2-10.1.1.100
Destination Address/Region	192.168.1.0/24
Action	Permit

The parameters of the security policy for the Untrust -> Local interzone are as follows:

Name	policy_ipsec_3
Source Zone	untrust
Destination Zone	local
Destination Address/Region	1.1.1.2/32
Action	Permit

The parameters of the security policy for the Local -> Untrust interzone are as follows:

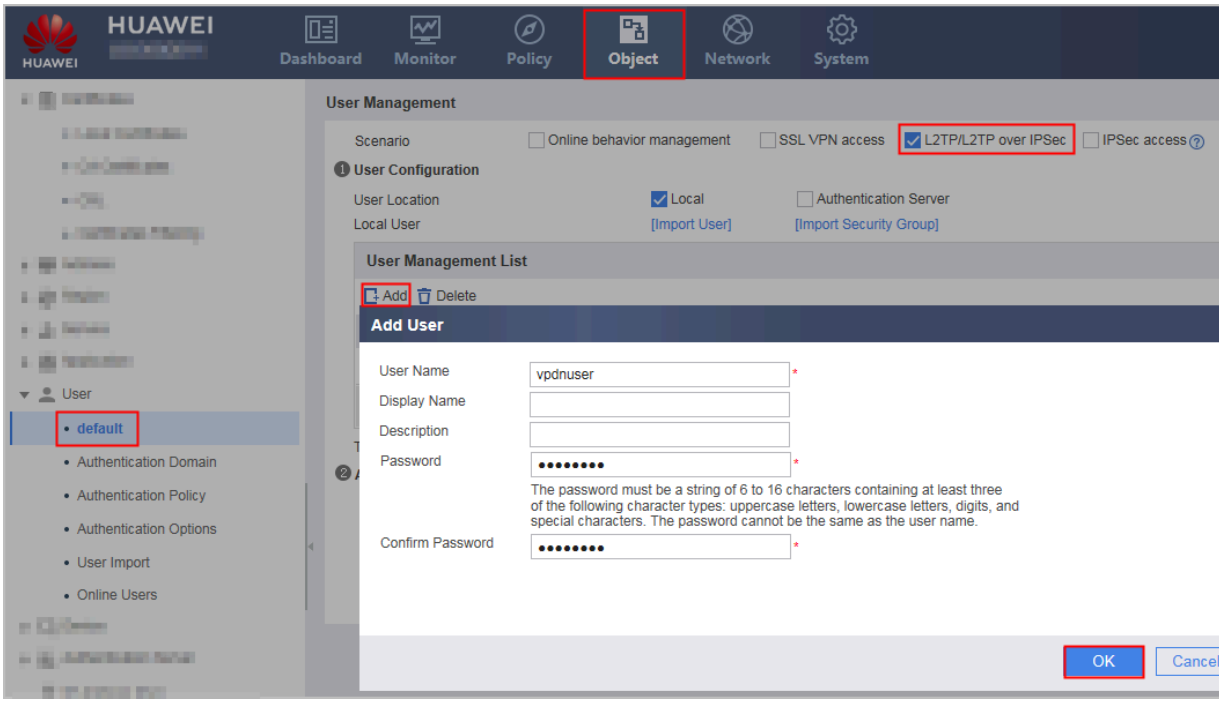
Name	policy_ipsec_4
Source Zone	local
Destination Zone	untrust
Source Address/Region	1.1.1.2/32

Previous

b. Select the **default** authentication domain.

c. Select the **L2TP/L2TP over IPSec** Scenario.

d. Under **User/User Group/Security Group Management List**, Click **Add**, select **Add User**, and set the following parameters.

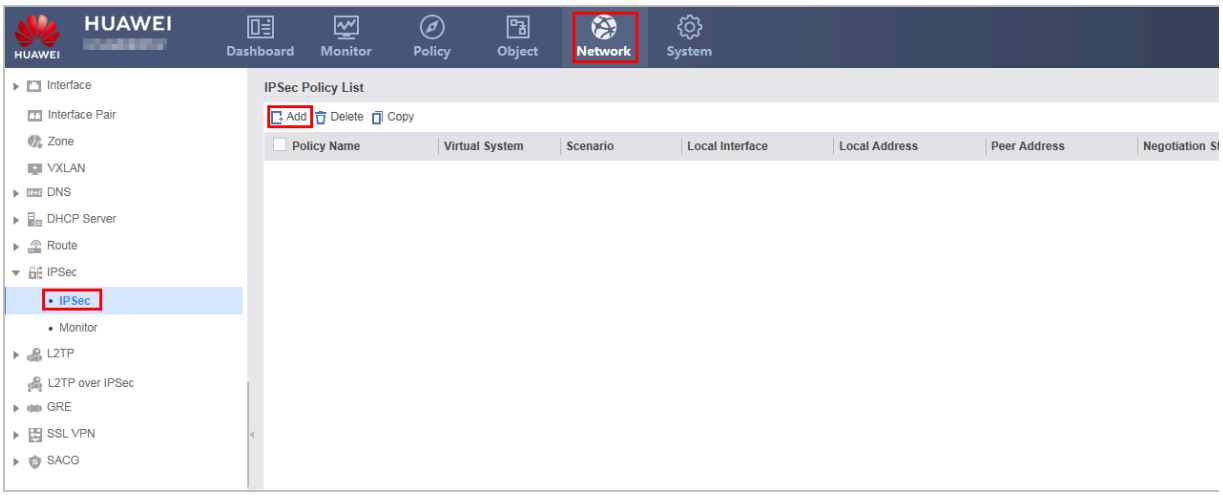


User Name	vpdnuser
Password	Hello123
Confirm Password	Hello123

e. Click **OK**.

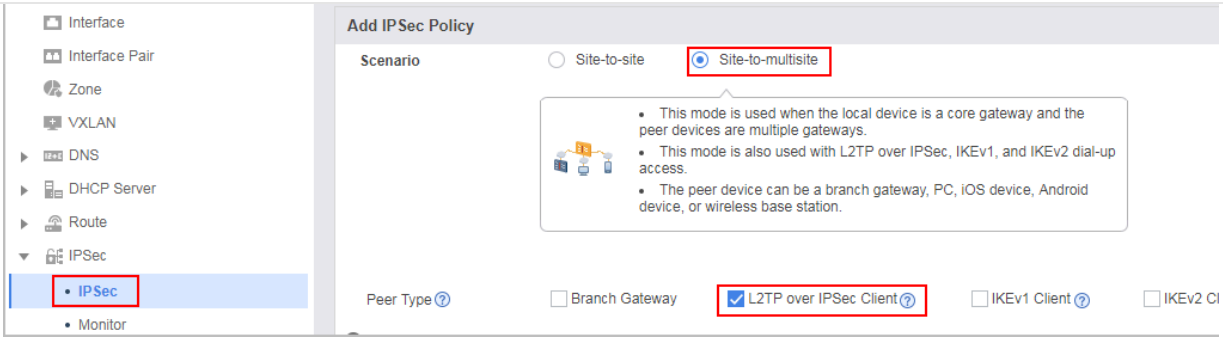
d. Configure the L2TP over IPSec tunnel.

a. Choose **Network** > **IPSec** > **IPSec**, and click **Add** under **IPSec Policy List**.

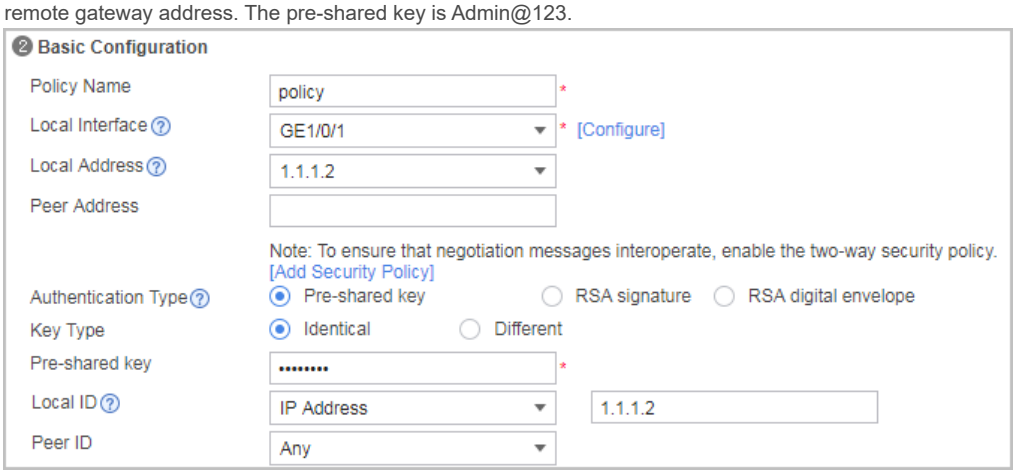


b. Select **Site-to-multisite** as **Scenario** as **L2TP over IPSec client**.

Previous



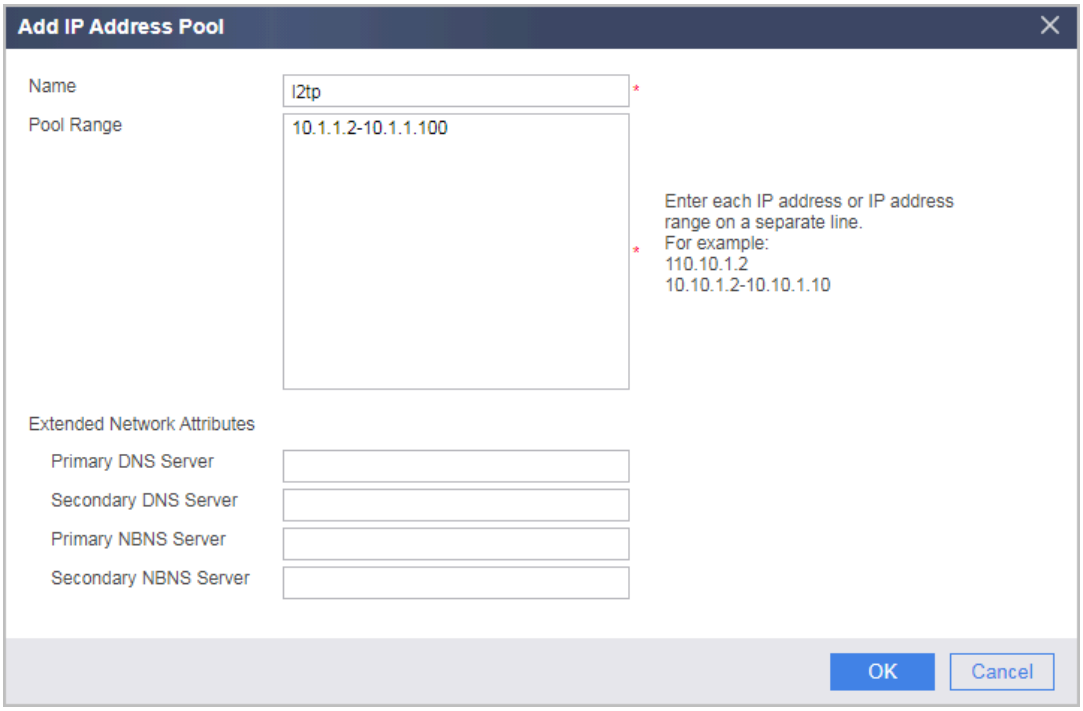
c. Configure **Basic Configuration** as follows. The headquarters needs to be accessed by multiple branches. Therefore, do not specify remote gateway address. The pre-shared key is Admin@123.



d. Configure **Dial-up User Configuration** as follows.

a. Choose **Add IP pool** in the **User address pool** drop-down list.

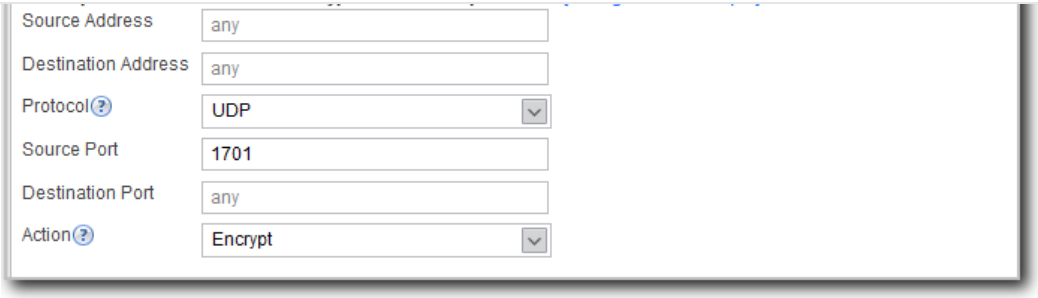
b. Set an IP pool.



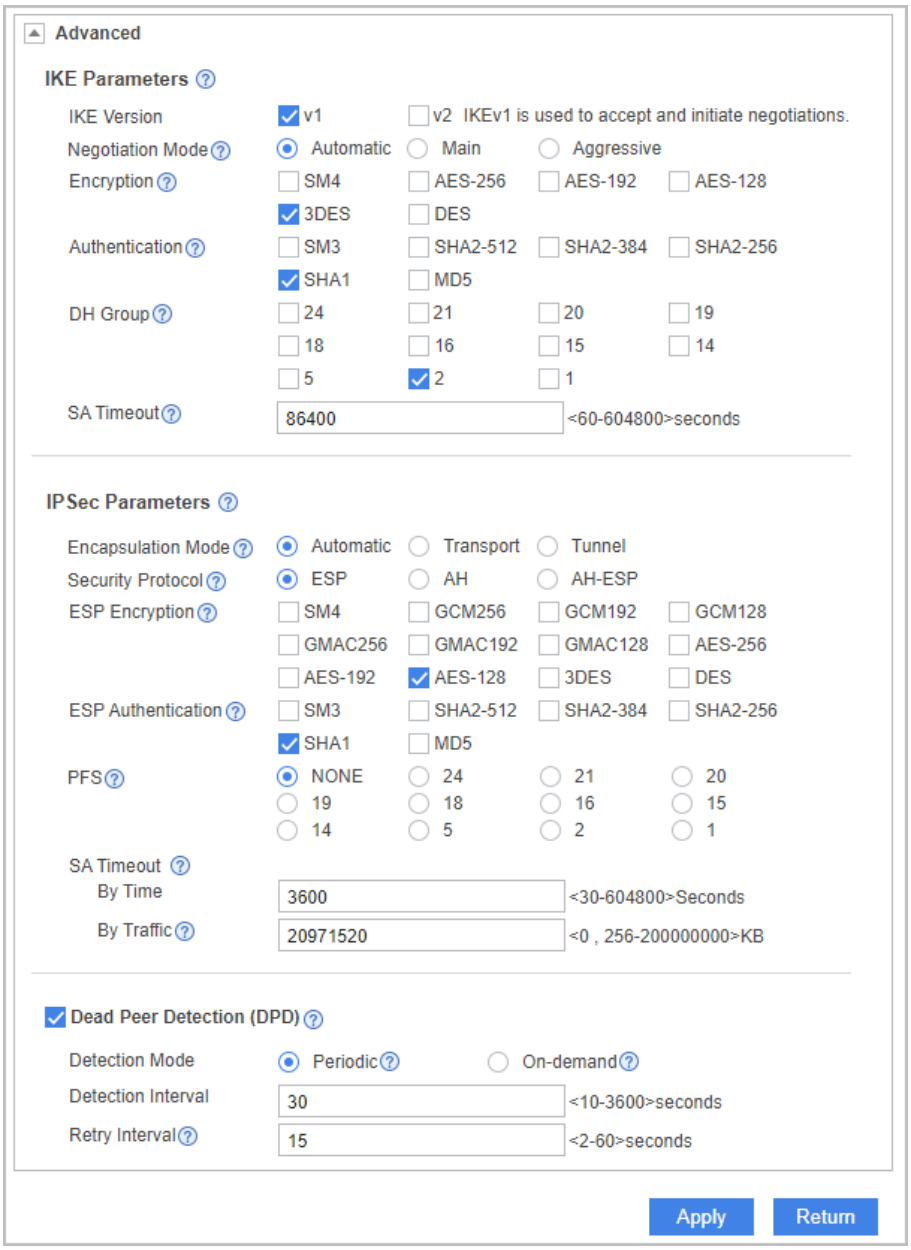
c. Click **OK**.

e. Under **Data Flow to Be Encrypted**, click **Add** to add a data flow as follows.

Previous



f. Configure IKE and IPSec protocol.



g. Click **Apply** to complete the configurations.

e. The LAC client uses the built-in L2TP client to dial up. Tunnel verification is not supported. Therefore, you need to disable tunnel verification on the FW.

a. Choose **Network** > **L2TP** > **L2TP**. In **L2TP Group List**, click **default-lns** and deselect **Tunnel Password Authentication**. Set the **Associated Zone** to **untrust**.

b. Click **OK**.

Previous

interface address of the FW.

3. Set dial-in parameters on the LAC client.

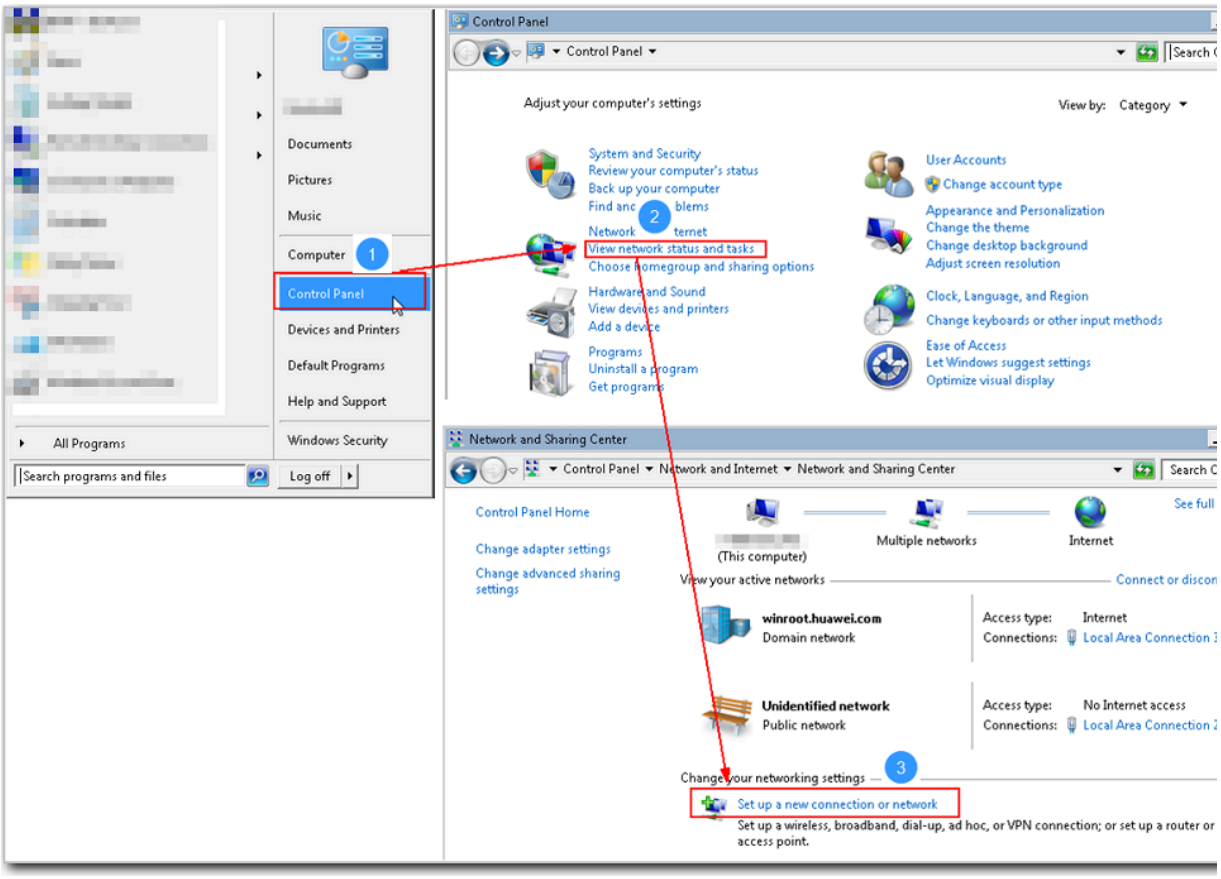
   a. View the status of the IPSec service and ensure that the IPSec service is enabled.

   a. Choose **Start** > **Run**, enter **services.msc**, and click **OK** to access the **Services** page.

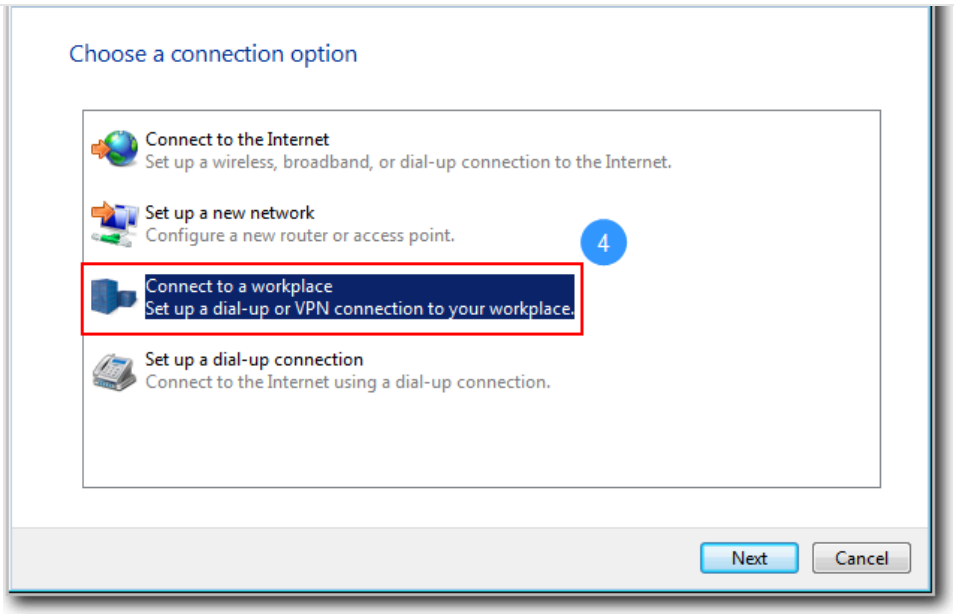
   b. In the **Name** column, view the **IPsec Policy Agent** status to ensure that IPsec Policy Agent are in **Started** state. Otherwise, right-cli **IPsec Policy Agent** and choose **Properties**. In **Properties**, set **Startup type** to **Automatic** and click **Apply**. Then select **Start** in **Service type**.

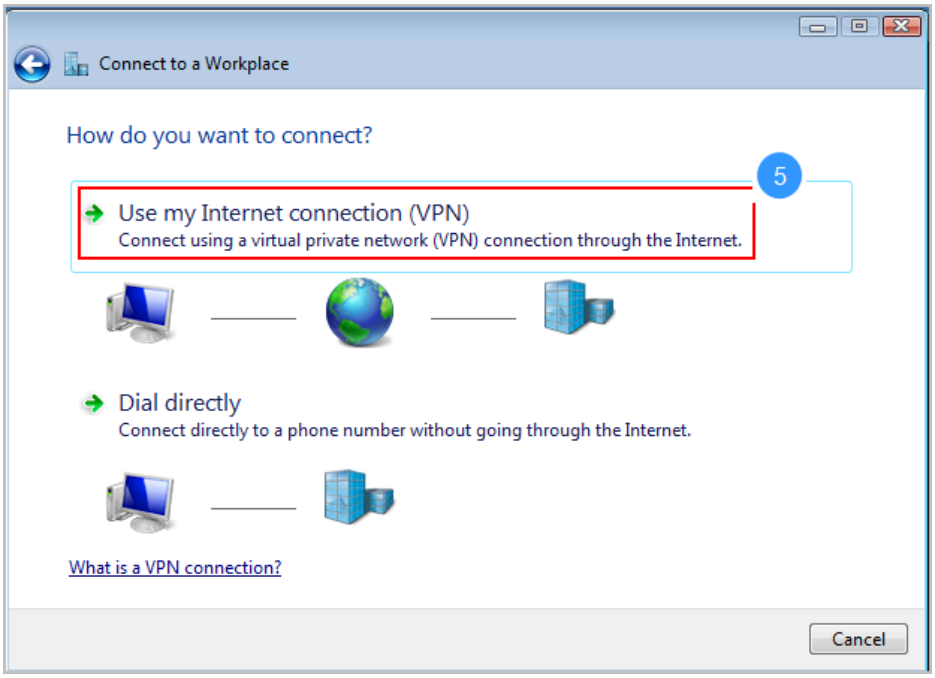
   c. Close the **Services** page.

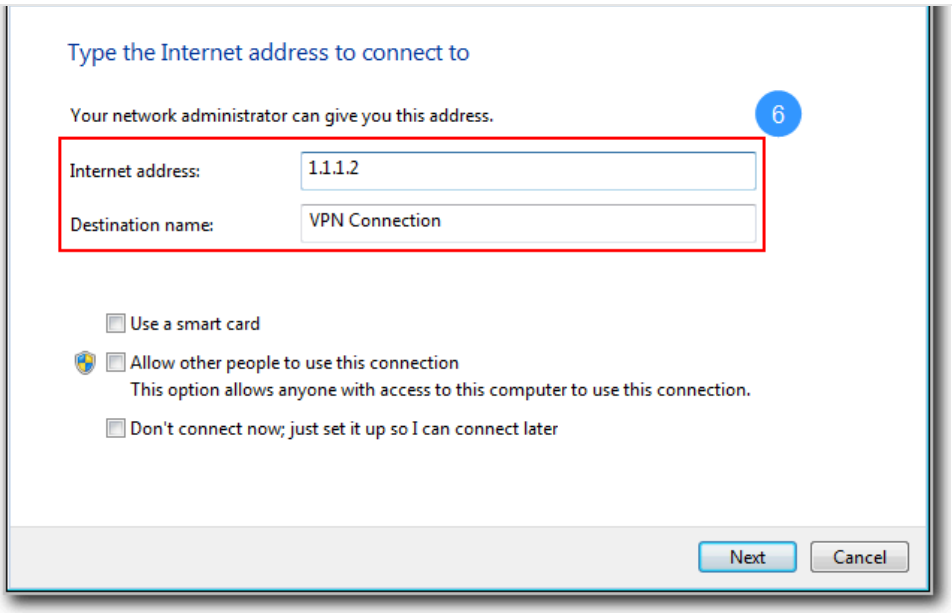
   b. Create an L2TP over IPSec connection.

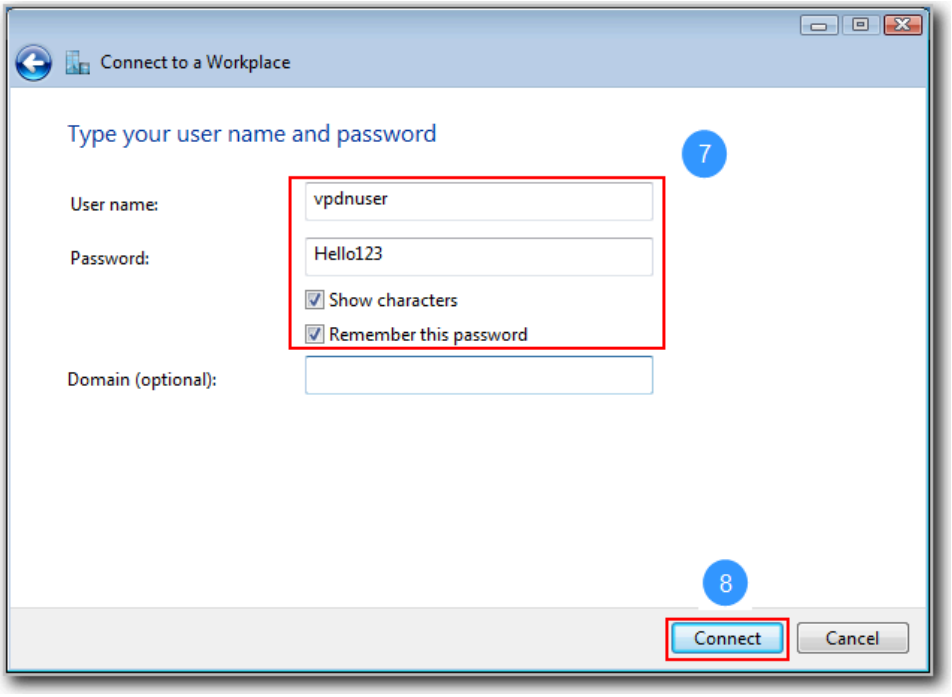


Previous

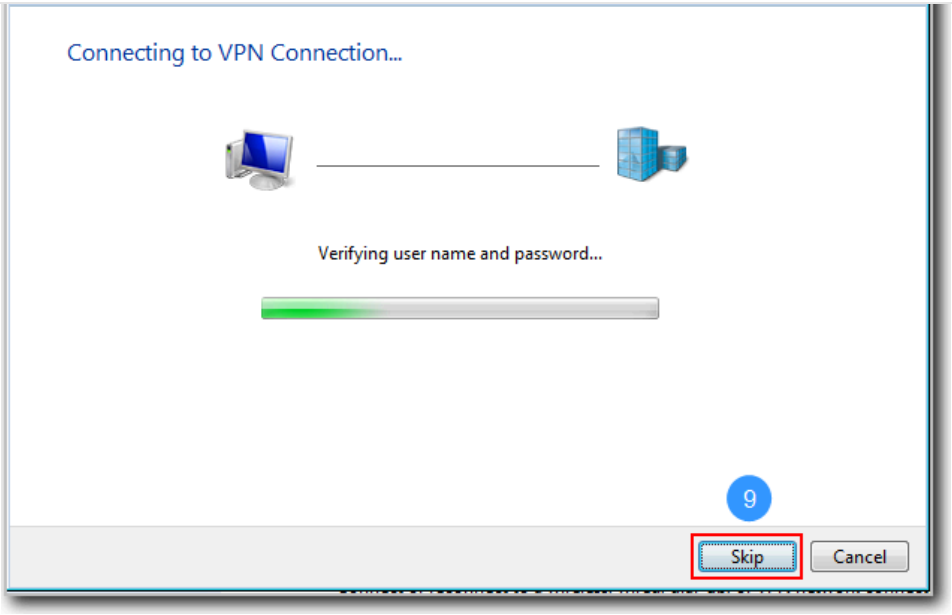

Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a new network
Configure a new router or access point.
4
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Next
Cancel

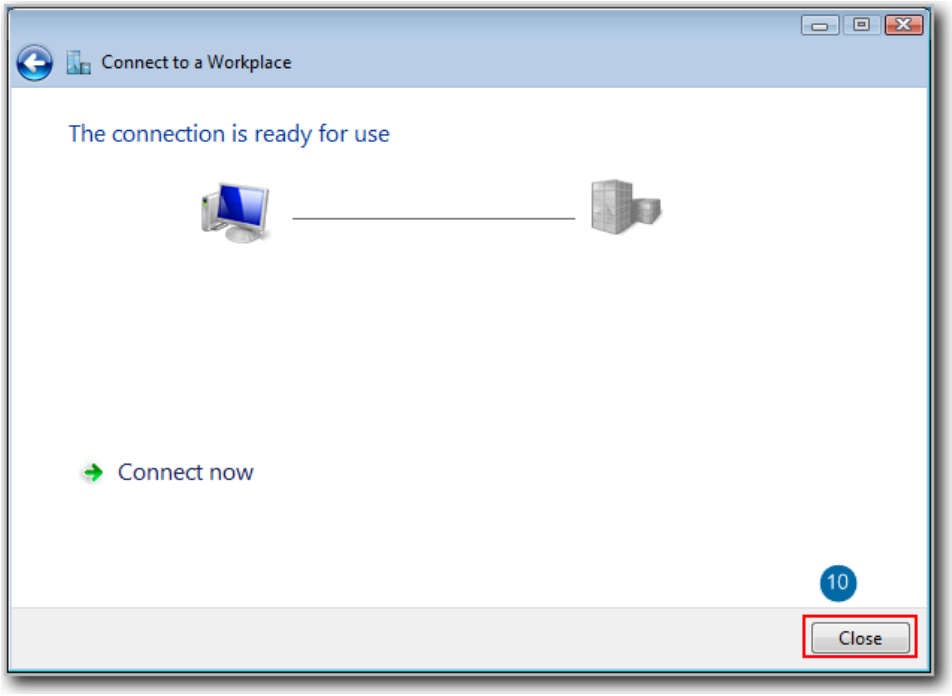

Connect to a Workplace
How do you want to connect?
5
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
What is a VPN connection?
Cancel


Type the Internet address to connect to
Your network administrator can give you this address.
6
Internet address:
1.1.1.2
Destination name:
VPN Connection
Use a smart card
Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.
Don't connect now; just set it up so I can connect later
Next
Cancel

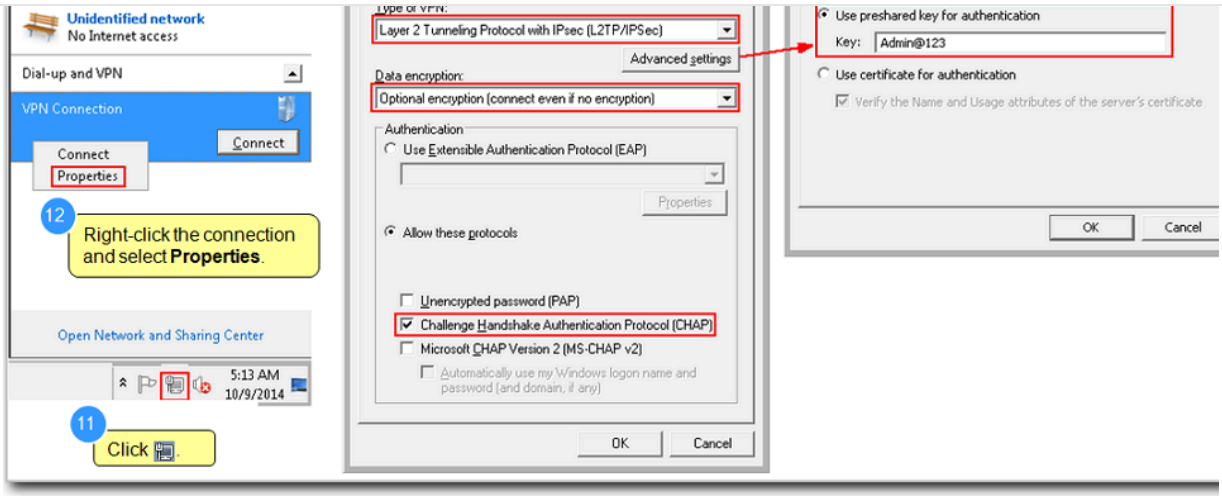

Connect to a Workplace
Type your user name and password
7
User name:
vpdnuser
Password:
Hello123
Show characters
Remember this password
Domain (optional):
8
Connect
Cancel

Previous


Connecting to VPN Connection...
Verifying user name and password...
9
Skip
Cancel

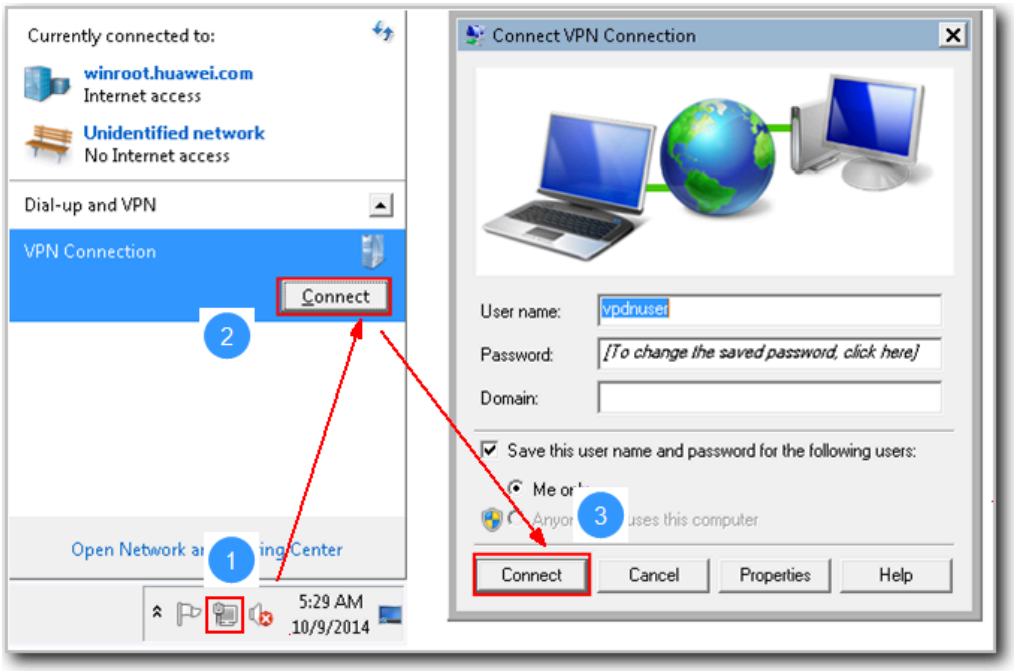

Connect to a Workplace
The connection is ready for use
Connect now
10
Close

Previous



Configuration Verification

1. The LAC Client succeeds in dialing up using the built-in software.



2. On the LAC, you can view that the 10.1.1.2/24-10.1.1.100/24 address range is assigned to the LAC, and mobile employees can access HQ server.
3. After the LAC dials up, check whether the L2TP tunnel is established on the LNS.



4. Check the IPSec tunnel establishment on the LNS. If the following information is displayed, the IPSec tunnel is established.



Co Previous

```
 l2tp enable
l2tp domain suffix-separator @
#
acl number 3001
 rule 5 permit udp source-port eq 1701
#
ike proposal pro91165721597
 encryption-algorithm 3des
 authentication-algorithm sha1
 dh group14
#
ike peer ike91165721597
 pre-shared-key %$%$Z1}*8w'rH;MD;%$%$
 ike-proposal pro91165721597
#
ipsec proposal prop91165721597
 encapsulation-mode transport
 esp authentication-algorithm sha1
 esp encryption-algorithm aes-128
```

About Us

How to Buy

Partner

Resources

Quick Links

Huawei e+ App

HUAWEI eKit App

Huawei HiKnow APP

HUAWEI eFly App

Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

Privacy Terms of use Cookies Cookie Settings Report content

```
#
l2tp-group default-lns
 allow l2tp virtual-template 1
 undo tunnel authentication
#
ip pool pool1
 section 1 10.1.1.2 10.1.1.100
#
aa
```

Previous

```
 domain default
  authentication-schem default
  service-scheme l2tp
#
security-policy
 rule name policy_ipsec_1
  source-zone trust
  destination-zone untrust
  source-address 192.168.1.0 24
  destination-address range 10.1.1.2 10.1.1.100
  action permit
 rule name policy_ipsec_2
  source-zone untrust
  destination-zone trust
  source-address range 10.1.1.2 10.1.1.100
  destination-address 192.168.1.0 24
  action permit
 rule name policy_ipsec_3
  source-zone untrust
  destination-zone local
  destination-address 1.1.1.2 32
  action permit
 rule name policy_ipsec_4
  source-zone local
  destination-zone untrust
  source-address 1.1.1.2 32
  action permit
# The following user/group creation configuration is stored in the database, but not in the configuration profi
user-manage user vpdnuser domain default
 password *********
```

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

L2TP

Guía de configuración de interoperabilidad del firewall de HUAWEI para VPN

Este documento proporciona una guía para configurar un firewall de Huawei para usar VPN para comunicarse con un dispositivo que no sea Huawei.

Buscar este documento. 0 / 500

Por favor evalúa y deja tus comentarios:

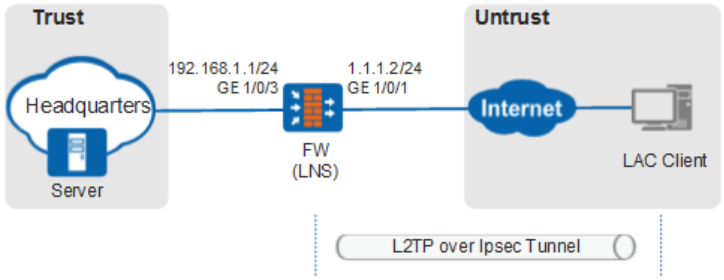
Web: Ejemplo de configuración de L2TP sobre IPSec para permitir a los usuarios acceder a la sede central mediante terminales de Windows 7

L2TP sobre VPN IPSec permite que los empleados móviles se comuniquen con el servidor de la sede central (HQ) mediante el cliente L2T

Requisitos de red

El cliente LAC inicia directamente una solicitud de conexión al LNS. El cliente LAC y el LNS negocian un túnel IPSec y realizan la negociac la identidad del usuario y establecer un túnel L2TP sobre IPSec. Los datos entre el cliente LAC y el LNS se transmiten a través del túnel. L encapsulan mediante L2TP y posteriormente se cifran mediante IPSec.

Figura 2-6 Diagrama de red para configurar L2TP sobre IPSec para que los usuarios accedan a la sede central mediante el cliente L2TP d



Planificación de datos

Artículo	Datos
LNS	Interfaz: GigabitEthernet 1/0/1 Dirección IP: 1.1.1.2/24 Zona de seguridad: No confiable
	Interfaz: GigabitEthernet 1/0/3 Dirección IP: 192.168.1.1/24 Zona de seguridad: Confianza
	Dirección IP y usuario para L2TP Grupo de IP 1

Anterior

	Contraseña de autenticación de usuario: Hello123
	Configuración de IPSec Protocolo de seguridad: ESP Algoritmo de autenticación IKE: sha1 Algoritmo de cifrado IKE: 3des Algoritmo de autenticación ESP: sha1 Algoritmo de cifrado ESP: AES128 Clave precompartida: Admin@123 ID local: Dirección IP ID de par: cualquier tipo Versión de IKE: IKEv1
LACA	Dirección de Internet: 1.1.1.2 Nombre de usuario: vpdnuser Contraseña: Hello123 Clave precompartida: Admin@123

Hoja de ruta de configuración

1. Configuraciones básicas completas, incluidas las configuraciones de interfaces, políticas de seguridad y rutas.
2. Complete la configuración de L2TP sobre IPSec en FW .
3. En la PC del empleado móvil, complete las configuraciones. Los parámetros de la PC deben coincidir con los del firmware .

Procedimiento

1. Configurar el LNS.

   a. Establezca una dirección IP para cada interfaz y asigne las interfaces a zonas de seguridad.

   a. Seleccione **Red** > **Interfaz** .

   b. Haga clic en GE1/0/1 y configure los siguientes parámetros:

Zona	desconfianza
IPv4	
Dirección IP	1.1.1.2/24

   c. Haga clic en **Aceptar** .

   d. Repita los pasos anteriores para configurar los parámetros de la interfaz GE1/0/3 .

Zona	confianza
IPv4	
Dirección IP	192.168.1.1/24

   b. Configure políticas de seguridad para permitir que subredes específicas se comuniquen.

   a. Seleccione **Políticas** > **Políticas de seguridad** > **Políticas de seguridad**

Anterior

Zona de origen	confianza
Zona de destino	desconfianza
Dirección de origen/Región	192.168.1.0/24
Dirección/Región de destino	10.1.1.2-10.1.1.100
Acción	Permiso

c. Haga clic en **Aceptar** .

d. Repita los pasos anteriores para configurar las políticas de seguridad para las interzonas Untrust -> Trust, Untrust -> Local y Local ·

Los parámetros de la política de seguridad para la zona intermedia Untrust -> Trust son los siguientes:

Nombre	política_ipsec_2
Zona de origen	desconfianza
Zona de destino	confianza
Dirección de origen/Región	10.1.1.2-10.1.1.100
Dirección/Región de destino	192.168.1.0/24
Acción	Permiso

Los parámetros de la política de seguridad para la interzona Untrust -> Local son los siguientes:

Nombre	política_ipsec_3
Zona de origen	desconfianza
Zona de destino	local
Dirección/Región de destino	1.1.1.2/32
Acción	Permiso

Los parámetros de la política de seguridad para la interzona Local -> No confiable son los siguientes:

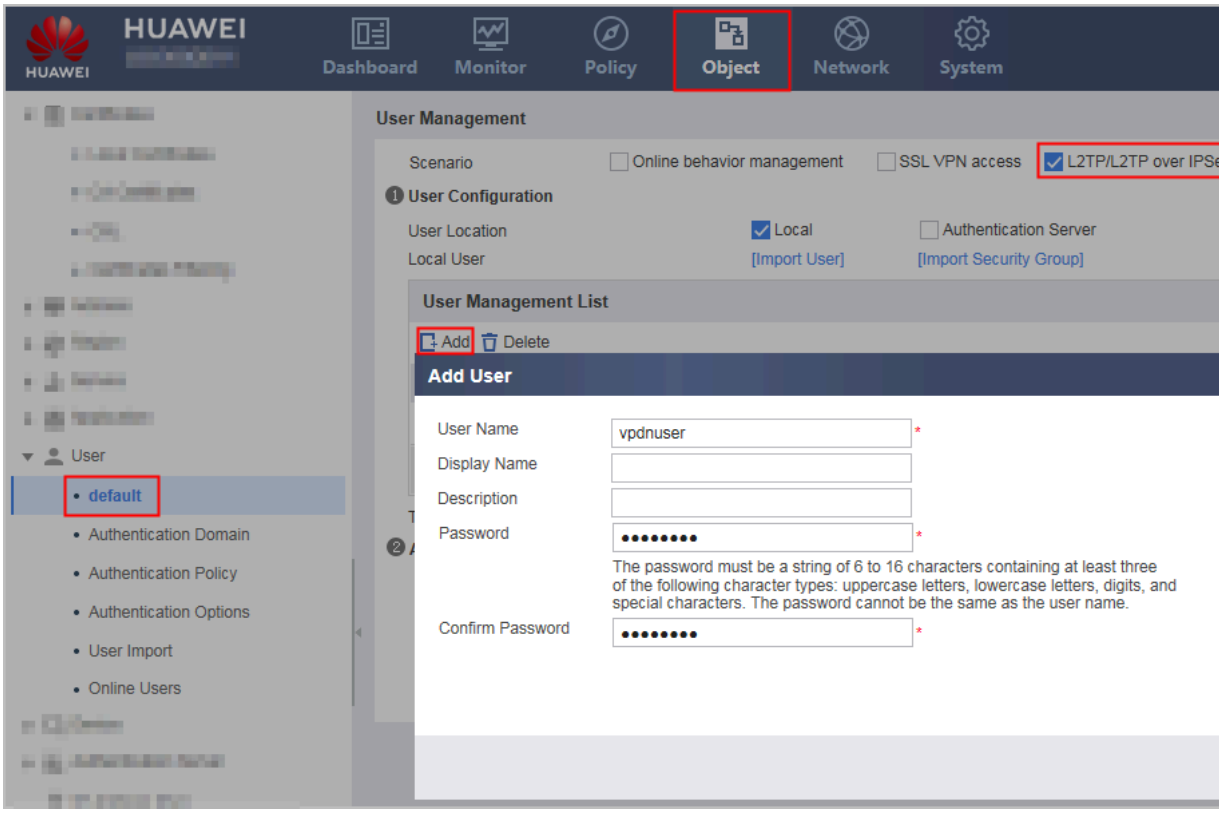
Nombre	política_ipsec_4
Zona de origen	local
Zona de destino	desconfianza
Dirección de origen/Región	1.1.1.2/32
Acción	Permiso

Anterior

b. Seleccione el dominio de autenticación **predeterminado .**

c. Seleccione el escenario **L2TP/L2TP sobre IPSec** .

d. En **la Lista de administración de usuarios/grupos de usuarios/grupos de seguridad** , haga clic en **Agregar** , seleccione **Agreg** los siguientes parámetros.



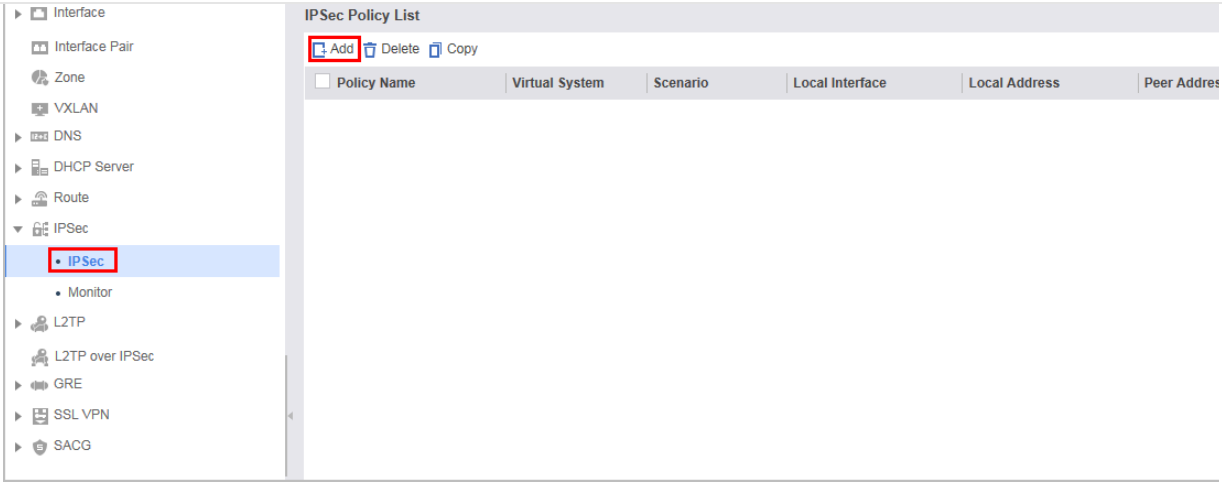
Nombre de usuario	usuariovpdn
Contraseña	Hola123
confirmar Contraseña	Hola123

e. Haga clic en **Aceptar** .

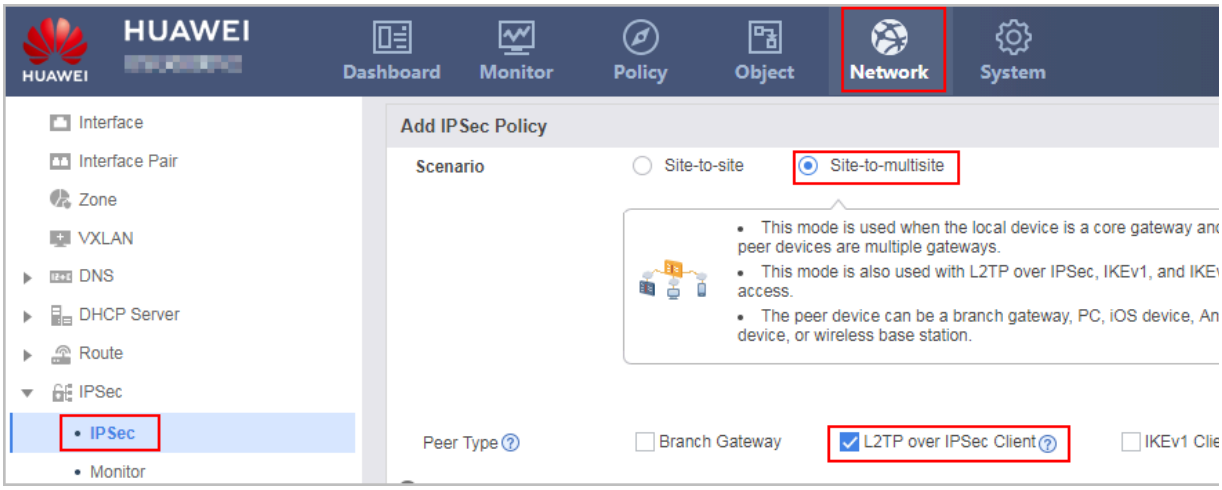
d. Configurar el túnel L2TP sobre IPSec.

a. Seleccione **Red** > **IPSec** > **IPSec** y haga clic en **Agregar** en **Lista de políticas IPSec** .

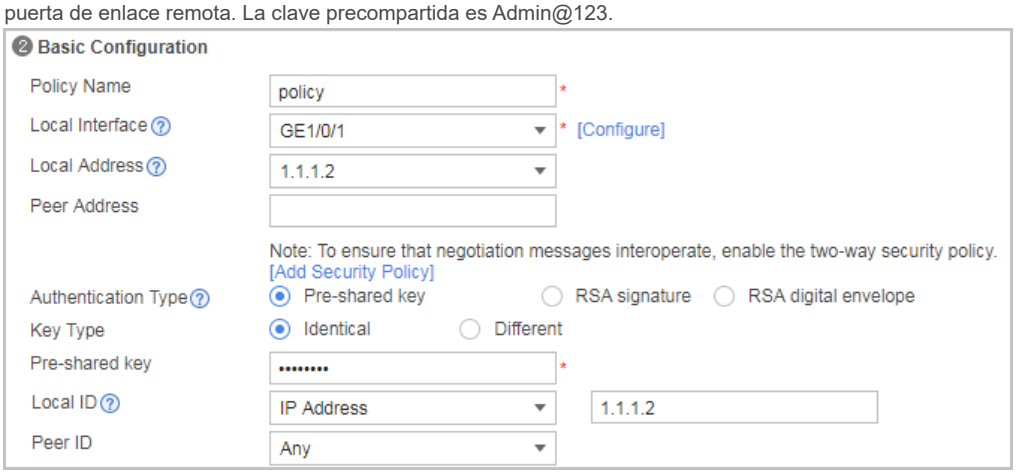
Anterior



b. Seleccione **Sitio a multisitio** como **Escenario** como **cliente L2TP sobre IPSec** .



c. Configure **la configuración básica** como se indica a continuación. Varias sucursales deben acceder a la sede. Por lo tanto, no esp
puerta de enlace remota. La clave precompartida es Admin@123.

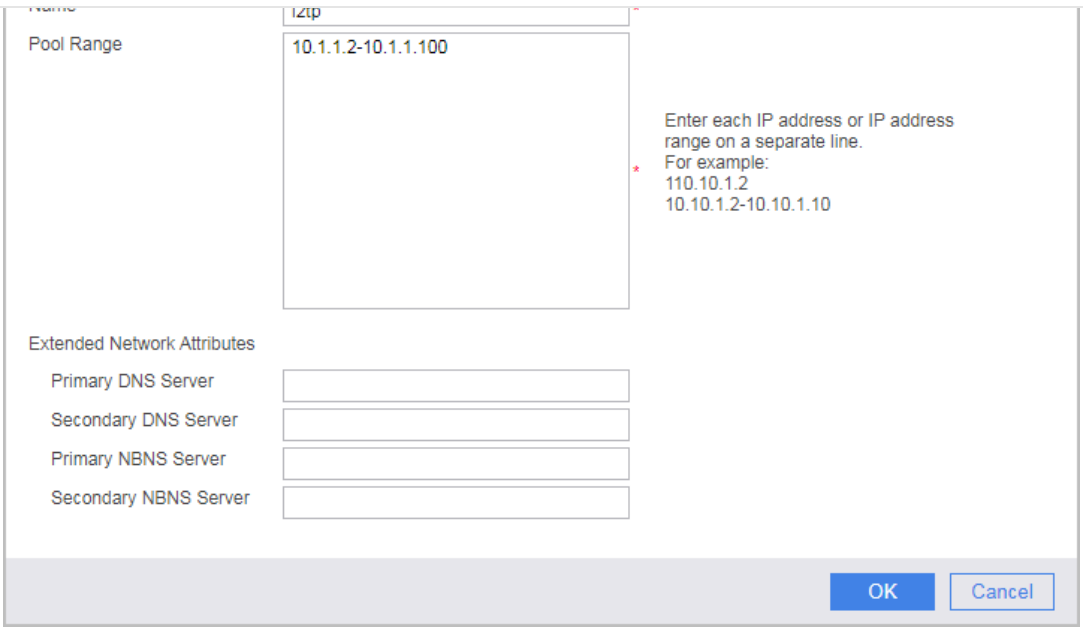


d. Configure **la configuración de usuario de acceso telefónico** de la siguiente manera.

a. Seleccione **Agregar grupo de IP** en la lista desplegable **Grupo de direcciones de usuario .**

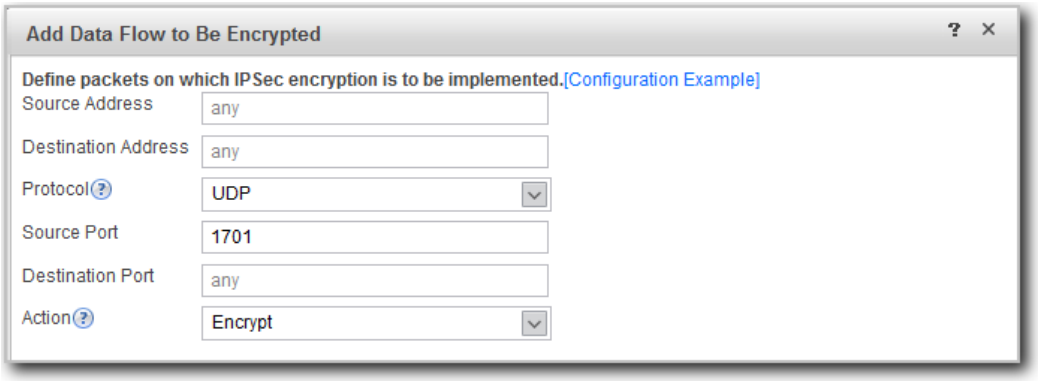
b. Establecer un grupo de IP.

Anterior



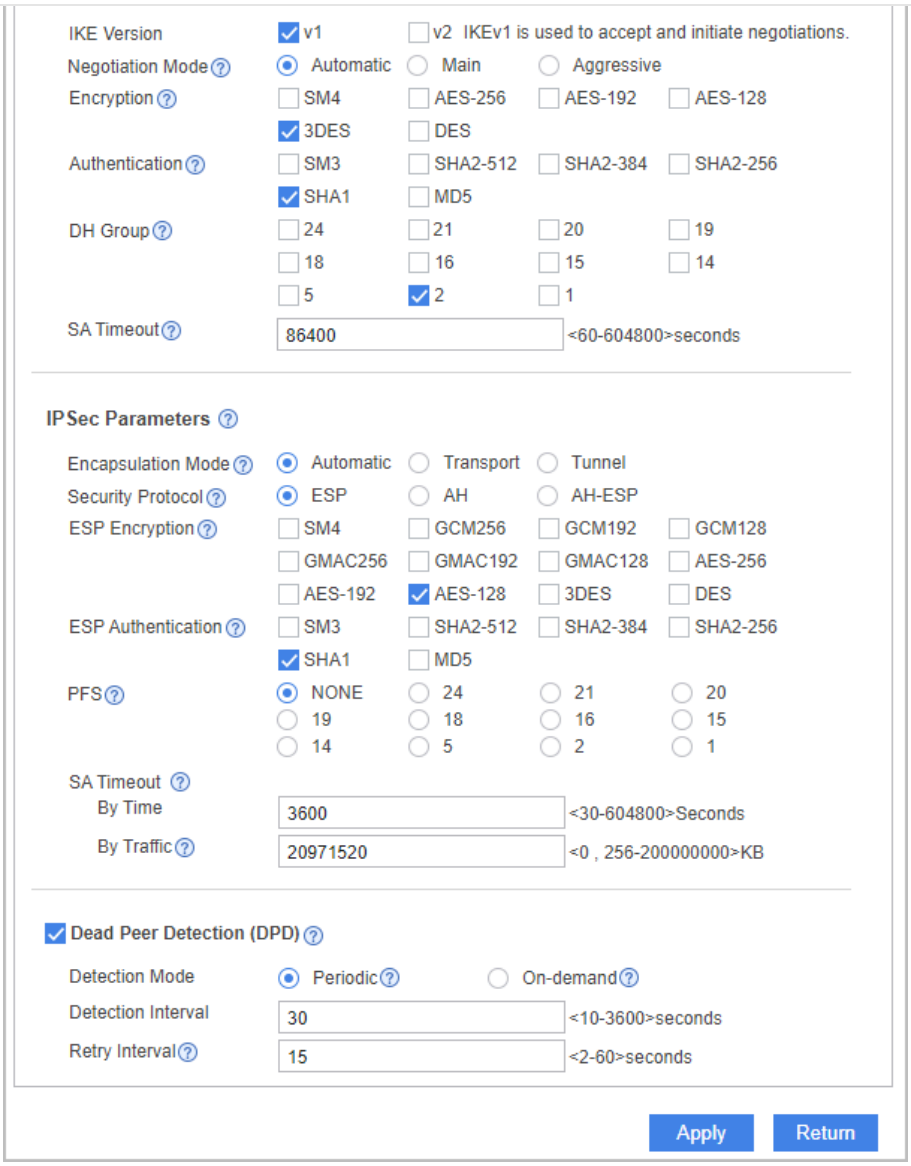
c. Haga clic en **Aceptar** .

e. En **Flujo de datos a cifrar** , haga clic en **Agregar** para agregar un flujo de datos de la siguiente manera.



f. Configurar el protocolo IKE e IPSec.

Anterior



g. Haga clic **en Aplicar** para completar las configuraciones.

e. El cliente LAC utiliza el cliente L2TP integrado para acceder por línea telefónica. No se admite la verificación de túnel. Por lo tanto, firewall .

a. Seleccione **Red** > **L2TP** > **L2TP** . En **la Lista de grupos L2TP** , haga clic en **default-lns** y desmarque **la opción "Autenticación c** Configure la **Zona asociada** como **"untrust"** .

b. Haga clic en **Aceptar** .

2. Configurar una ruta en el servidor HQ.

   Para comunicarse con empleados móviles, el servidor HQ debe tener una ruta al grupo de direcciones de usuarios, con el siguiente sal dirección de la interfaz LAN del FW .

3. Establecer parámetros de acceso telefónico en el cliente LAC.

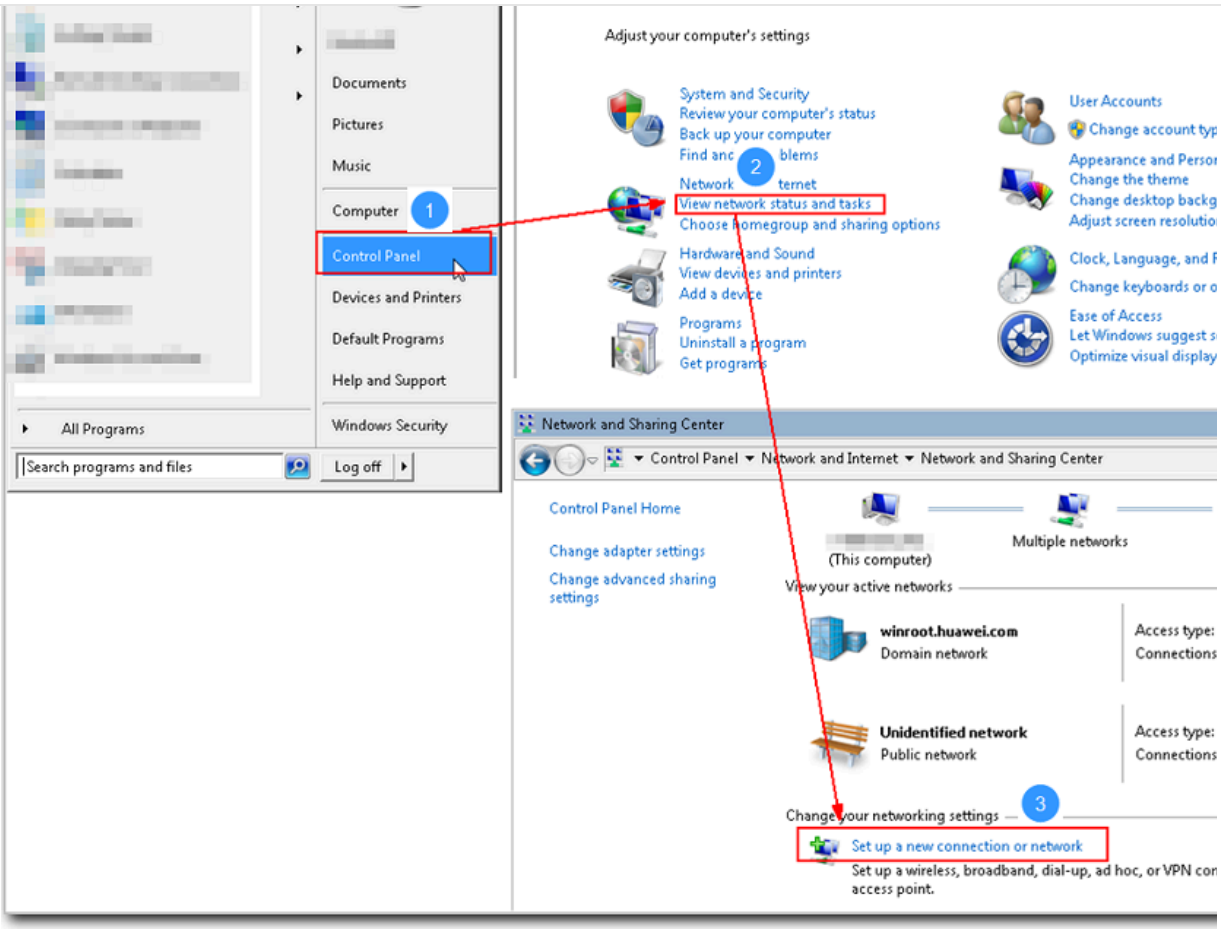
   a. Vea el estado del servicio IPSec y asegúrese de que esté habilitado.

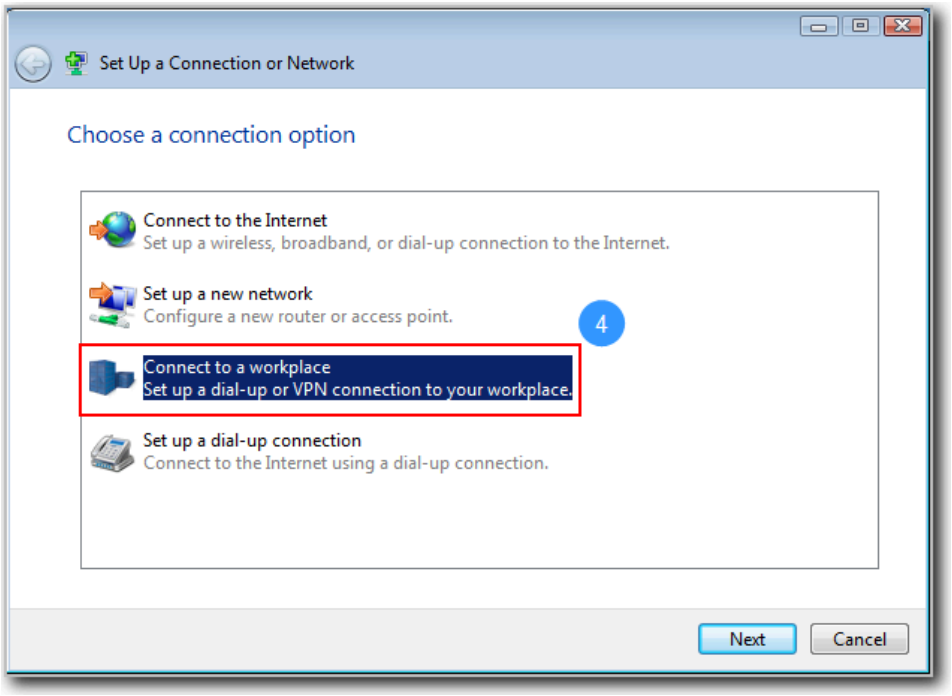
   a. Seleccione **Inicio** > **Ejecutar** , ingrese **services.msc** y haga clic en **Aceptar** para acceder a la página **Servicios** .

   b. En la columna **Nombre** , revise el estado **del Agente de Políticas IPsec para asegurarse de que esté en estado Iniciado** . De lc el botón derecho **en Agente de Políticas IPsec** y seleccione **Propiedades** . En **Propiedades** , configure **Tipo de inicio** como **Aut Aplicar** . Luego, seleccione **Iniciar** en **Tipo de servicio** .

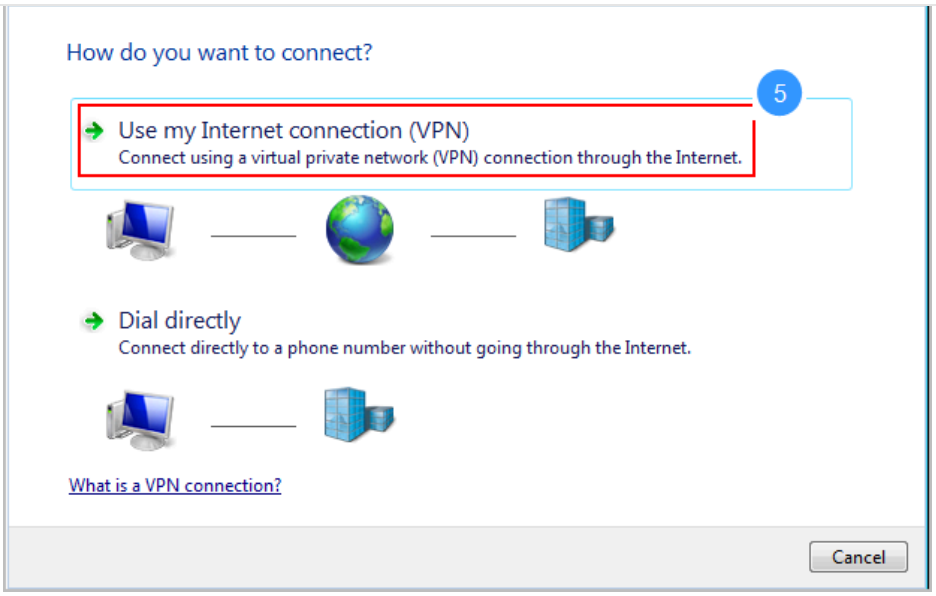
   c. Cerrar la página de **Servicios** .

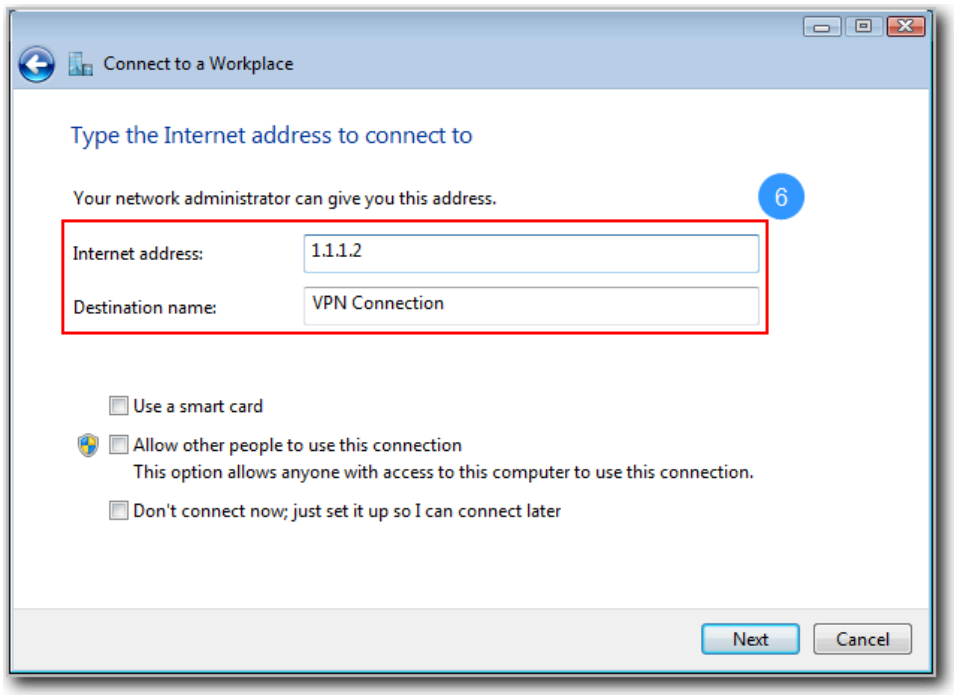
Anterior


Documents
Pictures
Music
Computer
1
Control Panel
Devices and Printers
Default Programs
Help and Support
All Programs
Windows Security
Search programs and files
Log off
Adjust your computer's settings
System and Security
Review your computer's status
Back up your computer
Network
2
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
Get programs
User Accounts
Change the theme
Change desktop backg
Adjust screen resolutio
Clock, Language, and
Change keyboards or o
Ease of Access
Let Windows suggest s
Optimize visual display
Network and Sharing Center
Control Panel ▸ Network and Internet ▸ Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
(This computer)
Multiple networks
View your active networks
winroot.huawei.com
Domain network
Access type:
Connections
Unidentified network
Public network
Access type:
Connections
Change your networking settings
3
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN con
access point.

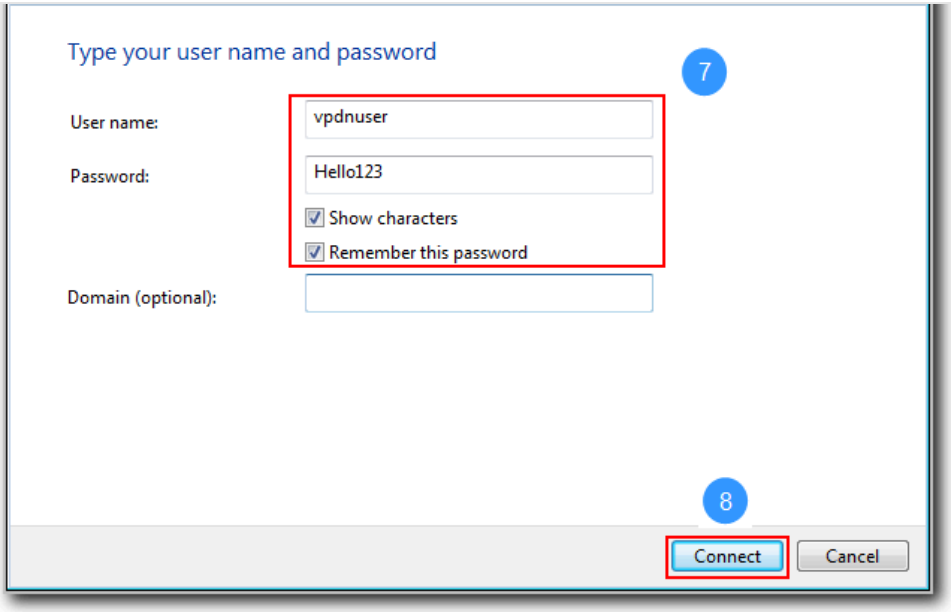

Set Up a Connection or Network
Choose a connection option
Connect to the Internet
Set up a wireless, broadband, or dial-up connection to the Internet.
Set up a new network
Configure a new router or access point.
4
Connect to a workplace
Set up a dial-up or VPN connection to your workplace.
Set up a dial-up connection
Connect to the Internet using a dial-up connection.
Next
Cancel

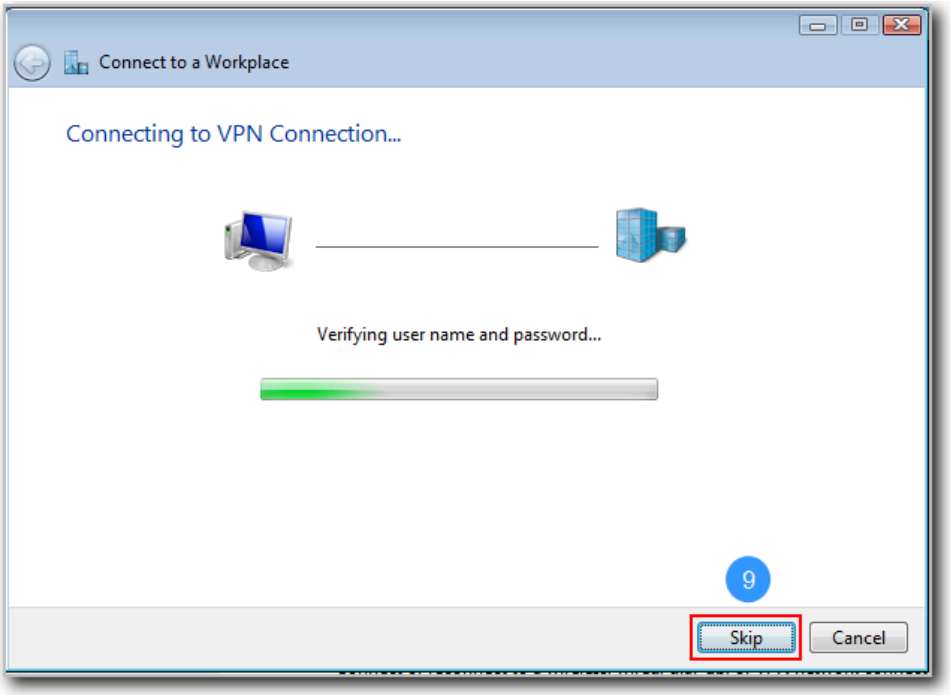
Anterior


How do you want to connect?
5
Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.
Dial directly
Connect directly to a phone number without going through the Internet.
What is a VPN connection?
Cancel

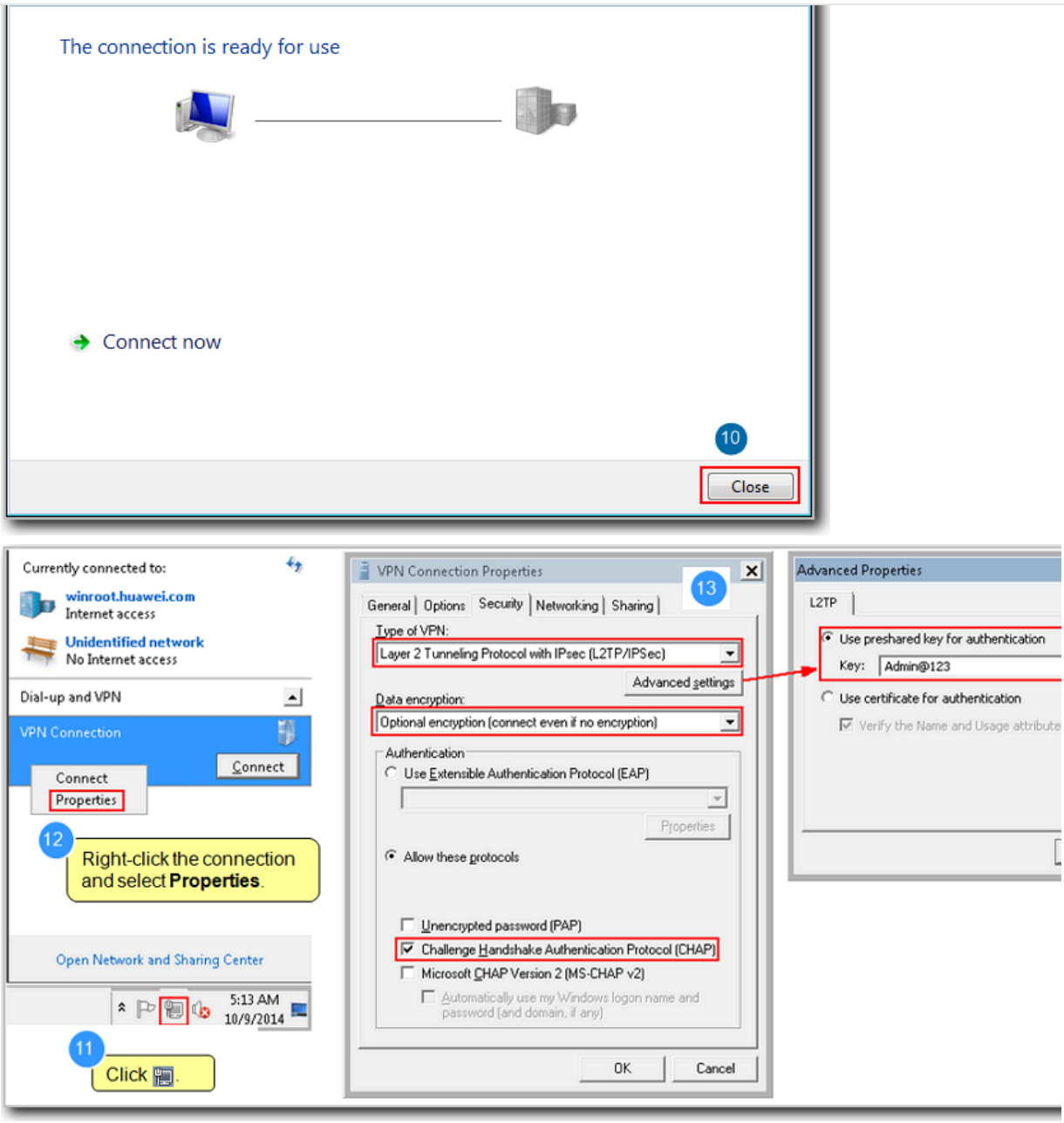

Connect to a Workplace
Type the Internet address to connect to
Your network administrator can give you this address.
6
Internet address:
1.1.1.2
Destination name:
VPN Connection
Use a smart card
Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.
Don't connect now; just set it up so I can connect later
Next
Cancel

Anterior


Type your user name and password
7
User name:
vpdnuser
Password:
Hello123
Show characters
Remember this password
Domain (optional):
8
Connect
Cancel


Connect to a Workplace
Connecting to VPN Connection...
Verifying user name and password...
9
Skip
Cancel

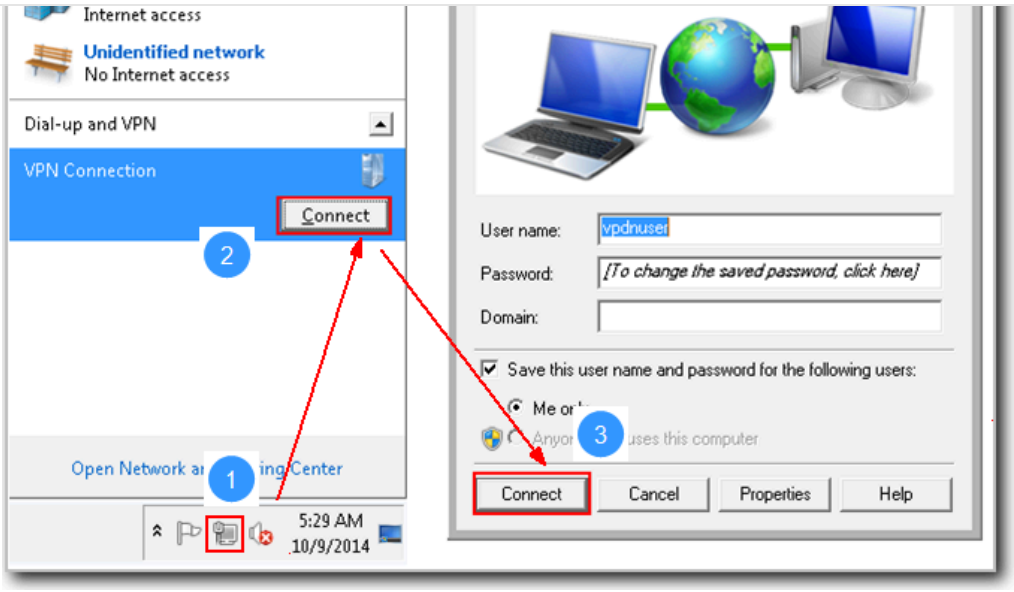
Anterior



Verificación de la configuración

1. El cliente LAC logra conectarse mediante el software integrado.

Anterior

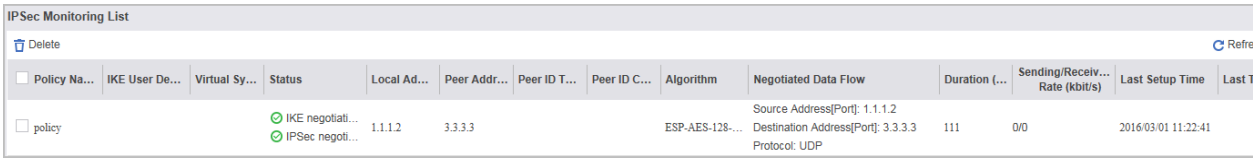


2. En el LAC, puede ver que el rango de direcciones 10.1.1.2/24-10.1.1.100/24 está asignado al LAC y los empleados móviles pueden ac

3. Después de que el LAC se conecta, verifique si el túnel L2TP está establecido en el LNS.



4. Compruebe el establecimiento del túnel IPSec en el LNS. Si se muestra la siguiente información, el túnel IPSec está establecido.



