Virtual Private Network

FAQs

Edición 01

Fecha 2023-11-13

HUAWEI TECHNOLOGIES CO., LTD.

Marcas y permisos


y otras marcas registradas de Huawei pertenecen a Huawei Technologies Co., Ltd.
Todas las demás marcas registradas y los otros nombres comerciales mencionados en este documento son propiedad de sus respectivos titulares.

Aviso

Las funciones, los productos y los servicios adquiridos están estipulados en el contrato celebrado entre Huawei y el cliente. Es posible que la totalidad o parte de los productos, las funciones y los servicios descritos en el presente documento no se encuentren dentro del alcance de compra o de uso. A menos que el contrato especifique lo contrario, ninguna de las afirmaciones, informaciones ni recomendaciones contenidas en este documento constituye garantía alguna, ni expresa ni implícita.

La información contenida en este documento se encuentra sujeta a cambios sin previo aviso. En la preparación de este documento se realizaron todos los esfuerzos para garantizar la precisión de sus contenidos. Sin embargo, ninguna declaración, información ni recomendación contenida en el presente constituye garantía alguna, ni expresa ni implícita.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to “Vul. Response Process”. For details about the policy, see the following website:https://www.huawei.com/en/psirt/vul-response-process
For enterprise customers who need to obtain vulnerability information, visit:https://securitybulletin.huawei.com/enterprise/en/security-advisory

Índice

1 Preguntas populares

1.1 ¿Qué dispositivos se pueden conectar a Huawei Cloud por una VPN?

Huawei Cloud VPN admite el protocolo de Internet Protocol Security (IPsec) estándar. Un dispositivo de su centro de datos local puede conectarse a Huawei Cloud si el dispositivo cumple los siguientes requisitos:

1. Soporta la VPN sobre IPsec.
2. Tiene una dirección IP pública fija, que se puede configurar estáticamente, o traducir con NAT en escenarios transversales de NAT (su dispositivo se despliega detrás de un gateway NAT).

La mayoría de los dispositivos son routers y firewalls. Para obtener más información sobre la configuración de la interconexión, consulte la **Guía del administrador**.

NOTA

- Los routers de banda ancha domésticos comunes, los hosts de Windows que proporcionan servicios VPN (como L2TP) y los terminales móviles personales no pueden conectarse a Huawei Cloud con una VPN.
- Los siguientes productos pueden conectarse a Huawei Cloud con VPN:
  - Dispositivos: firewalls y enrutadores de acceso (AR) de Huawei, firewalls de Hillstone y firewalls de Check Point
  - Servicios en la nube: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) y Microsoft Azure
  - Software: strongSwan
- El protocolo IPsec es un protocolo de IETF estándar. Los dispositivos que admiten IPsec pueden interconectarse con Huawei Cloud con una VPN.

  La mayoría de los routers y firewalls de clase empresarial admiten el protocolo de IPsec.
- Algunos dispositivos admiten IPsec VPN solo después de comprar las licencias de software requeridas.

  El administrador del centro de datos local puede consultar con el proveedor del dispositivo si se requiere una licencia según el modelo del dispositivo.

1.2 ¿Qué son los parámetros de negociación de VPN? ¿Cuáles son sus valores predeterminados?

Tabla 1-1 Parámetros de negociación de VPN

Protocolo	Parámetro	Valor
IKE	Authentication Algorithm	● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● AES-256-GCM-16
	DH Algorithm	● Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 14 (valor predeterminado) ● Group 16 ● Group 19 ● Group 20 ● Group 21
	Version	● v1 (no recomendado debido a riesgos de seguridad) ● v2 (valor predeterminado)
	Lifetime (s)	**86400** (valor predeterminado) Unidad: segundo Rango de valores: de **60** a **604800**

Protocolo	Parámetro	Valor
	Local ID	● Dirección IP La dirección IP local se muestra automáticamente como la EIP del gateway de VPN, eliminando la necesidad de configurarlo manualmente. ● FQDN De forma predeterminada, el tipo de ID local es la dirección IP y el valor de ID local es la EIP del gateway de VPN.
	Customer ID	● 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 del gateway del cliente.
IPsec	Authentication Algorithm	● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● AES-256-GCM-16
	PFS	● DH grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 14 (valor predeterminado) ● DH group 15 ● DH group 16 ● DH group 19 ● DH group 20 ● DH group 21 ● Deshabilitar

Protocolo	Parámetro	Valor
	Transfer Protocol	● ESP (valor predeterminado)
	Lifetime (s)	**3600** (valor predeterminado) Unidad: segundo Rango de valores: de **30** a **604800**

NOTA

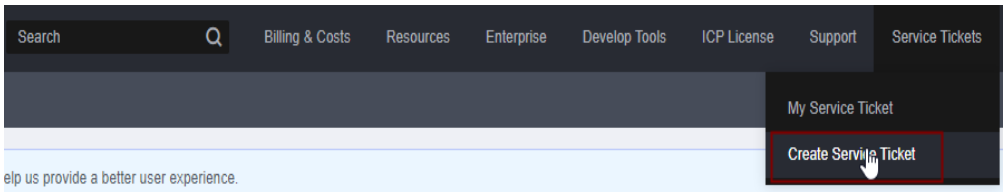
- Perfect Forward Secrecy (PFS) es una característica de seguridad.

  La negociación de IKE tiene dos fases, la fase 1 y la fase 2. La clave de la fase 2 (IPsec SA) se deriva de la clave generada en la fase 1. Una vez que se divulga la clave en la fase 1, la seguridad de la VPN IPsec puede verse afectada negativamente. Para mejorar la seguridad de la clave, IKE proporciona PFS. Cuando PFS está habilitado, se realizará un intercambio de DH adicional durante la negociación de SA de IPsec para generar una nueva clave de SA de IPsec, lo que mejorará la seguridad de SA de IPsec.
- Por motivos de seguridad, PFS está habilitado en Huawei Cloud de forma predeterminada. Asegúrese de que PFS también esté habilitado en el dispositivo de gateway del centro de datos local y de que la configuración de PFS en ambos extremos sea la misma. De lo contrario, la negociación no funcionará.
- La vida útil predeterminada basada en el tráfico de una SA IPsec es de 1,843,200 KB y no se puede cambiar para Huawei Cloud VPN. Este parámetro no participa en la negociación y no tiene ningún impacto en el establecimiento de una SA IPsec.

1.3 ¿Qué tipos de tickets de servicio VPN hay? ¿Cómo puedo crear un ticket de servicio de VPN?

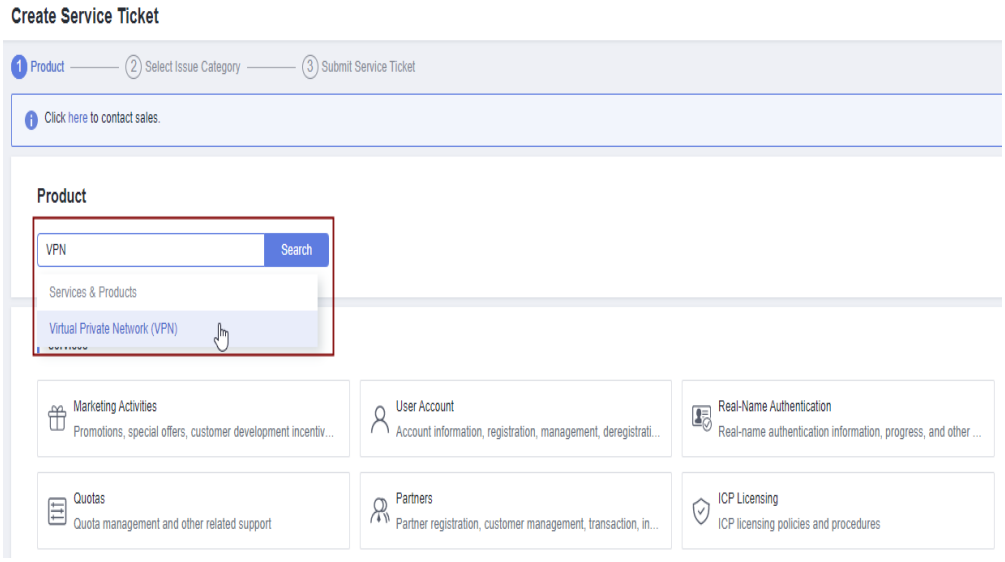
1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la consola de gestión, seleccione **Service Tickets** > **Create Service Ticket**.

   Figura 1-1 Crear ticket de servicio

3. Busque **VPN** y seleccione **Virtual Private Network (VPN)**.

Figura 1-2 Selección de **Virtual Private Network (VPN)**



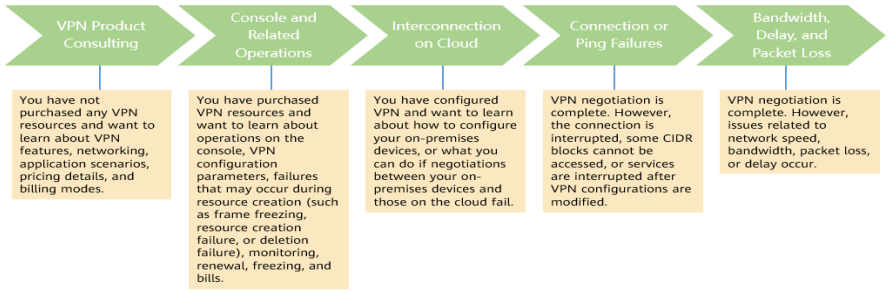
4. Seleccione una categoría de error.

Figura 1-3 Seleccionar categoría de problema

NOTA

Cuando **envía un ticket de servicio**, seleccione una categoría de problema para facilitar la gestión del problema.

Figura 1-4 Categoría de emisión y base de clasificación



1.4 ¿Puedo desplegar una aplicación en la nube y una base de datos en un centro de datos local y conectarlos por una VPN?

Sí.

Una VPN conecta una VPC y un centro de datos local.

Después de configurar una VPN, el tráfico de servicio se puede transmitir entre la VPC y el centro de datos local. Para un servidor de aplicaciones en la nube, el acceso a una base de datos local es lógicamente el mismo que el acceso a otros hosts en la misma LAN. Dado esto, es factible utilizar una VPN para conectar una aplicación en la nube a una base de datos en un centro de datos local.

Este es un escenario típico de IPsec VPN.

Además, no hay limitaciones en el iniciador de servicio. Es decir, las solicitudes de servicio se pueden iniciar desde la nube o el centro de datos local.

AVISO

- Después de configurar una VPN, compruebe la latencia de la red y la tasa de pérdida de paquetes para garantizar un buen funcionamiento del servicio.
- Se recomienda que ejecute el comando ping para comprobar la pérdida de paquetes y los detalles de latencia de red.

1.5 ¿Puedo visitar sitios web internacionales con una VPN?

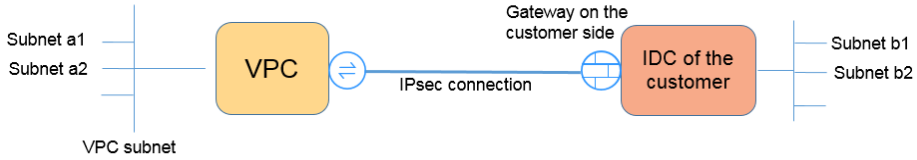
No.

La VPN conecta una VPC y la red de un centro de datos local, es decir, una conexión sitio a sitio.

1.6 ¿Qué es una conexión de VPN? ¿Cómo configuro el número de conexiones de VPN al comprar un gateway de VPN?

Una conexión de VPN de Huawei Cloud es una conexión IPsec establecida entre un gateway de VPN en la nube y una dirección IP pública independiente de un centro de datos local. Puede configurar varias subredes locales (subredes VPC) y subredes de clientes (subredes locales) para una conexión de VPN.

El número de conexiones de VPN que se van a crear viene determinado por el número de centros de datos locales. Cada conexión de VPN puede conectar una VPC a un solo centro de datos local.



NOTA

En la figura anterior, si las subredes a1 y a2 en Huawei Cloud necesitan comunicarse con las subredes b1 y b2 en la red local, solo necesita crear una conexión de VPN, con los bloques CIDR de origen establecidos en a1 y a2 y los bloques CIDR de destino establecidos en b1 y b2.

1.7 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Para ver el estado de una conexión de VPN, haga clic en en la columna **Monitoring** de la conexión de VPN.

1.8 ¿Se requiere un nombre de usuario y contraseña para crear una conexión VPN IPsec?

No. Huawei Cloud IPsec VPN utiliza una clave precompartida (PSK) para la autenticación. El PSK se configura en un gateway de VPN y se establecerá una conexión después de que se complete la negociación de VPN. Por lo tanto, no se requiere ningún nombre de usuario o contraseña para crear una conexión de VPN IPsec. En general, las VPN SSL, PPTP y L2TP usan nombres de usuario y contraseñas para la autenticación.

NOTA

IPsec XAUTH proporciona autenticación extendida para IPsec VPN. Requiere que los usuarios introduzcan sus nombres de usuario y contraseñas durante la negociación de VPN.

Huawei Cloud VPN no es compatible con IPsec XAUTH.

1.9 ¿Cuáles son las diferencias entre IPsec VPN y SSL VPN en escenarios de aplicaciones y modos de conexión?

Escenarios de aplicación

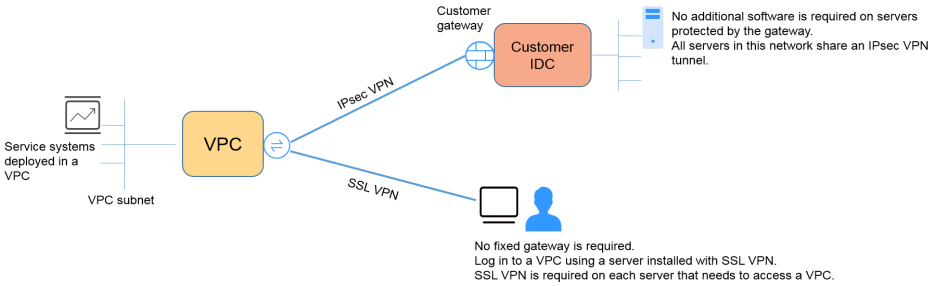
IPsec VPN conecta dos LAN, como una sucursal y su sede, o un centro de datos local y una VPC.

SSL VPN conecta un cliente a una LAN. Por ejemplo, el ordenador portátil de un empleado en un viaje de negocios accede a la red interna de la empresa.

Modos de conexión

IPsec VPN requiere gateway fijos, como firewalls o enrutadores, en ambos extremos. El administrador debe configurar gateway en ambos extremos para permitirles completar la negociación de IPsec VPN.

SSL VPN requiere un programa cliente específico instalado en los hosts. Los usuarios deben ingresar nombres de usuario y contraseña para conectar los hosts a los servidores de SSL.



NOTA

Huawei Cloud solo admite IPsec VPN.

1.10 ¿Se establece automáticamente una conexión de VPN IPsec?

Sí. Una conexión IPsec de VPN se establece automáticamente.

1.11 ¿Cómo se me cobrará por el uso de una VPN? ¿Se me cobrará por las EIP del gateway de VPN?

Las VPN son facturadas por los siguientes elementos en una base anual/mensual o de pago por uso.

- Gateway de VPN
- Conexión VPN

  Por defecto, se incluyen 10 grupos de conexiones de VPN gratuitos en la compra de un gateway de VPN. Puede comprar las conexiones de VPN adicionales si es necesario.
- Ancho de banda de EIP de un gateway de VPN

  El ancho de banda del gateway de VPN se puede facturar por el tráfico o el ancho de banda.

  a. Un gateway de VPN anual/mensual solo se puede facturar por ancho de banda. El precio de un gateway de VPN anual/mensual incluye el precio de las conexiones de VPN que se pueden crear para el gateway y el precio del ancho de banda.

  b. El ciclo de facturación del modo de facturación de pago por uso es de 1 hora. Cuando crea un gateway de VPN de pago por uso, el sistema le solicita que cree conexiones de VPN. Por defecto, se incluyen 10 grupos de conexiones de VPN gratuitos en la compra de un gateway de VPN. Si se requieren más grupos de conexión, debe comprarlos.

NOTA

Un gateway de VPN no puede compartir un ancho de banda con una EIP vinculada a un ECS.

1.12 ¿Se puede retener la EIP de un gateway de VPN después de que se elimine el gateway de VPN?

Si una EIP de pago por uso está vinculada a un gateway de VPN de pago por uso, la eliminación del gateway de VPN también eliminará la EIP vinculada.

Para conservar tal EIP de pago por uso, desvíselo antes de eliminar el gateway de VPN.

1.13 ¿Qué recursos de VPN se pueden monitorear?

Gateway de VPN

Se puede supervisar la siguiente información de ancho de banda de una dirección IP de gateway de VPN: tráfico entrante, ancho de banda entrante, tráfico saliente, ancho de banda saliente y uso de ancho de banda saliente.

Para ver la información de supervisión, haga clic en  en la columna **Gateway IP Address** de la lista de gateway de VPN.

Conexión de VPN

Se puede supervisar la siguiente información sobre una conexión de VPN: estado de la conexión de 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 supervisar RTT de enlace promedio, RTT de enlace máximo, tasa de pérdida de paquetes de enlace, RTT de túnel promedio, RTT de túnel máximo y tasa de pérdida de paquetes de túnel, haga clic en el nombre de la conexión de VPN y haga clic en **Add** en el área **Health Check** de la página de fichas **Summary** para agregar elementos de comprobación de estado.

Para ver el estado de una conexión de VPN, haga clic en  en la columna **Monitoring** de la conexión de VPN.

1.14 ¿En qué dirección está limitado el ancho de banda de VPN? ¿Cuál es la unidad de ancho de banda?