Scripts de configuración

Sobre nosotros
Cómo comprar
Pareja
Recursos
Enlaces rápidos

Aplicación Huawei e+
Aplicación HUAWEI eKit
Aplicación Huawei HiKnow
Aplicación HUAWEI eFly

Anterior

Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

Privacidad Condiciones de uso Galletas Configuración de cookies Reportar contenido

```
interfaz GigabitEthernet1/0/1
 dirección IP 1.1.1.2 255.255.255.0
 Política IPsec ipsec9116572166
#
interfaz GigabitEthernet1/0/3
 dirección IP 192.168.1.1 255.255.255.0
#
Interfaz Virtual-Template1
 modo de autenticación ppp chap pap
 esquema de servicio remoto l2tpSScheme_1445251722019
 dirección IP 10.1.1.2 255.255.255.0
 alias L2TP_LNS_0
#
confianza de la zona de firewall
 establecer prioridad 85
 agregar interfaz GigabitEthernet1/0/3
#
zona de firewall no confiable
 establecer prioridad 5
 agregar interfaz GigabitEthernet1/0/1
 agregar interfaz Virtual-Template1
#
l2tp-group predeterminado-lns
 permitir l2tp plantilla virtual 1
 deshacer la autenticación del túnel
#
grupo de direcciones IP grupo1
 Sección 1 10.1.1.2 10.1.1.100
#
aaa
 esquema de autenticación predeterminado
  modo de autenticación local
 #
 dominio predeterminado
  esquema de autenticación predeterminado
  esquema de servicio l2tp
#
política de seguridad
 nombre de la regla policy_ipsec_1
  confianza en la zona de origen
  desconfianza en la zona de destino
  dirección de origen 192.168.1.0 24
  rango de direcciones de destino 10.1.1.2 10.1.1.100
  permiso de acción
 nombre de la regla policy_ipsec_2
  desconfianza en la zona de origen
  confianza en la zona de destino
  rango de direcciones de origen 10.1.1.2 10.1.1.100
  dirección de destino 192.168.1.0 24
  permiso de acción
 nombre de la regla policy_ipsec_3
  desconfianza en la zona de origen
```

Anterior

```
  zona de origen local
  desconfianza en la zona de destino
  dirección de origen 1.1.1.2 32
  permiso de acción
# La siguiente configuración de creación de usuarios/grupos se almacena en la base de datos, pero no en el perf
usuario-administrar usuario vpdnuser dominio predeterminado
 contraseña *********
```

REFERENCIAS TECNICAS

INGLES

Limiting the ASPFALG

Size: 264.12MB

Enter keywords 0 / 256

Limiting the ASPF/ALG Processing Range of Stun Protocol Traffic

Context

The device allows you to use the CLI to configure whether to permit packets matching the STUN server map table.

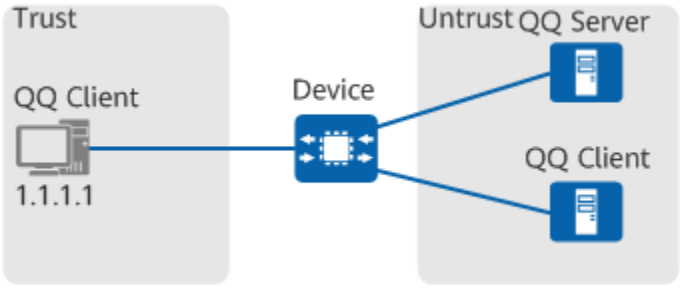
Generating server map entries through ASPF/ALG has fewer restrictions on the 5-Tuple session information. Some ports become available during packet forwarding, which causes security risks. Therefore, when the user-defined ASPF/ALG function is configured, the ACL rules for matching traffic shall be as accurate as possible. For packets that have server map entries created, although the device does not perform security policy-based check on the packets, the forwarding of certain packets can be blocked through configuration.

NOTE

This function applies only to STUN protocols, such as QQ (an instant messaging software service developed by the Chinese tech giant Tencent), MSN, and user-defined protocols.

The following describes how to disable the communication between user 1.1.1.1 in the Trust zone and QQ in the Untrust zone.

Figure 1 Networking diagram of QQ communication



Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Limiting the ASPFALG

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Limitación del rango de procesamiento ASPF/ALG del tráfico del protocolo Stun

Contexto

El dispositivo le permite utilizar la CLI para configurar si se permiten paquetes que coincidan con la tabla de mapas del servidor STUN.

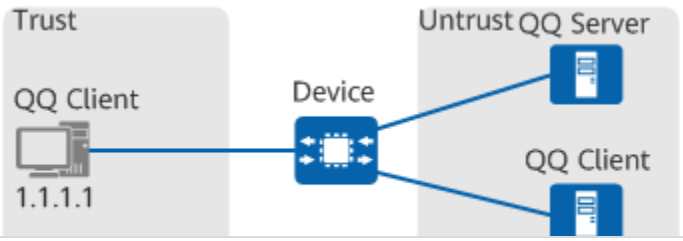
La generación de entradas de mapa de servidor mediante ASPF/ALG presenta menos restricciones en la información de sesión de 5-Tuplas. Algunos puertos se liberan durante el reenvío de paquetes, lo que genera riesgos de seguridad. Por lo tanto, al configurar la función ASPF/ALG definida por el usuario, las reglas de ACL para la coincidencia de tráfico deben ser lo más precisas posible. En el caso de los paquetes con entradas de mapa de servidor creadas, aunque el dispositivo no realiza una comprobación basada en políticas de seguridad, el reenvío de ciertos paquetes puede bloquearse mediante la configuración.

NOTE

Esta función se aplica únicamente a los protocolos STUN, como QQ (un servicio de software de mensajería instantánea desarrollado por el gigante tecnológico chino Tencent), MSN y protocolos definidos por el usuario.

A continuación se describe cómo deshabilitar la comunicación entre el usuario 1.1.1.1 en la zona de confianza y QQ en la zona de no confianza.

Figura 1 Diagrama de red de comunicación QQ



Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

REFERENCIAS TECNICAS

INGLES

NAT Dynamic

Size: 264.12MB

Enter keywords 0 / 256

HiSecEngine USG6000F Product Documentation ...

Configuration Examples for NAT Bidirectional NAT

Examples for Configuring Bidirectional NAT (Source NAT + Destination NAT)

3955 /23582

Example for Configuring Bidirectional NAT (Source NAT + Dynamic Destination NAT) for Internet Users to Access Intranet Servers

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Dynamic destination NAT needs to be configured on DeviceA to prevent a large number of Internet users from accessing a specific server. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained another public IP address (1.1.10.10) from the ISP, which is used by intranet servers to provide services to Internet users. A source NAT policy is required so that intranet servers can send response packets to DeviceA, removing the need to configure return routes for intranet servers. Figure 1 shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 1 Network diagram of bidirectional NAT (source NAT + dynamic destination NAT) allowing Internet users to access intranet servers

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



We use cookies on this site, in order for the site to work properly and to analyse traffic, offer enhanced functionality and personalise content.Learn more

cookie settings

Accept Cookies

Reject Cookies

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

NAT Dynamic

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Ejemplo de configuración de NAT bidireccional (NAT de origen + NAT de destino dinámico) para que los usuarios de Internet accedan a servidores de intranet

Requisitos de red

Una empresa ha implementado el Dispositivo A como puerta de enlace de seguridad en el límite de la intranet. Es necesario configurar una NAT de destino dinámica en el Dispositivo A para evitar que un gran número de usuarios de Internet accedan a un servidor específico. Además de la dirección IP pública de la interfaz WAN del Dispositivo A, la empresa ha obtenido otra dirección IP pública (1.1.10.10) del ISP, que utilizan los servidores de la intranet para prestar servicios a los usuarios de Internet. Se requiere una política de NAT de origen para que los servidores de la intranet puedan enviar paquetes de respuesta al Dispositivo A, eliminando así la necesidad de configurar rutas de retorno para los servidores de la intranet. La Figura 1 muestra el diagrama de red, en el que el router es la puerta de enlace de acceso proporcionada por el ISP.

Figura 1 Diagrama de red de NAT bidireccional (NAT de origen + NAT de destino dinámico) que permite a los usuarios de Internet acceder a servidores de intranet

NOTE

En este ejemplo, las interfaces 1 y 2 representan GE 0/0/1 y GE 0/0/2 , respectivamente.

Utilizamos cookies en este sitio para su correcto funcionamiento, analizar el tráfico, ofrecer una mejor funcionalidad y personalizar el contenido. Más información

configuración de cookies

Aceptar cookies

Rechazar cookies

REFERENCIAS TECNICAS

INGLES

NAT Static

Size: 264.12MB

Enter keywords 0 / 256

Example for Configuring Bidirectional NAT (Source NAT + Static Destination NAT) for Internet Users to Access Intranet Servers

Networking Requirements

An enterprise has deployed DeviceA as a security gateway at the intranet border. Destination NAT needs to be configured on DeviceA so that the web and FTP servers on the enterprise's private network can provide services to Internet users. In addition to the public IP address of the WAN interface on DeviceA, the enterprise has obtained public IP addresses 1.1.10.10 and 1.1.10.11 from the ISP, which are used by the intranet servers to provide services to Internet users. A source NAT policy is also required to enable intranet servers to send response packets to DeviceA, removing the need to configure return routes for intranet servers. Figure 1 shows the network diagram, in which the router is the access gateway provided by the ISP.

Figure 1 Network diagram of bidirectional NAT (source NAT + static destination NAT) allowing Internet users to access intranet servers

NOTE

In this example, interfaces 1 and 2 represent GE 0/0/1 and GE 0/0/2, respectively.



We use cookies on this site, in order for the site to work properly and to analyse traffic, offer enhanced functionality and personalise content.Learn more

cookie settings

Accept Cookies

Reject Cookies

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

NAT Static

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Ejemplo de configuración de NAT bidireccional (NAT de origen + NAT de destino estático) para que los usuarios de Internet accedan a servidores de intranet

Requisitos de red

Una empresa ha implementado el Dispositivo A como puerta de enlace de seguridad en el límite de la intranet. Es necesario configurar la NAT de destino en el Dispositivo A para que los servidores web y FTP de la red privada de la empresa puedan prestar servicios a los usuarios de Internet. Además de la dirección IP pública de la interfaz WAN del Dispositivo A, la empresa ha obtenido las direcciones IP públicas 1.1.10.10 y 1.1.10.11 del ISP, que utilizan los servidores de la intranet para prestar servicios a los usuarios de Internet. También se requiere una política de NAT de origen para que los servidores de la intranet puedan enviar paquetes de respuesta al Dispositivo A, eliminando así la necesidad de configurar rutas de retorno para los servidores de la intranet. La Figura 1 muestra el diagrama de red, en el que el router es la puerta de enlace de acceso proporcionada por el ISP.

Figura 1 Diagrama de red de NAT bidireccional (NAT de origen + NAT de destino estático) que permite a los usuarios de Internet acceder a servidores de intranet

NOTE

En este ejemplo, las interfaces 1 y 2 representan GE 0/0/1 y GE 0/0/2 , respectivamente.

Utilizamos cookies en este sitio para su correcto funcionamiento, analizar el tráfico, ofrecer una mejor funcionalidad y personalizar el contenido. Más información

configuración de cookies

Aceptar cookies

Rechazar cookies

REFERENCIAS TECNICAS

INGLES

NATALG

Conoce la función de NAT ALG en los firewalls de Huawei

Destacado

Publicado 2019-1-21 17:30:40 Última respuesta nov. 27, 2020 20:38:12 1132 6 4 1

Ver publicación original 1#

71 26

Seguir Ch

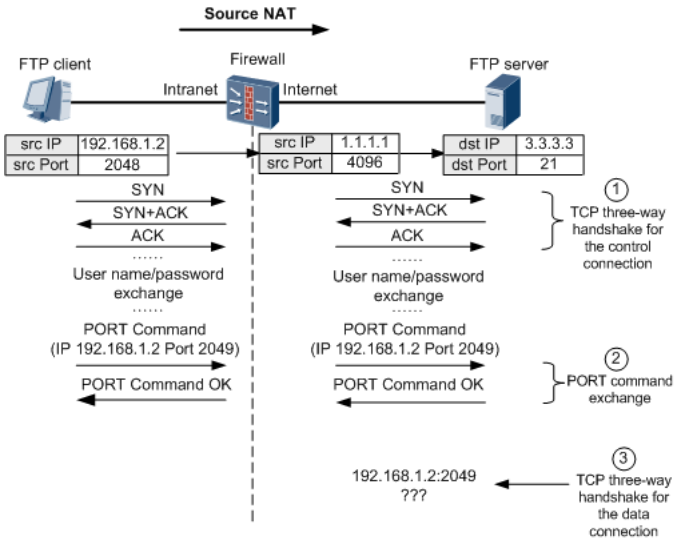
Publicar

En las secciones anteriores, he introducido **Source NAT** y **NAT Server** y **NAT bidireccional** soportado por **firewalls.**
Estas funciones NAT se pueden utilizar de forma flexible en diferentes escenarios.

Como sabemos, NAT sólo traduce las direcciones en los encabezados. Para algunos protocolos, como **FTP**, las cargas útiles de paquetes también llevan información de direcciones. Si los firewalls no pueden procesar correctamente dicha información, FTP puede no funcionar correctamente. Bueno, ¿cómo deberían los cortafuegos procesar paquetes de protocolo?

1. **FTP Packets Traversing NAT Devices.**
Usemos FTP como ejemplo para ver qué problemas ocurren cuando los paquetes FTP intentan pasar a través de dispositivos NAT.
En este ejemplo, un cliente FTP reside en una intranet, y un servidor FTP reside en Internet. FTP funciona en modo activo.
La Figura 1-1 muestra el proceso de interacción FTP en el dispositivo NAT.

Figura 1-1 Proceso de interacción FTP 1 cuando la fuente NAT es configured



Podemos ver que después de establecer una conexión de control entre el **cliente FTP** y el servidor, el cliente envía un paquete de comandos PORT al servidor, y el paquete contiene la dirección privada y el puerto del cliente.

El firewall envía directamente el paquete al servidor. Después de recibir el paquete, el servidor FTP inicia una conexión de datos a 192.168.1.2 según las instrucciones del comando PORT.

El problema es incurrido. 192.168.1.2 es una dirección privada. Los paquetes destinados a esta dirección no pueden transmitirse en Internet. Como resultado, el servicio FTP es anormal.

¿Qué debería hacer el firewall para resolver el problema?
Si el firewall traduce tanto la dirección de origen en la cabecera como la dirección IP en la información de la capa de aplicación en la carga útil, se puede establecer la conexión de datos.

El Gateway de Nivel de Aplicaciones NAT (la función ALG) resuelve el problema.

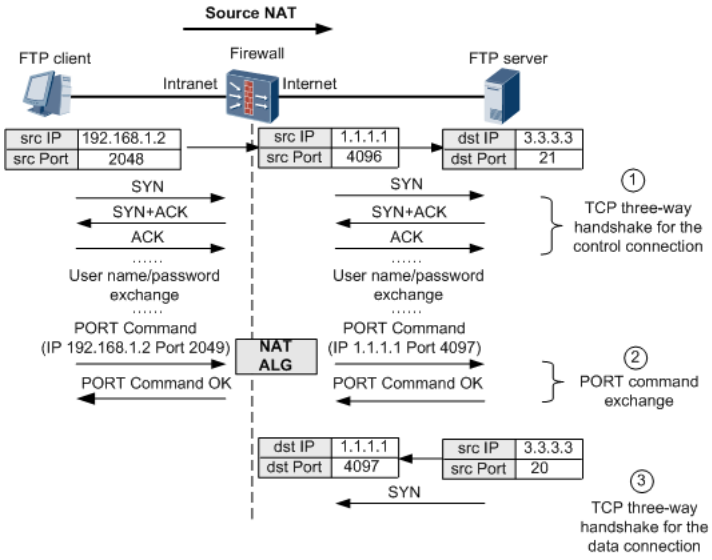
Como técnica para ayudar a los paquetes que atraviesan cortafuegos, el NAT ALG permite que un firewall traduzca las direcciones IP tanto en encabezados como en cargas útiles.

La Figura 1-2 muestra el proceso de interacción FTP después de habilitar el ALG NAT en el firewall.

Figura 1-2 Pr

Utilizamos cookies en este sitio, incluyendo cookies de terceros, para que el sitio funcione correctamente y para analizar el tráfico, ofrecer una funcionalidad mejorada, características de redes sociales y personalizar el contenido y los ads. aprender másMás información

configuración de cookies Aceptar cookies



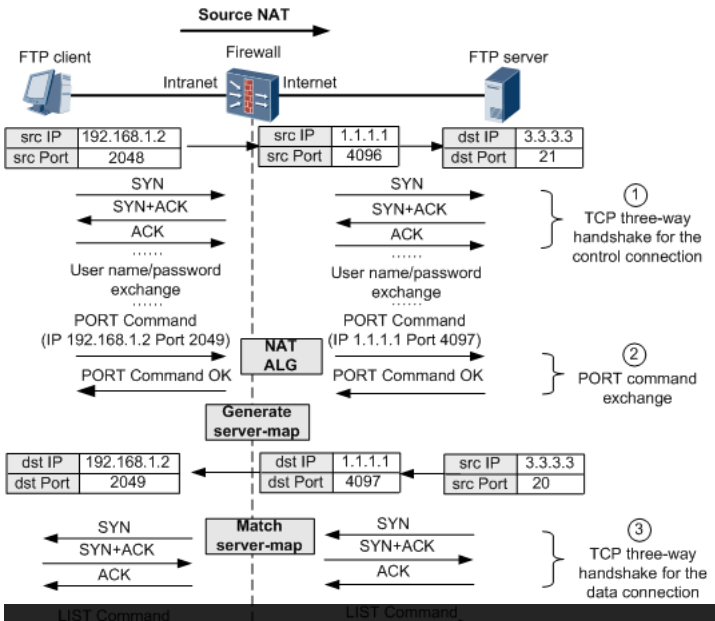
Una vez habilitado el NAT ALG, el firewall traduce la dirección IP transportada en la carga útil del paquete de comandos PORT a la dirección pública 1.1.1.1. Después de recibir el paquete, el servidor FTP inicia una conexión de datos a 1.1.1.1

Puede que tengas otra pregunta. ¿Puede el firewall permitir la solicitud de conexión incluso si el servidor FTP puede iniciar la solicitud de conexión?
Esta pregunta es tan familiar. ¿Cierto?Para encontrar la respuesta, volvamos a la función ASPF en el capítulo 2 "Política de seguridad".
Después de habilitar ASPF, el firewall abre un canal invisible para que los datos de FTP eviten las verificaciones de la política de seguridad, atravesando el cortafuegos. El servicio FTP requiere ASPF en escenarios NAT. En realidad, NAT ALG y ASPF se implementan utilizando un comando. Enabling NAT ALG también cuenta con ASPF habilitado. Por lo tanto, después de habilitar NAT ALG, se genera la siguiente entrada del mapa del servidor:

```
Type: ASPF,  3.3.3.3 -> 1.1.1.1:24576[192.168.1.2:55177],  Zone:---
 Protocol: tcp(Appro: ftp-data),  Left-Time:00:00:03,  Pool: ---
 Vpn: public -> public
```

Esta entrada del mapa del servidor tiene información de traducción de direcciones. Antes de que expire el tiempo de envejecimiento, esta entrada ayuda a que el paquete de solicitud de conexión de datos del servidor FTP atraviese el cortafuegos y llegue con precisión al cliente FTP de la intranet. La Figura 1-3 muestra el proceso completo de interacción FTP.

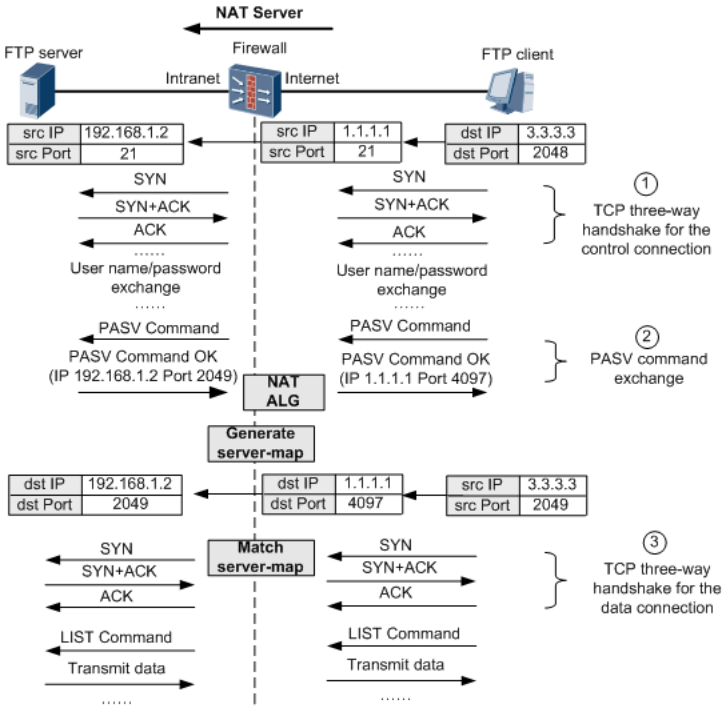
Figura 1-3 Proceso de interacción FTP 3 cuando se configura Source NAT



Utilizamos cookies en este sitio, incluyendo cookies de terceros, para que el sitio funcione correctamente y para analizar el tráfico, ofrecer una funcionalidad mejorada, características de redes sociales y personalizar el contenido y los ads. aprender másMás información
> configuración de cookies
Aceptar cookies

Además del escenario NAT de origen, el escenario NAT Server requiere ALG y ASPF de NAT. En este ejemplo, un cliente FTP reside en Internet, y un servidor FTP reside en una intranet. FTP funciona en modo pasivo. La Figura 1-4 muestra el proceso completo de interacción FTP.

Figura 1-4 Proceso de interacción FTP cuando se configura NAT Server



Las siguientes entradas del server-map se generan en el firewall:

```
[FW] display firewall server-map
server-map item(s)
 --------------------------------------------------------------------------------
 Nat Server, any -> 1.1.1.1:21[192.168.1.2:21], Zone: ---
   Protocol: tcp(Appro: ftp), Left-Time: --:--:--, Addr-Pool: ---
   VPN: public -> public

 Nat Server Reverse, 192.168.1.2[1.1.1.1] -> any, Zone: ---
   Protocol: any(Appro: ---), Left-Time: --:--:--, Addr-Pool: ---
   VPN: public -> public

 ASPF, 3.3.3.3 -> 1.1.1.1:4097[192.168.1.2:2049], Zone: ---
   Protocol: tcp(Appro: ftp-data), Left-Time: 00:00:53, Addr-Pool: ---
   VPN: public -> public
```

El paquete de conexión de control iniciado por el cliente FTP coincide con la entrada del mapa del servidor hacia adelante para NAT Server y se traduce la dirección. El paquete de conexión de datos iniciado por el cliente FTP coincide con la entrada del mapa del servidor para ASPF y se traduce la dirección.

En conclusión, si se utilizan protocolos multicanal tales como FTP, SIP y H.323 y NAT se aplica en una red, se recomienda tanto NAT ALG como ASPF en el firewall, para que los protocolos puedan funcionar correctamente.

2. **Paquetes de protocolo definidos por el usuario QQ/MSN/que atraviesan dispositivos NAT**
También mencionamos QQ y MSN, y protocolos definidos por el usuario en "Security Policy". Firewalls clasifica estos protocolos en un tipo: "STUN". STUN es corto para Simple Traversal of UDP Through Network Address Translators que es un modo de transversal NAT. A diferencia de ALG NAT, el STUN no necesita ningún procesamiento en dispositivos NAT. En cambio, el cliente STUN en una intranet obtiene su dirección pública a través de intercambios de información entre el cliente STUN y el servidor. Luego, el cliente agrega la dirección pública en la carga útil y envía el paquete. De esta manera, el servidor en Internet obtiene la dirección pública del cliente desde la carga útil e inicia una solicitud de conexión al cliente.

Los protocolos STUN son responsables de su funcionamiento durante la traducción de direcciones. Por lo tanto, no se requiere NAT ALG para estos protocolos. Sin embargo, todavía tenemos que considerar cómo hacer que sus paquetes de servicios pasen a través del firewall. La solución también es ASPF Después de un paquete m

El TFTP se utiliza como ejemplo. La siguiente parte proporciona una entrada de mapa de servidor ASPF para el protocolo definido por el usuario en un escenario NAT (las entradas del servidor-mapa generadas para QQ y MSN son similares

```
Type: STUN,   ANY -> 1.1.1.1:4096[192.168.1.2:63212],   Zone:---
```

Utilizamos cookies en este sitio, incluyendo cookies de terceros, para que el sitio funcione correctamente y para analizar el tráfico, ofrecer una funcionalidad mejorada, características de redes sociales y personalizar el contenido y los ads. aprender másMás información
configuración de cookies
Aceptar cookies

```
 Protocol: udp(Appro: stun-derived),  Left-Time:00:04:58,  Pool: 1, Section: 0
 Vpn: public -> public
 Type: STUN Reverse,  192.168.1.2:63212[1.1.1.1:4096] -> ANY,  Zone:---
 Protocol: udp(Appro: stun-derived),  Left-Time:00:04:58,  Pool: 1, Section: 0
 Vpn: public -> public
```

A diferencia de las entradas generadas en escenarios no NAT, estas entradas contienen información de traducción de direcciones. Además, se generan dos entradas del mapa del servidor. La entrada con el Tipo ser STUN es la entrada avanzada, mientras que la entrada con el Tipo ser STUN Reverse es la entrada inversa.

Antes de que expire el tiempo de envejecimiento, la entrada avanzada ayuda a la solicitud de conexión iniciada por el servidor TFTP atravesar el firewall y llegar con precisión al cliente TFTP en la intranet; la entrada inversa ayuda al firewall a traducir la dirección y el puerto (63212). Esta implementación garantiza que una aplicación específica (identificada por el número de puerto) para un usuario de intranet se presente utilizando la dirección pública fija y el puerto, asegurando el funcionamiento normal de los servicios TFTP.

3. **Un comando que controla dos funciones**
En los firewalls de Huawei, se controlan ASPF y NAT ALG utilizando comandos separados. En la actualidad, la mayoría de los firewalls utilizan un comando para controlar estas dos funciones. Para ser específico, el comando detect se puede utilizar en la vista Intrazone o interzona para habilitar ASPF Luego, el ALG de NAT se activa automáticamente.

El firewall determina el uso del ALG de NAT, el ASPF o ambos según sea necesario. Lo que debemos hacer es sólo ejecutar el comando, reduciendo la carga de trabajo de configuración.

Especifica los protocolos típicos, la Tabla 1-1 enumera los modos de procesamiento del firewall después de utilizar el comando detect.

Tabla 1-1 Modos de procesamiento para protocolos típicos

Typical Protocol	NAT Scenario or Not	Effective Function	Effect
FTP SIP H323	Non-NAT scenario	ASPF	Server-map entries are generated to help the packets from other hosts to FTP, SIP, and H.323 hosts traverse the firewall.
	NAT scenario	NAT ALG	The IP addresses in payloads are translated.
		ASPF	Server-map entries (with address translation information) are generated to help the packets from other hosts on the Internet to FTP, SIP, and H.323 hosts on an intranet traverse the firewall.
QQ MSN User-defined	Non-NAT scenario	ASPF	Triplet server-map entries are generated to help the packets from other hosts to QQ, MSN, and user-defined hosts traverse the firewall.
	NAT scenario	ASPF	Triplet server-map entries (with address translation information) are generated to help the packets from other hosts on the Internet to QQ, MSN, and user-defined hosts on an intranet traverse the firewall.

Como se indica en la tabla anterior, el ASPF genera una entrada triplet server-map para un protocolo definido por el usuario en el escenario NAT. También mencionamos a Triplet NAT en la sección 4.1.6 Triplet NAT. ¿Cuál es la diferencia entre ellos?

4. **Diferencias entre ASPF para protocolos definidos por el usuario y Triplet NAT**
Triplet NAT permite la coexistencia de P2P y NAT. Cuando un host de intranet accede a Internet, se establece un sistema de red asimétrico después de que NAT se realiza en un firewall. Esto significa que el host de intranet puede acceder a Internet, pero los usuarios de Internet no pueden iniciar el acceso al host de la intranet.

Después de la implementación de triplet NAT, el firewall genera una entrada del servidor-mapa para permitir que los paquetes de un usuario de Internet al usuario de la intranet atraviesen el firewall. De esta manera, las aplicaciones basadas en P2P como el intercambio de archivos, las comunicaciones de voz y la transmisión de vídeo pueden ejecutarse correctamente en escenarios NAT.

El mapa del servidor para el triple NAT contiene las entradas de origen (forward) y destino (inversa).

```
Type: FullCone Src,  192.168.1.2:51451[1.1.1.1:2048] -> ANY,  Zone:---
 Protocol: tcp(Appro: ---),  Left-Time:00:00:57,  Pool: 1, Section: 0
 Vpn: public -> public
 Type: FullCone Dst,  ANY -> 1.1.1.1:2048[192.168.1.2:51451],  Zone:---
 Protocol: tcp(Appro: ---),  Left-Time:00:00:57,  Pool: 1, Section: 0
 Vpn: public -> public
```

En el ejemplo anterior, la entrada marcada FullCone Src es la entrada del servidor-mapa de origen. Antes de que expire el tiempo de envejecimiento, las direcciones de los paquetes que el host de intranet inicia utilizando el puerto específico (51451) a Internet se traducen a la dirección pública (1.1.1.1) y el puerto (2048). Esta implementación garantiza que una aplicación específica (identificada por el número de puerto) para un usuario de la intranet se presente utilizando la dirección pública fija y el puerto, asegurando el funcionamiento normal de los servicios P2P.

Utilizamos cookies en este sitio, incluyendo cookies de terceros, para que el sitio funcione correctamente y para analizar el tráfico, ofrecer una funcionalidad mejorada, características de redes sociales y personalizar el contenido y los ads. aprender más Más información
> configuración de cookies
Aceptar cookies

La entrada marcada FullCone Dst es la entrada del servidor-mapa de destino. Antes de que expire el tiempo de envejecimiento, los usuarios de Internet pueden iniciar el acceso al usuario de intranet especificado.

Si comparamos estas entradas del mapa del servidor con las entradas triplet server-map que ASPF genera para los protocolos definidos por user en los escenarios NAT, podemos encontrar que dos entradas del mapa del servidor se generan en ambas condiciones, incluyendo la dirección, el puerto y la información del protocolo. El procesamiento de ASPF para protocolos definidos por el usuario en escenarios NAT puede considerarse como una implementación NAT especial de triplet. Ambas técnicas permiten que los paquetes P2P atraviesen cortafuegos.

Vamos a ver su diferencia. ASPF se aplica tanto a los escenarios NAT como no -NAT. En los escenarios no -NAT, el mapa del servidor de triplet entries no lleva información de traducción de direcciones. En los escenarios NAT, las entradas triplet server-map llevan información de traducción de direcciones. Como modo NAT, triplet NAT sólo funciona en escenarios NAT, y sus entradas de mapa de servidores llevan información de traducción de direcciones.

Otra diferencia importante es que después de que un paquete coincida con una entrada de mapa de servidor de tripleta ASPF, el firewall permite que el paquete pase a través de las políticas de seguridad (el comando aspf packet-filter acl-number {inbound by outbound} en la vista interzone. Si esta función está habilitada, el firewall no verifica el paquete. Si esta función está deshabilitada, el firewall comprueba el paquete.

Desde la perspectiva de la configuración, la configuración de ASPF para un protocolo definido por el usuario requiere la familiaridad de las características del protocolo para la definición exacta de ACL. Una configuración incorrecta puede hacer que el protocolo no pueda funcionar o afectar el funcionamiento normal de otros servicios. En comparación con la configuración ASPF, la configuración NAT de triplet es más sencilla. Lo que debemos hacer es configurar una política NAT y especificar el modo de pool de direcciones para triplet NAT (full-cone).

Sus condiciones de soporte en los firewalls de Huawei también difieren. La serie USG9500 soporta tanto ASPF para protocolos definidos por el usuario como NAT de triplet; la serie USG2000/5000/6000 soporta sólo ASPF para protocolos usuario defined. Cuando existen aplicaciones NAT y P2P en una red, se recomienda configurar el NAT triplet en la serie USG9500 o ASPF para los protocolos definidos por el usuario en la serie USG2000/5000/6000 para el funcionamiento normal de los servicios P2P.

Tabla 1-2 Lista de comparación entre ASPF para protocolos definidos por el usuario y el triplete NAT.

Item	ASPF for User-defined Protocols	Triplet NAT
Server-map entry elements	Triplet Including the address, port, and protocol type	Triplet Including the address, port, and protocol type
Number of server-map entries	Two Including the forward and reverse entries	Two Including the source and destination entries
Operating environment	NAT and non-NAT scenarios	NAT scenario
Impact on security policies	The packets matching ASPF server-map entries are not controlled by security policies.	A specific command setting determines whether the packets matching triplet NAT server-map entries are controlled by security policies.
Configuration requirement	ACL rules must be accurately defined.	The NAT address pool must be set to the full-cone mode.
Support condition	Supported by the USG2000/5000/6000/9500 series	Supported only by the USG9500

Saludos.

Seguridad Firewall NAT ALG FTP

♡ Útil (4) ☆ Favorito(1) Compartir ⚠ Reporte

‹ Previo: La función de conocimiento de la seguridad de… Próximo: Falta el módulo antispam en el firewall USG6600 ›

Jorge VIP Publicado 2019-9-13 12:34:30 ♡(0) ⚠ 2#

@Dr.Vegeta buen día.

Me podría ayudar con la siguiente pregunta que tengo:

¿Qué co
Utilizamos cookies en este sitio, incluyendo cookies de terceros, para que el sitio funcione correctamente y para analizar el tráfico, ofrecer una funcionalidad mejorada, características de redes sociales y personalizar el contenido y los ads. aprender másMás información
configuración de cookies Aceptar cookies

a) NAT ALG Protocol
b) ALG protocol
c) NAT protocol
d) detect protocol

Espero su valiosa respuesta, respecto que veo que conoce del tema.

Saludos!

> **user_3915171** Publicado 2021-2-5 21:31
> tengo la misma inquietud, he visto en algunos sitios que la respuesta es la D, pero he buscado informacion acerca de la funcion detect protocol y no encuentro nada. creo que la respuesta podria estar entre la opcion A y la C. haber si hay alguien que sepa la respuesta.

user_3915171 Publicado 2020-11-23 18:23:29 ♡(0) 3#

gracias por la informacion

Jazmin Publicado 2020-11-23 18:40:43 ♡(0) 4#

Gracias!!

user_4000619 Publicado 2020-11-25 16:31:36 ♡(0) #5

gracias.

Arzobispo982 VIP Publicado 2020-11-27 20:38:12 ♡(0) #6

Gracias por compartir tan buena información.

Utilizamos cookies en este sitio, incluyendo cookies de terceros, para que el sitio funcione correctamente y para analizar el tráfico, ofrecer una funcionalidad mejorada, características de redes sociales y personalizar el contenido y los ads. aprender másMás información
configuración de cookies
Aceptar cookies

Comentar



Debe iniciar sesión para responder la publicación Inicio de sesión | Registrarse

Editor Avanzado

Responde

⚠ **Aviso:** Para garantizar sus legítimos derechos e intereses, la comunidad y los terceros no publicarán contenido que pueda generar riesgos legales a las partes, por ejemplo, pornografía, contenido político, contenido sobre juego, consumo y tráfico de drogas, así como contenido que viole los derechos de propiedad intelectual de terceros, por ejemplo, secretos comerciales, marcas, derechos de autor, patentes y privacidad personal. No comparta su cuenta ni su contraseña con terceros. Todas las operaciones realizadas usando su cuenta se considerarán como sus acciones y todas las consecuencias que estas acciones generen serán responsabilidad suya. Para obtener información detallada, consulte la " Política de privacidad."

Copyright © 2021 Huawei Technologies Co., Ltd. Todos los derech

Utilizamos cookies en este sitio, incluyendo cookies de terceros, para que el sitio funcione correctamente y para analizar el tráfico, ofrecer una funcionalidad mejorada, características de redes sociales y personalizar el contenido y los ads. aprender másMás información

configuración de cookies

Aceptar cookies

REFERENCIAS TECNICAS

INGLES

NTLM

Portal Authentication on Internet Access Users

In portal authentication, the FW or a third-party server provides a portal authentication page to authenticate users.

FW Built-in Portal Authentication

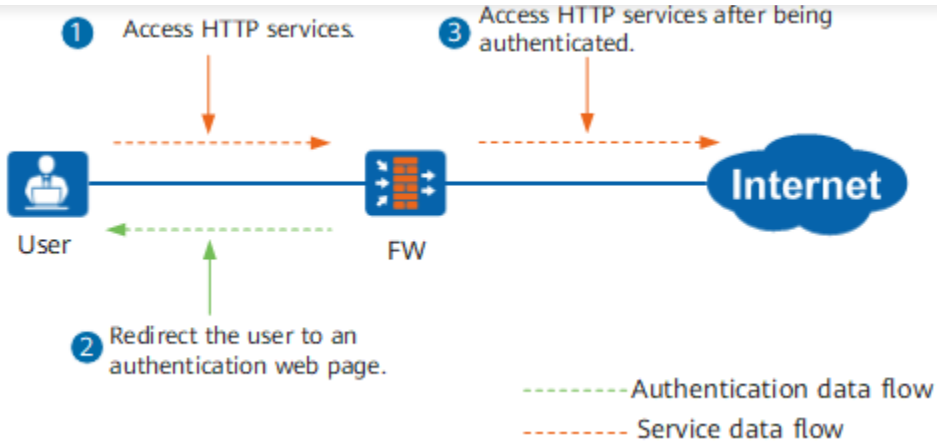
You can trigger built-in portal authentication using the following methods:

- **Redirected authentication**
  If users use only the HTTP/HTTPS service to access network resources, you can configure redirected authentication. Redirected authentication implements authentication on Internet access users when they attempt to access HTTP/HTTPS services. The users can access network resources after being authenticated. By default, the FW pushes an authentication page for HTTP request packets whose destination port number is 80. You can configure the FW to push an authentication page for HTTPS request packets whose destination port number is 443. The FW discards other request packets, including those identified as HTTP/HTTPS packets using port mapping.

  NOTICE

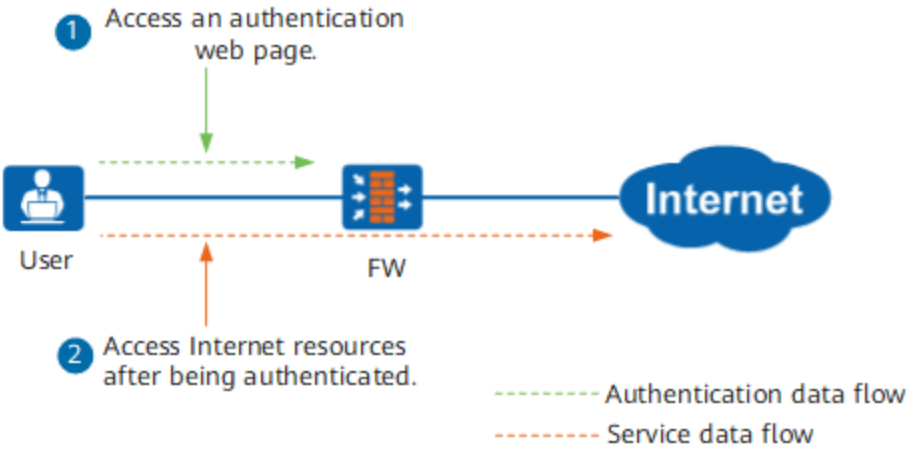
  If a user accesses the HTTP service using a URL, DNS service packets must be exchanged between the user and the DNS server to resolve the URL. If a FW is deployed between the user and the DNS server, you must configure a security policy to allow the exchanged DNS packets to pass through the FW.

  As shown in Figure 1, after receiving HTTP packets whose destination port is 80 from an Internet access user, a FW redirects the user to an authentication web page and triggers identity authentication. The user can access network resources after being authenticated. FW authentication modes include local authentication, proxy authentication by forwarding authentication requests to an authentication server. Local authentication and proxy authentication use the portal page that requires the user name and password.



- **User-initiated authentication**
  If users need to use multiple services to access network resources, configure the FW to trigger user-initiated authentication. User-initiated authentication indicates that Internet access users proactively access web pages for identity authentication before accessing network resources. The users can access network resources after being authenticated.
  As shown in Figure 2, an Internet access user initiates an authentication request on the authentication web page of a FW. After receiving the authentication request, the FW implements identity authentication on the user. The user can access Internet resources after being authenticated.
  FW authentication modes include local authentication, proxy authentication by forwarding authentication requests to an authentication server. Local authentication and proxy authentication use the portal page that requires the user name and password.

  Figure 2 User-initiated authentication

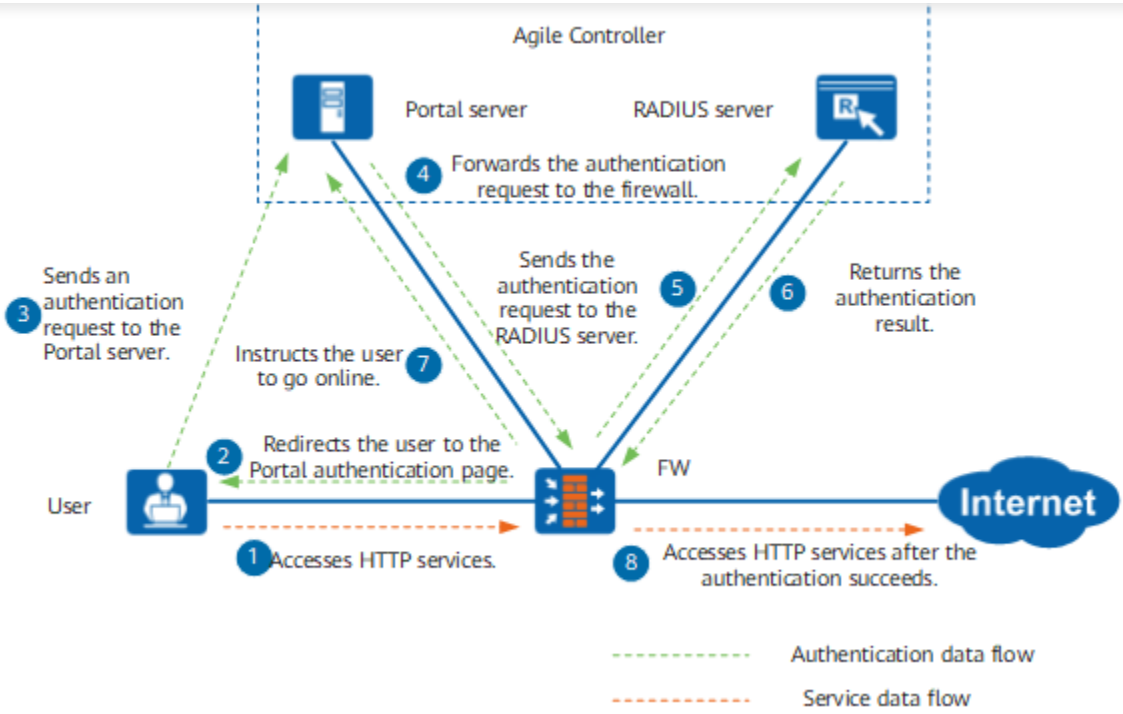


User-defined Portal Authentication

The FW supports user-defined portal authentication. Currently, there are two types of user-defined portal authentication.

external Portal server independently. For example, the Agile Controller can serve as a portal server.

- **Method 1: The FW does not participate in user authentication (Agile Controller SSO).**
  When this type of portal authentication is used, the portal server completes user authentication independently.
  For details, see Method 2: Users access HTTP services to trigger Agile Controller SSO.
  The HTTP requests of users are redirected to the portal authentication page of the Agile Controller. The Agile Controller authenticates users and notifies the FW of mappings between users and IP addresses.
- **Method 2: The FW participates in user authentication.**
  When this type of Portal authentication is used, the portal server and FW work together to complete user authentication.
  After receiving an HTTP service data flow from a user, the FW redirects an HTTP request to the portal authentication page of the Agile Controller.
  After receiving a user authentication request, the portal server forwards the request to the FW. The FW requests the RADIUS server to authenticate the user. After the authentication succeeds, the user goes online from the FW, as shown in Figure 3.
  The portal server and RADIUS server are two components of the Agile Controller. The two components can be installed on one or two servers. Currently, only the RADIUS server can serve as an authentication server.
  In this scenario, the portal server and FW use Portal2.0 for communication. Portal2.0 is the portal standards V2.01 for broadband products of Huawei.
  The Agile Controller can deliver security groups of users to the FW so that the FW can implement policy control on users by security group.



Users can go offline from the portal server. The portal server notifies the FW of users' logout.

User-defined portal authentication depends on the user-defined portal authentication template referenced in the authentication policy. The user-defined Portal address is specified in the user-defined Portal authentication template.

In scenarios where users log in to the FW for the first time and user device IP addresses frequently change, users may be prompted for re-authentication when the FW receives access requests. In this case, use **Method 2: The FW participates in user authentication** combined with **MAC address-prioritized portal authentication**.

In this combined authentication mode, if user device IP addresses change after users pass **Method 2: The FW participates in user authentication**, the FW performs MAC authentication on the users within a given time range (MAC address validity period configured on the Agile Controller). During MAC authentication, users are not required to enter authentication information and therefore are unaware of the authentication, facilitating their access to services.

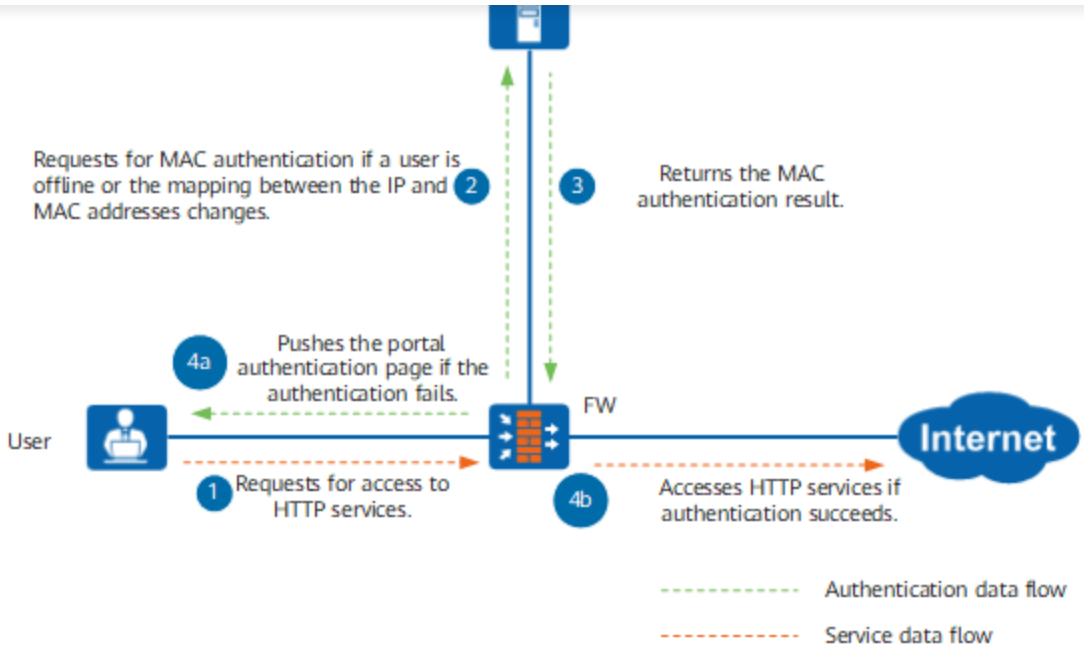
Figure 4 shows the specific procedure for the FW to process user requests. If the FW receives the HTTP service data flows of the users and the users are offline or the mappings between their IP addresses and MAC addresses change, the FW sends MAC authentication requests to the Agile Controller.

If MAC authentication succeeds, users can directly access services.

If the Agile Controller fails to respond or MAC authentication fails within a given time range, the FW pushes the portal authentication page to the users and the users enter the authentication process as shown in Figure 3. After the users are authenticated, they can properly access services.

Figure 4 User-defined portal authentication (the FW participates in user authentication)+MAC address-prioritized portal authentication

Home



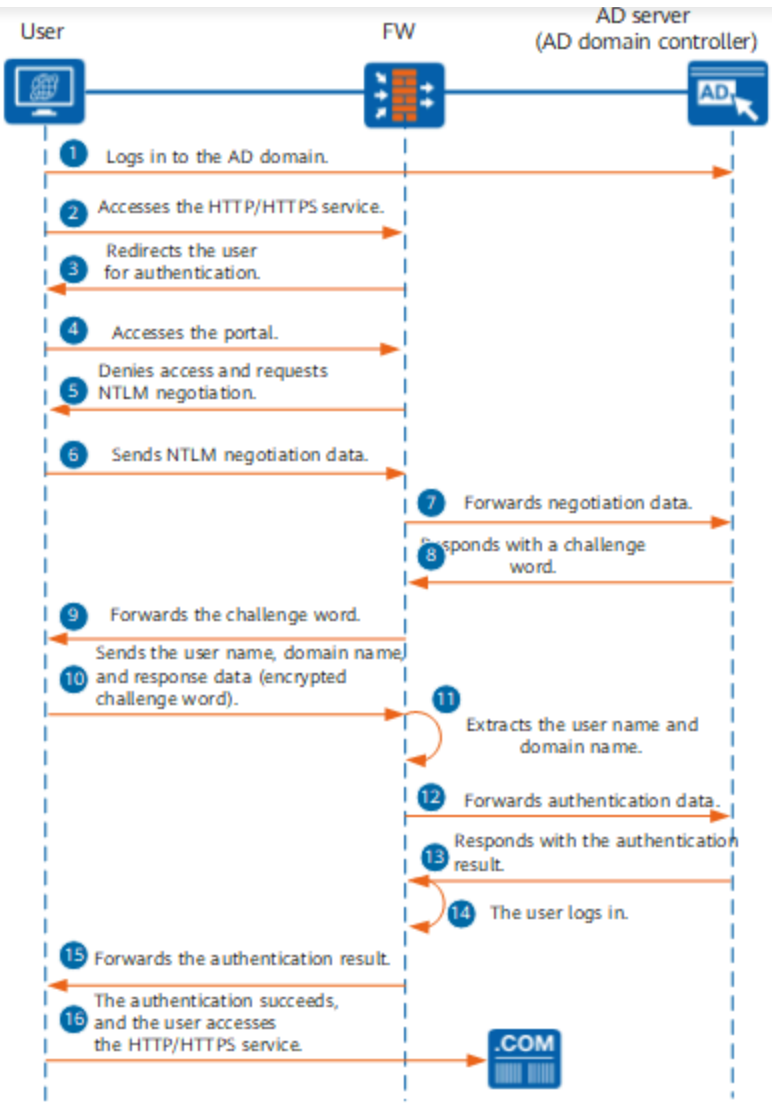
Authentication Exemption

If users need to directly access network resources without entering any user names or passwords, you can configure authentication exemption on the FW.

The local user names are bidirectionally bound with IP addresses, MAC addresses, or IP/MAC address pairs. The FW identifies the Internet access users according to the bound IP and MAC addresses. The Internet access users who are exempted from authentication must use the bound IP and MAC addresses to access network resources.

NTLM Authentication

If a user in the AD domain wants to access the Internet, the FW serves as **NTLM** authentication proxy to trigger and forward **NTLM** authentication packets exchanged between the browser and AD server and obtain the user identity in the authentication process. **NTLM** authentication is a portal authentication mode in which the user is unaware of entering the user name and password. Figure 5 shows the detailed mechanism.



1. A user logs in to the AD domain.
2. The user accesses the HTTP/HTTPS service through a browser.
3. The FW discovers that the traffic is not authenticated, and the traffic matches the **NTLM** authentication policy. The FW redirects the user for authentication.
4. The user accesses the portal page redirected by the FW. In this process, the browser and FW interact internally without prompting the user to enter the user name or password.
5. The FW denies the access through the browser and requires the browser perform **NTLM** authentication.
6. The browser sends an **NTLM** negotiation request.
7. The FW forwards the negotiation request to the AD server.
8. The AD server generates a random number, uses it as the challenge word, and sends it to the browser.
9. The FW forwards the challenge word to the browser.

Home

and response data.
The response value is obtained by encrypting the challenge word with the hash value of the password. This prevents the password from being transmitted over the network, securing the password.
The browser must support **NTLM** authentication. Otherwise, the browser cannot automatically provide user login information.

11. The FW extracts the user name.
12. The FW forwards the **NTLM** negotiation data to the AD server.
13. The AD server responds with the authentication result.
    The AD server searches locally for the password hash value corresponding to the user name, uses this hash value to encrypt the challenge word, and compares the encryption result with the response value sent from the browser. If the two values are the same, the user passes the authentication.
14. If the authentication succeeds, the FW enables the user to log in on the FW.
15. The FW forwards the authentication result to the browser.
16. If the authentication succeeds, the user successfully accesses the HTTP service.

After the user logs in on the FW, the FW logs out the user based on the timeout period.

Parent Topic: **User Authentication**

Copyright © Huawei Technologies Co., Ltd.

Previous Next topic

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

NTLM

Autenticación del portal en usuarios de acceso a Internet

En la autenticación del portal, el FW o un servidor de terceros proporciona una página de autenticación del portal para autenticar a los usuarios.

Autenticación del portal integrado de FW

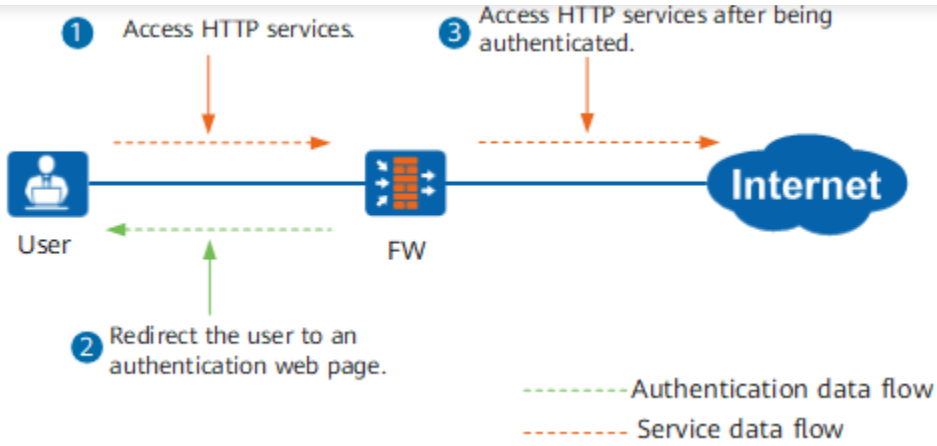
Puede activar la autenticación del portal incorporada mediante los siguientes métodos:

- **Autenticación redirigida**
  Si los usuarios solo utilizan el servicio HTTP/HTTPS para acceder a los recursos de red, puede configurar la autenticación redirigida. Esta autenticación implementa la autenticación de los usuarios con acceso a Internet cuando intentan acceder a servicios HTTP/HTTPS. Los usuarios pueden acceder a los recursos de red después de la autenticación. De forma predeterminada, el firewall envía una página de autenticación para los paquetes de solicitud HTTP cuyo puerto de destino es 80. Puede configurar el firewall para que envíe una página de autenticación para los paquetes de solicitud HTTPS cuyo puerto de destino es 443. El firewall descarta otros paquetes de solicitud, incluidos los identificados como paquetes HTTP/HTTPS mediante la asignación de puertos.

  NOTICE

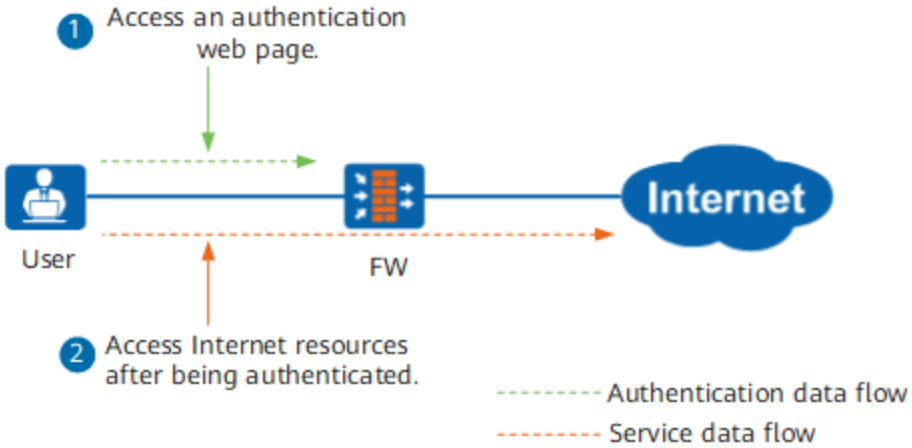
  Si un usuario accede al servicio HTTP mediante una URL, se deben intercambiar paquetes de servicio DNS entre el usuario y el servidor DNS para resolver la URL. Si se implementa un firewall entre el usuario y el servidor DNS, se debe configurar una política de seguridad para permitir que los paquetes DNS intercambiados pasen a través de él .

  Como se muestra en la Figura 1 , tras recibir paquetes HTTP con el puerto de destino 80 de un usuario con acceso a Internet, un firewall redirige al usuario a una página web de autenticación y activa la autenticación de identidad. El usuario puede acceder a los recursos de la red tras la autenticación.
  Los modos de autenticación de FW incluyen la autenticación local y la autenticación por proxy, que reenvía las solicitudes a un servidor. Ambas utilizan la página del portal, que requiere el nombre de usuario y la contraseña.



- **Autenticación iniciada por el usuario**
  Si los usuarios necesitan usar varios servicios para acceder a los recursos de red, configure el firewall para que active la autenticación iniciada por el usuario. Esta autenticación implica que los usuarios con acceso a Internet acceden proactivamente a las páginas web para autenticar su identidad antes de acceder a los recursos de red. Los usuarios pueden acceder a los recursos de red después de autenticarse.
  Como se muestra en la Figura 2 , un usuario con acceso a Internet inicia una solicitud de autenticación en la página web de autenticación de un FW . Tras recibir la solicitud, el FW implementa la autenticación de identidad del usuario. El usuario puede acceder a los recursos de Internet tras la autenticación.
  Los modos de autenticación de FW incluyen la autenticación local y la autenticación por proxy, que reenvía las solicitudes a un servidor. Ambas utilizan la página del portal, que requiere el nombre de usuario y la contraseña.

  Figura 2 Autenticación iniciada por el usuario



Autenticación de portal definida por el usuario

El FW admite la autenticación de portales definida por el usuario. Actualmente, existen dos tipos de autenticación de portales definida por el usuario.

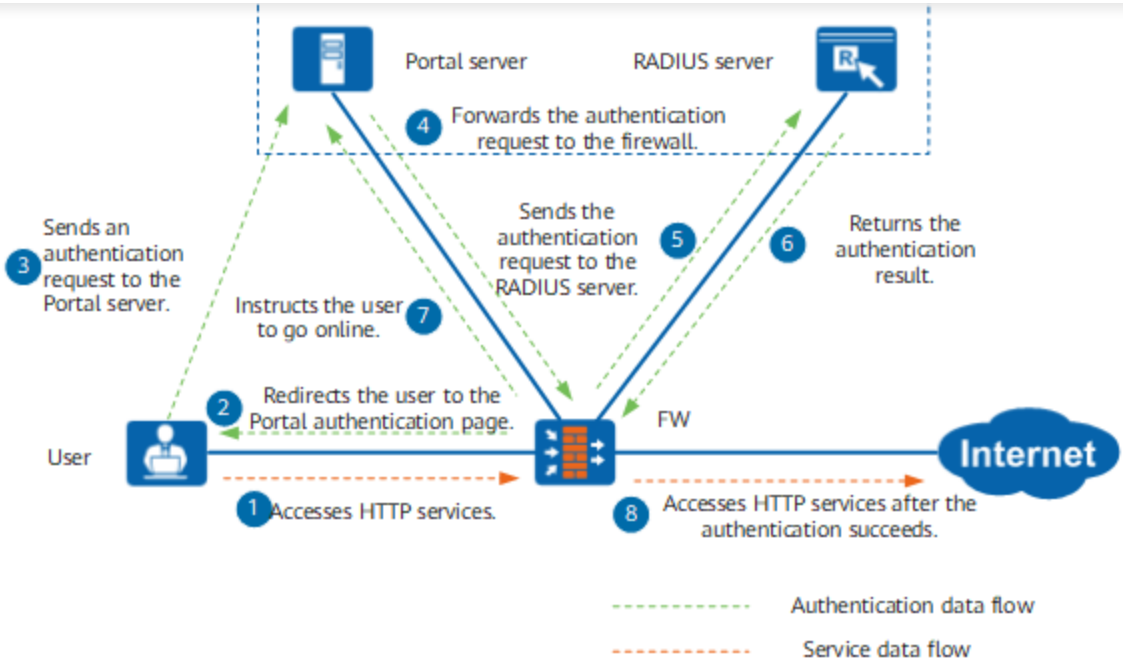
Inicio

implementar un servidor de portal externo de forma independiente. Por ejemplo, Agile Controller puede servir como servidor de portal.

- **Método 1: El FW no participa en la autenticación del usuario (Agile Controller SSO).**
  Cuando se utiliza este tipo de autenticación de portal, el servidor del portal completa la autenticación del usuario de forma independiente.
  Para obtener más detalles, consulte Método 2: Los usuarios acceden a servicios HTTP para activar el inicio de sesión único (SSO) de Agile Controller .
  Las solicitudes HTTP de los usuarios se redirigen a la página de autenticación del portal del Controlador Agile. El Controlador Agile autentica a los usuarios y notifica al servidor de seguridad las asignaciones entre usuarios y direcciones IP.
- **Método 2: El FW participa en la autenticación del usuario.**
  Cuando se utiliza este tipo de autenticación de portal, el servidor del portal y el FW trabajan juntos para completar la autenticación del usuario.
  Después de recibir un flujo de datos de servicio HTTP de un usuario, el FW redirige una solicitud HTTP a la página de autenticación del portal del Agile Controller.
  Tras recibir una solicitud de autenticación de usuario, el servidor del portal la reenvía al servidor de seguridad . Este solicita al servidor RADIUS que autentique al usuario. Una vez realizada la autenticación, el usuario se conecta desde el servidor de seguridad , como se muestra en la Figura 3 .
  El servidor del portal y el servidor RADIUS son dos componentes del Agile Controller. Ambos componentes pueden instalarse en uno o dos servidores. Actualmente, solo el servidor RADIUS puede servir como servidor de autenticación.
  En este escenario, el servidor del portal y el firmware utilizan Portal 2.0 para la comunicación. Portal 2.0 es el estándar de portal V2.01 para productos de banda ancha de Huawei.
  El controlador ágil puede entregar grupos de seguridad de usuarios al FW para que éste pueda implementar el control de políticas sobre los usuarios por grupo de seguridad.

  Figura 3 Autenticación del portal definido por el usuario (el FW participa en la autenticación del usuario)

521



Los usuarios pueden desconectarse del servidor del portal. Este notifica al servidor de seguridad (FW) sobre su cierre de sesión.

La autenticación del portal definida por el usuario depende de la plantilla de autenticación del portal definida por el usuario a la que se hace referencia en la política de autenticación. La dirección del portal definida por el usuario se especifica en la plantilla de autenticación del portal definida por el usuario.

En escenarios donde los usuarios inician sesión en el firewall por primera vez y las direcciones IP de sus dispositivos cambian con frecuencia, es posible que se les solicite que se vuelvan a autenticar cuando el firewall recibe solicitudes de acceso. En este caso, utilice **el Método 2: El firewall participa en la autenticación del usuario** combinada con **la autenticación del portal priorizada por dirección MAC** .

En este modo de autenticación combinada, si las direcciones IP de los dispositivos de usuario cambian después de que los usuarios aprueben **el método 2: El firewall participa en la autenticación de usuarios** , este realiza la autenticación MAC de los usuarios dentro de un período determinado (el período de validez de la dirección MAC configurado en el controlador Agile). Durante la autenticación MAC, los usuarios no necesitan ingresar información de autenticación y, por lo tanto, no son conscientes de ella, lo que facilita su acceso a los servicios.

La Figura 4 muestra el procedimiento específico para que el FW procese las solicitudes de usuario.

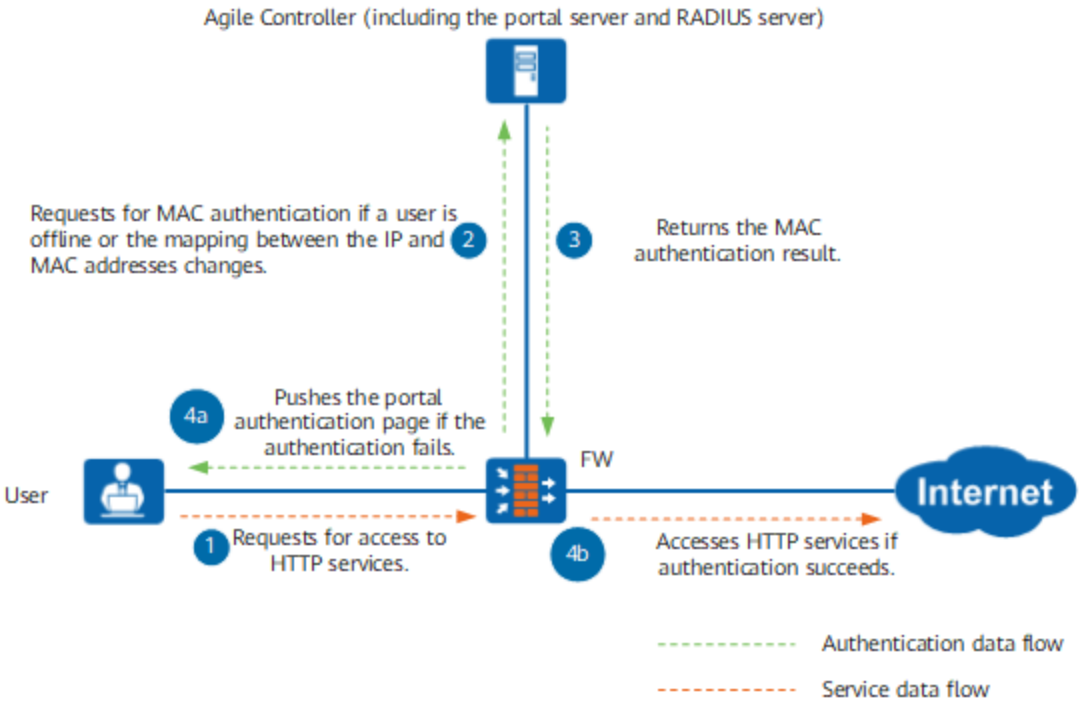
Si el FW recibe los flujos de datos del servicio HTTP de los usuarios y estos están desconectados o la correspondencia entre sus direcciones IP y MAC cambia, el FW envía solicitudes de autenticación MAC al Controlador Agile.

Si la autenticación MAC tiene éxito, los usuarios pueden acceder directamente a los servicios.

Si el Controlador Ágil no responde o la autenticación MAC falla dentro de un plazo determinado, el FW envía la página de autenticación del portal a los usuarios, quienes inician el proceso de

a los servicios correctamente.

Figura 4 Autenticación de portal definida por el usuario (el FW participa en la autenticación del usuario) + autenticación de portal priorizada por dirección MAC

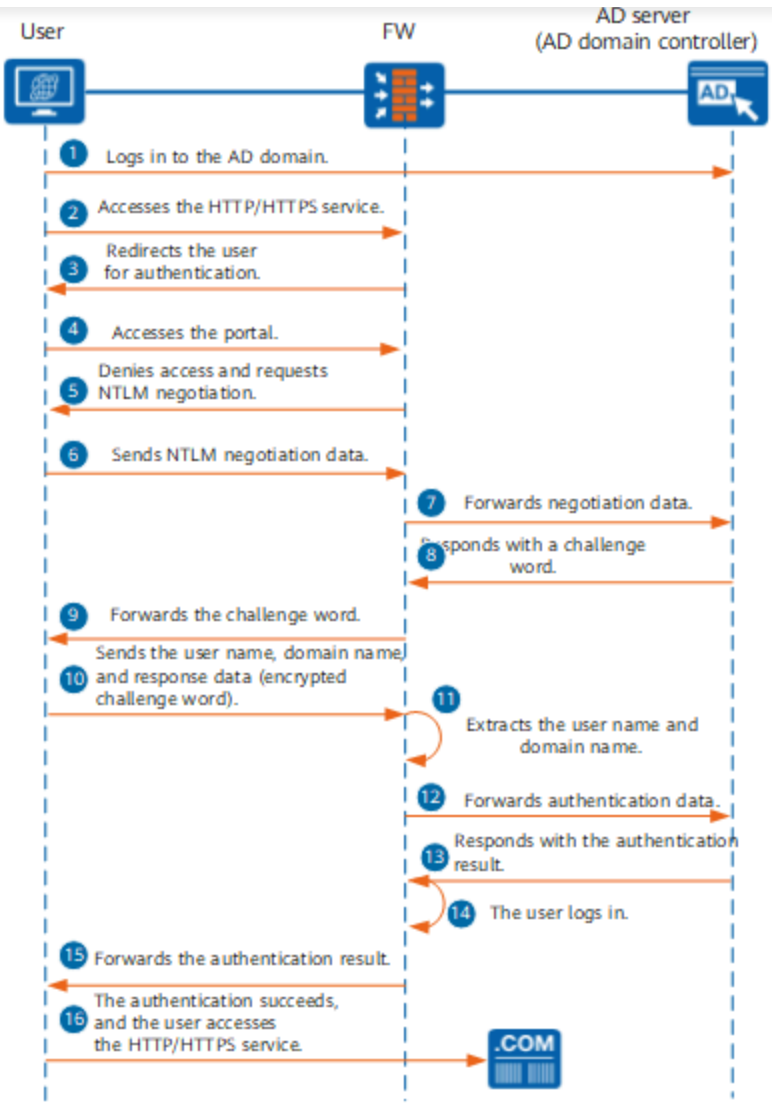


Exención de autenticación

Si los usuarios necesitan acceder directamente a los recursos de la red sin ingresar ningún nombre de usuario ni contraseña, puede configurar la exención de autenticación en el FW .
Los nombres de usuario locales están vinculados bidireccionalmente con direcciones IP, direcciones MAC o pares de direcciones IP/MAC. El firewall identifica a los usuarios con acceso a Internet según las direcciones IP y MAC vinculadas. Los usuarios con acceso a Internet exentos de autenticación deben usar las direcciones IP y MAC vinculadas para acceder a los recursos de red.

Autenticación NTLM

Si un usuario del dominio AD desea acceder a Internet, el firewall actúa como proxy de autenticación NTLM para activar y reenviar los paquetes de autenticación NTLM intercambiados entre el navegador y el servidor AD, y obtener la identidad del usuario durante el proceso de autenticación. La autenticación NTLM es un modo de autenticación de portal en el que el usuario no es consciente de haber introducido su nombre de usuario y contraseña. La Figura 5 muestra el mecanismo detallado.



1. Un usuario inicia sesión en el dominio de AD.
2. El usuario accede al servicio HTTP/HTTPS a través de un navegador.
3. El firewall detecta que el tráfico no está autenticado y que cumple con la política de autenticación NTLM. El firewall redirige al usuario para su autenticación.
4. El usuario accede a la página del portal redirigida por el firewall . En este proceso, el navegador y el firewall interactúan internamente sin solicitar al usuario que introduzca su nombre de usuario ni contraseña.
5. El FW niega el acceso a través del navegador y requiere que el navegador realice la autenticación NTLM.
6. El navegador envía una solicitud de negociación NTLM.
7. El FW reenvía la solicitud de negociación al servidor AD.
8. El servidor AD genera un número aleatorio, lo utiliza como palabra clave y lo envía al navegador.

Inicio

10. El navegador envía nuevamente datos de negociación NTLM, incluido el nombre de usuario, el nombre de dominio y los datos de respuesta.
    El valor de respuesta se obtiene cifrando la palabra de desafío con el valor hash de la contraseña. Esto impide que la contraseña se transmita por la red, protegiéndola.
    El navegador debe ser compatible con la autenticación NTLM. De lo contrario, no podrá proporcionar automáticamente la información de inicio de sesión del usuario.
11. El FW extrae el nombre de usuario.
12. El FW reenvía los datos de negociación NTLM al servidor AD.
13. El servidor AD responde con el resultado de la autenticación.
    El servidor AD busca localmente el valor hash de la contraseña correspondiente al nombre de usuario, lo utiliza para cifrar la palabra de seguridad y compara el resultado del cifrado con la respuesta enviada desde el navegador. Si ambos valores coinciden, el usuario pasa la autenticación.
14. Si la autenticación tiene éxito, el FW permite que el usuario inicie sesión en el FW .
15. El FW envía el resultado de la autenticación al navegador.
16. Si la autenticación tiene éxito, el usuario accede exitosamente al servicio HTTP.

Después de que el usuario inicia sesión en el FW , el FW cierra la sesión del usuario según el período de tiempo de espera.

Tema principal: **Autenticación de usuario**

Tema **Siguiente**

Derechos de autor © Huawei Technologies Co., Ltd.

REFERENCIAS TECNICAS

INGLES

Overview of Mirroring

Overview of Mirroring

Definition

Mirroring is a function used to copy (or mirror) traffic received or sent (or both) on a specified source (known as a mirrored source) to a destination port (known as an observing port) for analysis. Copied packets are known as mirrored packets.

Purpose

During network maintenance, you may need to obtain and analyze packets. For example, if you suspect that there are attack packets on the network, you need to be able to obtain and analyze the packets without affecting packet forwarding.
The mirroring function is able to achieve such results. Mirroring copies packets on a mirrored port to an observing port for analysis by a monitoring device without affecting switching of packets on the mirrored port. This function facilitates network monitoring and troubleshooting.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Overview of Mirroring

Descripción general de la duplicación

Definición

La duplicación es una función que se utiliza para copiar (o reflejar) el tráfico recibido o enviado (o ambos) en un origen específico (conocido como origen reflejado) a un puerto de destino (conocido como puerto de observación) para su análisis. Los paquetes copiados se conocen como paquetes reflejados.

Objetivo

Durante el mantenimiento de la red, es posible que necesite obtener y analizar paquetes. Por ejemplo, si sospecha que hay paquetes de ataque en la red, necesita poder obtenerlos y analizarlos sin afectar el reenvío.
La función de duplicación permite lograr estos resultados. La duplicación copia los paquetes de un puerto replicado a un puerto de observación para su análisis por parte de un dispositivo de monitoreo, sin afectar la conmutación de paquetes en dicho puerto. Esta función facilita la monitorización y la resolución de problemas de la red.

REFERENCIAS TECNICAS

INGLES

Overview of NAT

Enterprise Support

Size: 264.12MB

Enter keywords 0 / 256

Overview of NAT

Definition

Network Address Translation (NAT) translates IP addresses in the packet header into other IP addresses.

Purpose

As the Internet expands and becomes more accessible, an increasing number of private network users access the Internet using public IPv4 addresses. The rapid exhaustion of IPv4 address space causes a significant depletion of public addresses. Although IPv6 technology can be used to solve this problem, most contents and applications are still based on IPv4, and therefore they cannot be completely switched to IPv6 within a short period of time. NAT technology allows public IPv4 addresses to be reused, offering a short-term solution to IPv4 address exhaustion.

Benefits

NAT has the following advantages:

- Translates a large number of private addresses into a few public IP addresses, resulting in private network users being able to access the Internet while the number of required public IP addresses is reduced.

We use cookies on this site, in order for the site to work properly and to analyse traffic, offer enhanced functionality and personalise content.Learn more

cookie settings

Accept Cookies

Reject Cookies

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Overview of NAT

Soporte empresarial

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Descripción general de NAT

Definición

La traducción de direcciones de red (NAT) traduce las direcciones IP del encabezado del paquete a otras direcciones IP.

Objetivo

A medida que Internet se expande y se vuelve más accesible, un número creciente de usuarios de redes privadas acceden a Internet utilizando direcciones IPv4 públicas. El rápido agotamiento del espacio de direcciones IPv4 provoca una disminución significativa de las direcciones públicas. Si bien la tecnología IPv6 puede utilizarse para resolver este problema, la mayoría de los contenidos y aplicaciones aún se basan en IPv4 y, por lo tanto, no pueden migrarse completamente a IPv6 en un corto plazo. La tecnología NAT permite la reutilización de direcciones IPv4 públicas, lo que ofrece una solución a corto plazo al agotamiento de direcciones IPv4.

Beneficios

NAT tiene las siguientes ventajas:

Utilizamos cookies en este sitio para su correcto funcionamiento, analizar el tráfico, ofrecer una mejor funcionalidad y personalizar el contenido. Más información

configuración de cookies

Aceptar cookies

Rechazar cookies

REFERENCIAS TECNICAS

INGLES

Overview of RESTCONF

Overview of RESTCONF

Definition

RESTCONF, an HTTP-based protocol, provides RESTful programming interfaces and allows users to add, delete, modify, as well as query network device data.

Purpose

Increasing network scale and complexity are driving the growing demand for automated O&M. The Network Configuration Protocol (NETCONF) provides application programming interfaces (APIs) based on the remote procedure call (RPC) mechanism. However, networks are developing faster than NETCONF, necessitating standard programming interfaces that support web application access and network device operations.
RESTCONF is developed based on both NETCONF and HTTP, and it provides core NETCONF functions using HTTP methods. The programming interface complies with the RESTful style of the IT industry and provides users with the capability of efficiently developing web O&M tools.
Table 1 compares RESTCONF and NETCONF based on the YANG data model.

Table 1 Comparison between RESTCONF and NETCONF

Item	NETCONF+YANG	RESTCONF+YANG
Transmission channel (protocol)	NETCONF prefers Secure Shell (SSH) at the transport layer and uses SSH to transmit XML information.	RESTCONF accesses device resources based on HTTP. The programming interfaces provided by RESTCONF comply with the RESTful style of the IT industry.
Packet format	XML code	XML
Operation Characteristics	NETCONF operations are complex. For example: • NETCONF supports addition, deletion, modification, and query, multiple configuration datastores, as well as configuration rollback.	RESTCONF operations are simple. For example: • RESTCONF supports addition, deletion, modification, and query operations, and it supports only the <running/> configuration database. • The RESTCONF operations take effect immediately, without the need for two-phase submission.

Benefits

- RESTCONF provides RESTful programming interfaces to support web-based development.
- Standard interfaces are compatible with multi-vendor devices, reducing development and maintenance costs.
- RESTCONF provides high extensibility, allowing various vendors to define additional NETCONF operations.
- No NMS tool is required.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Overview of RESTCONF

Descripción general de RESTCONF

Definición

RESTCONF , un protocolo basado en HTTP, proporciona interfaces de programación RESTful y permite a los usuarios agregar, eliminar, modificar y consultar datos de dispositivos de red.

Objetivo

La creciente escala y complejidad de la red impulsan la creciente demanda de operaciones y mantenimiento automatizados. El Protocolo de Configuración de Red (NETCONF) proporciona interfaces de programación de aplicaciones (API) basadas en el mecanismo de llamada a procedimiento remoto (RPC). Sin embargo, las redes se desarrollan a un ritmo mayor que NETCONF, lo que requiere interfaces de programación estándar que admitan el acceso a aplicaciones web y las operaciones de dispositivos de red.
RESTCONF se basa en NETCONF y HTTP, y proporciona las funciones principales de NETCONF mediante métodos HTTP. La interfaz de programación se ajusta al estilo RESTful de la industria de TI y permite a los usuarios desarrollar eficientemente herramientas de operación y mantenimiento web. La Tabla 1 compara RESTCONF y NETCONF según el modelo de datos YANG.

Tabla 1 Comparación entre RESTCONF y NETCONF

Artículo	**NETCONF+YANG**	**RESTCONF +YANG**
Canal de transmisión (protocolo)	NETCONF prefiere Secure Shell (SSH) en la capa de transporte y utiliza SSH para transmitir información XML.	RESTCONF accede a los recursos del dispositivo mediante HTTP. Las interfaces de programación que ofrece RESTCONF cumplen con el estilo RESTful del sector de TI.
Formato de paquete	Código XML	XML
Características de operación	Las operaciones de NETCONF son complejas. Por ejemplo: • NETCONF admite la adición, eliminación, modificación y consulta de múltiples almacenes de datos de configuración, así como la reversión de la configuración.	Las operaciones RESTCONF son sencillas. Por ejemplo: • RESTCONF admite operaciones de adición, eliminación, modificación y consulta, y solo admite la base de datos de configuración <running/>. • Las operaciones RESTCONF entran en vigor inmediatamente, sin necesidad de presentación en dos fases.