El ancho de banda del gateway de VPN comprado se aplica a la dirección de salida de Huawei Cloud. Para lograr un balanceo entre los anchos de banda en las direcciones de entrada y de salida, el ancho de banda en la dirección de entrada se limita de la siguiente manera:

- Si el ancho de banda adquirido es de 10 Mbit/s o menos, el ancho de banda en la dirección de entrada está limitado a 10 Mbit/s.
- Si el ancho de banda adquirido es mayor que 10 Mbit/s, el ancho de banda en la dirección de entrada es el mismo que el ancho de banda comprado.

La unidad de ancho de banda es Mbit/s y la del tráfico es GB.

1.15 ¿Cómo se prueba la velocidad de red de una conexión de VPN?

Entorno de prueba: Se ha creado una conexión de VPN. Se han creado ECS en las subredes locales de las VPC en los dos extremos de la conexión de VPN. Los ECS pueden hacer ping entre sí.

Cuando el ancho de banda de un gateway de VPN adquirido es de 200 Mbit/s:

1. Cuando los ECS en los dos extremos de la conexión de VPN ejecutan Windows, iPerf3 y FileZilla (una aplicación de FTP gratuita para cargar y descargar archivos) se utilizan para probar la velocidad de la red. El resultado de la prueba es de 180 Mbit/s, cumpliendo los requisitos.

   NOTA

   El protocolo FTP basado en TCP tiene un mecanismo de control de congestión, y el protocolo IPsec añade nuevas cabeceras a los paquetes originales. Como tal, es normal en la industria, tener una desviación de velocidad de red de aproximadamente el 10%.

   Figura 1-5 muestra el resultado de probar el ancho de banda de 200 Mbit/s en el cliente iPerf3.

   Figura 1-5 Resultado de la prueba para 200 Mbit/s de ancho de banda (cliente de iPerf3)

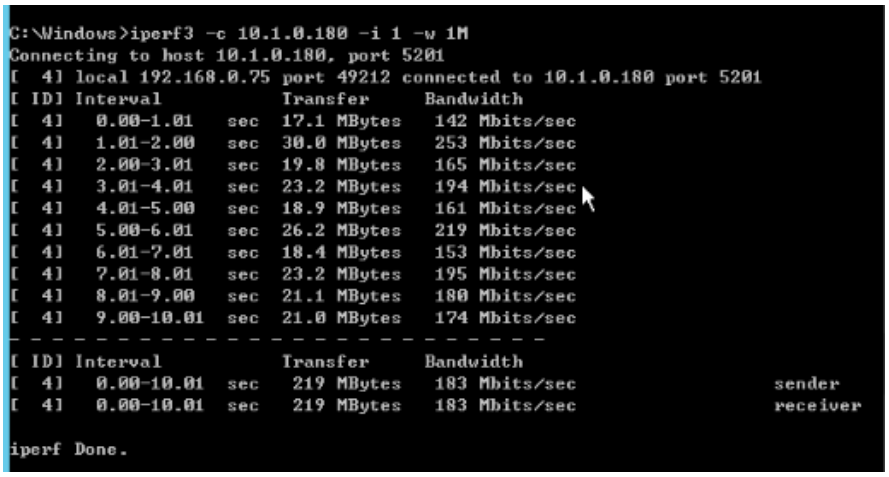
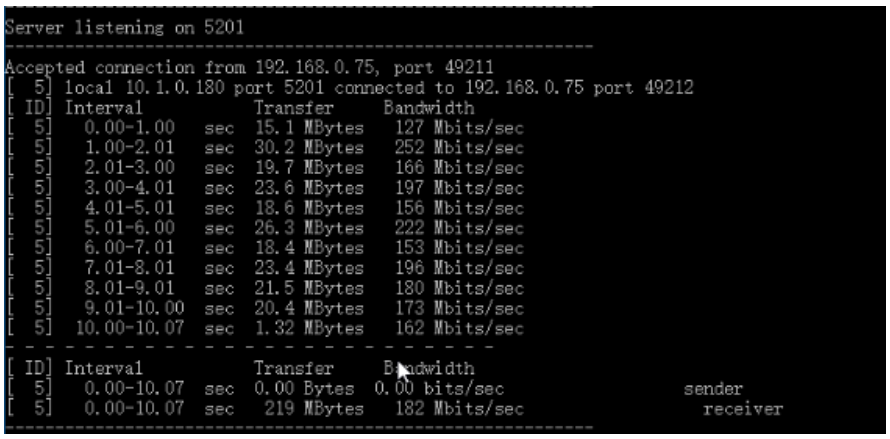


   Figura 1-6 muestra el resultado de probar el ancho de banda de 200 Mbit/s en el servidor iPerf3.

Figura 1-6 Resultado de la prueba para un ancho de banda de 200 Mbit/s (servidor de iPerf3)

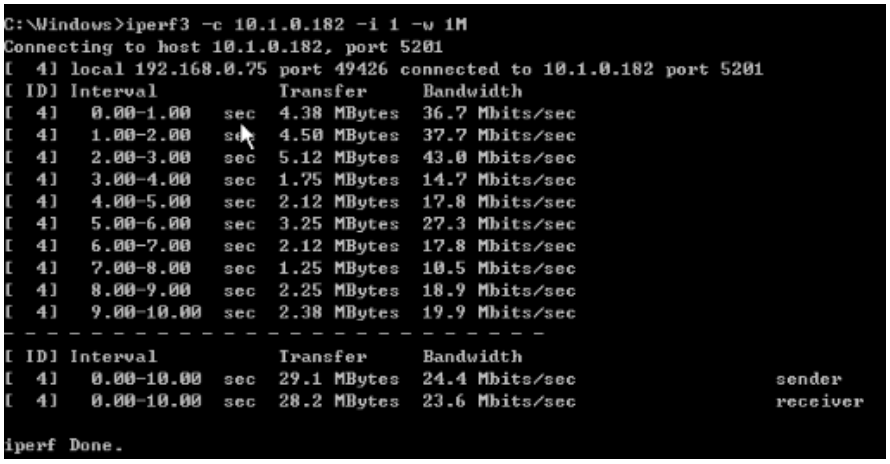


2. Cuando los ECS en los dos extremos de la conexión de VPN ejecutan CentOS 7, iPerf3 se utiliza para probar la velocidad de la red. El resultado de la prueba es de 180 Mbit/s, cumpliendo los requisitos.
3. Cuando el ECS que funciona como un servidor ejecuta CentOS 7 y el ECS que funciona como un cliente ejecuta Windows, iPerf3 y FileZilla se utilizan para probar la velocidad de la red. El resultado de la prueba es de 20 Mbit/s, no cumpliendo los requisitos.

   Esto se debe a que las implementaciones de TCP en Windows y Linux son diferentes.

   Figura 1-7 muestra el resultado del uso de iPerf3 para probar la velocidad de red entre dos ECS que ejecutan diferentes sistemas operativos.

Figura 1-7 Resultado de la prueba en iPerf3



Cuando el ancho de banda de un gateway de VPN adquirido es de 1000 Mbit/s:

NOTA

Algunas regiones admiten solo 300 Mbit/s de ancho de banda de forma predeterminada. Si se requiere un ancho de banda más alto, solicite un ancho de banda de 300 Mbit/s y luego **envíe un ticket de servicio** para ampliar la capacidad.

El ancho de banda del gateway de VPN es compartido por todas sus conexiones de VPN. Para utilizar plenamente el gran ancho de banda de 1000 Mbit/s, despliegar múltiples ECS con altas especificaciones ya que el rendimiento de reenvío de un solo ECS es limitado. Se recomiendan ECS con sus NICs que admitan un ancho de banda de 2 Gbit/s o superior.

Conclusiones: Según los resultados de las pruebas anteriores, los anchos de banda de los gateways de Huawei Cloud VPN cumplen los requisitos. Para aprovechar al máximo el ancho de banda adquirido, se recomienda utilizar servidores que ejecuten el mismo sistema operativo y NIC que cumplan determinados requisitos en los dos extremos de una conexión de VPN.

1.16 ¿Puede una VPN facturada por tráfico usar un paquete de datos compartidos?

No.

El servicio VPN se factura de forma independiente y no puede usar paquetes de datos compartidos.

1.17 ¿Cómo cambio el modo de facturación de un gateway de VPN de pago por uso a anual/mensual?

Requisitos previos

- El gateway de VPN de pago por uso se factura por ancho de banda.
- Para cambiar el modo de facturación de un gateway de VPN facturado por tráfico de pago por uso a anual/mensual, primero cambie el gateway de VPN de ser facturado por tráfico a ser facturado por ancho de banda y luego de pago por uso a anual/mensual.

Procedimiento

Realice las siguientes operaciones:

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** y elija **Networking** > **Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network** >**Enterprise - VPN Gateways**.
5. En la página **VPN Gateways**, busque la fila que contiene el gateway de VPN de destino, elija **More** > **Change Billing Mode** en la columna **Operation**.
6. En el cuadro de diálogo **Change Billing Mode**, haga clic en **OK**.

   NOTA

   El modo de facturación de un gateway VPN no se puede cambiar de anual/mensual a pago por uso y el ancho de banda del gateway VPN incluido en la suscripción anual/mensual no se puede reducir.
7. Confirme la información del gateway de VPN, establezca una duración de renovación y haga clic en **Pay**.
8. En la página de pago, confirme la información del pedido, seleccione un cupón o descuento, seleccione un método de pago y haga clic en **Pay**.

NOTA

Cambiar el modo de facturación de un gateway de VPN de pago por uso a anual/mensual no afectará sus servicios.

1.18 ¿Cuáles son las relaciones entre una VPC, un gateway de VPN y una conexión de VPN?

- Una VPC es una red privada en la nube. Se pueden crear múltiples VPC en la misma región mientras están aisladas entre sí. Una VPC se puede dividir en varias subredes.
- Se crea un gateway de VPN en una VPC y es el punto de acceso de una conexión de VPN. Una VPC en Huawei Cloud puede tener múltiples gateway de VPN, y un gateway de VPN puede tener múltiples conexiones de VPN.
- Se crea una conexión de VPN para un gateway de VPN y conecta una VPC a un centro de datos local (o una VPC en otra región).

  NOTA

  El número de conexiones de VPN es irrelevante para el número de subredes locales o el número de subredes de clientes. Solo está relacionado con el número de centros de datos locales (o VPC en otras regiones) que se van a conectar a su VPC. Las conexiones de VPN creadas se muestran en la lista de conexiones de VPN. También puede ver el número de conexiones de VPN creadas para cada gateway de VPN.

1.19 ¿Qué son un gateway de cliente y una subred de cliente en una conexión de VPN?

Se crea una conexión de VPN en Huawei Cloud. Como tal, una subred de una VPC de Huawei Cloud es una subred local, y un gateway de VPN creada en Huawei Cloud es un gateway local. La subred y el gateway de un centro de datos local conectado a la VPC son una subred de cliente y un gateway de cliente, respectivamente.

La dirección IP de un cliente es una dirección IP pública.

1.20 ¿Cuántas conexiones de VPN necesito para conectar varios servidores locales a la nube?

Huawei Cloud VPN utiliza tecnología de IPsec VPN. Conecta una VPC en la nube y su centro de datos local. Por lo tanto, el número de conexiones de VPN es irrelevante para el número de servidores que se conectarán a la nube, pero para el número de centros de datos donde se encuentran los servidores.

Se pueden enlazar dos EIP a un gateway de VPN para la comunicación con un gateway de cliente.

- Si un centro de datos local solo tiene un gateway de salida, todos los servidores o hosts del centro de datos se conectan a Internet con este gateway. En este caso, debe configurar un grupo de conexiones de VPN que consta de dos conexiones de VPN. Es decir, configure una conexión de VPN para cada una de las dos EIP del gateway de VPN para comunicarse con el gateway de salida en el centro de datos local.

- Si un centro de datos local tiene dos gateway de salida, los servidores o hosts de usuario en el centro de datos se conectan a Internet con las gateway de salida de remolque. En este caso, debe configurar dos grupos de conexiones de VPN, cada uno de los cuales consta de dos conexiones de VPN. Es decir, configure una conexión de VPN para cada uno de los dos EIP de cada gateway de VPN para comunicarse con ambos gateway de salida en el centro de datos local.

1.21 ¿Una VPN permite comunicaciones entre dos VPC?

- Si las dos VPC están en la misma región, utilice una interconexión de VPC para conectarlas.
- Si las dos VPC están en diferentes regiones, use una VPN para conectarlas. Las operaciones son las siguientes:
  a. Cree un gateway de VPN para cada VPC y cree una conexión de VPN entre los dos gateway de VPN.
  b. Para la conexión de VPN, establezca el gateway del cliente en la EIP del gateway de VPN del mismo nivel.
  c. Para la conexión de VPN, establezca la subred del cliente en la subred de la VPC del mismo nivel.
  d. Establezca las mismas claves precompartidas (PSK) y algoritmos para las dos VPC.

1.22 ¿Cuáles son los impactos de una VPN en una red local? ¿Cuáles son los cambios en la ruta para acceder a un ECS?

Al configurar una VPN, debe realizar las siguientes operaciones en el gateway en su centro de datos local:

- Configure las políticas IKE e IPsec.
- Establezca el modo de conexión como basado en ruta o basado en políticas.
- Compruebe la configuración de la ruta en el gateway para asegurarse de que el tráfico destinado a una VPC de Huawei Cloud se puede enrutar a la interfaz de salida correcta (interfaz que tiene una política IPsec vinculada).

1.23 ¿Puedo conectar una red con dos salidas a una VPC por dos conexiones de VPN?

Sí.

1.24 ¿Cómo puedo evitar las desconexiones de VPN?

Las conexiones de VPN se renegocian cuando la vida útil de la SA IPsec está a punto de expirar o cuando los datos transmitidos con una conexión de VPN superan los 20 GB. Por lo general, la renegociación no interrumpe las conexiones de VPN.

La mayoría de las desconexiones se deben a configuraciones incorrectas en los dos extremos de la conexión de VPN o a fallos de renegociación debidos a excepciones de Internet.

Las causas comunes de las desconexiones son las siguientes:

- Las ACL en ambos extremos de la conexión de VPN no coinciden.
- La configuración de la vida útil de SA en ambos extremos de la conexión de VPN es diferente.
- Dead Peer Detection (DPD) no está configurada en el dispositivo del centro de datos local.
- La configuración se modifica cuando la conexión de VPN está en uso.
- La fluctuación se produce en la red del operador.

Por lo tanto, asegúrese de que las siguientes configuraciones de VPN son correctas para mantener las conexiones de VPN activas:

- En los dos extremos de la conexión de VPN, se invierten las configuraciones de subred local y remota.
- La configuración de la duración de la SA en ambos extremos de la conexión de VPN es la misma.
- DPD está habilitado en el dispositivo del gateway local y el número de veces de detección es de 3 o más.
- Los parámetros se modifican en ambos extremos de la conexión de VPN durante el uso de la conexión de VPN.
- Establezca TCP MAX-MSS en 1300 para el dispositivo del gateway local.
- El ancho de banda del dispositivo del gateway local es lo suficientemente grande para la conexión de VPN.
- La negociación de conexión de VPN se puede activar por ambos extremos y la negociación activa se ha habilitado en el dispositivo de gateway local.

1.25 ¿Qué hago si no se establece una conexión de VPN?

1. Inicie sesión en la consola de gestión y elija **Virtual Private Network** > **Enterprise – VPN Connections**.
2. En la lista de conexiones de VPN, localice la conexión de VPN de destino y elija **More** > **Modify Policy Settings** a la derecha para ver las políticas IKE e IPsec de la conexión de VPN.
3. Compruebe las políticas IKE e IPsec para ver si los modos de negociación y los algoritmos de encriptación en ambos extremos de la conexión de 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 de VPN pueden ser inconsistentes.
4. Compruebe si las reglas 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 para permitir la comunicación con las subredes de VPC. A continuación se proporciona un ejemplo de configuraciones de ACL:

   ```
   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. Haga ping a los dos extremos de la conexión de VPN entre sí para comprobar si la conexión de VPN es normal.

1.26 ¿Se pueden usar las EIP como direcciones IP de gateway de VPN?

No.

Cuando crea un gateway de VPN, su dirección IP se asigna automáticamente. Esta dirección IP tiene configuraciones preestablecidas y se puede utilizar para la interconexión con una VPC. Sin embargo, una EIP no puede utilizarse para la interconexión con una VPC.

1.27 ¿Por qué una conexión de VPN siempre está en estado no conectado después de completar su configuración?

La configuración puede ser incorrecta.

1. En los dos extremos (en la nube y en el centro de datos local) de la conexión de VPN, asegúrese de que las claves precompartidas (PSK) y la información de negociación sean consistentes, las subredes locales y remotas se inviertan, y los gateway locales y remotos también se invierten.
2. Asegúrese de que las rutas, NAT y políticas de seguridad estén correctamente configuradas en el dispositivo de su centro de datos local.

1.28 ¿Necesito configurar las reglas de ACL en la consola de gestión de Huawei Cloud después de configurar las reglas de ACL en el dispositivo de gateway local?

Es necesario configurar las reglas de política (reglas de ACL) para una conexión de VPN en la consola de gestión de Huawei Cloud solo cuando **VPN Type** está configurado en **Policy-based**.

2 Consultoría General

2.1 ¿Cuáles son los escenarios típicos de IPsec VPN?

Una VPN es una conexión punto a punto que implementa el acceso a la red privada entre dos puntos.

- Casos de aplicación:
  - Se crea una VPN entre diferentes regiones de Huawei Cloud para permitir las comunicaciones de VPC entre regiones.
  - Se crea una VPN entre las VPC de Huawei Cloud y otra nube pública, por ejemplo, Alibaba Cloud.
  - Se crea una VPN entre una VPC de Huawei Cloud y su centro de datos local.
  - Un concentrado de VPN se utiliza junto con las interconexiones de VPC y conexiones de Cloud Connect para permitir las comunicaciones entre un centro de datos local y varias VPC en la nube.
  - Una VPN se utiliza junto con NAT de origen para permitir el acceso a direcciones IP específicas en las nubes.
- Escenarios no aplicables:
  - No se puede usar una VPN para conectar VPCs en la misma región de Huawei Cloud. Se recomienda utilizar las interconexiones de VPC para habilitar las comunicaciones entre VPC en la misma región.
  - No se puede usar una VPN entre Huawei Cloud y su red doméstica que utilice PPPoE dial-up.
  - No se puede usar una VPN entre Huawei Cloud y los routers 4G/5G.
  - No se puede usar una VPN entre Huawei Cloud y sus terminales personales.

2.2 ¿Qué son una VPC, un gateway de VPN y una conexión de VPN?

VPC permite crear redes virtuales privadas y aisladas. Puede usar VPN para acceder de forma segura a ECS en VPC.

Un gateway VPN es un gateway de salida para una VPC. Con un gateway de VPN, puede crear una conexión segura, confiable y cifrada entre una VPC y un centro de datos local o entre dos VPC en diferentes regiones.

Una conexión de VPN es un túnel de comunicaciones cifrado IPsec seguro y confiable establecido entre un gateway de VPN y el gateway del cliente en un centro de datos local.

Para crear una VPN en la nube, realice las siguientes operaciones:

1. Cree un gateway de VPN. Debe especificar la VPC que se va a conectar, así como el ancho de banda y las EIP del gateway de VPN.
2. Cree una conexión de VPN. Debe especificar la EIP de gateway utilizado para conectarse al gateway del cliente, las subredes y las políticas de negociación.

2.3 ¿Cuáles son las relaciones entre una VPC, un gateway de VPN y una conexión de VPN?

- Una VPC es una red privada en la nube. Se pueden crear múltiples VPC en la misma región mientras están aisladas entre sí. Una VPC se puede dividir en varias subredes.
- Se crea un gateway de VPN en una VPC y es el punto de acceso de una conexión de VPN. Una VPC en Huawei Cloud puede tener múltiples gateway de VPN, y un gateway de VPN puede tener múltiples conexiones de VPN.
- Se crea una conexión de VPN para un gateway de VPN y conecta una VPC a un centro de datos local (o una VPC en otra región).

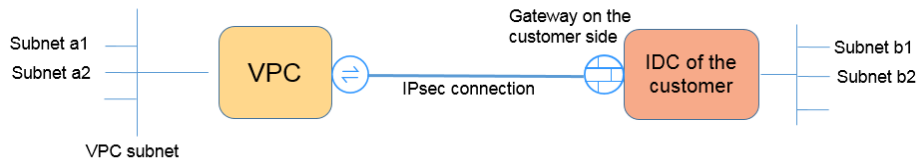
  NOTA

  El número de conexiones de VPN es irrelevante para el número de subredes locales o el número de subredes de clientes. Solo está relacionado con el número de centros de datos locales (o VPC en otras regiones) que se van a conectar a su VPC. Las conexiones de VPN creadas se muestran en la lista de conexiones de VPN. También puede ver el número de conexiones de VPN creadas para cada gateway de VPN.

2.4 ¿Qué es una conexión de VPN? ¿Cómo configuro el número de conexiones de VPN al comprar un gateway de VPN?

Una conexión de VPN de Huawei Cloud es una conexión IPsec establecida entre un gateway de VPN en la nube y una dirección IP pública independiente de un centro de datos local. Puede configurar varias subredes locales (subredes VPC) y subredes de clientes (subredes locales) para una conexión de VPN.

El número de conexiones de VPN que se van a crear viene determinado por el número de centros de datos locales. Cada conexión de VPN puede conectar una VPC a un solo centro de datos local.



NOTA

En la figura anterior, si las subredes a1 y a2 en Huawei Cloud necesitan comunicarse con las subredes b1 y b2 en la red local, solo necesita crear una conexión de VPN, con los bloques CIDR de origen establecidos en a1 y a2 y los bloques CIDR de destino establecidos en b1 y b2.

2.5 ¿Qué son un gateway de cliente y una subred de cliente en una conexión de VPN?

Se crea una conexión de VPN en Huawei Cloud. Como tal, una subred de una VPC de Huawei Cloud es una subred local, y un gateway de VPN creada en Huawei Cloud es un gateway local. La subred y el gateway de un centro de datos local conectado a la VPC son una subred de cliente y un gateway de cliente, respectivamente.

La dirección IP de un cliente es una dirección IP pública.

2.6 ¿Cómo planifico los bloques CIDR para el acceso a una VPC por una conexión de VPN?

- Los bloques CIDR de una VPC no pueden entrar en conflicto con bloques CIDR locales.
- Para evitar conflictos con 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.

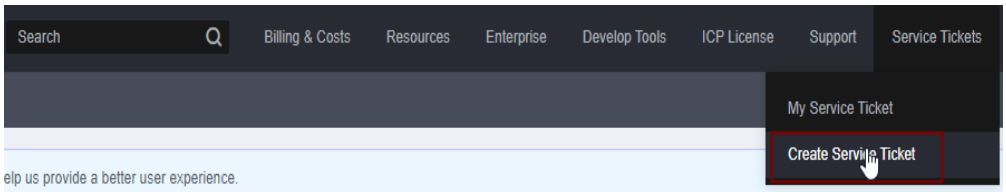
2.7 ¿Se establece automáticamente una conexión de VPN IPsec?

Sí. Una conexión IPsec de VPN se establece automáticamente.

2.8 ¿Qué tipos de tickets de servicio VPN hay? ¿Cómo puedo crear un ticket de servicio de VPN?

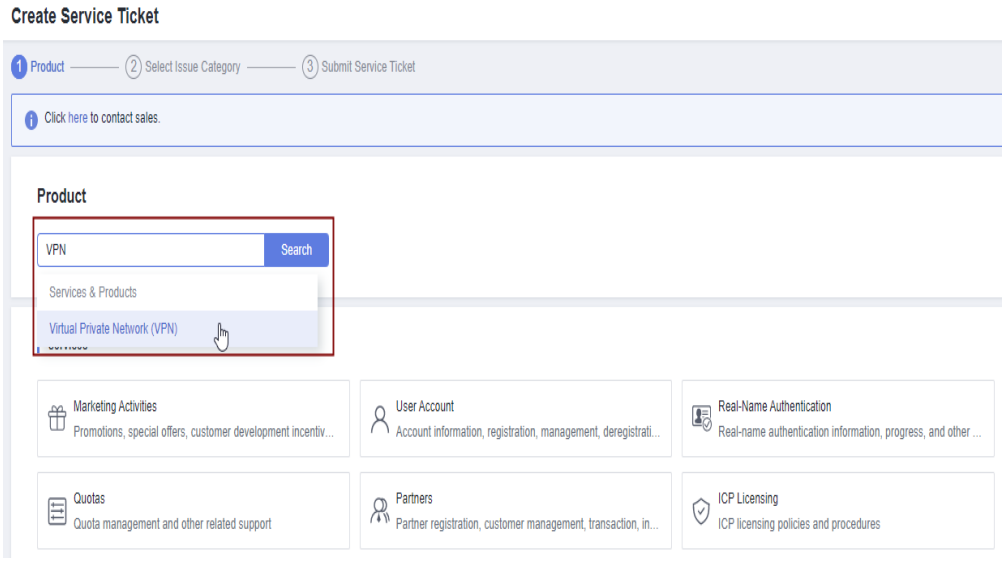
1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la consola de gestión, seleccione **Service Tickets** > **Create Service Ticket**.

   Figura 2-1 Crear ticket de servicio

3. Busque **VPN** y seleccione **Virtual Private Network (VPN)**.

Figura 2-2 Selección de **Virtual Private Network (VPN)**



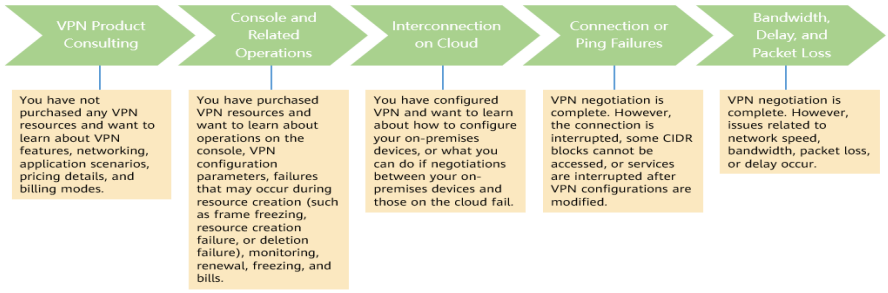
4. Seleccione una categoría de error.

Figura 2-3 Seleccionar categoría de problema

NOTA

Cuando **envía un ticket de servicio**, seleccione una categoría de problema para facilitar la gestión del problema.

Figura 2-4 Categoría de emisión y base de clasificación



2.9 ¿Qué dispositivos se pueden conectar a Huawei Cloud por una VPN?

Huawei Cloud VPN admite el protocolo de Internet Protocol Security (IPsec) estándar. Un dispositivo de su centro de datos local puede conectarse a Huawei Cloud si el dispositivo cumple los siguientes requisitos:

1. Soporta la VPN sobre IPsec.
2. Tiene una dirección IP pública fija, que se puede configurar estáticamente, o traducir con NAT en escenarios transversales de NAT (su dispositivo se despliega detrás de un gateway NAT).

La mayoría de los dispositivos son routers y firewalls. Para obtener más información sobre la configuración de la interconexión, consulte la **Guía del administrador**.

NOTA

- Los routers de banda ancha domésticos comunes, los hosts de Windows que proporcionan servicios VPN (como L2TP) y los terminales móviles personales no pueden conectarse a Huawei Cloud con una VPN.
- Los siguientes productos pueden conectarse a Huawei Cloud con VPN:
  - Dispositivos: firewalls y enrutadores de acceso (AR) de Huawei, firewalls de Hillstone y firewalls de Check Point
  - Servicios en la nube: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) y Microsoft Azure
  - Software: strongSwan
- El protocolo IPsec es un protocolo de IETF estándar. Los dispositivos que admiten IPsec pueden interconectarse con Huawei Cloud con una VPN.

  La mayoría de los routers y firewalls de clase empresarial admiten el protocolo de IPsec.
- Algunos dispositivos admiten IPsec VPN solo después de comprar las licencias de software requeridas.

  El administrador del centro de datos local puede consultar con el proveedor del dispositivo si se requiere una licencia según el modelo del dispositivo.

2.10 ¿Qué son los parámetros de negociación de VPN? ¿Cuáles son sus valores predeterminados?

Tabla 2-1 Parámetros de negociación de VPN

Protocolo	Parámetro	Valor
IKE	Authentication Algorithm	● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● AES-256-GCM-16
	DH Algorithm	● Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 14 (valor predeterminado) ● Grupo 16 ● Grupo 19 ● Grupo 20 ● Grupo 21
	Version	● v1 (no recomendado debido a riesgos de seguridad) ● v2 (valor predeterminado)
	Lifetime (s)	**86400** (valor predeterminado) Unidad: segundo Rango de valores: de **60** a **604800**

Protocolo	Parámetro	Valor
	Local ID	● Dirección IP La dirección IP local se muestra automáticamente como la EIP del gateway de VPN, eliminando la necesidad de configurarlo manualmente. ● FQDN De forma predeterminada, el tipo de ID local es la dirección IP y el valor de ID local es la EIP del gateway de VPN.
	Customer ID	● 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 del gateway del cliente.
IPsec	Authentication Algorithm	● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● AES-256-GCM-16
	PFS	● DH grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 14 (valor predeterminado) ● DH grupo 15 ● DH grupo 16 ● DH grupo 19 ● DH grupo 20 ● DH grupo 21 ● Deshabilitar

Protocolo	Parámetro	Valor
	Transfer Protocol	● ESP (valor predeterminado)
	Lifetime (s)	**3600** (valor predeterminado) Unidad: segundo Rango de valores: de **30** a **604800**

NOTA

- Perfect Forward Secrecy (PFS) es una característica de seguridad.

  La negociación de IKE tiene dos fases, la fase 1 y la fase 2. La clave de la fase 2 (IPsec SA) se deriva de la clave generada en la fase 1. Una vez que se divulga la clave en la fase 1, la seguridad de la VPN IPsec puede verse afectada negativamente. Para mejorar la seguridad de la clave, IKE proporciona PFS. Cuando PFS está habilitado, se realizará un intercambio de DH adicional durante la negociación de SA de IPsec para generar una nueva clave de SA de IPsec, lo que mejorará la seguridad de SA de IPsec.
- Por motivos de seguridad, PFS está habilitado en Huawei Cloud de forma predeterminada. Asegúrese de que PFS también esté habilitado en el dispositivo de gateway del centro de datos local y de que la configuración de PFS en ambos extremos sea la misma. De lo contrario, la negociación no funcionará.
- La vida útil predeterminada basada en el tráfico de una SA IPsec es de 1,843,200 KB y no se puede cambiar para Huawei Cloud VPN. Este parámetro no participa en la negociación y no tiene ningún impacto en el establecimiento de una SA IPsec.

2.11 ¿Se requiere un nombre de usuario y contraseña para crear una conexión de VPN IPsec?

No. Huawei Cloud IPsec VPN utiliza una clave precompartida (PSK) para la autenticación. El PSK se configura en un gateway de VPN y se establecerá una conexión después de que se complete la negociación de VPN. Por lo tanto, no se requiere ningún nombre de usuario o contraseña para crear una conexión de VPN IPsec. En general, las VPN SSL, PPTP y L2TP usan nombres de usuario y contraseñas para la autenticación.

NOTA

IPsec XAUTH proporciona autenticación extendida para IPsec VPN. Requiere que los usuarios introduzcan sus nombres de usuario y contraseñas durante la negociación de VPN.

Huawei Cloud VPN no es compatible con IPsec XAUTH.

2.12 ¿Cómo permito que hosts específicos accedan a una subred de VPC por una conexión de VPN creada?

Restricciones en el centro de datos local:

- Políticas de control de acceso en el dispositivo de VPN
- Reglas de ACL en el router o switch

Restricciones en el lado de la nube:

- Reglas de grupo de seguridad que permiten el acceso solo desde direcciones IP especificadas
- Reglas de ACL

NOTA

Se recomienda no cambiar la subred local o de cliente para controlar el acceso.

2.13 ¿Qué recursos de VPN se pueden monitorear?

VPN gateway

Se puede supervisar la siguiente información de ancho de banda de una dirección IP de gateway de VPN: tráfico entrante, ancho de banda entrante, tráfico saliente, ancho de banda saliente y uso de ancho de banda saliente.

Para ver la información de supervisión, haga clic en  en la columna **Gateway IP Address** de la lista de gateway de VPN.

VPN connection

Se puede supervisar la siguiente información sobre una conexión de VPN: estado de la conexión de 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 supervisar RTT de enlace promedio, RTT de enlace máximo, tasa de pérdida de paquetes de enlace, RTT de túnel promedio, RTT de túnel máximo y tasa de pérdida de paquetes de túnel, haga clic en el nombre de la conexión de VPN y haga clic en **Add** en el área **Health Check** de la página de fichas **Summary** para agregar elementos de comprobación de estado.

Para ver el estado de una conexión de VPN, haga clic en  en la columna **Monitoring** de la conexión de VPN.

2.14 ¿Se pueden usar las EIP como direcciones IP de gateway de VPN?

No.

Cuando crea un gateway de VPN, su dirección IP se asigna automáticamente. Esta dirección IP tiene configuraciones preestablecidas y se puede utilizar para la interconexión con una VPC. Sin embargo, una EIP no puede utilizarse para la interconexión con una VPC.

2.15 ¿Necesito comprar EIP para que los hosts se comuniquen entre sí por una VPN?

Si sus hosts locales necesitan acceder a un ECS en la nube con una VPN, no necesita comprar ninguna EIP para el ECS.

Si un ECS necesita proporcionar servicios accesibles desde Internet, usted necesita comprar una EIP para el ECS.

2.16 ¿Se admiten las VPN SSL?

Las VPN SSL no son compatibles.

2.17 ¿Cuánto tiempo toma para que las configuraciones de VPN entregadas surtan efecto?

Las configuraciones de VPN tardan 1 – 5 minutos en entrar en vigor.

NOTA

Después de que las configuraciones de VPN surtan efecto, configure su dispositivo de gateway en su red local para completar la negociación del túnel con el gateway de VPN en Huawei Cloud.

2.18 ¿Huawei Cloud VPN admite direcciones de IPv6?

No.

Huawei Cloud VPN solo admite las direcciones IPv4.

2.19 ¿Cómo puedo determinar el ancho de banda de mi VPN?

Tenga en cuenta lo siguiente cuando determine el ancho de banda:

- Cantidad de datos transmitidos a través de un túnel de VPN en un período de tiempo (Reserve suficiente ancho de banda para evitar la congestión del enlace.)
- Ancho de banda de salida en los dos extremos de una conexión de VPN: El ancho de banda de salida en el lado de la nube debe ser menor que en el lado local.

2.20 ¿Una conexión VPN admite algoritmos criptográficos de la serie SM?

No.

Utilice los algoritmos proporcionados en la consola de gestión de Huawei Cloud para la negociación de VPN. Además, asegúrese de que los dos extremos de una conexión de VPN utilizan los mismos algoritmos.

2.21 ¿Qué versión de IKE debo seleccionar al crear una conexión de VPN?

Huawei Cloud recomienda IKEv2 porque IKEv1 no es seguro. Además, IKEv2 supera a IKEv1 en negociación y establecimiento de conexiones, métodos de autenticación, procesamiento de tiempo de espera de detección de pares muertos (DPD) y procesamiento de tiempo de espera de asociación de seguridad (SA).

Huawei Cloud no será compatible con IKEv1 pronto.

Introducción a IKEv1 e IKEv2

- Como protocolo híbrido, IKEv1 trae algunos defectos de seguridad y rendimiento debido a su complejidad. Como tal, se ha convertido en un cuello de botella en el sistema IPsec.
- IKEv2 resuelve los problemas de IKEv1 mientras conserva las funciones básicas de IKEv1. IKEv2 es más simplificado, eficiente, seguro y robusto que IKEv1. Adicionalmente, IKEv2 se define por RFC 4306 en un único documento, mientras que IKEv1 se definen en múltiples documentos. Al minimizar las funciones principales y los algoritmos de contraseña predeterminados, IKEv2 mejora en gran medida la interoperabilidad entre diferentes VPN IPsec.

Riesgos de seguridad de IKEv1

- Los algoritmos criptográficos soportados por IKEv1 no se han actualizado durante más de 10 años. Además, IKEv1 no admite algoritmos criptográficos fuertes como AES-GCM y ChaCha20-Poly1305. Para IKEv1, el bit E (Encryption) en la cabecera ISALMP especifica que las cargas útiles que siguen a la cabecera ISALMP están cifradas, pero cualquier verificación de integridad de datos de esas cargas útiles es manejada por una carga útil hash separada. Esta separación de la encriptación de la protección de la integridad de los datos impide el uso de encriptación autenticada (AES-GCM) con IKEv1.
- IKEv1 es vulnerable a ataques de amplificación DoS y ataques de conexión semiabierta. Después de responder a paquetes falsificados, el respondedor mantiene relaciones iniciador-respondedor, consumiendo un gran número de recursos del sistema.

  Este defecto es inherente a IKEv1 y se aborda en IKEv2.
- El modo agresivo de IKEv1 no es seguro. En este modo, los paquetes de información no están cifrados, lo que plantea riesgos de fuga de información. También hay ataques de fuerza bruta dirigidos al modo agresivo, como los ataque de intermediario.

Diferencias entre IKEv1 e IKEv2

- **Negotiation process**
  - IKEv1 es complejo y consume una gran cantidad de ancho de banda. La negociación IKEv1 SA consta de dos fases. En IKEv1 fase 1, se establece un IKE SA en modo principal o modo agresivo. El modo principal requiere tres intercambios entre pares que suman seis mensajes ISAKMP, mientras que el modo agresivo requiere dos intercambios que suman tres mensajes ISAKMP. El modo agresivo es más rápido, pero no proporciona protección de identidad para los pares, ya que el intercambio de claves y la autenticación de identidad se realizan simultáneamente. En IKEv1 fase 2, las SA IPsec se establecen con tres mensajes ISAKMP en modo rápido.
  - En comparación con IKEv1, IKEv2 simplifica el proceso de negociación de SA. IKEv2 requiere solamente dos intercambios, totalizando 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 para cada par adicional de SA.

    NOTA

    Para la negociación IKEv1, su modo principal implica nueve (6+3) mensajes, y su modo agresivo implica seis (3+3) mensajes. Por el contrario, la negociación IKEv2 requiere solamente cuatro (2+2) mensajes.

- **Métodos de autenticación**
  - Solo IKEv1 (que requiere una tarjeta de encriptación) admite la autenticación de envolvente digital (HSS-DE).
  - IKEv2 admite la autenticación del Extensible Authentication Protocol (EAP). IKEv2 puede utilizar un servidor AAA para autenticar remotamente a los usuarios móviles y de PC y asignar direcciones IP privadas a estos usuarios. IKEv1 no proporciona esta función y debe usar L2TP para asignar direcciones IP privadas.
  - Solo IKEv2 admite algoritmos de integridad de IKE SA.
- **DPD timeout processing**
  - Solo IKEv1 admite el parámetro **retry-interval**. Si un dispositivo envía un paquete DPD pero no recibe respuesta dentro del intervalo de reintento especificado, el dispositivo registra un evento de fallo DPD. Cuando el número de eventos de error de DPD llega a 5, se eliminan tanto las SA IKE como las SA IPsec. La negociación IKE SA se iniciará de nuevo solo cuando haya tráfico que se transmita a través del túnel IPsec.
  - En IKEv2, el intervalo de retransmisión aumenta de 1, 2, 4, 8, 16, 32 a 64, en segundos. Si no se recibe respuesta dentro de ocho transmisiones consecutivas, el extremo par se considera muerto, y se eliminan las SA IKE y las SA IPsec.
- **Procesamiento del tiempo de espera de IKE SA y del tiempo de espera de IPsec SA**

  En IKEv2, la vida útil suave de IKE SA es 9/10 de la vida útil dura de IKE SA más o menos un número aleatorio. Esto reduce la probabilidad de que dos extremos inicien la renegociación simultáneamente. Por lo tanto, no se establece manualmente la vida útil de software 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 la autenticación de EAP, lo que mejora la flexibilidad y la escalabilidad de la autenticación.

  EAP es un protocolo de autenticación que admite múltiples métodos de autenticación. La mayor ventaja de EAP es su escalabilidad. Es decir, se pueden agregar nuevos métodos de autenticación sin cambiar el sistema de autenticación original. La autenticación EAP ha sido ampliamente utilizada en redes de acceso telefónico.
- Emplea una carga útil cifrada sobre la base de ESP. Esta carga útil contiene tanto un algoritmo de encriptación como un algoritmo de integridad de datos. AES-GCM garantiza la confidencialidad, integridad y autenticación, y funciona bien con IKEv2.

2.22 ¿Cuántos bits tienen los grupos DH que utiliza Huawei Cloud VPN?

Los grupos Diffie-Hellman (DH) determinan la fuerza de la clave utilizada en el proceso de intercambio de claves. Los números de grupo DH más altos suelen ser más seguros, pero se requiere más tiempo para calcular la clave.

Tabla 2-2 enumera el número de bits correspondientes a los grupos DH utilizados por VPN.

Tabla 2-2 Número de bits correspondientes a cada grupo DH

Grupo DH	Módulo
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	256 bits (ECP)
20	384 bits (ECP)
21	521 bits (ECP)

NOTA

Los siguientes algoritmos de DH tienen riesgos de seguridad y no se recomiendan: DH grupo 1, DH grupo 2 y DH grupo 5.

2.23 ¿Puedo visitar sitios web internacionales con una VPN?

No.

La VPN conecta una VPC y la red de un centro de datos local, es decir, una conexión sitio a sitio.

2.24 ¿Puedo desplegar una aplicación en la nube y una base de datos en un centro de datos local y conectarlos por una VPN?

Sí.

Una VPN conecta una VPC y un centro de datos local.

Después de configurar una VPN, el tráfico de servicio se puede transmitir entre la VPC y el centro de datos local. Para un servidor de aplicaciones en la nube, el acceso a una base de datos local es lógicamente el mismo que el acceso a otros hosts en la misma LAN. Dado esto, es factible utilizar una VPN para conectar una aplicación en la nube a una base de datos en un centro de datos local.

Este es un escenario típico de IPsec VPN.

Además, no hay limitaciones en el iniciador de servicio. Es decir, las solicitudes de servicio se pueden iniciar desde la nube o el centro de datos local.

AVISO

- Después de configurar una VPN, compruebe la latencia de la red y la tasa de pérdida de paquetes para garantizar un buen funcionamiento del servicio.
- Se recomienda que ejecute el comando ping para comprobar la pérdida de paquetes y los detalles de latencia de red.

2.25 ¿Cuáles son las diferencias entre IPsec VPN y SSL VPN en escenarios de aplicaciones y modos de conexión?

Escenarios de aplicación

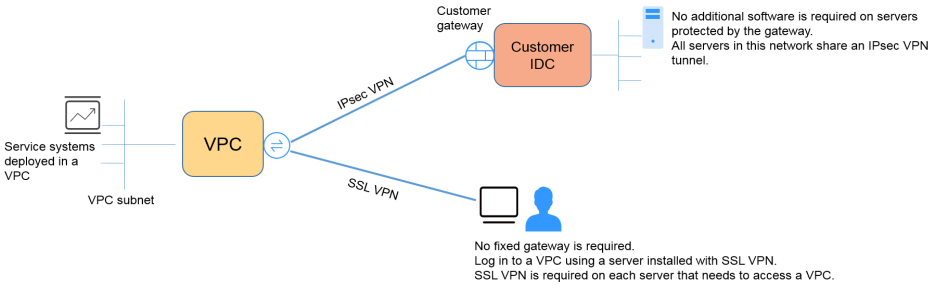
IPsec VPN conecta dos LAN, como una sucursal y su sede, o un centro de datos local y una VPC.

SSL VPN conecta un cliente a una LAN. Por ejemplo, el ordenador portátil de un empleado en un viaje de negocios accede a la red interna de la empresa.

Modos de conexión

IPsec VPN requiere gateway fijos, como firewalls o enrutadores, en ambos extremos. El administrador debe configurar gateway en ambos extremos para permitirles completar la negociación de IPsec VPN.

SSL VPN requiere un programa cliente específico instalado en los hosts. Los usuarios deben ingresar nombres de usuario y contraseña para conectar los hosts a los servidores de SSL.



NOTA

Huawei Cloud solo admite IPsec VPN.

2.26 ¿Cómo se me cobrará por el uso de una VPN? ¿Se me cobrará por las EIP del gateway de VPN?

Las VPN son facturadas por los siguientes elementos en una base anual/mensual o de pago por uso.

- Gateway de VPN

- Conexión de VPN

  Por defecto, se incluyen 10 grupos de conexiones de VPN gratuitos en la compra de un gateway de VPN. Puede comprar las conexiones de VPN adicionales si es necesario.

- Ancho de banda de EIP de un gateway de VPN

  El ancho de banda del gateway de VPN se puede facturar por el tráfico o el ancho de banda.

  a. Un gateway de VPN anual/mensual solo se puede facturar por ancho de banda. El precio de un gateway de VPN anual/mensual incluye el precio de las conexiones de VPN que se pueden crear para el gateway y el precio del ancho de banda.

  b. El ciclo de facturación del modo de facturación de pago por uso es de 1 hora. Cuando crea un gateway de VPN de pago por uso, el sistema le solicita que cree conexiones de VPN. Por defecto, se incluyen 10 grupos de conexiones de VPN gratuitos en la compra de un gateway de VPN. Si se requieren más grupos de conexión, debe comprarlos.

  NOTA

  Un gateway de VPN no puede compartir un ancho de banda con una EIP vinculada a un ECS.

2.27 ¿Cuáles son las diferencias entre la facturación del ancho de banda de EIP del gateway de VPN por ancho de banda y por tráfico?

El ancho de banda de EIP del gateway de VPN se puede facturar por ancho de banda o por tráfico.

A continuación, se detallan las diferencias:

- Facturación por ancho de banda: El ciclo de facturación es de 1 hora. La tarifa generada depende del ancho de banda.
- Facturado por tráfico: La tarifa se calcula en función del tráfico saliente de una VPC generada cada hora, que no se ve afectado por el ancho de banda.

2.28 ¿Puede una VPN facturada por tráfico usar un paquete de datos compartidos?

No.

El servicio VPN se factura de forma independiente y no puede usar paquetes de datos compartidos.

2.29 ¿Se puede retener la EIP de un gateway de VPN después de que se elimine el gateway de VPN?

Si una EIP de pago por uso está vinculada a un gateway de VPN de pago por uso, la eliminación del gateway de VPN también eliminará la EIP vinculada.

Para conservar tal EIP de pago por uso, desvíselo antes de eliminar el gateway de VPN.

2.30 ¿Dónde puedo agregar rutas a las subredes del cliente en la consola de VPN?

Cuando se crea una conexión de VPN, las rutas a las subredes de los clientes se entregan automáticamente.

2.31 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Para ver el estado de una conexión de VPN, haga clic en  en la columna **Monitoring** de la conexión de VPN.

2.32 ¿Qué hago si no se establece una conexión de VPN?

1. Inicie sesión en la consola de gestión y elija **Virtual Private Network** > **Enterprise – VPN Connections**.
2. En la lista de conexiones de VPN, localice la conexión de VPN de destino y elija **More** > **Modify Policy Settings** a la derecha para ver las políticas IKE e IPsec de la conexión de VPN.
3. Compruebe las políticas IKE e IPsec para ver si los modos de negociación y los algoritmos de encriptación en ambos extremos de la conexión de 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 de VPN pueden ser inconsistentes.
4. Compruebe si las reglas 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 para permitir la comunicación con las subredes de VPC. A continuación se proporciona un ejemplo de configuraciones de ACL:

   ```
   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. Haga ping a los dos extremos de la conexión de VPN entre sí para comprobar si la conexión de VPN es normal.