Beneficios

- RESTCONF proporciona interfaces de programación RESTful para respaldar el desarrollo basado en web.
- Las interfaces estándar son compatibles con dispositivos de múltiples proveedores, lo que reduce los costos de desarrollo y mantenimiento.
- RESTCONF proporciona alta extensibilidad, lo que permite que varios proveedores definan operaciones NETCONF adicionales.
- No se requiere ninguna herramienta NMS.

REFERENCIAS TECNICAS

INGLES

PRF

prf

Function

The **prf** command configures the pseudo-random function (PRF) algorithm used in IKEv2 negotiation.
The **undo prf** command restores the default configuration.
By default, the HMAC-SHA2-256 PRF algorithm is used in IKEv2 negotiation.

Format

prf { **aes-xcbc-128** | **hmac-md5** | **hmac-sha1** | **hmac-sha2-256** | **hmac-sha2-384** | **hmac-sha2-512** } *
undo prf

Parameters

Parameter	Description	Value
aes-xcbc-128	Indicates the AES-XCBC-128 authentication algorithm. This algorithm applies only to IKEv2 negotiation.	-
hmac-md5	Indicates the HMAC-MD5 authentication algorithm.	-
hmac-sha1	Indicates the HMAC-SHA1 authentication algorithm.	-
hmac-sha2-256	Indicates the HMAC-SHA2-256 authentication algorithm.	-
hmac-sha2-384	Indicates the HMAC-SHA2-384 authentication algorithm.	-
hmac-sha2-512	Indicates the HMAC-SHA2-512 authentication algorithm.	-

Views

IKE proposal view, IKE proposal view of the virtual system

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario
The PRF algorithm is required in IKEv2 negotiation. The PRF algorithm is listed as follows from the highest security level to the lowest security level: hmac-sha2-512 > hmac-sha2-384 > hmac-sha2-256 > aes-xcbc-128 > hmac-sha1 > hmac-md5. If multiple PRF algorithms are configured, the device selects the algorithm in the following sequence: aes-xcbc-128 > hmac-sha2-512 > hmac-sha2-384 > hmac-sha2-256 > hmac-sha1 > hmac-md5.
If you run the **prf** command multiple times, only the latest configuration takes effect.
Precautions
The hmac-md5, hmac-sha1, and aes-xcbc-128 algorithms are not recommended because they are insecure.
Parameters hmac-md5, hmac-sha1, and aes-xcbc-128 in this command can be used only after the weak security algorithm/protocol feature package (WEAKEA) has been installed using the **install feature-software WEAKEA** command.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

PRF

prf

Función

El comando **prf** configura el algoritmo de función pseudoaleatoria (PRF) utilizado en la negociación IKEv2.
El comando **undo prf** restaura la configuración predeterminada.
De forma predeterminada, se utiliza el algoritmo PRF HMAC-SHA2-256 en la negociación IKEv2.

Formato

prf { **aes-xcbc-128** | **hmac-md5** | **hmac-sha1** | **hmac-sha2-256** | **hmac-sha2-384** | **hmac-sha2-512** }*
deshacer prf

Parámetros

Parámetro	Descripción	Valor
aes-xcbc-128	Indica el algoritmo de autenticación AES-XCBC-128. Este algoritmo se aplica únicamente a la negociación IKEv2.	-
hmac-md5	Indica el algoritmo de autenticación HMAC-MD5.	-
hmac-sha1	Indica el algoritmo de autenticación HMAC-SHA1.	-
hmac-sha2-256	Indica el algoritmo de autenticación HMAC-SHA2-256.	-
hmac-sha2-384	Indica el algoritmo de autenticación HMAC-SHA2-384.	-
hmac-sha2-512	Indica el algoritmo de autenticación HMAC-SHA2-512.	-

Vistas

Vista de propuesta de IKE, vista de propuesta de IKE del sistema virtual

Nivel predeterminado

2: Nivel de configuración

Instrucciones de uso

Escenario de uso
El algoritmo PRF es necesario en la negociación de IKEv2. El algoritmo PRF se enumera de la siguiente manera, desde el nivel de seguridad más alto hasta el más bajo: hmac-sha2-512 > hmac-sha2-384 > hmac-

sha2-256 > aes-xcbc-128 > hmac-sha1 > hmac-md5. Si se configuran varios algoritmos PRF , el dispositivo selecciona el algoritmo en la siguiente secuencia: aes-xcbc-128 > hmac-sha2-512 > hmac-sha2-384 > hmac-sha2-256 > hmac-sha1 > hmac-md5.

Si ejecuta el comando **prf** varias veces, solo tendrá efecto la última configuración.

Precauciones

No se recomiendan los algoritmos hmac-md5, hmac-sha1 y aes-xcbc-128 porque no son seguros.

Los parámetros hmac-md5 , hmac-sha1 y aes-xcbc-128 en este comando solo se pueden usar después de que se haya instalado el paquete de características del algoritmo/protocolo de seguridad débil (WEAKEA) utilizando el comando **install feature-software WEAKEA** .

REFERENCIAS TECNICAS

INGLES

QUOTA

Configuring a Quota Control Policy

The quota control policy defines users whose quota needs to be managed, assigns the quota to them, and specify the management and control actions after the quota is exceeded.

Prerequisites

- Users whose quota statistics need to be collected, managed, and controlled have been specified.
- The quota allocation mode and quota data planning have been clarified based on bandwidth requirements of the enterprise.

NOTE

The quota control policy differs from other policies (such as the security policy and traffic policy) in that if the parameter **user** of a policy is set to **any**, this policy applies to all users. Therefore, use this setting with caution to prevent complaints about such network problems as slow or failed to access the Internet at a large scope.

Procedure

1. Choose **Policy** > **Quota Control Policy** > **Quota Control Policy**.
2. Click **Add**.
3. Configure basic information of the quota control policy, including the name, description, tag, user, and time range.

Parameter	Description
Name	Indicates a quota control policy name. The name must be different from any existing one.
Description	Indicates description information of the quota control policy. Description information needs to be clearly described so that an administrator can easily query and maintain the policy.
Tag	The tag identifies and categorizes the policy. You can query policies based on tags and delete, move, enable, or disable

	policies in batches based on the query results. For the tag description and configuration, see Tag.
User	Indicates the users whose quota statistics need to be collected and controlled. You can reference local users, user groups, or security groups or create new ones. If the server has a great number of users, user groups, or security groups and only some of them need to be imported to the FW to implement policy control, select **Server Import** from the matching conditions of **User**, online query and import the desired users, user groups, or security groups, and then reference them in policies. **NOTE:** Only the AD and AD LDAP servers support online query and import of users, user groups, or security groups. Before that, you need to configure a server import policy in the **New User Authentication Options** and associate an authentication domain with the configured server import policy. The server import policy determines the target groups, online query path, and filtering parameter. However, the import type configured in the server import policy does not take effect in this function. The user name (**cn** value) on the server is suggested to be the same as the login name (**sAMAccountName** value). A policy can reference a maximum of 64 users, user groups, or security groups. Select **Import from Server** from the matching conditions of **User**. If **Type** is set to **User**, the device will imports only the names of users, not the user groups or security groups to which the users belong.
Schedule	Indicates the validity period of the quota control policy.

NOTE

- If multiple users (user groups) are configured for a quota control policy, the daily traffic quota, monthly traffic quota, and daily Internet access duration defined in the policy are exclusively used by individual users instead of shared among multiple users.
- If the daily traffic quota, monthly traffic quota, and daily Internet access duration are jointly used, the management and control action is triggered as long as one of them reaches the upper threshold.
- After the quota of a user reaches 100%, the device pushes a portal page to the user's browser to remind the exhaustion of the quota, and the user cannot continue accessing the Internet.

Parameter		Description
Daily	Traffic Quota	Indicates the daily traffic quota for each user.
	Duration of Internet Use	Indicates the daily Internet access duration for each user.
	Reset Time	You can configure the start (reset) time for the collection of daily traffic quota and daily online duration quota statistics if the statistics are not collected on natural days (for example, from 07:00 on each day to 07:00 on the next day). The default start time for the collection of daily traffic quota and daily online duration quota statistics is 00:00 midnight each day. If daylight saving time (DST) is applied, do not set the start (reset) time for statistics collection to the calibration time. Otherwise, the quota control policies will be abnormal on the DST start and end days.
Mont	Traffic Quota	Indicates the monthly traffic quota for each user.
	Reset Time	If the statistics are not collected by calendar month (such as from the 15th day of each month to the 14th day of the next month), you can specify the start date

Home

		for collecting the monthly traffic quota statistics. The default start date is the 1st day of each month.
Notification Threshold		Indicates a reminder threshold for the quota usage for each user. If the quota usage reaches the preset reminder threshold, the device pushes a portal page to the user's browser to remind the user of the quota usage.

5. Limit the maximum bandwidth of each user whose quota is exhausted.

Parameter	Description
Excess Max. Bandwidth	Implements direct block (if this value is set to 0) or limits the maximum bandwidth. The user or user group to which a quota control policy is applied can be configured. If a user is referenced by multiple quota control policies (including the reference of the user group), the actual maximum bandwidth value is determined by the quota specified in the policy of the highest priority.

6. Click **OK**.

Follow-up Procedure

Choose **Policy** > **Quota Control Policy** > **User Quota Config**. In the page displayed, you can:

- View the quota usage of the user in real time.
- Clear the quota statistics of the user. Note that if over two quotas reach the threshold, clearing statistics on one quota cannot prevent the FW from performing the management and control action.

Parent Topic: **Configuring a Quota Control Policy Using the Web UI**

Next topic

Copyright © Huawei Technologies Co., Ltd.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

QUOTA

Inicio

Configuración de una política de control de cuotas

La política de control de cuotas define los usuarios cuya cuota necesita ser administrada, les asigna la cuota y especifica las acciones de administración y control después de que se excede la cuota.

Prerrequisitos

- Se han especificado los usuarios cuyas estadísticas de cuota deben recopilarse, administrarse y controlarse.
- Se han aclarado el modo de asignación de cuotas y la planificación de datos de cuotas en función de los requisitos de ancho de banda de la empresa.

NOTE

La política de control de cuotas se diferencia de otras políticas (como la de seguridad y la de tráfico) en que si el parámetro " **usuario"** de una política se establece en **"cualquiera"** , esta política se aplica a todos los usuarios. Por lo tanto, utilice esta configuración con precaución para evitar quejas sobre problemas de red, como acceso lento o fallos de acceso a Internet a gran escala.

Procedimiento

1. Seleccione **Política** > **Política de control de cuotas** > **Política de control de cuotas** .
2. Haga clic **en Agregar** .
3. Configure la información básica de la política de control de cuotas, incluido el nombre, la descripción, la etiqueta, el usuario y el rango de tiempo.

Parámetro	Descripción
Nombre	Indica el nombre de una política de control de cuotas. El nombre debe ser diferente de cualquier otro existente.
Descripción	Indica información descriptiva de la política de control de cuotas.

	La información descriptiva debe estar claramente descrita para que un administrador pueda consultar y mantener la política fácilmente.
Etiqueta	La etiqueta identifica y categoriza la política. Puede consultar políticas según las etiquetas y eliminarlas, moverlas, habilitarlas o deshabilitarlas por lotes según los resultados de la consulta. Para obtener la descripción y la configuración de la etiqueta, consulte Etiqueta .
Usuario	Indica los usuarios cuyas estadísticas de cuota deben recopilarse y controlarse. Puede hacer referencia a usuarios locales, grupos de usuarios o grupos de seguridad o crear otros nuevos. Si el servidor tiene una gran cantidad de usuarios, grupos de usuarios o grupos de seguridad y solo es necesario importar algunos de ellos al FW para implementar el control de políticas, seleccione **Importar servidor** en las condiciones coincidentes de **Usuario** , realice una consulta en línea e importe los usuarios, grupos de usuarios o grupos de seguridad deseados y luego haga referencia a ellos en las políticas. **NOTA:** Solo los servidores AD y AD LDAP admiten la consulta e importación en línea de usuarios, grupos de usuarios o grupos de seguridad. Antes de eso, debe configurar una política de importación de servidor en las **Opciones de autenticación de nuevo usuario** y asociar un dominio de autenticación con la política de importación de servidor configurada. La política de importación del servidor determina los grupos de destino, la ruta de consulta en línea y el parámetro de filtrado. Sin embargo, el tipo de importación configurado en la política de importación del servidor no se aplica a esta función. Se sugiere que el nombre de usuario (valor **cn**) en el servidor sea el mismo que el nombre de inicio de sesión (valor **sAMAccountName).**

Inicio

	Una política puede hacer referencia a un máximo de 64 usuarios, grupos de usuarios o grupos de seguridad. Seleccione **"Importar del servidor"** en las condiciones coincidentes de **"Usuario"** . Si **"Tipo"** se establece en **"Usuario"** , el dispositivo importará solo los nombres de los usuarios, no los grupos de usuarios ni los grupos de seguridad a los que pertenecen.
Cronograma	Indica el período de validez de la política de control de cuotas.

4. Configurar los recursos de acceso a Internet disponibles para los usuarios, es decir, la cuota de acceso a Internet.

NOTE

- Si se configuran varios usuarios (grupos de usuarios) para una política de control de cuotas, la cuota de tráfico diaria, la cuota de tráfico mensual y la duración diaria del acceso a Internet definidas en la política son utilizadas exclusivamente por usuarios individuales en lugar de compartirse entre varios usuarios.
- Si la cuota de tráfico diaria, la cuota de tráfico mensual y la duración diaria del acceso a Internet se utilizan conjuntamente, la acción de gestión y control se activa siempre que una de ellas alcance el umbral superior.
- Una vez que la cuota de un usuario alcanza el 100%, el dispositivo envía una página de portal al navegador del usuario para recordarle el agotamiento de la cuota y el usuario no puede seguir accediendo a Internet.

Parámetro		**Descripción**
A diario	Cuota de tráfico	Indica la cuota de tráfico diaria para cada usuario.
	Duración del uso de Internet	Indica la duración diaria del acceso a Internet para cada usuario.
	Tiempo de reinicio	Puede configurar la hora de inicio (reinicio) para la recopilación de estadísticas de cuota de tráfico diaria y de duración de la conexión si estas no se recopilan en días naturales (por ejemplo, desde las 07:00 de cada día hasta las 07:00 del día siguiente). La hora de inicio

Inicio

		predeterminada para la recopilación de estadísticas de cuota de tráfico diaria y de duración de la conexión es a las 00:00 de la medianoche de cada día. Si se aplica el horario de verano (DST), no configure la hora de inicio (reinicio) de la recopilación de estadísticas con la hora de calibración. De lo contrario, las políticas de control de cuotas serán anormales en los días de inicio y fin del DST.
Mont	Cuota de tráfico	Indica la cuota de tráfico mensual para cada usuario.
	Tiempo de reinicio	Si las estadísticas no se recopilan por mes calendario (por ejemplo, del 15 de cada mes al 14 del mes siguiente), puede especificar la fecha de inicio para la recopilación de las estadísticas mensuales de cuota de tráfico. La fecha de inicio predeterminada es el 1 de cada mes.
Umbral de notificación		Indica un umbral de recordatorio para el uso de la cuota para cada usuario. Si el uso de la cuota alcanza el umbral de recordatorio preestablecido, el dispositivo envía una página del portal al navegador del usuario para recordarle el uso de la cuota.

5. Limite el ancho de banda máximo de cada usuario cuya cuota esté agotada.

Parámetro	**Descripción**
Exceso de ancho de banda máximo	Implementa bloqueo directo (si este valor se establece en 0) o limita el ancho de banda máximo. Se puede configurar el usuario o grupo de usuarios al que se aplica una política de control de cuotas. Si un usuario está referenciado por varias políticas de control de cuotas (incluida la referencia del grupo de usuarios), el valor máximo real del ancho de banda se determina por la cuota especificada en la política de mayor prioridad.

6. Haga clic en **Aceptar** .

Procedimiento de seguimiento

Inicio

página que se muestra, puede:

- Ver el uso de cuota del usuario en tiempo real.
- Borre las estadísticas de cuota del usuario. Tenga en cuenta que si más de dos cuotas alcanzan el umbral, borrar las estadísticas de una de ellas no impedirá que el servidor de seguridad realice la acción de administración y control.

Tema principal: **Configuración de una política de control de cuotas n interfaz web**

Siguiente

Derechos de autor © Huawei Technologies Co., Ltd.

REFERENCIAS TECNICAS

INGLES

Referencing Regions

Huawei Firewall Security Policy Essentials

Search this document. 0 / 500

Please evaluate and leave your comments:

Referencing Regions and Region Groups in Security Policies

A region maps a public IP address to a geographical location, and a region group is a set of regions. Therefore, a region and a region group You can use regions and region groups to configure security policies based on geographical locations. For example, an enterprise provides denies access from country A for security purposes. In this case, you can configure a security policy with the source address set to country A prevent users in country A from accessing the web service.

To simplify user operations, Huawei firewalls provide the geolocation database (pre-defined regions). Pre-defined regions in China can be s pre-defined regions outside China can be set at the country level.

The geolocation database is an IP address group divided by country and region. It is collected and maintained by Huawei and can be updat the upgrade center. The geolocation database is not updated in time. Therefore, three user-defined configuration methods are available for defined region is higher than that of a pre-defined region.

- User-defined region: You can manually create a region and add IP addresses that meet the requirements to it.
- Adding an IP address to a pre-defined region: If an IP address is missing in a pre-defined region, you can add it to the pre-defined region
- Excluding an IP address from a pre-defined region: If an IP address is incorrectly classified into a region, you can add the IP address to t region.

User-defined Region

User-defined regions are isolated and do not belong to pre-defined regions. Private IP addresses are used on the local area network (LAN) geographical country or region. By default, private IP addresses belong to the unknown zone. To manage and display LAN services by regic region for the private IP addresses of the LAN.

Create a user-defined region named **HangZhouBranch** and add the local LAN address segment to it.

```
location
 geo-location user-defined HangZhouBranch
  description Hangzhou branch
  add address 10.10.1.0 mask 24
```

Adding IP Addresses to a Pre-defined Region

If an IP address is not added to a region, service access may be affected. For example, an administrator configures a security policy to allo services, but a PC in region A fails to access the web services. If the security policy is correctly configured, the IP address of the PC must b region. In this case, you can add the IP address to region A.

Add IP address segment 10.20.20.20 to 10.20.20.30 to a pre-defined region named **BeiJing**.

```
location
 geo-location pre-defined BeiJing
  add address range 10.20.20.20 10.20.20.30
```

Excluding IP Addresses from a Pre-defined Region

Exclude IP address range 10.10.10.1 to 10.10.10.20 from pre-defined region **BeiJing** and add it to the unknown zone.

```
location
 geo-location pre-defined unknown-zone
  add address range 10.10.10.1 10.10.10.20
```

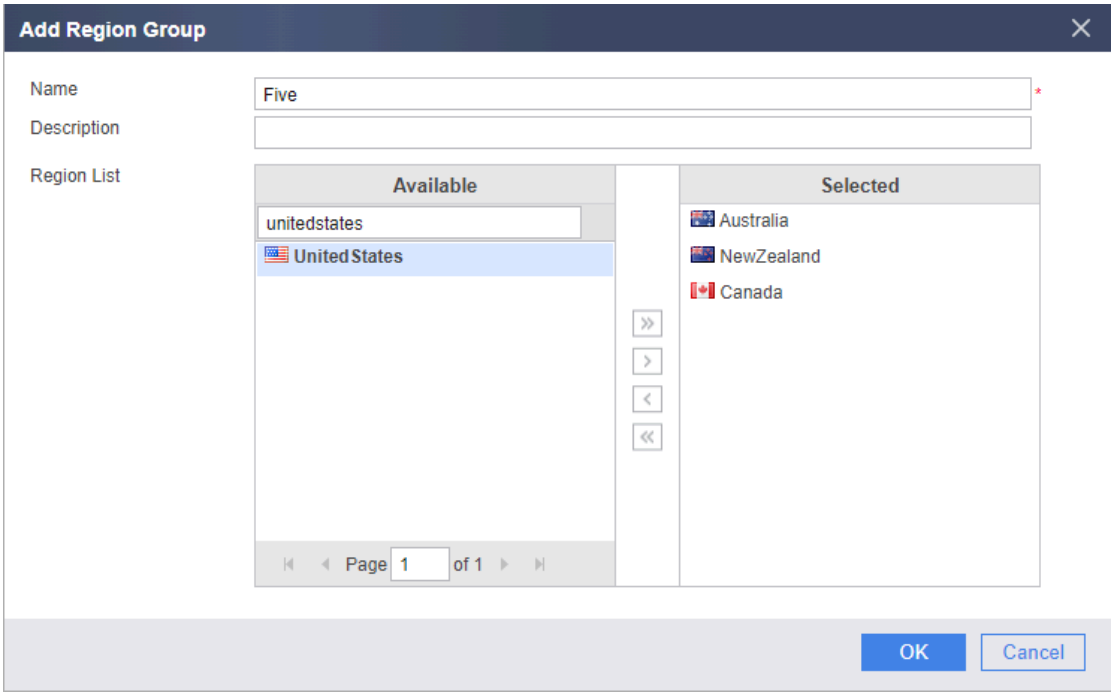
Referencing Region Groups in Security Policies

The following describes how to use a region group to prevent certain countries from accessing the HTTPS service in the DMZ.

Create region group **Five**. When adding countries in the command line, you can use the two-digit country code defined by the ISO standa names.

```
location
 geo-location-set Five
  add geo-location AU          //Add Australia using a two-digit country code.
  add geo-location CA
  add geo-location NewZealand    //Enter the country name directly. Pay attention to the case of and delete spa
  add geo-location UnitedKingdom
  add geo-location UnitedStates
```

Many countries and regions exist, and the country and region names need to be strictly input in the command line, which brings inconvenier region groups on the web page. In the **Available** area, you can enter a country name in the search box to quickly locate and select the cour



Configure a security policy to deny traffic from source address **Five** to access the HTTPS service.

```
security-policy
  rule name "Deny Five"
    source-zone untrust
    destination-zone dmz
    source-address geo-location Five   // Specify the source addresses using the region group
    service protocol https
    action deny
```

HUAWEI

About Us

How to Buy

Partner

Resources

Quick Links

Huawei e+ App

HUAWEI eKit App

Huawei HiKnow APP

HUAWEI eFly App

Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

Privacy Terms of use Cookies Cookie Settings Report content

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Referencing Regions

Fundamentos de la política de seguridad del firewall de Huawei

Buscar este documento. 0 / 500

Por favor evalúa y deja tus comentarios:

Referencias a regiones y grupos de regiones en políticas de seguridad

Una región asigna una dirección IP pública a una ubicación geográfica, y un grupo de regiones es un conjunto de regiones. Por lo tanto, un y grupos de regiones para configurar políticas de seguridad basadas en ubicaciones geográficas. Por ejemplo, una empresa proporciona s En este caso, puede configurar una política de seguridad con la dirección de origen establecida en el país A y la acción establecida en den

Para simplificar las operaciones del usuario, los firewalls de Huawei proporcionan una base de datos de geolocalización (regiones predefin las regiones predefinidas fuera de China se pueden configurar a nivel de país.

La base de datos de geolocalización es un grupo de direcciones IP dividido por país y región. Huawei la recopila y mantiene, y puede actua geolocalización no se actualiza periódicamente. Por lo tanto, existen tres métodos de configuración definidos por el usuario para los firewal

- Región definida por el usuario: puede crear manualmente una región y agregarle direcciones IP que cumplan con los requisitos.
- Agregar una dirección IP a una región predefinida: si falta una dirección IP en una región predefinida, puede agregarla a la región predef
- Excluir una dirección IP de una región predefinida: si una dirección IP se clasifica incorrectamente en una región, puede agregar la direc

Región definida por el usuario

Las regiones definidas por el usuario están aisladas y no pertenecen a regiones predefinidas. Las direcciones IP privadas se utilizan en la r direcciones IP privadas pertenecen a la zona desconocida. Para administrar y mostrar los servicios de LAN por región, puede crear una reg

Cree una región definida por el usuario denominada **HangZhouBranch** y agréguele el segmento de dirección LAN local.

```
ubicación
 Geolocalización definida por el usuario HangZhouBranch
  Descripción de la sucursal de Hangzhou
  agregar dirección 10.10.1.0 máscara 24
```

Agregar direcciones IP a una región predefinida

Si no se agrega una dirección IP a una región, el acceso a los servicios podría verse afectado. Por ejemplo, un administrador configura una pero un PC de la región A no puede acceder a ellos. Si la política de seguridad está configurada correctamente, la dirección IP del PC podr región A.

Agregue el segmento de dirección IP 10.20.20.20 a 10.20.20.30 a una región predefinida llamada **BeiJing** .

```
ubicación
 geolocalización predefinida de Pekín
  agregar rango de direcciones 10.20.20.20 10.20.20.30
```

Exclusión de direcciones IP de una región predefinida

Anterior

Excluir el rango de direcciones IP 10.10.10.1 a 10.10.10.20 de la región predefinida **Beijing** y agregarlo a la zona desconocida.

```
ubicación
 geolocalización predefinida zona desconocida
  agregar rango de direcciones 10.10.10.1 10.10.10.20
```

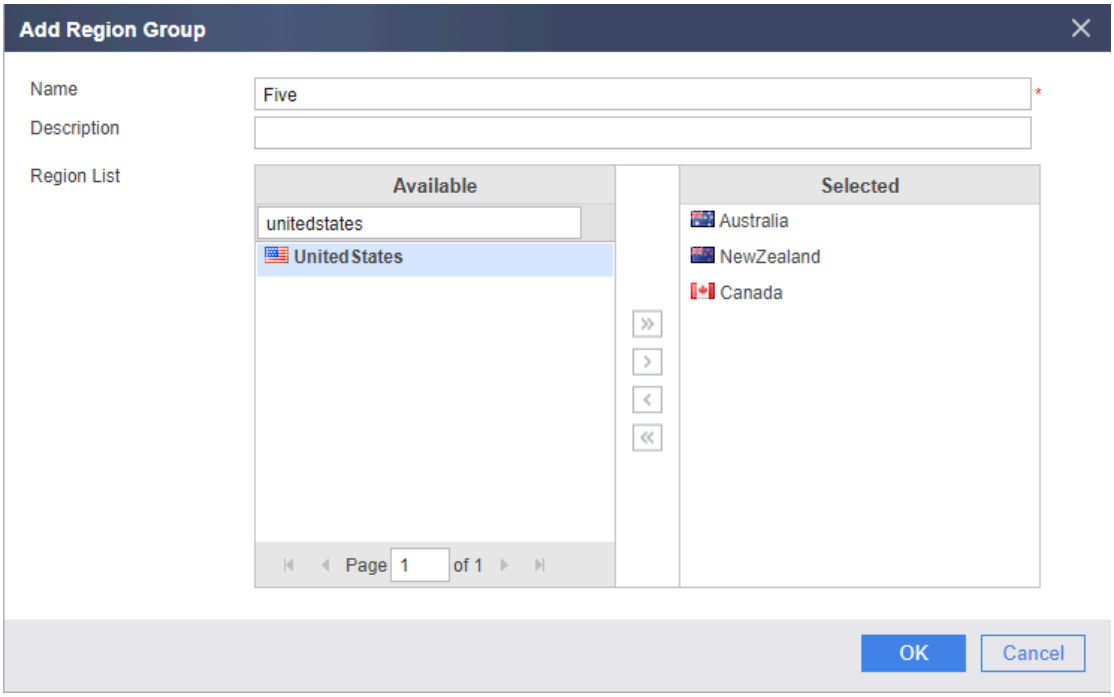
Referencias a grupos de regiones en políticas de seguridad

A continuación se describe cómo utilizar un grupo de regiones para evitar que ciertos países accedan al servicio HTTPS en la DMZ.

Crear el grupo de regiones **Cinco** . Al agregar países en la línea de comandos, puede usar el código de país de dos dígitos definido por l

```
ubicación
 conjunto de geolocalización cinco
  Agregar ubicación geográfica AU //Agregue Australia usando un código de país de dos dígitos.
  añadir geolocalización CA
  Agregar geolocalización de Nueva Zelanda // Ingrese el nombre del país directamente. Preste atención a las ma
  añadir geolocalización Reino Unido
  añadir geolocalización Estados Unidos
```

Existen muchos países y regiones, y los nombres de cada uno deben introducirse estrictamente en la línea de comandos, lo cual resulta in **Disponibles** ", puede introducir el nombre de un país en el cuadro de búsqueda para localizarlo y seleccionarlo rápidamente.



Configure una política de seguridad para denegar el tráfico desde la dirección de origen **Cinco** para acceder al servicio HTTPS.

```
política de seguridad
  Nombre de la regla: "Denegar cinco"
    desconfianza en la zona de origen
    zona de destino dmz
    geolocalización de la dirección de origen Cinco // Especifique las direcciones de origen utilizando el grup
    protocolo de servicio https
    acción denegar
```

Anterior

561

Cómo comprar

Pareja

Recursos

Enlaces rápidos

Aplicación Huawei e+

Aplicación HUAWEI eKit

Aplicación Huawei HiKnow

Aplicación HUAWEI eFly

Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

Privacidad Condiciones de uso Galletas Configuración de cookies Reportar contenido

Anterior

REFERENCIAS TECNICAS

INGLES

SNMP Version

SNMP Versions

SNMP versions include SNMPv1, SNMPv2c, and SNMPv3.
Both SNMPv1 and SNMPv2c use community name-based authentication. The NMS uses the community name list to control the device access rights, but the agent does not check whether the community name used by a given sender is authorized. Additionally, SNMP messages are not encrypted for transmission, so secure authentication and privacy are not ensured.
Compared with SNMPv1, SNMPv2c supports more operations, data types, error codes, and transport protocols.
SNMPv3 provides all the functions of SNMPv1 and SNMPv2c and also includes authentication and encryption of SNMP packets.
In terms of security, SNMPv3 emphasizes data security and access control.
SNMPv3 ensures the security of SNMP packets in the following ways:

- Data integrity checks: Data cannot be modified without an authorization and the sequence of data cannot be modified beyond what is specifically authorized.
- Data source verification: This verification makes it clear which user the received data comes from. SNMPv3 is user-based. Users who have generated data packets can be verified, but applications that generate the packets cannot.
- Data confidentiality check: When the NMS or an agent receives a packet, it checks when the packet was generated. If the difference between the generation time and the current system time exceeds a specified time range, the packet is discarded. This prevents packets from being maliciously modified during transmission and prevents malicious packets from being received or processed.

SNMPv3 access control involves security check and controls access to managed objects based on protocol operations.
Different SNMP versions are used in different scenarios. The differences are described in Table 1.

Table 1 Usage scenarios of SNMP versions

SNMP Version	Application Scenario
SNMPv1	SNMPv1 is used for simple small-scale networks that are secure and stable or have low security requirements, such as campus networks and small enterprise networks.
SNMPv2c	SNMPv2c is used for medium- and large-scale networks, which are secure (such as VPN networks) or have low security requirements but may get congested due to heavy traffic. SNMPv2c supports the Inform function, which ensures that the NMS can receive traps from managed devices.
SNMPv3	SNMPv3 is used for networks of any scale, particularly networks that have high security requirements and allow only authorized administrators to manage network devices. For example, in scenarios where the data exchanged between the NMS and managed devices needs to be transmitted over a public network, SNMPv3 can be used to authenticate and encrypt the data, ensuring the communication between the NMS and managed devices.

The features supported by different SNMP versions are listed in Table 2.

Table 2 Features supported by SNMP versions

Supported Feature	SNMPv1	SNMPv2c	SNMPv3
Access control	Community-name-based access control	Community-name-based access control	User- or user-group-based access control
Authentication and encryption	Not supported	Not supported	Authentication and encryption supported
Error code	Five error codes supported	16 error codes supported	16 error codes supported
Trap	Supported	Supported	Supported
Inform trap	Not supported	Supported	Supported
GetBulk	Not supported	Supported	Supported

The features are as follows:

- Access control is used to restrict a user's device management rights. This function allows a specified NMS to manage specified nodes on a device, achieving refined management.
- Authentication and encryption are used to prevent data packets transmitted between the NMS and managed devices from being intercepted or tampered with.

- Error codes help administrators to identify and rectify faults. The more varied and detailed the available error codes are, the easier it is for administrators to manage the devices.
- Traps are sent by managed devices to the NMS so that the administrator can detect device exceptions in a timely manner. A managed device does not require an acknowledgement from the NMS after sending traps.
- Inform alarms are sent from managed devices to the NMS as well. Upon receiving an Inform alarm from a managed device, the NMS needs to send a response packet for confirmation. If no response packet is received, the managed device sends Inform alarms repeatedly and generates the corresponding alarm log. In this way, if the NMS restarts, it can synchronize the Inform alarms sent during the restart. If no confirmation packet is received, the system saves the Inform alarms in the memory. That is why Inform alarms may consume a lot of system resources.
- GetBulk allows an administrator to perform GetNextRequest operations in batches. This reduces the workload and improves management efficiency especially on large networks.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

SNMP Version

Versiones de SNMP

Las versiones de SNMP incluyen SNMPv1, SNMPv2c y SNMPv3.
Tanto SNMPv1 como SNMPv2c utilizan autenticación basada en nombres de comunidad. El NMS utiliza la lista de nombres de comunidad para controlar los derechos de acceso del dispositivo, pero el agente no comprueba si el nombre de comunidad utilizado por un remitente determinado está autorizado. Además, los mensajes SNMP no se cifran para su transmisión, por lo que no se garantiza la autenticación segura ni la privacidad.
En comparación con SNMPv1, SNMPv2c admite más operaciones, tipos de datos, códigos de error y protocolos de transporte.
SNMPv3 proporciona todas las funciones de SNMPv1 y SNMPv2c y también incluye autenticación y cifrado de paquetes SNMP.
En términos de seguridad, SNMPv3 enfatiza la seguridad de los datos y el control de acceso.
SNMPv3 garantiza la seguridad de los paquetes SNMP de las siguientes maneras:

- Comprobaciones de integridad de los datos: los datos no se pueden modificar sin autorización y la secuencia de datos no se puede modificar más allá de lo que está específicamente autorizado.
- Verificación de la fuente de datos: Esta verificación permite determinar de qué usuario provienen los datos recibidos. SNMPv3 se basa en el usuario. Los usuarios que han generado paquetes de datos pueden verificarse, pero las aplicaciones que los generan no.
- Comprobación de confidencialidad de datos: Cuando el NMS o un agente recibe un paquete, verifica cuándo se generó. Si la diferencia entre la hora de generación y la hora actual del sistema supera un rango de tiempo especificado, el paquete se descarta. Esto evita que los paquetes se modifiquen maliciosamente durante la transmisión y que se reciban o procesen.

El control de acceso SNMPv3 implica una verificación de seguridad y controla el acceso a los objetos administrados en función de las operaciones del protocolo.
Se utilizan diferentes versiones de SNMP en distintos escenarios. Las diferencias se describen en la Tabla 1 .

Tabla 1 Escenarios de uso de las versiones de SNMP

Versión SNMP	Escenario de aplicación
SNMPv1	SNMPv1 se utiliza para redes simples de pequeña escala que son seguras y estables o tienen requisitos de seguridad bajos, como redes de campus y redes de pequeñas empresas.
SNMPv2c	SNMPv2c se utiliza para redes de escala mediana y grande que son seguras (como las redes VPN) o tienen requisitos de seguridad bajos pero que pueden congestionarse debido al tráfico pesado. SNMPv2c admite la función Inform, que garantiza que el NMS pueda recibir capturas de los dispositivos administrados.
SNMPv3	SNMPv3 se utiliza en redes de cualquier escala, especialmente en redes con altos requisitos de seguridad que permiten que solo administradores autorizados administren dispositivos de red. Por ejemplo, en escenarios donde los datos intercambiados entre el NMS y los dispositivos administrados deben transmitirse a través de una red pública, SNMPv3 puede utilizarse para autenticar y cifrar los datos, garantizando así la comunicación entre el NMS y los dispositivos administrados.

Las características admitidas por las diferentes versiones de SNMP se enumeran en la Tabla 2 .

Tabla 2 Características compatibles con las versiones de SNMP

Función compatible	SNMPv1	SNMPv2c	SNMPv3
Control de acceso	Control de acceso basado en nombres de la comunidad	Control de acceso basado en nombres de la comunidad	Control de acceso basado en usuarios o grupos de usuarios
Autenticación y cifrado	No compatible	No compatible	Admite autenticación y cifrado
Código de error	Se admiten cinco códigos de error	Se admiten 16 códigos de error	Se admiten 16 códigos de error
Trampa	Apoyado	Apoyado	Apoyado
Trampa de información	No compatible	Apoyado	Apoyado
Obtener a granel	No compatible	Apoyado	Apoyado

Las características son las siguientes:

- El control de acceso se utiliza para restringir los derechos de administración de dispositivos de un usuario. Esta función permite que un NMS específico administre nodos específicos en un dispositivo, logrando una gestión optimizada.

- La autenticación y el cifrado se utilizan para evitar que los paquetes de datos transmitidos entre el NMS y los dispositivos administrados sean interceptados o manipulados.
- Los códigos de error ayudan a los administradores a identificar y corregir fallos. Cuanto más variados y detallados sean los códigos de error disponibles, más fácil será para los administradores gestionar los dispositivos.
- Los dispositivos administrados envían traps al NMS para que el administrador pueda detectar excepciones de dispositivos a tiempo. Un dispositivo administrado no requiere confirmación del NMS después de enviar traps.
- Las alarmas de Inform también se envían desde los dispositivos administrados al NMS. Al recibir una alarma de Inform de un dispositivo administrado, el NMS debe enviar un paquete de respuesta de confirmación. Si no se recibe ningún paquete de respuesta, el dispositivo administrado envía alarmas de Inform repetidamente y genera el registro de alarmas correspondiente. De esta forma, si el NMS se reinicia, puede sincronizar las alarmas de Inform enviadas durante el reinicio. Si no se recibe ningún paquete de confirmación, el sistema guarda las alarmas de Inform en la memoria. Por ello, las alarmas de Inform pueden consumir muchos recursos del sistema.
- GetBulk permite al administrador ejecutar operaciones GetNextRequest por lotes. Esto reduce la carga de trabajo y mejora la eficiencia de la administración, especialmente en redes grandes.

REFERENCIAS TECNICAS

INGLES

Traffic Shaping

Enterprise Support

Size: 264.12MB

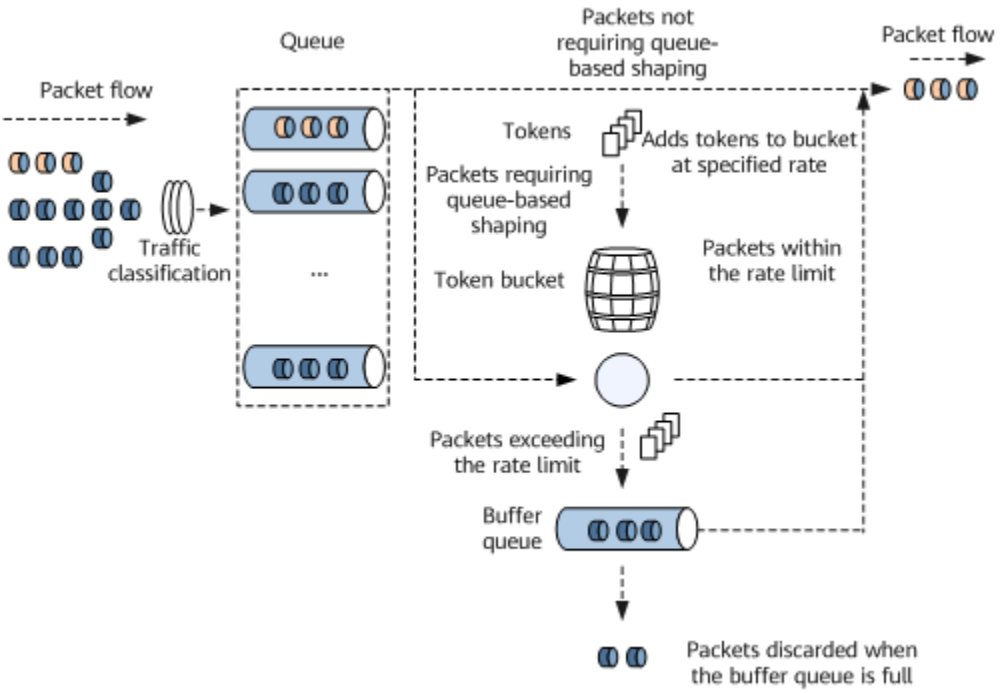
Enter keywords 0 / 256

Traffic Shaping

Traffic shaping adjusts the rate of outgoing traffic to reduce traffic bursts so that outgoing packets can be transmitted at a stable rate. Traffic shaping uses a buffer and token buckets to control the traffic rate. When packets are sent at a high rate, the system buffers packets and then sends them evenly under the control of the token buckets.

Figure 1 shows an example of traffic shaping, using flow-based queue shaping in single-rate-single-bucket mode.

Figure 1 Traffic shaping



Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Traffic Shaping

Tamaño: 264,12 MB

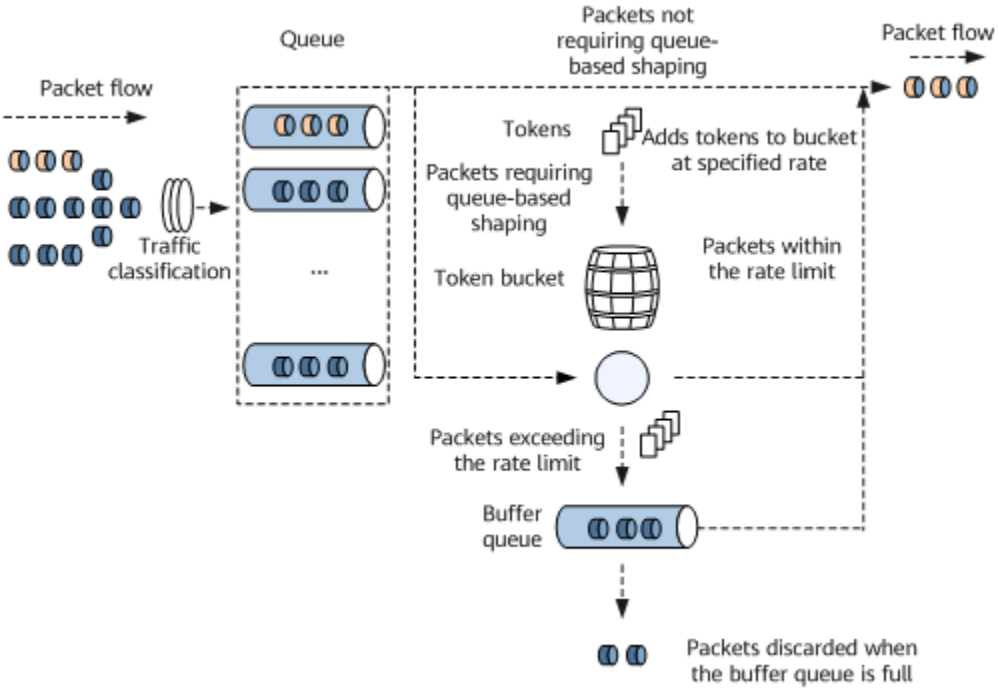
Introduzca palabras clave 0 / 256

Modelado del tráfico

El modelado de tráfico ajusta la velocidad del tráfico saliente para reducir las ráfagas de tráfico, de modo que los paquetes salientes se transmitan a una velocidad estable. El modelado de tráfico utiliza un búfer y contenedores de tokens para controlar la velocidad del tráfico. Cuando los paquetes se envían a una velocidad alta, el sistema los almacena en el búfer y los envía uniformemente bajo el control de los contenedores de tokens.

La figura 1 muestra un ejemplo de modelado de tráfico , utilizando modelado de cola basado en flujo en modo de tasa única y contenedor único.

Figura 1 Conformación del tráfico



Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

REFERENCIAS TECNICAS

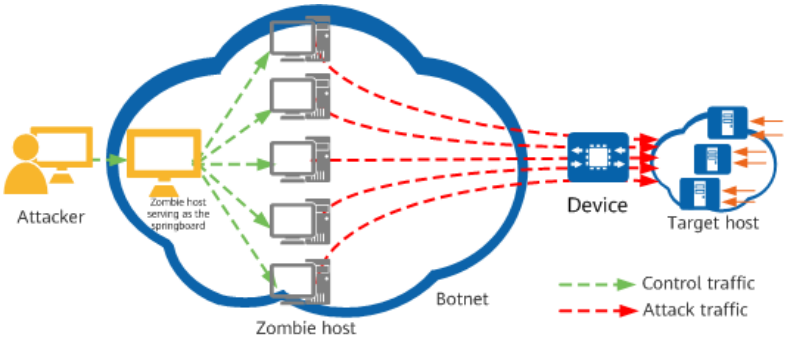
INGLES

Understanding Attack

Understanding Attack Defense

Also known as traffic attacks, DDoS attacks use controlled zombie hosts to send a large number of attack packets to a target. These attack packets congest network links and exhaust system resources, preventing the target from providing services for legitimate users.
Figure 1 shows a schematic diagram of a DDoS attack. Zombie hosts are online hosts controlled by an attacker, and a network comprised of attackers and zombie hosts is called a botnet.

Figure 1 Schematic diagram of a DDoS attack



DDoS attacks on the network are categorized into various types depending on the types of packets used. The device can defend against the following types of DDoS attacks: SYN flood, UDP flood, ICMP flood, HTTP flood, HTTPS flood, DNS flood, and SIP flood.
Table 1 lists the key technologies used by the device to defend against DDoS attacks.

Table 1 Key technologies for defense against the DDoS attack

Technology	Mechanism	Applicable Attack Type	Restriction
Source IP address detection	The device detects the source IP address of a request packet. If the source IP address is real, the packet is forwarded; otherwise, the packet is discarded.	SYN flood, HTTP flood, HTTPS flood, DNS request flood, DNS reply flood, and SIP flood	This defense technology requires the client to support source detection (that is, the client can properly process source detection reply packets). If the client does not support source detection, normal client requests will be discarded. In addition, this defense technology cannot mitigate flood attacks initiated using real IP addresses.
Fingerprint	The device collects statistics on a segment of data in packets destined for the destination IP address. The same characteristic is used as the fingerprint, and the device discards the packets that match the fingerprint.	UDP flood and UDP fragment flood	If normal service packets also carry fingerprints, fingerprint-based defense does not apply.
Dynamic traffic limiting	The device checks the attack traffic on the CPU. When either the session packet rate or traffic rate reaches the specified threshold, the device delivers dynamic rules to the advanced ACL referenced in the specified traffic policy, thereby limiting the rate of attack traffic on the chip and reducing the CPU usage.	All transport-layer traffic attacks	Traffic limiting discards all packets that exceed the upper limit. Therefore, exercise caution when enabling traffic limiting.

NOTE

- In DDoS attack defense, the device identifies abnormal packets based on the preceding technologies, which have restrictions on application scenarios. Applied to a wrong scenario, a defense technology may cause the device to identify normal service packets as abnormal packets and discard them. You are advised to enable attack defense functions based on network conditions, attack defense mechanisms, and restrictions. For details, see "Configuration Precautions for Attack Defense" and sections on each type of attack defense.

- The device can defend against DDoS attacks of both IPv4 and IPv6 packets.
- The device can protect only the internal network behind it. Congestion between the device and carrier network needs to be prevented by the carrier.

In addition to DDoS attacks, the attack defense function can also defend against single-packet attacks, which are categorized as scanning attacks, malformed packet attacks, and special packet attacks:

- Scanning attacks can be further classified as IP sweep and port scanning attacks. In an IP sweep attack, an attacker sends IP packets such as TCP, UDP, and ICMP packets where the destination IP addresses change constantly, to find existing hosts and networks. This approach enables potential attack targets to be accurately detected. In a port scanning attack, an attacker scans TCP and UDP ports in order to detect the operating system and potential services of the target. Through scanning and sniffing, the attacker can roughly determine which types of services the target system provides as well as its potential vulnerabilities, allowing it to prepare for further intrusions on the target system.
- In a malformed packet attack, an attacker sends defective IP packets to a target system, which can cause the target system to encounter errors or crash. Malformed packet attacks can be further classified as Ping of Death and Teardrop attacks.
- In a special packet attack, an attacker probes the network environment using packets that are legitimate but rarely used. Special packet attacks include large ICMP packet control, Tracert packet attack, and IP timestamp option control.
  In order to effectively defend against single-packet attacks, the device obtains the characteristics of attack packets, identifies attack packets based on these characteristics, and performs corresponding operations. The attack defense function can defend against all types of single-packet attacks that use IPv4 packets. For IPv6 packets, however, the attack defense function can only defend against IP address spoofing attacks and IPv6 extension header attacks.

REFERENCIAS TECNICAS

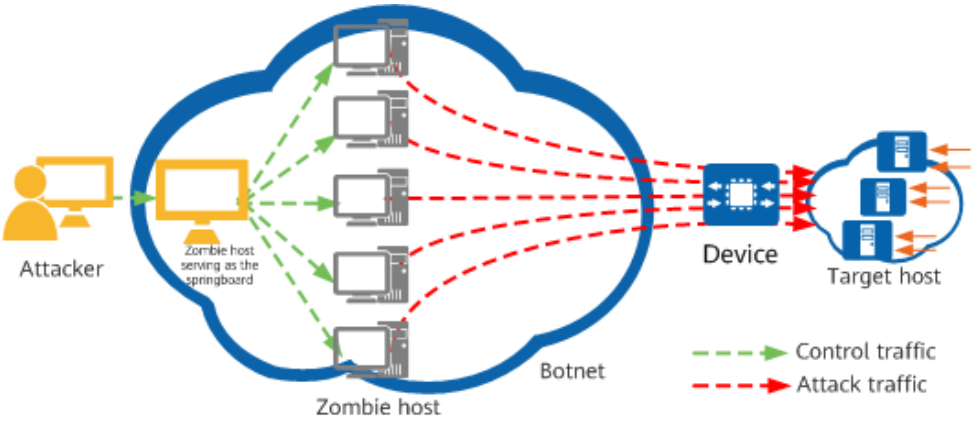
TRADUCCION SIMPLE

Understanding Attack

Entendiendo la defensa contra ataques

También conocidos como ataques de tráfico, los ataques DDoS utilizan hosts zombi controlados para enviar una gran cantidad de paquetes de ataque a un objetivo. Estos paquetes de ataque congestionan los enlaces de red y agotan los recursos del sistema, impidiendo que el objetivo preste servicios a usuarios legítimos.
La Figura 1 muestra un diagrama esquemático de un ataque DDoS. Los hosts zombi son hosts en línea controlados por un atacante, y una red compuesta por atacantes y hosts zombi se denomina botnet.

Figura 1 Diagrama esquemático de un ataque DDoS



Los ataques DDoS a la red se clasifican en varios tipos según el tipo de paquete utilizado. El dispositivo puede defenderse de los siguientes tipos de ataques DDoS: inundación SYN, inundación UDP, inundación ICMP, inundación HTTP, inundación HTTPS, inundación DNS e inundación SIP.
En la Tabla 1 se enumeran las tecnologías clave que utiliza el dispositivo para defenderse de ataques DDoS.

Tabla 1 Tecnologías clave para la defensa contra el ataque DDoS

Tecnología	Mecanismo	Tipo de ataque aplicable	Restricción
Detección de la dirección IP de origen	El dispositivo detecta la dirección IP de origen de un paquete de solicitud. Si la dirección IP de origen es real, el paquete se reenvía; de lo contrario, se descarta.	Inundación SYN, inundación HTTP, inundación HTTPS, inundación de solicitudes DNS, inundación de respuestas DNS e inundación SIP	Esta tecnología de defensa requiere que el cliente admita la detección de origen (es decir, que pueda procesar correctamente los paquetes de respuesta de detección de origen). Si el cliente no admite la detección de origen, se descartarán las solicitudes normales del cliente. Además, esta tecnología de defensa no puede mitigar los ataques de inundación iniciados con direcciones IP reales.

Tecnología	Mecanismo	Tipo de ataque aplicable	Restricción
Huella dactilar	El dispositivo recopila estadísticas sobre un segmento de datos en paquetes destinados a la dirección IP de destino. Se utiliza la misma característica que la huella digital y el dispositivo descarta los paquetes que coinciden con ella.	Inundación de UDP e inundación de fragmentos de UDP	Si los paquetes de servicio normales también llevan huellas dactilares, la defensa basada en huellas dactilares no se aplica.
Limitación dinámica del tráfico	El dispositivo verifica el tráfico de ataque en la CPU. Cuando la tasa de paquetes de sesión o la tasa de tráfico alcanzan el umbral especificado, el dispositivo envía reglas dinámicas a la ACL avanzada referenciada en la política de tráfico especificada, lo que limita la tasa de tráfico de ataque en el chip y reduce el uso de la CPU.	Todos los ataques al tráfico de la capa de transporte	La limitación de tráfico descarta todos los paquetes que superan el límite superior. Por lo tanto, tenga cuidado al activarla.

NOTE

- En la defensa contra ataques DDoS, el dispositivo identifica paquetes anormales según las tecnologías anteriores, las cuales tienen restricciones según los escenarios de aplicación. Si se aplica una tecnología de defensa a un escenario incorrecto, el dispositivo puede identificar paquetes de servicio normales como anormales y descartarlos. Se recomienda habilitar las funciones de defensa contra ataques según las condiciones de la red, los mecanismos de defensa contra ataques y las restricciones. Para obtener más información, consulte "Precauciones de configuración para la defensa contra ataques" y las secciones sobre cada tipo de defensa.
- El dispositivo puede defenderse contra ataques DDoS de paquetes IPv4 e IPv6.
- El dispositivo solo puede proteger la red interna que lo respalda. El operador debe evitar la congestión entre el dispositivo y la red del operador.

Además de los ataques DDoS, la función de defensa contra ataques también puede defenderse contra ataques de un solo paquete, que se clasifican como ataques de escaneo, ataques de paquetes malformados y ataques de paquetes especiales:

- Los ataques de escaneo pueden clasificarse en barridos de IP y de puertos. En un ataque de barrido de IP, el atacante envía paquetes IP, como TCP, UDP e ICMP, cuyas direcciones IP de destino cambian constantemente, para encontrar hosts y redes existentes. Este enfoque permite detectar con precisión los posibles objetivos de ataque. En un ataque de escaneo de puertos, el atacante escanea los puertos TCP y UDP para detectar el sistema operativo y los posibles servicios del objetivo. Mediante el escaneo y el rastreo, el atacante puede determinar de forma aproximada qué tipos de servicios ofrece el sistema objetivo, así como sus posibles vulnerabilidades, lo que le permite prepararse para futuras intrusiones en el sistema objetivo.
- En un ataque de paquete malformado, un atacante envía paquetes IP defectuosos a un sistema objetivo, lo que puede provocar errores o un bloqueo en el sistema objetivo. Los ataques de paquete malformado se clasifican en

ataques de ping de la muerte y ataques de lágrima.

- En un ataque de paquetes especiales, un atacante explora el entorno de red mediante paquetes legítimos, pero poco utilizados. Entre estos ataques se incluyen el control de paquetes ICMP de gran tamaño, el ataque de paquetes Tracert y el control de opciones de marca de tiempo IP.
  Para defenderse eficazmente contra ataques de un solo paquete, el dispositivo obtiene las características de los paquetes de ataque, los identifica basándose en ellas y realiza las operaciones correspondientes. La función de defensa contra ataques puede defenderse contra todo tipo de ataques de un solo paquete que utilizan paquetes IPv4. Sin embargo, para los paquetes IPv6, la función de defensa contra ataques solo puede defenderse contra ataques de suplantación de direcciones IP y ataques de encabezados de extensión IPv6.

REFERENCIAS TECNICAS

INGLES

Understanding SIP

Size: 264.12MB

Enter keywords 0 / 256

Understanding SIP ASPF/ALG

The Session Initiation Protocol (SIP) is an IETF standard protocol used to create, modify, and release sessions of one or more participants. These sessions can be interactive user sessions that involve multimedia elements such as voice calls, multimedia conferences, and virtual reality.

SIP is a multi-channel protocol. In addition to establishing signaling channels for transmitting signaling, the calling and called parties also establish data channels for transmitting media data such as voice and video data. Therefore, SIP traffic is classified into signaling streams and media streams. Signaling streams are transmitted through UDP or TCP, including requests and responses from both parties. Media streams are transmitted through RTP and RTCP, including media (such as voice and video) data packets.

SIP can use UDP port 5060 or TCP port 5060 (non-encryption)/5061 (TLS encryption) to transmit signaling streams. To ensure that signaling streams can pass through the security device (Device used as an example), you need to configure a security policy on the Device to allow SIP signaling traffic to pass through. Media streams, however, are transmitted through a port negotiated dynamically and the port number cannot be learned in advance; therefore, the administrator cannot configure refined security policies to control the forwarding of media streams.

In the NAT scenario, common NAT can only translate the IP address and port carried in the network layer information of the packets and cannot translate the IP address and port carried in the application layer information. As a result, subsequent signaling and media streams cannot be exchanged.

In this case, the SIP ASPF/ALG function needs to be enabled on the Device for detecting and translating the IP address and port carried in the application layer information and recording the information in the server map. The media data packets match the server map when passing through the Device and are permitted, which are no longer controlled by security policies.

As shown in Figure 1, client A is located on the intranet, and client B and the SIP proxy are located on the Internet in the source NAT scenario. This section describes the key interaction process among client A, client B, and the SIP proxy and the processing of packets after the ASPF/ALG function is enabled on the Device.

Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Understanding SIP

Tamaño: 264,12 MB

Introduzca palabras clave 0 / 256

Entendiendo SIP ASPF/ALG

El Protocolo de Iniciación de Sesión (SIP) es un protocolo estándar del IETF que se utiliza para crear, modificar y liberar sesiones de uno o más participantes. Estas sesiones pueden ser sesiones de usuario interactivas que incluyen elementos multimedia como llamadas de voz, conferencias multimedia y realidad virtual.

SIP es un protocolo multicanal. Además de establecer canales de señalización para la transmisión de señales, tanto la parte llamante como la parte llamada también establecen canales de datos para la transmisión de datos multimedia, como voz y vídeo. Por lo tanto, el tráfico SIP se clasifica en flujos de señalización y flujos multimedia. Los flujos de señalización se transmiten mediante UDP o TCP, incluyendo solicitudes y respuestas de ambas partes. Los flujos multimedia se transmiten mediante RTP y RTCP, incluyendo paquetes de datos multimedia (como voz y vídeo). SIP puede usar el puerto UDP 5060 o el puerto TCP 5060 (sin cifrado)/5061 (cifrado TLS) para transmitir flujos de señalización. Para garantizar que los flujos de señalización puedan pasar a través del dispositivo de seguridad (el dispositivo se usa como ejemplo), debe configurar una política de seguridad en el dispositivo que permita el tráfico de señalización SIP . Sin embargo, los flujos de medios se transmiten a través de un puerto negociado dinámicamente y el número de puerto no se puede conocer de antemano; por lo tanto, el administrador no puede configurar políticas de seguridad refinadas para controlar el reenvío de flujos de medios.

En el escenario NAT, el NAT común solo puede traducir la dirección IP y el puerto presentes en la información de la capa de red de los paquetes, pero no la de la capa de aplicación. Por lo tanto, no se pueden intercambiar señales ni flujos de medios posteriores.

En este caso, es necesario habilitar la función SIP ASPF/ALG en el dispositivo para detectar y traducir la dirección IP y el puerto presentes en la información de la capa de aplicación y registrarlos en el mapa del servidor. Los paquetes de datos multimedia coinciden con el mapa del servidor al pasar por el dispositivo y se permiten, lo que ya no está controlado por las políticas de seguridad.

Como se muestra en la Figura 1 , el cliente A se encuentra en la intranet, mientras que el cliente B y el proxy SIP se encuentran en Internet en el escenario NAT de origen. Esta sección describe la

Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

REFERENCIAS TECNICAS

INGLES

Understanding URL

Enterprise Support

Size: 264.12MB

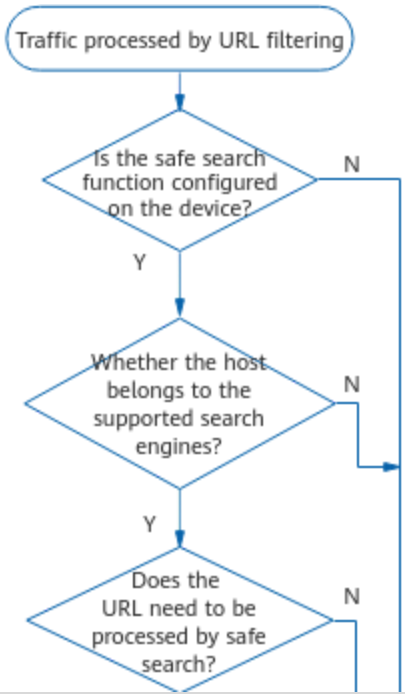
Enter keywords 0 / 256

Understanding URL Safe Search

Safe search is a function of the search engine that automatically filters pornographic contents and potential attacks. To regulate Internet access behavior, you can enable URL safe search on the device, so as to enable safe search for all Internet access users. After the URL safe search function is enabled on the device, the device forcibly performs safe search on the search requests of Bing, Google, Yahoo, Yandex, and YouTube search engines to filter the search results of the five engines.

URL safe search is performed after URL filtering is completed. After URL filtering is completed, safe search needs to be performed for all the packets excluding the whitelisted or blocked packets. For details, see Figure 1.

Figure 1 URL safe search process



Copyright © 2025 Huawei Technologies Co., Ltd. All rights reserved.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Understanding URL

Soporte empresarial

Tamaño: 264,12 MB

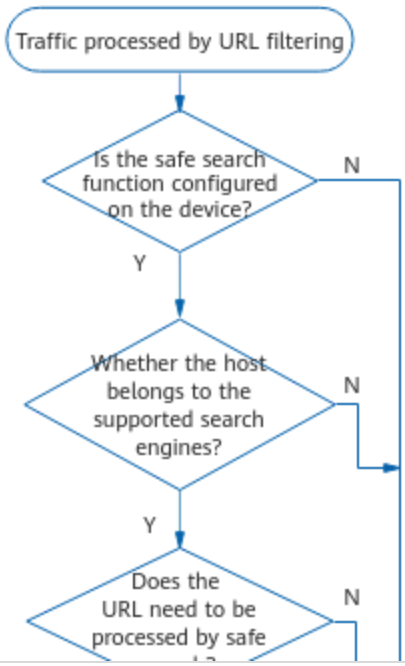
Introduzca palabras clave 0 / 256

Comprensión de la búsqueda segura de URL

La búsqueda segura es una función del motor de búsqueda que filtra automáticamente el contenido pornográfico y posibles ataques. Para controlar el acceso a Internet, puede habilitar la búsqueda segura de URL en el dispositivo para que todos los usuarios puedan acceder a ella. Una vez habilitada, el dispositivo realiza búsquedas seguras en las solicitudes de búsqueda de Bing, Google, Yahoo, Yandex y YouTube para filtrar los resultados de los cinco motores.

La búsqueda segura de URL se realiza tras completar el filtrado de URL. Una vez finalizado el filtrado, se debe realizar una búsqueda segura de todos los paquetes, excepto los incluidos en la lista blanca o bloqueados. Para más detalles, consulte la Figura 1 .

Figura 1 Proceso de búsqueda segura de URL



Copyright © 2025 Huawei Technologies Co., Ltd. Todos los derechos reservados.

REFERENCIAS TECNICAS

INGLES

User Authentication

User Authentication Modes

The CloudCampus Solution supports three authentication modes: Portal authentication, MAC address authentication, and 802.1X authentication.

- Portal authentication is also called web authentication. Generally, Portal authentication websites are referred to as web portals. When a user accesses the Internet, the user must be authenticated on the web portal. If the user fails to be authenticated, the user can access only specified network resources. The user can access other network resources only after passing the authentication. A Portal server pushes the web authentication page to the user's terminal. The user enters the user name and password on the authentication page, and is then authenticated through the protocol interaction between the Portal server, access control device, and authentication server. Portal authentication does not require any client software to be installed on a terminal, which is flexible and a good choice for guests and traveling users. Additionally, the authentication page can be customized.
- MAC address authentication enables terminals to be authenticated based on their MAC addresses. When a terminal attempts to access the network, an access control device obtains the MAC address of the terminal and uses the MAC address as the user name and password for authentication. MAC addresses can be easily forged, so the MAC address authentication mode is less secure. In addition, MAC addresses need to be registered on an authentication server, resulting in complex management. In some special cases, this authentication mode can be used when end users do not want to or are unable to enter user account information for authentication. For example, user account information cannot be entered on dumb terminals such as printers and IP phones.
- 802.1X is a port-based NAC protocol, which authenticates users based on the ports of LAN access devices. In 802.1X authentication, an authentication client must be installed on a terminal, and the user name and password must be entered on the authentication client. The authentication client, access control device, and authentication server communicate with each other to authenticate and verify the user identity. 802.1X authentication has the highest security among all authentication modes and applies to scenarios where new networks are deployed, users are centralized, and strict information security requirements are imposed. It is recommended that 802.1X authentication be deployed on access devices.

Table 1 compares the three authentication modes.

Table 1 Comparison between user authentication technologies

Item	Portal Authentication	MAC Address Authentication	802.1X Authentication

Item	Portal Authentication	MAC Address Authentication	802.1X Authentication
Client	Not required	Not required	Required
Advantage	Flexible deployment	No client required	High security
Disadvantage	Low security	MAC address registration required, making management complex	Inflexible deployment
Application scenario	Authentication of guests who move frequently and use different types of terminals	Authentication of dumb terminals such as printers and fax machines	Authentication of office users in scenarios with high security requirements

To adapt to various application scenarios, the following Portal authentication modes are supported: user name and password authentication, anonymous authentication, SMS authentication, and social media authentication.

Table 2 Portal authentication modes

Authentication Mode	Characteristics	Prerequisites	Application Scenarios
User name and password authentication	An end user can use the user name and password created by the tenant administrator or register an account for access authentication.	-	• Authentication based on the user name and password created by an administrator is applicable to a fixed user group, for example, enterprise employees. • Authentication based on accounts registered by users is applicable to scenarios where access permission

Authentication Mode	Characteristics	Prerequisites	Application Scenarios
			of guests such as membership needs to be verified. The accounts registered by users need to be approved.
Anonymous authentication	Guests access the network without using any accounts. The controller automatically displays the login accounts of the guests as anonymous accounts.	-	This mode is applicable to open networks on which the Internet access service is provided for customers free of charge.
SMS authentication	A user enters a mobile number as the user name and clicks the button for obtaining a password. The SMS server then sends a password to the user. The system automatically registers and authenticates the user name and password after the user enters the password.	An SMS server has been configured.	This mode is applicable to guest authentication. SMS authentication improves the validity of guest identities and enables merchants to obtain user information more conveniently so that they can interact with the guests.

Authentication Mode	Characteristics	Prerequisites	Application Scenarios
Social media authentication	iMaster NCE-Campus interworks with the WeChat or Facebook platform, so that users can use their existing social media accounts and passwords to perform authentication on the iMaster NCE-Campus web UI. After being authenticated, users can access the network.	• For WeChat authentication, an enterprise has its own WeChat official account platform, which can communicate with iMaster NCE-Campus. • For Facebook authentication, an enterprise has applied for and obtained an independent Facebook account from Facebook.	• WeChat authentication is applicable to the scenario where shopping malls provide free Internet access services for guests who follow their public accounts. • Facebook authentication is applicable to shopping malls that provide free Internet access services for guests.
Passcode authentication	Users enter the passcode on the pushed page for access authentication.	-	This authentication mode is simple and ideal to guest access scenarios in stores.

Parent Topic: **NAC Design**

Copyright © Huawei Technologies Co., Ltd.

〈 Previous Next topic 〉

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

User Authentication

Modos de autenticación de usuario

La solución CloudCampus admite tres modos de autenticación: autenticación de portal, autenticación de dirección MAC y autenticación 802.1X.

- La autenticación de portal también se denomina autenticación web. Generalmente, los sitios web con autenticación de portal se denominan portales web. Cuando un usuario accede a Internet, debe autenticarse en el portal web. Si no se autentica, solo podrá acceder a los recursos de red especificados. Solo podrá acceder a otros recursos de red después de pasar la autenticación. Un servidor de portal envía la página de autenticación web al terminal del usuario. El usuario introduce su nombre de usuario y contraseña en la página de autenticación y se autentica mediante la interacción de protocolo entre el servidor de portal, el dispositivo de control de acceso y el servidor de autenticación. La autenticación de portal no requiere la instalación de ningún software cliente en el terminal, lo que resulta flexible y una excelente opción para huéspedes y usuarios que viajan. Además, la página de autenticación se puede personalizar.
- La autenticación por dirección MAC permite autenticar terminales según sus direcciones MAC. Cuando un terminal intenta acceder a la red, un dispositivo de control de acceso obtiene la dirección MAC del terminal y la utiliza como nombre de usuario y contraseña para la autenticación. Las direcciones MAC se pueden falsificar fácilmente, por lo que el modo de autenticación por dirección MAC es menos seguro. Además, las direcciones MAC deben registrarse en un servidor de autenticación, lo que resulta en una gestión compleja. En algunos casos especiales, este modo de autenticación puede utilizarse cuando los usuarios finales no desean o no pueden introducir la información de su cuenta de usuario para la autenticación. Por ejemplo, la información de la cuenta de usuario no se puede introducir en terminales de baja potencia como impresoras y teléfonos IP.
- 802.1X es un protocolo NAC basado en puertos que autentica a los usuarios según los puertos de los dispositivos de acceso LAN. Para la autenticación 802.1X, se debe instalar un cliente de autenticación en un terminal, donde se deben introducir el nombre de usuario y la contraseña. El cliente de autenticación, el dispositivo de control de acceso y el servidor de autenticación se comunican entre sí para autenticar y verificar la identidad del usuario. La autenticación 802.1X ofrece la mayor seguridad entre todos los modos de autenticación y se aplica en escenarios donde se implementan nuevas redes, se centraliza a los usuarios y se imponen estrictos requisitos de seguridad de la información. Se recomienda implementar la autenticación 802.1X en los dispositivos de acceso.

En la Tabla 1 se comparan los tres modos de autenticación.

Tabla 1 Comparación entre tecnologías de autenticación de usuarios

Artículo	Autenticación del portal	Autenticación de dirección MAC	Autenticación 802.1X
Cliente	No requerido	No requerido	Requerido
Ventaja	Implementación flexible	No se requiere cliente	Alta seguridad
Desventaja	Baja seguridad	Se requiere el registro de la dirección MAC, lo que hace que la gestión sea compleja	Despliegue inflexible

Artículo	Autenticación del portal	Autenticación de dirección MAC	Autenticación 802.1X
Escenario de aplicación	Autenticación de huéspedes que se desplazan con frecuencia y utilizan distintos tipos de terminales	Autenticación de terminales tontas como impresoras y máquinas de fax	Autenticación de usuarios de oficina en escenarios con altos requerimientos de seguridad

Para adaptarse a varios escenarios de aplicación, se admiten los siguientes modos de autenticación del Portal: autenticación de nombre de usuario y contraseña, autenticación anónima, autenticación por SMS y autenticación por redes sociales.

Tabla 2 Modos de autenticación del portal

Modo de autenticación	Características	Prerrequisitos	Escenarios de aplicación
Autenticación de nombre de usuario y contraseña	Un usuario final puede utilizar el nombre de usuario y la contraseña creados por el administrador del inquilino o registrar una cuenta para la autenticación del acceso.	-	• La autenticación basada en el nombre de usuario y la contraseña creada por un administrador es aplicable a un grupo de usuarios fijo, por ejemplo, empleados de la empresa. • La autenticación basada en cuentas registradas por los usuarios es aplicable a situaciones en las que se requiere verificar el acceso de invitados, como la membresía. Las cuentas

Modo de autenticación	Características	Prerrequisitos	Escenarios de aplicación
			registradas por los usuarios deben ser aprobadas.
Autenticación anónima	Los invitados acceden a la red sin usar ninguna cuenta. El controlador muestra automáticamente las cuentas de inicio de sesión de los invitados como anónimas.	-	Esta modalidad es aplicable a redes abiertas en las que se presta el servicio de acceso a Internet a los clientes de forma gratuita.
Autenticación por SMS	El usuario introduce un número de teléfono móvil como nombre de usuario y pulsa el botón para obtener una contraseña. El servidor SMS le envía una contraseña. El sistema registra y autentica automáticamente el nombre de usuario y la contraseña una vez que el usuario la introduce.	Se ha configurado un servidor SMS.	Este modo se aplica a la autenticación de invitados. La autenticación por SMS mejora la validez de la identidad de los invitados y permite a los comerciantes obtener información del usuario con mayor facilidad para interactuar con ellos.
Autenticación en redes sociales	iMaster NCE-Campus interactúa con las plataformas WeChat o Facebook, lo que permite a los usuarios usar sus cuentas y contraseñas de redes sociales para autenticarse en la interfaz web de iMaster NCE-Campus . Tras la autenticación, pueden acceder a la red.	• Para la autenticación de WeChat, una empresa tiene su propia plataforma de cuenta oficial de WeChat, que puede comunicarse con iMaster NCE-Campus.	• La autenticación de WeChat es aplicable al escenario en el que los centros comerciales ofrecen servicios de acceso gratuito a Internet para los huéspedes que siguen sus

Modo de autenticación	Características	Prerrequisitos	Escenarios de aplicación
		• Para la autenticación de Facebook, una empresa ha solicitado y obtenido una cuenta de Facebook independiente de Facebook.	cuentas públicas. • La autenticación de Facebook se aplica a los centros comerciales que ofrecen servicios de acceso gratuito a Internet para sus huéspedes.
Autenticación con código de acceso	Los usuarios ingresan el código de acceso en la página enviada para autenticar el acceso.	-	Este modo de autenticación es simple e ideal para escenarios de acceso de invitados en tiendas.

REFERENCIAS TECNICAS

INGLES

User Organizational

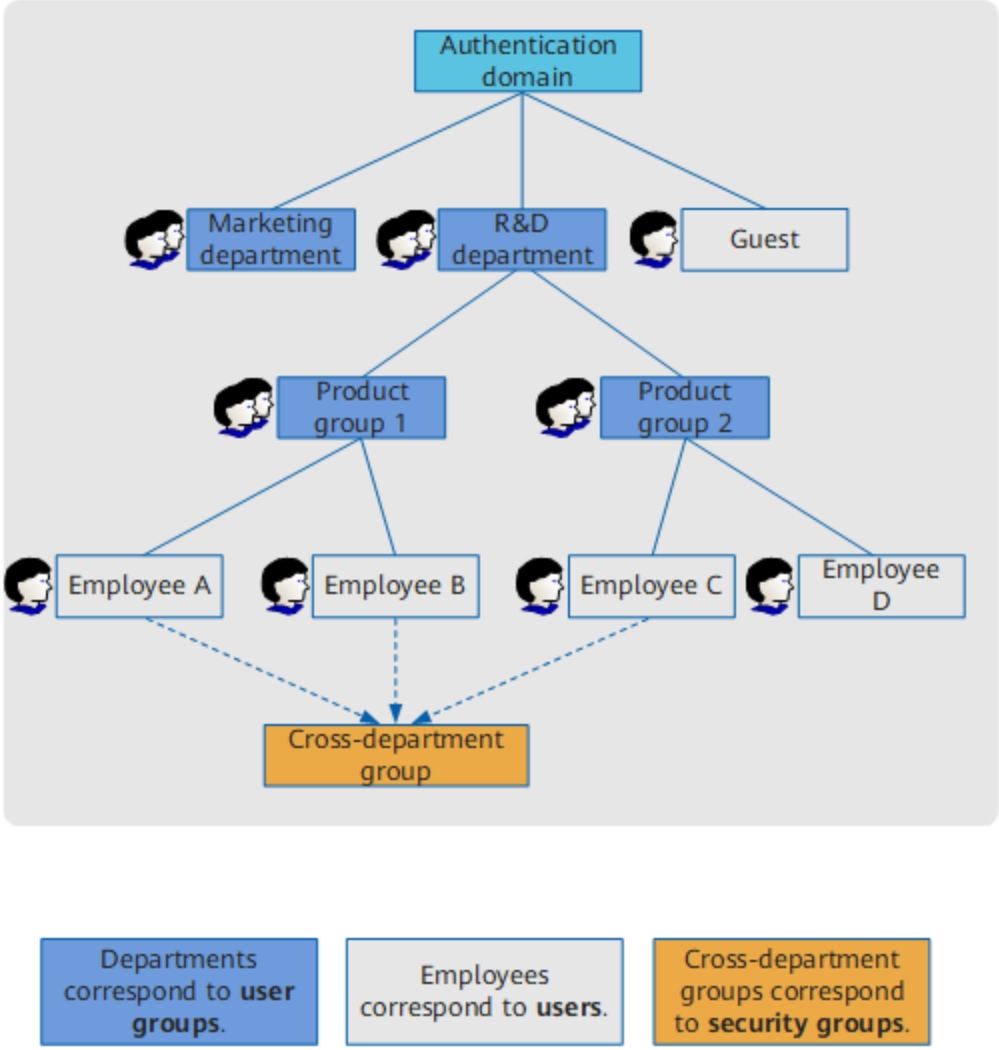
User Organizational Structure

A FW controls network behaviors and access permissions by the granularity of user.
The user organizational structure on the FW is a reflection of real organizational structures in enterprises and is the basis of user-specific permission control. As shown in Figure 1, a user organizational structure can be a tree-shaped structure that divides users by department or divides users cross departments in the horizontal dimension.

The user organizational structure involves the concepts:

- Authentication domain: The authentication domain is a container of the user organizational structure, similar to the domain in the Microsoft Active Directory (AD) server. The FW provides a default authentication domain. You can create authentication domains as required.
- User group/User: Users and the departments to which they belong are the basic units of an enterprise. The administrator can divide users into user groups based on their departments to form a tree-shaped organizational structure for the intranet. The tree-shaped organizational structure is commonly used, and allows users or user groups to be easily searched and located.
- Security group: A security group is a cross-department group in the horizontal organizational structure. You can create cross-department security groups if you need to manage users in a dimension other than by department. For example, you can create a group between multiple departments. In addition, the server provides similar horizontal groups when enterprises use third-party authentication servers to store organizational structures. To configure policies based on cross-department security groups, you need to keep the security groups created on the FW consistent with the organizational structures on the servers.

Figure 1 User organizational structure on the FW



This section describes the rules of the preceding organizational structures.

Tree-shaped Organizational Structure

The top node of the tree-shaped organizational structure is "Authentication domain", which is also considered the root group. The subordinates of an authentication domain can be user groups or users. The default authentication domain equals the /default root group.
In most cases, only the default authentication domain is used. If users have different authentication modes are used, or domain names must be consistent with those on servers, you need to plan other authentication domains.
If new authentication domains are required, the FW provides the following modes for user organizational structure planning:

- **Each authentication domain has independent user accounts.**
  Each authentication domain is an independent tree-shaped organizational structure, similar to the domain structure on an AD or LDAP authentication server. Each authentication domain has independent user accounts. Different authentication domains can have the same account.
- **All authentication domains share user accounts of the default authentication domain.**
  There is only one tree-shaped organizational structure: default authentication domain. Other authentication domains share accounts with the default authentication domain. In this mode, a new

authentication domain determines the authentication mode of its users, and the authentication domain is not the top node of the user organizational structure.

NOTE

The first mode is recommended for you to plan the user organizational structure, corresponding to the server organizational structure. The second mode applies when one user account needs to use different authentication modes or earlier version-compatible. The authentication domain configuration determines the deployment mode.

A tree-shaped organizational structure complies with the following rules:

- The default authentication domain cannot be deleted or renamed.
- A FW supports an organizational structure with a maximum of twenty layers, including the authentication domain and users. That is, the FW supports a maximum of eighteen layers between the authentication domain and users.
- A user group can contain multiple users and child user groups, but each user group can belong only to one parent group.
- Each user belongs to one group only.
- User groups can have identical names, but must each have a unique full path in the organizational structure.
- Users and user groups can be referenced by policies. If a user group is referenced by a policy, all the users in this group inherit this policy.

Security Group-based Horizontal Organizational Structure

User groups (departments) reflect the vertical organizational structure of users, whereas security groups reflect the horizontal organizational structure. You can add users from different departments to one security group for management. After you configure a policy for a security group, the policy takes effect on all users in this security group, which makes user management easier and more flexible.
You can also configure security groups in the scenarios in which the FW functions with a third-party authentication server. When AD, AD LDAP, and Sun ONE LDAP servers are deployed on a network, the AD, AD LDAP, and Sun ONE LDAP servers have other types of organizational structures except organizational units (OU). For example, the AD and AD LDAP servers have security groups, and the Sun ONE LDAP server has static and dynamic groups. To enable the FW to manage users based on the security groups on the AD and AD LDAP servers and static and dynamic groups on the Sun ONE LDAP server, use the security groups on the FW.

NOTE

The security groups on the AD servers and static and dynamic groups on the Sun ONE LDAP server are usually used to control and manage user access to resources and objects in network sharing locations, files, directories, and printers. User groups on the FW correspond to the OUs on the AD, AD LDAP, and Sun ONE LDAP servers, and the security groups on the FW correspond to the security groups on the AD and AD LDAP servers and static and dynamic groups on the Sun ONE LDAP server.

For details on the security groups or static and dynamic groups, refer to the documents of AD and AD LDAP servers or the Sun ONE LDAP server.

The FW has two types of security groups:

- Static
  In static security groups, the member users and user groups are fixed. Source of static security groups: You can manually create a static security group, import security groups from AD and AD LDAP servers, or import static security groups from the Sun ONE LDAP server.
- Dynamic
  In dynamic security groups, the member users are dynamically generated on the basis of specific filtering conditions. Source of dynamic security groups: You can manually create AD and Sun ONE LDAP dynamic security groups and import dynamic security groups from the Sun ONE LDAP server.
  In the portal authentication scenario, during user authentication, the FW looks up the authentication server based on local dynamic security group filtering conditions for each user. If a match is found, the user is authenticated as a temporary user of the security group.

Observe the following rules when you plan security groups:

- A security group can belong to no parent security group or belong to a maximum of 40 parent security groups.
- A user can belong to no parent security group or belong to a maximum of 40 parent security groups.
- The parent security group of a user can be a security group in any authentication domain, but a security group and its parent security group must belong to the same authentication domain.
- Security groups support a maximum of three layers, namely, parent security group, security group, and child security group.
- Security groups can contain other security groups. For example, security group B can contain security group A, security group C can contain security group B, and security group A can contain security group C. The organizational structure of security groups is a net structure.
- Dynamic security groups cannot be the parent groups of any security group, but can be members of static security groups.
- Security groups can be referenced by policies. If a security group is referenced by a policy, the policy applies to all users of the security group, but not to the users of the sub-security groups.