2.33 ¿En qué dirección está limitado el ancho de banda de VPN? ¿Cuál es la unidad de ancho de banda?

El ancho de banda del gateway de VPN comprado se aplica a la dirección de salida de Huawei Cloud. Para lograr un balanceo entre los anchos de banda en las direcciones de entrada y de salida, el ancho de banda en la dirección de entrada se limita de la siguiente manera:

- Si el ancho de banda adquirido es de 10 Mbit/s o menos, el ancho de banda en la dirección de entrada está limitado a 10 Mbit/s.
- Si el ancho de banda adquirido es mayor que 10 Mbit/s, el ancho de banda en la dirección de entrada es el mismo que el ancho de banda comprado.

La unidad de ancho de banda es Mbit/s y la del tráfico es GB.

2.34 ¿Puedo restaurar un gateway de VPN o una conexión de VPN que se elimina incorrectamente?

- No se puede restaurar un gateway anual/mensual de VPN o una conexión de VPN.
- Un gateway de VPN de pago por uso solo se puede restaurar cuando se cumplen las siguientes condiciones:
  - El gateway de VPN se eliminó en 24 horas.
  - Ambas EIP unidas al gateway de VPN no han sido ilimitados.
  - La VPC o el router empresarial interconectado con el gateway de VPN está disponible. Si la VPC o el router empresarial no existen, restaure primero la VPC o el router empresarial.
  - Su cuenta es normal y no está en mora o congelada.
- Una conexión de VPN de un gateway de VPN de pago por uso solo se puede restaurar cuando se cumplen las siguientes condiciones:
  - El gateway de VPN y el gateway del cliente están disponibles. Si uno de ellos no existe, restáurelo primero.
  - Su cuenta es normal y no está en mora o congelada.

  La configuración de comprobación de estado de una conexión de VPN de pago por uso no se puede restaurar incluso después de restaurar la conexión de VPN. Por lo tanto, es necesario volver a configurar la función de comprobación de estado.

3 Escenarios de redes y aplicaciones

3.1 ¿Puedo visitar sitios web internacionales con una VPN?

No.

La VPN conecta una VPC y la red de un centro de datos local, es decir, una conexión sitio a sitio.

3.2 ¿Puedo desplegar una aplicación en la nube y una base de datos en un centro de datos local y conectarlos por una VPN?

Sí.

Una VPN conecta una VPC y un centro de datos local.

Después de configurar una VPN, el tráfico de servicio se puede transmitir entre la VPC y el centro de datos local. Para un servidor de aplicaciones en la nube, el acceso a una base de datos local es lógicamente el mismo que el acceso a otros hosts en la misma LAN. Dado esto, es factible utilizar una VPN para conectar una aplicación en la nube a una base de datos en un centro de datos local.

Este es un escenario típico de IPsec VPN.

Además, no hay limitaciones en el iniciador de servicio. Es decir, las solicitudes de servicio se pueden iniciar desde la nube o el centro de datos local.

AVISO

- Después de configurar una VPN, compruebe la latencia de la red y la tasa de pérdida de paquetes para garantizar un buen funcionamiento del servicio.
- Se recomienda que ejecute el comando ping para comprobar la pérdida de paquetes y los detalles de latencia de red.

3.3 ¿Cuántas conexiones de VPN necesito para conectar varios servidores locales a la nube?

Huawei Cloud VPN utiliza tecnología de IPsec VPN. Conecta una VPC en la nube y su centro de datos local. Por lo tanto, el número de conexiones de VPN es irrelevante para el número de servidores que se conectarán a la nube, pero para el número de centros de datos donde se encuentran los servidores.

Se pueden enlazar dos EIP a un gateway de VPN para la comunicación con un gateway de cliente.

- Si un centro de datos local solo tiene un gateway de salida, todos los servidores o hosts del centro de datos se conectan a Internet con este gateway. En este caso, debe configurar un grupo de conexiones de VPN que consta de dos conexiones de VPN. Es decir, configure una conexión de VPN para cada una de las dos EIP del gateway de VPN para comunicarse con el gateway de salida en el centro de datos local.
- Si un centro de datos local tiene dos gateway de salida, los servidores o hosts de usuario en el centro de datos se conectan a Internet con las gateway de salida de remolque. En este caso, debe configurar dos grupos de conexiones de VPN, cada uno de los cuales consta de dos conexiones de VPN. Es decir, configure una conexión de VPN para cada uno de los dos EIP de cada gateway de VPN para comunicarse con ambos gateway de salida en el centro de datos local.

3.4 ¿Cuáles son las diferencias entre IPsec VPN y SSL VPN en escenarios de aplicaciones y modos de conexión?

Escenarios de aplicación

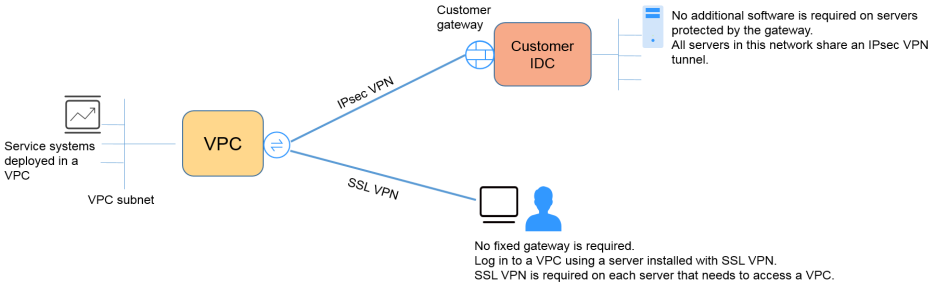
IPsec VPN conecta dos LAN, como una sucursal y su sede, o un centro de datos local y una VPC.

SSL VPN conecta un cliente a una LAN. Por ejemplo, el ordenador portátil de un empleado en un viaje de negocios accede a la red interna de la empresa.

Modos de conexión

IPsec VPN requiere gateway fijos, como firewalls o enrutadores, en ambos extremos. El administrador debe configurar gateway en ambos extremos para permitirles completar la negociación de IPsec VPN.

SSL VPN requiere un programa cliente específico instalado en los hosts. Los usuarios deben ingresar nombres de usuario y contraseña para conectar los hosts a los servidores de SSL.



NOTA

Huawei Cloud solo admite IPsec VPN.

3.5 ¿Una VPN permite comunicaciones entre dos VPC?

- Si las dos VPC están en la misma región, utilice una interconexión de VPC para conectarlas.
- Si las dos VPC están en diferentes regiones, use una VPN para conectarlas. Las operaciones son las siguientes:
  a. Cree un gateway de VPN para cada VPC y cree una conexión de VPN entre los dos gateway de VPN.
  b. Para la conexión de VPN, establezca el gateway del cliente en la EIP del gateway de VPN del mismo nivel.
  c. Para la conexión de VPN, establezca la subred del cliente en la subred de la VPC del mismo nivel.
  d. Establezca las mismas claves precompartidas (PSK) y algoritmos para las dos VPC.

3.6 ¿Cuáles son los impactos de una VPN en una red local? ¿Cuáles son los cambios en la ruta para acceder a un ECS?

Al configurar una VPN, debe realizar las siguientes operaciones en el gateway en su centro de datos local:

- Configure las políticas IKE e IPsec.
- Establezca el modo de conexión como basado en ruta o basado en políticas.
- Compruebe la configuración de la ruta en el gateway para asegurarse de que el tráfico destinado a una VPC de Huawei Cloud se puede enrutar a la interfaz de salida correcta (interfaz que tiene una política IPsec vinculada).

3.7 ¿Qué configuraciones se requieren en ambos extremos de una VPN que conecta un centro de datos local a una VPC?

Para implementar la interconexión de VPN, cree una VPN en la nube y configure el dispositivo VPN en el centro de datos local.

- Cree una VPN en la nube.
  - Compre un gateway de VPN y configure el modo de facturación, el ancho de banda y la VPC interconectada.
  - Cree un gateway de cliente y configure el modo de enrutamiento.
  - Compre una conexión de VPN y configure las direcciones IP y subredes de gateway en ambos extremos, así como las políticas de negociación.
- Configure el dispositivo VPN en el centro de datos local.
  a. Configure la dirección IP pública utilizada por el centro de datos local para conectarse a la nube y complete las configuraciones de negociación IPsec fase 1 y fase 2 en el dispositivo de VPN.
  b. Configurar rutas, NAT y políticas de seguridad en el dispositivo de VPN.

3.8 ¿Puedo conectar una red con dos salidas a una VPC por dos conexiones de VPN?

Sí.

3.9 ¿Puedo conectar dos VPC en la misma región a través de una VPN?

No.

Puede utilizar una interconexión de VPC o una conexión de Cloud Connect para conectar dos VPC en la misma región.

3.10 ¿Cómo puedo conectar dos VPC en la misma región?

Puede utilizar una interconexión de VPC o una conexión de Cloud Connect para conectar dos VPC en la misma región. La interconexión de VPC solo puede conectar VPC en la misma región; Cloud Connect también puede conectar VPC en diferentes regiones.

3.11 ¿Cómo puedo habilitar las comunicaciones entre dos VPC y una red local?

Topología de red

IDC–VPC 1–VPC 2

IDC indica un centro de datos local. Se establece una conexión de VPN entre la VPC 1 y el IDC.

Procedimiento

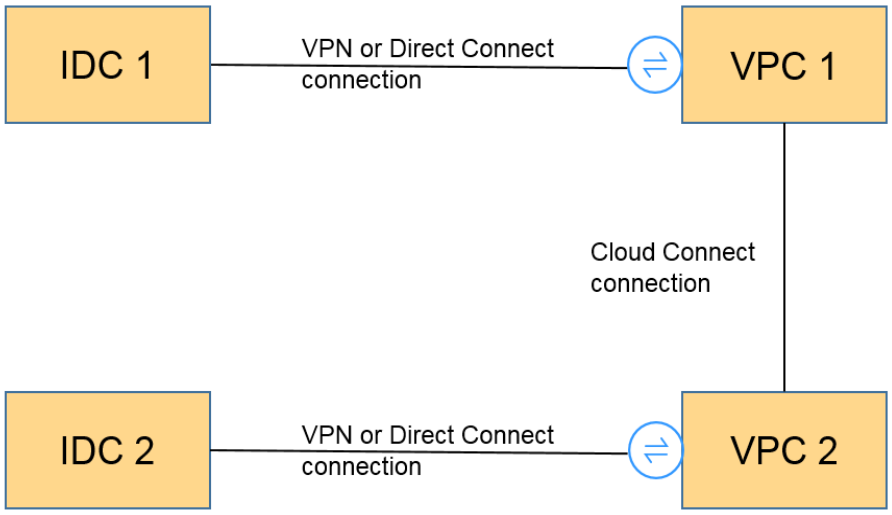
1. Compruebe si las dos VPC están en la misma región.
   - Si es así, utilice una interconexión de VPC o una conexión de Cloud Connect para conectar las dos VPC. Tal conexión es gratuita.
   - Si no es así, utilice una conexión de Cloud Connect para conectar las dos VPC. Debe pagar por el ancho de banda de Cloud Connect.
2. Establezca una conexión de VPN entre el IDC y una VPC (VPC 1 en este ejemplo).

   En el centro de datos local, establezca las subredes de VPC 1 y VPC 2 como subredes remotas. La subred local de VPC 1 debe contener la subred conectada con una interconexión de VPC o una conexión de Cloud Connect. La ruta de subred de la conexión de interconexión de VPC o Cloud Connect debe destinarse a la subred local.

3.12 ¿Cómo conecto cuatro subredes?

La **Figura 3-1** muestra la topología de red.

Figura 3-1 Topología de red



1. Utilice una conexión de VPN o una conexión de Direct Connect para conectar IDC 1 a VPC 1.
2. Utilice una conexión de Cloud Connect para conectar VPC 1 a VPC 2. (También puede utilizar una interconexión de VPC para conectar VPC 1 a VPC 2 si están en la misma región.)
3. Utilice una conexión de VPN o una conexión de Direct Connect para conectar VPC 2 a IDC 2.
4. Actualice las subredes de VPN, las rutas de subred de Cloud Connect y las rutas de subred de Direct Connect. Entonces, las cuatro subredes son accesibles para llegar a otras.

3.13 ¿Necesito dos conexiones de VPN para conectar cuatro subredes de dos regiones si cada región tiene dos subredes?

No.

Solo se requiere una conexión de VPN entre dos regiones. Todas las subredes se pueden agregar a la conexión de VPN.

En este escenario, si intenta crear una segunda conexión de VPN, la consola de gestión muestra un mensaje que indica que se produce un conflicto porque las dos conexiones tienen la misma dirección de gateway de cliente.

3.14 ¿Puedo acceder a OBS por una VPN?

Sí.

1. Con la ayuda del servicio punto de conexión de VPC, puede acceder a OBS con una VPN. Es necesario crear dos puntos de conexión de VPC para el servidor DNS privado y OBS de Huawei Cloud, respectivamente.
2. Configure el servidor de DNS privado y las rutas en su centro de datos local.

3.15 ¿Cómo conecto mi computadora personal a la nube por una VPN?

Los routers de banda ancha domésticos comunes, los hosts de Windows que proporcionan servicios VPN (como L2TP) y los terminales móviles personales no pueden conectarse a Huawei Cloud con una VPN.

Para usar Huawei Cloud VPN, los dispositivos locales deben admitir el protocolo de IPsec estándar.

3.16 ¿Cómo puedo acceder a los ECS de Huawei Cloud en casa cuando mi red empresarial se ha conectado a Huawei Cloud por una VPN?

Una VPN en Huawei Cloud es una VPN IPsec que conecta una LAN local a una VPC en la nube. Su red doméstica no forma parte de su LAN empresarial, por lo que no puede conectarse directamente a la VPC en la nube en el hogar.

Si su host en casa necesita acceder a los recursos de VPC en la nube, su host puede acceder directamente a la EIP del servicio correspondiente. Alternativamente, su host puede conectarse a la LAN de su empresa con SSL VPN (si es compatible) y, a continuación, acceder a los recursos de VPC en la nube con la LAN.

3.17 ¿Cómo puedo establecer una conexión de VPN temporalmente si no hay disponible un dispositivo local con capacidad IPsec después de comprar un gateway de Huawei Cloud VPN y una conexión de VPN?

Para establecer una conexión de VPN con Huawei Cloud, debe tener un dispositivo local que admita el protocolo IPsec estándar y una dirección IP pública fija.

Si no se cumplen los requisitos anteriores, puede instalar software IPsec de terceros en un host para conectarse temporalmente a Huawei Cloud.

El software IPsec de terceros recomendado incluye strongSwan, Openswan y GreenBow. Para obtener más información sobre la interconexión, consulte la **Guía del administrador de Virtual Private Network**.

3.18 ¿Cómo selecciono una región adecuada en la nube cuando compro un gateway de VPN?

Puede seleccionar una VPC en cualquier región cuando compre un gateway de VPN.

Se recomienda que seleccione la región más cercana a su centro de datos local para minimizar el impacto de Internet en la VPN.

- Para conectarse a varias VPC en la misma región, puede usar VPN y Direct Connect.
- Para conectarse a varias VPC en diferentes regiones, puede usar VPN y Cloud Connect.

4 Facturación y pagos

4.1 ¿Cómo se me cobrará por el uso de una VPN? ¿Se me cobrará por las EIP del gateway de VPN?

Las VPN son facturadas por los siguientes elementos en una base anual/mensual o de pago por uso.

- Gateway de VPN
- Conexión de VPN

  Por defecto, se incluyen 10 grupos de conexiones de VPN gratuitos en la compra de un gateway de VPN. Puede comprar las conexiones de VPN adicionales si es necesario.
- Ancho de banda de EIP de un gateway de VPN

  El ancho de banda del gateway de VPN se puede facturar por el tráfico o el ancho de banda.

  a. Un gateway de VPN anual/mensual solo se puede facturar por ancho de banda. El precio de un gateway de VPN anual/mensual incluye el precio de las conexiones de VPN que se pueden crear para el gateway y el precio del ancho de banda.

  b. El ciclo de facturación del modo de facturación de pago por uso es de 1 hora. Cuando crea un gateway de VPN de pago por uso, el sistema le solicita que cree conexiones de VPN. Por defecto, se incluyen 10 grupos de conexiones de VPN gratuitos en la compra de un gateway de VPN. Si se requieren más grupos de conexión, debe comprarlos.

  NOTA

  Un gateway de VPN no puede compartir un ancho de banda con una EIP vinculada a un ECS.

4.2 ¿Cuáles son las diferencias entre la facturación del ancho de banda de EIP del gateway de VPN por ancho de banda y por tráfico?

El ancho de banda de EIP del gateway de VPN se puede facturar por ancho de banda o por tráfico.

A continuación, se detallan las diferencias:

- Facturación por ancho de banda: El ciclo de facturación es de 1 hora. La tarifa generada depende del ancho de banda.
- Facturado por tráfico: La tarifa se calcula en función del tráfico saliente de una VPC generada cada hora, que no se ve afectado por el ancho de banda.

4.3 ¿Puede una VPN facturada por tráfico usar un paquete de datos compartidos?

No.

El servicio VPN se factura de forma independiente y no puede usar paquetes de datos compartidos.

4.4 ¿Por cuántas conexiones de VPN se me cobrará para conectar las VPC en diferentes regiones?

Las VPN se pueden usar para conectar VPCs en diferentes regiones. El ancho de banda y las conexiones de VPN de cada región se facturarán de forma independiente. Por lo tanto, al calcular las tarifas estimadas, debe comprobar el número total de regiones y sus relaciones de conexión.

Por ejemplo, supongamos que la Región A necesita establecer una conexión de VPN con la Región B y la Región C, respectivamente. El gateway de VPN de la Región A tiene dos conexiones; el gateway de VPN de la Región B tiene una conexión; y el gateway de VPN de la Región C tiene una conexión.

En este caso, se le cobrará por cuatro conexiones de VPN.

4.5 ¿Cómo cambio el modo de facturación de un gateway de VPN de pago por uso a anual/mensual?

Requisitos previos

- El gateway de VPN de pago por uso se factura por ancho de banda.
- Para cambiar el modo de facturación de un gateway de VPN facturado por tráfico de pago por uso a anual/mensual, primero cambie el gateway de VPN de ser facturado por tráfico a ser facturado por ancho de banda y luego de pago por uso a anual/mensual.

Procedimiento

Realice las siguientes operaciones:

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** y elija **Networking** > **Virtual Private Network**.

4. En el panel de navegación de la izquierda, elija **Virtual Private Network** >**Enterprise** – **VPN Gateways**.
5. En la página **VPN Gateways**, busque la fila que contiene el gateway de VPN de destino, elija **More** > **Change Billing Mode** en la columna **Operation**.
6. En el cuadro de diálogo **Change Billing Mode**, haga clic en **OK**.

   NOTA

   El modo de facturación de un gateway VPN no se puede cambiar de anual/mensual a pago por uso y el ancho de banda del gateway VPN incluido en la suscripción anual/mensual no se puede reducir.
7. Confirme la información del gateway de VPN, establezca una duración de renovación y haga clic en **Pay**.
8. En la página de pago, confirme la información del pedido, seleccione un cupón o descuento, seleccione un método de pago y haga clic en **Pay**.

   NOTA

   Cambiar el modo de facturación de un gateway de VPN de pago por uso a anual/mensual no afectará sus servicios.

4.6 ¿Se renovará automáticamente un gateway de VPN anual/mensual?

Sí.

Huawei Cloud cobrará automáticamente las tarifas de renovación de su saldo.

Un gateway de VPN anual/mensual necesita ser prepagado. Para asegurarse de que su conexión es normal, recargue su cuenta si su saldo no es suficiente.

4.7 ¿Puedo cancelar mi suscripción a un gateway de VPN anual/mensual?

Sí.

En la página **VPN Gateways**, busque la fila que contiene el gateway de VPN que desea cancelar y elija **More** > **Delete** en la columna **Operation**. Después de darse de baja de un gateway de VPN anual/mensual, todas las conexiones VPN creadas para el gateway también se eliminarán y no se podrán recuperar.

Después de la cancelación de la suscripción, se reembolsará el resto de las tarifas prepagadas.

4.8 ¿Cuándo se congelarán mis recursos de VPN? ¿Cómo puedo descongelar los recursos de VPN?

- Si los recursos de VPN de pago por uso están atrasados, los recursos ingresan el período de gracia, durante el cual aún puede acceder y usar los recursos. Si el período de gracia finaliza y no ha pagado los atrasos, los recursos ingresan el período de retención, durante el cual se congelan los recursos. Los recursos congelados no están disponibles y no se

pueden modificar ni eliminar. Si el período de retención finaliza y aún no ha recargado su cuenta y pagado los atrasos, los recursos se liberarán y no se podrán restaurar. Para asegurarse de que los recursos estén disponibles, recargue su cuenta y pague los atrasos antes de que expiren los recursos.

- Los recursos de VPN congelados estarán disponibles después de renovarlos o recargar su cuenta.

4.9 ¿Cómo se facturan los recursos de VPN y cómo uso cupones?

Un gateway de VPN se puede facturar sobre una base de pago por uso o anual/mensual.

- Pago por uso: Los cargos se deducen del saldo de la cuenta en función del uso de recursos.
- Anual/Mensual: La suscripción debe pagarse por adelantado.

Si tiene un cupón Huawei Cloud, puede usarlo para recargar su cuenta, siempre y cuando el cupón sea válido. A continuación, puede utilizar el nuevo saldo de su cuenta para pagar sus recursos.

Los recursos anuales/mensuales son rentables.

Los usuarios del contrato de Huawei Cloud deben seleccionar **Download Contract and Pay** en la consola.

5 Operaciones en la consola

5.1 ¿Cuáles son las relaciones entre una VPC, un gateway de VPN y una conexión de VPN?

- Una VPC es una red privada en la nube. Se pueden crear múltiples VPC en la misma región mientras están aisladas entre sí. Una VPC se puede dividir en varias subredes.
- Se crea un gateway de VPN en una VPC y es el punto de acceso de una conexión de VPN. Una VPC en Huawei Cloud puede tener múltiples gateway de VPN, y un gateway de VPN puede tener múltiples conexiones de VPN.
- Se crea una conexión de VPN para un gateway de VPN y conecta una VPC a un centro de datos local (o una VPC en otra región).

  NOTA

  El número de conexiones de VPN es irrelevante para el número de subredes locales o el número de subredes de clientes. Solo está relacionado con el número de centros de datos locales (o VPC en otras regiones) que se van a conectar a su VPC. Las conexiones de VPN creadas se muestran en la lista de conexiones de VPN. También puede ver el número de conexiones de VPN creadas para cada gateway de VPN.

5.2 ¿Cuánto tiempo toma para que las configuraciones de VPN entregadas surtan efecto?

Las configuraciones de VPN tardan 1 – 5 minutos en entrar en vigor.

NOTA

Después de que las configuraciones de VPN surtan efecto, configure su dispositivo de gateway en su red local para completar la negociación del túnel con el gateway de VPN en Huawei Cloud.

5.3 ¿Por qué una conexión de VPN siempre está en estado no conectado después de completar su configuración?

La configuración puede ser incorrecta.

1. En los dos extremos (en la nube y en el centro de datos local) de la conexión de VPN, asegúrese de que las claves precompartidas (PSK) y la información de negociación sean consistentes, las subredes locales y remotas se inviertan, y los gateway locales y remotos también se invierten.
2. Asegúrese de que las rutas, NAT y políticas de seguridad estén correctamente configuradas en el dispositivo de su centro de datos local.