Creating Users, User Groups and Security Groups

You can create users, user groups and security groups on a FW as follows:

NOTE

As users, user groups or security groups are referenced in policies to control user permissions, the users for which server authentication is used must also have the corresponding user groups, security groups, or users on the FW, at least they should have the corresponding user groups and security groups.

- Manual creation

You can manually create users, user groups and security groups and configure user attributes. For example, you can create user groups based on the vertical organizational structure, create security groups based on the horizontal organizational structure, and then add users to each group.
This method is recommended if no third-party authentication server is deployed or user information cannot be imported to the FW from a third-party authentication server.

- Import from a CSV file
  You can write user information into a CSV file and import the CSV file to a FW. You can also import a previously exported CSV file to a FW to create users and user groups in batches.
  You can write security group information into a CSV file and import the CSV file to a FW. You can also import a previously exported CSV file to a FW to create security groups in batches.
  This method is recommended if no third-party authentication server is deployed or user information cannot be imported to the FW from a third-party authentication server. Compared with manual creation, importing a CSV file simplifies system configuration.
- Import from a server
  If an identity authentication mechanism is set up and user information is stored on a third-party authentication server, you can use an import policy to import users, user groups and security groups from the third-party authentication server to a FW.
  Currently, only AD, LDAP, and Agile Controller servers can be used to import users and user groups to a FW, and only AD and Sun ONE LDAP servers can be used to import security groups to a FW If other third-party authentication servers are deployed, manually create users, user groups and security groups, import users, user groups and security groups from a CSV file, or configure the FW to automatically discover and create users, user groups and security groups.

User Attribute

Table 1 lists major user attributes.

Table 1 User attributes

Attribute	**Description**
Login Name	User name used for authentication
Display Name	User name displayed on a FW as a user identification The user field in logs and reports is generally displayed as **Login Name (Display Name)**.
Description	User description, which helps administrators identify users and maintain user information
Parent Group	Parent group to which a user belongs Each user can belong to a maximum of three parent groups.

Attribute	Description
Parent Security Group	Parent security group to which a user belongs Each user can belong to no parent security group or belong to a maximum of 40 parent security groups.
Password	User password If local authentication is used, you must configure a password on a FW. If server authentication is used, you must configure a password on a third-party authentication server.
Expiration Date	Expiration date of an account
Allow Users to Share This Account to Log In	If you select this item, multiple users are allowed to share the same login name to log in from multiple PCs.
IP/MAC Binding	You can bind a user to an IP address or a MAC address so that the user can use only the IP address or MAC address to log in.

Online User

An online user is a user who goes online after passing the authentication and attribute check. If the user using an IP address is authenticated, the FW checks the user attributes, including the user status, account expiration date, IP/MAC binding, and account sharing setting.
The online user list on the FW records the mapping between IP addresses and online users and users can use only the mapping IP addresses. If you apply a policy to a user, the policy also takes effect with the mapping IP address.
If a user does not initiate any service traffic during the validity period (30 minutes by default) of a connection, the online user monitoring table of the user will be deleted. This user needs to be authenticated again when initiating a service request next time.

Online User Information Synchronization

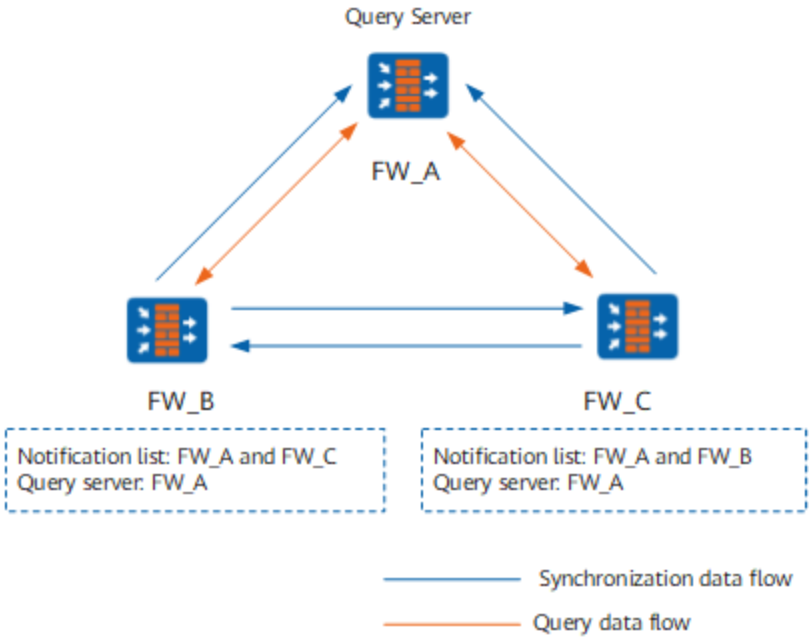
If you deploy FWs on different locations of a network and require user login information on one FW to be synchronized to other FWs for user permission control, you can use the online user information synchronization function to allow users to log in to multiple FWs at the same time.
In this deployment mode, there are two operations: synchronize and query, as shown in Figure 2. The configuration on FW_B is used as an example.

- Synchronize
  When a user logs in to or out from FW_B through built-in portal authentication and AD/Agile Controller/RADIUS SSO, FW_B sends this information to the devices in the notification list, so that the user can simultaneously log in to or out of FW_A and FW_C.

In addition, when the user initiates traffic and remaining time of the user is updated, FW_B synchronizes the update to other devices every five minutes. This prevents entries of other devices from expiring.

- Query
  If traffic passing FW_B does not match any online user entries, FW_B can initiate a query to the query server FW_A. If FW_A has the required user entry, it will send the entry to FW_B.
  Generally, a device with frequent user traffic, such as an egress firewall, is selected as the query server because entries on such a device are not easy to expire.

Figure 2 Online user information synchronization



REFERENCIAS TECNICAS

TRADUCCION SIMPLE

User Organizational

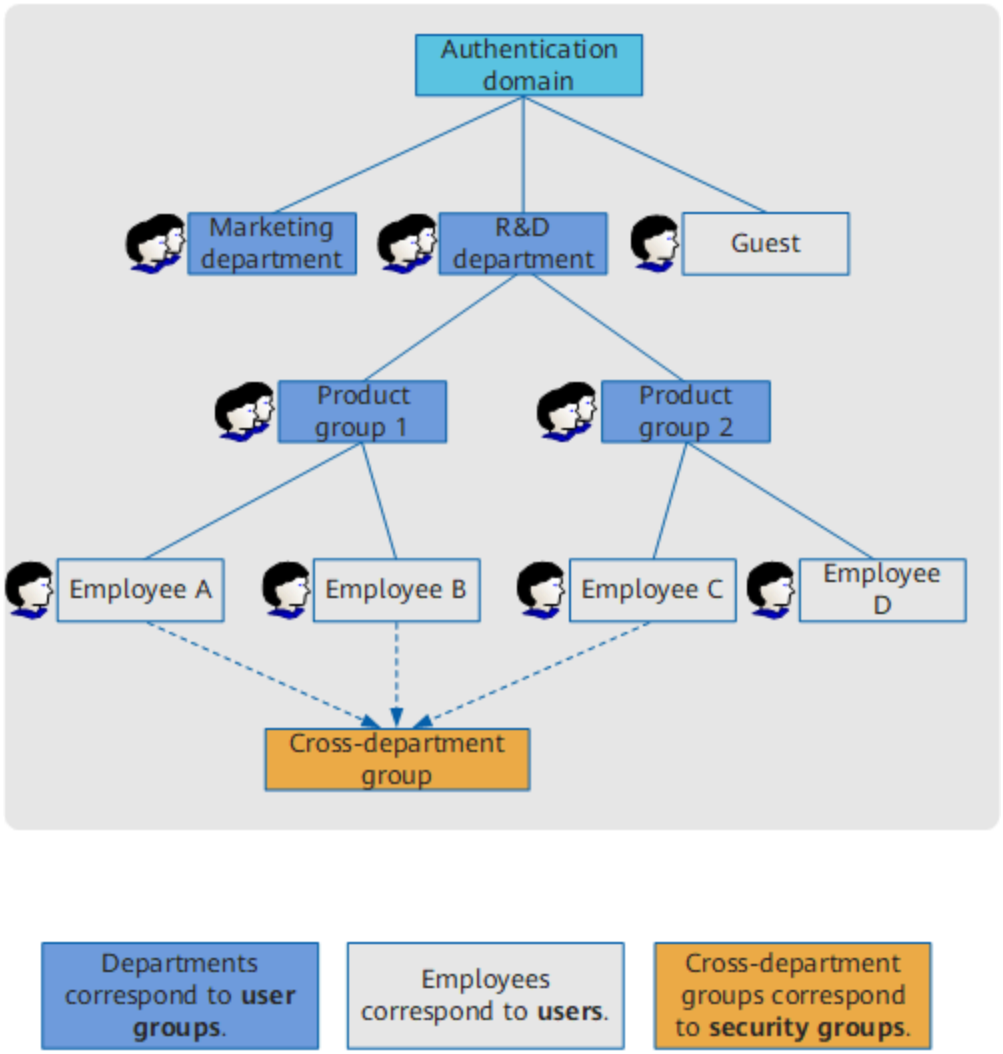
Estructura organizativa del usuario

Un FW controla los comportamientos de la red y los permisos de acceso según la granularidad del usuario. La estructura organizativa de usuarios en el FW refleja las estructuras organizativas reales de las empresas y constituye la base del control de permisos específicos para cada usuario. Como se muestra en la Figura 1 , una estructura organizativa de usuarios puede tener forma de árbol, que divide a los usuarios por departamento o entre departamentos en la dimensión horizontal.

La estructura organizativa del usuario involucra los conceptos:

- Dominio de autenticación: El dominio de autenticación es un contenedor de la estructura organizativa del usuario, similar al dominio del servidor Microsoft Active Directory (AD). El FW proporciona un dominio de autenticación predeterminado. Puede crear dominios de autenticación según sea necesario.
- Grupo de usuarios/Usuario: Los usuarios y los departamentos a los que pertenecen son las unidades básicas de una empresa. El administrador puede dividir a los usuarios en grupos según sus departamentos para formar una estructura organizativa en árbol para la intranet. Esta estructura organizativa en árbol es de uso común y permite buscar y localizar fácilmente a los usuarios o grupos de usuarios.
- Grupo de seguridad: Un grupo de seguridad es un grupo interdepartamental en la estructura organizativa horizontal. Puede crear grupos de seguridad interdepartamentales si necesita administrar usuarios en una dimensión distinta a la departamental. Por ejemplo, puede crear un grupo entre varios departamentos. Además, el servidor proporciona grupos horizontales similares cuando las empresas utilizan servidores de autenticación de terceros para almacenar estructuras organizativas. Para configurar políticas basadas en grupos de seguridad interdepartamentales, debe mantener la coherencia entre los grupos de seguridad creados en el firewall y las estructuras organizativas de los servidores.

Figura 1 Estructura organizativa del usuario en el FW



En esta sección se describen las reglas de las estructuras organizativas anteriores.

Estructura organizativa en forma de árbol

El nodo superior de la estructura organizativa en forma de árbol es el " Dominio de autenticación ", que también se considera el grupo raíz. Los subordinados de un dominio de autenticación pueden ser grupos de usuarios o usuarios. El dominio de autenticación predeterminado equivale al grupo raíz predeterminado. En la mayoría de los casos, solo se utiliza el dominio de autenticación predeterminado. Si los usuarios utilizan diferentes modos de autenticación, o si los nombres de dominio deben ser coherentes con los de los servidores, es necesario planificar otros dominios de autenticación.
Si se requieren nuevos dominios de autenticación, el FW proporciona los siguientes modos para la planificación de la estructura organizativa del usuario:

- **Cada dominio de autenticación tiene cuentas de usuario independientes.**
  Cada dominio de autenticación es una estructura organizativa independiente en forma de árbol, similar a la estructura de dominios de un servidor de autenticación AD o LDAP. Cada dominio de autenticación tiene cuentas de usuario independientes. Diferentes dominios de autenticación pueden tener la misma cuenta.
- **Todos los dominios de autenticación comparten cuentas de usuario del dominio de autenticación predeterminado.**

Solo existe una estructura organizativa en forma de árbol: el dominio de autenticación predeterminado. Otros dominios de autenticación comparten cuentas con el dominio de autenticación predeterminado. En este modo, un nuevo dominio de autenticación determina el modo de autenticación de sus usuarios, y este no es el nodo superior de la estructura organizativa de usuarios.

NOTE

Se recomienda el primer modo para planificar la estructura organizativa de usuarios, que corresponde a la estructura organizativa del servidor. El segundo modo se aplica cuando una cuenta de usuario necesita usar diferentes modos de autenticación o versiones anteriores compatibles. La configuración del dominio de autenticación determina el modo de implementación.

Una estructura organizativa en forma de árbol cumple las siguientes reglas:

- El dominio de autenticación predeterminado no se puede eliminar ni cambiar de nombre.
- Un FW admite una estructura organizativa con un máximo de veinte capas, incluyendo el dominio de autenticación y los usuarios. Es decir, el FW admite un máximo de dieciocho capas entre el dominio de autenticación y los usuarios.
- Un grupo de usuarios puede contener varios usuarios y grupos de usuarios secundarios, pero cada grupo de usuarios solo puede pertenecer a un grupo principal.
- Cada usuario pertenece a un solo grupo.
- Los grupos de usuarios pueden tener nombres idénticos, pero cada uno debe tener una ruta completa única en la estructura organizacional.
- Las políticas pueden referenciar a usuarios y grupos de usuarios. Si una política hace referencia a un grupo de usuarios, todos los usuarios de este grupo heredan dicha política.

Estructura organizativa horizontal basada en grupos de seguridad

Los grupos de usuarios (departamentos) reflejan la estructura organizativa vertical de los usuarios, mientras que los grupos de seguridad reflejan la horizontal. Puede agregar usuarios de diferentes departamentos a un grupo de seguridad para su administración. Tras configurar una política para un grupo de seguridad, esta se aplica a todos los usuarios de dicho grupo, lo que facilita y flexibiliza la administración de usuarios. También puede configurar grupos de seguridad en los escenarios en los que el firewall funciona con un servidor de autenticación de terceros. Cuando se implementan servidores AD, AD LDAP y Sun ONE LDAP en una red, estos servidores tienen otros tipos de estructuras organizativas, excepto las unidades organizativas (OU). Por ejemplo, los servidores AD y AD LDAP tienen grupos de seguridad, y el servidor Sun ONE LDAP tiene grupos estáticos y dinámicos. Para que el firewall administre usuarios según los grupos de seguridad de los servidores AD y AD LDAP, y los grupos estáticos y dinámicos del servidor Sun ONE LDAP, utilice los grupos de seguridad del firewall .

NOTE

Los grupos de seguridad de los servidores AD y los grupos estáticos y dinámicos del servidor LDAP de Sun ONE se utilizan habitualmente para controlar y gestionar el acceso de los usuarios a recursos y objetos en ubicaciones de red compartidas, archivos, directorios e impresoras. Los grupos de usuarios del servidor de seguridad corresponden a las unidades organizativas de los servidores AD,

AD LDAP y Sun ONE LDAP, y los grupos de seguridad del servidor de seguridad corresponden a los grupos de seguridad de los servidores AD y AD LDAP, y a los grupos estáticos y dinámicos del servidor LDAP de Sun ONE. Para obtener más información sobre los grupos de seguridad, ya sean estáticos o dinámicos, consulte la documentación de los servidores AD y AD LDAP o del servidor LDAP de Sun ONE.

El FW tiene dos tipos de grupos de seguridad:

- Estático
  En los grupos de seguridad estáticos, los usuarios miembros y los grupos de usuarios son fijos. Origen de los grupos de seguridad estáticos: Puede crear manualmente un grupo de seguridad estático, importar grupos de seguridad desde servidores AD y LDAP de AD, o importar grupos de seguridad estáticos desde el servidor LDAP de Sun ONE.
- Dinámica
  En los grupos de seguridad dinámicos, los usuarios miembros se generan dinámicamente según condiciones de filtrado específicas. Origen de los grupos de seguridad dinámicos: Puede crear manualmente grupos de seguridad dinámicos de AD y Sun ONE LDAP e importarlos desde el servidor LDAP de Sun ONE.
  En el escenario de autenticación del portal, durante la autenticación del usuario, el firewall busca el servidor de autenticación según las condiciones de filtrado del grupo de seguridad dinámico local para cada usuario. Si se encuentra una coincidencia, el usuario se autentica como usuario temporal del grupo de seguridad.

Tenga en cuenta las siguientes reglas al planificar grupos de seguridad:

- Un grupo de seguridad puede no pertenecer a ningún grupo de seguridad principal o pertenecer a un máximo de 40 grupos de seguridad principales.
- Un usuario puede no pertenecer a ningún grupo de seguridad principal o pertenecer a un máximo de 40 grupos de seguridad principales.
- El grupo de seguridad principal de un usuario puede ser un grupo de seguridad en cualquier dominio de autenticación, pero un grupo de seguridad y su grupo de seguridad principal deben pertenecer al mismo dominio de autenticación.
- Los grupos de seguridad admiten un máximo de tres capas, a saber: grupo de seguridad principal, grupo de seguridad y grupo de seguridad secundario.
- Los grupos de seguridad pueden contener otros grupos de seguridad. Por ejemplo, el grupo de seguridad B puede contener al grupo de seguridad A, el grupo de seguridad C puede contener al grupo de seguridad B, y el grupo de seguridad A puede contener al grupo de seguridad C. La estructura organizativa de los grupos de seguridad es una estructura de red.
- Los grupos de seguridad dinámicos no pueden ser grupos principales de ningún grupo de seguridad, pero pueden ser miembros de grupos de seguridad estáticos.
- Las políticas pueden hacer referencia a los grupos de seguridad. Si una política hace referencia a un grupo de seguridad, esta se aplica a todos los usuarios del grupo, pero no a los usuarios de los subgrupos de seguridad.

Creación de usuarios, grupos de usuarios y grupos de seguridad

Puede crear usuarios, grupos de usuarios y grupos de seguridad en un FW de la siguiente manera:

NOTE

Como los usuarios, grupos de usuarios o grupos de seguridad se referencian en las políticas para controlar los permisos de los usuarios, los usuarios para los cuales se utiliza la autenticación del servidor también deben tener los grupos de usuarios, grupos de seguridad o usuarios correspondientes en el FW , al menos deben tener los grupos de usuarios y grupos de seguridad correspondientes.

- Creación manual
  Puede crear manualmente usuarios, grupos de usuarios y grupos de seguridad, y configurar sus atributos. Por ejemplo, puede crear grupos de usuarios según la estructura organizativa vertical, grupos de seguridad según la estructura organizativa horizontal y, a continuación, agregar usuarios a cada grupo.
  Este método se recomienda si no se implementa ningún servidor de autenticación de terceros o si no se puede importar información del usuario al FW desde un servidor de autenticación de terceros.
- Importar desde un archivo CSV
  Puede escribir la información del usuario en un archivo CSV e importarlo a un servidor de seguridad . También puede importar un archivo CSV previamente exportado a un servidor de seguridad para crear usuarios y grupos de usuarios por lotes.
  Puede escribir la información del grupo de seguridad en un archivo CSV e importarlo a un servidor de seguridad . También puede importar un archivo CSV previamente exportado a un servidor de seguridad para crear grupos de seguridad por lotes.
  Este método se recomienda si no se implementa un servidor de autenticación de terceros o si no se puede importar la información del usuario al firewall desde un servidor de autenticación de terceros. En comparación con la creación manual, importar un archivo CSV simplifica la configuración del sistema.
- Importar desde un servidor
  Si se configura un mecanismo de autenticación de identidad y la información del usuario se almacena en un servidor de autenticación de terceros, puede usar una política de importación para importar usuarios, grupos de usuarios y grupos de seguridad desde el servidor de autenticación de terceros a un FW .
  Actualmente, solo se pueden usar servidores AD, LDAP y Agile Controller para importar usuarios y grupos de usuarios a un FW , y solo se pueden usar servidores AD y Sun ONE LDAP para importar grupos de seguridad a un FW. Si se implementan otros servidores de autenticación de terceros, cree manualmente usuarios, grupos de usuarios y grupos de seguridad, importe usuarios, grupos de usuarios y grupos de seguridad desde un archivo CSV, o configure el FW para que descubra y cree automáticamente usuarios, grupos de usuarios y grupos de seguridad.

Atributo de usuario

En la Tabla 1 se enumeran los principales atributos del usuario.

Tabla 1 Atributos del usuario

Atributo	Descripción
Nombre de inicio de sesión	Nombre de usuario utilizado para la autenticación

Atributo	Descripción
Nombre para mostrar	Nombre de usuario que se muestra en un FW como identificación de usuario El campo de usuario en los registros e informes generalmente se muestra como **Nombre de inicio de sesión (Nombre para mostrar)** .
Descripción	Descripción del usuario, que ayuda a los administradores a identificar a los usuarios y mantener la información del usuario.
Grupo de padres	Grupo principal al que pertenece un usuario Cada usuario puede pertenecer a un máximo de tres grupos de padres.
Grupo de seguridad para padres	Grupo de seguridad principal al que pertenece un usuario Cada usuario puede no pertenecer a ningún grupo de seguridad principal o pertenecer a un máximo de 40 grupos de seguridad principales.
Contraseña	Contraseña de usuario Si se utiliza autenticación local, se debe configurar una contraseña en un firewall . Si se utiliza autenticación de servidor, se debe configurar una contraseña en un servidor de autenticación externo.
Fecha de expiración	Fecha de vencimiento de una cuenta
Permitir que los usuarios compartan esta cuenta para iniciar sesión	Si selecciona este elemento, varios usuarios podrán compartir el mismo nombre de inicio de sesión para iniciar sesión desde varias PC.
Vinculación IP/MAC	Puede vincular a un usuario a una dirección IP o una dirección MAC para que el usuario pueda usar únicamente la dirección IP o la dirección MAC para iniciar sesión.

Usuario en línea

Un usuario en línea es aquel que se conecta tras pasar la autenticación y la verificación de atributos. Si el usuario que usa una dirección IP está autenticado, el firewall verifica sus atributos, incluyendo su estado, la fecha de vencimiento de la cuenta, la vinculación de IP/MAC y la configuración de uso compartido de la cuenta.

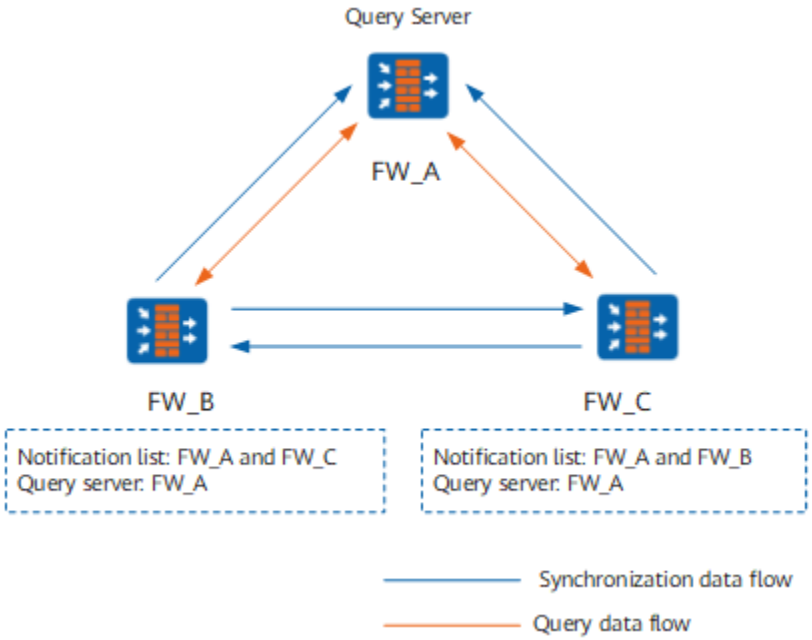
La lista de usuarios en línea del firewall registra la asignación entre direcciones IP y usuarios en línea, y estos solo pueden usar las direcciones IP asignadas. Si se aplica una política a un usuario, esta también se aplica a la dirección IP asignada.
Si un usuario no inicia tráfico de servicio durante el periodo de validez de una conexión (30 minutos por defecto), se eliminará su tabla de monitorización en línea. Este usuario deberá autenticarse de nuevo la próxima vez que inicie una solicitud de servicio.

Sincronización de información de usuario en línea

Si implementa FW en diferentes ubicaciones de una red y requiere que la información de inicio de sesión del usuario en un FW se sincronice con otros FW para controlar los permisos de los usuarios, puede usar la función de sincronización de información de usuario en línea para permitir que los usuarios inicien sesión en varios FW al mismo tiempo.
En este modo de implementación, hay dos operaciones: sincronizar y consultar, como se muestra en la Figura 2. La configuración en FW _B se utiliza como ejemplo.

- Sincronizar
  Cuando un usuario inicia o cierra sesión en FW _B a través de la autenticación del portal integrado y AD/Agile Controller/RADIUS SSO, FW _B envía esta información a los dispositivos en la lista de notificaciones, para que el usuario pueda iniciar o cerrar sesión simultáneamente en FW _A y FW _C. Además, cuando el usuario inicia el tráfico y se actualiza su tiempo restante, FW_B sincroniza la actualización con otros dispositivos cada cinco minutos. Esto evita que caduquen las entradas de otros dispositivos.
- Consulta
  Si el tráfico que pasa por FW_B no coincide con ninguna entrada de usuario en línea, FW_B puede iniciar una consulta al servidor de consultas FW_A . Si FW_A tiene la entrada de usuario requerida, la enviará a FW_B .
  Generalmente, se selecciona un dispositivo con tráfico de usuarios frecuente, como un firewall de salida, como servidor de consulta porque las entradas en dicho dispositivo no son fáciles de caducar.

Figura 2 Sincronización de información de usuario en línea



REFERENCIAS TECNICAS

INGLES

Virtual Private Network

Virtual Private Network

User Guide

Issue 01

Date 2025-04-30



HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Copyright © Huawei Technologies Co., Ltd. 2025. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process.* For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Overview 1
1.1 What Is VPN? 1
1.2 Product Advantages 1
1.3 Application Scenarios 2
1.4 Product Specifications 3
1.5 Quotas and Constraints 4
1.6 Reference Standards and Protocols 6
1.7 Differences between Enterprise Edition VPN and Classic VPN 7
1.8 Billing (Enterprise Edition VPN) 7
1.9 Billing (Classic VPN) 9
1.10 Security 9
1.10.1 Data Protection Technologies 9
1.11 Permissions Management 12
1.12 Basic Concepts 15
1.12.1 IPsec VPN 15
1.12.2 VPN Gateway Bandwidth 16
1.12.3 Local Subnet 16
1.12.4 Customer Subnet 16
2 Getting Started 18
2.1 Configuring Enterprise Edition VPN to Connect an On-premises Data Center to a VPC 18
2.1.1 Overview 18
2.1.2 Step 1: Creating a VPN Gateway 21
2.1.3 Step 2: Creating a Customer Gateway 23
2.1.4 Step 3: Creating VPN Connection 1 23
2.1.5 Step 4: Creating VPN Connection 2 25
2.1.6 Step 5: Configuring the Customer Gateway Device 28
2.1.7 Step 6: Verifying Network Connectivity 30
2.2 VPN Creation Process 31
2.2.1 Buying a VPN Gateway 31
2.2.2 Buying a VPN Connection 32
3 Management 38
3.1 Enterprise Edition S2C VPN 38

 Copyright © Huawei Technologies Co., Ltd.

3.1.1 Enterprise Edition VPN Gateway Management 38
3.1.2 Customer Gateway Management of Enterprise Edition VPN 49
3.1.3 Enterprise Edition VPN Connection Management 53
3.2 Classic VPN 71
3.2.1 Classic VPN Gateway Management 71
3.2.2 Classic VPN Connection Management 72
3.3 Monitoring 74
3.3.1 Metrics (S2C Enterprise Edition VPN) 74
3.3.2 Viewing Metrics 77
3.3.3 Creating Alarm Rules 78
3.4 Audit 79
3.4.1 VPN Operations That Can Be Recorded by CTS 79
3.5 Permissions Management 80
3.5.1 Creating a User and Granting VPN Permissions 80
3.5.2 VPN Custom Policies 81
3.6 Quotas 82

4 Best Practice 84

4.1 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active-Active Mode) 84
4.1.1 Overview 84
4.1.2 Planning Networks and Resources 85
4.1.3 Procedure 86
4.2 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active/Standby Mode) 90
4.2.1 Overview 90
4.2.2 Planning Networks and Resources 91
4.2.3 Procedure 93
4.3 Connecting Multiple On-premises Branch Networks Through a VPN Hub 97
4.3.1 Overview 97
4.3.2 Planning Networks and Resources 98
4.3.3 Procedure 100
4.4 Classic VPN 106
4.4.1 Connecting an On-Premises Data Center to a VPC Through a VPN 106

5 Troubleshooting 108

5.1 The State of a VPN Connection Is **Not connected** 108
5.2 Ping Tests Between Cloud and On-premises Networks Fail 110
5.3 Packet Loss Occurs 111
5.4 Classic VPN 112
5.4.1 Common Check Items 112
5.4.2 Common Configuration Issues and Solutions 113

6 FAQs 115

6.1 Enterprise Edition VPN 115

 Copyright © Huawei Technologies Co., Ltd.

6.1.1 What Are VPN Negotiation Parameters? What Are Their Default Values?....115
6.1.2 Are a Username and Password Required for Creating an IPsec VPN Connection?....118
6.1.3 Is an IPsec VPN Connection Automatically Established?....118
6.1.4 What VPN Resources Can Be Monitored?....118
6.1.5 What Do I Do If a VPN Connection Fails to Be Established?....119
6.1.6 Can EIPs Be Used as VPN Gateway IP Addresses?....119
6.1.7 What Are the Typical Scenarios of IPsec VPN?....119
6.1.8 What Are a VPC, a VPN Gateway, and a VPN Connection?....120
6.1.9 How Do I Plan CIDR Blocks for Access to a VPC Through a VPN Connection?....120
6.1.10 Which IKE Version Should I Select When I Create a VPN Connection?....120
6.1.11 Does a VPN Allow for Communications Between Two VPCs?....122
6.2 Classic VPN....122
6.2.1 Will I Be Notified If a VPN Connection Is Interrupted?....123
6.2.2 What Are the Differences Between the Application Scenarios and Connection Modes of IPsec and SSL VPNs?....123
6.2.3 How Many VPN Connections Do I Need to Connect to Multiple On-premises Servers?....123
6.2.4 What Are the Impacts of a VPN on an On-premises Network? What Are the Changes to the Route for Accessing an ECS?....124
6.2.5 Why Is Not Connected Displayed as the Status for a Successfully Created VPN Connection?....124
6.2.6 Where Can I Add Routes on the VPN Console to Reach the Remote Subnets?....124
6.2.7 How Do I Replace a Direct Connect Connection with a VPN?....125
6.2.8 How Do I Access ECSs at Home When My Enterprise Network Has Been Connected to the Cloud Through a VPN?....125
6.2.9 How Do I Configure DPD for Interconnection with the Cloud?....125
6.2.10 What Is the VPN Quota?....126
A Change History....127

 Copyright © Huawei Technologies Co., Ltd.

1 Overview

1.1 What Is VPN?

Overview

Virtual Private Network (VPN) establishes secure, reliable, and cost-effective encrypted connections between your on-premises network or data center and a virtual network on the cloud.

NOTE

VPN supports only non-cross-border connections.

- A VPN gateway provides an Internet egress for a Virtual Private Cloud (VPC) to connect to a customer gateway in your on-premises data center.
- A VPN connection connects a VPN gateway to a customer gateway through encrypted tunnels, enabling communication between a VPC and your on-premises data center. This helps quickly establish a secure hybrid cloud environment.

Components

- **VPN gateway**: a virtual gateway of VPN on the cloud. It establishes secure private connections with a customer gateway in your on-premises network or data center.
- **Customer gateway**: a resource that provides information to the cloud about your customer gateway device. It can be a physical device or software application in your on-premises data center.
- **VPN connection**: a secure channel between a VPN gateway and a customer gateway. VPN connections use the Internet Key Exchange (IKE) and IPsec protocols to encrypt the transmitted data.

1.2 Product Advantages

VPN has the following advantages:

 Copyright © Huawei Technologies Co., Ltd.

- **High security**
  - Data is encrypted using IKE/IPsec, ensuring high data security.
  - A VPN gateway is exclusive to a tenant, isolating tenants from each other.
- **High availability**
  - A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.
  - Active-active gateways are deployed in different availability zones (AZs) to ensure AZ-level high availability.
  - Active/Standby mode: In normal cases, a VPN gateway communicates with a customer gateway through the active connection. If the active connection fails, traffic is automatically switched to the standby VPN connection. After the fault is rectified, traffic is switched back to the active VPN connection.
- **Cost-effectiveness**
  - IPsec connections over the Internet provide a cost-effective alternative to Direct Connect.
  - A VPN gateway can be bound to elastic IP addresses (EIPs) that share bandwidth, reducing bandwidth costs.
  - The bandwidth can be adjusted when an EIP instance is created.
- **Easy to use**
  - A VPN gateway supports multiple connection modes, including policy-based, static routing, and BGP routing, to meet different access requirements of customer gateways.
  - A VPN gateway on the cloud can function as a VPN hub, enabling on-premises branch sites to access each other.
  - A VPN connection can be created in a few simple steps on the VPN device in an on-premises data center and on the VPN console, and is ready to use immediately after being created.
  - Private VPN gateways are supported to encrypt traffic transmitted over Direct Connect connections, improving data transmission security.

1.3 Application Scenarios

Hybrid Cloud Deployment

You can use a VPN to connect your on-premises data center to a VPC and use the elastic and fast scaling capabilities of the cloud to expand application computing capabilities. shows the hybrid cloud deployment.

Inter-region Connection Between VPCs

With VPNs, you can connect VPCs in different regions to enable connectivity between user services in these regions, as shown in .

Copyright © Huawei Technologies Co., Ltd.

622

Enterprise Branch Interconnection

A VPN gateway functions as a VPN hub to connect enterprise branches, as shown in . This eliminates the need to configure VPN connections between every two branches.

1.4 Product Specifications

NOTE

- The specification of a VPN gateway can be changed between Professional 1 and Professional 2.

Table 1-1 VPN specifications

Item	Professional 1	Professional 2
Exclusive gateway resources	Supported	Supported
Dual connections	Supported	Supported
Active-active gateways	Supported	Supported
Active/Standby gateways	Supported	Supported
Policy-based mode	Supported	Supported
Routing mode: static routing	Supported	Supported
Routing mode: BGP routing	Supported	Supported
Policy template mode	Not supported	Not supported
Maximum forwarding bandwidth	300 Mbit/s	1 Gbit/s
Maximum number of VPN connection groups	100	100
Private network	Supported	Supported
Supported regions	Subject to the regions available on the console	Subject to the regions available on the console

Copyright © Huawei Technologies Co., Ltd.

623

1.5 Quotas and Constraints

VPN Gateway

Table 1-2 Constraints on VPN gateways

VPN Type	Resource	Default Quota
Enterprise Edition VPN	VPN gateways per tenant in each region	50 • If you have only one VPC, you can create a maximum of 50 VPN gateways for the VPC. • If you have multiple VPCs, you can create a maximum of 50 VPN gateways for all these VPCs.
	VPN connection groups per VPN gateway	100
	Local subnets per VPN gateway	50
	Number of BGP routes that a VPN gateway can receive from a customer gateway through a connection	100
Classic VPN	VPN gateways per tenant in each region	2 Only one VPN gateway can be created for a VPC.

- By default, the maximum length of TCP packets supported by a VPN gateway is 1300 bytes.

Customer Gateway

Table 1-3 Constraints on customer gateways

VPN Type	Resource	Default Quota
Enterprise Edition VPN	Customer gateways per tenant in each region	100

- Enable NAT traversal on the customer gateway based on the networking.
  - If the customer gateway is connected to the Internet through a NAT device, enable NAT traversal on the customer gateway.

Copyright © Huawei Technologies Co., Ltd.

  - If the customer gateway is directly connected to the Internet, you do not need to enabled NAT traversal on the customer gateway.
- Dead Peer Detection (DPD) must be enabled on a customer gateway.
- A customer gateway must support IPsec tunnel interfaces and be configured with a corresponding security policy.
- When Network Quality Analysis (NQA) is enabled for a connection in static routing mode, the IPsec tunnel interface of a customer gateway must have an IP address and be able to respond to ICMP requests.
- It is recommended that the maximum segment size (MSS) of TCP packets be set to a value less than 1399 on a customer gateway, so as to prevent fragmentation caused by addition of an IPsec header.

VPN Connection

Table 1-4 Constraints on VPN connections

VPN Type	Resource	Default Quota	How to Increase Quota
Enterprise Edition VPN	Policy rules per VPN connection	5	The quotas cannot be increased.
	Customer subnets per VPN connection	50	
Classic VPN	VPN connections per tenant in each region	12	This quota cannot be increased.

- In multi-subnet scenarios, you are advised to use VPN connections in routing mode. For a VPN connection in policy-based or policy template mode, a VPN gateway creates a communications tunnel for each pair of the local and customer subnets by default. If there are multiple local or customer subnets for a VPN connection in policy-based or policy template mode, multiple communications tunnels are created.

  Each IP address of a VPN gateway supports a maximum of 100 communications tunnels for connecting to customer gateways.

  - In routing mode, each VPN connection occupies only one communications tunnel of the corresponding VPN gateway IP address.
  - In policy-based or policy template mode, each VPN connection occupies *M* x *N* communications tunnels of the corresponding VPN gateway IP address. *M* indicates the number of local subnets, and *N* indicates the number of customer subnets.

  If the number of communications tunnels occupied by all VPN connections in different modes established by a single gateway IP address has reached 100, excess VPN connections will fail to be created.
- When creating a VPN connection in policy-based mode and adding multiple policy rules, ensure that the source and destination CIDR blocks in different policy rules do not overlap. Otherwise, data flows may be incorrectly matched or IPsec tunnels may flap.

Copyright © Huawei Technologies Co., Ltd.

1.6 Reference Standards and Protocols

The following standards and protocols are associated with VPN:

- RFC 2403: The Use of HMAC-MD5-96 within ESP and AH
- RFC 2404: The Use of HMAC-SHA-1-96 within ESP and AH
- RFC 2409: The Internet Key Exchange (IKE)
- RFC 2451: The ESP CBC-Mode Cipher Algorithms
- RFC 3526: More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE)
- RFC 3566: The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec
- RFC 3602: The AES-CBC Cipher Algorithm and Its Use with IPsec
- RFC 3664: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4106: The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP)
- RFC 4109: Algorithms for Internet Key Exchange version 1 (IKEv1)
- RFC 4434: The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)
- RFC 4868: Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec
- RFC 4301: Security Architecture for the Internet Protocol
- RFC 4302: IP Authentication Header
- RFC 4303: IP Encapsulating Security Payload (ESP)
- RFC 4305: Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 4306: Internet Key Exchange (IKEv2)Protocol
- RFC 4307: Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)
- RFC 4308: Cryptographic Suites for IPsec
- RFC 5282: Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol
- RFC 6989: Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7296: Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 7321: Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)
- RFC 8247: Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)
- RFC 3947: Negotiation of NAT-Traversal in the IKE
- RFC 3948: UDP Encapsulation of IPsec ESP Packets
- RFC 3706: A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers

Copyright © Huawei Technologies Co., Ltd.

626

- RFC 4271: A Border Gateway Protocol 4 (BGP-4)

1.7 Differences between Enterprise Edition VPN and Classic VPN

Table 1-5 Differences between Enterprise Edition VPN and Classic VPN

Category	Item	Enterprise Edition VPN	Classic VPN
Tenant isolation	Tenant-exclusive gateway	Supported	Not supported
Features	Policy-based mode	Supported	Supported
	Routing mode	Static routing and BGP routing	Not supported
	VPN hub	Supported	Not supported
	Enterprise router	Not supported	Not supported
	Network type	Public network and private network	Public network
Capacity	Number of subnets	• Route-based mode: 50 • Policy-based mode: 5	Policy-based mode: 5
	For more information, see **Table 1-1**.		
Reliability	Gateway protection mode	Active/Standby or active-active	-
	Inter-AZ gateway deployment	Supported	Not supported
	Active-active VPN connections	Supported	Not supported
	Backup with Direct Connect	Supported	Not supported

1.8 Billing (Enterprise Edition VPN)

NOTE

Unless otherwise specified, VPN mentioned in this section refers to Enterprise Edition VPN.

 Copyright © Huawei Technologies Co., Ltd.

Billing Items

Table 1-6 VPN billing items

Billing Mode	Billing Item 1	Billing Item 2	Billing Formula
Pay-per-use	VPN instance (billed by hour)	EIP bandwidth	VPN instance fee + EIP bandwidth fee
Pay-per-use	VPN instance (billed by hour)	EIP traffic	VPN instance fee + EIP traffic fee

The total price of VPN consists of the following parts:

- **VPN instance fee**: indicates the fee charged for the use of a single VPN gateway and the connection between the VPN gateway and a customer gateway. A VPN gateway is dedicated to a tenant, ensuring its forwarding performance.
- **EIP bandwidth fee**: indicates the fee charged for the bandwidth consumed by the EIPs bound to a VPN gateway.
  - By default, an active-active VPN gateway has two EIPs. You need to purchase bandwidth for each EIP.
  - If you use existing EIPs as the EIPs of a VPN gateway, you will not be charged again for these EIPs.

    For details, see EIP Pricing Details.

Billing Modes

Pay-per-use

VPN instances are billed by usage duration, and the billing cycle is 1 hour. EIP bandwidth can be billed by bandwidth or traffic.

- **Billed by bandwidth**
  - **Billing formula**: Total price = VPN instance fee + EIP bandwidth fee

    EIP bandwidth refers to outbound bandwidth, that is, bandwidth for traffic sent from a VPC on the cloud to a customer gateway in an on-premises data center.

    i. If the purchased bandwidth is 10 Mbit/s or less, the inbound bandwidth is limited to 10 Mbit/s.

    ii. If the purchased bandwidth is greater than 10 Mbit/s, the inbound bandwidth is the same as the purchased bandwidth.

    For example, assuming that the bandwidth you purchased is 50 Mbit/s and you use the VPN gateway for 5 hours and then delete it, you will be charged for the use of 50 Mbit/s bandwidth for 5 hours even if you do not transmit any data during the 5 hours.
- **Billed by traffic**

  If you select billing by traffic, you will be charged for the traffic generated in every hour, with the billing unit being 1 GB. If less than 1 GB is generated, the

 Copyright © Huawei Technologies Co., Ltd.

fee is calculated based on the actually generated traffic volume. In this case, modifying the bandwidth size does not change the public network traffic price per GB. Only traffic in the outbound direction is billed.

- **Billing formula**: Total price = VPN instance fee + EIP traffic fee

1.9 Billing (Classic VPN)

Classic VPN supports the pay-per-use (hourly) billing mode. You pay only for what you use, for as long as you need it. No complex forecasts and budgets are required. You can buy one or more VPN connections, and will be billed based on the number of created VPN connections and usage duration.

NOTE

Unless otherwise specified, VPN in this section refers to Classic VPN.

Billing Items

Table 1-7 Billing items of Classic VPNs

Billing Mode	Billing Item 1	Billing Item 2	Billing Formula
Pay-per-use	Public network traffic	VPN connection	Total price = Public network traffic fee + VPN connection fee

Billing Modes

Pay-per-use

- **Billed by traffic**

  If you select billing by traffic, you will be charged for the traffic generated in every hour, with the billing unit being 1 GB. If less than 1 GB is generated, the fee is calculated based on the actually generated traffic volume.

  Total price = Public network traffic fee + VPN connection fee

1.10 Security

1.10.1 Data Protection Technologies

- S2C VPN is a tunneling technology that provides IP-layer security using the IKE/IPsec protocol suite. It ensures confidentiality and integrity of IP data packets and prevents them from being intercepted, disclosed, or tampered with on insecure networks (such as the Internet).
- When creating an S2C VPN connection, you can configure data encryption and authentication algorithms in a policy.

Copyright © Huawei Technologies Co., Ltd.

629

Table 1-8 lists the algorithms recommended for S2C VPN in descending order of security.

Table 1-8 Parameters for configuring S2C VPN policies

Parameter		Description
IKE Policy	Version	• v2 • v1 (IKEv1 has low security. If the device supports IKEv2, IKEv2 is recommended.) The default value is **v2**.
	Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA2-512 • SHA2-384 • SHA2-256 • MD5(Insecure. Not recommended.) • SHA1(Insecure. Not recommended.) By default, the SHA2-256 algorithm is used.
	Encryption Algorithm	The following encryption algorithms are supported: • AES-256-GCM-16 (supported only by Enterprise Edition VPN) • AES-128-GCM-16 (supported only by Enterprise Edition VPN) • AES-256(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • 3DES(Insecure. Not recommended.) By default, the AES-128 algorithm is used.

Copyright © Huawei Technologies Co., Ltd.

630

Parameter		Description
	DH Algorithm	The following algorithms are supported: • Group 21 • Group 20 • Group 19 • Group 16 • Group 15 • Group 14(Insecure. Not recommended.) • Group 5(Insecure. Not recommended.) • Group 2(Insecure. Not recommended.) • Group 1(Insecure. Not recommended.) By default, Group 15 is used.
IPsec Policy	Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA2-512 • SHA2-384 • SHA2-256 • MD5(Insecure. Not recommended.) • SHA1(Insecure. Not recommended.) By default, the SHA2-256 algorithm is used.
	Encryption Algorithm	The following encryption algorithms are supported: • AES-256-GCM-16 • AES-128-GCM-16 • AES-256(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • 3DES(Insecure. Not recommended.) By default, the AES-128 algorithm is used.

 Copyright © Huawei Technologies Co., Ltd.

PFS

Perfect Forward Secrecy (PFS) ensures that the compromise of the keys of an IPsec tunnel does not affect the security of other tunnels by leveraging that the keys of these tunnels are irrelevant to each other. By default, the PFS function is enabled for S2C VPN.

Each IPsec VPN connection consists of at least one IPsec tunnel, each of which uses an independent set of keys to protect user traffic.

S2C VPN supports the following algorithms:

- DH group 1 (This algorithm is insecure. Exercise caution when using it.)
- DH group 2 (This algorithm is insecure. Exercise caution when using it.)
- DH group 5 (This algorithm is insecure. Exercise caution when using it.)
- DH group 14
- DH group 15
- DH group 16
- DH group 19
- DH group 20
- DH group 21

Anti-replay

Anti-replay uses sequence numbers to protect IPsec encrypted packets against replay attacks, which are initiated by repeatedly sending intercepted data packets. By default, the anti-replay function is enabled for the VPN service.

Resource Isolation

A VPN gateway is exclusive to a tenant. As such, tenants are isolated from each, ensuring tenant data security.

1.11 Permissions Management

If you need to assign different permissions to personnel in your enterprise to access your VPN resources on the cloud service platform, Identity and Access Management (IAM) is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your resources.

With IAM, you can use your account to create IAM users, and assign permissions to the users to control their access to specific cloud resources. For example, some software developers in your enterprise need to use VPN resources but should not be allowed to delete them or perform any high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using VPN resources.

If your account does not need individual IAM users for permissions management, skip this section, which has no impact on using functions of VPN.

IAM is a free service. You only pay for the resources in your account.

Copyright © Huawei Technologies Co., Ltd.

632

For more information about IAM, see **IAM Service Overview**.

VPN Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

VPN is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for VPN in the selected projects. If you set **Scope** to **All resources**, users have permissions for VPN in all region-specific projects. When accessing VPN, the users need to switch to the authorized region.

You can grant permissions by using roles or policies.

- Roles: A type of coarse-grained authorization mechanism that defines permissions related to user responsibilities. There are only a limited number of roles for granting permissions to users. Some roles depend other roles to take effect. When you assign such roles to users, remember to assign the roles they depend on. However, roles are not an ideal choice for fine-grained authorization and secure access control.
- Policies: a type of fine-grained authorization mechanism that defines permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible policy-based authorization, meeting requirements for secure access control. For example, administrators can grant IAM users only permissions to manage VPN resources of a certain type.

Table 1-9 lists all system-defined permissions for VPN.

Table 1-9 System-defined permissions for VPN

System Role/ Policy Name	Description	Dependency
VPN Administrator (not recommended)	Administrator permissions for VPN. Users with these permissions can perform all operations on VPN. Users with these permissions have the **VPC Administrator** and **Tenant Guest** permissions by default. • **VPC Administrator**: project-level policy, which is selected in the same project as **VPN Administrator**. • **Tenant Guest**: project-level policy, which is selected in the same project as **VPN Administrator**.	-

Copyright © Huawei Technologies Co., Ltd.

633

Table 1-10 lists the common operations supported by system-defined permissions for S2C VPN.

Table 1-10 Common operations supported by system-defined permissions for S2C VPN

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
Creating a VPN gateway	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×
Viewing a VPN gateway	√	√	√
Querying the VPN gateway list	√	√	√
Updating a VPN gateway	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×
Deleting a VPN gateway	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×
Creating a VPN connection	√	• Enterprise Edition VPN: √ • Classic VPN: √	×
Viewing a VPN connection	√	√	√
Querying the VPN connection list	√	√	√
Updating a VPN connection	√	• Enterprise Edition VPN: √ • Classic VPN: √	×
Deleting a VPN connection	√	• Enterprise Edition VPN: × • Classic VPN: √	×
Creating a customer gateway	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	×
Viewing a customer gateway	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	√

Copyright © Huawei Technologies Co., Ltd.

Operation	VPN Administrator (Not Recommended)	VPN FullAccess (Recommended)	VPN ReadOnlyAccess
Querying the customer gateway list	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	√
Updating a customer gateway	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	×
Deleting a customer gateway	√	• Enterprise Edition VPN: √ • Classic VPN: N/A	×
Creating a VPN connection monitor	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×
Querying a VPN connection monitor	√	• Enterprise Edition VPN: √ • Classic VPN: ×	√
Querying the VPN connection monitor list	√	• Enterprise Edition VPN: √ • Classic VPN: ×	√
Deleting a VPN connection monitor	√	• Enterprise Edition VPN: √ • Classic VPN: ×	×

Helpful Links

- IAM Service Overview

1.12 Basic Concepts

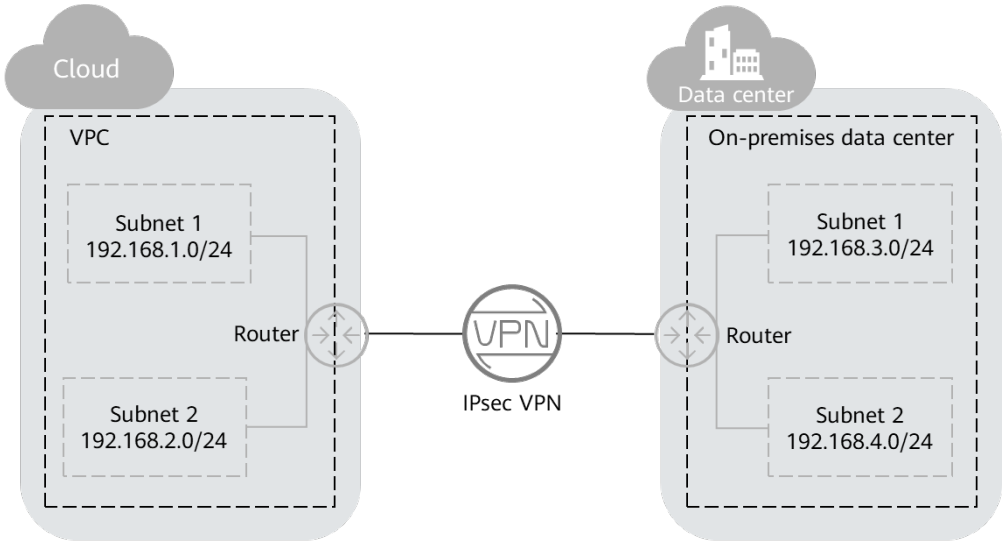
1.12.1 IPsec VPN

Internet Protocol Security (IPsec) VPN uses a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between different networks.

In the example shown in **Figure 1-1**, assume that you have created a VPC with two subnets (192.168.1.0/24 and 192.168.2.0/24) on the cloud, and the router in your on-premises data center also has two subnets (192.168.3.0/24 and 192.168.4.0/24). In this case, you can create a VPN to connect the VPC subnets and the data center subnets.

Copyright © Huawei Technologies Co., Ltd.

Figure 1-1 IPsec VPN



Site-to-site VPN is supported to enable communication between VPC subnets and on-premises data center subnets.

1.12.2 VPN Gateway Bandwidth

The bandwidth you purchased for a VPN gateway refers to outbound bandwidth, that is, bandwidth for traffic sent from a VPC on the cloud to a customer gateway in an on-premises data center.

- If the purchased bandwidth is 10 Mbit/s or less, the inbound bandwidth is limited to 10 Mbit/s.
- If the purchased bandwidth is greater than 10 Mbit/s, the inbound bandwidth is the same as the EIP bandwidth.

1.12.3 Local Subnet

Local subnets are VPC subnets that need to communicate with an on-premises network through VPN. When you buy a VPN gateway, you can set **Local Subnet** to either of the following options:

- **Select subnet**: Select subnets from the drop-down list. This is recommended if all subnets that require VPN communication are in the VPC.
- **Enter CIDR block**: Enter a subnet using CIDR notation (example: 192.168.0.0/16). If multiple subnets are specified, separate them by a comma (,). This is recommended if the CIDR blocks requiring VPN communication are not in the VPC to which the VPN gateway belongs. For example, CIDR blocks (such as 0.0.0.0/0) that are connected using a VPC peering are not in the VPC to which the VPN gateway belongs.

1.12.4 Customer Subnet

Customer subnets are subnets in an on-premises data center that access a VPC on the cloud through a VPN. You need to enter subnets using CIDR notation (example: 192.168.0.0/16), and with each entry separated by a comma.

 Copyright © Huawei Technologies Co., Ltd.

636

After configuring a customer subnet, you do not need to add a route for it. The VPN service will automatically deliver routes pointing to the customer subnet.

NOTE

A customer subnet cannot be set to a Class D or Class E IP address or an IP address starting with 127.

 Copyright © Huawei Technologies Co., Ltd.

2 Getting Started

2.1 Configuring Enterprise Edition VPN to Connect an On-premises Data Center to a VPC

2.1.1 Overview

The supported regions are subject to those available on the console.

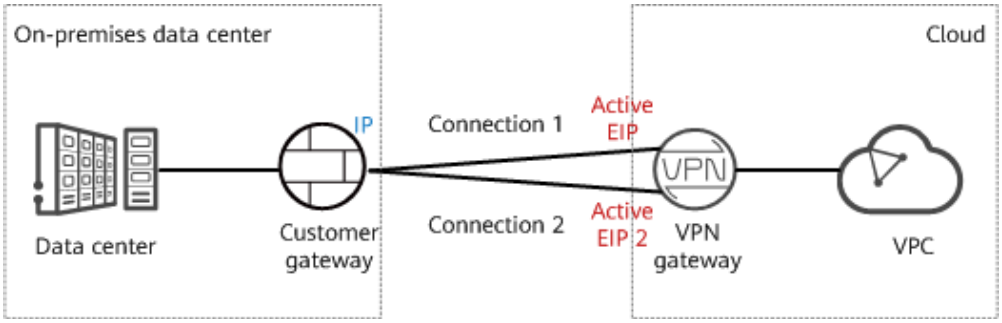
Scenario

To meet business development requirements, enterprise A needs to implement communication between its on-premises data center and its VPC. In this case, enterprise A can use the VPN service to create connections between the on-premises data center and the VPC.

- If the on-premises data center has only one customer gateway and this gateway can be configured with only one IP address, it is recommended that the VPN gateway use the active-active mode. **Figure 2-1** shows the networking.

  In active-active mode, if connection 1 fails, traffic is automatically switched to connection 2, without affecting enterprise services. After connection 1 recovers, VPN still uses connection 2 for data transmission.

Figure 2-1 Active-active mode



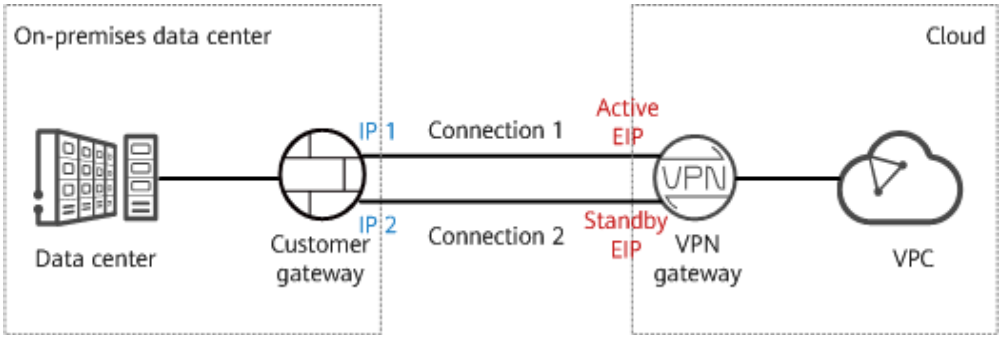
 Copyright © Huawei Technologies Co., Ltd.

638

- If the on-premises data center has two customer gateways or has only one customer gateway that can be configured with two IP addresses, it is recommended that the VPN gateway use the active/standby mode. **Figure 2-2** shows the networking.

  In active/standby mode, connection 1 is the active link and connection 2 is the standby link. By default, traffic is transmitted only through the active link. If the active link fails, traffic is automatically switched to the standby link, without affecting enterprise services. After the active link recovers, traffic is switched back to the active link.

Figure 2-2 Active/Standby mode



Limitations and Constraints

- The customer gateway device must support standard IKE and IPsec protocols.
- The interconnection subnets of the on-premises data center neither overlap with those of the VPC nor contain 100.64.0.0/10 or 214.0.0.0/8.

  If the VPC uses Direct Cloud or Cloud Connect connections to communicate with other VPCs, the on-premises data center subnets cannot overlap with those of these VPCs.

Data Plan

Table 2-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	192.168.0.0/16
VPN gateway	Interconnection subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	HA mode	Active-active

Copyright © Huawei Technologies Co., Ltd.

Category	Item	Data
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 11.xx.xx.11 • Active EIP 2: 11.xx.xx.12
VPN connection	Tunnel interface address	This address is used by a VPN gateway to establish an IPsec tunnel with a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • VPN connection 1: 169.254.70.1/30 • VPN connection 2: 169.254.71.1/30
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Gateway IP address	The gateway IP address is assigned by a carrier. In this example, the gateway IP address is: 22.xx.xx.22
	Tunnel interface address	• VPN connection 1: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30

Operation Process

Figure 2-3 shows the process of using the VPN service to enable communication between an on-premises data center and a VPC.

Figure 2-3 Operation process

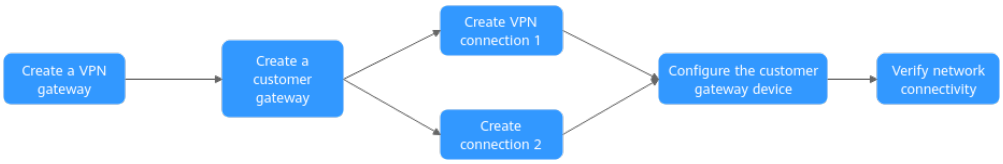


Table 2-2 Operation process description

No.	Step	Description
1	2.1.2 Step 1: Creating a VPN Gateway	Bind two EIPs to the VPN gateway. If you have purchased EIPs, you can directly bind them to the VPN gateway.

Copyright © Huawei Technologies Co., Ltd.

No.	Step	Description
2	2.1.3 Step 2: Creating a Customer Gateway	Configure the VPN device in the on-premises data center as the customer gateway.
3	2.1.4 Step 3: Creating VPN Connection 1	Create a VPN connection between the active EIP of the VPN gateway and the customer gateway.
4	2.1.5 Step 4: Creating VPN Connection 2	Create a VPN connection between active EIP 2 of the VPN gateway and the customer gateway. It is recommended that the routing mode, PSK, IKE policy, and IPsec policy settings of the two VPN connections be the same.
5	2.1.6 Step 5: Configuring the Customer Gateway Device	• The local and remote tunnel interface addresses configured on the customer gateway device must be the same as the customer and local tunnel interface addresses of the VPN connection, respectively. • The routing mode, PSK, IKE policy, and IPsec policy settings on the customer gateway device must be same as those of the VPN connection.
6	2.1.7 Step 6: Verifying Network Connectivity	Log in to an ECS and run the **ping** command to verify the network connectivity.

2.1.2 Step 1: Creating a VPN Gateway

Prerequisites

- A VPC has been created. For details about how to create a VPC, see the *Virtual Private Cloud User Guide*.
- Security group rules have been configured for ECSs in the VPC, and allow the customer gateway in the on-premises data center to access VPC resources. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner, and choose > **Virtual Private Network**.

Step 3 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.

Step 4 Click **Buy S2C VPN Gateway**.

Step 5 Set parameters as prompted, click **Create Now**, and complete the payment.

Copyright © Huawei Technologies Co., Ltd.

641

Step 6 The following describes only key parameters.

Table 2-3 Key VPN gateway parameters

Parameter	Description	Example Value
Region	Select the region nearest to you.	-
Name	Name a VPN gateway.	vpngw-001
Network Type	• **Public network**: A VPN gateway communicates with a customer gateway in an on-premises data center through the Internet. • **Private network**: A VPN gateway communicates with a customer gateway in an on-premises data center through a private network.	Public network
Associate With	Select **VPC**.	VPC
VPC	Select the VPC that needs to access the on-premises data center.	vpc-001(192.168.0.0/16)
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	Specify the VPC subnet that needs to access the on-premises data center. You can manually enter a CIDR block or select a subnet from the drop-down list box.	192.168.0.0/24
Specification	Select **Professional 1**.	Professional 1
HA Mode	Select **Active-active**.	Active-active
Active EIP	You can buy a new EIP or use an existing EIP.	11.xx.xx.11
Active EIP 2		11.xx.xx.12

----End

Verification

Check the created VPN gateway on the **VPN Gateways** page. The initial state of the VPN gateway is **Creating**. When the VPN gateway state changes to **Normal**, the VPN gateway is successfully created.

Copyright © Huawei Technologies Co., Ltd.

642

2.1.3 Step 2: Creating a Customer Gateway

Procedure

Step 1 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.

Step 2 On the **Customer Gateways** page, click **Create Customer Gateway**.

Step 3 Set parameters as prompted and click **Create Now**.

The following describes only key parameters.

Table 2-4 Customer gateway parameters

Parameter	Description	Example Value
Name	Name a customer gateway.	cgw-001
Identifier	Enter the IP address of the customer gateway.	IP Address, 22.xx.xx.22
BGP ASN	Enter the ASN of your on-premises data center or private network. The BGP ASN of the customer gateway must be different from that of the VPN gateway.	65000

----End

Verification

Check the created customer gateway on the **Customer Gateways** page.

2.1.4 Step 3: Creating VPN Connection 1

Procedure

Step 1 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.

Step 2 On the **VPN Connections** page, click **Create VPN Connection**.

Step 3 Set parameters for VPN connection 1 as prompted and click **Submit**.

The following describes only key parameters.

Table 2-5 Parameter settings for VPN connection 1

Parameter	Description	Example Value
Name	Enter the name of VPN connection 1.	vpn-001

Copyright © Huawei Technologies Co., Ltd.

643

Parameter	Description	Example Value
VPN Gateway	Select the VPN gateway created in **2.1.2 Step 1: Creating a VPN Gateway**.	vpngw-001
Gateway IP Address	Select the active EIP of the VPN gateway.	11.xx.xx.11
Customer Gateway	Select the customer gateway created in **2.1.3 Step 2: Creating a Customer Gateway**.	cgw-001
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Enter the subnet of the on-premises data center that needs to access the VPC. **NOTE** • The customer subnet can overlap with the local subnet but cannot be the same as the local subnet. • A customer subnet cannot be included in the existing subnets of the VPC associated with the VPN gateway. It also cannot be the destination address in the route table of the VPC associated with the VPN gateway. • Customer subnets cannot be the reserved CIDR blocks of VPCs, for example, 100.64.0.0/10 or 214.0.0.0/8. • If the interconnection subnet is associated with an ACL rule, ensure that the ACL rule permits the TCP port for traffic between all local and customer subnets. • Address groups cannot be used to configure the source and destination subnets in a policy on customer gateway devices.	172.16.0.0/16
Interface IP Address Assignment	The options include **Manually specify** and **Automatically assign**.	Manually specify
Local Tunnel Interface Address	Specify the tunnel interface address configured on the VPN gateway. **NOTE** The local and remote interface addresses configured on the customer gateway device must be the same as the values of **Customer Tunnel Interface IP Address** and **Local Tunnel Interface IP Address**, respectively.	169.254.70.2/30

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Customer Tunnel Interface Address	Specify the tunnel interface address configured on the customer gateway device.	169.254.70.1/30
Link Detection	This function is used for route reliability detection in multi-link scenarios. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, VPN traffic will fail to be forwarded.	**NQA** enabled
PSK, Confirm PSK	Specify the negotiation key of the VPN connection. The PSKs configured on the VPN console and the customer gateway device must be the same.	Test@123
Policy Settings	Configure the IKE and IPsec policies, which define the encryption algorithms used by the VPN tunnel. The policy settings on the VPN console and the customer gateway device must be the same.	Default

----End

Verification

Check the created VPN connection on the **VPN Connections** page. The initial state of the VPN connection is **Creating**. As the customer gateway device has not been configured, no VPN connection can be established. After about 2 minutes, the VPN connection state changes to **Not connected**.

2.1.5 Step 4: Creating VPN Connection 2

Procedure

Step 1 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.

Step 2 On the **VPN Connections** page, click **Buy VPN Connection**.

For VPN connection 2, you are advised to use the same settings as VPN connection 1, except the connection name, gateway IP address, local tunnel interface IP address, and customer tunnel interface IP address.

 Copyright © Huawei Technologies Co., Ltd.

645

Table 2-6 Parameter settings for VPN connection 2

Parameter	Description	Example Value
Name	Enter the name of VPN connection 2.	vpn-002
VPN Gateway	Select the VPN gateway created in **2.1.2 Step 1: Creating a VPN Gateway**.	vpngw-001
Gateway IP Address	Select active EIP 2 of the VPN gateway.	11.xx.xx.12
Customer Gateway	Select the customer gateway created in **2.1.3 Step 2: Creating a Customer Gateway**.	cgw-001
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Enter the subnet of the on-premises data center that needs to access the VPC. **NOTE** • The customer subnet can overlap with the local subnet but cannot be the same as the local subnet. • A customer subnet cannot be included in the existing subnets of the VPC associated with the VPN gateway. It also cannot be the destination address in the route table of the VPC associated with the VPN gateway. • Customer subnets cannot be the reserved CIDR blocks of VPCs, for example, 100.64.0.0/10 or 214.0.0.0/8. • If the interconnection subnet is associated with an ACL rule, ensure that the ACL rule permits the TCP port for traffic between all local and customer subnets. • Address groups cannot be used to configure the source and destination subnets in a policy on customer gateway devices.	172.16.0.0/16
Interface IP Address Assignment	The options include **Manually specify** and **Automatically assign**.	Manually specify

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Local Tunnel Interface Address	Specify the tunnel interface address configured on the VPN gateway. **NOTE** The local and remote interface addresses configured on the customer gateway device must be the same as the values of **Customer Tunnel Interface IP Address** and **Local Tunnel Interface IP Address**, respectively.	169.254.71.2/30
Customer Tunnel Interface Address	Specify the tunnel interface address configured on the customer gateway device.	169.254.71.1/30
Link Detection	This function is used for route reliability detection in multi-link scenarios. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, VPN traffic will fail to be forwarded.	**NQA** enabled
PSK, Confirm PSK	Specify the negotiation key of the VPN connection. The PSKs configured on the VPN console and the customer gateway device must be the same.	Test@123
Policy Settings	Configure the IKE and IPsec policies, which define the encryption algorithms used by the VPN tunnel. The policy settings on the VPN console and the customer gateway device must be the same.	Default

----End

Verification

Check the created VPN connection on the **VPN Connections** page. The initial state of the VPN connection is **Creating**. As the customer gateway device has not been configured, no VPN connection can be established. After about 2 minutes, the VPN connection state changes to **Not connected**.

 Copyright © Huawei Technologies Co., Ltd.

2.1.6 Step 5: Configuring the Customer Gateway Device

Procedure

NOTE

In this example, the customer gateway device is an AR router.

Step 1 Log in to the AR router.

Step 2 Enter the system view.

```
<AR651>system-view
```

Step 3 Configure an IP address for the WAN interface. In this example, the WAN interface of the AR router is GigabitEthernet 0/0/8.

```
[AR651]interface GigabitEthernet 0/0/8
[AR651-GigabitEthernet0/0/8]ip address 22.xx.xx.22 255.255.255.0
[AR651-GigabitEthernet0/0/8]quit
```

Step 4 Configure a default route.

```
[AR651]ip route-static 0.0.0.0 0.0.0.0 22.xx.xx.1
```

In this command, *22.xx.xx.1* is the gateway address of the AR router's public IP address. Replace it with the actual gateway address.

Step 5 Enable the SHA-2 algorithm to be compatible with the standard RFC algorithms.

```
[AR651]IPsec authentication sha2 compatible enable
```

Step 6 Configure an IPsec proposal.

```
[AR651]IPsec proposal hwproposal1
[AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
[AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
[AR651-IPsec-proposal-hwproposal1]quit
```

Step 7 Configure an IKE proposal.

```
[AR651]ike proposal 2
[AR651-ike-proposal-2]encryption-algorithm aes-128
[AR651-ike-proposal-2]dh group14
[AR651-ike-proposal-2]authentication-algorithm sha2-256
[AR651-ike-proposal-2]authentication-method pre-share
[AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
[AR651-ike-proposal-2]prf hmac-sha2-256
[AR651-ike-proposal-2]quit
```

Step 8 Configure IKE peers.

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]undo version 1
[AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer1]ike-proposal 2
[AR651-ike-peer-hwpeer1]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer1]remote-address 11.xx.xx.11
[AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer1]rsa signature-padding pss
[AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer1]quit
[AR651]ike peer hwpeer2
[AR651-ike-peer-hwpeer2]undo version 1
[AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer2]ike-proposal 2
[AR651-ike-peer-hwpeer2]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer2]remote-address 11.xx.xx.12
[AR651-ike-peer-hwpeer2]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer2]rsa signature-padding pss
```

 Copyright © Huawei Technologies Co., Ltd.

```
[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer2]quit
```

The commands are described as follows:

- **pre-shared-key cipher**: configures a PSK, which must be the same as that configured on the VPN console.
- **local-address**: specifies the public IP address of the AR router.
- **remote-address**: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 9 Configure an IPsec profile.

```
[AR651]IPsec profile hwpro1
[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1
[AR651-IPsec-profile-hwpro1]proposal hwproposal1
[AR651-IPsec-profile-hwpro1]pfs dh-group14
[AR651-IPsec-profile-hwpro1]quit
[AR651]IPsec profile hwpro2
[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2
[AR651-IPsec-profile-hwpro2]proposal hwproposal1
[AR651-IPsec-profile-hwpro2]pfs dh-group14
[AR651-IPsec-profile-hwpro2]quit
```

Step 10 Configure virtual tunnel interfaces.

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 22.xx.xx.22
[AR651-Tunnel0/0/1]destination 11.xx.xx.11
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 22.xx.xx.22
[AR651-Tunnel0/0/2]destination 11.xx.xx.12
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

The commands are described as follows:

- **interface Tunnel0/0/1** and **interface Tunnel0/0/2**: indicate the tunnel interfaces corresponding to the two VPN connections.

  In this example, Tunnel0/0/1 establishes a VPN connection with the active EIP of the VPN gateway, and Tunnel0/0/2 establishes a VPN connection with active EIP 2 of the VPN gateway.
- **ip address**: configures an IP address for a tunnel interface on the AR router.
- **source**: specifies the public IP address of the AR router.
- **destination**: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 11 Configure NQA.

```
[AR651]nqa test-instance IPsec_nqa1 IPsec_nqa1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]test-type icmp
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
```

 Copyright © Huawei Technologies Co., Ltd.

```
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit
```

The commands are described as follows:

- **nqa test-instance IPsec_nqa1 IPsec_nqa1** and **nqa test-instance IPsec_nqa2 IPsec_nqa2**: configure two NQA test instances named **IPsec_nqa1** and **IPsec_nqa2**.

  In this example, the test instance **IPsec_nqa1** is created for the VPN connection to which the active EIP of the VPN gateway belongs; the test instance **IPsec_nqa2** is created for the VPN connection to which active EIP 2 of the VPN gateway belongs.
- **destination-address**: specifies the tunnel interface address of the VPN gateway.
- **source-address**: specifies the tunnel interface address of the AR router.

Step 12 Configure association between the static route and NQA.

```
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 track nqa IPsec_nqa2 IPsec_nqa2
```

The parameters are described as follows:

- **192.168.0.0** indicates the local subnet of the VPC.
- **Tunnel***x* and **IPsec_nqa***x* in the same command correspond to the same VPN connection.

----End

Verification

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner, and choose > **Virtual Private Network**.

Step 3 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.

Verify that the states of the two VPN connections are both **Normal**.

----End

2.1.7 Step 6: Verifying Network Connectivity

Procedure

Step 1 Log in to the management console.

Step 2 Click  in the upper left corner and select the desired region and project.

Step 3 Click **Service List** and choose **Compute** > **Elastic Cloud Server**.

Step 4 Log in to an ECS.

 Copyright © Huawei Technologies Co., Ltd.

In this example, use VNC provided on the management console to log in to an ECS.

Step 5 Run the following command on the ECS:

ping 172.16.0.100

172.16.0.100 is the IP address of a server in the on-premises data center. Replace it with an actual server IP address.

If information similar to the following is displayed, the VPC on the cloud and the on-premises data center can communicate with each other.