5.4 ¿Se puede retener la EIP de un gateway de VPN después de que se elimine el gateway de VPN?

Si una EIP de pago por uso está vinculada a un gateway de VPN de pago por uso, la eliminación del gateway de VPN también eliminará la EIP vinculada.

Para conservar tal EIP de pago por uso, desvíselo antes de eliminar el gateway de VPN.

5.5 ¿Qué información sobre una VPN creada se puede modificar y qué información no se puede modificar?

- Gateway de VPN
  - Puede modificar la siguiente información:
    - Nombre
    - Subred local
    - EIPs activas y en espera
      - Para modificar la EIP activa o en espera, desvincule la EIP original y vincule una nueva.

        Si se ha creado una conexión de VPN para una EIP, la EIP no puede ser independiente.
      - Para obtener detalles sobre cómo modificar los atributos de EIP, como el nombre, el tipo y el ancho de banda, consulte la **documentación del servicio de EIP**.
  - No puede modificar la siguiente información:
    - Región
    - Modo de asociación (VPC o router empresarial)
    - Enrutador empresarial

      El router empresarial asociado debe especificarse solo cuando **Associate With** está establecido en **Enterprise Router**.
    - VPC
    - Subred de interconexión
    - BGP ASN
    - Modo de facturación (anual/mensual o de pago por uso)
    - Especificación
    - AZ
    - Número de grupos de conexión de VPN

El número de grupos de conexión de VPN solo debe especificarse cuando **Billing Mode** está establecido en **Yearly/Monthly**.

- Gateway del cliente
  - Puede modificar la siguiente información:
    - Nombre
  - No puede modificar la siguiente información:
    - Modo de enrutamiento
    - BGP ASN

      El ASN de BGP solo necesita especificarse cuando **Routing Mode** está establecido en **Dynamic (BGP)**.
    - Dirección IP pública
- Conexión de VPN
  - Puede modificar la siguiente información:
    - Nombre
    - Dirección de interfaz local
    - Gateway del cliente
    - Subred del cliente
    - Configuración de políticas, incluidas las políticas IKE e IPsec
    - PSK
  - No puede modificar la siguiente información:
    - Gateway de VPN
    - EIP
    - Tipo de VPN (basado en ruta o basado en políticas)
    - Modo de enrutamiento (estático o BGP)

      El modo de enrutamiento debe especificarse solo cuando **VPN Type** está establecido en **Route-based**.
    - Configuración de detección de enlaces

      La configuración de detección de enlace solo está disponible cuando **VPN Type** se establece en **Route-based**.
    - Configuración de políticas, incluidos los bloques CIDR de origen y destino

      La configuración de política solo está disponible cuando **VPN Type** está establecida en **Route-based**.

5.6 ¿Necesito configurar las reglas de ACL en la consola de gestión de Huawei Cloud después de configurar las reglas de ACL en el dispositivo de gateway local?

Es necesario configurar las reglas de política (reglas de ACL) para una conexión de VPN en la consola de gestión de Huawei Cloud solo cuando **VPN Type** está configurado en **Policy-based**.

5.7 ¿Qué hago si ocurre una excepción cuando agrego una subred de cliente durante la creación de una conexión de VPN?

Compruebe si esta subred de cliente está involucrada en una ruta de una interconexión de VPC, Cloud Connect o Direct Connect. Si es así, se produce un conflicto de ruta y es necesario eliminar la ruta y crear una nueva para evitar el conflicto.

5.8 ¿Dónde puedo configurar las rutas a las subredes del cliente en la consola de VPN?

Cuando se crea una conexión de VPN, las rutas a las subredes de los clientes se entregan automáticamente.

5.9 ¿Puedo invocar a las API para gestionar los recursos de Huawei Cloud VPN?

Sí.

5.10 ¿Qué son un gateway de cliente y una subred de cliente en una conexión de VPN?

Se crea una conexión de VPN en Huawei Cloud. Como tal, una subred de una VPC de Huawei Cloud es una subred local, y un gateway de VPN creada en Huawei Cloud es un gateway local. La subred y el gateway de un centro de datos local conectado a la VPC son una subred de cliente y un gateway de cliente, respectivamente.

La dirección IP de un cliente es una dirección IP pública.

5.11 ¿Cómo desactivo PFS al crear una conexión de VPN?

- Huawei Cloud

  En la configuración de conexión de VPN, establezca **PFS** en la política IPsec en **Disable**. De forma predeterminada, PFS está habilitado en Huawei Cloud.

- Gateway de clientes en su centro de datos local

  De forma predeterminada, PFS está deshabilitado en los dispositivos de algunos proveedores. Para obtener más información sobre cómo deshabilitar PFS, consulte la documentación del producto correspondiente.

  NOTA

  Asegúrese de que la configuración de PFS en la nube de Huawei y el gateway del cliente sean consistentes. De lo contrario, la negociación no funcionará.

  Por motivos de seguridad, se recomienda habilitar PFS tanto en Huawei Cloud como en el gateway del cliente.

5.12 ¿Cuántas subredes locales y de clientes puedo agregar a una VPN?

- Puede configurar un máximo de 50 subredes locales para cada gateway de VPN.
- Puede configurar un máximo de 50 subredes de cliente para cada conexión de VPN.

5.13 ¿Cuáles son las precauciones para configurar las subredes locales y de cliente para una conexión de VPN?

- El número de subredes locales y el número de subredes de clientes son limitados. Si el número de subredes locales o de cliente excede el límite superior, agregue las subredes.
  - Número máximo de subredes locales para cada gateway de VPN: 50
  - Número máximo de subredes de clientes para cada conexión de VPN: 50
- La subred local no puede incluir el bloque CIDR de la subred remota. La subred remota puede incluir el bloque CIDR de la subred local.
- Hay rutas que apuntan a las subredes locales en la VPC donde reside el gateway de VPN.
- Si hay dos conexiones (conexión A y conexión B) creadas para un gateway de VPN, y la subred remota de la conexión A está dentro de la conexión B, cuando la red de destino a la que se va a acceder pertenece al bloque CIDR solapado, la conexión creada primero se hace coincidir primero. Independientemente del estado de la conexión. (La coincidencia de longitud de máscara no se utiliza para la VPN basada en políticas.)

5.14 ¿Por qué una conexión de VPN está en estado no conectado en la consola de gestión cuando ya está disponible?

Hay un cierto retraso en la actualización del estado de conexión de VPN en la consola de gestión.

Si el acceso al servicio es normal, se ha establecido la conexión de VPN. El estado de la conexión de VPN se actualizará a **Connected** después de varios minutos.

5.15 ¿Qué puedo hacer si se muestra un mensaje que indica que la conexión de VPN no existe después de que se modifiquen las políticas de negociación?

Este problema se debe al intervalo de actualización de la página.

Cuando modifica la configuración avanzada de la política, el sistema elimina la conexión de VPN y, a continuación, crea una. Si la página muestra temporalmente un mensaje que indica que se está eliminando o creando la conexión, no vuelva a crear la misma conexión con la misma subred local, subred de cliente y gateway de cliente.

Si la página permanece en el estado de eliminación o creación de conexión durante mucho tiempo, **envíe un ticket de servicio**.

5.16 ¿Cuál es el ancho de banda máximo admitido por un gateway de VPN?

El ancho de banda máximo soportado por un gateway de VPN es de 1 Gbit/s.

5.17 ¿Qué versión de IKE debo seleccionar al crear una conexión de VPN?

Huawei Cloud recomienda IKEv2 porque IKEv1 no es seguro. Además, IKEv2 supera a IKEv1 en negociación y establecimiento de conexiones, métodos de autenticación, procesamiento de tiempo de espera de detección de pares muertos (DPD) y procesamiento de tiempo de espera de asociación de seguridad (SA).

Huawei Cloud no será compatible con IKEv1 pronto.

Introducción a IKEv1 e IKEv2

- Como protocolo híbrido, IKEv1 trae algunos defectos de seguridad y rendimiento debido a su complejidad. Como tal, se ha convertido en un cuello de botella en el sistema IPsec.
- IKEv2 resuelve los problemas de IKEv1 mientras conserva las funciones básicas de IKEv1. IKEv2 es más simplificado, eficiente, seguro y robusto que IKEv1. Adicionalmente, IKEv2 se define por RFC 4306 en un único documento, mientras que IKEv1 se definen en múltiples documentos. Al minimizar las funciones principales y los algoritmos de contraseña predeterminados, IKEv2 mejora en gran medida la interoperabilidad entre diferentes VPN IPsec.

Riesgos de seguridad de IKEv1

- Los algoritmos criptográficos soportados por IKEv1 no se han actualizado durante más de 10 años. Además, IKEv1 no admite algoritmos criptográficos fuertes como AES-GCM y ChaCha20-Poly1305. Para IKEv1, el bit E (Encryption) en la cabecera ISALMP especifica que las cargas útiles que siguen a la cabecera ISALMP están cifradas, pero cualquier verificación de integridad de datos de esas cargas útiles es manejada por una carga útil hash separada. Esta separación de la encriptación de la protección de la integridad de los datos impide el uso de encriptación autenticada (AES-GCM) con IKEv1.
- IKEv1 es vulnerable a ataques de amplificación DoS y ataques de conexión semiabierta. Después de responder a paquetes falsificados, el respondedor mantiene relaciones iniciador-respondedor, consumiendo un gran número de recursos del sistema.

  Este defecto es inherente a IKEv1 y se aborda en IKEv2.
- El modo agresivo de IKEv1 no es seguro. En este modo, los paquetes de información no están cifrados, lo que plantea riesgos de fuga de información. También hay ataques de fuerza bruta dirigidos al modo agresivo, como los ataque de intermediario.

Diferencias entre IKEv1 e IKEv2

- **Proceso de negociación**
  - IKEv1 es complejo y consume una gran cantidad de ancho de banda. La negociación IKEv1 SA consta de dos fases. En IKEv1 fase 1, se establece un IKE SA en modo principal o modo agresivo. El modo principal requiere tres intercambios entre pares que suman seis mensajes ISAKMP, mientras que el modo agresivo requiere dos intercambios que suman tres mensajes ISAKMP. El modo agresivo es más rápido, pero no proporciona protección de identidad para los pares, ya que el intercambio de claves y la autenticación de identidad se realizan simultáneamente. En IKEv1 fase 2, las SA IPsec se establecen con tres mensajes ISAKMP en modo rápido.
  - En comparación con IKEv1, IKEv2 simplifica el proceso de negociación de SA. IKEv2 requiere solamente dos intercambios, totalizando 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 para cada par adicional de SA.

    NOTA

    Para la negociación IKEv1, su modo principal implica nueve (6+3) mensajes, y su modo agresivo implica seis (3+3) mensajes. Por el contrario, la negociación IKEv2 requiere solamente cuatro (2+2) mensajes.
- **Métodos de autenticación**
  - Solo IKEv1 (que requiere una tarjeta de encriptación) admite la autenticación de envolvente digital (HSS-DE).
  - IKEv2 admite la autenticación del Extensible Authentication Protocol (EAP). IKEv2 puede utilizar un servidor AAA para autenticar remotamente a los usuarios móviles y de PC y asignar direcciones IP privadas a estos usuarios. IKEv1 no proporciona esta función y debe usar L2TP para asignar direcciones IP privadas.
  - Solo IKEv2 admite algoritmos de integridad de IKE SA.
- **Procesamiento de tiempo de espera de DPD**
  - Solo IKEv1 admite el parámetro **retry-interval**. Si un dispositivo envía un paquete DPD pero no recibe respuesta dentro del intervalo de reintento especificado, el dispositivo registra un evento de fallo de DPD. Cuando el número de eventos de error de DPD llega a 5, se eliminan tanto las SA IKE como las SA IPsec. La negociación IKE SA se iniciará de nuevo solo cuando haya tráfico que se transmita a través del túnel IPsec.
  - En IKEv2, el intervalo de retransmisión aumenta de 1, 2, 4, 8, 16, 32 a 64, en segundos. Si no se recibe respuesta dentro de ocho transmisiones consecutivas, el extremo par se considera muerto, y se eliminan las SA IKE y las SA IPsec.
- **Procesamiento del tiempo de espera de IKE SA y del tiempo de espera de IPsec SA**

  En IKEv2, la vida útil suave de IKE SA es 9/10 de la vida útil dura de IKE SA más o menos un número aleatorio. Esto reduce la probabilidad de que dos extremos inicien la renegociación simultáneamente. Por lo tanto, no se establece manualmente la vida útil de software en IKEv2.

Ventajas de IKEv2 sobre IKEv1

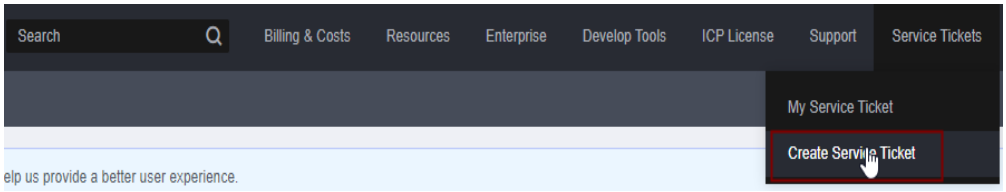
- Simplifica el proceso de negociación de SA, mejorando la eficiencia.
- Corrige muchas vulnerabilidades de seguridad criptográfica, mejorando la seguridad.

- Admite la autenticación de EAP, lo que mejora la flexibilidad y la escalabilidad de la autenticación.
- EAP es un protocolo de autenticación que admite múltiples métodos de autenticación. La mayor ventaja de EAP es su escalabilidad. Es decir, se pueden agregar nuevos métodos de autenticación sin cambiar el sistema de autenticación original. La autenticación EAP ha sido ampliamente utilizada en redes de acceso telefónico.
- Emplea una carga útil cifrada sobre la base de ESP. Esta carga útil contiene tanto un algoritmo de encriptación como un algoritmo de integridad de datos. AES-GCM garantiza la confidencialidad, integridad y autenticación, y funciona bien con IKEv2.

5.18 ¿Qué tipos de tickets de servicio VPN hay? ¿Cómo puedo crear un ticket de servicio de VPN?

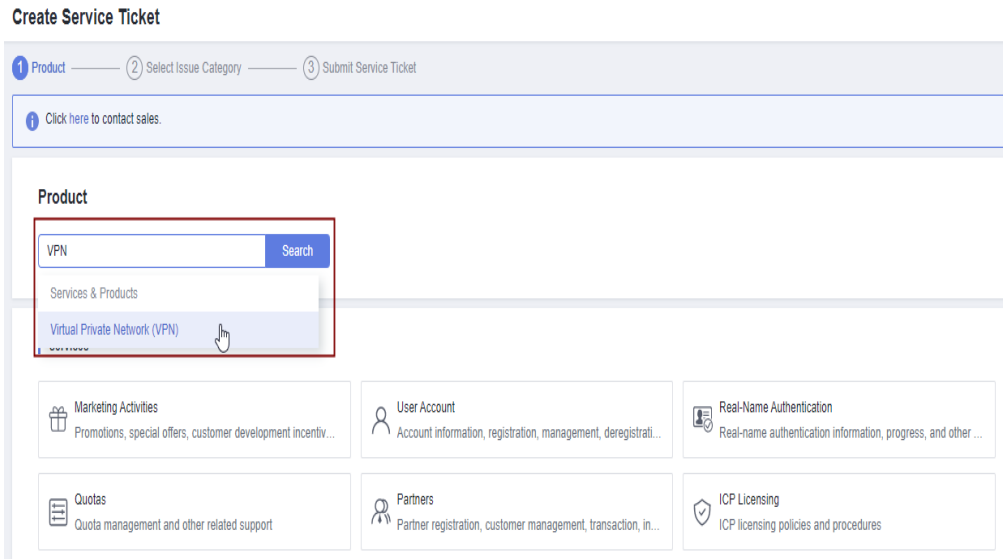
1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la consola de gestión, seleccione **Service Tickets** > **Create Service Ticket**.

Figura 5-1 Crear ticket de servicio



3. Busque **VPN** y seleccione **Virtual Private Network (VPN)**.

Figura 5-2 Selección de **Virtual Private Network (VPN)**



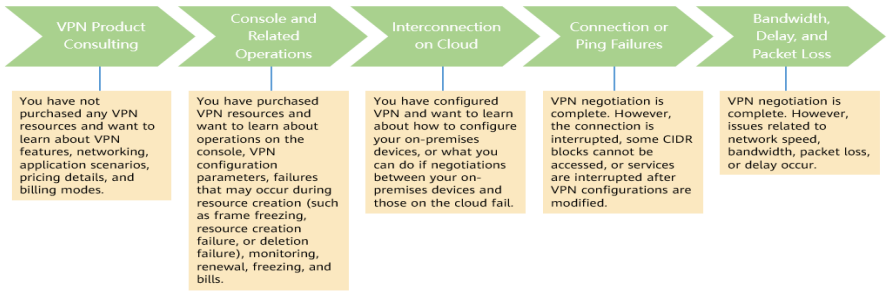
4. Seleccione una categoría de error.

Figura 5-3 Seleccionar categoría de problema

NOTA

Cuando **envía un ticket de servicio**, seleccione una categoría de problema para facilitar la gestión del problema.

Figura 5-4 Categoría de emisión y base de clasificación



5.19 ¿Se requiere un nombre de usuario y contraseña para crear una conexión de VPN IPsec?

No. Huawei Cloud IPsec VPN utiliza una clave precompartida (PSK) para la autenticación. El PSK se configura en un gateway de VPN y se establecerá una conexión después de que se complete la negociación de VPN. Por lo tanto, no se requiere ningún nombre de usuario o contraseña para crear una conexión de VPN IPsec. En general, las VPN SSL, PPTP y L2TP usan nombres de usuario y contraseñas para la autenticación.

NOTA

IPsec XAUTH proporciona autenticación extendida para IPsec VPN. Requiere que los usuarios introduzcan sus nombres de usuario y contraseñas durante la negociación de VPN.

Huawei Cloud VPN no es compatible con IPsec XAUTH.

5.20 ¿Qué recursos de VPN se pueden monitorear?

VPN gateway

Se puede supervisar la siguiente información de ancho de banda de una dirección IP de gateway de VPN: tráfico entrante, ancho de banda entrante, tráfico saliente, ancho de banda saliente y uso de ancho de banda saliente.

Para ver la información de supervisión, haga clic en  en la columna **Gateway IP Address** de la lista de gateway de VPN.

VPN connection

Se puede supervisar la siguiente información sobre una conexión de VPN: estado de la conexión de 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 supervisar RTT de enlace promedio, RTT de enlace máximo, tasa de pérdida de paquetes de enlace, RTT de túnel promedio, RTT de túnel máximo y tasa de pérdida de paquetes de túnel, haga clic en el nombre de la conexión de VPN y haga clic en **Add** en el área **Health Check** de la página de fichas **Summary** para agregar elementos de comprobación de estado.

Para ver el estado de una conexión de VPN, haga clic en  en la columna **Monitoring** de la conexión de VPN.

5.21 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Para ver el estado de una conexión de VPN, haga clic en  en la columna **Monitoring** de la conexión de VPN.

6 Negociación e interconexión de VPN

6.1 ¿Qué dispositivos se pueden conectar a Huawei Cloud por una VPN?

Huawei Cloud VPN admite el protocolo de Internet Protocol Security (IPsec) estándar. Un dispositivo de su centro de datos local puede conectarse a Huawei Cloud si el dispositivo cumple los siguientes requisitos:

1. Soporta la VPN sobre IPsec.
2. Tiene una dirección IP pública fija, que se puede configurar estáticamente, o traducir con NAT en escenarios transversales de NAT (su dispositivo se despliega detrás de un gateway NAT).

La mayoría de los dispositivos son routers y firewalls. Para obtener más información sobre la configuración de la interconexión, consulte la **Guía del administrador**.

NOTA

- Los routers de banda ancha domésticos comunes, los hosts de Windows que proporcionan servicios VPN (como L2TP) y los terminales móviles personales no pueden conectarse a Huawei Cloud con una VPN.
- Los siguientes productos pueden conectarse a Huawei Cloud con VPN:
  - Dispositivos: firewalls y enrutadores de acceso (AR) de Huawei, firewalls de Hillstone y firewalls de Check Point
  - Servicios en la nube: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) y Microsoft Azure
  - Software: strongSwan
- El protocolo IPsec es un protocolo de IETF estándar. Los dispositivos que admiten IPsec pueden interconectarse con Huawei Cloud con una VPN.

  La mayoría de los routers y firewalls de clase empresarial admiten el protocolo de IPsec.
- Algunos dispositivos admiten IPsec VPN solo después de comprar las licencias de software requeridas.

  El administrador del centro de datos local puede consultar con el proveedor del dispositivo si se requiere una licencia según el modelo del dispositivo.

6.2 ¿Qué son los parámetros de negociación de VPN? ¿Cuáles son sus valores predeterminados?

Tabla 6-1 Parámetros de negociación de VPN

Protocolo	Parámetro	Valor
IKE	Authentication Algorithm	● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● AES-256-GCM-16
	DH Algorithm	● Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 14 (valor predeterminado) ● Grupo 16 ● Grupo 19 ● Grupo 20 ● Grupo 21
	Version	● v1 (no recomendado debido a riesgos de seguridad) ● v2 (valor predeterminado)
	Lifetime (s)	**86400** (valor predeterminado) Unidad: segundo Rango de valores: de **60** a **604800**

Protocolo	Parámetro	Valor
	Local ID	● Dirección IP La dirección IP local se muestra automáticamente como la EIP del gateway de VPN, eliminando la necesidad de configurarlo manualmente. ● FQDN De forma predeterminada, el tipo de ID local es la dirección IP y el valor de ID local es la EIP del gateway de VPN.
	Customer ID	● 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 del gateway del cliente.
IPsec	Authentication Algorithm	● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● AES-256-GCM-16
	PFS	● DH grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 14 (valor predeterminado) ● DH grupo 15 ● DH grupo 16 ● DH grupo 19 ● DH grupo 20 ● DH grupo 21 ● Deshabilitar

Protocolo	Parámetro	Valor
	Protocolo de transferencia	● ESP (valor predeterminado)
	Lifetime (s)	**3600** (valor predeterminado) Unidad: segundo Rango de valores: de **30** a **604800**

NOTA

- Perfect Forward Secrecy (PFS) es una característica de seguridad.

  La negociación de IKE tiene dos fases, la fase 1 y la fase 2. La clave de la fase 2 (IPsec SA) se deriva de la clave generada en la fase 1. Una vez que se divulga la clave en la fase 1, la seguridad de la VPN IPsec puede verse afectada negativamente. Para mejorar la seguridad de la clave, IKE proporciona PFS. Cuando PFS está habilitado, se realizará un intercambio de DH adicional durante la negociación de SA de IPsec para generar una nueva clave de SA de IPsec, lo que mejorará la seguridad de SA de IPsec.
- Por motivos de seguridad, PFS está habilitado en Huawei Cloud de forma predeterminada. Asegúrese de que PFS también esté habilitado en el dispositivo de gateway del centro de datos local y de que la configuración de PFS en ambos extremos sea la misma. De lo contrario, la negociación no funcionará.
- La vida útil predeterminada basada en el tráfico de una SA IPsec es de 1,843,200 KB y no se puede cambiar para Huawei Cloud VPN. Este parámetro no participa en la negociación y no tiene ningún impacto en el establecimiento de una SA IPsec.

6.3 ¿Se establece automáticamente una conexión de VPN IPsec?

Sí. Una conexión IPsec de VPN se establece automáticamente.

6.4 ¿Cómo configuro una VPN en un dispositivo local? (Ejemplo de configuración de VPN en un firewall de Huawei serie USG6600)

La configuración de VPN en el dispositivo de su centro de datos local debe ser coherente con la de la nube. De lo contrario, no se puede establecer la VPN.

Para configurar una VPN, también debe configurar un túnel de VPN IPsec en el router o firewall en su centro de datos local. El método de configuración varía según el dispositivo de red en uso. Para obtener más información, consulte la guía de configuración de su dispositivo de red.

El siguiente ejemplo utiliza un firewall de Huawei serie USG6600 que ejecuta V100R001C30SPC300 para describir cómo configurar una VPN en un dispositivo local.

Supongamos que las subredes de un centro de datos local son 192.168.3.0/24 y 192.168.4.0/24, y la dirección IP pública de la salida del túnel IPsec en el centro de datos

local es 1.1.1.2. Las subredes de una VPC son 192.168.1.0/24 y 192.168.2.0/24, y la dirección IP pública de la salida del túnel IPsec en la VPC es 1.1.1.1.

Procedimiento

1. Inicie sesión en la interfaz de línea de comandos (CLI) del firewall.
2. Compruebe la información de la versión del firewall.
```
display version
17:20:502017/03/09
Huawei Versatile Security Platform Software
Software Version: USG6600 V100R001C30SPC300 (VRP (R) Software, Version 5.30)
```
3. Cree una ACL.
```
acl number 3065 vpn-instance vpn64
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
q
```
4. Cree una propuesta IKE.
```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```
5. Cree un par IKE y vincúlelo a la propuesta IKE creada. La dirección IP del par es 1.1.1.1.
```
ike peer vpnikepeer_64
pre-shared-key ******** (******** indicates a pre-shared key.)
ike-proposal 64
undo version 2
remote-address vpn-instance vpn64 1.1.1.1
sa binding vpn-instance vpn64
q
```
6. Configure una propuesta de IPsec.
```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```
7. Configure una política IPsec y vincule la propuesta IPsec a ella.
```
IPsec policy vpnIPsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal IPsecpro64
local-address 1.1.1.2
q
```
8. Aplique la política IPsec a la subinterfaz correspondiente.
```
interface GigabitEthernet0/0/2.64
IPsec policy vpnIPsec64
q
```
9. Prueba de conectividad.

   Pruebe la conectividad entre su ECS en la nube y un host en su centro de datos local, como se muestra en **Figura 6-1**.

Figura 6-1 Prueba de conectividad

```
root@i-psiybqhh:/home/ubuntu# ifconfig
eth0      Link encap:Ethernet  HWaddr 52:54:7c:ba:bf:cc
          inet addr:192.168.3.2  Bcast:192.168.3.255  Mask:255.255.255.0
          inet6 addr: fe80::5054:7cff:feba:bfcc/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2304 (2.3 KB)  TX bytes:3404 (3.4 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:16 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1296 (1.2 KB)  TX bytes:1296 (1.2 KB)

root@i-psiybqhh:/home/ubuntu# ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_req=1 ttl=62 time=4.55 ms
64 bytes from 192.168.1.2: icmp_req=2 ttl=62 time=1.27 ms
64 bytes from 192.168.1.2: icmp_req=3 ttl=62 time=1.25 ms
64 bytes from 192.168.1.2: icmp_req=4 ttl=62 time=0.871 ms
64 bytes from 192.168.1.2: icmp_req=5 ttl=62 time=0.886 ms
64 bytes from 192.168.1.2: icmp_req=6 ttl=62 time=0.676 ms
64 bytes from 192.168.1.2: icmp_req=7 ttl=62 time=1.06 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6008ms
rtt min/avg/max/mdev = 0.676/1.510/4.554/1.258 ms
```

6.5 ¿Huawei Cloud VPN admite la interconexión con un gateway del cliente a través de un nombre de dominio?

No. Huawei Cloud VPN admite la interconexión con un gateway del cliente solo con la dirección IP pública del gateway del cliente.

6.6 ¿Cuántos túneles tiene mi conexión de VPN?

Número de túneles en una conexión de VPN = Número de subredes locales x Número de subredes de clientes

- Un túnel IPsec está en estado activo cuando el tráfico de datos se transmite entre dos subredes en los dos extremos del túnel de IPsec.
- Una conexión de VPN está en estado Connected siempre que uno de sus túneles esté en estado Active.

6.7 ¿Cómo permito que hosts específicos accedan a una subred de VPC por una conexión de VPN creada?

Restricciones en el centro de datos local:

- Políticas de control de acceso en el dispositivo de VPN
- Reglas de ACL en el router o switch

Restricciones en el lado de la nube:

- Reglas de grupo de seguridad que permiten el acceso solo desde direcciones IP especificadas

- Reglas de ACL

NOTA

Se recomienda no cambiar la subred local o de cliente para controlar el acceso.

6.8 ¿Las VPN en Huawei Cloud tienen habilitada la función DPD?

Sí.

De forma predeterminada, la función de detección de pares muertos (DPD) está habilitada para que las VPN de Huawei Cloud detecten el estado del proceso IKE en un centro de datos local.

Después de tres fallos de detección consecutivos, el proceso IKE en el centro de datos local se considera anormal y el túnel en la nube se elimina automáticamente.

El protocolo DPD no requiere que el extremo par también esté configurado con DPD, pero requiere que el extremo par sea capaz de responder a las detecciones de DPD. Para garantizar estados de túnel consistentes en los dos extremos, se recomienda habilitar DPD en su gateway local para detectar el estado del proceso IKE del servicio VPN en Huawei Cloud.

NOTA

La eliminación del túnel en caso de fallos de detección de DPD no afectará la estabilidad del servicio.

6.9 ¿Cómo puedo usar grupos de seguridad para evitar el acceso de VPN a algunos ECS en una VPC para implementar el aislamiento de seguridad?

Puede configurar grupos de seguridad para permitir el acceso solo a bloques CIDR o ECS específicos en una VPC con una VPN.

ejemplo de configuración: Evite que la subred 192.168.1.0/24 del cliente acceda a los ECS en la subred 10.1.0.0/24 de VPC.

Procedimiento:

1. Cree los grupos de seguridad 1 y 2.
2. Configure el grupo de seguridad 1 para denegar el acceso desde la subred 192.168.1.0/24.
3. Configure el grupo de seguridad 2 para permitir el acceso desde la subred 192.168.1.0/24.
4. Asociar ECS en la subred 10.1.0.0/24 con el grupo de seguridad 1 y asociar otros ECS en la VPC con el grupo de seguridad 2.

6.10 ¿Se restablecerá una conexión de VPN después de que se modifique su configuración?

Una conexión de VPN consta de subredes locales, subredes de clientes, gateway de clientes, claves previamente compartidas (PSK), política de negociación IKE y política de negociación IPsec. Una conexión de VPN se modifica si ocurre alguna de las siguientes situaciones:

- Si se modifican las subredes locales y de cliente, el ID de conexión permanecerá sin cambios. Si no se actualizan todas las subredes, el túnel establecido entre las subredes no se restablecerá.
- Si se cambia la dirección IP del gateway del cliente, el ID de conexión permanecerá sin cambios, pero se restablecerá la conexión de VPN.
- Si solo se cambian las PSK, el ID de conexión y el estado permanecerán sin cambios. El PSK se comprobará de nuevo durante la renegociación. Si las PSK no coinciden, la renegociación falla.
- Si se modifica una política de negociación (se requiere la verificación de PSK), se cambiará el ID de conexión y se deberá restablecer la conexión.

6.11 ¿Por qué no puedo iniciar la negociación de Amazon Web Services con Huawei Cloud después de que estén interconectados?

Después de establecer una conexión de VPN entre Amazon Web Services (AWS) y Huawei Cloud, AWS funciona en modo de respuesta y no inicia la negociación. Como tal, el establecimiento de SA no se activará cuando un AWS EC2 acceda a un ECS de Huawei Cloud.

Según el documento de AWS, la negociación solo puede iniciarse desde el lado del cliente (en este caso, Huawei Cloud).

6.12 ¿Cómo configuro DPD para la interconexión con Huawei Cloud?

De forma predeterminada, DPD está habilitado en Huawei Cloud y no se puede deshabilitar.

Puede configurar DPD de la siguiente manera:

- DPD-type: bajo demanda
- DPD idle-time: 30s
- DPD retransmit-interval: 15s
- DPD retry-limit: 3
- DPD msg: seq-hash-notify

El formato **DPD msg** en ambos extremos de la conexión de VPN debe ser el mismo, pero el tipo DPD, el tiempo de inactividad, el intervalo de retransmisión y el límite de reintentos pueden ser diferentes.

6.13 ¿Qué debo hacer si mi firewall no puede recibir paquetes de respuesta desde el gateway de Huawei Cloud VPN en la fase 1 de IKE?

1. Compruebe si las direcciones IP públicas de los dos extremos pueden comunicarse entre sí ejecutando el comando ping. De forma predeterminada, las EIP de gateway de VPN en Huawei Cloud se pueden hacer ping.
2. Verifique que el gateway local (firewall) y el gateway de Huawei Cloud VPN puedan intercambiar paquetes con los puertos UDP 500 y 4500.
3. Compruebe que el número de puerto de origen no se traduce cuando el gateway local accede al gateway de VPN en Huawei Cloud. En un escenario de NAT transversal, asegúrese de que el número de puerto de origen no se cambie después de NAT transversal.
4. Verifique que la configuración de los parámetros de negociación IKE sea coherente en los dos extremos de la VPN.

   En un escenario NAT transversal, establezca el tipo de ID de cliente en dirección IP y el valor en la dirección IP pública post-NAT del gateway local.

6.14 ¿Qué debo hacer si mi firewall no puede recibir paquetes de respuesta de una subred de VPN en Huawei Cloud?

1. Compruebe las rutas, las políticas de seguridad, la configuración de NAT, el tráfico interesante y las políticas de negociación para la negociación de la fase 2 en el dispositivo de gateway local.
   - Configuraciones de ruta: Enrute los datos para acceder a las subredes de la nube a los túneles.
   - Políticas de seguridad: permite el tráfico de subredes locales a subredes en la nube.
   - Políticas de NAT: no realice NAT de origen en el tráfico originado desde las subredes locales a las subredes de la nube.
   - Tráfico interesante: Las configuraciones de tráfico interesantes en ambos extremos se invierten en los dos extremos de una conexión de VPN. El nombre del objeto de dirección no se puede utilizar para el tráfico interesante configurado con IKEv2.
   - Políticas de negociación: Garantizar que las políticas de negociación, especialmente las PFS, en ambos extremos sean las mismas.
2. Después de confirmar que las negociaciones de la fase 1 y la fase 2 son normales, asegúrese de que los grupos de seguridad en la nube permiten los paquetes de ICMP originados desde subredes locales a subredes en la nube.

6.15 ¿Cuántos bits tienen los grupos DH que utiliza Huawei Cloud VPN?

Los grupos Diffie-Hellman (DH) determinan la fuerza de la clave utilizada en el proceso de intercambio de claves. Los números de grupo DH más altos suelen ser más seguros, pero se requiere más tiempo para calcular la clave.

Tabla 6-2 enumera el número de bits correspondientes a los grupos DH utilizados por VPN.

Tabla 6-2 Número de bits correspondientes a cada grupo DH

Grupo DH	Módulo
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	256 bits (ECP)
20	384 bits (ECP)
21	521 bits (ECP)

NOTA

Los siguientes algoritmos de DH tienen riesgos de seguridad y no se recomiendan: DH grupo 1, DH grupo 2 y DH grupo 5.

7 Error de conexión o de ping

7.1 ¿Por qué una conexión de VPN siempre está en estado no conectado después de completar su configuración?

La configuración puede ser incorrecta.

1. En los dos extremos (en la nube y en el centro de datos local) de la conexión de VPN, asegúrese de que las claves precompartidas (PSK) y la información de negociación sean consistentes, las subredes locales y remotas se inviertan, y los gateway locales y remotos también se invierten.
2. Asegúrese de que las rutas, NAT y políticas de seguridad estén correctamente configuradas en el dispositivo de su centro de datos local.