```
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=27ms TTL=245
```

----End

2.2 VPN Creation Process

2.2.1 Buying a VPN Gateway

Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, buy a VPN gateway first.

Prerequisites

- A VPC has been created. For details about how to create a VPC, see the *Virtual Private Cloud User Guide*.
- Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
3. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
4. On the **VPN Gateways** page, click **Create VPN Gateway**.
5. Configure VPN gateway parameters based on **Table 2-7** and click **Create Now**.

Table 2-7 Description of VPN gateway parameters

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	-
Name	Name of a VPN gateway.	vpngw-001
VPC	Name of the VPC to which the VPN gateway connects.	vpc-001
Type	VPN type. **IPsec** is selected by default.	IPsec
Reliability	Only **Active-active** is supported.	Active-active

2.2.2 Buying a VPN Connection

Scenarios

To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a VPN connection after a VPN gateway is obtained.

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
3. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
4. On the **VPN Connections** page, click **Create VPN Connection**.
5. Configure the parameters as prompted and click **Create Now**. Table 2-8 lists the VPN connection parameters.

Copyright © Huawei Technologies Co., Ltd.

Table 2-8 Description of VPN connection parameters

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across regions. For low network latency and fast resource access, select the region nearest to your target users.	N/A
Name	Name of a VPN connection.	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created.	vpcgw-001
Local Subnet	VPC subnets that will access your on-premises network through a VPN. You can set the local subnet using either of the following methods: • **Select subnet**: Select the subnets that need to access your on-premises data center or private network. • **Specify CIDR block**: Enter the CIDR blocks that need to access your on-premises data center or private network.	192.168.1.0/24, 192.168.2.0/24
Remote Gateway	The public IP address of the gateway in your data center or on the private network. This IP address is used for communicating with your VPC. In active-active mode, you can enter two remote gateway addresses.	N/A
Remote Subnet	The subnets of your on-premises network that will access a VPC through a VPN. The remote and local subnets cannot overlap with each other. The remote subnet cannot overlap with CIDR blocks involved in existing VPC peering, Direct Connect, or Cloud Connect connections created for the local VPC.	192.168.3.0/24, 192.168.4.0/24

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
PSK	Private key shared by two ends of a VPN connection for negotiation. PSKs configured at both ends of the VPN connection must be the same. The PSK: • Contains 6 to 128 characters. • Can contain only: – Digits – Letters – Special characters: ~ ` ! @ # $ % ^ ( ) - _ + = [ ] { } | \ , . / : ;	Test@123
Confirm PSK	Enter the PSK again.	Test@123
Advanced Settings	• **Default**: Use default IKE and IPsec policies. • **Existing**: Use existing IKE and IPsec policies. • **Custom**: including **IKE Policy** and **IPsec Policy**, which specifies the encryption and authentication algorithms of a VPN tunnel. For details about the policies, see **Table 2-9** and **Table 2-10**.	Custom

Table 2-9 IKE policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512 The default algorithm is **SHA1**.	SHA1

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128
DH Algorithm	Diffie-Hellman key exchange algorithm. The following algorithms are supported: • Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 14 • Group 15 • Group 16 • Group 19 • Group 20 • Group 21	Group 5
Version	Version of the IKE protocol. The value can be one of the following: • v1 (not recommended due to security risks) • v2 The default value is **v2**.	v2
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **86400**.	86400

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Negotiation Mode	This parameter is only available when **Version** is set to **v1**. You can set **Negotiation Mode** to **Main** or **Aggressive**. The default mode is **Main**.	Main

Table 2-10 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following algorithms are supported: • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 • SHA2-384 • SHA2-512	SHA1
Encryption Algorithm	Encryption algorithm. The following algorithms are supported: • AES-128 • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) The default algorithm is **AES-128**.	AES-128

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: • DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 14 • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21	DH group 5
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • AH • ESP • AH-ESP The default protocol is **ESP**.	ESP
Lifetime (s)	Lifetime of an SA, in seconds An SA will be renegotiated when its lifetime expires. The default value is **3600**.	3600

NOTE

An IKE policy specifies the encryption and authentication algorithms to be used in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to be used in the data transmission phase of an IPsec tunnel. The IKE and IPsec policies must be the same at both ends of a VPN connection. If they are different, the VPN connection cannot be set up.

6. Click **Submit**.
7. You need to configure an IPsec VPN tunnel on the router or firewall in your on-premises data center.

Copyright © Huawei Technologies Co., Ltd.

3 Management

3.1 Enterprise Edition S2C VPN

3.1.1 Enterprise Edition VPN Gateway Management

Creating a VPN Gateway

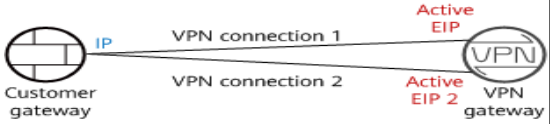
Scenario

To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a VPN gateway before creating a VPN connection.

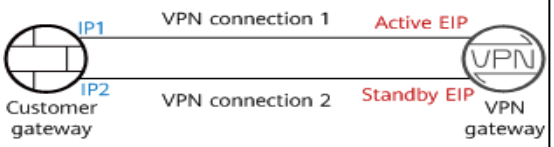
Context

The recommended networking varies according to the number of customer gateway IP addresses, as described in **Table 3-1**.

Table 3-1 Networking

Number of Customer Gateway IP Addresses	Recommended Networking	Description
1		It is recommended that the VPN gateway uses the active-active mode. In this case, one VPN connection group is used.

 Copyright © Huawei Technologies Co., Ltd.

Number of Customer Gateway IP Addresses	Recommended Networking	Description
2		It is recommended that the VPN gateway uses the active/standby mode. In this case, two VPN connection groups are used.

- If your on-premises data center has only one customer gateway configured with only one IP address, it is recommended that the VPN gateway uses the active-active mode. In this mode, you need to create a VPN connection between each of the active EIP and active EIP 2 of the VPN gateway and the IP address of the customer gateway. In this scenario, only one VPN connection group is used.
- If your on-premises data center has two customer gateways or one customer gateway configured with two IP addresses, it is recommended that the VPN gateway uses the active/standby mode. In this mode, you need to create a VPN connection with each of the customer gateway IP addresses using the active and standby EIPs of the VPN gateway. In this scenario, two VPN connection groups are used.

Prerequisites

- A VPC has been created. For details about how to create a VPC, see the *Virtual Private Cloud User Guide*.
- Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.

Procedure

Step 1 Log in to the management console.

Step 2 Click in the upper left corner and select the desired region and project.

Step 3 Click in the upper left corner, and choose > **Virtual Private Network**.

Step 4 In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.

Step 5 Click **Buy S2C VPN Gateway**.

Step 6 Set parameters as prompted and click **Create Now**.

 Copyright © Huawei Technologies Co., Ltd.

Table 3-2 lists the VPN gateway parameters.

Table 3-2 Description of VPN gateway parameters

Parameter	Description	Example Value
Region	For low network latency and fast resource access, select the region nearest to your target users. Resources cannot be shared across regions.	Select a region as required.
Name	Name of a VPN gateway. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	vpngw-001
Network Type	• **Public network**: A VPN gateway establishes VPN connections through the Internet. • **Private network**: A VPN gateway establishes VPN connections through a private network.	Public network
Associate With	• VPC Through a VPC, the VPN gateway sends messages to the customer gateway or servers in the local subnet.	VPC
VPC	Select a VPC.	vpc-001(192.168.0.0/16)
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.66.0/24
Local Subnet	VPC subnets with which your on-premises data center needs to communicate through the customer gateway. • Select subnet Select subnets of the local VPC. • Enter CIDR block Enter subnets of the local VPC or subnets of the VPC that establishes a peering connection with the local VPC.	192.168.1.0/24,192.168.2.0/24
BGP ASN	BGP ASN of the VPN gateway, which must be different from that of the customer gateway.	64512
Specification	Two options are available: **Professional 1** and **Professional 2**.	Professional 1

Copyright © Huawei Technologies Co., Ltd.

660

Parameter	Description	Example Value
AZ	An AZ is a geographic location with independent power supply and network facilities in a region. AZs in the same VPC are interconnected through private networks and are physically isolated. • If two or more AZs are available, select two AZs. The VPN gateway deployed in two AZs has higher availability. You are advised to select the AZs where resources in the VPC are located. • If only one AZ is available, select this AZ.	AZ1, AZ2
HA Mode	• Active-active – When **Associate With** is set to **VPC**, the outgoing traffic from the VPN gateway to the customer subnet is preferentially forwarded through the first VPN connection (VPN connection 1) set up between the customer subnet and an EIP. If VPN connection 1 fails, the outgoing traffic is automatically switched to the other VPN connection (VPN connection 2) set up with the customer subnet. After VPN connection 1 recovers, the outgoing traffic is still transmitted through VPN connection 2 and will not be switched back to VPN connection 1. • Active/Standby The outgoing traffic from the VPN gateway to the customer subnet is preferentially transmitted through the VPN connection (VPN connection 1) set up between the customer subnet and the active EIP. If VPN connection 1 fails, the outgoing traffic is automatically switched to the other VPN connection (VPN connection 2) set up between the customer subnet and the standby EIP. After VPN connection 1 recovers, the outgoing traffic is automatically switched back to VPN connection 1.	Active-active
Bandwidth Name	EIP bandwidth name.	Vpngw-bandwidth1

Copyright © Huawei Technologies Co., Ltd.

661

Parameter	Description	Example Value
Active EIP	This parameter is available only when **Network Type** is set to **Public network**. EIP used by the VPN gateway to communicate with a customer gateway. • **Create now**: Create an EIP. • **Use existing**: Use an existing EIP.	Create Now
Bandwidth (Mbit/s)	This parameter is available only when **Network Type** is set to **Public network**. Bandwidth of the EIP, in Mbit/s. • All VPN connections created using the EIP share the bandwidth of the EIP. The total bandwidth consumed by all the VPN connections cannot exceed the bandwidth of the EIP. If network traffic exceeds the bandwidth of the EIP, network congestion may occur and VPN connections may be interrupted. As such, ensure that you configure enough bandwidth. • You can configure alarm rules on Cloud Eye to monitor the bandwidth. • You can customize the bandwidth within the allowed range.	20 Mbit/s
Bandwidth Name	This parameter is available only when **Network Type** is set to **Public network**. EIP bandwidth name.	Vpngw-bandwidth2
Active EIP 2	This parameter is available only when the **Network Type** is set to **Public network** and **HA Mode** is set to **Active-active**. A VPN gateway needs to be bound to a group of EIPs (active EIP and active EIP 2). You can plan the bandwidth for each EIP.	Create Now
Standby EIP	This parameter is available only when the **Network Type** is set to **Public network** and **HA Mode** is set to **Active/Standby**. A VPN gateway needs to be bound to a group of EIPs (active EIP and standby EIP). You can plan the bandwidth for each EIP. The EIPs can share bandwidth with the EIPs used by other network services.	Create Now

Copyright © Huawei Technologies Co., Ltd.

662

Parameter	Description	Example Value
Bandwidth (Mbit/s)	This parameter is available only when **Network Type** is set to **Public network** and **Active EIP 2** or **Standby EIP** is set to **Create Now**. Bandwidth of the EIP, in Mbit/s. • All VPN connections created using the EIP share the bandwidth of the EIP. The total bandwidth consumed by all the VPN connections cannot exceed the bandwidth of the EIP. If network traffic exceeds the bandwidth of the EIP, network congestion may occur and VPN connections may be interrupted. As such, ensure that you configure enough bandwidth. • You can configure alarm rules on Cloud Eye to monitor the bandwidth. • You can customize the bandwidth within the allowed range.	20 Mbit/s
Advanced Settings	Parameters under **Advanced Settings** are available only when **Network Type** is set to **Private network**. • **Select**: This option applies to the scenario where VPCs of the same tenant are connected. Select the access VPC, access subnet, gateway IP address, and tags of the current tenant.	Select
Advanced Settings > Access VPC	• This parameter is available only when **Associate With** is set to **VPC** and **Network Type** is set to **Private network**. If a VPN gateway needs to connect to different VPCs in the southbound and northbound directions, set the VPC in the northbound direction as the access VPC. The VPC in the southbound direction is the VPC associated with the VPN gateway.	Same as the associated VPC
Advanced Settings > Access Subnet	• This parameter is available only when **Associate With** is set to **VPC** and **Network Type** is set to **Private network**. By default, a VPN gateway uses the interconnection subnet to connect to the associated VPC. Set this parameter when another subnet needs to be used.	Same as the interconnection subnet

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Advanced Settings > Gateway IP Address	This parameter is available only when **Associate With** is set to **VPC** and **Network Type** is set to **Private network**. • Self-assigned IP address (default) An IP address on the access subnet will be automatically assigned to the VPN gateway. You can view the automatically assigned IP address on the **VPN Gateways** page. • Manually-specified IP address Manually configure IP addresses on the access subnet for the VPN gateway.	Self-assigned IP address
Advanced Settings > Tags	Identifier of a VPN resource. The value consists of a key and a value. A maximum of 20 tags can be added. You can select predefined tags or customize tags. To view predefined tags, click **View predefined tags**. Configure **Tags** in **Advanced Settings**.	-

Step 7 Click **Create Now**.

Step 8 Confirm the VPN gateway information and click **Submit**.

----End

Viewing a VPN Gateway

Scenario

After creating a VPN gateway, you can view its details.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. On the **S2C VPN Gateways** tab page, view the VPN gateway list.
6. Click the name of a VPN gateway to view its details.
   - For a VPN gateway of the public network type, you can view the basic information and EIPs.

 Copyright © Huawei Technologies Co., Ltd.

- For VPN gateways of the private network type, you can view the basic information and advanced settings.

Modifying a VPN Gateway

Scenario

You can modify basic information about a VPN gateway, including the name and local subnet.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **S2C VPN Gateways** tab.
6. Locate the row that contains the target VPN gateway, and click **Modify Basic Information** in the **Operation** column.

   To modify only the name of a VPN gateway, you can also click  on the right of the VPN gateway name.
7. Modify the name and local subnet of the VPN gateway as prompted.
8. Click **OK**.

Table 3-3 describes the parameters for modifying the VPN gateway.

Table 3-3 Parameters for modifying the VPN gateway

Parameter	Description	Modifiable or Not
Name	Name of a VPN connection. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Y
Local Subnet	VPC subnets with which your on-premises data center needs to communicate through the customer gateway.	Y
Region	For low network latency and fast resource access, select the region nearest to your target users. Resources cannot be shared across regions.	N

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Modifiable or Not
Associate With	Select **VPC**.	N
VPC	VPC that the on-premises data center needs to access.	N
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	N
BGP ASN	BGP AS number.	N
Billing Mode	The value can be **Pay-per-use**.	N
Specification	Two options are available: **Professional 1** and **Professional 2**.	N
AZ	An AZ is a geographic location with independent power supply and network facilities in a region. AZs in the same VPC are interconnected through private networks and are physically isolated. • If two or more AZs are available, select two AZs. The VPN gateway deployed in two AZs has higher availability. You are advised to select the AZs where resources in the VPC are located. • If only one AZ is available, select this AZ.	N

Binding an EIP to a VPN Gateway

Scenario

You can bind EIPs to a VPN gateway that has been created.

Procedure

1. Log in to the management console.

Copyright © Huawei Technologies Co., Ltd.

666

2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **S2C VPN Gateways** tab.
6. Locate the row that contains the target VPN gateway, and click **Bind EIP** in the **Operation** column.
   - If the VPN gateway uses the active-active mode, the VPN gateway can have an active EIP and active EIP 2 bound.
   - If the VPN gateway uses the active/standby mode, the VPN gateway can have an active EIP and a standby EIP bound.
7. Select the desired EIP and click **OK**.

Unbinding an EIP from a VPN Gateway

Scenario

After a VPN gateway is created, you can unbind an EIP from it.

Notes and Constraints

An EIP that is in use by a VPN connection cannot be unbound from a VPN gateway.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. Click the **S2C VPN Gateways** tab.
6. Locate the row that contains the target VPN gateway, and click **Unbind EIP** or choose **More** > **Unbind EIP** in the **Operation** column.
   - If the VPN gateway uses the active-active mode, the active EIP and active EIP 2 can be unbound from the VPN gateway.
   - If the VPN gateway uses the active/standby mode, the active EIP and standby EIP can be unbound from the VPN gateway.
7. In the displayed dialog box, click **Yes**.

   NOTE

   An EIP will continue to be billed after being unbound from a VPN gateway. If you no longer need an EIP, you are advised to release it.

 Copyright © Huawei Technologies Co., Ltd.

Deleting a VPN Gateway

Scenario

You can delete a VPN gateway that is no longer required.

Notes and Constraints

- The delete operation is not supported for a VPN gateway that is being created, updated, or deleted.
- If a VPN gateway has VPN connections configured, you need to delete all the VPN connections before deleting the VPN gateway.

  For details about how to delete a VPN connection, see **Deleting a VPN Connection**.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
5. If the number of bound EIPs is greater than 1, click **Delete** in the **Operation** column of the target VPN gateway.
6. In the displayed dialog box, click **Yes**.

Searching for VPN Gateways by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the VPN console.

Prerequisites

You have added tags to VPN resources.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.

 Copyright © Huawei Technologies Co., Ltd.

5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.
   - You can only select existing keys and values from the drop-down list.
   - You can select a maximum of 20 tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.
   - You can use tags together with other types of filter criteria. The relationship between them is AND.

3.1.2 Customer Gateway Management of Enterprise Edition VPN

Creating a Customer Gateway

Scenario

To connect your on-premises data center or private network to your ECSs in a VPC, you need to create a customer gateway before creating a VPN connection.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. On the **Customer Gateways** page, click **Create Customer Gateway**.
6. Set parameters as prompted and click **Create Now**.

   Table 3-4 lists the customer gateway parameters.

Table 3-4 Description of customer gateway parameters

Parameter	Description	Example Value
Name	Name of a customer gateway. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	cgw-001

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Identifier	• **IP Address**: Specify the IP address of the customer gateway. • **FQDN**: Enter an FQDN. The value is a string of 1 to 128 case-sensitive characters, including letters, digits, and special characters (excluding & < > [ ] \). Spaces are not supported. If the customer gateway does not have a fixed IP address, select **FQDN**. Ensure that UDP port 4500 is permitted in a firewall rule on the customer gateway in your on-premises data center or private network.	• IP Address, 1.2.3.4 • FQDN, cgw-fqdn
BGP ASN	Enter the ASN of your on-premises data center or private network. The BGP ASN of the customer gateway must be different from that of the VPN gateway.	65000
Advanced Settings > Tags	Identifier of a VPN resource. The value consists of a key and a value. A maximum of 20 tags can be added. You can select predefined tags or customize tags. To view predefined tags, click **View predefined tags**.	-

7. (Optional) If there are two customer gateways, repeat the preceding operations to configure the other customer gateway with a different identifier.

Related Operations

You need to configure an IPsec VPN tunnel on the router or firewall in your on-premises data center.

Viewing a Customer Gateway

Scenario

After creating a customer gateway, you can view its details.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.

 Copyright © Huawei Technologies Co., Ltd.

3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. On the **Customer Gateways** page, view the customer gateway list.
6. Click the name of a customer gateway to view its details.
   - In the **Basic Information** area, you can view the **Name**, **ID**, **BGP ASN**, and **VPN Connection** of the customer gateway.

Modifying a Customer Gateway

Scenario

After creating a customer gateway, you can modify its name.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. On the **Customer Gateways** page, click next to the name of a customer gateway.
6. Enter a new name for the customer gateway and click **OK**.

   Table 3-5 describes the parameters related to customer gateway modification.

Table 3-5 Parameters related to customer gateway modification

Parameter	Description	Modifiable or Not
Name	Name of a VPN connection. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Y
BGP ASN	The BGP ASN needs to be specified only when **Routing Mode** is set to **Dynamic (BGP)**.	N

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Modifiable or Not
Gateway IP Address	IP address used by the customer gateway to communicate with the VPN gateway. The value must be a static address. Ensure that UDP port 4500 is permitted in a firewall rule on the customer gateway in your on-premises data center or private network.	N

Deleting a Customer Gateway

Scenario

You can delete a customer gateway that you have created.

Notes and Constraints

Before deleting a customer gateway associated with a VPN connection, remove the customer gateway from the VPN connection.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. On the **Customer Gateways** page, locate the customer gateway to delete, and click **Delete** in the **Operation** column.
6. Click **Yes**.

Searching for Customer Gateways by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the VPN console.

Copyright © Huawei Technologies Co., Ltd.

Prerequisites

You have added tags to VPN resources.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – Customer Gateways**.
5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.
   - You can only select existing keys and values from the drop-down list.
   - You can select a maximum of 20 tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.
   - You can use tags together with other types of filter criteria. The relationship between them is AND.

3.1.3 Enterprise Edition VPN Connection Management

Creating a VPN Connection

Scenario

To connect your on-premises data center or private network to your ECSs in a VPC, you need to create VPN connections after creating a VPN gateway and a customer gateway.

Notes and Constraints

- When creating a VPN connection in static routing mode, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection before enabling NQA. Otherwise, traffic will fail to be forwarded.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connections** page, click **Create VPN Connection**.

Copyright © Huawei Technologies Co., Ltd.

NOTE

For higher reliability, you are advised to create a VPN connection between each of the two EIPs of a VPN gateway and a customer gateway.

6. Set parameters as prompted and click **Buy Now**.

   Table 3-6 lists the VPN connection parameters.

Table 3-6 Description of VPN connection parameters

Parameter	Description	Example Value
Name	Name of a VPN connection. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	vpn-001
VPN Gateway	Name of the VPN gateway for which the VPN connection is created. You can also click **Buy S2C VPN Gateway** to create a VPN gateway. For details about the configuration parameters, see **Table 3-2**.	vpngw-001
Gateway IP Address	IP address of the VPN gateway. The same EIP of a VPN gateway cannot be repeatedly selected when you create VPN connections between the VPN gateway and the same customer gateway.	Available gateway IP address
Customer Gateway	Name of a customer gateway. You can also click **Create Customer Gateway** to create a customer gateway. For details about related parameters, see **Table 3-4**. **NOTE** If a customer gateway connects to multiple VPN gateways, the BGP ASNs and VPN types of the VPN gateways must be the same.	cgw-001

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
VPN Type	IPsec connection mode, which can be route-based or policy-based. • Static routing Determines the data that enters the IPsec VPN tunnel based on the route configuration (local subnet and customer subnet). **Application scenario: Communication between customer gateways** • BGP routing Determines the traffic that can enter the IPsec VPN tunnel based on BGP routes. **Application scenario: Communication between customer gateways, many or frequently changing interconnection subnets, or backup between VPN and Direct Connect** • Policy-based Determines the data that enters the IPsec VPN tunnel based on the policy (between the customer network and VPC). Policy rules can be defined based on the source and destination CIDR blocks. **Application scenario: Isolation between customer gateways**	Static routing

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Customer Subnet	Customer-side subnet that needs to access the VPC on the cloud through VPN connections. If there are multiple customer subnets, separate them with commas (,). **NOTE** • The customer subnet can overlap with the local subnet but cannot be the same as the local subnet. • A customer subnet cannot be included in the existing subnets of the VPC associated with the VPN gateway. It also cannot be the destination address in the route table of the VPC associated with the VPN gateway. • Customer subnets cannot be the reserved CIDR blocks of VPCs, for example, 100.64.0.0/10 or 214.0.0.0/8. • If the interconnection subnet is associated with an ACL rule, ensure that the ACL rule permits the TCP port for traffic between all local and customer subnets. • Address groups cannot be used to configure the source and destination subnets in a policy on customer gateway devices.	172.16.1.0/24,172.16.2.0/24

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Interface IP Address Assignment	This parameter is available only when **VPN Type** is set to **Static routing** or **BGP routing**. **NOTE** • Set interface IP addresses to the tunnel interface IP addresses used by the VPN gateway and customer gateway to communicate with each other. • If the tunnel interface address of the customer gateway is fixed, select **Manually specify**, and set the tunnel interface address of the VPN gateway based on the tunnel interface address of the customer gateway. • Manually specify – Set **Local Tunnel Interface Address** to the tunnel interface address of the VPN gateway, which can reside only on the 169.254.x.x/30 CIDR block (except 169.254.195.x/30). Then, the system automatically sets **Customer Tunnel Interface Address** to a random value based on the setting of **Local Tunnel Interface Address**. For example, when you set **Local Tunnel Interface Address** to **169.254.1.6/30**, the system automatically sets **Customer Tunnel Interface Address** to **169.254.1.5/30**. – When you set **VPN Type** to **BGP routing** and configure tunnel interface addresses in **Manually specify** mode, ensure that the local and remote tunnel interface addresses configured on the customer gateway device (the other end of the VPN connection) are the same as the values of **Customer Tunnel Interface Address** and **Local Tunnel Interface Address**, respectively. • Automatically assign	Automatically assign

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
	– By default, an IP address on the 169.254.x.x/30 CIDR block is assigned to the tunnel interface of the VPN gateway. – To view the automatically assigned local and customer interface IP addresses, click **Modify VPN Connection** on the **VPN Connections** page. – When you set **VPN Type** to **BGP routing** and select **Automatically assign**, check the automatically assigned local and customer tunnel interface addresses after the VPN connection is created. Ensure that the local and remote tunnel interface addresses configured on the customer gateway device (the other end of the VPN connection) are the reverse of the settings on the cloud side.	
Local Tunnel Interface Address	This parameter is available only when **Interface IP Address Assignment** is set to **Manually specify**. Tunnel interface IP address configured on the VPN gateway.	N/A
Customer Tunnel Interface Address	This parameter is available only when **Interface IP Address Assignment** is set to **Manually specify**. Tunnel interface IP address configured on the customer gateway device.	N/A

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Link Detection	This parameter is available only when **VPN Type** is set to **Static routing**. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, traffic will fail to be forwarded. After this function is enabled, the VPN gateway automatically performs Network Quality Analysis (NQA) on the customer interface IP address of the customer gateway.	Selected
PSK	The PSKs configured for the VPN gateway and customer gateway must be the same. The PSK: • Contains 8 to 128 characters. • Can contain only three or more types of the following characters: – Digits – Uppercase letters – Lowercase letters – Special characters: ~ ! @ # $ % ^ ( ) - _ + = { } , . / : ;	Test@123
Confirm PSK	Enter the PSK again.	Test@123

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Policy	This parameter is available only when **VPN Type** is set to **Policy-based**. Defines the data flow that enters the encrypted VPN connection between the local and customer subnets. You need to configure the source and destination CIDR blocks in each policy rule. By default, a maximum of five policy rules can be configured. • Source CIDR Block The source CIDR block must contain some CIDR blocks of the local subnets. **0.0.0.0/0** indicates any IP address. • Destination CIDR Block The destination CIDR block must contain all the CIDR blocks of the customer subnets. A policy rule supports a maximum of five destination CIDR blocks, which are separated by commas (,).	• Source CIDR block 1: 192.168.1.0/24 • Destination CIDR block 1: 172.16.1.0/24,172.16.2.0/24 • Source CIDR block 2: 192.168.2.0/24 • Destination CIDR block 2: 172.16.1.0/24,172.16.2.0/24
Policy Settings	• **Default**: Use default IKE and IPsec policies. • **Custom**: Use custom IKE and IPsec policies. For details about the policies, see **Table 3-7** and **Table 3-8**.	Custom
Advanced Settings > Tags	Identifier of a VPN resource. The value consists of a key and a value. A maximum of 20 tags can be added. You can select predefined tags or customize tags. To view predefined tags, click **View predefined tags**.	-

Copyright © Huawei Technologies Co., Ltd.

Table 3-7 IKE policy

Parameter	Description	Example Value
Version	Version of the IKE protocol. The value can be one of the following: • v1 (v1 has low security. If the device supports v2, v2 is recommended.) • v2 The default value is **v2**.	v2
Negotiation Mode	This parameter is available only when **Version** is **v1**. • Main • Aggressive	Main
Authentication Algorithm	Hash algorithm used for authentication. The following options are available: • SHA1(Insecure. Not recommended.) • MD5(Insecure. Not recommended.) • SHA2-256 • SHA2-384 • SHA2-512 The default value is **SHA2-256**.	SHA2-256
Encryption Algorithm	Encryption algorithm. The following options are available: • 3DES(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-256(Insecure. Not recommended.) • AES-128-GCM-16 • AES-256-GCM-16 When this encryption algorithm is used, the IKE version can only be **v2**. The default value is **AES-128**.	AES-128

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
DH Algorithm	The following algorithms are supported: • Group 1(Insecure. Not recommended.) • Group 2(Insecure. Not recommended.) • Group 5(Insecure. Not recommended.) • Group 14(Insecure. Not recommended.) • Group 15 • Group 16 • Group 19 • Group 20 • Group 21 The default value is **Group 15**.	Group 15
Lifetime (s)	Lifetime of a security association (SA). An SA will be renegotiated when its lifetime expires. • Unit: second • The value ranges from **60** to **604800**. • The default value is **86400**.	86400
Local ID	Authentication identifier of the VPN gateway used in IPsec negotiation. The VPN gateway ID configured on the customer gateway must be the same as the local ID configured here. Otherwise, IPsec negotiation fails. • IP Address (default value) The system automatically sets this parameter to the selected EIP of the VPN gateway. • FQDN Set the FQDN to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces).	IP Address

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Customer ID	Authentication identifier of the customer gateway used in IPsec negotiation. The customer gateway ID configured on the customer gateway must be the same as the customer ID configured here. Otherwise, IPsec negotiation fails. • IP Address (default value) The system automatically sets this parameter to the IP address of the customer gateway. • FQDN Set the FQDN to a string of 1 to 128 case-sensitive characters that can contain letters, digits, and special characters (excluding &, <, >, [,], \, ?, and spaces).	IP Address

Table 3-8 IPsec policy

Parameter	Description	Example Value
Authentication Algorithm	Hash algorithm used for authentication. The following options are available: • SHA1(Insecure. Not recommended.) • MD5(Insecure. Not recommended.) • SHA2-256 • SHA2-384 • SHA2-512 The default value is **SHA2-256**.	SHA2-256

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Encryption Algorithm	Encryption algorithm. The following options are available: • 3DES(Insecure. Not recommended.) • AES-128(Insecure. Not recommended.) • AES-192(Insecure. Not recommended.) • AES-256(Insecure. Not recommended.) • AES-128-GCM-16 • AES-256-GCM-16 The default value is **AES-128**.	AES-128
PFS	Algorithm used by the Perfect forward secrecy (PFS) function. PFS supports the following algorithms: • Disable(Insecure. Not recommended.) • DH group 1(Insecure. Not recommended.) • DH group 2(Insecure. Not recommended.) • DH group 5(Insecure. Not recommended.) • DH group 14(Insecure. Not recommended.) • DH group 15 • DH group 16 • DH group 19 • DH group 20 • DH group 21 The default value is **DH group 15**.	DH group 15
Transfer Protocol	Security protocol used in IPsec to transmit and encapsulate user data. The following protocols are supported: • ESP The default value is **ESP**.	ESP

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Example Value
Lifetime (s)	Lifetime of an SA. An SA will be renegotiated when its lifetime expires. • Unit: second • The value ranges from **30** to **604800**. • The default value is **3600**.	3600

NOTE

An IKE policy specifies the encryption and authentication algorithms to use in the negotiation phase of an IPsec tunnel. An IPsec policy specifies the protocol, encryption algorithm, and authentication algorithm to use in the data transmission phase of an IPsec tunnel. The policy settings for VPN connections must be the same at the VPC and on-premises data center sides. If they are different, VPN negotiation will fail, causing the failure to establish VPN connections.

The following algorithms are not recommended because they are not secure enough:

- Authentication algorithms: SHA1 and MD5
- Encryption algorithms: 3DES, AES-128, AES-192, and AES-256

  Because some customer devices do not support secure encryption algorithms, the default encryption algorithm of VPN connections is still AES-128. You are advised to use a more secure encryption algorithm if customer devices support secure encryption algorithms.
- DH algorithms: Group 1, Group 2, Group 5, and Group 14

7. Confirm the VPN connection configuration and click **Submit**.
8. Repeat the preceding operations to create the other VPN connection.

   For details about the IP address configuration, see **Context**.

Configuring Health Check

Scenario

After VPN connections are created, you can configure health check to enable the VPN gateway to send probe packets to the customer gateway to collect statistics about the round-trip time and packet loss rate of physical links. The statistics help you learn about the VPN connection quality. The Cloud Eye service monitors the round-trip time and packet loss rate of VPN links. For details, see **3.3.1 Metrics (S2C Enterprise Edition VPN)**.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner, and choose > **Virtual Private Network**.

Copyright © Huawei Technologies Co., Ltd.

4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connections** page, click the name of the target VPN connection. On the **Summary** tab page, click **Add** in the **Health Check** area.
6. In the **Add Health Check** dialog box, click **OK**.

Viewing a VPN Connection

Scenario

After creating a VPN connection, you can view its details.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connections** page, view the VPN connection list.
6. Click the name of a VPN connection to view its basic information and policy configuration.

NOTE

- In the VPN connection list, locate the target VPN connection, and choose **More** > **Modify Policy Settings** on the right to view IKE and IPsec policies of the VPN connection.

Modifying a VPN Connection

Scenario

A VPN connection is an encrypted communications channel established between a VPN gateway in a VPC and a customer gateway in your on-premises data center. You can modify a VPN connection when required.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connections** page, locate the VPN connection to modify, and click **Modify VPN Connection** or **Modify Policy Settings**.
6. Modify VPN connection parameters as prompted.

Copyright © Huawei Technologies Co., Ltd.

686

7. Click **OK**.

CAUTION

If you change the PSK or modify the IKE or IPsec policy of a VPN connection, ensure that the new configurations are consistent with those on the customer gateway. Otherwise, the VPN connection will be interrupted.

Only some of the parameters take effect immediately after being modified, as described in **Table 3-9**.

Table 3-9 Time when new parameter settings take effect

Item	Parameter	When New Settings Take Effect	How to Modify
-	PSK	• When IKEv1 is used, the new setting takes effect in the next negotiation period. • When IKEv2 is used, the new setting takes effect after the VPN connection is re-established.	• When IKEv1 is used: Locate the VPN connection to modify, choose **More** > **Reset PSK** on the right, and change the PSK as prompted. • When IKEv2 is used: 1. Delete the current VPN connection. 2. Create a new VPN connection.
IKEv1 policy	Encryption Algorithm	The new settings take effect in the next negotiation period.	Locate the VPN connection to modify, and click **Modify VPN Configuration**.
	Authentication Algorithm		
	DH Algorithm		
	Negotiation Mode		
	Local ID		
	Customer ID		

Copyright © Huawei Technologies Co., Ltd.

Item	Parameter	When New Settings Take Effect	How to Modify
	Lifetime (s)		
	Version	The new settings take effect immediately.	
IKEv2 policy	Encryption Algorithm	The new settings take effect in the next negotiation period.	Locate the VPN connection to modify, and click **Modify VPN Configuration**.
	Authentication Algorithm		
	DH Algorithm		
	Lifetime (s)		
	Version	The new settings take effect immediately.	
	Local ID	The new settings take effect after the VPN connection is re-established.	1. Delete the current VPN connection. 2. Create a new VPN connection.
	Customer ID		
IPsec policy	Encryption Algorithm	The new settings take effect in the next negotiation period.	Locate the VPN connection to modify, and click **Modify VPN Configuration**.
	Authentication Algorithm		
	PFS		
	Lifetime (s)		
	Transfer Protocol	This parameter cannot be modified on the management console.	

Table 3-10 describes the parameters related to VPN connection modification.

Copyright © Huawei Technologies Co., Ltd.

Table 3-10 Parameters related to VPN connection modification

Parameter	Description	Modifiable or Not
Name	Name of a VPN connection. The value can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	Y
Customer Gateway	Gateway used for communicating with a VPC through VPN.	Y
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC.	Y
Policy Settings	There are IKE and IPsec policies.	Y
PSK	The PSKs configured for the VPN gateway and customer gateway must be the same.	Y
VPN Gateway	VPN gateway that has been created.	N
Gateway IP Address	IP address used by the customer gateway to communicate with the VPN gateway. The value must be a static address. Ensure that UDP port 4500 is permitted in a firewall rule on the customer gateway in your on-premises data center or private network.	N
Interface IP Address Assignment	Mode in which IP addresses of the local and customer interfaces are assigned. The options include **Manually specify** and **Automatically assign**.	N
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	N
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	N

Copyright © Huawei Technologies Co., Ltd.

Deleting a VPN Connection

Scenario

If a VPN connection is no longer required, you can delete it to release network resources.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. On the **VPN Connections** page, locate the row that contains the target VPN connection, and choose **More** > **Delete**.
6. In the displayed dialog box, click **Yes**.

Searching for VPN Connections by Tag

Scenario

When using the VPN service, you can classify VPN resources based on specific rules to facilitate resource management and fee calculation.

With the Tag Management Service (TMS), you can add tags to your VPN resources to classify them. Additionally, you can quickly search for VPN resources by tag on the VPN console.

Prerequisites

You have added tags to VPN resources.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, and choose > **Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Connections**.
5. Click in the text box for selecting a property or entering a keyword, choose a tag key under **Resource Tag**, and select a tag value.
   - You can only select existing keys and values from the drop-down list.
   - You can select a maximum of 20 tags to search for VPN resources. If you select multiple tags, the relationship between them is AND.
   - You can use tags together with other types of filter criteria. The relationship between them is AND.

Copyright © Huawei Technologies Co., Ltd.

3.2 Classic VPN

3.2.1 Classic VPN Gateway Management

Viewing a VPN Gateway

Scenarios

After creating a VPN gateway, you can view its details.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
3. In the navigation pane on the left, choose **Virtual Private Network**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
4. View VPN gateway information.

Modifying a VPN Gateway

1. Log in to the management console.
2. Click  in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
3. In the navigation pane on the left, choose **Virtual Private Network**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
4. On the **VPN Gateways** page, locate the row that contains the target VPN gateway and click **Modify** in the **Operation** column.
5. Modify the VPN gateway name or description as required.
6. Click **OK**.

Modifying Basic Information About a VPN Gateway

Scenario

You can modify the name and description of a VPN gateway.

Procedure

1. Log in to the management console.

Copyright © Huawei Technologies Co., Ltd.

2. Click in the upper left corner and select the desired region and project.
3. Click in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
4. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
5. Locate the row that contains the VPN gateway that you want to modify, and choose **More** > **Modify Basic Information** in the **Operation** column.
6. Modify the VPN gateway name or description as required.

   NOTE

   The name of a VPN gateway can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
7. Click **OK**.

Deleting a VPN Gateway

Scenarios

If a VPN gateway is no longer required, you can delete it to release network resources as long as it has no VPN connections configured.

If it has any connections configured, delete the connections first.

Procedure

1. Log in to the management console.
2. Click in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
3. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Gateways**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**.
4. Locate the row that contains the target VPN gateway, and choose **More** > **Delete** in the **Operation** column.

   If Enterprise Edition VPN is available for the selected region, locate the row that contains the target VPN gateway, and choose **More** > **Delete**.
5. In the displayed dialog box, click **Yes**.

3.2.2 Classic VPN Connection Management

Copyright © Huawei Technologies Co., Ltd.

Viewing a VPN Connection

Scenarios

After creating a VPN connection, you can view its details.

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
3. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**. Then, click the **VPN Connections** tab.
4. View the VPN connection information. You can also locate the row that contains the target VPN connection, and click **View Policy** in the **Operation** column to view IKE and IPsec policy details of the VPN connection.

Modifying a VPN Connection

Scenarios

A VPN connection is an encrypted communications channel established between the VPN gateway in your VPC and that in an on-premises data center. The VPN connection can be modified after creation.

CAUTION

If you modify the advanced settings, network communications may be interrupted. Exercise caution when performing this operation.

Changing the PSK only will not delete the current VPN connection. The new PSK takes effect during IKE renegotiation after the IKE lifetime expires.

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
3. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**. Then, click the **VPN Connections** tab.

Copyright © Huawei Technologies Co., Ltd.

4. Locate the row that contains the target VPN connection, and click **Modify** in the **Operation** column.
5. In the displayed **Modify VPN Connection** dialog box, modify parameters as required.

   NOTE

   The name of a VPN gateway can contain only letters, digits, underscores (_), hyphens (-), and periods (.).
6. Click **OK**.

Deleting a VPN Connection

Scenarios

If a VPN connection is no longer required, you can delete it to release network resources.

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner, select a region, and choose **Network** > **Virtual Private Network**.

   The VPN console is displayed.
3. In the navigation pane on the left, choose **Virtual Private Network** > **Classic – VPN Connections**.

   If Enterprise Edition VPN is available for the selected region, choose **Virtual Private Network** > **Classic**. Then, click the **VPN Connections** tab.
4. Locate the row that contains the target VPN connection, and choose **More** > **Delete** in the **Operation** column.
5. In the displayed dialog box, click **Yes**.

3.3 Monitoring

3.3.1 Metrics (S2C Enterprise Edition VPN)

Description

This section describes monitored metrics reported by VPN to Cloud Eye as well as their namespaces and dimensions. You can use the Cloud Eye management console to query the metrics of the monitored objects and alarms generated for VPN.

Namespace

SYS.VPN

Copyright © Huawei Technologies Co., Ltd.

Metrics

Table 3-11 Metrics supported for Enterprise Edition VPN gateways

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
gateway_send_pkt_rate	Outbound Packet Rate	Average number of data packets leaving the cloud per second.	≥ 0 pps	Gateway	1 minute
gateway_recv_pkt_rate	Inbound Packet Rate	Average number of data packets entering the cloud per second.	≥ 0 pps	Gateway	1 minute
gateway_send_rate	Outbound Bandwidth	Average volume of traffic leaving the cloud per second.	0–1 Gbit/s	Gateway	1 minute
gateway_recv_rate	Inbound Bandwidth	Average volume of traffic entering the cloud per second.	0–1 Gbit/s	Gateway	1 minute
gateway_send_rate_usage	Outbound Bandwidth Usage	Bandwidth utilization for traffic leaving the cloud.	0-100%	Gateway	1 minute
gateway_recv_rate_usage	Inbound Bandwidth Usage	Bandwidth utilization for traffic entering the cloud.	0-100%	Gateway	1 minute
gateway_connection_num	Number of Connections	Number of VPN connections.	≥ 0	Gateway	1 minute

Copyright © Huawei Technologies Co., Ltd.

Table 3-12 Enterprise Edition VPN connection metrics

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
tunnel_average_latency	Average Tunnel RTT	Average round-trip time on the tunnel between the VPN gateway and customer gateway.	0–5000 ms	VPN connection	1 minute
tunnel_max_latency	Maximum Tunnel RTT	Maximum round-trip time on the tunnel between the VPN gateway and customer gateway.	0–5000 ms	VPN connection	1 minute
tunnel_packet_loss_rate	Tunnel Packet Loss Rate	Packet loss rate on the tunnel between the VPN gateway and customer gateway.	0–100 %	VPN connection	1 minute
link_average_latency	Average Link RTT	Average round-trip time on the physical link between the VPN gateway and customer gateway.	0–5000 ms	VPN connection	1 minute
link_max_latency	Maximum Link RTT	Maximum round-trip time on the physical link between the VPN gateway and customer gateway.	0–5000 ms	VPN connection	1 minute
link_packet_loss_rate	Link Packet Loss Rate	Packet loss rate on the physical link between the VPN gateway and customer gateway.	0–100 %	VPN connection	1 minute
connection_status	VPN Connection Status	Status of a VPN connection: **0**: not connected **1**: connected **2**: unknown	0, 1, or 2	VPN connection	1 minute
recv_pkt_rate	Packet Receive Rate	Average number of data packets received per second.	≥ 0 pps	VPN connection	1 minute
send_pkt_rate	Packet Send Rate	Average number of data packets sent per second.	≥ 0 pps	VPN connection	1 minute

Copyright © Huawei Technologies Co., Ltd.

696

Metric ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
recv_rate	Traffic Receive Rate	Average volume of traffic received per second.	0~1G bit/s	VPN connection	1 minute
send_rate	Traffic Send Rate	Average volume of traffic sent per second.	0~1G bit/s	VPN connection	1 minute

Dimensions

key	Value
evpn_connection_id	Enterprise Edition VPN connection
evpn_gateway_id	Enterprise Edition VPN gateway

3.3.2 Viewing Metrics

Scenarios

View the VPN connection status and usages of bandwidth and EIP. You can view data of the last 1, 3, 12, or 24 hours, or last 7 days.

Viewing VPN Gateway Metrics

- Viewing metrics on the VPN console
  a. Log in to the management console.
  b. Click in the upper left corner and select the desired region and project.
  c. Click in the upper left corner of the management console, and choose **Network** > **Virtual Private Network**.
  d. View metrics.
     - VPN: Choose **Virtual Private Network** > **Enterprise – VPN Gateways** > **S2C VPN Gateways**, and click in the **Gateway IP Address** column of a VPN gateway. You can view metrics of two EIPs separately.

       The metrics are EIP metrics, including **Outbound Bandwidth**, **Inbound Bandwidth**, **Inbound Bandwidth Usage**, **Outbound Bandwidth Usage**, **Outbound Traffic**, and **Inbound Traffic**.

Copyright © Huawei Technologies Co., Ltd.

Viewing VPN Connection Metrics

- Viewing metrics on the VPN console
  a. Log in to the management console.
  b. Click  in the upper left corner and select the desired region and project.
  c. Click  in the upper left corner of the management console, and choose **Network** > **Virtual Private Network**.
  d. View metrics.
     - VPN: Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click  **View Metric** under the name of a VPN connection.

       The metrics include the following:
       - VPN Connection Status
       - Average Link RTT, Maximum Link RTT, Link Packet Loss Rate

         These metrics are displayed only after the health check function is enabled. To enable this function, click the name of a VPN connection and add health check items on the **Summary** tab page.
       - Average Tunnel RTT, Maximum Tunnel RTT, Tunnel Packet Loss Rate

         These metrics are displayed only when **VPN Type** is set to **Static routing** and the NQA function is enabled.

3.3.3 Creating Alarm Rules

Scenarios

You can create alarm rules to customize monitored objects and notification policies, so that you can be well-informed of the VPN service status.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner of the management console, and choose **Management & Governance** > **Cloud Eye**.
4. Choose **Cloud Service Monitoring** > **Virtual Private Network**, and configure alarm rules for different types of alarms as required.
   - Alarms related to VPN gateways in S2C Enterprise Edition VPN: Click the **S2C VPN Gateway** tab, and click **Create Alarm Rule** in the **Operation** column of a VPN gateway.
   - Alarms related to VPN connections in S2C Enterprise Edition VPN: Click the **S2C VPN Connection** tab, and click **Create Alarm Rule** in the **Operation** column of a VPN connection.

Copyright © Huawei Technologies Co., Ltd.

5. Configure an alarm rule on the **Create Alarm Rule** page.
6. Click **Create**.

   After the alarm rule is created, if you have enabled **Alarm Notification** and configured required parameters, you will receive notifications once an alarm is triggered.

   NOTE

   For more information about VPN alarm rules, see the *Cloud Eye User Guide*.

3.4 Audit

3.4.1 VPN Operations That Can Be Recorded by CTS

Table 3-13 Operations related to S2C Enterprise Edition VPN that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a customer gateway	customer-gateway	createCgw
Updating a customer gateway	customer-gateway	updateCgw
Deleting a customer gateway	customer-gateway	deleteCgw
Creating a VPN gateway	vpn-gateway	createVgw
Updating a VPN gateway	vpn-gateway	updateVgw
Deleting a VPN gateway	vpn-gateway	deleteVgw
Updating the VPN gateway status	vpn-gateway	UpdateResourceState
Creating a VPN connection	vpn-connection	createVpnConnection
Updating a VPN connection	vpn-connection	updateVpnConnection
Deleting a VPN connection	vpn-connection	deleteVpnConnection
Creating a resource tag	instance	createResourceTag
Deleting a resource tag	instance	deleteResourceTag

Copyright © Huawei Technologies Co., Ltd.

3.5 Permissions Management

3.5.1 Creating a User and Granting VPN Permissions

Use the **Identity and Access Management (IAM)** service to implement fine-grained permissions control over your VPN resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing VPN resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Grant the permission to perform professional and efficient O&M on your VPN resources to other accounts or cloud services.

If your account meets your permissions requirements, you can skip this section.

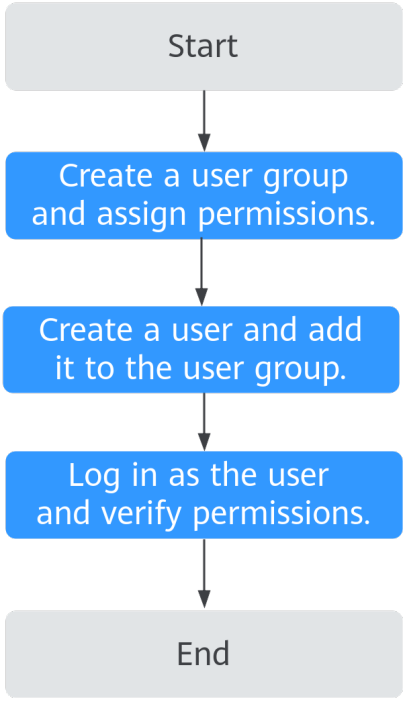
This section describes the procedure for granting permissions (see **Figure 3-1**).

Prerequisites

You have learned about the permissions supported by VPN, and determined the permissions to be granted to a user group. Before granting permissions of other services, learn about all **permissions** supported by IAM.

Process Flow

Figure 3-1 Process of granting VPN permissions



Copyright © Huawei Technologies Co., Ltd.

1. **Create a user group and assign permissions** to it.

   Create a user group on the IAM console and attach the **VPN Administrator** policy to the group.

2. **Create a user and add it to the user group**.

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in** and verify permissions.

   Log in to the management console as the created user. Switch to the authorized region and verify the permissions.

   - Click **Service List** and choose **Networking** > **Virtual Private Network**. On the **Enterprise – VPN Gateways** page, click **Buy VPN Gateway** in the upper right corner. If the VPN gateway is successfully created, the **VPN Administrator** policy has already taken effect.
   - Choose any other service in **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **VPN Administrator** policy has already taken effect.

3.5.2 VPN Custom Policies

Custom policies can be created to supplement the system-defined policies of VPN.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following section contains examples of common VPN custom policies.

Example VPN custom policy

- Example 1: Grant permission to delete VPN gateways.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpn:vpnGateways:delete"
         ]
      }
   ]
}
```

- Example 2: Deny VPN connection deletion.

  A policy with only "Deny" permissions must be used together with other policies. If the permissions granted to an IAM user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **VPN FullAccess** policy to a user but also forbid the user from deleting VPN connections. Create a custom policy for denying VPN connection deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on VPN except deleting VPN connections. The following is an example of a deny policy:

Copyright © Huawei Technologies Co., Ltd.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "vpn:vpnGateways:delete"
         ]
      }
   ]
}
```

- Example 3: defining multiple actions in a policy

  A custom policy can contain the actions of one or multiple services that are of the same type (global or project-level). The following is an example policy containing multiple actions.

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpn:vpnGateways:create",
            "vpn:vpnConnections:create",
            "vpn:customerGateways:create"
         ]
      },
      {
         "Effect": "Deny",
         "Action": [
            "vpn:vpnGateways:delete",
            "vpn:vpnConnections:delete",
            "vpn:customerGateways:create"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "vpc:vpcs:list",
            "vpc:subnets:get"
         ]
      }
   ]
}
```

3.6 Quotas

What Is a Quota?

Quotas put limits on the quantities and capacities of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

Resource Types

- VPN resources include VPN gateways, VPN connection groups, and customer gateways.

The total quota of each resource type varies according to regions.

 Copyright © Huawei Technologies Co., Ltd.

How Do I View My Quotas?

1. Log in to the management console.
2. Click  (the **My Quotas** icon) in the upper right corner.

   The **Service Quota** page is displayed.
3. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

Copyright © Huawei Technologies Co., Ltd.

4 Best Practice

4.1 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active-Active Mode)

4.1.1 Overview

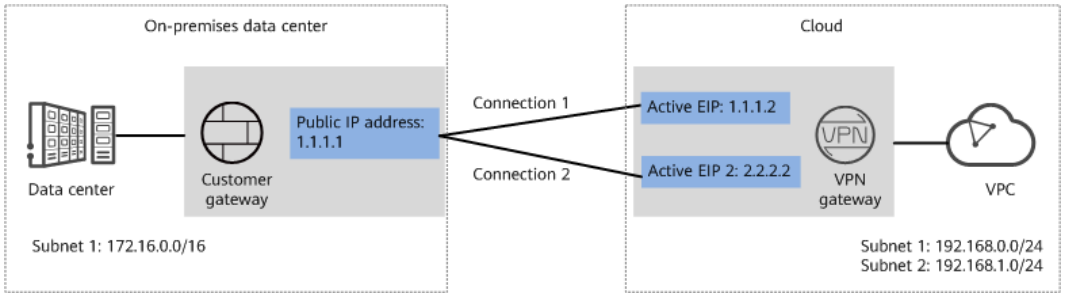
Scenario

VPN can be used to enable communication between an on-premises data center and ECSs in a VPC.

Networking

In this example, two VPN connections are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

Figure 4-1 Networking diagram



Solution Advantages

- A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.

 Copyright © Huawei Technologies Co., Ltd.

- Active-active VPN gateways can be deployed in different AZs to ensure AZ-level high availability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

4.1.2 Planning Networks and Resources

Data Plan

Table 4-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	• 192.168.0.0/24 • 192.168.1.0/24
VPN gateway	Interconnection subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	HA mode	Active-active
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2
VPN connection	Tunnel interface address	This address is used by a VPN gateway to establish an IPsec tunnel with a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • VPN connection 1: 169.254.70.1/30 • VPN connection 2: 169.254.71.1/30

Copyright © Huawei Technologies Co., Ltd.

705

Category	Item	Data
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: 1.1.1.1
	Tunnel interface address	• VPN connection 1: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	• Version: v2 • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 15 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group15 • Transfer protocol: ESP • Lifetime (s): 3600

4.1.3 Procedure

Prerequisites

- Cloud side
  - A VPC has been created. For details about how to create a VPC, see the *Virtual Private Cloud User Guide*.
  - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center.

 Copyright © Huawei Technologies Co., Ltd.

Procedure

VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy VPN Gateway**.
2. Set parameters as prompted.

   Table 4-2 only describes the key parameters for creating a VPN gateway.

Table 4-2 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**.	VPC
VPC	VPC to which the interconnection subnet belongs.	vpc-001(192.168.0.0/16)
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
Local Subnet	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active-active**.	Active-active
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	1.1.1.2

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure the customer gateway.

1. Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.
2. Set parameters as prompted.

   Table 4-3 only describes the key parameters for creating a customer gateway.

Table 4-3 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

Step 5 Configure VPN connections.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.
2. Set parameters for VPN connection 1 and click **Submit**.

   Table 4-4 only describes the key parameters for creating a VPN connection.

Table 4-4 Parameter settings for VPN connection 1

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-fw
VPN Type	Select **Static routing**.	Static routing

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

   NOTE

   For VPN connection 2, you are advised to use the same parameter settings as VPN connection 1, except the parameters listed in the following table.

Copyright © Huawei Technologies Co., Ltd.

Table 4-5 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device.

----End

Verification

- About 5 minutes later, check states of the VPN connections.

  Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the two VPN connections are both **Normal**.
- Verify that servers in the on-premises data center and ECSs in the VPC subnet can ping each other.

4.2 Connecting an On-premises Data Center to a VPC on the Cloud Through VPN (Active/Standby Mode)

4.2.1 Overview

Scenario

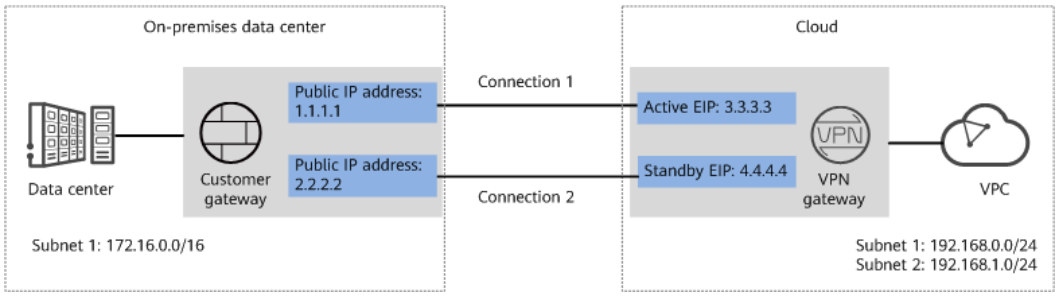
VPN can be used to enable communication between an on-premises data center and ECSs in a VPC.

Networking

In this example, two VPN connections working in active/standby mode are set up between an on-premises data center and a VPC to ensure network reliability. If one VPN connection fails, traffic is automatically switched to the other VPN connection, ensuring service continuity.

 Copyright © Huawei Technologies Co., Ltd.

Figure 4-2 Networking diagram



Solution Advantages

- A VPN gateway provides two IP addresses to establish dual independent VPN connections with a customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection.
- Active and standby VPN gateways can be deployed in different AZs to ensure AZ-level high availability.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

4.2.2 Planning Networks and Resources

Data Plan

Table 4-6 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	• 192.168.0.0/24 • 192.168.1.0/24
VPN gateway	Interconnection subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24

Copyright © Huawei Technologies Co., Ltd.

711

Category	Item	Data
	HA mode	Active/Standby
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 3.3.3.3 • Standby EIP: 4.4.4.4
VPN connection	Tunnel interface address	This address is used by a VPN gateway to establish an IPsec tunnel with a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • VPN connection 1: 169.254.70.1/30 • VPN connection 2: 169.254.71.1/30
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: • 1.1.1.1 • 2.2.2.2
	Tunnel interface address	• VPN connection 1: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30
IKE and IPsec policies	PSK	Test@123
	IKE policy	• Version: v2 • Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 15 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group15 • Transfer protocol: ESP • Lifetime (s): 3600

Copyright © Huawei Technologies Co., Ltd.

4.2.3 Procedure

Prerequisites

- Cloud side
  - A VPC has been created. For details about how to create a VPC, see the *Virtual Private Cloud User Guide*.
  - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.
- Data center side
  - IPsec has been configured on the VPN device in the on-premises data center.

Procedure

VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy VPN Gateway**.
2. Set parameters as prompted.

   Table 4-7 only describes the key parameters for creating a VPN gateway.

Table 4-7 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**.	VPC
VPC	VPC to which the interconnection subnet belongs.	vpc-001(192.168.0.0/16)
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
Local Subnet	This parameter is available only when **Associate With** is set to **VPC**. – Enter CIDR block Enter the subnet that needs to access the on-premises data center. The subnet can belong to the associated VPC or not. – Select subnet Select a subnet that belongs to the associated VPC and needs to access the on-premises data center.	192.168.0.0/24,192.168.1.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active/Standby**.	Active/Standby
Active EIP	Active EIP used by the VPN gateway to access the on-premises data center.	1.1.1.2
Standby EIP	Standby EIP used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 4 Configure the customer gateway.

1. Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.
2. Set parameters as prompted.

   Table 4-8 only describes the key parameters for creating a customer gateway.

Table 4-8 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw
Routing Mode	Select **Static**.	Static
Gateway IP Address	IP address used by the customer gateway to communicate with the VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

Step 5 Configure VPN connections.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.

Copyright © Huawei Technologies Co., Ltd.

2. Set parameters for VPN connection 1 and click **Submit**.
   Table 4-9 only describes the key parameters for creating a VPN connection.

   Table 4-9 Parameter settings for VPN connection 1

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-fw
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in the on-premises data center that needs to access the VPC. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

   NOTE

   For VPN connection 2, you are advised to use the same parameter settings as VPN connection 1, except the parameters listed in the following table.

   Table 4-10 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Standby EIP bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2

Step 6 Configure the customer gateway device.

The configuration procedures may vary according to the type of the customer gateway device.

----End

Verification

- About 5 minutes later, check states of the VPN connections.

  Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the two VPN connections are both **Available**.
- Verify that servers in the on-premises data center and ECSs in the VPC subnet can ping each other.

Copyright © Huawei Technologies Co., Ltd.

4.3 Connecting Multiple On-premises Branch Networks Through a VPN Hub

4.3.1 Overview

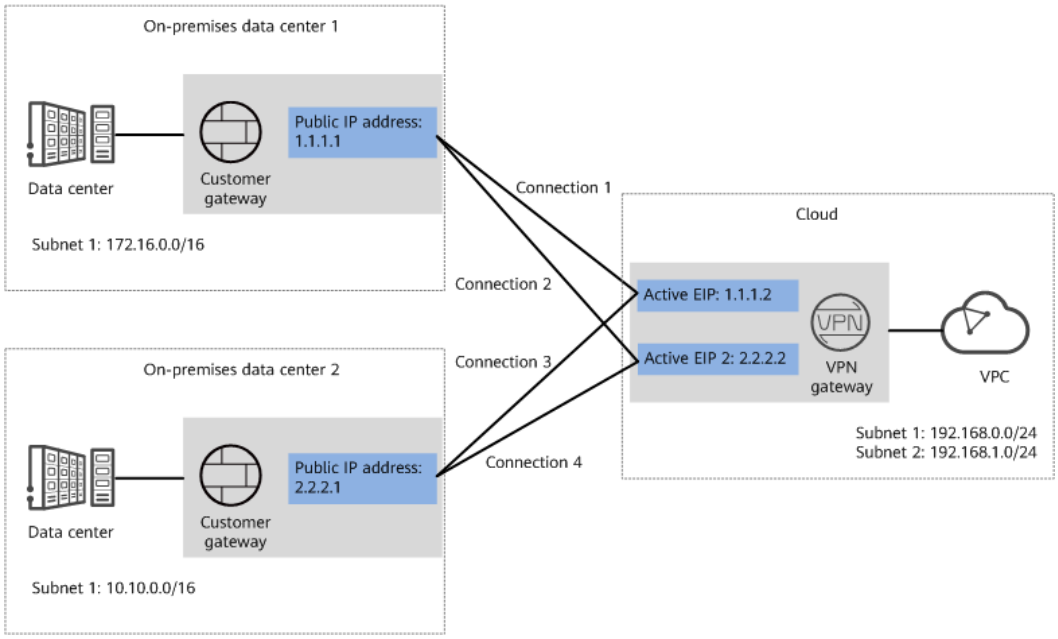
Scenario

To meet service requirements, enterprise A needs to implement communication between its two on-premises data centers.

Networking

Figure 4-3 shows the networking where the VPN service is used to connect the two on-premises data centers.

Figure 4-3 Networking diagram



Solution Advantages

- A VPN gateway on the cloud can function as a VPN hub to enable communication between on-premises branch sites. This eliminates the need to configure VPN connections between every two sites.
- A VPN gateway provides two IP addresses to establish dual independent VPN connections with each customer gateway. If one VPN connection fails, traffic can be quickly switched to the other VPN connection, ensuring reliability.

Copyright © Huawei Technologies Co., Ltd.

Limitations and Constraints

- The local and customer subnets of the VPN gateway cannot be the same. That is, the VPC subnet and the data center subnet to be interconnected cannot be the same.
- The IKE policy, IPsec policy, and PSK of the VPN gateway must be the same as those of the customer gateway.
- The local and remote interface address configurations on the VPN gateway and customer gateway are reversed.
- The security groups associated with ECSs in the VPC permit access from and to the on-premises data center.

4.3.2 Planning Networks and Resources

Data Plan

Table 4-11 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data centers	• 192.168.0.0/24 • 192.168.1.0/24
VPN gateway	Interconnection subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24
	HA Mode	Active-active
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: • Active EIP: 1.1.1.2 • Active EIP 2: 2.2.2.2

Copyright © Huawei Technologies Co., Ltd.

Category	Item	Data
VPN connection	Tunnel interface address	This address is used by a VPN gateway to establish an IPsec tunnel with a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. • VPN connections set up with on-premises data center 1 – VPN connection 1: 169.254.70.1/30 – VPN connection 2: 169.254.71.1/30 • VPN connections set up with on-premises data center 2 – VPN connection 3: 169.254.72.1/30 – VPN connection 4: 169.254.73.1/30
On-premises data center 1	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway in on-premises data center 1	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: 1.1.1.1
	Tunnel interface address	• VPN connection 1: 169.254.70.2/30 • VPN connection 2: 169.254.71.2/30
On-premises data center 2	Subnet that needs to access the VPC	10.10.0.0/16
Customer gateway in on-premises data center 2	Public IP address	This public IP address is assigned by a carrier. In this example, the public IP address is: 2.2.2.1
	Tunnel interface address	• VPN connection 3: 169.254.72.2/30 • VPN connection 4: 169.254.73.2/30
IKE and IPsec policies	PSK	Test@123

Copyright © Huawei Technologies Co., Ltd.

Category	Item	Data
	IKE policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • DH algorithm: Group 15 • Version: v2 • Lifetime (s): 86400 • Local ID: IP address • Peer ID: IP address
	IPsec policy	• Authentication algorithm: SHA2-256 • Encryption algorithm: AES-128 • PFS: DH Group15 • Transfer protocol: ESP • Lifetime (s): 3600

4.3.3 Procedure

Prerequisites

- Cloud side
  - A VPC has been created. For details about how to create a VPC, see the *Virtual Private Cloud User Guide*.
  - Security group rules have been configured for the VPC, and ECSs can communicate with other devices on the cloud. For details about how to configure security group rules, see the *Virtual Private Cloud User Guide*.
- Data center side
  - IPsec has been configured on the VPN devices in the two on-premises data centers.
  - The remote subnets of the VPN device in on-premises data center 1 must contain the local subnet of the VPC and the subnet to be interconnected in on-premises data center 2. The remote subnets of the VPN device in on-premises data center 2 must contain the local subnet of the VPC and the subnet to be interconnected in on-premises data center 1.

Procedure

VPNs support static routing mode, BGP routing mode, and policy-based mode. The following uses the static routing mode as an example.

Step 1 Configure a VPN gateway.

1. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy VPN Gateway**.
2. Set parameters as prompted.

   Table 4-12 only describes the key parameters for creating a VPN gateway.

 Copyright © Huawei Technologies Co., Ltd.

Table 4-12 Description of VPN gateway parameters

Parameter	Description	Value
Name	Name of a VPN gateway.	vpngw-001
Network Type	Select **Public network**.	Public network
Associate With	Select **VPC**.	VPC
VPC	VPC that the on-premises data centers need to access.	vpc-001(192.168.0.0/16)
Local Subnet	VPC subnets that the on-premises data centers need to access.	192.168.0.0/24,192.168.1.0/24
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
BGP ASN	BGP AS number.	64512
HA Mode	Select **Active-active**.	Active-active
Active EIP	EIP 1 used by the VPN gateway to access the on-premises data center.	1.1.1.2
Active EIP 2	EIP 2 used by the VPN gateway to access the on-premises data center.	2.2.2.2

Step 2 Configure customer gateways.

1. Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.
2. Set parameters as prompted.

   Table 4-13 only describes the key parameters for creating a customer gateway.

Table 4-13 Description of customer gateway parameters

Parameter	Description	Value
Name	Name of a customer gateway.	cgw-fw1
Routing Mode	Select **Static**.	Static

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
Gateway IP Address	IP address used by the customer gateway in on-premises data center 1 to communicate with the VPN gateway. Ensure that UDP port 4500 is permitted on the customer gateway device in the on-premises data center.	1.1.1.1

3. Repeat the preceding operations to configure the customer gateway (2.2.2.1) in on-premises data center 2.

Step 3 Configure VPN connections between the cloud side and on-premises data center 1.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.
2. Set parameters for VPN connection 1 and click **Submit**.

   Table 4-14 only describes the key parameters for creating a VPN connection.

Table 4-14 Description of VPN connection parameters

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-001
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
VPN Type	Select **Static routing**.	Static routing
Customer Gateway	Name of a customer gateway.	cgw-fw1
Customer Subnet	Subnet in on-premises data center 1 that needs to access the VPC. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	172.16.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.70.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.70.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device.	Test@123
Policy Settings	The policy settings must be the same as those on the customer gateway device.	Default

3. Create VPN connection 2.

   NOTE

   For VPN connection 2, you are advised to use the same parameter settings as VPN connection 1, except the parameters listed in the following table.

   Table 4-15 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-002
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.71.1
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway.	169.254.71.2

Step 4 Configure VPN connections between the cloud side and on-premises data center 2.

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.

 Copyright © Huawei Technologies Co., Ltd.

2. Set parameters for VPN connection 1 as prompted and click **Submit**.
   Table 4-16 only describes the key parameters for creating a VPN connection.

Table 4-16 Description of VPN connection parameters

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-003
VPN Gateway	VPN gateway for which the VPN connection is created.	vpngw-001
Gateway IP Address	Active EIP bound to the VPN gateway.	1.1.1.2
Customer Gateway	Name of a customer gateway.	cgw-fw2
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Subnet in on-premises data center 2 that needs to access the VPC. – A customer subnet cannot be included in any local subnet or any subnet of the VPC to which the VPN gateway is attached. – Reserved VPC CIDR blocks such as 100.64.0.0/10 and 214.0.0.0/8 cannot be used as customer subnets.	10.10.0.0/16
Interface IP Address Assignment	– Manually specify In this example, select **Manually specify**. – Automatically assign	Manually specify
Local Tunnel Interface Address	Tunnel interface IP address configured on the VPN gateway.	169.254.72.1
Customer Tunnel Interface Address	Tunnel interface IP address configured on the customer gateway device.	169.254.72.2
Link Detection	Whether to enable route reachability detection in multi-link scenarios. When NQA is enabled, ICMP packets are sent for detection and your device needs to respond to these ICMP packets.	**NQA** enabled

Copyright © Huawei Technologies Co., Ltd.

Parameter	Description	Value
PSK, Confirm PSK	The value must be the same as the PSK configured on the customer gateway device in on-premises data center 2.	Test@123
Policy Settings	The policy settings must be the same as those configured on the customer gateway device in on-premises data center 2.	Default

3. Create VPN connection 2.

   NOTE

   For VPN connection 2, you are advised to use the same parameter settings as VPN connection 1, except the parameters listed in the following table.

   Table 4-17 Parameter settings for VPN connection 2

Parameter	Description	Value
Name	Name of a VPN connection.	vpn-004
Gateway IP Address	Active EIP 2 bound to the VPN gateway.	2.2.2.2
Local Tunnel Interface Address	Tunnel IP address of the VPN gateway.	169.254.73.1
Customer Tunnel Interface Address	Tunnel IP address of the customer gateway in on-premises data center 2.	169.254.73.2

Step 5 Configure customer gateway devices in on-premises data centers 1 and 2.

The configuration procedures may vary according to the type of the customer gateway device.

----End

Verification

- About 5 minutes later, check states of the VPN connections.

  Choose **Virtual Private Network** > **Enterprise – VPN Connections**. The states of the four VPN connections are all **Normal**.
- Verify that servers in on-premises data center 1 and servers in on-premises data center 2 can ping each other.

Copyright © Huawei Technologies Co., Ltd.

4.4 Classic VPN

4.4.1 Connecting an On-Premises Data Center to a VPC Through a VPN

Scenarios

By default, ECSs in a VPC cannot communicate with devices in your on-premises data center or private network. To enable communication between them, you can configure VPN. After that, you need to configure security group rules and check subnet connectivity to ensure that the VPN is available. VPNs can be classified into the following two types:

- A site-to-site VPN functions as a communication tunnel between a VPC and a single on-premises data center.
- By contrast, a hub-and-spoke VPN is between a VPC and multiple on-premises data centers.

Pay attention to the following when you configure a VPN:

- The local and remote subnets cannot conflict.
- The IKE policies, IPsec policies, and PSKs configured on the cloud and in the on-premises data center must be the same.
- The parameters configured for the local and remote subnets and gateways must be symmetric.
- Security group rules permit access to and from the ECSs in the VPC.
- The status of a VPN changes to **Normal** only after ECSs and on-premises servers access each other.

Prerequisites

You have created the VPC and subnets that the on-premises data center wants to access.

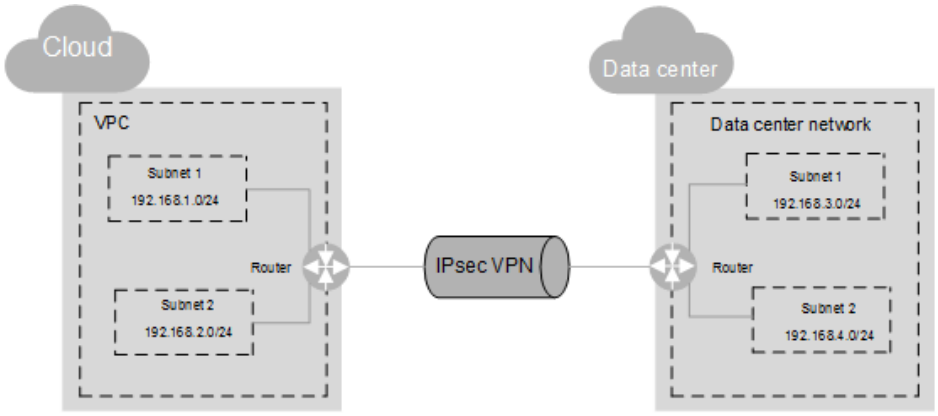
Procedure

1. On the management console, select the appropriate IKE and IPsec policies to create a VPN.
2. Check the IP address pools for the local and remote subnets.

   In **Figure 4-4**, the VPC has subnets 192.168.1.0/24 and 192.168.2.0/24. Your on-premises data center has subnets 192.168.3.0/24 and 192.168.4.0/24. You can set up a VPN to connect these subnets.

Copyright © Huawei Technologies Co., Ltd.

Figure 4-4 IPsec VPN



The IP address pools for the local subnets cannot overlap with those for the remote subnets. Like in this example, the IP address pool for the remote subnets cannot contain the two subnets of the VPC.

3. Configure security group rules for the ECSs to allow packets from and to the on-premises data center over the VPN.
4. Ping the ECSs from the on-premises data center to verify that the security group allows packets from and to the on-premises data center over the VPN.
5. Check the on-premises network configuration.

   A route must be configured for the on-premises network to enable traffic to be forwarded to network devices on the network over the VPN. If the data transmitted through the VPN cannot be forwarded to the network devices, check whether the remote LAN has rules configured to refuse the traffic.

 Copyright © Huawei Technologies Co., Ltd.

5 Troubleshooting

5.1 The State of a VPN Connection Is Not connected

Symptom

On the **Enterprise – VPN Connections** page of the VPN console, the state of a VPN connection is displayed as **Not connected**.

Possible Causes

- The configurations at the two ends of the VPN connection are incorrect.
- The security group configuration on the management console or the ACL configuration on the customer gateway device is incorrect.

Procedure

- Check the configurations at the two ends of the VPN connection.
  - Check whether the gateway IP addresses configured at the two ends of the VPN connection are reversed.
    - To check the active and standby EIPs of the VPN gateway, choose **Virtual Private Network** > **Enterprise – VPN Gateways** and view the IP addresses in the **Gateway IP Address** column.
    - To check the IP address of the customer gateway, choose **Virtual Private Network** > **Enterprise – Customer Gateways** and view the IP address in the **Gateway IP Address** column.
  - Check whether the IKE and IPsec policies at the two ends of the VPN connection are consistent.
    - To view the IKE and IPsec policy settings on the VPN console, choose **Virtual Private Network** > **Enterprise – VPN Connections**, locate the target VPN connection, and choose **More** > **Modify Policy Settings**.
  - Check whether the PSKs at the two ends of the VPN connection are the same.

 Copyright © Huawei Technologies Co., Ltd.

    - The PSK cannot be checked on the VPN console. If you are not sure whether the PSK configured on the VPN console is correct, you are advised to change it to be the same as that configured on the customer gateway device.

      To change the PSK on the VPN console, choose **Virtual Private Network** > **Enterprise – VPN Connections**, locate the target VPN connection, and choose **More** > **Reset PSK**.
  - If the policy-based mode is used, check whether the source and destination CIDR blocks in the policy rules at the two ends of the VPN connection are reversed.

    To check policy rules on the VPN console, choose **Virtual Private Network** > **Enterprise – VPN Connections**, locate the target VPN connection, and click **Modify VPN Connection**.
  - If the static routing mode is used and the NQA function is enabled on the VPN console, check whether tunnel interface IP addresses are correctly configured on the customer gateway device.

    - To check whether NQA is enabled on the VPN console, choose **Virtual Private Network** > **Enterprise – VPN Connections**, click the name of the target VPN connection, and view the value of **Link Detection** on the **Summary** tab page.
    - To check the tunnel interface IP addresses configured on the VPN console, choose **Virtual Private Network** > **Enterprise – VPN Connections**, click **Modify VPN Connection**, and view the values of **Local Interface IP Address** and **Customer Interface IP Address**. The local and remote interface IP addresses configured on the customer gateway device must be the same as the values of **Customer Interface IP Address** and **Local Interface IP Address** configured on the VPN console, respectively.
  - If the BGP routing mode is used, check whether the BGP ASNs at the two ends of the VPN connection are reversed.

    - To check the BGP ASN of the VPN gateway, choose **Virtual Private Network** > **Enterprise – VPN Gateways**, click the VPN gateway name, and view the BGP ASN in the **Basic Information** area.
    - To check the BGP ASN of the customer gateway, choose **Virtual Private Network** > **Enterprise – Customer Gateways** and view the value in the **BGP ASN** column.
- Check the security group configuration on the management console and the ACL configuration on the customer gateway device.
  - Check whether the default security group on the management console permits traffic of UDP ports 500 and 4500 originated from the public IP address of the customer gateway.

    To check the default security group on the management console, perform the following steps:

    i. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click the name of the VPC associated with the VPN gateway.

    ii. On the **Virtual Private Cloud** page, click the number in the **Route Tables** column.

 Copyright © Huawei Technologies Co., Ltd.

iii. On the **Route Tables** page, click the name of the route table.
iv. Locate and click the next hop of the active or standby EIP of the VPN gateway.
v. On the **Associated Security Groups** tab page, check whether the security group permits traffic of the ports.

- Verify that an ACL on the customer gateway device permits traffic of UDP ports 500 and 4500 originated from the active and standby EIPs of the VPN gateway.

5.2 Ping Tests Between Cloud and On-premises Networks Fail

Symptom

- Servers in an on-premises data center cannot ping ECSs in a VPC.
- ECSs in a VPC cannot ping the servers in an on-premises data center.

Possible Causes

- The security group configuration on the management console is incorrect.
- The ACL rule associated with the interconnection subnet is incorrectly configured.
- The ACL configuration on the customer gateway device is incorrect.
- The route configuration on the customer gateway device is incorrect.

Procedure

- Check the security group configuration on the management console.
  - Verify that the default security group on the management console permits data flows destined for the customer subnet.

    To check the default security group on the management console, perform the following steps:

    i. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click the name of the VPC associated with the VPN gateway.
    ii. Click the number of route tables corresponding to the VPC.
    iii. On the **Route Tables** page, click the name of the route table.
    iv. Locate and click the next hop of the active or standby EIP of the VPN gateway.
    v. On the **Associated Security Groups** tab page, check the ports permitted by the security group.
  - Verify that the default security group on the management console permits data flows originated from the customer subnet.
  - Verify that the default security group on the management console permits data flows destined for the local subnet.
  - Verify that the default security group on the management console permits data flows originated from the local subnet.

Copyright © Huawei Technologies Co., Ltd.

  - Verify that a security group permits data flows from the ECSs to the customer subnet.

    To check whether such a security group has been configured, choose **Compute** > **Elastic Cloud Server**, click an ECS name, click the **Security Groups** tab, and click **Manage Rule**.
  - Verify that a security group permits data flows from the customer subnet to the ECSs.
- The ACL rule associated with the interconnection subnet is incorrectly configured.
  - Check whether the ACL rule associated with the interconnection subnet permits the TCP port for traffic between all local and customer subnets.
    i. Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click the name of target VPN gateway.
    ii. In the **Basic Information** area, check and record the interconnection subnet.
    iii. In the **Basic Information** area, click the name of the associated VPC.
    iv. On the **Summary** tab page of the VPC, click the number of subnets in the **Networking Components** area.
    v. Find the interconnection subnet in the subnet list, and click the ACL name in the **Network ACL** column.
    vi. Permit the TCP port for traffic between all local and customer subnets.
- Check the ACL configuration on the customer gateway device.
  - Verify that an ACL rule on the customer gateway device permits data flows destined for the local subnet of the VPN gateway.
  - Verify that an ACL rule on the customer gateway device permits data flows originated from the local subnet of the VPN gateway.

  To check the local subnet of the VPN gateway, choose **Virtual Private Network** > **Enterprise – VPN Gateways**, click the VPN gateway name, and view the value of **Local Subnet** in the **Basic Information** area.
- Check the route configuration on the customer gateway device.
  - Verify that the public network route is correctly configured. That is, the destination address is an EIP of the VPN gateway, and the next hop is the egress interface address of the customer gateway device.
  - Verify that the private network route is correctly configured. That is, the destination address is the local subnet of the VPN gateway, and the next hop is the egress interface address of the customer gateway device.

    To check the local subnet of the VPN gateway, choose **Virtual Private Network** > **Enterprise – VPN Gateways**, click the VPN gateway name, and view the value of **Local Subnet** in the **Basic Information** area.

5.3 Packet Loss Occurs

Symptom

- Packet loss occurs when a server in an on-premises data center pings an ECS in a VPC.

 Copyright © Huawei Technologies Co., Ltd.

- Packet loss occurs when an ECS in a VPC pings a server in an on-premises data center.

Procedure

- Check the customer-side networking and bandwidth.
  - Check whether the customer network has multiple egresses working in load balancing mode and whether traffic destined for is distributed to a non-VPN egress. Ensure that the traffic destined for is transmitted through the same egress.
  - Ping the IP address of the VPN gateway and other public IP addresses (for example, 114.114.114.114) from the customer gateway to check the delay and packet loss rate on the public network.

    If the quality of the public network is poor, you are advised to seek help from the corresponding carrier.
  - Check whether traffic on the customer gateway device exceeds the bandwidth limit.
- Check the networking and bandwidth.
  - Check whether traffic exceeds the bandwidth of the VPN gateway.

    i. Check the bandwidth of active and standby EIPs of the VPN gateway as follows: Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, click the VPN gateway name, and check the value of **Bandwidth (Mbit/s)** in the **EIP** area.

    ii. Check the actual bandwidth usage of the VPN gateway as follows: Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click  in the **Public IP Address** column of the VPN gateway.

    If traffic exceeds the bandwidth of the VPN gateway, increase the bandwidth.

5.4 Classic VPN

5.4.1 Common Check Items

VPN connections or ping operations fail when configurations (such as the negotiation policy, firewall, route table, interzone policy, NAT configuration, and security group) are incorrect.

Check the following configurations.

- **Checking the Negotiation Information on Both Sides of a VPN Connection**
- **Checking the Firewall Configuration on Your Local Network and the Security Group Configuration on the Cloud**
- **Checking the Firewall Route Table**
- **Checking the Firewall Inter-zone Policy**
- **Checking the NAT Configurations on the Firewall**

Copyright © Huawei Technologies Co., Ltd.

Checking the Negotiation Information on Both Sides of a VPN Connection

- Ensure that the PSKs of the two sides are the same.
- Ensure the IKE policies and the IPsec policies of the two sides are the same.
- Local and remote subnets are matched pairs.

Checking the Firewall Configuration on Your Local Network and the Security Group Configuration on the Cloud

- Ensure that data packets from your network to the VPC subnet are permitted.
- Ensure that data packets from the VPC subnet to your network are permitted.

Checking the Firewall Route Table

Verify that there is a route to the VPC subnet.

- Ensure that a route table contains a route to the target network.
- Ensure that the forwarding table of the route works properly.

  NOTE

  Incorrect route configurations:

  1. The destination CIDR block is different from the VPC CIDR block. In this case, traffic cannot be routed to the public network interface configured with the IPsec policy.
  2. The outbound interface rather than the next hop is specified when configuring a static route.

     On an Ethernet network, the outbound interface cannot learn the ARP entries from the remote side, leading to route forwarding failure.
  3. The VPN gateway address is specified as the next hop of the route.

     Some third-party devices do not support automatic route recursion. VPN traffic is sent from the public network interface. Therefore, the next hop must be the gateway address provided by the carrier.

Checking the Firewall Inter-zone Policy

- From the Trust zone to the Untrust zone: Allows access from your local network to the VPC subnet on the cloud.
- From the Untrust zone to the Trust zone: Allows access from the VPC on the cloud to your local network.

Checking the NAT Configurations on the Firewall

Check whether the local VPN gateway is behind the NAT device (usually the border firewall). That is, the outbound interface of the VPN gateway uses a private IP address, and then it is translated into a public IP address by the NAT device.

This scenario is also called IPsec NAT traversal.

5.4.2 Common Configuration Issues and Solutions

- Inconsistent PSKs: PSK update takes effect in the next IKE negotiation. Ensure that the PSKs at both ends are the same.
- Inconsistent negotiation policies: Check the authentication algorithm, encryption algorithm, version, DH algorithm, and negotiation mode in the IKE

 Copyright © Huawei Technologies Co., Ltd.

733

policy, and the authentication algorithm, encryption algorithm, encapsulation format, and PFS algorithm in the IPsec policy. Ensure the PFSs at both ends are the same. By default, the PFS configuration is disabled on some devices.

- Interesting traffic: Check the ACL configurations at both ends. The actual IP address and mask must be used.
- NAT configuration: Do not perform NAT on the on-premises subnet that used to access the cloud.
- Security policies: Allow all protocols used by the on-premises subnet to access the cloud subnet, and allow two public IP addresses to communicate on UDP port 500 and UDP port 4500 using ESP or AH.
- Route configurations: Set the outbound interface for accessing the cloud subnet to the tunnel interface or IPsec negotiation interface. Ensure that the next-hop ARP resolution of the outbound interface is reachable.

 Copyright © Huawei Technologies Co., Ltd.

6 FAQs

6.1 Enterprise Edition VPN

6.1.1 What Are VPN Negotiation Parameters? What Are Their Default Values?

Table 6-1 VPN negotiation parameters

Protocol	Parameter	Value
IKE	Authentication Algorithm	• MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 (default value) • SHA2-384 • SHA2-512
	Encryption Algorithm	• 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) • AES-128 (default value) • AES-192 • AES-256 • AES-256-GCM-16

 Copyright © Huawei Technologies Co., Ltd.

Protocol	Parameter	Value
	DH Algorithm	• Group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 14 (This algorithm is insecure. Exercise caution when using this algorithm.) • Group 15 (default value) • Group 16 • Group 19 • Group 20 • Group 21
	Version	• v1 (not recommended due to security risks) • v2 (default value)
	Lifetime (s)	**86400** (default value) Unit: second Value range: **60** to **604800**
	Local ID	• IP Address The local IP address is automatically displayed as the EIP of the VPN gateway, removing the need to manually configure it. • FQDN By default, the local ID type is IP address and the local ID value is the EIP of the VPN gateway.
	Customer ID	• IP Address • FQDN By default, the customer ID type is IP address and the customer ID value is the public IP address of the customer gateway.

 Copyright © Huawei Technologies Co., Ltd.

Protocol	Parameter	Value
IPsec	Authentication Algorithm	• SHA1 (This algorithm is insecure. Exercise caution when using this algorithm.) • MD5 (This algorithm is insecure. Exercise caution when using this algorithm.) • SHA2-256 (default value) • SHA2-384 • SHA2-512
	Encryption Algorithm	• AES-128 (default value) • AES-192 • AES-256 • 3DES (This algorithm is insecure. Exercise caution when using this algorithm.) • AES-256-GCM-16
	PFS	• Disable (not recommended due to security risks) • DH group 1 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 2 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 5 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 14 (This algorithm is insecure. Exercise caution when using this algorithm.) • DH group 15 (default value) • DH group 16 • DH group 19 • DH group 20 • DH group 21
	Transfer Protocol	• ESP (default value)
	Lifetime (s)	**3600** (default value) Unit: second Value range: **30** to **604800**

 Copyright © Huawei Technologies Co., Ltd.

NOTE

- Perfect Forward Secrecy (PFS) is a security feature.

  IKE negotiation has two phases, phase one and phase two. The key of phase two (IPsec SA) is derived from the key generated in phase one. Once the key in phase one is disclosed, the security of the IPsec VPN may be adversely affected. To improve the key security, IKE provides PFS. When PFS is enabled, an additional DH exchange will be performed during IPsec SA negotiation to generate a new IPsec SA key, improving IPsec SA security.
- For security purposes, PFS is enabled on the cloud side by default. Ensure that PFS is also enabled on the gateway device in your on-premises data center and the PFS settings on both ends are the same. Otherwise, the negotiation will fail.
- The default traffic-based lifetime of an IPsec SA is 1,843,200 KB on the cloud side and cannot be changed for the VPN gateway. This parameter is not involved in negotiation and has no impact on the establishment of an IPsec SA.

6.1.2 Are a Username and Password Required for Creating an IPsec VPN Connection?

No. IPsec VPN uses a pre-shared key (PSK) for authentication. The PSK is configured on a VPN gateway, and a connection will be established after VPN negotiation is complete. Therefore, no username or password is required for creating an IPsec VPN connection. Generally, SSL, PPTP, and L2TP VPNs use usernames and passwords for authentication.

NOTE

IPsec XAUTH provides extended authentication for IPsec VPN. It requires users to enter their usernames and passwords during VPN negotiation.

Currently, VPN does not support IPsec XAUTH.

6.1.3 Is an IPsec VPN Connection Automatically Established?

Yes. An IPsec VPN connection is automatically established.

6.1.4 What VPN Resources Can Be Monitored?

VPN gateway

The following bandwidth information of a VPN gateway IP address can be monitored: inbound traffic, inbound bandwidth, outbound traffic, outbound bandwidth, and outbound bandwidth usage.

VPN connection

The following information about a VPN connection can be monitored: VPN connection status, average link round-trip time (RTT), maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate.

To monitor average link RTT, maximum link RTT, link packet loss rate, average tunnel RTT, maximum tunnel RTT, and tunnel packet loss rate, click the VPN connection name and click **Add** in the **Health Check** area on the **Summary** tab page to add health check items.

 Copyright © Huawei Technologies Co., Ltd.

6.1.5 What Do I Do If a VPN Connection Fails to Be Established?

1. Log in to the management console and choose **Virtual Private Network** > **Enterprise – VPN Connections**.
2. In the VPN connection list, locate the target VPN connection, and choose **More** > **Modify Policy Settings** on the right to view IKE and IPsec policies of the VPN connection.
3. Check the IKE and IPsec policies to see whether the negotiation modes and encryption algorithms at both ends of the VPN connection are the same.

   If the IKE SA has been set up in phase 1 but no IPsec SA has been established in phase 2, the IPsec policies at both ends of the VPN connection may be inconsistent.
4. Check whether the ACL configurations are correct.

   If the subnets of your on-premises data center are 192.168.3.0/24 and 192.168.4.0/24, and the VPC subnets are 192.168.1.0/24 and 192.168.2.0/24, configure the ACL rules for each on-premises subnet to allow communication with the VPC subnets. The following provides an example of ACL configurations:

   ```
   rule 1 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 2 permit ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   rule 3 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.1.0 0.0.0.255
   rule 4 permit ip source 192.168.4.0 0.0.0.255 destination 192.168.2.0 0.0.0.255
   ```
5. Ping the two ends of the VPN connection from each other to check whether the VPN connection is normal.

6.1.6 Can EIPs Be Used as VPN Gateway IP Addresses?

In Enterprise Edition VPN, EIPs can be used as VPN gateway IP addresses.

When creating a VPN gateway, you can bind EIPs as the gateway IP addresses.

6.1.7 What Are the Typical Scenarios of IPsec VPN?

A VPN is a point-to-point connection that implements private network access between two points.

- Applicable scenarios:
  - A VPN is created between different regions to enable cross-region VPC communications.
  - A VPN hub is used together with VPC peering connections and Cloud Connect connections to enable communications between an on-premises data center and multiple VPCs on the cloud.
  - A VPN is used together with source NAT to enable access to specific IP addresses across clouds.
- Not applicable scenarios:
  - A VPN cannot be used to connect VPCs in the same region. It is recommended that you use VPC peering connections to enable communications between VPCs in the same region.
  - A VPN cannot be used between the cloud and your home network that uses PPPoE dial-up.

Copyright © Huawei Technologies Co., Ltd.

- A VPN cannot be used between the cloud and 4G/5G routers.
- A VPN cannot be used between the cloud and your personal terminals.

6.1.8 What Are a VPC, a VPN Gateway, and a VPN Connection?

VPC enables you to create private, isolated virtual networks. You can use VPN to securely access ECSs in VPCs.

A VPN gateway is an egress gateway for a VPC. With a VPN gateway, you can create a secure, reliable, and encrypted connection between a VPC and an on-premises data center or between two VPCs in different regions.

A VPN connection is a secure and reliable IPsec encrypted communications tunnel established between a VPN gateway and the customer gateway in an on-premises data center.

To create a VPN on the cloud, perform the following operations:

1. Create a VPN gateway. You need to specify the VPC to be connected, as well as the bandwidth and EIPs of the VPN gateway.
2. Create a VPN connection. You need to specify the gateway EIP used to connect to the customer gateway, subnets, and negotiation policies.

6.1.9 How Do I Plan CIDR Blocks for Access to a VPC Through a VPN Connection?

- The CIDR blocks of a VPC cannot conflict with on-premises CIDR blocks.
- To avoid conflicts with cloud service addresses, do not use 127.0.0.0/8, 169.254.0.0/16, 224.0.0.0/3, or 100.64.0.0/10 for your on-premises network.

6.1.10 Which IKE Version Should I Select When I Create a VPN Connection?

IKEv2 is recommended because IKEv1 is not secure. In addition, IKEv2 outperforms IKEv1 in connection negotiation and establishment, authentication methods, dead peer detection (DPD) timeout processing, and security association (SA) timeout processing.

IKEv2 will be widely used, and IKEv1 will gradually phase out.

Introduction to IKEv1 and IKEv2

- As a hybrid protocol, IKEv1 brings some security and performance defects due to its complexity. As such, it has become a bottleneck in the IPsec system.
- IKEv2 addresses the issues of IKEv1 while retaining basic functions of IKEv1. IKEv2 is more simplified, efficient, secure, and robust than IKEv1. Additionally, IKEv2 is defined by RFC 4306 in a single document, whereas IKEv1 are defined in multiple documents. By minimizing core functions and default password algorithms, IKEv2 greatly improves interoperability between different IPsec VPNs.

 Copyright © Huawei Technologies Co., Ltd.

Security Risks of IKEv1

- The cryptographic algorithms supported by IKEv1 have not been updated for more than 10 years. In addition, IKEv1 does not support strong cryptographic algorithms such as AES-GCM and ChaCha20-Poly1305. For IKEv1, the E (Encryption) bit in the ISALMP header specifies that the payloads following the ISALMP header are encrypted, but any data integrity verification of those payloads is handled by a separate hash payload. This separation of encryption from data integrity protection prevents the use of authenticated encryption (AES-GCM) with IKEv1.
- IKEv1 is vulnerable to DoS amplification attacks and half-open connection attacks. After responding to spoofed packets, the responder maintains initiator-responder relationships, consuming a large number of system resources.

  This defect is inherent to IKEv1 and is addressed in IKEv2.
- The aggressive mode of IKEv1 is not secure. In this mode, information packets are not encrypted, posing risks of information leakage. There are also brute-force attacks targeting at the aggressive mode, such as man-in-the-middle attacks.

Differences Between IKEv1 and IKEv2

- **Negotiation process**
  - IKEv1 is complex and consumes a large amount of bandwidth. IKEv1 SA negotiation consists of two phases. In IKEv1 phase 1, an IKE SA is established in either main mode or aggressive mode. Main mode requires three exchanges between peers totaling six ISAKMP messages, whereas aggressive mode requires two exchanges totaling three ISAKMP messages. Aggressive mode is faster, but does not provide identity protection for peers as key exchange and identity authentication are performed simultaneously. In IKEv1 phase 2, IPsec SAs are established through three ISAKMP messages in quick mode.
  - Compared with IKEv1, IKEv2 simplifies the SA negotiation process. IKEv2 requires only two exchanges, totaling four messages, to establish an IKE SA and a pair of IPsec SAs. To create multiple pairs of IPsec SAs, only one additional exchange is needed for each additional pair of SAs.

    NOTE

    For IKEv1 negotiation, its main mode involves nine (6+3) messages, and its aggressive mode involves six (3+3) messages. In contrast, IKEv2 negotiation requires only four (2+2) messages.
- **Authentication methods**
  - Only IKEv1 (requiring an encryption card) supports digital envelope authentication (HSS-DE).
  - IKEv2 supports Extensible Authentication Protocol (EAP) authentication. IKEv2 can use an AAA server to remotely authenticate mobile and PC users and assign private IP addresses to these users. IKEv1 does not provide this function and must use L2TP to assign private IP addresses.
  - Only IKEv2 supports IKE SA integrity algorithms.
- **DPD timeout processing**

 Copyright © Huawei Technologies Co., Ltd.

  - Only IKEv1 supports the **retry-interval** parameter. If a device sends a DPD packet but receives no reply within the specified retry-interval, the device records a DPD failure event. When the number of DPD failure events reaches 5, both the IKE SA and IPsec SAs are deleted. IKE SA negotiation will start again only when there is traffic to be transmitted over the IPsec tunnel.
  - In IKEv2, the retransmission interval increases from 1, 2, 4, 8, 16, 32 to 64, in seconds. If no reply is received within eight consecutive transmissions, the peer end is considered dead, and the IKE SA and IPsec SAs are deleted.
- **IKE SA timeout processing and IPsec SA timeout processing**

  In IKEv2, the IKE SA soft lifetime is 9/10 of the IKE SA hard lifetime plus or minus a random number. This reduces the likelihood that two ends initiate renegotiation simultaneously. Therefore, you do not manually set the soft lifetime in IKEv2.

Advantages of IKEv2 over IKEv1

- Simplifies the SA negotiation process, improving efficiency.
- Fixes many cryptographic security vulnerabilities, improving security.
- Supports EAP authentication, improving authentication flexibility and scalability.

  EAP is an authentication protocol that supports multiple authentication methods. The biggest advantage of EAP is its scalability. That is, new authentication methods can be added without changing the original authentication system. EAP authentication has been widely used in dial-up access networks.
- Employs an Encrypted Payload on basis of ESP. This payload contains both an encryption algorithm and a data integrity algorithm. AES-GCM ensures confidentiality, integrity, and authentication, and works well with IKEv2.

6.1.11 Does a VPN Allow for Communications Between Two VPCs?

- If the two VPCs are in the same region, use a VPC peering connection to connect them.
- If the two VPCs are in different regions, use a VPN to connect them. The operations are as follows:
  a. Create a VPN gateway for each VPC, and create a VPN connection between the two VPN gateways.
  b. For the VPN connection, set the customer gateway to the EIP of the peer VPN gateway.
  c. For the VPN connection, set the customer subnet to the subnet of the peer VPC.
  d. Set the same pre-shared keys (PSKs) and algorithms for the two VPCs.

6.2 Classic VPN

 Copyright © Huawei Technologies Co., Ltd.

6.2.1 Will I Be Notified If a VPN Connection Is Interrupted?

The VPN connection status can be monitored. After a VPN connection is created, the VPN service reports the connection status information to Cloud Eye, but does not automatically send alarm notifications to you. To receive notifications, create alarm rules and enable **Alarm Notification** on the Cloud Eye console.

After a VPN connection is created, you can locate the row that contains the VPN connection and choose **Operation** > **View Metric** to view the VPN connection status.

6.2.2 What Are the Differences Between the Application Scenarios and Connection Modes of IPsec and SSL VPNs?

Scenarios

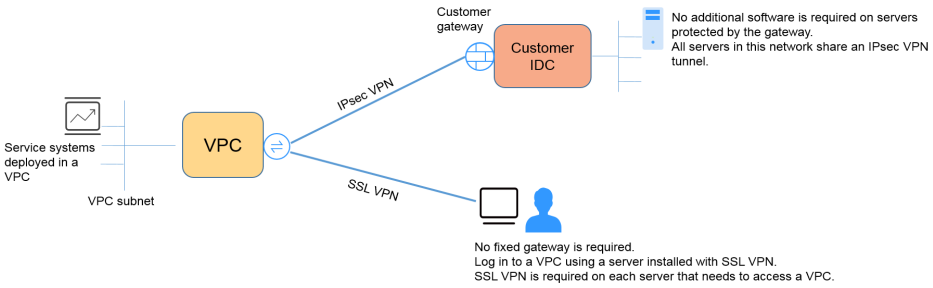
IPsec VPN connects two LANs, such as a branch and its headquarters (or a VPC), or an on-premises data center and a VPC.

SSL VPN connects a client to a LAN. For example, the portable computer of an employee on a business trip accesses the internal network of the company.

Connection Modes

IPsec VPN requires fixed gateways, such as firewalls or routers, at both ends. The administrator needs to configure gateways at both ends to complete IPsec VPN negotiation.

SSL VPN needs to install a specified client software on the server, then the server connects to the SSL device through the username and password.



NOTE

Currently, only IPsec VPN is supported; SSL VPN is not supported.

6.2.3 How Many VPN Connections Do I Need to Connect to Multiple On-premises Servers?

VPN uses the IPsec technology to connect your on-premises data center to a VPC on the cloud. As such, the number of VPN connections is related to the number of data centers where the servers to be connected to the cloud are located, but not to the number of servers.

 Copyright © Huawei Technologies Co., Ltd.

In most cases, one on-premises data center has one public gateway. All servers connect to the Internet through this gateway. Therefore, you only need to configure one VPN connection to allow communications between the VPC and your on-premises data center.

6.2.4 What Are the Impacts of a VPN on an On-premises Network? What Are the Changes to the Route for Accessing an ECS?

When you configure a VPN, perform the following operations on the on-premises gateway:

1. Configure IKE and IPsec policies.
2. Specify interesting traffic (ACL rules).
3. Check the route configuration on the gateway to ensure that traffic destined for a VPC can be routed to the correct outbound interface (interface having an IPsec policy bound).

After the VPN configuration is complete, only the traffic matching the ACL rules enters the VPN tunnel.

For example, before a VPN is created, on-premises users access the ECS through the EIP bound to the ECS. After a VPN is created, data flows matching the ACL rules access the private IP address of the ECS through the VPN tunnel.

6.2.5 Why Is Not Connected Displayed as the Status for a Successfully Created VPN Connection?

After a VPN connection is created, its status changes to **Normal** only after servers at both ends of the VPN connection communicate with each other.

- IKE v1:

  If no traffic goes through the VPN connection for a period of time, the VPN connection needs to be renegotiated. The negotiation time depends on the **Lifecycle (s)** value in the IPsec policy. Generally, **Lifecycle (s)** is set to **3600** (1 hour), indicating that the negotiation will be initiated in the fifty-fourth minute. If the negotiation succeeds, the connection remains to the next round of negotiation. If the negotiation fails, the VPN connection status changes to **Not Connected** within one hour. The connection can be restored only after the two ends of the VPN connection communicate with each other. The disconnection can be avoided by using a network monitoring tool, such as IP SLA, to generate packets.
- IKE v2: If no traffic goes through the VPN connection for a period of time, the VPN connection remains in the connected status.

6.2.6 Where Can I Add Routes on the VPN Console to Reach the Remote Subnets?

When a VPN connection is created, routes are automatically delivered to reach the remote subnets.

Copyright © Huawei Technologies Co., Ltd.

6.2.7 How Do I Replace a Direct Connect Connection with a VPN?

1. Ensure that the on-premises gateway supports IPsec VPN.
2. Create a VPN gateway and a VPN connection on the cloud. Select the VPC to which the Direct Connect connection uses for the VPN gateway.

NOTICE

When creating a VPN connection, configure its remote subnet as follows to avoid routing conflicts.

- Delete the virtual interface of the Direct Connect connection first and then configure the VPN connection.
- Divide the remote subnet into two subnets and configure the VPN connection. After the Direct Connect connection is deleted, configure the VPN connection again.

6.2.8 How Do I Access ECSs at Home When My Enterprise Network Has Been Connected to the Cloud Through a VPN?

A VPN connects a VPC on the cloud and an on-premises local area network (LAN).

The home network is not a part of the LAN of your enterprise and cannot be directly connected to the VPC on the cloud.

If your host at home needs to access VPC resources on the cloud, your host can directly access the EIP of the cloud service or connect to the LAN of your enterprise through SSL VPN (if your enterprise supports SSL access) and then access VPC resources on the cloud through the LAN.

6.2.9 How Do I Configure DPD for Interconnection with the Cloud?

By default, DPD is enabled on the cloud side and cannot be disabled.

Configure DPD as follows:

- DPD-type: on-demand
- DPD idle-time: 30s
- DPD retransmit-interval: 15s
- DPD retry-limit: 3
- DPD msg: seq-hash-notify

The **DPD msg** format at both ends of the VPN connection must be the same, but the DPD type, idle time, retransmission interval, and retry limit can be different.

Copyright © Huawei Technologies Co., Ltd.

6.2.10 What Is the VPN Quota?

What Is a Quota?

Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quota?

1. Log in to the management console.
2. Click  (the **My Quotas** icon) in the upper right corner.

   The **Service Quota** page is displayed.
3. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

Copyright © Huawei Technologies Co., Ltd.

A Change History

Released On	Description
2025-04-30	This issue is the third official release, which incorporates the following change: Added information about Enterprise Edition VPN.
2020-08-30	This issue is the second official release, which incorporates the following change: Added IKE and IPsec extended algorithms.
2018-08-15	This issue is the first official release.

Copyright © Huawei Technologies Co., Ltd.

REFERENCIAS TECNICAS

TRADUCCION SIMPLE

Virtual Private Network

Machine Translated by Google

Red privada virtual

Guía del usuario

Asunto	01
Fecha	30 de abril de 2025



HUAWEI TECHNOLOGIES CO., LTD.

Machine Translated by Google

Copyright © Huawei Technologies Co., Ltd. 2025. Todos los derechos reservados.

Ninguna parte de este documento puede ser reproducida o transmitida en ninguna forma ni por ningún medio sin el consentimiento previo por escrito de Huawei Technologies Co., Ltd.

Marcas comerciales y permisos



y otras marcas comerciales de Huawei son marcas comerciales de Huawei Technologies Co., Ltd.
Todas las demás marcas comerciales y nombres comerciales mencionados en este documento son propiedad de sus respectivos propietarios.

Aviso

Los productos, servicios y funciones adquiridos se estipulan en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, servicios y funciones descritos en este documento no estén incluidos en el alcance de la compra ni en el uso. Salvo que se especifique lo contrario en el contrato, todas las declaraciones, información y recomendaciones de este documento se proporcionan "tal cual", sin garantías ni representaciones de ningún tipo, ni expresas ni implícitas.

La información de este documento está sujeta a cambios sin previo aviso. Se ha hecho todo lo posible para garantizar la precisión de su contenido, pero las declaraciones, la información y las recomendaciones que contiene no constituyen garantía alguna, ni expresa ni implícita.

Machine Translated by Google

Declaración de seguridad

Vulnerabilidad

Las regulaciones de Huawei sobre la gestión de vulnerabilidades de productos están sujetas a los detalles sobre Proceso de Respuesta Vulnerable. Para este proceso, visite la siguiente página web:

https://www.huawei.com/en/psirt/vul-response-process

Para obtener información sobre vulnerabilidades, los clientes empresariales pueden visitar la siguiente página web:

https://securitybulletin.huawei.com/enterprise/es/advertencia-de-seguridad

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Contenido

1 Descripción general.....1
1.1 ¿Qué es una VPN?..... 1
1.2 Ventajas del producto.....1 1.3
Escenarios de aplicación.....2 1.4
Especificaciones del producto.....3 1.5
Cuotas y restricciones.....4
1.6 Normas y protocolos de referencia.....6
1.7 Diferencias entre Enterprise Edition VPN y Classic VPN.....7 1.8 Facturación
(Enterprise Edition VPN)..... 7 1.9 Facturación (Classic
VPN)..... 9 1.10
Seguridad..... 9 1.10.1
Tecnologías de protección de datos..... 9 1.11
Administración de permisos..... 12 1.12 Conceptos
básicos..... 15 1.12.1 VPN
IPsec..... 15
1.12.2 Ancho de banda de la puerta de enlace VPN..... 16
1.12.3 Subred local..... 16
1.12.4 Subred del cliente.....16

2 Primeros pasos..... 18 2.1 Configuración de la VPN de Enterprise
Edition para conectar un centro de datos local a una VPC..... 18
2.1.1 Descripción general.....18
2.1.2 Paso 1: Creación de una puerta de enlace VPN..... 21 2.1.3 Paso
2: Creación de una puerta de enlace de cliente..... 23 2.1.4 Paso 3:
Creación de una conexión VPN 1..... 23 2.1.5 Paso 4: Creación de una
conexión VPN 2..... 25 2.1.6 Paso 5: Configuración del dispositivo
de puerta de enlace de cliente..... 28 2.1.7 Paso 6: Verificación de la conectividad de
red..... 30
2.2 Proceso de creación de VPN..... 31
2.2.1 Comprar una puerta de enlace VPN..... 31 2.2.2
Comprar una conexión VPN..... 32

3 Administración..... 38 3.1 VPN S2C Enterprise
Edition..... 38

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

3.1.1 Administración de la puerta de enlace VPN de Enterprise Edition..... 38 3.1.2
Administración de la puerta de enlace del cliente de VPN de Enterprise Edition..... 49 3.1.3 Administración
de la conexión VPN de Enterprise Edition..... 53 3.2 VPN
clásica.....71
3.2.1 Administración de la puerta de enlace VPN clásica.....71 3.2.2
Administración de la conexión VPN clásica.....72 3.3
Monitoreo.....74 3.3.1 Métricas
(S2C Enterprise Edition VPN).....74 3.3.2 Visualización de
métricas.....77 3.3.3 Creación de reglas de
alarma.....78 3.4
Auditoría.....79
3.4.1 Operaciones de VPN que CTS puede registrar.....79 3.5
Administración de permisos.....80 3.5.1
Creación de un usuario y concesión de permisos de VPN.....80 3.5.2 Políticas
personalizadas de VPN..... 81
3.6 Cuotas..... 82
4 Mejores prácticas..... 84 4.1 Conexión de un centro de datos
local a una VPC en la nube a través de VPN (modo activo-
activo) 84
4.1.1 Descripción general.....84
4.1.2 Planificación de redes y recursos..... 85
4.1.3 Procedimiento..... 86
4.2 Conexión de un centro de datos local a una VPC en la nube a través de VPN (modo activo/en
espera) 90
4.2.1 Descripción general.....90
4.2.2 Planificación de redes y recursos..... 91 4.2.3
Procedimiento..... 93
4.3 Conexión de varias redes de sucursales locales a través de un concentrador VPN.....97
4.3.1 Descripción general.....97
4.3.2 Planificación de redes y recursos..... 98 4.3.3
Procedimiento..... 100
4.4 VPN clásica..... 106
4.4.1 Conexión de un centro de datos local a una VPC a través de una VPN.....106
5 Solución de problemas.....108
5.1 El estado de una conexión VPN es No conectado..... 108
5.2 Las pruebas de ping entre las redes en la nube y locales fallan.....110 5.3 Se
produce pérdida de paquetes.....111
5.4 VPN clásica..... 112
5.4.1 Elementos de verificación comunes..... 112
5.4.2 Problemas de configuración comunes y soluciones..... 113
6 Preguntas frecuentes..... 115 6.1 VPN Enterprise
Edition..... 115

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

6.1.1 ¿Qué son los parámetros de negociación de VPN? ¿Cuáles son sus valores predeterminados?.....115
6.1.2 ¿Se requiere un nombre de usuario y una contraseña para crear una conexión VPN IPsec?.....118 6.1.3 ¿Se establece automáticamente una conexión VPN IPsec?.....118 6.1.4 ¿Qué recursos VPN se pueden monitorizar?.....118
6.1.5 ¿Qué hago si no se puede establecer una conexión VPN?.....119
6.1.6 ¿Se pueden usar las EIP como direcciones IP de puerta de enlace de VPN?..... 119 6.1.7 ¿Cuáles son los escenarios típicos de VPN con IPsec?..... 119
6.1.8 ¿Qué son una VPC, una puerta de enlace de VPN y una conexión VPN?..... 120 6.1.9 ¿Cómo planifico bloques CIDR para el acceso a una VPC a través de una conexión VPN?..... 120 6.1.10 ¿Qué versión de IKE debo seleccionar al crear una conexión VPN?..... 120
6.1.11 ¿Permite una VPN la comunicación entre dos VPC?.....122
6.2 VPN clásica..... 122
6.2.1 ¿Recibiré una notificación si se interrumpe una conexión VPN?..... 123
6.2.2 ¿Cuáles son las diferencias entre los escenarios de aplicación y los modos de conexión de las VPN IPsec y SSL?.....123
6.2.3 ¿Cuántas conexiones VPN necesito para conectarme a varios servidores locales?..... 123 6.2.4 ¿Cuáles son los impactos de una VPN en una red local? ¿Qué cambios se producen en la ruta para acceder a un ECS?..... 124 6.2.5 ¿Por qué se muestra "No conectado" como estado para una conexión VPN creada correctamente?..... 124 6.2.6 ¿Dónde puedo agregar rutas en la consola VPN para acceder a las subredes remotas?..... 124
6.2.7 ¿Cómo reemplazo una conexión de Direct Connect con una VPN?.....125
6.2.8 ¿Cómo accedo a ECS en casa cuando mi red empresarial se ha conectado a la nube a través de una VPN?..... 125 6.2.9 ¿Cómo configuro DPD para la interconexión con la nube?.....125 6.2.10 ¿Qué es la cuota de VPN?.....126
Un historial de cambios.....127

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

1 Descripción general

1.1 ¿Qué es VPN?

Descripción general

La red privada virtual (VPN) establece conexiones cifradas seguras, confiables y rentables entre su red local o centro de datos y una red virtual en la nube.

NO TE

VPN solo admite conexiones que no sean transfronterizas.

- Una puerta de enlace VPN proporciona una salida de Internet para que una nube privada virtual (VPC) se conecte a una puerta de enlace de cliente en su centro de datos local.

Una conexión VPN conecta una puerta de enlace VPN con una puerta de enlace de cliente mediante túneles cifrados, lo que permite la comunicación entre una VPC y su centro de datos local. Esto ayuda a establecer rápidamente un entorno de nube híbrida seguro.

Componentes

- Puerta de enlace VPN: una puerta de enlace virtual de VPN en la nube. Establece una conexión segura. Conexiones privadas con una puerta de enlace de clientes en su red local o centro de datos.

Puerta de enlace del cliente: un recurso que proporciona información a la nube sobre su dispositivo de puerta de enlace del cliente. Puede ser un dispositivo físico o una aplicación de software en su centro de datos local.

Conexión VPN: un canal seguro entre una puerta de enlace VPN y una puerta de enlace de cliente. Las conexiones VPN utilizan los protocolos de Intercambio de Claves de Internet (IKE) e IPsec para cifrar los datos transmitidos.

1.2 Ventajas del producto

VPN tiene las siguientes ventajas:

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

• Alta seguridad : los

datos se cifran mediante IKE/IPsec, lo que garantiza una alta seguridad de los datos.

– Una puerta de enlace VPN es exclusiva para un inquilino, lo que aísla a los inquilinos entre sí.
otro.

• Alta disponibilidad

Una puerta de enlace VPN proporciona dos direcciones IP para establecer conexiones VPN duales e
independientes con una puerta de enlace de cliente. Si una conexión VPN falla, el tráfico se
puede transferir rápidamente a la otra conexión VPN.

– Las puertas de enlace activo-activo se implementan en diferentes zonas de disponibilidad (AZ) para
garantizar una alta disponibilidad a nivel de AZ.

Modo activo/en espera: Normalmente, una puerta de enlace VPN se comunica con una puerta
de enlace de cliente a través de la conexión activa. Si esta falla, el tráfico se redirige
automáticamente a la conexión VPN en espera. Una vez solucionado el fallo, el tráfico
se redirige de nuevo a la conexión VPN activa.

• Rentabilidad

– Las conexiones IPsec a través de Internet ofrecen una alternativa rentable a Direct Connect.

– Una puerta de enlace VPN se puede vincular a direcciones IP elásticas (EIP) que comparten
ancho de banda, reduciendo los costos de ancho de banda.

– El ancho de banda se puede ajustar cuando se crea una instancia EIP.

• Fácil de usar : una

puerta de enlace VPN admite múltiples modos de conexión, incluidos enrutamiento basado en
políticas, enrutamiento estático y enrutamiento BGP, para satisfacer los diferentes
requisitos de acceso de las puertas de enlace de los clientes.

– Una puerta de enlace VPN en la nube puede funcionar como un concentrador VPN, lo que
permite que las sucursales locales accedan entre sí.

– Se puede crear una conexión VPN en unos pocos y sencillos pasos en la VPN
dispositivo en un centro de datos local y en la consola VPN, y está listo para usarse
inmediatamente después de su creación.

– Se admiten puertas de enlace VPN privadas para cifrar el tráfico transmitido a través de conexiones
Direct Connect, lo que mejora la seguridad de la transmisión de datos.

1.3 Escenarios de aplicación

Implementación de nube híbrida

Puede utilizar una VPN para conectar su centro de datos local a una VPC y utilizar las capacidades de escalamiento elástico y rápido de la nube para expandir las capacidades informáticas de las aplicaciones. muestra la implementación de la nube híbrida.

Conexión entre regiones entre VPC

Con las VPN, puede conectar VPC en diferentes regiones para habilitar la conectividad entre los servicios de usuario en estas regiones, como se muestra en .

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Interconexión de sucursales empresariales

Una puerta de enlace VPN funciona como un concentrador VPN para conectar sucursales empresariales, como se muestra en . Esto elimina la necesidad de configurar conexiones VPN entre cada dos sucursales.

1.4 Especificaciones del producto

NO TE

- La especificación de una puerta de enlace VPN se puede cambiar entre Professional 1 y Profesional 2.

Tabla 1-1 Especificaciones de VPN

Artículo	Profesional 1	Profesional 2
Puerta de enlace exclusiva recursos	Apoyado	Apoyado
Conexiones duales	Apoyado	Apoyado
Pasarelas activas-activas compatibles		Apoyado
Activo/En espera puertas de enlace	Apoyado	Apoyado
Modo basado en políticas	Apoyado	Apoyado
Modo de enrutamiento: estático enrutamiento	Apoyado	Apoyado
Modo de enrutamiento: BGP enrutamiento	Apoyado	Apoyado
Modo de plantilla de política No compatible		No compatible
Reenvío máximo ancho de banda	300 Mbit/s	1 Gbit/s
Número máximo de Grupos de conexión VPN	100	100
Red privada	Apoyado	Apoyado
Regiones compatibles	Sujeto a las regiones disponible en la consola	Sujeto a las regiones disponible en la consola

 Derechos de autor © Huawei Technologies Co., Ltd.

757

Machine Translated by Google

1.5 Cuotas y restricciones

Puerta de enlace VPN

Tabla 1-2 Restricciones en las puertas de enlace VPN

Tipo de VPN	Recurso	Cuota predeterminada
Empresa Edición VPN	Puertas de enlace VPN por inquilino en cada región	50 • Si solo tiene una VPC, puede crear un máximo de 50 puertas de enlace VPN para la VPC. • Si tiene varias VPC, puede crear un máximo de 50 puertas de enlace VPN para todas estas VPC.
	Grupos de conexiones VPN por puerta de enlace VPN	100
	Subredes locales por puerta de enlace VPN	50
	Número de rutas BGP que una puerta de enlace VPN puede recibir desde una puerta de enlace de cliente a través de una conexión	100
VPN clásica	Puertas de enlace VPN por inquilino en cada región	2 Solo se puede crear una puerta de enlace VPN para una VPC.

• De forma predeterminada, la longitud máxima de los paquetes TCP admitidos por una puerta de enlace VPN Son 1300 bytes.

Portal del cliente

Tabla 1-3 Restricciones en las pasarelas de clientes

Tipo de VPN	Recurso	Cuota predeterminada
Empresa Edición VPN	Puertas de enlace de clientes por inquilino en cada región	100

• Habilite la travesía NAT en la puerta de enlace del cliente en función de la red.

– Si la puerta de enlace del cliente está conectada a Internet a través de un dispositivo NAT, habilite la travesía NAT en la puerta de enlace del cliente.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

– Si la puerta de enlace del cliente está conectada directamente a Internet, no es necesario habilitar NAT traversal en ella. • La detección de pares inactivos (DPD) debe estar

habilitada en la puerta de enlace del cliente. • La puerta de enlace del cliente debe ser

compatible con interfaces de túnel IPsec y estar configurada con la política de seguridad correspondiente. • Cuando el análisis de calidad de red (NQA)

está habilitado para una conexión en modo estático
En el modo de enrutamiento, la interfaz de túnel IPsec de una puerta de enlace de cliente debe tener una dirección IP y poder responder a solicitudes ICMP.

• Se recomienda que el tamaño máximo de segmento (MSS) de los paquetes TCP se establezca en un valor inferior a 1399 en una puerta de enlace de cliente, a fin de evitar la fragmentación causada por la adición de un encabezado IPsec.

Conexión VPN

Tabla 1-4 Restricciones en las conexiones VPN

VPN Tipo	Recurso	Cuota predeterminada: cómo aumentarla Cuota
Edición empresarial VPN	Reglas de política por conexión VPN	5
	Subredes de clientes por conexión VPN	50
Clásico VPN	Conexiones VPN por inquilino en cada región	12

En escenarios con múltiples subredes, se recomienda usar conexiones VPN en modo de enrutamiento. Para una conexión VPN en modo basado en políticas o de plantilla de políticas, una puerta de enlace VPN crea un túnel de comunicaciones para cada par de subredes local y de cliente de forma predeterminada. Si existen varias subredes locales o de cliente para una conexión VPN en modo basado en políticas o de plantilla de políticas, se crean varios túneles de comunicaciones.

Cada dirección IP de una puerta de enlace VPN admite un máximo de 100 túneles de comunicaciones para conectarse a puertas de enlace de clientes.

– En el modo de enrutamiento, cada conexión VPN ocupa solo una túnel de comunicaciones de la dirección IP de la puerta de enlace VPN correspondiente.

– En el modo basado en políticas o en plantilla de políticas, cada conexión VPN ocupa túneles de comunicaciones de la dirección IP de la puerta de enlace VPN correspondiente. indica la cantidad de subredes locales e indica la cantidad de subredes de clientes.

Si el número de túneles de comunicaciones ocupados por todas las conexiones VPN en diferentes modos establecidos por una única dirección IP de puerta de enlace ha llegado a 100, no se podrán crear conexiones VPN adicionales.

Al crear una conexión VPN en modo basado en políticas y agregar varias reglas de política, asegúrese de que los bloques CIDR de origen y destino de las diferentes reglas no se superpongan. De lo contrario, los flujos de datos podrían coincidir incorrectamente o los túneles IPsec podrían fallar.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

1.6 Normas y protocolos de referencia

Los siguientes estándares y protocolos están asociados con VPN:

• RFC 2403: El uso de HMAC-MD5-96 en ESP y AH

• RFC 2404: El uso de HMAC-SHA-1-96 en ESP y AH

• RFC 2409: El intercambio de claves de Internet (IKE) • RFC

2451: Los algoritmos de cifrado de modo CBC ESP • RFC 3526:

Grupos Diffie-Hellman exponenciales más modulares (MODP) para
Intercambio de claves de Internet

(IKE) • RFC 3566: El algoritmo AES-XCBC-MAC-96 y su uso con IPsec • RFC 3602: El algoritmo

de cifrado AES-CBC y su uso con IPsec • RFC 3664: El algoritmo AES-XCBC-PRF-128

para el intercambio de claves de Internet
Protocolo (IKE)

• RFC 4106: El uso del modo Galois/Contador (GCM) en la encapsulación de IPsec
Carga útil de seguridad (ESP)

• RFC 4109: Algoritmos para el intercambio de claves de Internet versión 1 (IKEv1) • RFC

4434: El algoritmo AES-XCBC-PRF-128 para el intercambio de claves de Internet
Protocolo (IKE)

• RFC 4868: Uso de HMAC-SHA-256, HMAC-SHA-384 y HMAC-SHA-512 con
IPsec

• RFC 4301: Arquitectura de seguridad para el protocolo de Internet • RFC 4302:

Encabezado de autenticación IP

• RFC 4303: Carga útil de seguridad encapsulada IP (ESP) • RFC 4305:

Requisitos de implementación de algoritmos criptográficos para
Encapsulamiento de carga útil de seguridad (ESP) y encabezado de autenticación (AH) • RFC

4306: Protocolo de intercambio de claves de Internet (IKEv2) • RFC

4307: Algoritmos criptográficos para su uso en el intercambio de claves de Internet
Versión 2 (IKEv2) •

RFC 4308: Suites criptográficas para IPsec • RFC 5282:

Uso de algoritmos de cifrado autenticados con el protocolo cifrado
Carga útil del protocolo de intercambio de claves de Internet versión 2 (IKEv2)

• RFC 6989: Pruebas Diffie-Hellman adicionales para el intercambio de claves de Internet
Protocolo versión 2 (IKEv2)

• RFC 7296: Protocolo de intercambio de claves de Internet versión 2 (IKEv2) • RFC

7321: Requisitos y uso de implementación de algoritmos criptográficos
Guía para encapsular la carga útil de seguridad (ESP) y el encabezado de autenticación
(AH)

• RFC 8247: Requisitos de implementación de algoritmos y guía de uso para
el Protocolo de intercambio de claves de Internet versión 2 (IKEv2)

• RFC 3947: Negociación de NAT-Traversal en IKE • RFC 3948:

Encapsulación UDP de paquetes ESP IPsec • RFC 3706: Un método

basado en el tráfico para detectar el intercambio de claves de Internet inactivo
(IKE) Pares

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

• RFC 4271: Protocolo de puerta de enlace fronteriza 4 (BGP-4)

1.7 Diferencias entre Enterprise Edition VPN y VPN clásica

Tabla 1-5 Diferencias entre la VPN Enterprise Edition y la VPN clásica

Categoría	Artículo	Edición empresarial VPN	VPN clásica
Arrendatario aislamiento	Exclusivo para inquilinos puerta	Apoyado	No compatible
Características	Modo basado en políticas compatible		Apoyado
	Modo de enrutamiento	Enrutamiento estático y Enrutamiento BGP	No compatible
	Centro de VPN	Apoyado	No compatible
	Enrutador empresarial	No compatible	No compatible
	Tipo de red	Red pública y red privada	Red pública
Capacidad	Número de subredes • Basado en ruta modo: 50 • Basado en políticas modo: 5		Basado en políticas modo: 5
	Para obtener más información, consulte la Tabla 1-1.		
Fiabilidad	Protección de puerta de enlace modo	Activo/En espera o activo-activo	-
	Puerta de enlace entre zonas horarias despliegue	Apoyado	No compatible
	VPN activo-activo conexiones	Apoyado	No compatible
	Copia de seguridad con Direct Conectar	Apoyado	No compatible

1.8 Facturación (VPN Enterprise Edition)

NO TE

A menos que se especifique lo contrario, la VPN mencionada en esta sección se refiere a la VPN Enterprise Edition.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Artículos de facturación

Tabla 1-6 Elementos de facturación de VPN

Facturación Modo	Artículo de facturación 1	Artículo de facturación 2	Fórmula de facturación
Pago por usar	Instancia VPN (facturada por hora)	Ancho de banda EIP	Tarifa de instancia VPN + tarifa de ancho de banda EIP
Pago por usar	Instancia VPN (facturada por hora)	Tráfico EIP	Tarifa de instancia VPN + tarifa de tráfico EIP

El precio total de la VPN consta de las siguientes partes:

Tarifa de instancia VPN: indica la tarifa que se cobra por el uso de una única puerta de enlace VPN y la conexión entre esta y la puerta de enlace de un cliente. Una puerta de enlace VPN está dedicada a un inquilino, lo que garantiza su rendimiento de reenvío.

• Tarifa de ancho de banda EIP: indica la tarifa que se cobra por el ancho de banda consumido por los EIP vinculados a una puerta de enlace VPN.

Por defecto, una puerta de enlace VPN activa-activa tiene dos EIP. Es necesario adquirir ancho de banda para cada EIP.

– Si utiliza EIP existentes como EIP de una puerta de enlace VPN, no se le cobrará nuevamente por estos EIP.

Para obtener más detalles, consulte Detalles de precios de EIP.

Modos de facturación

Pago por uso

Las instancias de VPN se facturan por duración de uso y el ciclo de facturación es de una hora. El ancho de banda de EIP se puede facturar por ancho de banda o por tráfico.

• Facturado por ancho de banda

– Fórmula de facturación: Precio total = tarifa de instancia de VPN + tarifa de ancho de banda de EIP El ancho de banda de EIP se refiere al ancho de banda de salida, es decir, el ancho de banda para el tráfico enviado desde una VPC en la nube a una puerta de enlace de cliente en un centro de datos local.

i. Si el ancho de banda adquirido es de 10 Mbit/s o menos, el ancho de banda entrante está limitado a 10 Mbit/s.

ii. Si el ancho de banda adquirido es superior a 10 Mbit/s, el ancho de banda de entrada es el mismo que el ancho de banda adquirido.

Por ejemplo, suponiendo que el ancho de banda que compró es de 50 Mbit/s y utiliza la puerta de enlace VPN durante 5 horas y luego la elimina, se le cobrará por el uso del ancho de banda de 50 Mbit/s durante 5 horas incluso si no transmite ningún dato durante las 5 horas.

• Facturación por tráfico Si selecciona la facturación por tráfico, se le cobrará por el tráfico generado en cada hora, siendo la unidad de facturación 1 GB. Si se genera menos de 1 GB, la

 Derechos de autor © Huawei Technologies Co., Ltd.

762

Machine Translated by Google

La tarifa se calcula en función del volumen de tráfico generado. En este caso, modificar el ancho de banda no modifica el precio por GB del tráfico de la red pública. Solo se factura el tráfico de salida.

– Fórmula de facturación: Precio total = tarifa de instancia VPN + tarifa de tráfico EIP

1.9 Facturación (VPN clásica)

La VPN clásica admite el pago por uso (por hora). Paga solo por lo que usa, mientras lo necesite. No requiere previsiones ni presupuestos complejos. Puede comprar una o más conexiones VPN y se le facturará según la cantidad de conexiones VPN creadas y la duración del uso.

NO TE

A menos que se especifique lo contrario, VPN en esta sección se refiere a VPN clásica.

Artículos de facturación

Tabla 1-7 Elementos de facturación de las VPN clásicas

Facturación Modo	Artículo de facturación 1	Artículo de facturación 2	Fórmula de facturación
Pago por usar	Tráfico de red pública	Conexión VPN	Precio total = Tarifa de tráfico de red pública + Tarifa de conexión VPN

Modos de facturación

Pago por uso •

Facturación por tráfico : Si

selecciona la facturación por tráfico, se le cobrará por el tráfico generado cada hora, con una unidad de facturación de 1 GB. Si se genera menos de 1 GB, la tarifa se calcula en función del volumen de tráfico generado.

Precio total = Tarifa de tráfico de red pública + Tarifa de conexión VPN

1.10 Seguridad

1.10.1 Tecnologías de protección de datos

• La VPN S2C es una tecnología de tunelización que proporciona seguridad en la capa IP mediante el conjunto de protocolos IKE/IPsec. Garantiza la confidencialidad e integridad de los paquetes de datos IP y evita que sean interceptados, divulgados o manipulados en redes inseguras (como Internet).

• Al crear una conexión VPN S2C, puede configurar el cifrado de datos y algoritmos de autenticación en una política.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

La Tabla 1-8 enumera los algoritmos recomendados para VPN S2C en orden descendente de seguridad.

Tabla 1-8 Parámetros para configurar políticas de VPN S2C

Parámetro		Descripción
FUERZA Política	Versión	• versión 2 • v1 (IKEv1 tiene baja seguridad. Si el dispositivo admite IKEv2, se recomienda IKEv2). El valor predeterminado es v2.
	Autenticación Algoritmo	Algoritmo hash utilizado para la autenticación. Se admiten los siguientes algoritmos: • SHA2-512 • SHA2-384 • SHA2-256 • MD5 (Inseguro. No recomendado). • SHA1 (Inseguro. No recomendado). De forma predeterminada, se utiliza el algoritmo SHA2-256.
	Algoritmo de cifrado	Se admiten los siguientes algoritmos de cifrado: • AES-256-GCM-16 (compatible solo con Enterprise Edition VPN) • AES-128-GCM-16 (compatible solo con Enterprise Edition VPN) • AES-256 (inseguro. No recomendado). • AES-192 (Inseguro. No recomendado). • AES-128 (Inseguro. No recomendado). • 3DES (Inseguro. No recomendado.) De forma predeterminada, se utiliza el algoritmo AES-128.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro		Descripción
	Algoritmo DH	Se admiten los siguientes algoritmos: • Grupo 21 • Grupo 20 • Grupo 19 • Grupo 16 • Grupo 15 • Grupo 14 (inseguro. No recomendado). • Grupo 5 (inseguro. No recomendado). • Grupo 2 (inseguro. No recomendado). • Grupo 1 (inseguro. No recomendado). De forma predeterminada, se utiliza el grupo 15.
IPsec Política	Autenticación Algoritmo	Algoritmo hash utilizado para la autenticación. Se admiten los siguientes algoritmos: • SHA2-512 • SHA2-384 • SHA2-256 • MD5 (Inseguro. No recomendado). • SHA1 (Inseguro. No recomendado). De forma predeterminada, se utiliza el algoritmo SHA2-256.
	Algoritmo de cifrado	Se admiten los siguientes algoritmos de cifrado: • AES-256-GCM-16 • AES-128-GCM-16 • AES-256 (inseguro. No recomendado). • AES-192 (Inseguro. No recomendado). • AES-128 (Inseguro. No recomendado). • 3DES (Inseguro. No recomendado.) De forma predeterminada, se utiliza el algoritmo AES-128.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

PFS

La confidencialidad directa perfecta (PFS) garantiza que la vulneración de las claves de un túnel IPsec no afecte la seguridad de otros túneles, aprovechando que las claves de estos túneles son irrelevantes entre sí. Por defecto, la función PFS está habilitada para VPN S2C.

Cada conexión VPN IPsec consta de al menos un túnel IPsec, cada uno de los cuales utiliza un conjunto independiente de claves para proteger el tráfico del usuario.

S2C VPN admite los siguientes algoritmos:

• Grupo DH 1 (este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 2 (este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 5 (este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 14 • Grupo DH 15 • Grupo DH 16 • Grupo DH 19 • Grupo DH 20 • Grupo DH 21

Anti-repetición

La tecnología anti-repetición utiliza números de secuencia para proteger los paquetes cifrados IPsec contra ataques de repetición, que se inician mediante el envío repetido de paquetes de datos interceptados.
De forma predeterminada, la función anti-reproducción está habilitada para el servicio VPN.

Aislamiento de recursos

Una puerta de enlace VPN es exclusiva de un inquilino. Por lo tanto, los inquilinos están aislados entre sí, lo que garantiza la seguridad de sus datos.

1.11 Gestión de permisos

Si necesita asignar diferentes permisos al personal de su empresa para acceder a sus recursos VPN en la plataforma de servicios en la nube, Identity and Access Management (IAM) es una buena opción para una gestión de permisos detallada.
IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a administrar de forma segura el acceso a sus recursos.

Con IAM, puede usar su cuenta para crear usuarios de IAM y asignarles permisos para controlar su acceso a recursos específicos de la nube. Por ejemplo, algunos desarrolladores de software de su empresa necesitan usar recursos VPN, pero no deberían poder eliminarlos ni realizar operaciones de alto riesgo. En este caso, puede crear usuarios de IAM para los desarrolladores de software y otorgarles solo los permisos necesarios para usar recursos VPN.

Si su cuenta no necesita usuarios IAM individuales para la administración de permisos, omita esta sección, que no tiene impacto en el uso de las funciones de VPN.

IAM es un servicio gratuito. Solo pagas por los recursos de tu cuenta.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Para obtener más información sobre IAM, consulte Descripción general del servicio IAM.

Permisos de VPN

Los nuevos usuarios de IAM no tienen permisos asignados de forma predeterminada. Primero debe agregarlos a uno o más grupos y asignarles políticas o roles. Los usuarios heredan los permisos de los grupos y pueden realizar operaciones específicas en los servicios en la nube según los permisos que se les hayan asignado.

La VPN es un servicio a nivel de proyecto implementado para regiones específicas. Al configurar el Ámbito en Proyectos específicos de la región y seleccionar los proyectos especificados en las regiones especificadas, los usuarios solo tendrán permisos de VPN en los proyectos seleccionados. Si configura el Ámbito en Todos los recursos, los usuarios tendrán permisos de VPN en todos los proyectos específicos de la región.
Al acceder a la VPN, los usuarios deben cambiar a la región autorizada.

Puede otorgar permisos mediante el uso de roles o políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define
  Permisos relacionados con las responsabilidades de los usuarios. Existe un número limitado de roles para otorgar permisos a los usuarios. Algunos roles dependen de otros para surtir efecto. Al asignar estos roles a los usuarios, recuerde asignar los roles de los que dependen. Sin embargo, los roles no son la opción ideal para una autorización detallada ni para un control de acceso seguro.

- Políticas: un tipo de mecanismo de autorización de grano fino que define
  Permisos necesarios para realizar operaciones en recursos específicos de la nube bajo ciertas condiciones. Este mecanismo permite una autorización basada en políticas más flexible, cumpliendo con los requisitos de control de acceso seguro. Por ejemplo, los administradores pueden otorgar a los usuarios de IAM permisos únicamente para administrar recursos VPN de un tipo específico.

La Tabla 1-9 enumera todos los permisos definidos por el sistema para VPN.

Tabla 1-9 Permisos definidos por el sistema para VPN

Rol del sistema/ Nombre de la póliza	Descripción	Dependencia
VPN Administrador (no recomendado)	Permisos de administrador para VPN. Los usuarios con estos permisos pueden realizar todas las operaciones en VPN. Los usuarios con estos permisos tienen los permisos de Administrador de VPC e Invitado de inquilino de forma predeterminada. • Administrador de VPC: política a nivel de proyecto, que se selecciona en el mismo proyecto que el Administrador de VPN. • Invitado inquilino: política a nivel de proyecto, que se selecciona en el mismo proyecto que el administrador de VPN.	-

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

La Tabla 1-10 enumera las operaciones comunes admitidas por los permisos definidos por el sistema para VPN S2C.

Tabla 1-10 Operaciones comunes admitidas por permisos definidos por el sistema para S2C VPN

Operación	VPN Administrador (No Recomendado)	VPN de acceso completo (Recomendado)	VPN Acceso de solo lectura
Creando una VPN puerta	√	• Empresa Edición VPN: √ • VPN clásica: ×	×
Visualización de una VPN puerta	√	√	√
Consultando la VPN lista de puertas de enlace	√	√	√
Actualizar una VPN puerta	√	• Empresa Edición VPN: √ • VPN clásica: ×	×
Eliminar una VPN puerta	√	• Empresa Edición VPN: √ • VPN clásica: ×	×
Creando una VPN conexión	√	• Empresa Edición VPN: √ • VPN clásica: √	×
Visualización de una VPN conexión	√	√	√
Consultando la VPN lista de conexiones	√	√	√
Actualizar una VPN conexión	√	• Empresa Edición VPN: √ • VPN clásica: √	×
Eliminar una VPN conexión	√	• Empresa Edición VPN: × • VPN clásica: √	×
Creando una puerta de enlace del cliente	√	• Empresa Edición VPN: √ • VPN clásica: N/D	×
Viendo una puerta de enlace del cliente	√	• Empresa Edición VPN: √ • VPN clásica: N/D	√

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Operación	VPN Administrador (No Recomendado)	VPN de acceso completo (Recomendado)	VPN Acceso de solo lectura
Consulta de la lista de la pasarela de clientes	√	• Empresa Edición VPN: √ • VPN clásica: N/D	√
Actualización de una pasarela de clientes	√	• Empresa Edición VPN: √ • VPN clásica: N/D	×
Eliminar una pasarela de clientes	√	• Empresa Edición VPN: √ • VPN clásica: N/D	×
Creación de un monitor de conexión VPN	√	• Empresa Edición VPN: √ • VPN clásica: ×	×
Consultar un monitor de conexión VPN	√	• Empresa Edición VPN: √ • VPN clásica: ×	√
Consulta de la lista de monitores de conexión VPN	√	• Empresa Edición VPN: √ • VPN clásica: ×	√
Eliminar un monitor de conexión VPN	√	• Empresa Edición VPN: √ • VPN clásica: ×	×

Enlaces útiles

- Descripción general del servicio IAM

1.12 Conceptos básicos

1.12.1 VPN IPsec

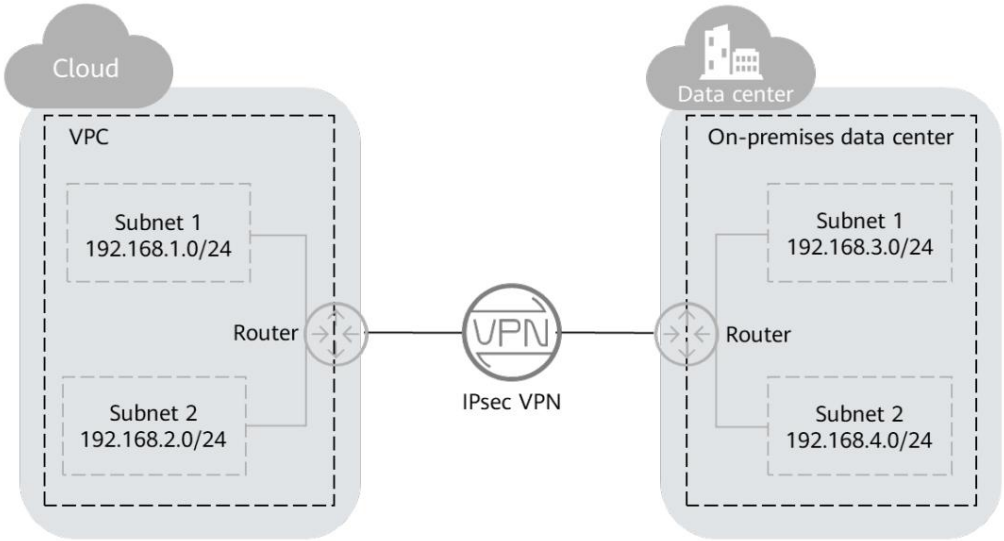
La VPN de protocolo de seguridad de Internet (IPsec) utiliza un conjunto de protocolos de red seguros que autentican y encriptan los paquetes de datos para proporcionar una comunicación encriptada segura entre diferentes redes.

En el ejemplo de la Figura 1-1, supongamos que ha creado una VPC con dos subredes (192.168.1.0/24 y 192.168.2.0/24) en la nube, y que el enrutador de su centro de datos local también tiene dos subredes (192.168.3.0/24 y 192.168.4.0/24). En este caso, puede crear una VPN para conectar las subredes de la VPC y las del centro de datos.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Figura 1-1 VPN IPsec



Se admite VPN de sitio a sitio para permitir la comunicación entre subredes de VPC y subredes de centros de datos locales.

1.12.2 Ancho de banda de la puerta de enlace VPN

El ancho de banda que compró para una puerta de enlace VPN se refiere al ancho de banda de salida, es decir, el ancho de banda para el tráfico enviado desde una VPC en la nube a una puerta de enlace de cliente en un centro de datos local.

- Si el ancho de banda adquirido es de 10 Mbit/s o menos, el ancho de banda entrante está limitado a 10 Mbit/s.
- Si el ancho de banda adquirido es mayor a 10 Mbit/s, el ancho de banda entrante es el mismo que el ancho de banda EIP.

1.12.3 Subred local

Las subredes locales son subredes de VPC que necesitan comunicarse con una red local mediante una VPN. Al adquirir una puerta de enlace VPN, puede configurar la subred local con cualquiera de las siguientes opciones:

- Seleccionar subred: Seleccione subredes de la lista desplegable. Esto se recomienda si todas las subredes que requieren comunicación VPN están en la VPC. • Introducir

bloque CIDR: Introduzca una subred usando la notación CIDR (ejemplo: 192.168.0.0/16). Si se especifican varias subredes, sepárelas con una coma (,). Esto se recomienda si los bloques CIDR que requieren comunicación VPN no se encuentran en la VPC a la que pertenece la puerta de enlace VPN. Por ejemplo, los bloques CIDR (como 0.0.0.0/0) que se conectan mediante peering de VPC no se encuentran en la VPC a la que pertenece la puerta de enlace VPN.

1.12.4 Subred del cliente

Las subredes de cliente son subredes en un centro de datos local que acceden a una VPC en la nube a través de una VPN. Debe introducir las subredes con notación CIDR (ejemplo: 192.168.0.0/16) y separar cada entrada con una coma.

 Derechos de autor © Huawei Technologies Co., Ltd.

770

Machine Translated by Google

Después de configurar una subred de cliente, no es necesario agregarle una ruta. El servicio VPN entregará automáticamente rutas que apunten a la subred del cliente.

NO TE

Una subred de cliente no se puede configurar en una dirección IP de clase D o clase E ni en una dirección IP que comience con 127.

 Derechos de autor © Huawei Technologies Co., Ltd.

771

Machine Translated by Google

2 Empezando

2.1 Configuración de la VPN de Enterprise Edition para conectar un centro de datos local a una VPC

2.1.1 Descripción general

Las regiones compatibles están sujetas a las disponibles en la consola.

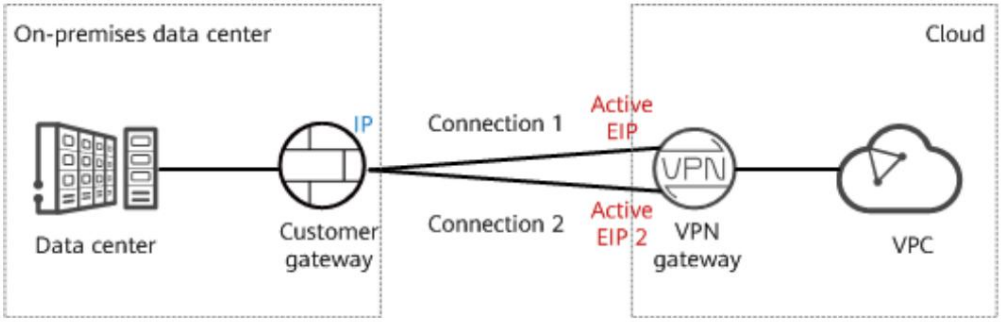
Guión

Para cumplir con los requisitos de desarrollo empresarial, la empresa A necesita implementar la comunicación entre su centro de datos local y su VPC. En este caso, la empresa A puede usar el servicio VPN para crear conexiones entre el centro de datos local y la VPC.

- Si el centro de datos local solo tiene una puerta de enlace de cliente y esta
  La puerta de enlace solo se puede configurar con una dirección IP. Se recomienda que la puerta de enlace VPN utilice el modo activo-activo. La Figura 2-1 muestra la red.

  En el modo activo-activo, si falla la conexión 1, el tráfico se redirige automáticamente a la conexión 2, sin afectar los servicios empresariales. Tras la recuperación de la conexión 1, la VPN sigue utilizando la conexión 2 para la transmisión de datos.

  Figura 2-1 Modo activo-activo



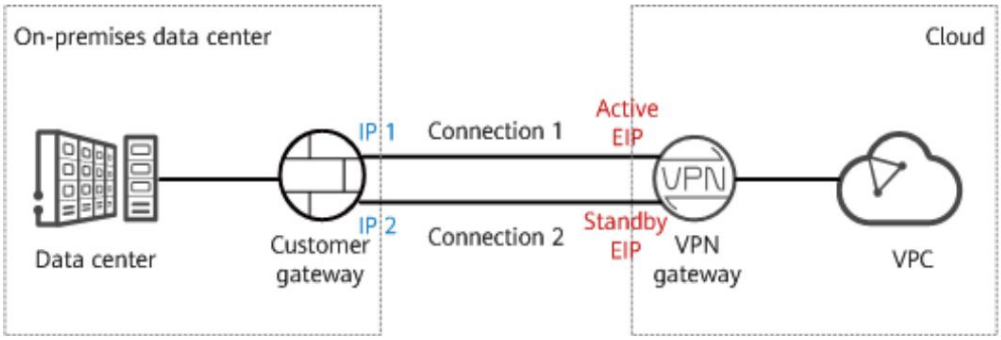
Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

• Si el centro de datos local tiene dos puertas de enlace de clientes o solo una puerta de enlace de clientes configurable con dos direcciones IP, se recomienda que la puerta de enlace VPN utilice el modo activo/en espera. La Figura 2-2 muestra la red.

En el modo activo/en espera, la conexión 1 es el enlace activo y la conexión 2, el enlace en espera. De forma predeterminada, el tráfico se transmite únicamente a través del enlace activo. Si el enlace activo falla, el tráfico se redirige automáticamente al enlace en espera, sin afectar los servicios empresariales. Una vez que el enlace activo se recupera, el tráfico se redirige de nuevo al enlace activo.

Figura 2-2 Modo activo/en espera



Limitaciones y restricciones

• El dispositivo de puerta de enlace del cliente debe ser compatible con los protocolos IKE e IPsec estándar. • Las subredes de interconexión del centro de datos local no se superponen con las de la VPC ni contienen 100.64.0.0/10 o 214.0.0.0/8.

Si la VPC usa conexiones Direct Cloud o Cloud Connect para comunicarse con otras VPC, las subredes del centro de datos local no pueden superponerse con las de estas VPC.

Plan de datos

Tabla 2-1 Plan de datos

Categoría Artículo		Datos
VPC	Subred que necesita acceder al centro de datos local	192.168.0.0/16
Puerta de enlace VPN	Interconexiones en subred	Esta subred se utiliza para la comunicación entre la puerta de enlace VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables. 192.168.2.0/24
	Modo HA	Activo-activo

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Categoría Artículo		Datos
	EIP	Las EIP se generan automáticamente al comprarlas. Por defecto, una puerta de enlace VPN utiliza dos EIP. En este ejemplo, las EIP son las siguientes: • EIP activo: 11.xx.xx.11 • EIP activo 2: 11.xx.xx.12
Conexión VPN norte	Dirección de interfaz del túnel	Una puerta de enlace VPN utiliza esta dirección para establecer un túnel IPsec con una puerta de enlace de cliente. En ambos extremos del túnel IPsec, las direcciones de interfaz del túnel local y remoto configuradas deben invertirse. • Conexión VPN 1: 169.254.70.1/30 • Conexión VPN 2: 169.254.71.1/30
Centro de datos local	Subred que necesita acceder a la VPC	172.16.0.0/16
Puerta de enlace del cliente	Dirección IP de la puerta de enlace	La dirección IP de la puerta de enlace la asigna un operador. En este ejemplo, la dirección IP de la puerta de enlace es: 22.xx.xx.22
	Dirección de interfaz del túnel	• Conexión VPN 1: 169.254.70.2/30 • Conexión VPN 2: 169.254.71.2/30

Proceso de operación

La Figura 2-3 muestra el proceso de uso del servicio VPN para habilitar la comunicación entre un centro de datos local y una VPC.

Figura 2-3 Proceso de operación

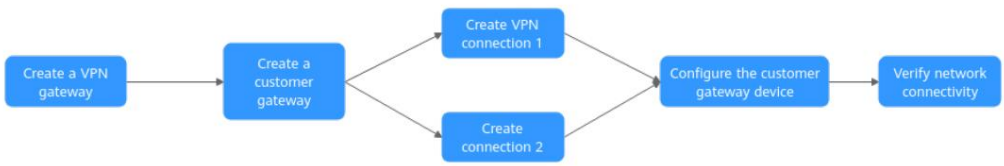


Tabla 2-2 Descripción del proceso de operación

norte el.	Paso	Descripción
1	2.1.2 Paso 1: Creación de una puerta de enlace VPN	Vincula dos EIP a la puerta de enlace VPN. Si ha adquirido EIP, puede vincularlos directamente a la puerta de enlace VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

norte el.	Paso	Descripción
2	2.1.3 Paso 2: Creación de una pasarela de clientes	Configure el dispositivo VPN en el centro de datos local como puerta de enlace del cliente.
3	2.1.4 Paso 3: Creación de una conexión VPN 1	Cree una conexión VPN entre el EIP activo de la puerta de enlace VPN y la puerta de enlace del cliente.
4	2.1.5 Paso 4: Creación de una conexión VPN 2	Cree una conexión VPN entre el EIP 2 activo de la puerta de enlace VPN y la puerta de enlace del cliente. Se recomienda que las configuraciones del modo de enrutamiento, PSK, política IKE y política IPsec de las dos conexiones VPN sean las mismas.
5	2.1.6 Paso 5: Configuración del dispositivo de puerta de enlace del cliente	• La interfaz del túnel local y remoto Las direcciones configuradas en el dispositivo de puerta de enlace del cliente deben ser las mismas que las direcciones de la interfaz del túnel local y del cliente de la conexión VPN, respectivamente. • El modo de enrutamiento, PSK, política IKE e IPsec La configuración de políticas en el dispositivo de puerta de enlace del cliente debe ser la misma que la de la conexión VPN.
6	2.1.7 Paso 6: Verificación de la conectividad de la red	Inicie sesión en un ECS y ejecute el comando ping para verificar la conectividad de la red.

2.1.2 Paso 1: Creación de una puerta de enlace VPN

Prerrequisitos

- Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte Guía del usuario de la nube privada virtual .
- Se han configurado reglas de grupo de seguridad para los ECS en la VPC y permiten que la puerta de enlace del cliente en el centro de datos local acceda a los recursos de la VPC. Para obtener más información sobre cómo configurar las reglas de grupo de seguridad, consulte Privado virtual Guía del usuario de la nube.

Procedimiento

Paso 1 Inicie sesión en la consola de administración.

Paso 2 Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.

Paso 3 En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace VPN.

Paso 4 Haga clic en Comprar S2C VPN Gateway.

Paso 5 Configure los parámetros según se le solicite, haga clic en Crear ahora y complete el pago.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Paso 6 A continuación se describen solo los parámetros clave.

Tabla 2-3 Parámetros clave de la puerta de enlace VPN

Descripción del parámetro		Valor de ejemplo
Región	Seleccione la región más cercana a usted.	-
Nombre	Nombra una puerta de enlace VPN.	vpngw-001
Red Tipo	• Red pública: una puerta de enlace VPN se comunica con una puerta de enlace de cliente en un centro de datos local a través de Internet. • Red privada: una puerta de enlace VPN se comunica con una puerta de enlace de cliente en un centro de datos local a través de una red privada.	Red pública
Asociado Con	Seleccione VPC.	VPC
VPC	Seleccione la VPC que necesita acceder al centro de datos local.	vpc-001(192.168.0.0/16)
Interconexión Subred	Esta subred se utiliza para la comunicación entre la puerta de enlace VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables.	192.168.2.0/24
Local Subred	Especifique la subred de VPC que necesita acceder al centro de datos local. Puede ingresar manualmente un bloque CIDR o seleccionar una subred del cuadro de lista desplegable.	192.168.0.0/24
Especificado en	Seleccionar Profesional 1.	Profesional 1
Modo HA	Seleccione Activo-activo.	Activo-activo
EIP activo	Puedes comprar un nuevo EIP o utilizar un EIP existente.	11.xx.xx.11
EIP 2 activo		11.xx.xx.12

----Fin

Verificación

Compruebe la puerta de enlace VPN creada en la página Puertas de enlace VPN . El estado inicial de la puerta de enlace VPN es Creando. Cuando el estado de la puerta de enlace VPN cambia a Normal, se ha creado correctamente.

Derechos de autor © Huawei Technologies Co., Ltd.

776

Machine Translated by Google

2.1.3 Paso 2: Creación de una pasarela de clientes

Procedimiento

Paso 1 En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Pasarelas de clientes.

Paso 2 En la página Puertas de enlace de clientes , haga clic en Crear puerta de enlace de clientes.

Paso 3 Establezca los parámetros según se le solicite y haga clic en Crear ahora.

A continuación se describen únicamente los parámetros clave.

Tabla 2-4 Parámetros de la puerta de enlace del cliente

Parámetro	Descripción	Valor de ejemplo
Nombre	Nombra una puerta de enlace de clientes.	cgw-001
Identificador	Introduzca la dirección IP del cliente puerta.	Dirección IP, 22.xx.xx.22
ASN de BGP	Ingrese el ASN de su sistema local centro de datos o red privada. El ASN BGP de la puerta de enlace del cliente debe ser diferente al de la VPN puerta.	65000

----Fin

Verificación

Verifique la pasarela de clientes creada en la página Pasarelas de clientes .

2.1.4 Paso 3: Creación de una conexión VPN 1

Procedimiento

Paso 1 En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.

Paso 2 En la página Conexiones VPN , haga clic en Crear conexión VPN.

Paso 3 Configure los parámetros para la conexión VPN 1 según se le solicite y haga clic en Enviar.

A continuación se describen únicamente los parámetros clave.

Tabla 2-5 Configuración de parámetros para la conexión VPN 1

Parámetro	Descripción	Valor de ejemplo
Nombre	Introduzca el nombre de la conexión VPN 1.	vpn-001

Derechos de autor © Huawei Technologies Co., Ltd.

777

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Puerta de enlace VPN	Seleccione la puerta de enlace VPN creada en 2.1.2 Paso 1: Creación de una puerta de enlace VPN.	vpngw-001
IP de puerta de enlace DIRECCIÓN	Seleccione el EIP activo de la puerta de enlace VPN.	11.xx.xx.11
Cliente Puerta	Seleccione la puerta de enlace de clientes creada en 2.1.3 Paso 2: Creación de una puerta de enlace de clientes.	cgw-001
Tipo de VPN	Seleccione enrutamiento estático.	Enrutamiento estático
Cliente Subred	Ingrese la subred del centro de datos local que necesita acceder a la VPC. NOTA • La subred del cliente puede superponerse con la subred local pero no puede ser el mismo que la subred local. • No se puede crear una subred de cliente Incluido en las subredes existentes de la VPC asociada a la puerta de enlace VPN. Tampoco puede ser la dirección de destino en la tabla de rutas de la VPC asociada a la puerta de enlace VPN. • Las subredes del cliente no pueden ser los bloques CIDR reservados de VPC, por ejemplo, 100.64.0.0/10 o 214.0.0.0/8. • Si la subred de interconexión es asociado con una regla de ACL, asegúrese de que la regla de ACL permita el puerto TCP para el tráfico entre todas las subredes locales y de cliente. • Los grupos de direcciones no se pueden utilizar para Configurar las subredes de origen y destino en una política en los dispositivos de puerta de enlace del cliente.	172.16.0.0/16
Interfaz IP DIRECCIÓN Asignación	Las opciones incluyen Especificar manualmente y Asignar automáticamente.	Especificar manualmente
Túnel local Interfaz DIRECCIÓN	Especifique la dirección de la interfaz de túnel configurada en la puerta de enlace VPN. NOTA Las direcciones de interfaz local y remota configuradas en el dispositivo de puerta de enlace del cliente deben ser las mismas que los valores de la Dirección IP de la interfaz del túnel del cliente y la Dirección IP de la interfaz del túnel local, respectivamente.	169.254.70.2/30

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Cliente Túnel Interfaz DIRECCIÓN	Especifique la dirección de la interfaz de túnel configurada en el dispositivo de puerta de enlace del cliente.	169.254.70.1/30
Detección de enlaces	Esta función se utiliza para la ruta Detección de confiabilidad en escenarios de múltiples enlaces. NOTA Al habilitar esta función, asegúrese de que la puerta de enlace del cliente sea compatible con ICMP y esté configurada correctamente con la dirección IP de la interfaz del cliente de la conexión VPN. De lo contrario, el tráfico VPN no se reenviará.	NQA habilitado
PSK, Confirm PSK	Especifique la clave de negociación de la conexión VPN. Las PSK configuradas en la consola VPN y en el dispositivo de puerta de enlace del cliente deben ser las mismas.	Prueba@123
Configuración de políticas	Configure las políticas IKE e IPsec, que definen los algoritmos de cifrado utilizados por el túnel VPN. La configuración de políticas en la consola VPN y el dispositivo de puerta de enlace del cliente deben ser las mismas.	Por defecto

----Fin

Verificación

Compruebe la conexión VPN creada en la página Conexiones VPN . El estado inicial de la conexión VPN es "Creando". Dado que el dispositivo de puerta de enlace del cliente no se ha configurado, no se puede establecer la conexión VPN. Después de unos 2 minutos, el estado de la conexión VPN cambia a "No conectado".

2.1.5 Paso 4: Creación de una conexión VPN 2

Procedimiento

Paso 1 En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.

Paso 2 En la página Conexiones VPN , haga clic en Comprar conexión VPN.

Para la conexión VPN 2, se recomienda utilizar la misma configuración que para la conexión VPN 1, excepto el nombre de la conexión, la dirección IP de la puerta de enlace, la dirección IP de la interfaz del túnel local y la dirección IP de la interfaz del túnel del cliente.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Tabla 2-6 Configuración de parámetros para la conexión VPN 2

Parámetro	Descripción	Valor de ejemplo
Nombre	Introduzca el nombre de la conexión VPN 2.	vpn-002
Puerta de enlace VPN	Seleccione la puerta de enlace VPN creada en 2.1.2 Paso 1: Creación de una puerta de enlace VPN.	vpngw-001
IP de puerta de enlace DIRECCIÓN	Seleccione EIP 2 activo del gateway VPN.	11.xx.xx.12
Cliente Puerta	Seleccione la puerta de enlace de clientes creada en 2.1.3 Paso 2: Creación de una puerta de enlace de clientes.	cgw-001
Tipo de VPN	Seleccione enrutamiento estático.	Enrutamiento estático
Cliente Subred	Ingrese la subred del centro de datos local que necesita acceder a la VPC. NOTA • La subred del cliente puede superponerse con la subred local pero no puede ser el mismo que la subred local. • No se puede crear una subred de cliente Incluido en las subredes existentes de la VPC asociada a la puerta de enlace VPN. Tampoco puede ser la dirección de destino en la tabla de rutas de la VPC asociada a la puerta de enlace VPN. • Las subredes del cliente no pueden ser los bloques CIDR reservados de VPC, por ejemplo, 100.64.0.0/10 o 214.0.0.0/8. • Si la subred de interconexión es asociado con una regla de ACL, asegúrese de que la regla de ACL permita el puerto TCP para el tráfico entre todas las subredes locales y de cliente. • Los grupos de direcciones no se pueden utilizar para Configurar las subredes de origen y destino en una política en los dispositivos de puerta de enlace del cliente.	172.16.0.0/16
Interfaz IP DIRECCIÓN Asignación	Las opciones incluyen Especificar manualmente y Asignar automáticamente.	Especificar manualmente

Derechos de autor © Huawei Technologies Co., Ltd.

780

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Túnel local Interfaz DIRECCIÓN	Especifique la dirección de la interfaz de túnel configurada en la puerta de enlace VPN. NOTA Las direcciones de interfaz local y remota configuradas en el dispositivo de puerta de enlace del cliente deben ser las mismas que los valores de la Dirección IP de la interfaz del túnel del cliente y la Dirección IP de la interfaz del túnel local, respectivamente.	169.254.71.2/30
Cliente Túnel Interfaz DIRECCIÓN	Especifique la dirección de la interfaz de túnel configurada en el dispositivo de puerta de enlace del cliente.	169.254.71.1/30
Detección de enlaces	Esta función se utiliza para la ruta Detección de confiabilidad en escenarios de múltiples enlaces. NOTA: Al habilitar esta función, asegúrese de que la puerta de enlace del cliente sea compatible con ICMP y esté configurada correctamente con la dirección IP de la interfaz del cliente de la conexión VPN. De lo contrario, el tráfico VPN no se reenviará.	NQA habilitado
PSK, Confirm PSK	Especifique la clave de negociación de la conexión VPN. Las PSK configuradas en la consola VPN y en el dispositivo de puerta de enlace del cliente deben ser las mismas.	Prueba@123
Configuración de políticas	Configure las políticas IKE e IPsec, que definen los algoritmos de cifrado utilizados por el túnel VPN. La configuración de políticas en la consola VPN y el dispositivo de puerta de enlace del cliente deben ser las mismas.	Por defecto

----Fin

Verificación

Compruebe la conexión VPN creada en la página Conexiones VPN . El estado inicial de la conexión VPN es "Creando". Dado que el dispositivo de puerta de enlace del cliente no se ha configurado, no se puede establecer la conexión VPN. Después de unos 2 minutos, el estado de la conexión VPN cambia a "No conectado".

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

2.1.6 Paso 5: Configuración del dispositivo de puerta de enlace del cliente

Procedimiento

NO TE

En este ejemplo, el dispositivo de puerta de enlace del cliente es un enrutador AR.

Paso 1 Inicie sesión en el enrutador AR.

Paso 2 Ingrese a la vista del sistema.

```
<AR651>vista del sistema
```

Paso 3: Configure una dirección IP para la interfaz WAN. En este ejemplo, la interfaz WAN...
del enrutador AR es GigabitEthernet 0/0/8.

```
[AR651]interfaz GigabitEthernet 0/0/8 [AR651-
GigabitEthernet0/0/8]dirección IP 22.xx.xx.22 255.255.255.0 [AR651-
GigabitEthernet0/0/8]salir
```

Paso 4 Configure una ruta predeterminada.

```
[AR651] ruta ip estática 0.0.0.0 0.0.0.0 22.xx.xx.1
```

En este comando, es la dirección de la puerta de enlace de la dirección IP pública del enrutador AR.
Reemplácela con la dirección de la puerta de enlace real.

Paso 5 Habilite el algoritmo SHA-2 para que sea compatible con los algoritmos RFC estándar.

```
[AR651]Habilitación de autenticación IPsec compatible con SHA2
```

Paso 6 Configurar una propuesta IPsec.

```
[AR651]Propuesta IPsec hwproposal1
[AR651-IPsec-proposal-hwproposal1]Algoritmo de autenticación esp sha2-256 [AR651-IPsec-
proposal-hwproposal1]Algoritmo de cifrado esp aes-128 [AR651-IPsec-proposal-
hwproposal1]Salir
```

Paso 7 Configurar una propuesta IKE.

```
[AR651]Propuesta ike 2
[AR651-ike-proposal-2]Algoritmo de cifrado AES-128 [AR651-ike-
proposal-2]Grupo DH 14 [AR651-ike-
proposal-2]Algoritmo de autenticación SHA2-256 [AR651-ike-
proposal-2]Método de autenticación pre-compartir [AR651-ike-
proposal-2]Algoritmo de integridad Hmac-Sha2-256 [AR651-ike-
proposal-2]PRF Hmac-Sha2-256 [AR651-ike-
proposal-2]Salir
```

Paso 8 Configurar pares IKE.

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]deshacer versión 1
[AR651-ike-peer-hwpeer1]cifrado de clave precompartida Test@123
[AR651-ike-peer-hwpeer1]ike-propuesta 2 [AR651-
ike-peer-hwpeer1]dirección local 22.xx.xx.22 [AR651-ike-peer-
hwpeer1]dirección remota 11.xx.xx.11 [AR651-ike-peer-
hwpeer1]relleno de cifrado RSA oaep [AR651-ike-peer-
hwpeer1]relleno de firma RSA pss [AR651-ike-peer-
hwpeer1]autenticación ikev2 sign-hash sha2-256 [AR651-ike-peer-hwpeer1]Salir
[AR651]ike peer hwpeer2 [AR651-ike-
peer-hwpeer2]Deshacer versión
1 [AR651-ike-peer-hwpeer2]Cifrado de clave
precompartida Prueba@123 [AR651-ike-peer-hwpeer2]Propuesta ike 2
[AR651-ike-peer-hwpeer2]Dirección local
22.xx.xx.22 [AR651-ike-peer-hwpeer2]Dirección remota
11.xx.xx.12 [AR651-ike-peer-hwpeer2]Relleno de cifrado RSA
oaep [AR651-ike-peer-hwpeer2]Relleno de firma RSA pss
```


Derechos de autor © Huawei Technologies Co., Ltd.

782

Machine Translated by Google


```
[AR651-ike-peer-hwpeer2]Autenticación ikev2, hash de firma sha2-256
[AR651-ike-peer-hwpeer2]salir
```

Los comandos se describen a continuación:

- cifrado de clave precompartida: configura una PSK, que debe ser la misma que la configurada en la consola VPN.
- dirección local: especifica la dirección IP pública del enrutador AR. •

dirección remota: especifica el EIP activo o EIP 2 activo de la puerta de enlace VPN.

Paso 9 Configure un perfil IPsec.

```
[AR651]Perfil IPsec hwpro1
[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1
[AR651-IPsec-profile-hwpro1]propuesta hwproposal1
[AR651-IPsec-profile-hwpro1]pfs dh-group14
[AR651-IPsec-profile-hwpro1]salir
[AR651]Perfil IPsec hwpro2
[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2
[AR651-IPsec-profile-hwpro2]propuesta hwproposal1
[AR651-IPsec-profile-hwpro2]pfs dh-group14
[AR651-IPsec-profile-hwpro2]salir
```

Paso 10 Configurar interfaces de túnel virtual.

```
[AR651] Interfaz Tunnel0/0/1
[AR651-Tunnel0/0/1] MTU 1400
[AR651-Tunnel0/0/1] Dirección IP 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1] Protocolo de túnel IPsec
[AR651-Tunnel0/0/1] Origen 22.xx.xx.22
[AR651-Tunnel0/0/1] Destino 11.xx.xx.11
[AR651-Tunnel0/0/1] Perfil IPsec hwpro1
[AR651-Tunnel0/0/1] Salir
[AR651] Interfaz Tunnel0/0/2
[AR651-Tunnel0/0/2] MTU 1400
[AR651-Tunnel0/0/2]dirección IP 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]protocolo de túnel IPsec
[AR651-Tunnel0/0/2]origen 22.xx.xx.22
[AR651-Tunnel0/0/2]destino 11.xx.xx.12 [AR651-
Tunnel0/0/2]perfil IPsec hwpro2 [AR651-
Tunnel0/0/2]salir
```

Los comandos se describen a continuación:

- Interfaz Tunnel0/0/1 e interfaz Tunnel0/0/2: indican las interfaces de túnel correspondientes a las dos conexiones VPN.

  En este ejemplo, Tunnel0/0/1 establece una conexión VPN con el EIP activo de la puerta de enlace VPN, y Tunnel0/0/2 establece una conexión VPN con el EIP 2 activo de la puerta de enlace

VPN. • dirección IP: configura una dirección IP para una interfaz de túnel en el

enrutador AR. • origen: especifica la dirección IP pública del

enrutador AR. • destino: especifica el EIP activo o el EIP 2 activo de la puerta de enlace VPN.

Paso 11 Configurar NQA.

```
[AR651]instancia de prueba nqa IPsec_nqa1
IPsec_nqa1 [AR651-nqa-IPsec_nqa1-IPsec_nqa1]tipo
de prueba icmp [AR651-nqa-IPsec_nqa1-IPsec_nqa1]dirección-destino ipv4
169.254.70.2 [AR651-nqa-IPsec_nqa1-IPsec_nqa1]dirección-fuente ipv4
169.254.70.1 [AR651-nqa-IPsec_nqa1-
IPsec_nqa1]frecuencia 15 [AR651-nqa-
IPsec_nqa1-IPsec_nqa1]ttl 255 [AR651-nqa-
IPsec_nqa1-IPsec_nqa1]empezar ahora
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]salir
[AR651]instancia de prueba nqa IPsec_nqa2 IPsec_nqa2 [AR651-nqa-IPsec_nqa2-IPsec_nqa2]icmp de tipo de prueba
```


Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google


```
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]dirección-destino ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]dirección-origen ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frecuencia 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]empezar
ahora [AR651-nqa-IPsec_nqa2-IPsec_nqa2]salir
```

Los comandos se describen a continuación:

• nqa test-instance IPsec_nqa1 IPsec_nqa1 y nqa test-instance IPsec_nqa2 IPsec_nqa2: configure dos instancias de prueba NQA denominadas IPsec_nqa1 e IPsec_nqa2.

En este ejemplo, se crea la instancia de prueba IPsec_nqa1 para la conexión VPN a la que pertenece el EIP activo de la puerta de enlace VPN; la instancia de prueba IPsec_nqa2 se crea para la conexión VPN a la que pertenece el EIP activo 2 de la puerta de enlace VPN. • destination-address: especifica la

dirección de la interfaz de túnel de la VPN puerta.

• source-address: especifica la dirección de la interfaz del túnel del enrutador AR.

Paso 12 Configure la asociación entre la ruta estática y NQA.

```
[AR651] ruta ip estática 192.168.0.0 255.255.255.0 Tunnel0/0/1 pista nqa IPsec_nqa1 IPsec_nqa1
[AR651] ruta ip estática 192.168.0.0 255.255.255.0 Tunnel0/0/2 pista nqa IPsec_nqa2 IPsec_nqa2
```

Los parámetros se describen a continuación:

• 192.168.0.0 indica la subred local de la VPC.

• Túnel y conexión en el mismo comando corresponden al mismo VPN IPsec_nqa .

----Fin

Verificación

Paso 1 Inicie sesión en la consola de administración.

Paso 2 Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.

Paso 3 En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.

Verifique que los estados de las dos conexiones VPN sean Normales.

----Fin

2.1.7 Paso 6: Verificación de la conectividad de la red

Procedimiento

Paso 1 Inicie sesión en la consola de administración.

Paso 2 Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.

Paso 3 Haga clic en Lista de servicios y seleccione Computación > Elastic Cloud Server.

Paso 4 Inicie sesión en un ECS.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

En este ejemplo, utilice VNC proporcionado en la consola de administración para iniciar sesión en un ECS.

Paso 5 Ejecute el siguiente comando en el ECS:

ping 172.16.0.100

172.16.0.100 es la dirección IP de un servidor en el centro de datos local. Reemplácela con la dirección IP real del servidor.

Si se muestra información similar a la siguiente, la VPC en la nube y el centro de datos local pueden comunicarse entre sí.

```
Respuesta de xx.xx.xx.xx: bytes=32 tiempo=28ms TTL=245
Respuesta de xx.xx.xx.xx: bytes=32 tiempo=28ms TTL=245
Respuesta de xx.xx.xx.xx: bytes=32 tiempo=28ms TTL=245
Respuesta de xx.xx.xx.xx: bytes=32 tiempo=27ms TTL=245
```

----Fin

2.2 Proceso de creación de VPN

2.2.1 Comprar una puerta de enlace VPN

Escenarios

Para conectar su centro de datos local o red privada a sus ECS en una VPC, primero compre una puerta de enlace VPN.

Prerrequisitos

- Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte Guía del usuario de la nube privada virtual .
- Se han configurado las reglas del grupo de seguridad para la VPC y los ECS pueden comunicarse con otros dispositivos en la nube. Para obtener más información sobre cómo configurar las reglas del grupo de seguridad, consulte Guía del usuario de la nube privada virtual .

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
3. En el panel de navegación de la izquierda, seleccione Red privada virtual > Clásico – Puertas de enlace VPN.

   Si Enterprise Edition VPN está disponible para la región seleccionada, elija Red privada virtual > Clásica.
4. En la página Puertas de enlace VPN , haga clic en Crear puerta de enlace VPN.
5. Configure los parámetros de la puerta de enlace VPN según la Tabla 2-7 y haga clic en Crear Ahora.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Tabla 2-7 Descripción de los parámetros de la puerta de enlace VPN

Parámetro	Descripción	Valor de ejemplo
Región	Las regiones son áreas geográficas que están físicamente aislados unos de otros otro. Las redes dentro de diferentes Las regiones no están conectadas entre sí otros, por lo que no se pueden compartir recursos en todas las regiones. Para redes bajas Latencia y acceso rápido a los recursos, Seleccione la región más cercana a su usuarios objetivo.	-
Nombre	Nombre de una puerta de enlace VPN.	vpngw-001
VPC	Nombre de la VPC a la que se conecta la VPN La puerta de enlace se conecta.	vpc-001
Tipo	Tipo de VPN. IPsec se selecciona mediante por defecto.	IPsec
Fiabilidad	Solo se admite activo-activo .	Activo-activo

2.2.2 Comprar una conexión VPN

Escenarios

Para conectar su centro de datos local o red privada a sus ECS en una VPC,
Es necesario crear una conexión VPN después de obtener una puerta de enlace VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
3. En el panel de navegación de la izquierda, seleccione Red privada virtual > Clásica – Conexiones VPN.

   Si Enterprise Edition VPN está disponible para la región seleccionada, elija Virtual Red Privada > Clásica.
4. En la página Conexiones VPN , haga clic en Crear conexión VPN.
5. Configure los parámetros según se le solicite y haga clic en Crear ahora. La Tabla 2-8 enumera Los parámetros de conexión VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

786

Machine Translated by Google

Tabla 2-8 Descripción de los parámetros de conexión VPN

Parámetro	Descripción	Valor de ejemplo
Región	Las regiones son áreas geográficas físicamente aisladas entre sí. Las redes dentro de las diferentes regiones no están conectadas entre sí, por lo que no se pueden compartir recursos entre ellas. Para una baja latencia de red y un acceso rápido a los recursos, seleccione la región más cercana a sus usuarios objetivo.	N / A
Nombre	Nombre de una conexión VPN.	vpn-001
Nombre de la puerta de enlace VPN	Nombre de la puerta de enlace VPN para la que se crea la conexión VPN.	vpcgw-001
Subred local: subredes	de VPC que accederán a su red local a través de una VPN. Puede configurar la subred local mediante cualquiera de los siguientes métodos: • Seleccionar subred: Seleccione las subredes que necesitan acceder a su centro de datos local o red privada. • Especificar bloque CIDR: Ingrese los bloques CIDR que necesitan acceder a su centro de datos local o red privada.	192.168.1.0/24, 192.168.2.0/24
Remoto Puerta	La dirección IP pública de la puerta de enlace en su centro de datos o en la red privada. Esta dirección IP se utiliza para comunicarse con su VPC. En el modo activo-activo, puede introducir dos direcciones de puerta de enlace remotas.	N / A
Remoto Subred	Las subredes de su red local que accederán a una VPC a través de una VPN. Las subredes remotas y locales no pueden superponerse. La subred remota no puede superponerse con bloques CIDR involucrados en el emparejamiento de VPC, las conexiones de Direct Connect o Cloud Connect existentes creadas para la VPC local.	192.168.3.0/24, 192.168.4.0/24

Derechos de autor © Huawei Technologies Co., Ltd.

787

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
PSK	Clave privada compartida por dos extremos de una VPN Conexión para negociación. PSKs configurado en ambos extremos de la VPN La conexión debe ser la misma. El PSK: • Contiene de 6 a 128 caracteres. • Solo puede contener: – Dígitos – Cartas – Caracteres especiales: ~ ! @ # $ % ^ ( ) - . /_: ; + = [ ] { } | \ ,	Prueba@123
Confirmar PSK	Ingrese el PSK nuevamente.	Prueba@123
Avanzado Ajustes	• Predeterminado: utilizar IKE e IPsec predeterminados políticas. • Existente: utilizar IKE e IPsec existentes políticas. • Personalizado: incluye política IKE y Política IPsec, que especifica la cifrado y autenticación algoritmos de un túnel VPN. Para Para más detalles sobre las políticas, consulte la Tabla 2-9 y Tabla 2-10.	Costumbre

Tabla 2-9 Política de IKE

Parámetro	Descripción	Valor de ejemplo
Autenticación Algoritmo n	Algoritmo hash utilizado para autenticación. Lo siguiente Se admiten algoritmos: • MD5 (este algoritmo es inseguro. Tenga cuidado cuando utilizando este algoritmo.) • SHA1 (este algoritmo es inseguro. Tenga cuidado cuando utilizando este algoritmo.) • SHA2-256 • SHA2-384 • SHA2-512 El algoritmo predeterminado es SHA1.	SHA1

Derechos de autor © Huawei Technologies Co., Ltd.

788

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Cifrado Algoritmo	Algoritmo de cifrado. Se admiten los siguientes algoritmos: • AES-128 • AES-192 • AES-256 • 3DES (este algoritmo no es seguro. Tenga cuidado al utilizarlo). El algoritmo predeterminado es AES-128.	AES-128
Algoritmo DH	Algoritmo de intercambio de claves Diffie-Hellman. Se admiten los siguientes algoritmos: • Grupo 1 (este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo 2 (este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo 5 (este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) • Grupo 14 • Grupo 15 • Grupo 16 • Grupo 19 • Grupo 20 • Grupo 21	Grupo 5
Versión	Versión del protocolo IKE. El valor puede ser uno de los siguientes: • v1 (no recomendado por riesgos de seguridad) • versión 2 El valor predeterminado es v2.	versión 2
Duración de la vida (s)	Tiempo de vida de una SA, en segundos Una SA se renegociará cuando expire su tiempo de vida. El valor predeterminado es 86400.	86400

Derechos de autor © Huawei Technologies Co., Ltd.

789

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Negociación Modo	Este parámetro solo está disponible cuando la versión es v1. Puedes configurar el modo de negociación como principal o agresivo. El modo predeterminado es Principal.	Principal

Tabla 2-10 Política IPsec

Parámetro	Descripción	Valor de ejemplo
Autenticación Algoritmo	Se utiliza un algoritmo hash para la autenticación. Se admiten los siguientes algoritmos: • SHA1 (este algoritmo no es seguro. Tenga cuidado al usarlo). • MD5 (este algoritmo no es seguro. Tenga cuidado al usarlo). • SHA2-256 • SHA2-384 • SHA2-512	SHA1
Cifrado Algoritmo	Algoritmo de cifrado. Se admiten los siguientes algoritmos: • AES-128 • AES-192 • AES-256 • 3DES (este algoritmo no es seguro. Tenga cuidado al utilizarlo). El algoritmo predeterminado es AES-128.	AES-128

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
PFS	Algoritmo utilizado por la función Perfect forward secrecy (PFS). PFS admite los siguientes algoritmos: • Grupo DH 1 (este algoritmo es • Grupo DH 2 (este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo DH 5 (este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo DH 14 • Grupo DH 15 • Grupo DH 16 • Grupo DH 19 • Grupo DH 20 • Grupo DH 21	Grupo DH 5
Transferir Protocolo	Protocolo de seguridad utilizado en IPsec para transmitir y encapsular datos de usuario. Se admiten los siguientes protocolos: • Ah • ESP • AH-ESP El protocolo predeterminado es ESP.	ESP
Duración de la vida (s)	Tiempo de vida de una SA, en segundos Una SA se renegociará cuando expire su tiempo de vida. El valor predeterminado es 3600.	3600

NO TE

Una política IKE especifica los algoritmos de cifrado y autenticación que se utilizarán en la fase de negociación de un túnel IPsec. Una política IPsec especifica el protocolo, el algoritmo de cifrado y el algoritmo de autenticación que se utilizarán en la fase de transmisión de datos de un túnel IPsec. Las políticas IKE e IPsec deben ser las mismas en ambos extremos de una conexión VPN. Si son diferentes, no se podrá establecer la conexión VPN.

6. Haga clic en Enviar.
7. Debe configurar un túnel VPN IPsec en el enrutador o firewall de su centro de datos local.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

3 Gestión

VPN S2C de edición empresarial 3.1

3.1.1 Administración de la puerta de enlace VPN de la edición empresarial

Creación de una puerta de enlace VPN

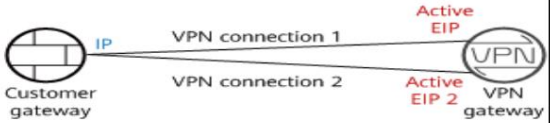
Guión

Para conectar su centro de datos local o red privada a sus ECS en una VPC, debe crear una puerta de enlace VPN antes de crear una conexión VPN.

Contexto

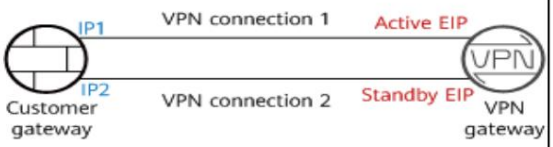
La red recomendada varía según la cantidad de direcciones IP de la puerta de enlace del cliente, como se describe en la Tabla 3-1.

Tabla 3-1 Redes

Número de Costumbre o Puerta — DIRECCIÓN s	Redes recomendadas	Descripción
1		Se recomienda que la puerta de enlace VPN utilice el modo activo-activo. En este caso, se utiliza un grupo de conexión VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Número de Costumbre o Puerta — DIRECCIÓN s	Redes recomendadas	Descripción
2		Se recomienda que la puerta de enlace VPN utilice el modo activo/en espera. En este caso, se utilizan dos grupos de conexiones VPN.

- Si su centro de datos local solo tiene una puerta de enlace de cliente configurada con una sola dirección IP, se recomienda que la puerta de enlace VPN utilice el modo activo-activo. En este modo, debe crear una conexión VPN entre cada EIP activo y EIP 2 activo de la puerta de enlace VPN y la dirección IP de la puerta de enlace de cliente. En este caso, solo se utiliza un grupo de conexiones VPN.

- Si su centro de datos local tiene dos puertas de enlace de clientes o una puerta de enlace de clientes configurada con dos direcciones IP, se recomienda que la puerta de enlace VPN utilice el modo activo/en espera. En este modo, debe crear una conexión VPN con cada dirección IP de la puerta de enlace de clientes utilizando las EIP activas y en espera de la puerta de enlace VPN. En este caso, se utilizan dos grupos de conexiones VPN.

Prerrequisitos

- Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte Guía del usuario de la nube privada virtual .
- Se han configurado las reglas del grupo de seguridad para la VPC y los ECS pueden comunicarse con otros dispositivos en la nube. Para obtener más información sobre cómo configurar las reglas del grupo de seguridad, consulte Guía del usuario de la nube privada virtual .

Procedimiento

Paso 1 Inicie sesión en la consola de administración.

Paso 2 Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.

Paso 3 Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.

Paso 4 En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace VPN.

Paso 5 Haga clic en Comprar S2C VPN Gateway.

Paso 6 Configure los parámetros según se le solicite y haga clic en Crear ahora.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

En la Tabla 3-2 se enumeran los parámetros de la puerta de enlace VPN.

Tabla 3-2 Descripción de los parámetros de la puerta de enlace VPN

Parlamento o	Descripción	Valor de ejemplo
Región	Para una baja latencia de red y un acceso rápido a los recursos, seleccione la región más cercana a su destino usuarios. Los recursos no se pueden compartir entre regiones.	Seleccione una región según sea necesario.
Nombre	Nombre de una puerta de enlace VPN. El valor solo puede contener letras, dígitos, guiones bajos (_), guiones (-) y puntos (.).	vpngw-001
Red Tipo	• Red pública: una puerta de enlace VPN establece conexiones VPN a través de Internet. • Red privada: una puerta de enlace VPN Establece conexiones VPN a través de una red privada.	Red pública
Asociado Con	• VPC A través de una VPC, la puerta de enlace VPN envía mensajes a la puerta de enlace del cliente o a los servidores en la subred local.	VPC
VPC	Seleccione una VPC.	vpc-001(192.168.0.0/16)
Interconexión Subred	Esta subred se utiliza para la comunicación entre la puerta de enlace VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables.	192.168.66.0/24
Local Subred	Subredes de VPC con las que su centro de datos local necesita comunicarse a través de la puerta de enlace del cliente. • Seleccionar subred Seleccionar subredes de la VPC local. • Ingresar bloque CIDR Ingrese subredes de la VPC local o subredes de la VPC que establece una conexión de emparejamiento con la VPC local.	192.168.1.0/24,19 2.168.2.0/24
BGP ASN	BGP ASN del gateway VPN, que debe ser diferente al del gateway del cliente.	64512
Especificado en	Hay dos opciones disponibles: Profesional 1 y Profesional 2.	Profesional 1

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parlamento o	Descripción	Valor de ejemplo
EL	Una AZ es una ubicación geográfica con suministro de energía e instalaciones de red independientes en una región. Las AZ en la misma VPC están interconectadas mediante redes privadas y físicamente aisladas. • Si hay dos o más AZ disponibles, seleccione dos. AZs. La puerta de enlace VPN implementada en dos zonas de disponibilidad (AZ) tiene mayor disponibilidad. Se recomienda seleccionar las AZ donde se ubican los recursos de la VPC. • Si solo hay una AZ disponible, seleccione esta AZ.	AZ1, AZ2
Modo HA • Activo-activo	– Cuando Asociar con se establece en VPC, el El tráfico saliente desde la puerta de enlace VPN a la subred del cliente se reenvía preferentemente a través de la primera conexión VPN (conexión VPN 1) configurada entre la subred del cliente y un EIP. Si falla la conexión VPN 1, el tráfico saliente se redirige automáticamente a la otra conexión VPN (conexión VPN 2) configurada con la subred del cliente. Tras la recuperación de la conexión VPN 1, el tráfico saliente se sigue transmitiendo a través de la conexión VPN 2 y no se redirige de nuevo a la conexión VPN 1. • Activa/En espera: El tráfico saliente desde la puerta de enlace VPN a la subred del cliente se transmite preferentemente a través de la conexión VPN (conexión VPN 1) establecida entre la subred del cliente y el EIP activo. Si la conexión VPN 1 falla, el tráfico saliente se redirige automáticamente a la otra conexión VPN (conexión VPN 2) establecida entre la subred del cliente y el EIP en espera. Una vez que la conexión VPN 1 se recupera, el tráfico saliente se redirige automáticamente a la conexión VPN 1.	Activo-activo
Ancho de banda h Nombre	Nombre del ancho de banda EIP.	Vpngw-ancho de banda1

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parlamento o	Descripción	Valor de ejemplo
EIP activo Este	parámetro solo está disponible cuando la red El tipo se establece en Red pública. EIP utilizado por la puerta de enlace VPN para comunicarse con una puerta de enlace de cliente. • Crear ahora: crea un EIP. • Utilizar existente: utilice un EIP existente.	Crea ahora
Ancho de banda h (Mbit/s)	Este parámetro solo está disponible cuando el Tipo de red está configurado como Red pública. Ancho de banda del EIP, en Mbit/s. • Todas las conexiones VPN creadas mediante el EIP comparten su ancho de banda. El consumo total de ancho de banda de todas las conexiones VPN no puede superar el ancho de banda del EIP. Si el tráfico de red supera el ancho de banda del EIP, podría producirse congestión e interrupciones en las conexiones VPN. Por lo tanto, asegúrese de configurar suficiente ancho de banda. • Puede configurar reglas de alarma en Cloud Eye para monitorear el ancho de banda. • Puede personalizar el ancho de banda dentro del rango permitido	20 Mbit/s
Ancho de banda h Nombre	Este parámetro solo está disponible cuando el Tipo de red está configurado como Red pública. Nombre del ancho de banda EIP.	Vpngw-ancho de banda2
EIP 2 activo	Este parámetro solo está disponible cuando el Tipo de red está configurado como Red pública y el Modo HA está configurado como Activo-activo. Una puerta de enlace VPN debe estar vinculada a un grupo de EIP (EIP activo y EIP activo 2). Puede planificar el ancho de banda para cada EIP.	Crea ahora
Apoyar EIP	Este parámetro solo está disponible cuando el Tipo de red está configurado como Red pública y el Modo HA está configurado como Activo/En espera. Una puerta de enlace VPN debe estar vinculada a un grupo de EIP (EIP activo y EIP en espera). Se puede planificar el ancho de banda para cada EIP. Los EIP pueden compartir ancho de banda con los EIP utilizados por otros servicios de red.	Crea ahora

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parlamento o	Descripción	Valor de ejemplo
Ancho de banda h (Mbit/s)	Este parámetro solo está disponible cuando el Tipo de red está configurado como Red pública y el EIP activo 2 o el EIP en espera está configurado como Crear ahora. Ancho de banda del EIP, en Mbit/s. • Todas las conexiones VPN creadas mediante el EIP comparten su ancho de banda. El consumo total de ancho de banda de todas las conexiones VPN no puede superar el ancho de banda del EIP. Si el tráfico de red supera el ancho de banda del EIP, podría producirse congestión e interrupciones en las conexiones VPN. Por lo tanto, asegúrese de configurar suficiente ancho de banda. • Puede configurar reglas de alarma en Cloud Eye para monitorear el ancho de banda. • Puede personalizar el ancho de banda dentro del rango permitido	20 Mbit/s
Avanzado Ajustes	Los parámetros en Configuración avanzada solo están disponibles cuando el Tipo de red está configurado como Red privada. • Seleccionar: Esta opción se aplica al escenario donde las VPC del mismo inquilino están conectadas. Seleccione la VPC de acceso, la subred de acceso, la dirección IP de la puerta de enlace y las etiquetas de la inquilino actual.	Seleccionar
Avanzado Ajustes > Acceso VPC	• Este parámetro solo está disponible cuando Asociar con está configurado en VPC y Tipo de red está configurado en Red privada. Si una puerta de enlace VPN necesita conectarse a diferentes VPC en dirección sur y norte, configure la VPC en dirección norte como la VPC de acceso. La VPC en dirección sur es la VPC asociada a la puerta de enlace VPN.	Igual que la VPC asociada
Avanzado Ajustes > Acceso Subred	• Este parámetro solo está disponible cuando Asociar con está configurado en VPC y Tipo de red está configurado en Red privada. De forma predeterminada, una puerta de enlace VPN utiliza la subred de interconexión para conectarse a la VPC asociada. Configure este parámetro cuando sea necesario usar otra subred.	Igual que la subred de interconexión

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parlamento o	Descripción	Valor de ejemplo
Avanzado Ajustes > Puerta Dirección IP	Este parámetro solo está disponible cuando Asociar con está configurado en VPC y Tipo de red está configurado en Red privada. • Dirección IP autoasignada (predeterminada) Se asignará automáticamente una dirección IP en la subred de acceso a la puerta de enlace VPN. Puede ver la dirección IP asignada automáticamente en la página Puertas de enlace VPN . • Dirección IP especificada manualmente Configure manualmente las direcciones IP en la subred de acceso para la puerta de enlace VPN.	Dirección IP autoasignada
Avanzado Ajustes > Etiquetas	Identificador de un recurso VPN. El valor consta de una clave y un valor. Se puede añadir un máximo de 20 etiquetas. Puede seleccionar etiquetas predefinidas o personalizar etiquetas. Para ver las etiquetas predefinidas, haga clic en Ver etiquetas predefinidas. Configurar etiquetas en Configuración avanzada.	-

Paso 7 Haga clic en Crear ahora.

Paso 8 Confirme la información de la puerta de enlace VPN y haga clic en Enviar.

----Fin

Visualización de una puerta de enlace VPN

Guión

Después de crear una puerta de enlace VPN, puede ver sus detalles.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace VPN.
5. En la página de la pestaña Puertas de enlace VPN S2C , vea la lista de puertas de enlace VPN.
6. Haga clic en el nombre de una puerta de enlace VPN para ver sus detalles.
   – Para una puerta de enlace VPN del tipo de red pública, puede ver la información básica Información y EIPs.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

– Para las puertas de enlace VPN del tipo de red privada, puede ver la información básica
Información y configuración avanzada.

Modificar una puerta de enlace VPN

Guión

Puede modificar información básica sobre una puerta de enlace VPN, incluido el nombre y la subred local.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace VPN.
5. Haga clic en la pestaña Puertas de enlace VPN S2C .
6. Localice la fila que contiene la puerta de enlace VPN de destino y haga clic en Modificar configuración básica.
Información en la columna Operación .

   Para modificar solo el nombre de una puerta de enlace VPN, también puede hacer clic a la derecha del nombre de la puerta de enlace VPN.
7. Modifique el nombre y la subred local de la puerta de enlace VPN según se le solicite.
8. Haga clic en Aceptar.

En la Tabla 3-3 se describen los parámetros para modificar la puerta de enlace VPN.

Tabla 3-3 Parámetros para modificar la puerta de enlace VPN

Parámetro	Descripción	Modificable o no
Nombre	Nombre de una conexión VPN. El valor solo puede contener letras, dígitos, guiones bajos (_), guiones (-) y puntos (.).	Y
Subred local	Subredes de VPC con las que su centro de datos local necesita comunicarse a través de la puerta de enlace del cliente.	Y
Región	Para una baja latencia de red y un acceso rápido a los recursos, seleccione la región más cercana a sus usuarios objetivo. Los recursos no se pueden compartir entre regiones.	norte

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Modificable o no
Asociarse con	Seleccione VPC.	norte
VPC	VPC que se encuentra en las instalaciones El centro de datos necesita acceso.	norte
Interconexión Subred	Esta subred se utiliza para comunicación entre el Puerta de enlace VPN y VPC. Asegúrese de que el seleccionado La subred de interconexión tiene cuatro o más IP asignables direcciones.	norte
ASN de BGP	Número AS BGP.	norte
Modo de facturación	El valor puede ser Pago por usar.	norte
Especificación	Hay dos opciones disponibles: Profesional 1 y Profesional 2.	norte
EL	Una AZ es una zona geográfica Ubicación con independiente fuente de alimentación y red instalaciones en una región. AZ en las mismas VPC son interconectados a través de redes privadas y son físicamente aislado. • Si hay dos o más AZ Disponible, seleccione dos AZ. La puerta de enlace VPN Se ha desplegado en dos zonas de disponibilidad mayor disponibilidad. Tú eres Se recomienda seleccionar las AZ donde los recursos en el Se encuentran las VPC. • Si solo hay una AZ disponible, Seleccione esta AZ.	norte

Vincular un EIP a una puerta de enlace VPN

Guión

Puede vincular EIP a una puerta de enlace VPN que se haya creado.

Procedimiento

1. Inicie sesión en la consola de administración.

Derechos de autor © Huawei Technologies Co., Ltd.

800

Machine Translated by Google

2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace VPN.
5. Haga clic en la pestaña Puertas de enlace VPN S2C .
6. Localice la fila que contiene la puerta de enlace VPN de destino y haga clic en Vincular EIP en La columna Operación .
   – Si la puerta de enlace VPN utiliza el modo activo-activo, la puerta de enlace VPN puede tener un EIP activo y un EIP 2 activo enlazado.
   – Si la puerta de enlace VPN utiliza el modo activo/en espera, la puerta de enlace VPN puede tener un EIP activo y un EIP en espera vinculados.
7. Seleccione el EIP deseado y haga clic en Aceptar.

Desvincular un EIP de una puerta de enlace VPN

Guión

Una vez creada una puerta de enlace VPN, puedes desvincularla de un EIP.

Notas y restricciones

Un EIP que está siendo utilizado por una conexión VPN no puede desvincularse de una puerta de enlace VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace VPN.
5. Haga clic en la pestaña Puertas de enlace VPN S2C .
6. Localice la fila que contiene la puerta de enlace VPN de destino y haga clic en Desenlazar EIP o Seleccione Más > Desvincular EIP en la columna Operación .
   – Si la puerta de enlace VPN utiliza el modo activo-activo, el EIP activo y el EIP 2 activo se pueden desvincular de la puerta de enlace VPN.
   – Si la puerta de enlace VPN utiliza el modo activo/en espera, el EIP activo y el EIP en espera se pueden desvincular de la puerta de enlace VPN.
7. En el cuadro de diálogo que aparece, haga clic en Sí.

NO TE

Se seguirá facturando un EIP después de desvincularlo de una puerta de enlace VPN. Si ya no necesita un EIP, le recomendamos liberarlo.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Eliminar una puerta de enlace VPN

Guión

Puedes eliminar una puerta de enlace VPN que ya no sea necesaria.

Notas y restricciones

- La operación de eliminación no es compatible con una puerta de enlace VPN que se está creando, actualizando o eliminando.
- Si una puerta de enlace VPN tiene conexiones VPN configuradas, debe eliminar todas las Conexiones VPN antes de eliminar la puerta de enlace VPN.

  Para obtener detalles sobre cómo eliminar una conexión VPN, consulte Eliminar una conexión VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace VPN.
5. Si la cantidad de EIP enlazadas es mayor a 1, haga clic en Eliminar en la columna Operación del portal VPN de destino.
6. En el cuadro de diálogo que aparece, haga clic en Sí.

Búsqueda de puertas de enlace VPN por etiqueta

Guión

Al utilizar el servicio VPN, puede clasificar los recursos VPN según reglas específicas para facilitar la gestión de recursos y el cálculo de tarifas.

Con el Servicio de Gestión de Etiquetas (TMS), puede agregar etiquetas a sus recursos VPN para clasificarlos. Además, puede buscar rápidamente recursos VPN por etiqueta en la consola VPN.

Prerrequisitos

Ha agregado etiquetas a los recursos VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

5. Haga clic en el cuadro de texto para seleccionar una propiedad o ingresar una palabra clave, elija una clave de etiqueta en Etiqueta de recurso y seleccione un valor de etiqueta.

– Solo puede seleccionar claves y valores existentes en la lista desplegable.

Puede seleccionar un máximo de 20 etiquetas para buscar recursos VPN. Si selecciona varias etiquetas, la relación entre ellas es AND.

– Puede utilizar etiquetas junto con otros tipos de criterios de filtro. La relación entre ellos es Y.

3.1.2 Administración de la puerta de enlace del cliente de la VPN Enterprise Edition

Creación de una pasarela de clientes

Guión

Para conectar su centro de datos local o red privada a sus ECS en una VPC, debe crear una puerta de enlace de cliente antes de crear una conexión VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace para clientes.
5. En la página Puertas de enlace de clientes , haga clic en Crear puerta de enlace de clientes.
6. Establezca los parámetros según se le solicite y haga clic en Crear ahora.

En la Tabla 3-4 se enumeran los parámetros de la puerta de enlace del cliente.

Tabla 3-4 Descripción de los parámetros de la puerta de enlace del cliente

Parámetro	Descripción	Ejemplo Valor
Nombre	Nombre de una pasarela de clientes. El valor solo puede contener letras, dígitos, guiones bajos (_), guiones (-) y puntos (.).	cgw-001

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Ejemplo Valor
Identificador	• Dirección IP: especifique la dirección IP de la puerta de enlace del cliente. • FQDN: Introduzca un FQDN. El valor es una cadena de 1 a 128 caracteres que distinguen entre mayúsculas y minúsculas, incluyendo letras, dígitos y caracteres especiales (excepto & < > [ ] \). No se admiten espacios. Si la puerta de enlace del cliente no tiene una dirección IP fija, seleccione FQDN. Asegúrese de que el puerto UDP 4500 esté permitido en una regla de firewall en la puerta de enlace del cliente en su centro de datos local o red privada.	• Dirección IP, 1.2.3.4 • FQDN, cgw-fqdn
ASN de BGP	Ingrese el ASN de su centro de datos local o red privada. El ASN BGP de la puerta de enlace del cliente debe ser diferente del de la puerta de enlace VPN.	65000
Avanzado Ajustes > Etiquetas	Identificador de un recurso VPN. El valor consta de una clave y un valor. Se puede añadir un máximo de 20 etiquetas. Puede seleccionar etiquetas predefinidas o personalizar etiquetas. Para ver las etiquetas predefinidas, haga clic en Ver etiquetas predefinidas.	-

7. (Opcional) Si hay dos puertas de enlace de clientes, repita el procedimiento anterior. operaciones para configurar la otra pasarela de clientes con un identificador diferente.

Operaciones relacionadas

Debe configurar un túnel VPN IPsec en el enrutador o firewall de su centro de datos local.

Visualización de una pasarela de clientes

Guión

Después de crear una puerta de enlace de clientes, puede ver sus detalles.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.

Derechos de autor © Huawei Technologies Co., Ltd.

804

Machine Translated by Google

3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace para clientes.
5. En la página Puertas de enlace de clientes , vea la lista de puertas de enlace de clientes.
6. Haga clic en el nombre de una pasarela de clientes para ver sus detalles.
   – En el área de Información básica , puede ver el nombre, ID, BGP ASN, y conexión VPN de la puerta de enlace del cliente.

Modificar una pasarela de clientes

Guión

Después de crear una puerta de enlace de clientes, puede modificar su nombre.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace para clientes.
5. En la página Puertas de enlace del cliente , haga clic en junto al nombre de un cliente Puerta de enlace.
6. Ingrese un nuevo nombre para la puerta de enlace del cliente y haga clic en Aceptar.

   La Tabla 3-5 describe los parámetros relacionados con la puerta de enlace del cliente modificación.

Tabla 3-5 Parámetros relacionados con la modificación de la pasarela del cliente

Parámetro	Descripción	Modificable o no
Nombre	Nombre de una conexión VPN. El valor sólo puede contener letras, dígitos, guiones bajos (_), guiones (-), y puntos (.).	Y
ASN de BGP	El ASN BGP debe ser especificado sólo cuando El modo de enrutamiento está configurado en Dinámico (BGP).	norte

Derechos de autor © Huawei Technologies Co., Ltd.

805

Machine Translated by Google

Parámetro	Descripción	Modificable o no
IP de puerta de enlace DIRECCIÓN	Dirección IP utilizada por la puerta de enlace del cliente para comunicarse con la puerta de enlace VPN. El valor debe ser una dirección estática. Asegúrese de que el puerto UDP 4500 esté permitido en una regla de firewall en la puerta de enlace del cliente en su centro de datos local o red privada.	norte

Eliminar una pasarela de clientes

Guión

Puedes eliminar una pasarela de clientes que hayas creado.

Notas y restricciones

Antes de eliminar una puerta de enlace de cliente asociada a una conexión VPN, elimine la puerta de enlace de cliente de la conexión VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace para clientes.
5. En la página Puertas de enlace de clientes , localice la puerta de enlace de clientes que desea eliminar. y haga clic en Eliminar en la columna Operación .
6. Haga clic en Sí.

Búsqueda de pasarelas de clientes por etiqueta

Guión

Al utilizar el servicio VPN, puede clasificar los recursos VPN según reglas específicas para facilitar la gestión de recursos y el cálculo de tarifas.

Con el Servicio de Gestión de Etiquetas (TMS), puede agregar etiquetas a sus recursos VPN para clasificarlos. Además, puede buscar rápidamente recursos VPN por etiqueta en la consola VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Prerrequisitos

Ha agregado etiquetas a los recursos VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Puertas de enlace para clientes.
5. Haga clic en el cuadro de texto para seleccionar una propiedad o ingresar una palabra clave, elija una clave de etiqueta en Etiqueta de recurso y seleccione un valor de etiqueta.
   – Solo puede seleccionar claves y valores existentes en la lista desplegable.
   Puede seleccionar un máximo de 20 etiquetas para buscar recursos VPN. Si selecciona varias etiquetas, la relación entre ellas es AND.
   – Puede utilizar etiquetas junto con otros tipos de criterios de filtro. La relación entre ellos es Y.

3.1.3 Administración de la conexión VPN de Enterprise Edition

Creación de una conexión VPN

Guión

Para conectar su centro de datos local o red privada a sus ECS en una VPC, debe crear conexiones VPN después de crear una puerta de enlace VPN y una puerta de enlace de cliente.

Notas y restricciones

• Al crear una conexión VPN en modo de enrutamiento estático, asegúrese de que la puerta de enlace del cliente admita ICMP y esté configurada correctamente con la dirección IP de la interfaz del cliente de la conexión VPN antes de habilitar NQA. De lo contrario, no se podrá reenviar el tráfico.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.
5. En la página Conexiones VPN , haga clic en Crear conexión VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

NO TE

Para una mayor confiabilidad, se recomienda crear una conexión VPN entre cada uno de los dos EIP de una puerta de enlace VPN y una puerta de enlace de cliente.

6. Configure los parámetros según se le solicite y haga clic en Comprar ahora.

En la Tabla 3-6 se enumeran los parámetros de conexión VPN.

Tabla 3-6 Descripción de los parámetros de conexión VPN

Parámetro	Descripción	Valor de ejemplo
Nombre	Nombre de una conexión VPN. El valor solo puede contener letras, dígitos, guiones bajos (_), guiones (-) y puntos (.).	vpn-001
Nombre de la puerta de enlace VPN	Nombre de la puerta de enlace VPN para la que se crea la conexión VPN. También puede hacer clic en Comprar S2C VPN Gateway para crear una puerta de enlace VPN. Para obtener detalles sobre los parámetros de configuración, consulte la Tabla 3-2.	vpngw-001
IP de puerta de enlace DIRECCIÓN	Dirección IP de la puerta de enlace VPN. No se puede seleccionar repetidamente el mismo EIP de una puerta de enlace VPN cuando se crean conexiones VPN entre la puerta de enlace VPN y la misma puerta de enlace del cliente.	Puerta de enlace disponible Dirección IP
Cliente Puerta	Nombre de una puerta de enlace de clientes. También puede hacer clic en "Crear pasarela de clientes" para crear una. Para obtener más información sobre los parámetros relacionados, consulte la Tabla 3-4. NOTA Si una puerta de enlace de cliente se conecta a varias puertas de enlace VPN, los ASN BGP y los tipos de VPN de las puertas de enlace VPN deben ser los mismos.	cgw-001

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Tipo de VPN	Modo de conexión IPsec, que puede basarse en rutas o en políticas. • Enrutamiento estático Determina los datos que ingresan al túnel VPN IPsec en función de la configuración de la ruta (subred local y subred del cliente). Escenario de aplicación: Comunicación entre pasarelas de clientes • Enrutamiento BGP Determina el tráfico que puede ingresar al túnel VPN IPsec en función de las rutas BGP. Escenario de aplicación: Comunicación entre puertas de enlace de clientes, subredes de interconexión múltiples o que cambian con frecuencia, o respaldo entre VPN y Conexión directa Basado en políticas: Determina los datos que entran al túnel VPN IPsec según la política (entre la red del cliente y la VPC). Las reglas de política se pueden definir según los bloques CIDR de origen y destino. Escenario de aplicación: Aislamiento entre pasarelas de clientes	Enrutamiento estático

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Cliente Subred	Subred del lado del cliente que necesita acceder a la VPC en la nube a través de conexiones VPN. Si hay varias subredes de clientes, sepárelas con comas (,). NOTA • La subred del cliente puede superponerse con la subred local pero no puede ser el mismo que la subred local. • No se puede crear una subred de cliente Incluido en las subredes existentes de la VPC asociada a la puerta de enlace VPN. Tampoco puede ser la dirección de destino en la tabla de rutas de la VPC asociada a la puerta de enlace VPN. • Las subredes del cliente no pueden ser los bloques CIDR reservados de VPC, por ejemplo, 100.64.0.0/10 o 214.0.0.0/8. • Si la subred de interconexión es asociado con una regla de ACL, asegúrese de que la regla de ACL permita el puerto TCP para el tráfico entre todas las subredes locales y de cliente. • Los grupos de direcciones no se pueden utilizar para Configurar las subredes de origen y destino en una política en los dispositivos de puerta de enlace del cliente.	172.16.1.0/24,172.16.2.0/24

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Interfaz IP DIRECCIÓN Asignación	Este parámetro solo está disponible cuando el tipo de VPN está configurado en enrutamiento estático o enrutamiento BGP. NOTA • Establecer direcciones IP de interfaz a la Direcciones IP de la interfaz de túnel utilizadas por la puerta de enlace VPN y la puerta de enlace del cliente para comunicarse entre sí. • Si la dirección de la interfaz de túnel de la puerta de enlace del cliente es fija, seleccione Especificar manualmente y configure la dirección de la interfaz de túnel de la puerta de enlace VPN en función de la dirección de la interfaz de túnel de la puerta de enlace del cliente. • Especificar manualmente – Configure la Dirección de Interfaz de Túnel Local (DIR) como la dirección de interfaz de túnel de la puerta de enlace VPN, que solo puede residir en el bloque CIDR 169.254.xx/30 (excepto 169.254.195.x/30). A continuación, el sistema configura automáticamente la DIR del Cliente con un valor aleatorio según la configuración de la DIR. Por ejemplo, cuando configura la dirección de interfaz de túnel local en 169.254.1.6/30, el sistema configura automáticamente la dirección de interfaz de túnel del cliente en 169.254.1.5/30. – Cuando configure el tipo de VPN en enrutamiento BGP y configure las direcciones de la interfaz de túnel en el modo de especificación manual , asegúrese de que las direcciones de la interfaz de túnel local y remota configuradas en el dispositivo de puerta de enlace del cliente (el otro extremo de la conexión VPN) sean las mismas que los valores de la dirección de la interfaz de túnel del cliente y la dirección de la interfaz de túnel local, respectivamente. • Asignar automáticamente	Asignar automáticamente

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
	– De forma predeterminada, una dirección IP en El bloque CIDR 169.254.xx/30 se asigna a la interfaz de túnel de la puerta de enlace VPN. – Para ver el automáticamente direcciones IP de interfaz local y de cliente asignadas, haga clic en Modificar conexión VPN en la página Conexiones VPN . – Cuando configura el tipo de VPN en enrutamiento BGP y selecciona Asignar automáticamente, verifica las direcciones de interfaz de túnel local y de cliente asignadas automáticamente después de crear la conexión VPN. Asegúrese de que las direcciones de interfaz de túnel local y remota configuradas en el dispositivo de puerta de enlace del cliente (el otro extremo de la conexión VPN) sean inversas a las configuraciones en el lado de la nube.	
Túnel local Interfaz DIRECCIÓN	Este parámetro solo está disponible cuando la Asignación de dirección IP de interfaz está configurada en Especificar manualmente. Dirección IP de la interfaz de túnel configurada en la puerta de enlace VPN.	N / A
Cliente Túnel Interfaz DIRECCIÓN	Este parámetro solo está disponible cuando la Asignación de dirección IP de interfaz está configurada en Especificar manualmente. Dirección IP de la interfaz del túnel configurada en el dispositivo de puerta de enlace del cliente.	N / A

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Detección de enlace	Este parámetro está disponible sólo cuando el tipo de VPN se establece en estático enrutamiento. NOTA Al habilitar esta función, asegúrese de que que la pasarela de clientes admite ICMP y está configurado correctamente con la dirección IP de la interfaz del cliente Conexión VPN. De lo contrario, el tráfico... no se pudo reenviar Una vez habilitada esta función, el Puerta de enlace VPN automática Realiza análisis de calidad de red (NQA) en la interfaz IP del cliente Dirección de la pasarela del cliente.	Seleccionado
PSK	Las PSK configuradas para la VPN puerta de enlace y puerta de enlace del cliente debe ser el mismo El PSK: • Contiene de 8 a 128 caracteres. • Puede contener solo tres o más tipos de los siguientes caracteres: – Dígitos – Letras mayúsculas – Letras minúsculas – Caracteres especiales: ~ ! @ # $ % ^ ( ) - + = {} , . / : ;	Prueba@123
Confirmar PSK	Ingrese el PSK nuevamente.	Prueba@123

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor de ejemplo
Política	Este parámetro solo está disponible cuando el tipo de VPN está configurado como Basado en políticas. Define el flujo de datos que entra en la conexión VPN cifrada entre las subredes local y del cliente. Debe configurar los bloques CIDR de origen y destino en cada regla de política. De forma predeterminada, se puede configurar un máximo de cinco reglas de política. • Bloque CIDR de origen El bloque CIDR de origen debe contener algunos bloques CIDR de las subredes locales. 0.0.0.0/0 indica cualquier dirección IP. • Bloque CIDR de destino: El bloque CIDR de destino debe contener todos los bloques CIDR de las subredes del cliente. Una regla de política admite un máximo de cinco bloques CIDR de destino, separados por comas (,).	• Bloque CIDR de origen 1: 192.168.1.0/24 • Bloque CIDR de destino 1: 172.16.1.0/24,17 2.16.2.0/24 • Bloque CIDR de origen 2: 192.168.2.0/24 • Bloque CIDR de destino 2: 172.16.1.0/24,17 2.16.2.0/24
Configuración de políticas	• Predeterminado: utiliza políticas IKE e IPsec predeterminadas. • Personalizado: utiliza políticas IKE y IPsec personalizadas. Políticas IPsec. Para más detalles sobre las políticas, consulte las Tablas 3-7 y 3-8.	Costumbre
Avanzado Ajustes > Etiquetas	Identificador de un recurso VPN. El valor consta de una clave y un valor. Se puede agregar un máximo de 20 etiquetas. Puede seleccionar etiquetas predefinidas o personalizar etiquetas. Para ver las etiquetas predefinidas, haga clic en Ver etiquetas predefinidas.	-

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Tabla 3-7 Política de IKE

Parámetro	Descripción	Ejemplo Valor
Versión	Versión del protocolo IKE. El valor puede ser uno de los siguientes: • v1 (v1 tiene baja seguridad. Si el dispositivo es compatible con v2, se recomienda v2). • versión 2 El valor predeterminado es v2.	versión 2
Modo de negociación	Este parámetro solo está disponible cuando la versión es v1. • Principal • Agresivo	Principal
Autenticación Algoritmo	Algoritmo hash utilizado para la autenticación. Las siguientes opciones están disponibles: • SHA1 (Inseguro. No recomendado). • MD5 (Inseguro. No recomendado). • SHA2-256 • SHA2-384 • SHA2-512 El valor predeterminado es SHA2-256.	SHA2-256
Cifrado Algoritmo	Algoritmo de cifrado. Están disponibles las siguientes opciones: • 3DES (Inseguro. No recomendado). • AES-128 (Inseguro. No recomendado). • AES-192 (Inseguro. No recomendado). • AES-256 (inseguro. No recomendado). • AES-128-GCM-16 • AES-256-GCM-16 Cuando se utiliza este algoritmo de cifrado, la versión de IKE solo puede ser v2. El valor predeterminado es AES-128.	AES-128

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Ejemplo Valor
Algoritmo DH	Se admiten los siguientes algoritmos: • Grupo 1 (inseguro. No recomendado). • Grupo 2 (inseguro. No recomendado). • Grupo 5 (Inseguro. No recomendado). • Grupo 14 (Inseguro. No recomendado). • Grupo 15 • Grupo 16 • Grupo 19 • Grupo 20 • Grupo 21 El valor predeterminado es el Grupo 15.	Grupo 15
Duración de la vida (s)	Duración de una asociación de seguridad (SA). Una SA se renegociará cuando expire su vigencia. • Unidad: segundo • El valor varía de 60 a 604800. • El valor predeterminado es 86400.	86400
Identificación local	Identificador de autenticación de la puerta de enlace VPN utilizado en la negociación de IPsec. El ID de la puerta de enlace VPN configurado en la puerta de enlace del cliente debe ser el mismo que el ID local configurado aquí. De lo contrario, la negociación de IPsec falla. • Dirección IP (valor predeterminado) El sistema establece automáticamente este parámetro en el EIP seleccionado de la puerta de enlace VPN. • FQDN Establezca el FQDN en una cadena de 1 a 128 caracteres sensibles a mayúsculas y minúsculas que puede contener letras, dígitos y caracteres especiales (excluyendo &, <, >, [,], \, ? y espacios).	Dirección IP

Derechos de autor © Huawei Technologies Co., Ltd.

816

Machine Translated by Google

Parámetro	Descripción	Ejemplo Valor
ID de cliente	Identificador de autenticación de la pasarela de clientes utilizado en la negociación de IPsec. El ID de la pasarela de clientes configurado en la pasarela de clientes debe ser el mismo que el configurado aquí. De lo contrario, la negociación de IPsec falla. • Dirección IP (valor predeterminado) El sistema establece automáticamente este parámetro en la dirección IP de la puerta de enlace del cliente. • FQDN Establezca el FQDN en una cadena de 1 a 128 caracteres que distinguen entre mayúsculas y minúsculas y que puede contener letras, dígitos y caracteres especiales (excluyendo &, <, >, [,], \, ? y espacios).	Dirección IP

Tabla 3-8 Política IPsec

Parámetro	Descripción	Ejemplo Valor
Autenticación Algoritmo	Algoritmo hash utilizado para la autenticación. Están disponibles las siguientes opciones: • SHA1 (Inseguro. No recomendado). • MD5 (Inseguro. No recomendado). • SHA2-256 • SHA2-384 • SHA2-512 El valor predeterminado es SHA2-256.	SHA2-256

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Ejemplo Valor
Cifrado Algoritmo	Algoritmo de cifrado. Están disponibles las siguientes opciones: • 3DES (Inseguro. No recomendado). • AES-128 (Inseguro. No recomendado). • AES-192 (Inseguro. No recomendado). • AES-256 (Inseguro. No recomendado). • AES-128-GCM-16 • AES-256-GCM-16 El valor predeterminado es AES-128.	AES-128
PFS	Algoritmo utilizado por la función Perfect forward secrecy (PFS). PFS admite los siguientes algoritmos: • Deshabilitar (Inseguro. No recomendado). • Grupo DH 1 (Inseguro. No recomendado). • Grupo DH 2 (Inseguro. No recomendado). • Grupo DH 5 (Inseguro. No recomendado). • Grupo DH 14 (Inseguro. No recomendado). • Grupo DH 15 • Grupo DH 16 • Grupo DH 19 • Grupo DH 20 • Grupo DH 21 El valor predeterminado es el grupo DH 15.	Grupo DH 15
Protocolo de transferencia	Protocolo de seguridad utilizado en IPsec para transmitir y encapsular datos del usuario. Se admiten los siguientes protocolos: • ESP El valor predeterminado es ESP.	ESP

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Ejemplo Valor
Duración de la vida (s)	Duración de la vida de un SA. Una SA se renegociará cuando expire su vigencia. • Unidad: segundo • El valor varía de 30 a 604800. • El valor predeterminado es 3600.	3600

NO TE

Una política IKE especifica los algoritmos de cifrado y autenticación que se utilizarán en la fase de negociación de un túnel IPsec. Una política IPsec especifica el protocolo, el algoritmo de cifrado y el algoritmo de autenticación que se utilizarán en la fase de transmisión de datos de un túnel IPsec. La configuración de la política para las conexiones VPN debe ser la misma en la VPC y en el centro de datos local. Si difieren, la negociación de la VPN fallará, lo que impedirá el establecimiento de las conexiones VPN.

No se recomiendan los siguientes algoritmos por su falta de seguridad: • Algoritmos de autenticación: SHA1 y MD5 • Algoritmos de cifrado: 3DES, AES-128, AES-192 y AES-256. Dado que algunos dispositivos de clientes no son compatibles con algoritmos de cifrado seguros, el algoritmo de cifrado predeterminado para las conexiones VPN sigue siendo AES-128. Se recomienda usar un algoritmo de cifrado más seguro si los dispositivos de clientes son compatibles con algoritmos de cifrado seguros. • Algoritmos DH: Grupo 1, Grupo 2, Grupo 5 y Grupo 14

7. Confirme la configuración de la conexión VPN y haga clic en Enviar.
8. Repita las operaciones anteriores para crear la otra conexión VPN.

Para obtener detalles sobre la configuración de la dirección IP, consulte Contexto.

Configuración de la comprobación de estado

Guión

Tras crear las conexiones VPN, puede configurar la comprobación del estado para que la puerta de enlace VPN envíe paquetes de prueba a la puerta de enlace del cliente y recopile estadísticas sobre el tiempo de ida y vuelta y la tasa de pérdida de paquetes de los enlaces físicos. Estas estadísticas le ayudan a conocer la calidad de la conexión VPN. El servicio Cloud Eye monitoriza el tiempo de ida y vuelta y la tasa de pérdida de paquetes de los enlaces VPN. Para obtener más información, consulte 3.3.1 Métricas (VPN S2C Enterprise Edition).

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.
5. En la página Conexiones VPN , haga clic en el nombre de la conexión VPN de destino.
   En la página de la pestaña Resumen , haga clic en Agregar en el área Comprobación de estado .
6. En el cuadro de diálogo Agregar comprobación de estado , haga clic en Aceptar.

Visualización de una conexión VPN

Guión

Después de crear una conexión VPN, puedes ver sus detalles.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.
5. En la página Conexiones VPN , vea la lista de conexiones VPN.
6. Haga clic en el nombre de una conexión VPN para ver su información básica y política. configuración.

NO TE

- En la lista de conexiones VPN, ubique la conexión VPN de destino y elija Más > Modificar configuración de políticas a la derecha para ver las políticas IKE e IPsec de la conexión VPN.

Modificar una conexión VPN

Guión

Una conexión VPN es un canal de comunicaciones cifrado que se establece entre una puerta de enlace VPN en una VPC y una puerta de enlace de cliente en su centro de datos local.
Puede modificar una conexión VPN cuando sea necesario.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.
5. En la página Conexiones VPN , busque la conexión VPN que desea modificar y haga clic en Modificar conexión VPN o Modificar configuración de política.
6. Modifique los parámetros de conexión VPN según se le solicite.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

7. Haga clic en Aceptar.

PRECAUCIÓN

Si cambia la clave PSK o modifica la política IKE o IPsec de una conexión VPN, asegúrese de que las nuevas configuraciones coincidan con las de la puerta de enlace del cliente. De lo contrario, la conexión VPN se interrumpirá.

Sólo algunos de los parámetros tienen efecto inmediatamente después de ser modificados, como se describe en la Tabla 3-9.

Tabla 3-9 Momento en que entran en vigor las nuevas configuraciones de parámetros

Artículo	Parámetro	Cuándo entran en vigor las nuevas configuraciones	Cómo modificar
-	PSK	• Cuando se utiliza IKEv1, la nueva configuración entra en vigor en el siguiente período de negociación. • Cuando se utiliza IKEv2, la nueva configuración entra en vigor después de que se restablezca la conexión VPN.	• Cuando se utiliza IKEv1: Localice la conexión VPN que desea modificar, seleccione Más > Restablecer PSK a la derecha y cambie el PSK según se le solicite. • Cuando se utiliza IKEv2: 1. Eliminar la conexión VPN actual. 2. Cree una nueva conexión VPN.
Política IKEv1	Cifrar ion El algoritmo hm	La nueva configuración entrará en vigor en el siguiente período de negociación.	Localice la conexión VPN que desea modificar y haga clic en Modificar configuración VPN.
	Autenticación El algoritmo hm		
	DH El algoritmo hm		
	Negocio Modo		
	Local		
	La costumbre es identificación		

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Artículo	Parámetro tener	Cuándo entran en vigor las nuevas configuraciones	Cómo modificar
	Vida útil e(s)		
	Versión Los nuevos ajustes entran en vigor inmediatamente.		
Política IKEv2	Cifrar ion El algoritmo hm	La nueva configuración entrará en vigor en el siguiente período de negociación.	Localice la conexión VPN que desea modificar y haga clic en Modificar configuración VPN.
	Autenticación El algoritmo hm		
	DH El algoritmo hm		
	Vida útil e(s)		
	Versión Los nuevos ajustes entran en vigor inmediatamente.		
	Local	La nueva configuración entrará en vigor después de que se restablezca la conexión VPN.	1. Eliminar la VPN actual conexión. 2. Cree una nueva conexión VPN.
	La costumbre es identificación		
Política IPsec	Cifrar ion El algoritmo hm	La nueva configuración entrará en vigor en el siguiente período de negociación.	Localice la conexión VPN que desea modificar y haga clic en Modificar configuración VPN.
	Autenticación El algoritmo hm		
	PFS		
	Vida útil e(s)		
	Transferir Protocolo l	Este parámetro no se puede modificar en la consola de administración.	

En la Tabla 3-10 se describen los parámetros relacionados con la modificación de la conexión VPN.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Tabla 3-10 Parámetros relacionados con la modificación de la conexión VPN

Parámetro	Descripción	Modificable o no
Nombre	Nombre de una conexión VPN. El valor solo puede contener letras, dígitos, guiones bajos (_), guiones (-) y puntos (.).	Y
Cliente Puerta	Puerta de enlace utilizada para comunicarse con una VPC a través de VPN.	Y
Subred del cliente Subred en el	centro de datos local que necesita acceder a la VPC.	Y
Configuración de políticas	Existen políticas IKE e IPsec.	Y
PSK	Las PSK configuradas para la puerta de enlace VPN y la puerta de enlace del cliente deben ser las mismas.	Y
Puerta de enlace VPN	Puerta de enlace VPN que se ha creado.	norte
IP de puerta de enlace DIRECCIÓN	Dirección IP utilizada por la puerta de enlace del cliente para comunicarse con la puerta de enlace VPN. El valor debe ser una dirección estática. Asegúrese de que el puerto UDP 4500 esté permitido en una regla de firewall en la puerta de enlace del cliente en su centro de datos local o red privada.	norte
Interfaz IP DIRECCIÓN Asignación	Modo de asignación de direcciones IP de las interfaces local y de cliente. Las opciones incluyen Especificar manualmente y Asignar automáticamente.	norte
Túnel local Dirección de interfaz	Dirección IP de la interfaz de túnel configurada en la puerta de enlace VPN.	norte
Túnel del cliente Dirección de interfaz	Dirección IP de la interfaz del túnel configurada en el dispositivo de puerta de enlace del cliente.	norte

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Eliminar una conexión VPN

Guión

Si ya no necesita una conexión VPN, puede eliminarla para liberar espacio en la red.
recursos.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.
5. En la página Conexiones VPN , localice la fila que contiene la VPN de destino conexión y seleccione Más > Eliminar.
6. En el cuadro de diálogo que aparece, haga clic en Sí.

Búsqueda de conexiones VPN por etiqueta

Guión

Al utilizar el servicio VPN, puede clasificar los recursos VPN según reglas específicas para facilitar la gestión de recursos y el cálculo de tarifas.

Con el Servicio de Gestión de Etiquetas (TMS), puede agregar etiquetas a sus recursos VPN para clasificarlos. Además, puede buscar rápidamente recursos VPN por etiqueta en la consola VPN.

Prerrequisitos

Ha agregado etiquetas a los recursos VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda y seleccione > Red Privada Virtual.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Empresa – Conexiones VPN.
5. Haga clic en el cuadro de texto para seleccionar una propiedad o ingresar una palabra clave, elija una clave de etiqueta en Etiqueta de recurso y seleccione un valor de etiqueta.
   – Solo puede seleccionar claves y valores existentes en la lista desplegable.
   Puede seleccionar un máximo de 20 etiquetas para buscar recursos VPN. Si selecciona varias etiquetas, la relación entre ellas es AND.
   – Puede utilizar etiquetas junto con otros tipos de criterios de filtro. La relación entre ellos es Y.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

3.2 VPN clásica

3.2.1 Administración de la puerta de enlace VPN clásica

Visualización de una puerta de enlace VPN

Escenarios

Después de crear una puerta de enlace VPN, puede ver sus detalles.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
3. En el panel de navegación de la izquierda, seleccione Red privada virtual.

   Si Enterprise Edition VPN está disponible para la región seleccionada, elija Red privada virtual > Clásica.
4. Ver la información de la puerta de enlace VPN.

Modificar una puerta de enlace VPN

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
3. En el panel de navegación de la izquierda, seleccione Red privada virtual.

   Si Enterprise Edition VPN está disponible para la región seleccionada, elija Red privada virtual > Clásica.
4. En la página Puertas de enlace VPN , localice la fila que contiene la puerta de enlace VPN de destino y haga clic en Modificar en la columna Operación .
5. Modifique el nombre o la descripción de la puerta de enlace VPN según sea necesario.
6. Haga clic en Aceptar.

Modificar la información básica de una puerta de enlace VPN

Guión

Puede modificar el nombre y la descripción de una puerta de enlace VPN.

Procedimiento

1. Inicie sesión en la consola de administración.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
4. En el panel de navegación de la izquierda, seleccione Red privada virtual > Clásica – Puertas de enlace VPN.

   Si Enterprise Edition VPN está disponible para la región seleccionada, elija Red privada virtual > Clásica.
5. Localice la fila que contiene la puerta de enlace VPN que desea modificar y elija Más > Modificar información básica en la columna Operación .
6. Modifique el nombre o la descripción de la puerta de enlace VPN según sea necesario.

   NO TE

   El nombre de una puerta de enlace VPN solo puede contener letras, dígitos, guiones bajos (_), guiones (-) y puntos (.).
7. Haga clic en Aceptar.

Eliminar una puerta de enlace VPN

Escenarios

Si ya no se necesita una puerta de enlace VPN, puede eliminarla para liberar recursos de red siempre que no tenga conexiones VPN configuradas.

Si tiene alguna conexión configurada, elimínela primero.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
3. En el panel de navegación de la izquierda, seleccione Red privada virtual > Clásico – Puertas de enlace VPN.

   Si Enterprise Edition VPN está disponible para la región seleccionada, elija Red privada virtual > Clásica.
4. Ubique la fila que contiene la puerta de enlace VPN de destino y seleccione Más > Eliminar en la columna Operación .

   Si Enterprise Edition VPN está disponible para la región seleccionada, ubique la fila que contiene la puerta de enlace VPN de destino y elija Más > Eliminar.
5. En el cuadro de diálogo que aparece, haga clic en Sí.

3.2.2 Gestión de la conexión VPN clásica

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Visualización de una conexión VPN

Escenarios

Después de crear una conexión VPN, puedes ver sus detalles.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
3. En el panel de navegación de la izquierda, seleccione Red privada virtual > Clásica – Conexiones VPN.

   Si la VPN Enterprise Edition está disponible para la región seleccionada, seleccione Red Privada Virtual > Clásica. A continuación, haga clic en la pestaña Conexiones VPN .
4. Vea la información de la conexión VPN. También puede localizar la fila que...

   contiene la conexión VPN de destino y haga clic en Ver política en la columna Operación para ver los detalles de la política IKE e IPsec de la conexión VPN.

Modificar una conexión VPN

Escenarios

Una conexión VPN es un canal de comunicación cifrado que se establece entre la puerta de enlace VPN de su VPC y la de un centro de datos local. La conexión VPN se puede modificar después de su creación.

PRECAUCIÓN

Si modifica la configuración avanzada, las comunicaciones de red podrían interrumpirse. Tenga cuidado al realizar esta operación.

Cambiar la clave PSK no eliminará la conexión VPN actual. La nueva clave PSK entra en vigor durante la renegociación de IKE, una vez finalizada su vida útil.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
3. En el panel de navegación de la izquierda, seleccione Red privada virtual > Clásica – Conexiones VPN.

   Si la VPN Enterprise Edition está disponible para la región seleccionada, seleccione Red Privada Virtual > Clásica. A continuación, haga clic en la pestaña Conexiones VPN .

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

4. Localice la fila que contiene la conexión VPN de destino y haga clic en Modificar en La columna Operación .
5. En el cuadro de diálogo Modificar conexión VPN que se muestra , modifique los parámetros según sea necesario.

   NO TE

   El nombre de una puerta de enlace VPN solo puede contener letras, dígitos, guiones bajos (_), guiones (-) y puntos (.).

6. Haga clic en Aceptar.

Eliminar una conexión VPN

Escenarios

Si ya no necesita una conexión VPN, puede eliminarla para liberar espacio en la red. recursos.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda, seleccione una región y elija Red > Red privada virtual.

   Se muestra la consola VPN.
3. En el panel de navegación de la izquierda, seleccione Red privada virtual > Clásica – Conexiones VPN.

   Si la VPN Enterprise Edition está disponible para la región seleccionada, seleccione Red Privada Virtual > Clásica. A continuación, haga clic en la pestaña Conexiones VPN .
4. Ubique la fila que contiene la conexión VPN de destino y seleccione Más > Eliminar en la columna Operación .
5. En el cuadro de diálogo que aparece, haga clic en Sí.

3.3 Monitoreo

3.3.1 Métricas (VPN S2C Enterprise Edition)

Descripción

Esta sección describe las métricas monitorizadas que VPN reporta a Cloud Eye, así como sus espacios de nombres y dimensiones. Puede usar la consola de administración de Cloud Eye para consultar las métricas de los objetos monitorizados y las alarmas generadas para VPN.

Espacio de nombres

SYS.VPN

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Métrica

Tabla 3-11 Métricas compatibles con las puertas de enlace VPN de Enterprise Edition

ID de métrica	Métrico Nombre	Descripción	Dolor y Corrió ge	Advertencia roja Objeto	Monitorizar intervalo g (Crudo Datos)
gateway_sen d_pkt_rate	Outbo y Paquete Tasa	Número promedio de paquetes de datos que salen de la nube por segundo.	≥ 0 Págs.	Puerta de enlace y	1 minuto
tasa de paquetes de recepción de puerta de enlace	Entrada d Paquete Tasa	Número promedio de paquetes de datos que ingresan a la nube por segundo.	≥ 0 Págs.	Puerta de enlace y	1 minuto
velocidad de transmisión de señales de puerta de enlace	Outbo y Ancho de banda	Volumen promedio de tráfico que sale de la nube por segundo.	0–1 Gbit/ s	Puerta de enlace y	1 minuto
tasa de recepción de puerta de enlace	Entrada d Ancho de banda	Volumen promedio de tráfico que ingresa a la nube por segundo.	0–1 Gbit/ s	Puerta de enlace y	1 minuto
Uso de la tasa de transmisión del sensor de puerta de enlace	Outbo y Ancho de banda Uso	Utilización del ancho de banda para el tráfico que sale de la nube.	0-10 0%	Puerta de enlace y	1 minuto
tasa de recepción de puerta de enlace	Entrada d Ancho de banda Uso	Utilización del ancho de banda para el tráfico que ingresa a la nube.	0-10 0%	Puerta de enlace y	1 minuto
número de conexión de puerta de enlace	Numb es de Conexiones	Número de conexiones VPN.	≥ 0	Puerta de enlace y	1 minuto

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Tabla 3-12 Métricas de conexión VPN de Enterprise Edition

ID de métrica	Métrico Nombre	Descripción	Valor Sonó y	Muchos bonitos Objeto el	Monitorizar intervalo g (Crudo Datos)
latencia de edad promedio del túnel	Promedio Túnel RTT	Tiempo promedio de ida y vuelta en el túnel entre la puerta de enlace VPN y la puerta de enlace del cliente.	0–5000 EM	VPN estúpido cción	1 minuto
latencia máxima del túnel	Túnel máximo RTT	Tiempo máximo de ida y vuelta en el túnel entre la puerta de enlace VPN y la puerta de enlace del cliente.	0–5000 EM	VPN conexión	1 minuto
tasa de pérdida y paquete de túnel	Túnel Paquete Tasa de pérdida	Tasa de pérdida de paquetes en el túnel entre la puerta de enlace VPN y la puerta de enlace del cliente.	0–100 %	VPN estúpido cción	1 minuto
latencia promedio del enlace	Promedio Enlace RTT	Tiempo promedio de ida y vuelta en el enlace físico entre la puerta de enlace VPN y la puerta de enlace del cliente.	0–5000 EM	VPN estúpido cción	1 minuto
latitud máxima del enlace	Enlace máximo RTT	Tiempo máximo de ida y vuelta en el enlace físico entre la puerta de enlace VPN y la puerta de enlace del cliente.	0–5000 EM	VPN estúpido cción	1 minuto
tasa de pérdida de paquetes de enlace	Enlace Paquete Tasa de pérdida	Tasa de pérdida de paquetes en el enlace físico entre la puerta de enlace VPN y la puerta de enlace del cliente.	0–100 %	VPN estúpido cción	1 minuto
estado de conexión	VPN Conecte on Status	Estado de una conexión VPN: 0: no conectado 1: conectado 2: desconocido	0, 1 o 2	VPN estúpido cción	1 minuto
receptor_pt_rata y	Paquete Recibir Tasa	Número promedio de paquetes de datos recibidos por segundo.	≥ 0 Págs.	VPN estúpido cción	1 minuto
enviar_paquete_rata y	Paquete Enviar Tasa	Número promedio de paquetes de datos enviados por segundo.	≥ 0 Págs.	VPN estúpido cción	1 minuto

Derechos de autor © Huawei Technologies Co., Ltd.

830

Machine Translated by Google

ID de métrica	Métrico Nombre	Descripción	Valor Sonó y	Muchos bonitos Objeto	Monitorizar intervalo g (Crudo Datos)
tasa de recepción	Tráfico Recibir Tasa	Volumen promedio de tráfico recibido por segundo.	0~1 Gbit/s	VPN estúpido cción	1 minuto
tasa de envío	Tráfico Enviar Tasa	Volumen promedio de tráfico enviado por segundo.	0~1 Gbit/s	VPN estúpido cción	1 minuto

Dimensiones

llave	Valor
id_de_conexión_evpn	Conexión VPN de Enterprise Edition
id. de puerta de enlace evpn	Puerta de enlace VPN de edición empresarial

3.3.2 Visualización de métricas

Escenarios

Consulta el estado de la conexión VPN y el uso del ancho de banda y EIP. Puedes ver datos de las últimas 1, 3, 12 o 24 horas, o de los últimos 7 días.

Visualización de métricas de la puerta de enlace VPN

- Visualización de métricas en la consola VPN
  a. Inicie sesión en la consola de administración.
  b. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseados.
  c. Haga clic en la esquina superior izquierda de la consola de administración y seleccione Red > Red privada virtual.
  d. Ver métricas.
     - VPN: Elija Red privada virtual > Empresa – VPN
       Puertas de enlace > Puertas de enlace VPN S2C y haga clic en la columna Dirección IP de la puerta de enlace de una puerta de enlace VPN. Puede ver las métricas de dos EIP por separado.
       Las métricas son métricas EIP, que incluyen ancho de banda de salida, ancho de banda de entrada, uso de ancho de banda de entrada, uso de ancho de banda de salida, tráfico de salida y tráfico de entrada.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Visualización de las métricas de la conexión VPN

- Visualización de métricas en la consola VPN
  a. Inicie sesión en la consola de administración.
  b. Haga clic en la esquina superior izquierda y seleccione la región deseada y en proyecto.
  c. Haga clic en la esquina superior izquierda de la consola de administración y seleccione Red > Red privada virtual.
  d. Ver métricas.
     - VPN: Elija Red privada virtual > Empresa – VPN
       Conexiones y haga clic en Ver métrica debajo del nombre de una conexión VPN.

       Las métricas incluyen lo siguiente:
       - Estado de la conexión VPN
       - RTT de enlace promedio, RTT de enlace máximo, tasa de pérdida de paquetes de enlace

         Estas métricas solo se muestran después de habilitar la función de comprobación de estado. Para habilitarla, haga clic en el nombre de una conexión VPN y agregue elementos de comprobación de estado en la pestaña Resumen .

       - RTT promedio del túnel, RTT máximo del túnel, pérdida de paquetes del túnel Tasa

         Estas métricas se muestran solo cuando el tipo de VPN está configurado en Enrutamiento estático y la función NQA está habilitada.

3.3.3 Creación de reglas de alarma

Escenarios

Puede crear reglas de alarma para personalizar los objetos monitoreados y las políticas de notificación, de modo que pueda estar bien informado del estado del servicio VPN.

Procedimiento

1. Inicie sesión en la consola de administración.
2. Haga clic en la esquina superior izquierda y seleccione la región y el proyecto deseado.
3. Haga clic en la esquina superior izquierda de la consola de administración y seleccione en Administración y gobernanza > Cloud Eye.
4. Elija Monitoreo de servicios en la nube > Red privada virtual y configure Reglas de alarma para diferentes tipos de alarmas según sea necesario.
   – Alarmas relacionadas con puertas de enlace VPN en S2C Enterprise Edition VPN: haga clic en la pestaña Puerta de enlace VPN de S2C y haga clic en Crear regla de alarma en la columna Operación de una puerta de enlace VPN.
   – Alarmas relacionadas con conexiones VPN en S2C Enterprise Edition VPN: haga clic en la pestaña Conexión VPN de S2C y haga clic en Crear regla de alarma en la columna Operación de una conexión VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

5. Configure una regla de alarma en la página Crear regla de alarma .
6. Haga clic en Crear.

Después de crear la regla de alarma, si ha habilitado la Notificación de alarma y
Una vez configurados los parámetros requeridos, recibirá notificaciones una vez que se active una alarma.
motivado.

NO TE

Para obtener más información sobre las reglas de alarma de VPN, consulte la Nube Ojo Guía del usuario.

3.4 Auditoría

3.4.1 Operaciones VPN que pueden ser grabadas por CTS

Tabla 3-13 Operaciones relacionadas con la VPN de S2C Enterprise Edition que se pueden grabar por CTS

Operación	Nombre de seguimiento	del tipo de recurso
Creando una puerta de enlace del cliente	puerta de enlace del cliente	crearCgw
Actualizando una puerta de enlace del cliente	puerta de enlace del cliente	updateCgw
Eliminar un puerta de enlace del cliente	puerta de enlace del cliente	eliminarCgw
Creando una VPN puerta	puerta de enlace VPN	crearVgw
Actualizar una VPN puerta	puerta de enlace VPN	actualizaciónVgw
Eliminar una VPN puerta	puerta de enlace VPN	eliminarVgw
Actualizar la VPN estado de la puerta de enlace	puerta de enlace VPN	ActualizarEstadoDeRecursos
Creando una VPN conexión	conexión VPN	crearConexiónVPN
Actualizar una VPN conexión	actualización de conexión VPN	
Eliminar una VPN conexión	conexión VPN	eliminarConexiónVPN
Creando una etiqueta de recurso	instancia	crearEtiquetaDeRecurso
Eliminar un etiqueta de recurso	instancia	eliminarRecursoEtiqueta

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

3.5 Gestión de permisos

3.5.1 Creación de un usuario y concesión de permisos de VPN

Utilice la Gestión de Identidad y Acceso (IAM) Servicio para implementar un control de permisos detallado sobre sus recursos VPN. Con IAM, puede:

- Cree usuarios de IAM para empleados según la organización de su empresa Estructura. Cada usuario de IAM tendrá sus propias credenciales de seguridad para acceder a los recursos VPN.
- Otorgar a los usuarios únicamente los permisos necesarios para realizar una tarea determinada en función de sus responsabilidades laborales.
- Otorgue permiso para realizar operaciones y mantenimiento profesionales y eficientes en su VPN recursos a otras cuentas o servicios en la nube.

Si su cuenta cumple con los requisitos de permisos, puede omitir esta sección.

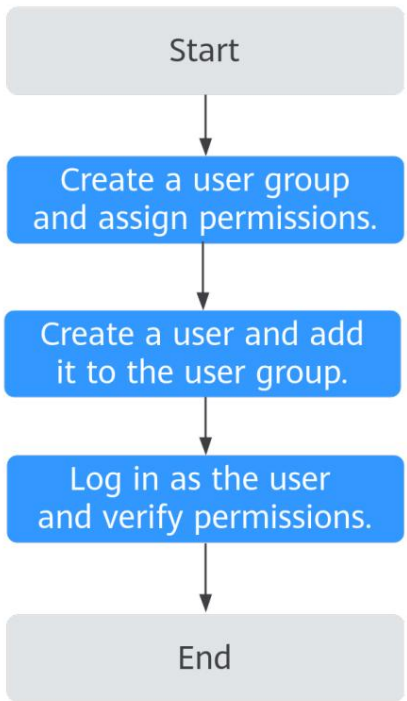
Esta sección describe el procedimiento para otorgar permisos (ver Figura 3-1).

Prerrequisitos

Ha aprendido sobre los permisos que admite la VPN y ha determinado los permisos que se otorgarán a un grupo de usuarios. Antes de otorgar permisos a otros servicios, infórmese sobre todos los permisos. con apoyo de IAM.

Flujo del proceso

Figura 3-1 Proceso de concesión de permisos de VPN



Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

1. Cree un grupo de usuarios y asigne permisos lo.

   Cree un grupo de usuarios en la consola IAM y adjunte la política de administrador de VPN al grupo.

2. Cree un usuario y agréguelo al grupo de usuarios.

   Cree un usuario en la consola IAM y agréguelo al grupo creado en 1.

3. Iniciar sesión y verificar los permisos.

   Inicie sesión en la consola de administración con el usuario creado. Cambie a la región autorizada y verifique los permisos.

   – Haga clic en Lista de servicios y seleccione Redes > Red privada virtual.
   En la página Enterprise – Puertas de enlace VPN , haga clic en "Comprar puerta de enlace VPN" en la esquina superior derecha. Si la puerta de enlace VPN se creó correctamente, la política del administrador de VPN ya se habrá aplicado.

   – Seleccione cualquier otro servicio en la Lista de Servicios. Si aparece un mensaje indicando que no tiene suficientes permisos para acceder al servicio, la política del Administrador de VPN ya se ha aplicado.

3.5.2 Políticas personalizadas de VPN

Se pueden crear políticas personalizadas para complementar las políticas definidas por el sistema de VPN.

Puede crear políticas personalizadas de cualquiera de las siguientes maneras:

• Editor visual: seleccione servicios en la nube, acciones, recursos y condiciones de solicitud.
Esto no requiere conocimiento de la sintaxis de políticas. •

JSON: edite políticas JSON desde cero o en función de una política existente.

Para obtener más detalles, consulte Creación de una política personalizada. La siguiente sección contiene ejemplos de políticas personalizadas de VPN comunes.

Ejemplo de política VPN personalizada •

Ejemplo 1: Otorgar permiso para eliminar puertas de enlace VPN.

```
{
    "Versión": "1.1",
    "Declaración":
        [ {
            "Efecto": "Permitir",
            "Acción":
                [ "vpn:vpnGateways:eliminar"
            ]
        }
    ]
}
```

• Ejemplo 2: Denegar la eliminación de la conexión VPN.

Una política con solo permisos de "Denegar" debe usarse junto con otras políticas. Si los permisos otorgados a un usuario de IAM contienen tanto "Permitir" como "Denegar", los permisos de "Denegar" prevalecen sobre los de "Permitir".

El siguiente método se puede usar si necesita asignar permisos de la política VPN FullAccess a un usuario, pero también prohibirle eliminar conexiones VPN. Cree una política personalizada para denegar la eliminación de conexiones VPN y asigne ambas políticas al grupo al que pertenece el usuario. De esta forma, el usuario podrá realizar todas las operaciones en la VPN, excepto eliminar conexiones VPN. A continuación, se muestra un ejemplo de una política de denegación:

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google


```
{
    "Versión": "1.1",
    "Declaración":
        [ {
            "Efecto": "Denegar",
            "Acción":
                [ "vpn:vpnGateways:eliminar"
            ]
        }
    ]
}
```

- Ejemplo 3: definir múltiples acciones en una política

  Una política personalizada puede contener las acciones de uno o varios servicios del mismo tipo (globales o de proyecto). A continuación, se muestra un ejemplo de política que contiene varias acciones .

```
    "Versión": "1.1",
    "Declaración":
        [ {
            "Efecto": "Permitir",
            "Acción":
                [ "vpn:vpnGateways:crear",
                "vpn:vpnConnections:crear",
                "vpn:customerGateways:crear"
            ]
        },
        {
            "Efecto": "Denegar",
            "Acción":
                [ "vpn:vpnGateways:eliminar",
                "vpn:vpnConnections:eliminar",
                "vpn:customerGateways:crear"
            ]
        },
        {
            "Efecto": "Permitir",
            "Acción":
                [ "vpc:vpcs:list",
                "vpc:subnets:get"
            ]
        }
    ]
}
```

3.6 Cuotas

¿Qué es una cuota?

Las cuotas imponen límites a las cantidades y capacidades de recursos disponibles para los usuarios, como la cantidad máxima de discos ECS o EVS que se pueden crear.

Si la cuota de recursos existente no puede satisfacer sus requisitos de servicio, puede solicitar una cuota más alta.

Tipos de recursos

- Los recursos VPN incluyen puertas de enlace VPN, grupos de conexión VPN y clientes.

  puertas de enlace.

La cuota total de cada tipo de recurso varía según las regiones.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

¿Cómo puedo ver mis cuotas?

1. Inicie sesión en la consola de administración.
2. Haga clic  (el ícono Mis cuotas) en la esquina superior derecha.

   Se muestra la página Cuota de servicio .
3. Visualiza la cuota utilizada y total de cada tipo de recurso en la pantalla.
   página.

   Si una cuota no puede satisfacer los requisitos del servicio, solicite una cuota más alta.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

4 Mejores prácticas

4.1 Conexión de un centro de datos local a una VPC en la nube a través de VPN (modo activo-activo)

4.1.1 Descripción general

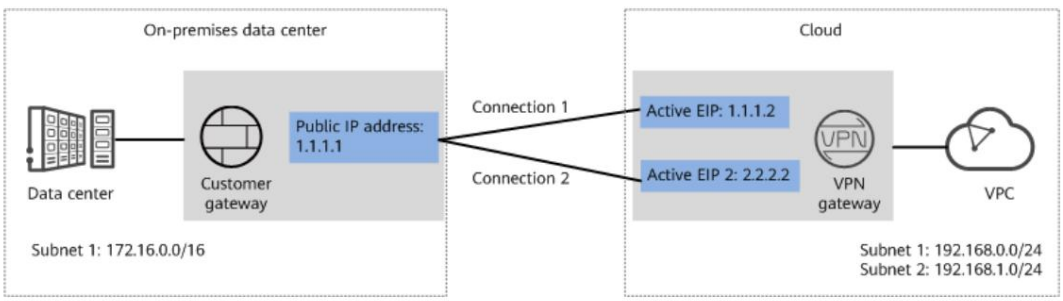
Guión

Se puede utilizar una VPN para habilitar la comunicación entre un centro de datos local y ECS en una VPC.

Redes

En este ejemplo, se configuran dos conexiones VPN entre un centro de datos local y una VPC para garantizar la fiabilidad de la red. Si una conexión VPN falla, el tráfico se redirige automáticamente a la otra, lo que garantiza la continuidad del servicio.

Figura 4-1 Diagrama de red



Ventajas de la solución

Una puerta de enlace VPN proporciona dos direcciones IP para establecer conexiones VPN duales e independientes con una puerta de enlace de cliente. Si una conexión VPN falla, el tráfico se puede transferir rápidamente a la otra conexión VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

• Las puertas de enlace VPN activas-activas se pueden implementar en diferentes AZ para garantizar una alta disponibilidad a nivel de AZ.

Limitaciones y restricciones

• Las subredes locales y del cliente de la puerta de enlace VPN no pueden ser las mismas. Es decir, la subred de VPC y la subred del centro de datos que se interconectarán no pueden ser la misma.

• La política IKE, la política IPsec y la PSK de la puerta de enlace VPN deben ser las mismas que las de la puerta de enlace del cliente. • Las configuraciones

de las direcciones de interfaz local y remota en la puerta de enlace VPN y la puerta de enlace del cliente están invertidas. • Los grupos de seguridad asociados

a los ECS en la VPC permiten el acceso desde y hacia el centro de datos local.

4.1.2 Planificación de redes y recursos

Plan de datos

Tabla 4-1 Plan de datos

Categoría Artículo		Datos
VPC	Subred que necesita acceder al centro de datos local	• 192.168.0.0/24 • 192.168.1.0/24
VPN puerta	Interconexiones en subred	Esta subred se utiliza para la comunicación entre la puerta de enlace VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables. 192.168.2.0/24
	Modo HA	Activo-activo
	EIP	Las EIP se generan automáticamente al comprarlas. Por defecto, una puerta de enlace VPN utiliza dos EIP. En este ejemplo, las EIP son las siguientes: • EIP activa: 1.1.1.2 • EIP activo 2: 2.2.2.2
Conexión VPN	Dirección de interfaz del túnel	Una puerta de enlace VPN utiliza esta dirección para establecer un túnel IPsec con una puerta de enlace de cliente. En ambos extremos del túnel IPsec, las direcciones de interfaz del túnel local y remoto configuradas deben invertirse. • Conexión VPN 1: 169.254.70.1/30 • Conexión VPN 2: 169.254.71.1/30

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Categoría Artículo		Datos
Datos locales centro	Subred que necesita acceder a la VPC	172.16.0.0/16
Puerta de enlace del cliente	Dirección IP pública	Esta dirección IP pública la asigna un operador. En este ejemplo, la dirección IP pública es: 1.1.1.1
	Dirección de interfaz del túnel	• Conexión VPN 1: 169.254.70.2/30 • Conexión VPN 2: 169.254.71.2/30
IKE y Políticas IPsec	PSK	Prueba@123
	Política de IKE	• Versión: v2 • Algoritmo de autenticación: SHA2-256 • Algoritmo de cifrado: AES-128 • Algoritmo DH: Grupo 15 • Duración (s): 86400 • ID local: dirección IP • ID de par: dirección IP
	Política IPsec	• Algoritmo de autenticación: SHA2-256 • Algoritmo de cifrado: AES-128 • PFS: DH Group15 • Protocolo de transferencia: ESP • Duración (s): 3600

4.1.3 Procedimiento

Prerrequisitos

- Lado de la nube
  - Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte Guía del usuario de la nube privada virtual .
  - Se han configurado reglas del grupo de seguridad para la VPC y los ECS pueden comunicarse con otros dispositivos en la nube. Para obtener más información sobre cómo configurar las reglas del grupo de seguridad, consulte Guía del usuario de la nube privada virtual .
- Lado del centro de datos
  - Se ha configurado IPsec en el dispositivo VPN en los datos locales centro.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Procedimiento

Las VPN admiten los modos de enrutamiento estático, BGP y basado en políticas. A continuación, se utiliza el modo de enrutamiento estático como ejemplo.

Paso 1 Inicie sesión en la consola de administración.

Paso 2 Haga clic en Lista de servicios y seleccione Redes > Red privada virtual.

Paso 3 Configure una puerta de enlace VPN.

1. Seleccione Red privada virtual > Empresa – Puertas de enlace VPN y haga clic en Comprar puerta de enlace VPN.
2. Establezca los parámetros según se le solicite.

La Tabla 4-2 solo describe los parámetros clave para crear una puerta de enlace VPN.

Tabla 4-2 Descripción de los parámetros de la puerta de enlace VPN

Parlamento o	Descripción	Valor
Nombre	Nombre de una puerta de enlace VPN.	vpngw-001
Red Tipo	Seleccione Red pública.	Red pública
Asociado Con	Seleccione VPC.	VPC
VPC	VPC a la que pertenece la subred de interconexión.	vpc-001(192.168.0.0/16)
Interconexión Subred	Esta subred se utiliza para la comunicación entre la puerta de enlace VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables.	192.168.2.0/24
Local Subred	Este parámetro solo está disponible cuando Asociar con está configurado en VPC. – Introducir bloque CIDR Ingrese la subred que necesita acceder al centro de datos local. La subred puede pertenecer o no a la VPC asociada. – Seleccionar subred Seleccione una subred que pertenezca a la VPC asociada y necesite acceder al centro de datos local.	192.168.0.0/24,192.168.1.0/24
BGP ASN	Número BGP AS.	64512
Modo HA	Seleccione Activo-activo.	Activo-activo
EIP activo	EIP 1 utilizado por la puerta de enlace VPN para acceder al centro de datos local.	1.1.1.2

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parlamento o	Descripción	Valor
EIP activo 2	EIP 2 utilizado por la puerta de enlace VPN para acceder El centro de datos local.	2.2.2.2

Paso 4 Configure la puerta de enlace del cliente.

1. Elija Red privada virtual > Empresa – Puertas de enlace de clientes y Haga clic en Crear puerta de enlace de clientes.
2. Establezca los parámetros según se le solicite.

   La Tabla 4-3 solo describe los parámetros clave para crear una puerta de enlace de clientes.

Tabla 4-3 Descripción de los parámetros de la puerta de enlace del cliente

Parámetro	Descripción	Valor
Nombre	Nombre de una puerta de enlace de clientes.	cgw-fw
Modo de enrutamiento	Seleccione Estático.	Estático
IP de puerta de enlace DIRECCIÓN	Dirección IP utilizada por el cliente puerta de enlace para comunicarse con el Puerta de enlace VPN. Asegúrese de que el puerto UDP 4500 esté Permitido en la pasarela del cliente dispositivo en los datos locales centro.	1.1.1.1

Paso 5 Configurar conexiones VPN.

1. Elija Red privada virtual > Empresa – Conexiones VPN y haga clic en Comprar conexión VPN.
2. Establezca los parámetros para la conexión VPN 1 y haga clic en Enviar.

   La Tabla 4-4 solo describe los parámetros clave para crear una conexión VPN.

Tabla 4-4 Configuración de parámetros para la conexión VPN 1

Parámetro	Descripción	Valor
Nombre	Nombre de una conexión VPN.	vpn-001
Puerta de enlace VPN	Puerta de enlace VPN para la cual se encuentra la VPN Se crea la conexión.	vpngw-001
IP de puerta de enlace DIRECCIÓN	EIP activo vinculado a la VPN puerta.	1.1.1.2
Cliente Puerta	Nombre de una puerta de enlace de clientes.	cgw-fw
Tipo de VPN	Seleccione enrutamiento estático.	Enrutamiento estático

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor
Cliente Subred	Subred en el centro de datos local que necesita acceder a la VPC. – Una subred de cliente no puede ser incluido en cualquier subred local o cualquier subred de la VPC a la que está conectada la puerta de enlace VPN. – Los bloques CIDR de VPC reservados, como 100.64.0.0/10 y 214.0.0.0/8, no se pueden usar como subredes de cliente.	172.16.0.0/16
Interfaz IP DIRECCIÓN Asignación	– Especificar manualmente En este ejemplo, seleccione Especificar manualmente. – Asignar automáticamente	Especificar manualmente
Túnel local Interfaz DIRECCIÓN	Dirección IP de la interfaz de túnel configurada en la puerta de enlace VPN.	169.254.70.1
Cliente Túnel Interfaz DIRECCIÓN	Dirección IP de la interfaz del túnel configurada en el dispositivo de puerta de enlace del cliente.	169.254.70.2
Detección de enlace	Si se debe habilitar la ruta Detección de accesibilidad en escenarios multienlace. Cuando NQA está habilitado, se envían paquetes ICMP para su detección y el dispositivo debe responder a ellos.	NQA habilitado
PSK, Confirm PSK	El valor debe ser el mismo que el PSK configurado en el dispositivo de puerta de enlace del cliente.	Prueba@123
Configuración de políticas	Las configuraciones de políticas deben ser las mismas que las del dispositivo de puerta de enlace del cliente.	Por defecto

3. Crear conexión VPN 2.

NO TE

Para la conexión VPN 2, se recomienda utilizar la misma configuración de parámetros que para la conexión VPN 1, excepto los parámetros enumerados en la siguiente tabla.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Tabla 4-5 Configuración de parámetros para la conexión VPN 2

Parámetro	Descripción	Valor
Nombre	Nombre de una conexión VPN.	vpn-002
IP de puerta de enlace DIRECCIÓN	EIP 2 activo vinculado a la puerta de enlace VPN.	2.2.2.2
Túnel local Interfaz DIRECCIÓN	Dirección IP del túnel de la puerta de enlace VPN.	169.254.71.1
Cliente Túnel Interfaz DIRECCIÓN	Dirección IP del túnel de la puerta de enlace del cliente.	169.254.71.2

Paso 6 Configure el dispositivo de puerta de enlace del cliente.

Los procedimientos de configuración pueden variar según el tipo de dispositivo de puerta de enlace del cliente.

----Fin

Verificación

- Aproximadamente 5 minutos después, verifique el estado de las conexiones VPN.

  Seleccione Red Privada Virtual > Empresa – Conexiones VPN. El estado de ambas conexiones VPN es Normal.

- Verifique que los servidores en el centro de datos local y los ECS en la subred de VPC puedan hacer ping entre sí.

4.2 Conexión de un centro de datos local a una VPC en la nube a través de VPN (modo activo/en espera)

4.2.1 Descripción general

Guión

Se puede utilizar una VPN para habilitar la comunicación entre un centro de datos local y ECS en una VPC.

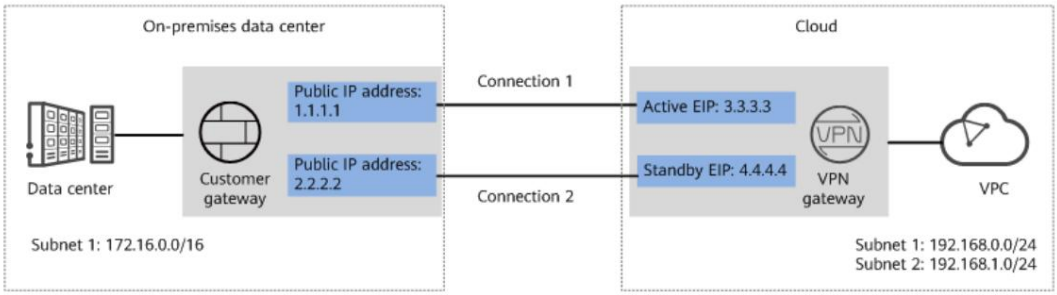
Redes

En este ejemplo, se configuran dos conexiones VPN en modo activo/en espera entre un centro de datos local y una VPC para garantizar la fiabilidad de la red. Si una conexión VPN falla, el tráfico se redirige automáticamente a la otra, lo que garantiza la continuidad del servicio.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Figura 4-2 Diagrama de red



Ventajas de la solución

• Una puerta de enlace VPN proporciona dos direcciones IP para establecer conexiones VPN duales e independientes con una puerta de enlace de cliente. Si una conexión VPN falla, el tráfico se puede transferir rápidamente a la otra conexión VPN. • Se pueden

implementar puertas de enlace VPN activas y en espera en diferentes zonas de disponibilidad (AZ) para garantizar... Alta disponibilidad a nivel AZ.

Limitaciones y restricciones

• Las subredes locales y del cliente de la puerta de enlace VPN no pueden ser las mismas. Es decir, la subred de VPC y la subred del centro de datos que se interconectarán no pueden ser la misma.

• La política IKE, la política IPsec y la PSK de la puerta de enlace VPN deben ser las mismas que las de la puerta de enlace del cliente. • Las

configuraciones de las direcciones de interfaz local y remota en la puerta de enlace VPN y la puerta de enlace del cliente están invertidas. • Los grupos

de seguridad asociados a los ECS en la VPC permiten el acceso desde y hacia el centro de datos local.

4.2.2 Planificación de redes y recursos

Plan de datos

Tabla 4-6 Plan de datos

Categoría Artículo		Datos
VPC	Subred que necesita acceder al centro de datos local	• 192.168.0.0/24 • 192.168.1.0/24
VPN puerta	Interconexiones en subred	Esta subred se utiliza para la comunicación entre la puerta de enlace VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables. 192.168.2.0/24

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Categoría Artículo		Datos
	Modo HA	Activo/En espera
	EIP	Las EIP se generan automáticamente al comprarlas. Por defecto, una puerta de enlace VPN utiliza dos EIP. En este ejemplo, las EIP son las siguientes: • EIP activa: 3.3.3.3 • EIP en espera: 4.4.4.4
Conexión VPN nota	Dirección de interfaz del túnel	Una puerta de enlace VPN utiliza esta dirección para establecer un túnel IPsec con una puerta de enlace de cliente. En ambos extremos del túnel IPsec, las direcciones de interfaz del túnel local y remoto configuradas deben invertirse. • Conexión VPN 1: 169.254.70.1/30 • Conexión VPN 2: 169.254.71.1/30
Datos locales centro	Subred que necesita acceder a la VPC	172.16.0.0/16
Puerta de enlace del cliente	Dirección IP pública	Esta dirección IP pública la asigna un operador. En este ejemplo, la dirección IP pública es: • 1.1.1.1 • 2.2.2.2
	Dirección de interfaz del túnel	• Conexión VPN 1: 169.254.70.2/30 • Conexión VPN 2: 169.254.71.2/30
IKE y Políticas IPsec	PSK	Prueba@123
	Política de IKE	• Versión: v2 • Algoritmo de autenticación: SHA2-256 • Algoritmo de cifrado: AES-128 • Algoritmo DH: Grupo 15 • Duración (s): 86400 • ID local: dirección IP • ID de par: dirección IP
	Política IPsec	• Algoritmo de autenticación: SHA2-256 • Algoritmo de cifrado: AES-128 • PFS: DH Group15 • Protocolo de transferencia: ESP • Duración (s): 3600

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

4.2.3 Procedimiento

Prerrequisitos

- Lado de la nube

  Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte Guía del usuario de la nube privada virtual .

  – Se han configurado reglas del grupo de seguridad para la VPC y los ECS pueden comunicarse con otros dispositivos en la nube. Para obtener más información sobre cómo configurar las reglas del grupo de seguridad, consulte Guía del usuario de la nube privada virtual .

- Lado del centro de datos

  – Se ha configurado IPsec en el dispositivo VPN en los datos locales centro.

Procedimiento

Las VPN admiten los modos de enrutamiento estático, BGP y basado en políticas. A continuación, se utiliza el modo de enrutamiento estático como ejemplo.

Paso 1 Inicie sesión en la consola de administración.

Paso 2 Haga clic en Lista de servicios y seleccione Redes > Red privada virtual.

Paso 3 Configure una puerta de enlace VPN.

1. Seleccione Red privada virtual > Empresa – Puertas de enlace VPN y haga clic en Comprar puerta de enlace VPN.
2. Establezca los parámetros según se le solicite.

   La Tabla 4-7 solo describe los parámetros clave para crear una puerta de enlace VPN.

Tabla 4-7 Descripción de los parámetros de la puerta de enlace VPN

Parlamento o	Descripción	Valor
Nombre	Nombre de una puerta de enlace VPN.	vpngw-001
Red Tipo	Seleccione Red pública.	Red pública
Asociado Con	Seleccione VPC.	VPC
VPC	VPC a la que pertenece la subred de interconexión.	vpc-001(192.168.0.0/16)
Interconexión Subred	Esta subred se utiliza para la comunicación entre la puerta de enlace VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables.	192.168.2.0/24

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parlamento o	Descripción	Valor
Local Subred	Este parámetro solo está disponible cuando Asociar con está configurado en VPC. – Introducir bloque CIDR Ingrese la subred que necesita acceder al centro de datos local. La subred puede pertenecer o no a la VPC asociada. – Seleccionar subred Seleccione una subred que pertenezca a la VPC asociada y necesite acceder al centro de datos local.	192.168.0.0/24,192.168.1.0/24
BGP ASN	Número BGP AS.	64512
Modo HA	Seleccione Activo/En espera.	Activo/En espera
EIP activo	EIP activo utilizado por la puerta de enlace VPN para acceder al centro de datos local.	1.1.1.2
Apoyar EIP	EIP en espera utilizado por la puerta de enlace VPN para acceder al centro de datos local.	2.2.2.2

Paso 4 Configure la puerta de enlace del cliente.

1. Seleccione Red privada virtual > Empresa – Puertas de enlace de clientes y haga clic en Crear puerta de enlace de clientes.
2. Establezca los parámetros según se le solicite.

   La Tabla 4-8 solo describe los parámetros clave para crear una puerta de enlace de clientes.

Tabla 4-8 Descripción de los parámetros de la puerta de enlace del cliente

Parámetro	Descripción	Valor
Nombre	Nombre de una puerta de enlace de clientes.	cgw-fw
Modo de enrutamiento	Seleccione Estático.	Estático
IP de puerta de enlace DIRECCIÓN	Dirección IP utilizada por la puerta de enlace del cliente para comunicarse con la puerta de enlace VPN. Asegúrese de que el puerto UDP 4500 esté permitido en el dispositivo de puerta de enlace del cliente en los datos locales. centro.	1.1.1.1

Paso 5 Configurar conexiones VPN.

1. Seleccione Red privada virtual > Empresa – Conexiones VPN y haga clic en Comprar conexión VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

2. Establezca los parámetros para la conexión VPN 1 y haga clic en Enviar.

La Tabla 4-9 solo describe los parámetros clave para crear una conexión VPN.

Tabla 4-9 Configuración de parámetros para la conexión VPN 1

Parámetro	Descripción	Valor
Nombre	Nombre de una conexión VPN.	vpn-001
Puerta de enlace VPN	Puerta de enlace VPN para la cual se encuentra la VPN Se crea la conexión.	vpngw-001
IP de puerta de enlace DIRECCIÓN	EIP activo vinculado a la puerta de enlace VPN.	1.1.1.2
Cliente Puerta	Nombre de una puerta de enlace de clientes.	cgw-fw
Tipo de VPN	Seleccione enrutamiento estático.	Enrutamiento estático
Cliente Subred	Subred en el centro de datos local que necesita acceder a la VPC. – Una subred de cliente no puede ser incluido en cualquier subred local o cualquier subred de la VPC a la que está conectada la puerta de enlace VPN. – Los bloques CIDR de VPC reservados, como 100.64.0.0/10 y 214.0.0.0/8, no se pueden usar como subredes de cliente.	172.16.0.0/16
Interfaz IP DIRECCIÓN Asignación	– Especificar manualmente En este ejemplo, seleccione Especificar manualmente. – Asignar automáticamente	Especificar manualmente
Túnel local Interfaz DIRECCIÓN	Dirección IP de la interfaz de túnel configurada en la puerta de enlace VPN.	169.254.70.1
Cliente Túnel Interfaz DIRECCIÓN	Dirección IP de la interfaz del túnel configurada en el dispositivo de puerta de enlace del cliente.	169.254.70.2
Detección de enlace	Si se debe habilitar la ruta Detección de accesibilidad en escenarios multienlace. Cuando NQA está habilitado, se envían paquetes ICMP para su detección y el dispositivo debe responder a ellos.	NQA habilitado

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor
PSK, Confirm PSK	El valor debe ser el mismo que el PSK configurado en el dispositivo de puerta de enlace del cliente.	Prueba@123
Configuración de políticas	Las configuraciones de políticas deben ser las mismas que las del dispositivo de puerta de enlace del cliente.	Por defecto

3. Crear conexión VPN 2.

NO TE

Para la conexión VPN 2, se recomienda utilizar la misma configuración de parámetros que para la conexión VPN 1, excepto los parámetros enumerados en la siguiente tabla.

Tabla 4-10 Configuración de parámetros para la conexión VPN 2

Parámetro	Descripción	Valor
Nombre	Nombre de una conexión VPN.	vpn-002
IP de puerta de enlace DIRECCIÓN	EIP en espera vinculado a la puerta de enlace VPN.	2.2.2.2
Túnel local Interfaz DIRECCIÓN	Dirección IP del túnel de la puerta de enlace VPN.	169.254.71.1
Cliente Túnel Interfaz DIRECCIÓN	Dirección IP del túnel de la puerta de enlace del cliente.	169.254.71.2

Paso 6 Configure el dispositivo de puerta de enlace del cliente.

Los procedimientos de configuración pueden variar según el tipo de dispositivo de puerta de enlace del cliente.

----Fin

Verificación

- Aproximadamente 5 minutos después, verifique el estado de las conexiones VPN.

  Seleccione Red Privada Virtual > Empresa – Conexiones VPN. Ambas conexiones VPN tienen el estado Disponible.

- Verifique que los servidores en el centro de datos local y los ECS en la subred de VPC puedan hacer ping entre sí.

Derechos de autor © Huawei Technologies Co., Ltd.

850

Machine Translated by Google

4.3 Conexión de varias redes de sucursales locales a través de un concentrador VPN

4.3.1 Descripción general

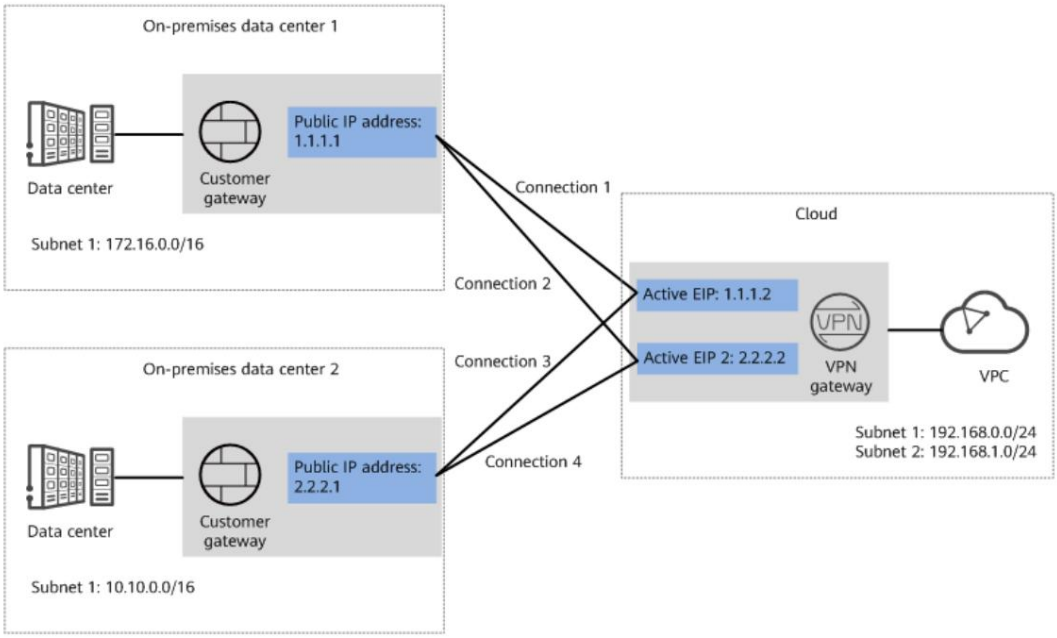
Guión

Para cumplir con los requisitos de servicio, la empresa A necesita implementar la comunicación entre sus dos centros de datos locales.

Redes

La Figura 4-3 muestra la red donde se utiliza el servicio VPN para conectar los dos centros de datos locales.

Figura 4-3 Diagrama de red



Ventajas de la solución

- Una puerta de enlace VPN en la nube puede funcionar como un concentrador VPN para habilitar Comunicación entre sucursales locales. Esto elimina la necesidad de configurar conexiones VPN entre cada dos sitios.

Una puerta de enlace VPN proporciona dos direcciones IP para establecer conexiones VPN duales e independientes con cada puerta de enlace del cliente. Si una conexión VPN falla, el tráfico se puede transferir rápidamente a la otra, lo que garantiza la fiabilidad.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Limitaciones y restricciones

- Las subredes locales y del cliente de la puerta de enlace VPN no pueden ser las mismas. Es decir, la subred de VPC y la subred del centro de datos que se interconectarán no pueden ser la misma.
- La política IKE, la política IPsec y la PSK de la puerta de enlace VPN deben ser las mismas que las de la puerta de enlace del cliente. • Las

configuraciones de las direcciones de interfaz local y remota en la puerta de enlace VPN y la puerta de enlace del cliente están invertidas. • Los

grupos de seguridad asociados a los ECS en la VPC permiten el acceso desde y hacia el centro de datos local.

4.3.2 Planificación de redes y recursos

Plan de datos

Tabla 4-11 Plan de datos

Categoría Artículo		Datos
VPC	Subred que necesita acceder a los centros de datos locales	• 192.168.0.0/24 • 192.168.1.0/24
Puerta de enlace VPN	Interconexiones en subred	Esta subred se utiliza para la comunicación entre la puerta de enlace VPN y la VPC. Asegúrese de que la subred de interconexión seleccionada tenga cuatro o más direcciones IP asignables. 192.168.2.0/24
	HA Moda	Activo-activo
	EIP	Las EIP se generan automáticamente al comprarlas. Por defecto, una puerta de enlace VPN utiliza dos EIP. En este ejemplo, las EIP son las siguientes: • EIP activa: 1.1.1.2 • EIP activo 2: 2.2.2.2

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Categoría Artículo		Datos
Conexión VPN	Dirección de interfaz del túnel	Una puerta de enlace VPN utiliza esta dirección para establecer un túnel IPsec con una puerta de enlace de cliente. En ambos extremos del túnel IPsec, las direcciones de interfaz del túnel local y remoto configuradas deben invertirse. • Conexiones VPN configuradas con datos locales centro 1 – Conexión VPN 1: 169.254.70.1/30 – Conexión VPN 2: 169.254.71.1/30 • Conexiones VPN configuradas con datos locales centro 2 – Conexión VPN 3: 169.254.72.1/30 – Conexión VPN 4: 169.254.73.1/30
Centro de datos local 1	Subred que necesita acceder a la VPC	172.16.0.0/16
Puerta de enlace del cliente en el centro de datos local 1	Dirección IP pública	Esta dirección IP pública la asigna un operador. En este ejemplo, la dirección IP pública es: 1.1.1.1
	Dirección de interfaz del túnel	• Conexión VPN 1: 169.254.70.2/30 • Conexión VPN 2: 169.254.71.2/30
Centro de datos local 2	Subred que necesita acceder a la VPC	10.10.0.0/16
Puerta de enlace del cliente en el centro de datos local 2	Dirección IP pública	Esta dirección IP pública la asigna un operador. En este ejemplo, la dirección IP pública es: 2.2.2.1
	Dirección de interfaz del túnel	• Conexión VPN 3: 169.254.72.2/30 • Conexión VPN 4: 169.254.73.2/30
IKE y Políticas IPsec	PSK	Prueba@123

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Categoría	Artículo	Datos
	Política de IKE	• Algoritmo de autenticación: SHA2-256 • Algoritmo de cifrado: AES-128 • Algoritmo DH: Grupo 15 • Versión: v2 • Vida útil (s): 86400 • ID local: dirección IP • ID de par: dirección IP
	Política IPsec	• Algoritmo de autenticación: SHA2-256 • Algoritmo de cifrado: AES-128 • PFS: DH Group15 • Protocolo de transferencia: ESP • Duración (s): 3600

4.3.3 Procedimiento

Prerrequisitos

• Lado de la nube

Se ha creado una VPC. Para obtener más información sobre cómo crear una VPC, consulte Guía del usuario de la nube privada virtual .

– Se han configurado reglas del grupo de seguridad para la VPC y los ECS pueden comunicarse con otros dispositivos en la nube. Para obtener más información sobre cómo configurar las reglas del grupo de seguridad, consulte Guía del usuario de la nube privada virtual .

• Lado del centro de datos

– Se ha configurado IPsec en los dispositivos VPN en las dos instalaciones locales centros de datos.

– Las subredes remotas del dispositivo VPN en el centro de datos local 1 deben contener la subred local de la VPC y la subred que se interconectará en el centro de datos local 2. Las subredes remotas del dispositivo VPN en el centro de datos local 2 deben contener la subred local de la VPC y la subred que se interconectará en el centro de datos local 1.

Procedimiento

Las VPN admiten los modos de enrutamiento estático, BGP y basado en políticas. A continuación, se utiliza el modo de enrutamiento estático como ejemplo.

Paso 1 Configure una puerta de enlace VPN.

1. Seleccione Red privada virtual > Empresa – Puertas de enlace VPN y haga clic en Comprar puerta de enlace VPN.
2. Establezca los parámetros según se le solicite.

La Tabla 4-12 solo describe los parámetros clave para crear una puerta de enlace VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Tabla 4-12 Descripción de los parámetros de la puerta de enlace VPN

Parlamento o	Descripción	Valor
Nombre	Nombre de una puerta de enlace VPN.	vpngw-001
Red Tipo	Seleccione Red pública.	Red pública
Asociado Con	Seleccione VPC.	VPC
VPC	VPC que los centros de datos locales necesidad de acceder.	vpc-001(192.168.0. 0/16)
Local Subred	Subredes de VPC que almacenan los datos locales Los centros necesitan acceder.	192.168.0.0/24,192. 168.1.0/24
Interconexión sección Subred	Esta subred se utiliza para la comunicación. entre la puerta de enlace VPN y la VPC. Asegúrese de que la interconexión seleccionada La subred tiene cuatro o más direcciones IP asignables direcciones.	192.168.2.0/24
BGP ASN	Número BGP AS.	64512
Modo HA	Seleccione Activo-activo.	Activo-activo
EIP activo	EIP 1 utilizado por la puerta de enlace VPN para acceder El centro de datos local.	1.1.1.2
EIP activo 2	EIP 2 utilizado por la puerta de enlace VPN para acceder El centro de datos local.	2.2.2.2

Paso 2: Configurar las puertas de enlace del cliente.

1. Elija Red privada virtual > Empresa – Puertas de enlace de clientes y Haga clic en Crear puerta de enlace de clientes.
2. Establezca los parámetros según se le solicite.

   La Tabla 4-13 solo describe los parámetros clave para crear un cliente. puerta.

Tabla 4-13 Descripción de los parámetros de la puerta de enlace del cliente

Parámetro	Descripción	Valor
Nombre	Nombre de una puerta de enlace de clientes.	cgw-fw1
Modo de enrutamiento	Seleccione Estático.	Estático

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor
IP de puerta de enlace DIRECCIÓN	Dirección IP utilizada por la puerta de enlace del cliente en el centro de datos local 1 para comunicarse con la puerta de enlace VPN. Asegúrese de que el puerto UDP 4500 esté permitido en el dispositivo de puerta de enlace del cliente en el centro de datos local.	1.1.1.1

3. Repita las operaciones anteriores para configurar la puerta de enlace del cliente (2.2.2.1) en el centro de datos local 2.

Paso 3 Configurar conexiones VPN entre el lado de la nube y el centro de datos local 1.

1. Seleccione Red privada virtual > Empresa – Conexiones VPN y haga clic en Comprar conexión VPN.

2. Establezca los parámetros para la conexión VPN 1 y haga clic en Enviar.

   La Tabla 4-14 solo describe los parámetros clave para crear una conexión VPN.

Tabla 4-14 Descripción de los parámetros de conexión VPN

Parámetro	Descripción	Valor
Nombre	Nombre de una conexión VPN.	vpn-001
Puerta de enlace VPN	Puerta de enlace VPN para la cual se encuentra la VPN Se crea la conexión.	vpngw-001
IP de puerta de enlace DIRECCIÓN	EIP activo vinculado a la puerta de enlace VPN.	1.1.1.2
Tipo de VPN	Seleccione enrutamiento estático.	Enrutamiento estático
Cliente Puerta	Nombre de una puerta de enlace de clientes.	cgw-fw1
Cliente Subred	Subred en el centro de datos local 1 que necesita acceder a la VPC. – Una subred de cliente no puede ser incluido en cualquier subred local o cualquier subred de la VPC a la que está conectada la puerta de enlace VPN. – Los bloques CIDR de VPC reservados, como 100.64.0.0/10 y 214.0.0.0/8, no se pueden usar como subredes de cliente.	172.16.0.0/16
Interfaz IP DIRECCIÓN Asignación	– Especificar manualmente En este ejemplo, seleccione Especificar manualmente. – Asignar automáticamente	Especificar manualmente

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor
Túnel local Interfaz DIRECCIÓN	Dirección IP de la interfaz de túnel configurada en la puerta de enlace VPN.	169.254.70.1
Cliente Túnel Interfaz DIRECCIÓN	Dirección IP de la interfaz del túnel configurada en el dispositivo de puerta de enlace del cliente.	169.254.70.2
Detección de enlace	Si se debe habilitar la ruta Detección de accesibilidad en escenarios multienlace. Cuando NQA está habilitado, se envían paquetes ICMP para su detección y el dispositivo debe responder a ellos.	NQA habilitado
PSK, Confirm PSK	El valor debe ser el mismo que el PSK configurado en el dispositivo de puerta de enlace del cliente.	Prueba@123
Configuración de políticas	Las configuraciones de políticas deben ser las mismas que las del dispositivo de puerta de enlace del cliente.	Por defecto

3. Crear conexión VPN 2.

NO TE

Para la conexión VPN 2, se recomienda utilizar la misma configuración de parámetros que para la conexión VPN 1, excepto los parámetros enumerados en la siguiente tabla.

Tabla 4-15 Configuración de parámetros para la conexión VPN 2

Parámetro	Descripción	Valor
Nombre	Nombre de una conexión VPN.	vpn-002
IP de puerta de enlace DIRECCIÓN	EIP 2 activo vinculado a la puerta de enlace VPN.	2.2.2.2
Túnel local Interfaz DIRECCIÓN	Dirección IP del túnel de la puerta de enlace VPN.	169.254.71.1
Cliente Túnel Interfaz DIRECCIÓN	Dirección IP del túnel de la puerta de enlace del cliente.	169.254.71.2

Paso 4 Configurar conexiones VPN entre el lado de la nube y el centro de datos local 2.

1. Seleccione Red privada virtual > Empresa – Conexiones VPN y haga clic en Comprar conexión VPN.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

2. Configure los parámetros para la conexión VPN 1 según se le solicite y haga clic en Enviar.

La Tabla 4-16 solo describe los parámetros clave para crear una conexión VPN.

Tabla 4-16 Descripción de los parámetros de conexión VPN

Parámetro	Descripción	Valor
Nombre	Nombre de una conexión VPN.	vpn-003
Puerta de enlace VPN	Puerta de enlace VPN para la cual se encuentra la VPN Se crea la conexión.	vpngw-001
IP de puerta de enlace DIRECCIÓN	EIP activo vinculado a la puerta de enlace VPN.	1.1.1.2
Cliente Puerta	Nombre de una puerta de enlace de clientes.	cgw-fw2
Tipo de VPN	Seleccione enrutamiento estático.	Enrutamiento estático
Cliente Subred	Subred en el centro de datos local 2 que necesita acceder a la VPC. – Una subred de cliente no puede ser incluido en cualquier subred local o cualquier subred de la VPC a la que está conectada la puerta de enlace VPN. – Los bloques CIDR de VPC reservados, como 100.64.0.0/10 y 214.0.0.0/8, no se pueden usar como subredes de cliente.	10.10.0.0/16
Interfaz IP DIRECCIÓN Asignación	– Especificar manualmente En este ejemplo, seleccione Especificar manualmente. – Asignar automáticamente	Especificar manualmente
Túnel local Interfaz DIRECCIÓN	Dirección IP de la interfaz de túnel configurada en la puerta de enlace VPN.	169.254.72.1
Cliente Túnel Interfaz DIRECCIÓN	Dirección IP de la interfaz del túnel configurada en el dispositivo de puerta de enlace del cliente.	169.254.72.2
Detección de enlace	Si se debe habilitar la ruta Detección de accesibilidad en escenarios multienlace. Cuando NQA está habilitado, se envían paquetes ICMP para su detección y el dispositivo debe responder a ellos.	NQA habilitado

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Parámetro	Descripción	Valor
PSK, Confirm PSK	El valor debe ser el mismo que el PSK configurado en el dispositivo de puerta de enlace del cliente en el centro de datos local 2.	Prueba@123
Configuración de políticas	Las configuraciones de políticas deben ser las mismas que las configuradas en el dispositivo de puerta de enlace del cliente en el centro de datos local 2.	Por defecto

3. Crear conexión VPN 2.

NO TE

Para la conexión VPN 2, se recomienda utilizar la misma configuración de parámetros que para la conexión VPN 1, excepto los parámetros enumerados en la siguiente tabla.

Tabla 4-17 Configuración de parámetros para la conexión VPN 2

Parámetro	Descripción	Valor
Nombre	Nombre de una conexión VPN.	vpn-004
IP de puerta de enlace DIRECCIÓN	EIP 2 activo vinculado a la puerta de enlace VPN.	2.2.2.2
Túnel local Interfaz DIRECCIÓN	Dirección IP del túnel de la puerta de enlace VPN.	169.254.73.1
Cliente Túnel Interfaz DIRECCIÓN	Dirección IP del túnel de la puerta de enlace del cliente en el centro de datos local 2.	169.254.73.2

Paso 5 Configure los dispositivos de puerta de enlace del cliente en los centros de datos locales 1 y 2.

Los procedimientos de configuración pueden variar según el tipo de dispositivo de puerta de enlace del cliente.

----Fin

Verificación

- Aproximadamente 5 minutos después, verifique el estado de las conexiones VPN.

  Seleccione Red Privada Virtual > Empresa – Conexiones VPN. El estado de las cuatro conexiones VPN es Normal.

- Verifique que los servidores en el centro de datos local 1 y los servidores en el centro de datos local 2 puedan hacer ping entre sí.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

4.4 VPN clásica

4.4.1 Conexión de un centro de datos local a una VPC a través de una VPN

Escenarios

De forma predeterminada, los ECS de una VPC no pueden comunicarse con los dispositivos de su centro de datos local ni de su red privada. Para habilitar la comunicación entre ellos, puede configurar una VPN. Después, debe configurar las reglas del grupo de seguridad y comprobar la conectividad de la subred para garantizar que la VPN esté disponible. Las VPN se clasifican en los dos tipos siguientes:

- Una VPN de sitio a sitio funciona como un túnel de comunicación entre una VPC y un único centro de datos local.
- Por el contrario, una VPN de concentrador y radio se encuentra entre una VPC y varias en centros de datos locales.

Preste atención a lo siguiente al configurar una VPN:

- Las subredes locales y remotas no pueden entrar en conflicto.
- Las políticas IKE, las políticas IPsec y las PSK configuradas en la nube y en el El centro de datos local debe ser el mismo.
- Los parámetros configurados para las subredes y puertas de enlace locales y remotas deben ser simétricos.
- Las reglas del grupo de seguridad permiten el acceso hacia y desde los ECS en la VPC. •

El estado de una VPN cambia a Normal solo después de que los ECS y las instalaciones locales Los servidores acceden entre sí.

Prerrequisitos

Ha creado la VPC y las subredes que el centro de datos local desea acceso.

Procedimiento

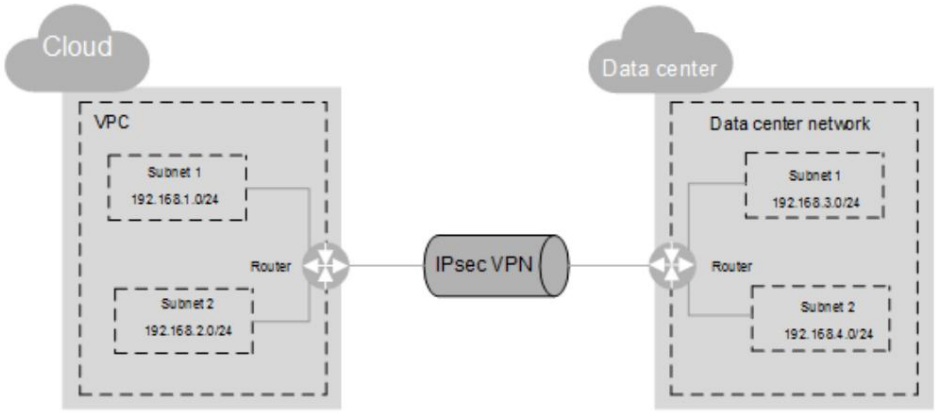
1. En la consola de administración, seleccione las políticas IKE e IPsec adecuadas para crear una VPN.
2. Verifique los grupos de direcciones IP para las subredes locales y remotas.

   En la Figura 4-4, la VPC tiene las subredes 192.168.1.0/24 y 192.168.2.0/24. Su centro de datos local tiene las subredes 192.168.3.0/24 y 192.168.4.0/24. Puede configurar una VPN para conectar estas subredes.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Figura 4-4 VPN IPsec



Los grupos de direcciones IP de las subredes locales no pueden superponerse con los de las subredes remotas. Como en este ejemplo, el grupo de direcciones IP de las subredes remotas no puede contener las dos subredes de la VPC.

3. Configure las reglas del grupo de seguridad para los ECS para permitir paquetes desde y hacia el centro de datos local a través de VPN.
4. Haga ping a los ECS desde el centro de datos local para verificar que la seguridad
   El grupo permite paquetes desde y hacia el centro de datos local a través de la VPN.
5. Verifique la configuración de la red local.

   Se debe configurar una ruta para la red local para permitir el reenvío de tráfico a los dispositivos de red a través de la VPN. Si los datos transmitidos a través de la VPN no se pueden reenviar a los dispositivos de red, verifique si la LAN remota tiene reglas configuradas para rechazar el tráfico.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

5 Solución de problemas

5.1 El estado de una conexión VPN es No conectado

Síntoma

En la página Empresa – Conexiones VPN de la consola VPN, el estado de una conexión VPN se muestra como No conectado.

Posibles causas

• Las configuraciones en los dos extremos de la conexión VPN son incorrectas. • La configuración del grupo de seguridad en la consola de administración o la configuración de ACL en el dispositivo de puerta de enlace del cliente es incorrecta.

Procedimiento

• Verifique las configuraciones en los dos extremos de la conexión VPN.

– Verifique si las direcciones IP de puerta de enlace configuradas en los dos extremos de la conexión VPN están invertidas.

▪ Para verificar las EIP activas y en espera de la puerta de enlace VPN, seleccione Red privada virtual > Empresa – Puertas de enlace VPN y vea las direcciones IP en la columna Dirección IP de la puerta de enlace .

▪ Para comprobar la dirección IP de la puerta de enlace del cliente, seleccione Virtual Red privada > Empresa – Puertas de enlace de clientes y ver la dirección IP en la columna Dirección IP de la puerta de enlace .

– Verifique si las políticas IKE e IPsec en los dos extremos de la conexión VPN son consistentes.

▪ Para ver la configuración de políticas de IKE e IPsec en la consola VPN, seleccione Red privada virtual > Empresa – Conexiones VPN, ubique la conexión VPN de destino y seleccione Más > Modificar configuración de políticas.

– Compruebe si las PSK en los dos extremos de la conexión VPN son las mismas mismo.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

▪ No se puede verificar la clave PSK en la consola VPN. Si no está seguro de si la clave PSK configurada en la consola VPN es correcta, le recomendamos modificarla para que coincida con la configurada en el dispositivo de puerta de enlace del cliente.

Para cambiar la PSK en la consola VPN, seleccione Red privada virtual > Empresa – Conexiones VPN, ubique la conexión VPN de destino y seleccione Más > Restablecer PSK.

– Si se utiliza el modo basado en políticas, verifique si la fuente y Los bloques CIDR de destino en las reglas de política en los dos extremos de la conexión VPN se invierten.

Para verificar las reglas de política en la consola VPN, seleccione Red privada virtual > Empresa – Conexiones VPN, ubique la conexión VPN de destino y haga clic en Modificar conexión VPN.

– Si se utiliza el modo de enrutamiento estático y la función NQA está habilitada en la consola VPN, verifique si las direcciones IP de la interfaz del túnel están configuradas correctamente en el dispositivo de puerta de enlace del cliente.

▪ Para comprobar si NQA está habilitado en la consola VPN, seleccione Red privada virtual > Empresa – Conexiones VPN, haga clic en el nombre de la conexión VPN de destino y vea el valor de Detección de enlace en la página de la pestaña Resumen .

Para comprobar las direcciones IP de la interfaz de túnel configuradas en la consola VPN, seleccione Red Privada Virtual > Empresa – Conexiones VPN, haga clic en Modificar Conexión VPN y consulte los valores de Dirección IP de la Interfaz Local y Dirección IP de la Interfaz del Cliente. Las direcciones IP de la interfaz local y remota configuradas en el dispositivo de puerta de enlace del cliente deben coincidir con los valores de Dirección IP de la Interfaz del Cliente y Dirección IP de la Interfaz Local configurados en la consola VPN, respectivamente.

– Si se utiliza el modo de enrutamiento BGP, verifique si los ASN BGP en los dos Los extremos de la conexión VPN están invertidos.

▪ Para comprobar el ASN BGP de la puerta de enlace VPN, seleccione Red privada virtual > Empresa – Puertas de enlace VPN, haga clic en el nombre de la puerta de enlace VPN y vea el ASN BGP en el área Información básica .

▪ Para comprobar el ASN BGP de la puerta de enlace del cliente, seleccione Virtual Red privada > Empresa – Puertas de enlace de clientes y ver el valor en la columna BGP ASN .

• Verifique la configuración del grupo de seguridad en la consola de administración y Configuración de ACL en el dispositivo de puerta de enlace del cliente.

– Verifique si el grupo de seguridad predeterminado en la consola de administración permite el tráfico de los puertos UDP 500 y 4500 originados desde la dirección IP pública de la puerta de enlace del cliente.

Para comprobar el grupo de seguridad predeterminado en la consola de administración, siga estos pasos: i. Seleccione Red

Privada Virtual > Enterprise – Puertas de enlace VPN y haga clic en el nombre de la VPC asociada a la puerta de enlace VPN. ii. En la página Nube Privada Virtual , haga clic en el

número en la sección Ruta.
Columna de tablas .

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

iii. En la página Tablas de rutas , haga clic en el nombre de la tabla de rutas. iv.

Localice y haga clic en el siguiente salto del EIP activo o en espera de la VPN.
puerta.

v. En la página de la pestaña Grupos de seguridad asociados , verifique si el grupo de seguridad permite el tráfico de los puertos.

– Verifique que una ACL en el dispositivo de puerta de enlace del cliente permita el tráfico de los puertos UDP 500 y 4500 originados desde los EIP activos y en espera de la puerta de enlace VPN.

5.2 Las pruebas de ping entre las redes en la nube y las locales fallan

Síntoma

• Los servidores en un centro de datos local no pueden hacer ping a los ECS en una

VPC. • Los ECS en una VPC no pueden hacer ping a los servidores en un centro de datos local.

Posibles causas

• La configuración del grupo de seguridad en la consola de administración es incorrecta. • La regla

de ACL asociada con la subred de interconexión es incorrecta.
configurado.

• La configuración de ACL en el dispositivo de puerta de enlace del cliente es incorrecta. •

La configuración de ruta en el dispositivo de puerta de enlace del cliente es incorrecta.

Procedimiento

• Verifique la configuración del grupo de seguridad en la consola de administración.

– Verifique que el grupo de seguridad predeterminado en la consola de administración permita flujos de datos destinados a la subred del cliente.

Para comprobar el grupo de seguridad predeterminado en la consola de administración, realice los siguientes pasos:

i. Seleccione Red Privada Virtual > Empresa – Puertas de enlace VPN y haga clic en el nombre de la VPC asociada a la puerta de enlace VPN. ii. Haga clic en el

número de tablas de rutas correspondientes a la VPC. iii. En la página Tablas

de rutas , haga clic en el nombre de la tabla de rutas. iv. Localice y haga clic en el

siguiente salto de la EIP activa o en espera de la VPN.
puerta.

v. En la página de la pestaña Grupos de seguridad asociados , verifique los puertos permitido por el grupo de seguridad.

– Verifique que el grupo de seguridad predeterminado en la consola de administración permita flujos de datos originados en la subred del cliente.

– Verifique que el grupo de seguridad predeterminado en la consola de administración permita flujos de datos destinados a la subred local.

– Verifique que el grupo de seguridad predeterminado en la consola de administración permita flujos de datos originados en la subred local.

Derechos de autor © Huawei Technologies Co., Ltd.

864

Machine Translated by Google

– Verificar que un grupo de seguridad permita flujos de datos desde los ECS a la subred del cliente.

Para comprobar si se ha configurado dicho grupo de seguridad, seleccione Computación > Elastic Cloud Server, haga clic en un nombre de ECS, haga clic en la pestaña Grupos de seguridad y haga clic en Administrar regla.

– Verificar que un grupo de seguridad permita flujos de datos desde la subred del cliente a los ECS.

• La regla de ACL asociada con la subred de interconexión es incorrecta configurado.

– Verifique si la regla de ACL asociada con la subred de interconexión permite el puerto TCP para el tráfico entre todas las subredes locales y de cliente.

i. Seleccione Red privada virtual > Empresa – Puertas de enlace VPN y Haga clic en el nombre de la puerta de enlace VPN de destino.

ii. En el área Información básica , verifique y registre la subred de interconexión.

iii. En el área Información básica , haga clic en el nombre de la VPC asociada. iv. En la pestaña Resumen de la VPC, haga clic en el número de subredes. en el área de Componentes de Red .

v. Busque la subred de interconexión en la lista de subredes y haga clic en la ACL nombre en la columna ACL de red .

vi. Permitir el puerto TCP para el tráfico entre todos los servidores locales y de cliente. subredes.

• Verifique la configuración de ACL en el dispositivo de puerta de enlace del cliente.

– Verifique que una regla de ACL en el dispositivo de puerta de enlace del cliente permita flujos de datos destinados a la subred local de la puerta de enlace VPN.

– Verifique que una regla de ACL en el dispositivo de puerta de enlace del cliente permita flujos de datos originados desde la subred local de la puerta de enlace VPN.

Para comprobar la subred local de la puerta de enlace VPN, seleccione Red privada virtual > Empresa – Puertas de enlace VPN, haga clic en el nombre de la puerta de enlace VPN y vea el valor de Subred local en el área Información básica .

• Verifique la configuración de ruta en el dispositivo de enlace del cliente.

– Verificar que la ruta de la red pública esté configurada correctamente. Es decir, La dirección de destino es una EIP de la puerta de enlace VPN y el siguiente salto es la dirección de la interfaz de salida del dispositivo de puerta de enlace del cliente.

Verifique que la ruta de red privada esté configurada correctamente. Es decir, la dirección de destino es la subred local de la puerta de enlace VPN y el siguiente salto es la dirección de la interfaz de salida del dispositivo de puerta de enlace del cliente.

Para comprobar la subred local de la puerta de enlace VPN, seleccione Red privada virtual > Empresa – Puertas de enlace VPN, haga clic en el nombre de la puerta de enlace VPN y vea el valor de Subred local en el área Información básica .

5.3 Se produce pérdida de paquetes

Síntoma

• La pérdida de paquetes ocurre cuando un servidor en un centro de datos local hace ping a un ECS en una VPC.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

• La pérdida de paquetes ocurre cuando un ECS en una VPC hace ping a un servidor en una red local. centro de datos.

Procedimiento

• Verifique la red y el ancho de banda del lado del cliente.

– Compruebe si la red del cliente tiene varias salidas funcionando en modo de balanceo de carga y si el tráfico se distribuye a una salida no VPN. Asegúrese de que el tráfico se transmita por la misma salida.

– Hacer ping a la dirección IP de la puerta de enlace VPN y otras direcciones IP públicas (por ejemplo, 114.114.114.114) desde la puerta de enlace del cliente para verificar el retraso y la tasa de pérdida de paquetes en la red pública.

Si la calidad de la red pública es mala, se recomienda buscar ayuda del operador correspondiente.

– Verifique si el tráfico en el dispositivo de puerta de enlace del cliente excede el límite de ancho de banda.

• Verifique la red y el ancho de banda.

– Verifique si el tráfico excede el ancho de banda de la puerta de enlace VPN.

i. Verifique el ancho de banda de las EIP activas y en espera de la puerta de enlace VPN de la siguiente manera: Seleccione Red Privada Virtual > Empresa – Puertas de enlace VPN, haga clic en el nombre de la puerta de enlace VPN y verifique el valor de Ancho de Banda (Mbit/s) en el área EIP .

ii. Verifique el uso real del ancho de banda de la puerta de enlace VPN de la siguiente manera: Seleccione Red privada virtual > Empresa – Puertas de enlace VPN y hacer clic  en la columna Dirección IP pública de la puerta de enlace VPN.

Si el tráfico excede el ancho de banda de la puerta de enlace VPN, aumente el ancho de banda.

5.4 VPN clásica

5.4.1 Elementos de verificación comunes

Las conexiones VPN o las operaciones de ping fallan cuando las configuraciones (como la política de negociación, el firewall, la tabla de rutas, la política entre zonas, la configuración de NAT y el grupo de seguridad) son incorrectas.

Compruebe las siguientes configuraciones.

• Cómo comprobar la información de negociación en ambos lados de una conexión VPN • Cómo comprobar la configuración del firewall en su red local y la Configuración del grupo de seguridad en la nube

• Comprobación de la tabla de rutas del firewall •

Comprobación de la política entre zonas del firewall •

Comprobación de las configuraciones de NAT en el firewall

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Cómo comprobar la información de negociación en ambos lados de una conexión VPN

• Asegúrese de que los PSK de ambos lados sean los mismos.

• Asegúrese de que las políticas IKE y las políticas IPsec de ambos lados sean las mismas. • Las subredes locales y remotas sean pares coincidentes.

Comprobación de la configuración del firewall en su red local y la seguridad Configuración de grupo en la nube

• Asegúrese de que se permitan los paquetes de datos desde su red a la subred de VPC. • Asegúrese de que se permitan los paquetes de datos desde la subred de VPC a su red.

Comprobación de la tabla de rutas del firewall

Verifique que haya una ruta a la subred VPC.

• Asegúrese de que una tabla de rutas contenga una ruta a la red de destino. •

Asegúrese de que la tabla de reenvío de la ruta funcione correctamente.

NO TE

Configuraciones de ruta incorrectas:

1. El bloque CIDR de destino es diferente del bloque CIDR de la VPC. En este caso, el tráfico no se puede enrutar a la interfaz de red pública configurada con la política IPsec.
2. Al configurar una conexión, se especifica la interfaz de salida, en lugar del siguiente salto. ruta estática

   En una red Ethernet, la interfaz de salida no puede aprender las entradas ARP del lado remoto, lo que genera una falla en el reenvío de ruta.
3. La dirección de la puerta de enlace VPN se especifica como el siguiente salto de la ruta.

   Algunos dispositivos de terceros no admiten la recursión automática de rutas. El tráfico VPN se envía desde la interfaz de red pública. Por lo tanto, el siguiente salto debe ser la dirección de puerta de enlace proporcionada por el operador.

Comprobación de la política entre zonas del firewall

• De la zona de confianza a la zona de no confianza: permite el acceso desde su red local red a la subred VPC en la nube.

• De la zona No confiable a la zona Confiable: permite el acceso desde la VPC en la Nube a su red local.

Comprobación de las configuraciones de NAT en el firewall

Compruebe si la puerta de enlace VPN local está detrás del dispositivo NAT (normalmente el firewall de borde). Es decir, la interfaz de salida de la puerta de enlace VPN utiliza una dirección IP privada, que luego el dispositivo NAT traduce a una dirección IP pública.

Este escenario también se denomina travesía NAT IPsec.

5.4.2 Problemas de configuración comunes y soluciones

• PSK inconsistentes: la actualización de PSK se aplica en la siguiente negociación de IKE. Asegúrese que los PSK en ambos extremos son los mismos.

• Políticas de negociación inconsistentes: Verifique el algoritmo de autenticación, Algoritmo de cifrado, versión, algoritmo DH y modo de negociación en IKE

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Política, así como el algoritmo de autenticación, el algoritmo de cifrado, el formato de encapsulación y el algoritmo PFS en la política IPsec. Asegúrese de que los PFS en ambos extremos sean iguales. De forma predeterminada, la configuración de PFS está deshabilitada en algunos dispositivos. • Tráfico de interés: Verifique las configuraciones de ACL en ambos extremos. Se deben usar la dirección IP y la máscara reales.

- Configuración de NAT: no realice NAT en la subred local que utilizó para acceder a la nube.
- Políticas de seguridad: Permitir que todos los protocolos utilizados por la subred local accedan a la subred de la nube y permitir que dos direcciones IP públicas se comuniquen en el puerto UDP 500 y el puerto UDP 4500 mediante ESP o AH. •

Configuraciones de ruta: Establecer la interfaz de salida para acceder a la nube. Subred a la interfaz de túnel o a la interfaz de negociación IPsec. Asegúrese de que la resolución ARP del siguiente salto de la interfaz de salida sea accesible.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

6 Preguntas frecuentes

VPN de edición empresarial 6.1

6.1.1 ¿Qué son los parámetros de negociación de VPN? ¿Cuáles son sus valores predeterminados?

Tabla 6-1 Parámetros de negociación de VPN

Protocolo	Parámetro	Valor
FUERZA	Autenticación Algoritmo	• MD5 (Este algoritmo no es seguro. Tenga cuidado al utilizar este algoritmo). • SHA1 (este algoritmo no es seguro). Tenga cuidado al utilizar este algoritmo). • SHA2-256 (valor predeterminado) • SHA2-384 • SHA2-512
	Cifrado Algoritmo	• 3DES (Este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • AES-128 (valor predeterminado) • AES-192 • AES-256 • AES-256-GCM-16

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Protocolo	Parámetro	Valor
	Algoritmo DH	• Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo 14 (este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) • Grupo 15 (valor predeterminado) • Grupo 16 • Grupo 19 • Grupo 20 • Grupo 21
	Versión	• v1 (no recomendado debido a riesgos de seguridad) • v2 (valor predeterminado)
	Duración de la vida (s)	86400 (valor predeterminado) Unidad: segundo Rango de valores: 60 a 604800
	Identificación local	• Dirección IP La dirección IP local se muestra automáticamente como la EIP de la puerta de enlace VPN, lo que elimina la necesidad de configurarla manualmente. • FQDN De forma predeterminada, el tipo de ID local es la dirección IP y el valor de ID local es el EIP de la puerta de enlace VPN.
	ID de cliente	• Dirección IP • FQDN De forma predeterminada, el tipo de ID de cliente es la dirección IP y el valor de ID de cliente es la dirección IP pública de la puerta de enlace del cliente.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Protocolo	Parámetro	Valor
IPsec	Autenticación Algoritmo	• SHA1 (Este algoritmo no es seguro. Tenga cuidado al utilizar este algoritmo). • MD5 (este algoritmo no es seguro). Tenga cuidado al utilizar este algoritmo). • SHA2-256 (valor predeterminado) • SHA2-384 • SHA2-512
	Cifrado Algoritmo	• AES-128 (valor predeterminado) • AES-192 • AES-256 • 3DES (Este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • AES-256-GCM-16
	PFS	• Deshabilitar (no recomendado debido a riesgos de seguridad) • Grupo DH 1 (este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo DH 2 (este algoritmo es inseguro. Tenga cuidado al utilizar este algoritmo). • Grupo DH 5 (este algoritmo es (Este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 14 (Este algoritmo no es seguro. Tenga cuidado al usarlo). • Grupo DH 15 (valor predeterminado) • Grupo DH 16 • Grupo DH 19 • Grupo DH 20 • Grupo DH 21
	Protocolo de transferencia	• ESP (valor predeterminado)
	Duración de la vida (s)	3600 (valor predeterminado) Unidad: segundo Rango de valores: 30 a 604800

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

NO TE

- Perfect Forward Secrecy (PFS) es una característica de seguridad.

  La negociación de IKE consta de dos fases: la primera y la segunda. La clave de la segunda fase (IPsec SA) se deriva de la clave generada en la primera fase. Una vez divulgada la clave de la primera fase, la seguridad de la VPN IPsec puede verse afectada. Para mejorar la seguridad de la clave, IKE proporciona PFS. Cuando PFS está habilitado, se realizará un intercambio DH adicional durante la negociación de IPsec SA para generar una nueva clave IPsec SA, lo que mejora la seguridad de IPsec SA.

- Por motivos de seguridad, PFS está habilitado en la nube de forma predeterminada. Asegúrese de que PFS también esté habilitado en el dispositivo de enlace de su centro de datos local y que la configuración de PFS en ambos extremos sea la misma. De lo contrario, la negociación fallará.

La vida útil predeterminada, basada en el tráfico, de una SA IPsec es de 1 843 200 KB en la nube y no se puede modificar para la puerta de enlace VPN. Este parámetro no participa en la negociación y no afecta al establecimiento de una SA IPsec.

6.1.2 ¿Se requieren un nombre de usuario y una contraseña para crear una conexión VPN IPsec?

No. Las VPN IPsec utilizan una clave precompartida (PSK) para la autenticación. La PSK se configura en una puerta de enlace VPN y se establecerá una conexión una vez finalizada la negociación de la VPN. Por lo tanto, no se requiere nombre de usuario ni contraseña para crear una conexión VPN IPsec. Generalmente, las VPN SSL, PPTP y L2TP utilizan nombres de usuario y contraseñas para la autenticación.

NO TE

IPsec XAUTH proporciona autenticación extendida para VPN IPsec. Requiere que los usuarios ingresen sus nombres de usuario y contraseñas durante la negociación de la VPN.

Actualmente, VPN no admite IPsec XAUTH.

6.1.3 ¿Se establece automáticamente una conexión VPN IPsec?

Sí. Se establece automáticamente una conexión VPN IPsec.

6.1.4 ¿Qué recursos VPN se pueden monitorear?

Puerta de enlace VPN

Se puede monitorear la siguiente información de ancho de banda de una dirección IP de puerta de enlace VPN: tráfico entrante, ancho de banda entrante, tráfico saliente, ancho de banda saliente y uso de ancho de banda saliente.

Conexión VPN

Se puede monitorear la siguiente información sobre una conexión VPN: estado de la conexión VPN, tiempo promedio de ida y vuelta del enlace (RTT), RTT máximo del enlace, tasa de pérdida de paquetes del enlace, RTT promedio del túnel, RTT máximo del túnel y tasa de pérdida de paquetes del túnel.

Para monitorear el RTT de enlace promedio, el RTT de enlace máximo, la tasa de pérdida de paquetes de enlace, el RTT de túnel promedio, el RTT de túnel máximo y la tasa de pérdida de paquetes de túnel, haga clic en el nombre de la conexión VPN y haga clic en Agregar en el área Control de estado en la página de la pestaña Resumen para agregar elementos de control de estado.

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

6.1.5 ¿Qué hago si no se puede establecer una conexión VPN?

1. Inicie sesión en la consola de administración y seleccione Red privada virtual > Empresa – Conexiones VPN.
2. En la lista de conexiones VPN, ubique la conexión VPN de destino y elija Más > Modificar configuración de políticas a la derecha para ver las políticas IKE e IPsec de la conexión VPN.
3. Verifique las políticas IKE e IPsec para ver si los modos de negociación y los algoritmos de cifrado en ambos extremos de la conexión VPN son los mismos.

   Si la SA IKE se ha configurado en la fase 1 pero no se ha establecido ninguna SA IPsec en la fase 2, las políticas IPsec en ambos extremos de la conexión VPN pueden ser inconsistentes.
4. Verifique si las configuraciones de ACL son correctas.

   Si las subredes de su centro de datos local son 192.168.3.0/24 y 192.168.4.0/24, y las subredes de VPC son 192.168.1.0/24 y 192.168.2.0/24, configure las reglas de ACL para cada subred local a fin de permitir la comunicación con las subredes de VPC. A continuación, se proporciona un ejemplo de configuraciones de ACL: regla 1 permitir IP origen 192.168.3.0

   ```
   0.0.0.255 destino 192.168.1.0 0.0.0.255 regla 2 permitir IP origen 192.168.3.0
   0.0.0.255 destino 192.168.2.0 0.0.0.255 regla 3 permitir IP origen 192.168.4.0
   0.0.0.255 destino 192.168.1.0 0.0.0.255 regla 4 permitir IP origen 192.168.4.0
   0.0.0.255 destino 192.168.2.0 0.0.0.255
   ```
5. Haga ping a los dos extremos de la conexión VPN entre sí para verificar si la conexión VPN es normal.

6.1.6 ¿Se pueden utilizar las EIP como direcciones IP de puerta de enlace VPN?

En Enterprise Edition VPN, las EIP se pueden utilizar como direcciones IP de puerta de enlace de VPN.

Al crear una puerta de enlace VPN, puede vincular EIP como direcciones IP de la puerta de enlace.

6.1.7 ¿Cuáles son los escenarios típicos de VPN IPsec?

Una VPN es una conexión punto a punto que implementa acceso a una red privada entre dos puntos.

- Escenarios aplicables:
  - Se crea una VPN entre diferentes regiones para habilitar VPC entre regiones comunicaciones.
  - Se utiliza un concentrador VPN junto con conexiones de peering VPC y Cloud Conecte conexiones para permitir las comunicaciones entre un centro de datos local y múltiples VPC en la nube.
  - Se utiliza una VPN junto con el NAT de origen para permitir el acceso a una IP específica direcciones a través de las nubes.
- Escenarios no aplicables: – No se
  puede usar una VPN para conectar VPC en la misma región. Se recomienda usar conexiones de peering de VPC para habilitar la comunicación entre VPC en la misma región.
  - No se puede utilizar una VPN entre la nube y su red doméstica que utiliza acceso telefónico PPPoE.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

– No se puede utilizar una VPN entre la nube y los enrutadores 4G/5G.

– No se puede utilizar una VPN entre la nube y sus terminales personales.

6.1.8 ¿Qué son una VPC, una puerta de enlace VPN y una conexión VPN?

VPC permite crear redes virtuales privadas y aisladas. Puede usar una VPN para acceder de forma segura a los ECS en VPC.

Una puerta de enlace VPN es una puerta de enlace de salida para una VPC. Con una puerta de enlace VPN, puede crear una conexión segura, fiable y cifrada entre una VPC y un centro de datos local o entre dos VPC en diferentes regiones.

Una conexión VPN es un túnel de comunicaciones encriptado IPsec seguro y confiable que se establece entre una puerta de enlace VPN y la puerta de enlace del cliente en un centro de datos local.

Para crear una VPN en la nube, realice las siguientes operaciones:

1. Cree una puerta de enlace VPN. Debe especificar la VPC a la que se conectará, así como el ancho de banda y las EIP de la puerta de enlace VPN.
2. Cree una conexión VPN. Debe especificar la EIP de la puerta de enlace utilizada para conectarse a la puerta de enlace del cliente, las subredes y las políticas de negociación.

6.1.9 ¿Cómo planifico bloques CIDR para el acceso a una VPC a través de una conexión VPN?

• Los bloques CIDR de una VPC no pueden entrar en conflicto con los bloques CIDR locales. •

Para evitar conflictos con las direcciones de servicios en la nube, no utilice 127.0.0.0/8. 169.254.0.0/16, 224.0.0.0/3 o 100.64.0.0/10 para su red local.

6.1.10 ¿Qué versión de IKE debo seleccionar al crear una conexión VPN?

Se recomienda IKEv2 porque IKEv1 no es seguro. Además, IKEv2 supera a IKEv1 en la negociación y el establecimiento de conexiones, los métodos de autenticación, el procesamiento del tiempo de espera de detección de pares inactivos (DPD) y el procesamiento del tiempo de espera de asociación de seguridad (SA).

IKEv2 se utilizará ampliamente y IKEv1 se irá eliminando gradualmente.

Introducción a IKEv1 e IKEv2

• Como protocolo híbrido, IKEv1 presenta algunas deficiencias de seguridad y rendimiento debido a su complejidad. Por ello, se ha convertido en un cuello de botella en el sistema IPsec. • IKEv2

soluciona los problemas de IKEv1, conservando sus funciones básicas.

IKEv2 es más simple, eficiente, seguro y robusto que IKEv1. Además, IKEv2 se define en un solo documento de RFC 4306, mientras que IKEv1 se define en varios. Al minimizar las funciones principales y los algoritmos de contraseña predeterminados, IKEv2 mejora considerablemente la interoperabilidad entre diferentes VPN IPsec.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

Riesgos de seguridad de IKEv1

Los algoritmos criptográficos compatibles con IKEv1 no se han actualizado en más de 10 años. Además, IKEv1 no admite algoritmos criptográficos robustos como AES-GCM y ChaCha20-Poly1305. En IKEv1, el bit E (Cifrado) del encabezado ISALMP especifica que las cargas útiles posteriores al encabezado ISALMP están cifradas, pero cualquier verificación de la integridad de los datos de dichas cargas se gestiona mediante una carga útil hash independiente. Esta separación del cifrado y la protección de la integridad de los datos impide el uso del cifrado autenticado (AES-GCM) con IKEv1.

- IKEv1 es vulnerable a ataques de amplificación DoS y ataques de conexión semiabierta. Tras responder a paquetes falsificados, el respondedor mantiene relaciones iniciador-respondedor, lo que consume una gran cantidad de recursos del sistema. recursos.

  Este defecto es inherente a IKEv1 y se soluciona en IKEv2.

El modo agresivo de IKEv1 no es seguro. En este modo, los paquetes de información no se cifran, lo que supone un riesgo de fuga de información. También existen ataques de fuerza bruta dirigidos contra el modo agresivo, como los ataques de intermediario.

Diferencias entre IKEv1 e IKEv2

- Proceso de negociación

  IKEv1 es complejo y consume mucho ancho de banda. La negociación de SA IKEv1 consta de dos fases. En la fase 1 de IKEv1, se establece una SA IKE en modo principal o en modo agresivo. El modo principal requiere tres intercambios entre pares, que totalizan seis mensajes ISAKMP, mientras que el modo agresivo requiere dos intercambios, que totalizan tres mensajes ISAKMP. El modo agresivo es más rápido, pero no ofrece protección de identidad a los pares, ya que el intercambio de claves y la autenticación de identidad se realizan simultáneamente. En la fase 2 de IKEv1, las SA IPsec se establecen mediante tres mensajes ISAKMP en modo rápido.

  En comparación con IKEv1, IKEv2 simplifica el proceso de negociación de SA. IKEv2 solo requiere dos intercambios, con un total de cuatro mensajes, para establecer una SA IKE y un par de SA IPsec. Para crear varios pares de SA IPsec, solo se necesita un intercambio adicional por cada par de SA adicional.

  NO TE

  Para la negociación IKEv1, el modo principal implica nueve (6+3) mensajes, y el modo agresivo implica seis (3+3) mensajes. En cambio, la negociación IKEv2 solo requiere cuatro (2+2) mensajes.

- Métodos de autenticación

  – Solo IKEv1 (que requiere una tarjeta de cifrado) admite la autenticación de sobre digital (HSS-DE).

  – IKEv2 admite la autenticación del Protocolo de autenticación extensible (EAP). IKEv2 puede usar un servidor AAA para autenticar remotamente a usuarios de dispositivos móviles y PC y asignarles direcciones IP privadas. IKEv1 no ofrece esta función y debe usar L2TP para asignar direcciones IP privadas.

  – Solo IKEv2 admite algoritmos de integridad IKE SA.

- Procesamiento de tiempo de espera de DPD

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

– Solo IKEv1 admite el parámetro de intervalo de reintento . Si un dispositivo envía un
Si se recibe un paquete DPD y no se recibe respuesta dentro del intervalo de reintento especificado, el dispositivo registra un evento de fallo de DPD. Cuando el número de
eventos de fallo de DPD llega a 5, se eliminan tanto las SA de IKE como las de IPsec. La negociación de las SA de IKE se reanudará solo cuando haya tráfico que transmitir a través del túnel IPsec.

En IKEv2, el intervalo de retransmisión aumenta de 1, 2, 4, 8, 16, 32 a 64 segundos. Si no se recibe respuesta en ocho transmisiones consecutivas, el extremo del par se considera inactivo y se eliminan las SA de IKE e IPsec.

• Procesamiento de tiempo de espera de IKE SA y procesamiento de tiempo de espera de IPsec SA

En IKEv2, la vida útil flexible de la SA de IKE es 9/10 de la vida útil rígida de la SA de IKE, más o menos un número aleatorio. Esto reduce la probabilidad de que dos extremos inicien la
renegociación simultáneamente. Por lo tanto, no se configura manualmente la vida útil flexible en IKEv2.

Ventajas de IKEv2 sobre IKEv1

• Simplifica el proceso de negociación de SA, mejorando la eficiencia. • Corrige
muchas vulnerabilidades de seguridad criptográfica, mejorando la seguridad. • Admite
autenticación EAP, mejorando la flexibilidad de autenticación y
escalabilidad.

EAP es un protocolo de autenticación que admite múltiples métodos. Su principal ventaja es su escalabilidad. Es decir, se pueden añadir nuevos métodos de autenticación sin modificar el sistema original. La autenticación EAP se ha utilizado ampliamente en redes de acceso telefónico.

• Utiliza una carga útil cifrada basada en ESP. Esta carga útil contiene un algoritmo de cifrado y un algoritmo de integridad de datos. AES-GCM garantiza la confidencialidad, la integridad y la autenticación, y es compatible con IKEv2.

6.1.11 ¿Una VPN permite comunicaciones entre dos VPC?

• Si las dos VPC están en la misma región, use una conexión de emparejamiento de VPC para conectarlas.

• Si las dos VPC están en diferentes regiones, use una VPN para conectarlas.
Las operaciones son las

siguientes: a. Crear una puerta de enlace VPN para cada VPC y crear una conexión VPN.
entre las dos puertas de enlace VPN.

b. Para la conexión VPN, configure la puerta de enlace del cliente en la EIP de la puerta de enlace VPN del par. c.

Para la conexión VPN, configure la subred del cliente en la subred de la
VPC de pares.

d. Establezca las mismas claves precompartidas (PSK) y algoritmos para las dos VPC.

6.2 VPN clásica

 Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

6.2.1 ¿Recibiré una notificación si se interrumpe una conexión VPN?

Se puede supervisar el estado de la conexión VPN. Tras crear una conexión VPN, el servicio VPN informa del estado de la conexión a Cloud Eye, pero no le envía notificaciones de alarma automáticamente. Para recibir notificaciones, cree reglas de alarma y active la función Notificación de Alarma en la consola de Cloud Eye.

Después de crear una conexión VPN, puede ubicar la fila que contiene la conexión VPN y elegir Operación > Ver métrica para ver el estado de la conexión VPN.

6.2.2 ¿Cuáles son las diferencias entre los escenarios de aplicación y los modos de conexión de las VPN IPsec y SSL?

Escenarios

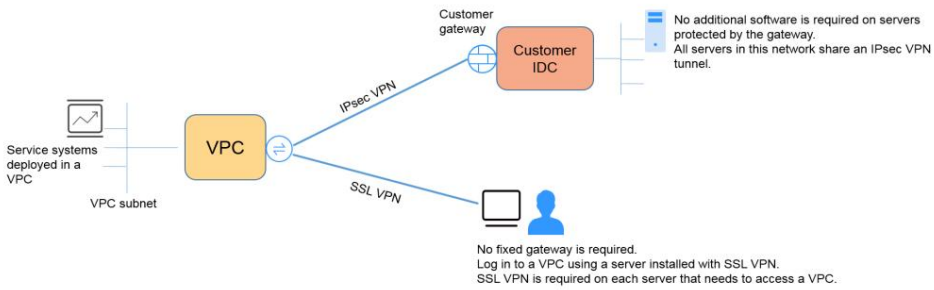
La VPN IPsec conecta dos LAN, como una sucursal y su sede central (o una VPC), o un centro de datos local y una VPC.

Una VPN SSL conecta a un cliente a una red LAN. Por ejemplo, el ordenador portátil de un empleado en viaje de negocios accede a la red interna de la empresa.

Modos de conexión

La VPN IPsec requiere puertas de enlace fijas, como firewalls o routers, en ambos extremos. El administrador debe configurar las puertas de enlace en ambos extremos para completar la negociación de la VPN IPsec.

SSL VPN necesita instalar un software de cliente específico en el servidor, luego el servidor se conecta al dispositivo SSL a través del nombre de usuario y la contraseña.



NO TE

Actualmente, solo se admite VPN IPsec; no se admite VPN SSL.

6.2.3 ¿Cuántas conexiones VPN necesito para conectarme a varios servidores locales?

Una VPN utiliza la tecnología IPsec para conectar su centro de datos local a una VPC en la nube. Por lo tanto, la cantidad de conexiones VPN está relacionada con la cantidad de centros de datos donde se ubican los servidores que se conectarán a la nube, pero no con la cantidad de servidores.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

En la mayoría de los casos, un centro de datos local cuenta con una puerta de enlace pública. Todos los servidores se conectan a Internet a través de esta puerta de enlace. Por lo tanto, solo necesita configurar una conexión VPN para permitir la comunicación entre la VPC y su centro de datos local.

6.2.4 ¿Cuáles son los impactos de una VPN en una red local? ¿Qué cambios se producen en la ruta de acceso a un ECS?

Al configurar una VPN, realice las siguientes operaciones en la puerta de enlace local:

1. Configurar las políticas IKE e IPsec.
2. Especifique el tráfico interesante (reglas ACL).
3. Verifique la configuración de ruta en la puerta de enlace para asegurarse de que el tráfico destinado a una VPC pueda enrutarse a la interfaz de salida correcta (interfaz que tiene una política IPsec limitada).

Una vez completada la configuración de VPN, solo el tráfico que coincide con las reglas de ACL ingresa al túnel VPN.

Por ejemplo, antes de crear una VPN, los usuarios locales acceden al ECS a través de la EIP vinculada a este. Una vez creada la VPN, los flujos de datos que cumplen las reglas de ACL acceden a la dirección IP privada del ECS a través del túnel VPN.

6.2.5 ¿Por qué se muestra No conectado como estado de una conexión VPN creada correctamente?

Después de que se crea una conexión VPN, su estado cambia a Normal solo después de que los servidores en ambos extremos de la conexión VPN se comuniquen entre sí.

- PODER v1:

  Si no pasa tráfico por la conexión VPN durante un tiempo, es necesario renegociarla. El tiempo de negociación depende del valor de Ciclo de vida (s) en la política IPsec. Generalmente, Ciclo de vida (s) se establece en 3600 (1 hora), lo que indica que la negociación se iniciará en el minuto cincuenta y cuatro. Si la negociación tiene éxito, la conexión continúa hasta la siguiente ronda de negociación. Si falla, el estado de la conexión VPN cambia a No conectado en una hora. La conexión solo se puede restablecer después de que ambos extremos de la conexión VPN se comuniquen. La desconexión se puede evitar utilizando una herramienta de monitorización de red, como IP SLA, para generar paquetes.

- IKE v2: si no pasa tráfico a través de la conexión VPN durante un período de tiempo, la conexión VPN permanece en estado conectado.

6.2.6 ¿Dónde puedo agregar rutas en la consola VPN para llegar a las subredes remotas?

Cuando se crea una conexión VPN, las rutas se envían automáticamente para llegar a las subredes remotas.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

6.2.7 ¿Cómo reemplazo una conexión directa con una VPN?

1. Asegúrese de que la puerta de enlace local admita VPN IPsec.
2. Cree una puerta de enlace VPN y una conexión VPN en la nube. Seleccione la VPC que la conexión de Conexión Directa utiliza para la puerta de enlace VPN.

AVISO

Al crear una conexión VPN, configure su subred remota de la siguiente manera para evitar conflictos de enrutamiento.

- Elimine primero la interfaz virtual de la conexión Direct Connect y luego configurar la conexión VPN.
- Divida la subred remota en dos subredes y configure la VPN Conexión. Después de eliminar la conexión Direct Connect, configure nuevamente la conexión VPN.

6.2.8 ¿Cómo puedo acceder a los ECS en casa cuando mi red empresarial está conectada a la nube a través de una VPN?

Una VPN conecta una VPC en la nube y una red de área local (LAN) local.

La red doméstica no es parte de la LAN de su empresa y no se puede conectar directamente a la VPC en la nube.

Si su host en casa necesita acceder a los recursos de VPC en la nube, su host puede acceder directamente al EIP del servicio en la nube o conectarse a la LAN de su empresa a través de VPN SSL (si su empresa admite el acceso SSL) y luego acceder a los recursos de VPC en la nube a través de la LAN.

6.2.9 ¿Cómo configuro DPD para la interconexión con la nube?

De forma predeterminada, DPD está habilitado en el lado de la nube y no se puede deshabilitar.

Configure DPD de la siguiente manera:

- Tipo de DPD: bajo demanda •

Tiempo de inactividad de DPD: 30 s

- Intervalo de retransmisión DPD: 15 s

• Límite de reintentos de DPD: 3 •

Mensaje de DPD: notificación de hash de secuencia

El formato del mensaje DPD en ambos extremos de la conexión VPN debe ser el mismo, pero el tipo de DPD, el tiempo de inactividad, el intervalo de retransmisión y el límite de reintentos pueden ser diferentes.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

6.2.10 ¿Qué es la cuota de VPN?

¿Qué es una cuota?

Las cuotas pueden limitar la cantidad o el número de recursos disponibles para los usuarios, como la cantidad máxima de discos ECS o EVS que se pueden crear.

Si la cuota de recursos existente no puede satisfacer sus requisitos de servicio, puede solicitar una cuota más alta.

¿Cómo puedo ver mi cuota?

1. Inicie sesión en la consola de administración.
2. Haga clic  (el ícono Mis cuotas) en la esquina superior derecha.

   Se muestra la página Cuota de servicio .
3. Visualiza la cuota utilizada y total de cada tipo de recurso en la pantalla.
   página.

   Si una cuota no puede satisfacer los requisitos del servicio, solicite una cuota más alta.

Derechos de autor © Huawei Technologies Co., Ltd.

Machine Translated by Google

A Historial de cambios

Liberado En	Descripción
2025-04-30	Este número es el tercer lanzamiento oficial, que incorpora la siguiente cambio: Se agregó información sobre Enterprise Edition VPN.
30/08/2020	Este número es el segundo lanzamiento oficial, que incorpora la siguiente cambio: Se agregaron algoritmos extendidos IKE e IPsec.
15-08-2018	Este número es el primer lanzamiento oficial.

Derechos de autor © Huawei Technologies Co., Ltd.

FORMATO A
PROPUESTA ECONÓMICA

Estado de México, a 08 de Julio de 2025

COLEGIO NACIONAL DE EDUCACIÓN PROFESIONAL TÉCNICA
P r e s e n t e

De conformidad con lo establecido en la Convocatoria de Invitación a Cuando Menos Tres Personas de Carácter Nacional Electrónica No. IA-11-L5X-011L5X001-N-25-2025, para la contratación del **SERVICIO DE SEGURIDAD PERIMETRAL PARA LA RED LOCAL DE OFICINAS NACIONALES**, manifiesto bajo protesta de decir verdad que:

Oferto los servicios objeto del procedimiento con los precios siguientes:
Servicio de seguridad perimetral a partir del dia siguiente de la notificación del fallo y hasta el 31 de diciembre de 2025.

Partida	Descripción	Tipo	Rango	Cantidad	Costo de renta mensual (sin IVA)	Costo de renta del 7 de junio al 31 de diciembre de 2025 (sin IVA)
1	Equipo de seguridad Firewall	1	1 a 50	2	$9,732.00	$116,784.00
					Subtotal	$116,784.00
					IVA	$18,685.44
					Total	$135,469.44

[Un ciento treinta y cinco mil cuatrocientos sesenta y nueve pesos 44/100 IVA incluido]

- Condiciones de Pago: DE CONFORMIDAD A ESTA CONVOCATORIA.
- Condiciones de Precio: EL PRECIO SERÁ FIJO DURANTE LA VIGENCIA DEL CONTRATO
- Lugar de ejecución del servicio: DE CONFORMIDAD A ESTA CONVOCATORIA.
- Moneda en que cotiza: PESOS MEXICANOS

El precio contenido en esta oferta económica estará vigente durante el procedimiento de contratación.

1) Mi representada acepta los términos y condiciones de pago que se establecen en la convocatoria, que los precios ofertados permanecerán fijos durante el procedimiento de contratación y hasta la emisión del fallo respectivo y, en caso de resultar adjudicado, se mantendrán dichos precios fijos y vigentes hasta la terminación del contrato correspondiente.
2) Estoy consciente de que el precio unitario será el único valor que se tomará en cuenta para efectos de evaluación y adjudicación.

3) Los equipos que se cotizan son nuevos, conforme al Anexo No. 1 "Especificaciones Técnicas" y a los formatos que se acompañan

Asimismo, manifiesto bajo protesta de decir verdad que el servicio que oferto en esta proposición cumple debidamente con las especificaciones establecidas en la convocatoria de referencia y que, en el evento de ser adjudicado, cumpliré cabalmente con las obligaciones a mi cargo que deriven del fallo correspondiente en los términos y condiciones estipulados en la Convocatoria de Invitación a Cuando Menos Tres Personas Pública Nacional Electrónica No. **IA-11-L5X-011L5X001-N-25-2025**, para la contratación del **"SERVICIO DE SEGURIDAD PERIMETRAL PARA LA RED LOCAL DE OFICINAS NACIONALES"**

Atentamente

Apoderado legal de Scitum S.A de C.V.