7.2 ¿Cómo puedo evitar las desconexiones de VPN?

Las conexiones de VPN se renegocian cuando la vida útil de la SA IPsec está a punto de expirar o cuando los datos transmitidos con una conexión de VPN superan los 20 GB. Por lo general, la renegociación no interrumpe las conexiones de VPN.

La mayoría de las desconexiones se deben a configuraciones incorrectas en los dos extremos de la conexión de VPN o a fallos de renegociación debidos a excepciones de Internet.

Las causas comunes de las desconexiones son las siguientes:

- Las ACL en ambos extremos de la conexión de VPN no coinciden.
- La configuración de la vida útil de SA en ambos extremos de la conexión de VPN es diferente.
- Dead Peer Detection (DPD) no está configurada en el dispositivo del centro de datos local.
- La configuración se modifica cuando la conexión de VPN está en uso.
- La fluctuación se produce en la red del operador.

Por lo tanto, asegúrese de que las siguientes configuraciones de VPN son correctas para mantener las conexiones de VPN activas:

- En los dos extremos de la conexión de VPN, se invierten las configuraciones de subred local y remota.
- La configuración de la duración de la SA en ambos extremos de la conexión de VPN es la misma.
- DPD está habilitado en el dispositivo del gateway local y el número de veces de detección es de 3 o más.
- Los parámetros se modifican en ambos extremos de la conexión de VPN durante el uso de la conexión de VPN.
- Establezca TCP MAX-MSS en 1300 para el dispositivo del gateway local.
- El ancho de banda del dispositivo del gateway local es lo suficientemente grande para la conexión de VPN.
- La negociación de conexión de VPN se puede activar por ambos extremos y la negociación activa se ha habilitado en el dispositivo de gateway local.

7.3 ¿Cómo puedo restaurar rápidamente una conexión VPN IPsec interrumpida?

1. Si no se puede activar la negociación, compruebe la conectividad entre las direcciones IP públicas de los gateway en ambos extremos de la conexión IPsec VPN. Por ejemplo, puede ejecutar el comando ping para comprobar la conectividad. De forma predeterminada, el gateway de Huawei Cloud VPN responde a los paquetes ICMP.
2. Si la conectividad es normal, compruebe si se produce la conmutación de enlace entre las interfaces salientes.That is, check whether the traffic for access to the Huawei Cloud VPN gateway is forwarded out from a non-negotiated interface.
3. If traffic is forwarded through the correct link, change the PSKs at both ends of the IPsec VPN connection to trigger re-negotiation.
4. Si la renegociación falla, compruebe si las políticas de negociación configuradas en ambos extremos son coherentes y si las configuraciones de tráfico interesantes en ambos extremos se invierten (el mismo número de configuraciones y las mismas subredes).
5. Si las políticas de negociación y las configuraciones de tráfico interesantes son correctas, deshabilite la conexión de VPN en el dispositivo local. Después de que el estado de conexión de VPN en Huawei Cloud cambie a **Not connected**, habilite la conexión de VPN en el dispositivo local y active un flujo de datos.
6. Si la negociación sigue fallando, realice las siguientes operaciones:
   a. Registre las políticas de negociación, PSK, subredes locales, gateway de cliente y subredes de cliente de la conexión de VPN configurada en Huawei Cloud.
   b. Utilice el gateway de VPN existente para crear otra conexión de VPN. Las políticas de negociación, PSK y subredes locales son las mismas que las de la conexión de VPN original. El gateway del cliente y las subredes del cliente se pueden configurar aleatoriamente.
   c. Después de crear la nueva conexión de VPN, elimine la conexión de VPN original y cambie el gateway del cliente y las subredes del cliente de la nueva conexión de VPN para que sean las mismas que las de la conexión de VPN original.
   d. Active la negociación de nuevo.

Si el fallo persiste, **envíe un ticket de servicio** al servicio de atención al cliente de Huawei Cloud.

7.4 ¿Qué sucederá si el tráfico supera el ancho de banda de un gateway de VPN?

El ancho de banda del gateway de VPN se aplica al tráfico en la dirección de salida de una VPC. Si el tráfico saliente en la VPC excede el ancho de banda, se producirá una congestión de la red, no se podrá acceder a algunas subredes o incluso se interrumpirá la conexión de VPN debido al tiempo de espera de detección de VPN.

En este caso, se recomienda aumentar el ancho de banda del gateway de VPN.

NOTA

El ancho de banda máximo de una VPN es de 1 Gbit/s.

7.5 ¿Se establece automáticamente una conexión de VPN IPsec?

Sí. Una conexión IPsec de VPN se establece automáticamente.

7.6 ¿Por qué los ECS en los dos extremos de una conexión de VPN normal entre regiones no pueden hacer ping entre sí?

De forma predeterminada, un grupo de seguridad permite el tráfico saliente con cualquier número de puerto. Para permitir el tráfico entrante, agregue reglas entrantes al grupo de seguridad. Asegúrese de que el grupo de seguridad asociado con el ECS que necesita recibir paquetes de ping permita las solicitudes de ICMP entrantes.

7.7 ¿Por qué las subredes en los dos extremos de una conexión de VPN normal no pueden acceder entre sí?

La conexión de VPN es normal, lo que indica que los parámetros de negociación en ambos extremos de la conexión de VPN son correctos. Debe realizar las siguientes operaciones:

- Verifique que las rutas al dispositivo de VPN en su centro de datos local estén correctamente configuradas.
- Compruebe que el intercambio de datos entre subred está permitido en el dispositivo de VPN.
- Compruebe que no se realiza NAT en las subredes locales que necesitan acceder a la nube.
- Verifique que se permita el acceso mutuo entre las direcciones IP públicas del gateway de VPN y el gateway del cliente.

7.8 ¿Qué hago si se interrumpe una conexión de VPN y se muestra un mensaje que indica que el flujo de datos no coincide?

Esto generalmente se debe a una falta de coincidencia de ACL entre el gateway de VPN en la nube y el gateway del cliente en su centro de datos local.

1. Verifique que en los dos extremos de la conexión de VPN, las subredes locales y remotas se inviertan y las configuraciones de ACL también se inviertan.
2. Utilice el formato de subred/máscara cuando configure tráfico interesante en su centro de datos local. No utilice el modo de objeto de dirección, ya que puede causar problemas de incompatibilidad.

7.9 ¿Qué hago si se interrumpe una conexión de VPN y se muestra un mensaje que indica el tiempo de espera de DPD?

Esto sucede porque no hay intercambio de datos a través de la conexión de VPN. Cuando finaliza la vida útil de la SA, la conexión de VPN se elimina ya que el extremo del par no responde a la detección del par muerto (DPD).

Solución

1. Habilite DPD en el dispositivo de gateway local y verifique que los flujos de datos de ambos extremos puedan activar el establecimiento de conexión.
2. Despliegue un script de shell ping en los servidores en ambos extremos. Alternativamente, configure una función Keepalive (por ejemplo, NQA en dispositivos Huawei) en el dispositivo de gateway local para mantener la conexión activa.

7.10 ¿Por qué una conexión de VPN está en estado no conectado en la consola de gestión cuando ya está disponible?

Hay un cierto retraso en la actualización del estado de conexión de VPN en la consola de gestión.

Si el acceso al servicio es normal, se ha establecido la conexión de VPN.

7.11 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Para ver el estado de una conexión de VPN, haga clic en  en la columna **Monitoring** de la conexión de VPN.

7.12 ¿Qué hago si no se establece una conexión de VPN?

1. Inicie sesión en la consola de gestión y elija **Virtual Private Network** > **Enterprise – VPN Connections**.
2. En la lista de conexiones de VPN, localice la conexión de VPN de destino y elija **More** > **Modify Policy Settings** a la derecha para ver las políticas IKE e IPsec de la conexión de VPN.
3. Compruebe las políticas IKE e IPsec para ver si los modos de negociación y los algoritmos de encriptación en ambos extremos de la conexión de 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 de VPN pueden ser inconsistentes.
4. Compruebe si las reglas 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 para permitir la comunicación con las subredes de VPC. A continuación se proporciona un ejemplo de configuraciones de ACL:

   ```
   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. Haga ping a los dos extremos de la conexión de VPN entre sí para comprobar si la conexión de VPN es normal.

7.13 ¿Qué debo hacer si no puedo acceder a los ECS en la nube desde mi centro de datos local o LAN después de que se haya configurado la conexión de VPN?

El grupo de seguridad deniega el acceso desde todos los orígenes de forma predeterminada. Si desea tener acceso a sus ECS, configure las reglas de grupo de seguridad para permitir el acceso desde sus subredes locales.

7.14 ¿Por qué se muestra el estado de una conexión de VPN creada con éxito como no conectada?

Hay un retraso en la actualización del estado de una conexión de VPN en la consola de gestión. Por favor, actualice la página en unos 2 minutos.

7.15 ¿Las VPN en Huawei Cloud tienen habilitada la función DPD?

Sí.

De forma predeterminada, la función de detección de pares muertos (DPD) está habilitada para que las VPN de Huawei Cloud detecten el estado del proceso IKE en un centro de datos local.

Después de tres fallos de detección consecutivos, el proceso IKE en el centro de datos local se considera anormal y el túnel en la nube se elimina automáticamente.

El protocolo DPD no requiere que el extremo par también esté configurado con DPD, pero requiere que el extremo par sea capaz de responder a las detecciones de DPD. Para garantizar estados de túnel consistentes en los dos extremos, se recomienda habilitar DPD en su gateway local para detectar el estado del proceso IKE del servicio VPN en Huawei Cloud.

NOTA

La eliminación del túnel en caso de fallos de detección de DPD no afectará la estabilidad del servicio.

DPD puede detectar excepciones en el proceso IKE en el extremo del par en el tiempo y restablecer el túnel para garantizar la sincronización del túnel entre los dos extremos. Después de eliminar un túnel, si hay tráfico transmitido a través del túnel, el túnel se puede restablecer con la negociación.

8 Direcciones públicas

8.1 ¿Se puede retener la EIP de un gateway de VPN después de que se elimine el gateway de VPN?

Si una EIP de pago por uso está vinculada a un gateway de VPN de pago por uso, la eliminación del gateway de VPN también eliminará la EIP vinculada.

Para conservar tal EIP de pago por uso, desvíselo antes de eliminar el gateway de VPN.

8.2 ¿Se pueden usar las EIP como direcciones IP de gateway de VPN?

No.

Cuando crea un gateway de VPN, su dirección IP se asigna automáticamente. Esta dirección IP tiene configuraciones preestablecidas y se puede utilizar para la interconexión con una VPC. Sin embargo, una EIP no puede utilizarse para la interconexión con una VPC.

8.3 ¿Necesito comprar EIP para que los hosts se comuniquen entre sí por una VPN?

Si sus hosts locales necesitan acceder a un ECS en la nube con una VPN, no necesita comprar ninguna EIP para el ECS.

Si un ECS necesita proporcionar servicios accesibles desde Internet, usted necesita comprar una EIP para el ECS.

8.4 ¿Por qué un ECS tiene información de acceso de EIP después de habilitar una VPN?

Una posible causa es que el ECS tiene una EIP enlazada antes de que se use la VPN. En este escenario, puede acceder al ECS con la VPN y la EIP.

Para permitir que solo los hosts de la VPN accedan al ECS, desvincule la EIP del ECS después de que se establezca la conexión de VPN.

8.5 ¿Puede mi gateway local tener una dirección IP pública no fija?

No.

Para conectar su centro de datos local a Huawei Cloud por una VPN, su gateway local debe tener una dirección IP pública fija. Esta dirección IP pública se puede configurar estáticamente, o traducir con NAT en escenarios transversales de NAT (su dispositivo se despliega detrás de un gateway de NAT).

NOTA

Los routers de banda ancha domésticos comunes, los hosts de Windows que proporcionan servicios VPN (como L2TP) y los terminales móviles personales no pueden conectarse a Huawei Cloud con una VPN.

9 Configuraciones de ruta

9.1 ¿Qué son un gateway de cliente y una subred de cliente en una conexión de VPN?

Se crea una conexión de VPN en Huawei Cloud. Como tal, una subred de una VPC de Huawei Cloud es una subred local, y un gateway de VPN creada en Huawei Cloud es un gateway local. La subred y el gateway de un centro de datos local conectado a la VPC son una subred de cliente y un gateway de cliente, respectivamente.

La dirección IP de un cliente es una dirección IP pública.

9.2 ¿Dónde puedo agregar rutas a las subredes del cliente en la consola de VPN?

Cuando se crea una conexión de VPN, las rutas a las subredes de los clientes se entregan automáticamente.

9.3 ¿Necesito agregar una ruta para un ECS con varias NICs para llegar a la red local?

- Si se utiliza la tarjeta de interfaz de red primaria (NIC) para establecer una conexión de VPN con la red local, no es necesario agregar ninguna ruta.
- Si se utiliza una NIC no primaria para establecer una conexión de VPN con la red local, agregue una ruta a la red local con la dirección de gateway de la NIC no primaria como salto siguiente.

10 Configuraciones de subred

10.1 ¿Cuáles son las precauciones para configurar las subredes locales y de cliente para una conexión de VPN?

- El número de subredes locales y el número de subredes de clientes son limitados. Si el número de subredes locales o de cliente excede el límite superior, agregue las subredes.
  - Número máximo de subredes locales para cada gateway de VPN: 50
  - Número máximo de subredes de clientes para cada conexión de VPN: 50
- La subred local no puede incluir el bloque CIDR de la subred remota. La subred remota puede incluir el bloque CIDR de la subred local.
- Hay rutas que apuntan a las subredes locales en la VPC donde reside el gateway de VPN.
- Si hay dos conexiones (conexión A y conexión B) creadas para un gateway de VPN, y la subred remota de la conexión A está dentro de la conexión B, cuando la red de destino a la que se va a acceder pertenece al bloque CIDR solapado, la conexión creada primero se hace coincidir primero. Independientemente del estado de la conexión. (La coincidencia de longitud de máscara no se utiliza para la VPN basada en políticas.)

10.2 ¿Cuántas subredes locales y de clientes puedo agregar a una VPN?

- Puede configurar un máximo de 50 subredes locales para cada gateway de VPN.
- Puede configurar un máximo de 50 subredes de cliente para cada conexión de VPN.

10.3 ¿Qué hago si ocurre una excepción cuando agrego una subred de cliente durante la creación de una conexión de VPN?

Compruebe si esta subred de cliente está involucrada en una ruta de una interconexión de VPC, Cloud Connect o Direct Connect. Si es así, se produce un conflicto de ruta y es necesario eliminar la ruta y crear una nueva para evitar el conflicto.

10.4 ¿Se puede retener la EIP de un gateway de VPN después de que se elimine el gateway de VPN?

Si una EIP de pago por uso está vinculada a un gateway de VPN de pago por uso, la eliminación del gateway de VPN también eliminará la EIP vinculada.

Para conservar tal EIP de pago por uso, desvíselo antes de eliminar el gateway de VPN.

10.5 ¿Cómo planifico los bloques CIDR para el acceso a una VPC por una conexión de VPN?

- Los bloques CIDR de una VPC no pueden entrar en conflicto con bloques CIDR locales.
- Para evitar conflictos con 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.

10.6 ¿Cómo se asigna una dirección IP de gateway de VPN?

Las direcciones IP del gateway de VPN de Huawei Cloud son un grupo de direcciones IP planificadas antes de comprar los gateway de VPN. Estas direcciones IP están preestablecidas con las configuraciones de VPN.

Cuando compra un gateway de VPN, el sistema asigna aleatoriamente una dirección IP y la vincula a la VPC que seleccionó. Esta dirección IP solo puede estar vinculada a una VPC.

No puede cambiar la dirección IP de un gateway de VPN, ya que esta dirección IP tiene configuraciones predefinidas. Cuando se elimina un gateway de VPN, se libera la relación de enlace entre la dirección IP de gateway y la VPC de gateway. Cuando se compra un nuevo gateway de VPN, el sistema asigna aleatoriamente una nueva dirección IP de gateway.

11 Tráfico interesante de VPN

11.1 ¿Necesito configurar las reglas de ACL en la consola de gestión de Huawei Cloud después de configurar las reglas de ACL en el dispositivo de gateway local?

Es necesario configurar las reglas de política (reglas de ACL) para una conexión de VPN en la consola de gestión de Huawei Cloud solo cuando **VPN Type** está configurado en **Policy-based**.

11.2 ¿Cómo configuro y modifico el tráfico interesante de una VPN en la nube?

El número de reglas que especifican tráfico interesante es el producto del número de subredes locales y el número de subredes de cliente. Por ejemplo, cuando hay subredes locales A y B y subredes de cliente C, D y E, las siguientes seis reglas deben configurarse para especificar tráfico interesante:

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

Si modifica las subredes locales o de cliente en la consola de gestión, la configuración de tráfico interesante se actualiza automáticamente. Es decir, se modifican las reglas de ACL en la nube.

12 Mantener las conexiones VPN activas

12.1 ¿Cómo puedo evitar las desconexiones de VPN?

Las conexiones de VPN se renegocian cuando la vida útil de la SA IPsec está a punto de expirar o cuando los datos transmitidos con una conexión de VPN superan los 20 GB. Por lo general, la renegociación no interrumpe las conexiones de VPN.

La mayoría de las desconexiones se deben a configuraciones incorrectas en los dos extremos de la conexión de VPN o a fallos de renegociación debidos a excepciones de Internet.

Las causas comunes de las desconexiones son las siguientes:

- Las ACL en ambos extremos de la conexión de VPN no coinciden.
- La configuración de la vida útil de SA en ambos extremos de la conexión de VPN es diferente.
- Dead Peer Detection (DPD) no está configurada en el dispositivo del centro de datos local.
- La configuración se modifica cuando la conexión de VPN está en uso.
- La fluctuación se produce en la red del operador.

Por lo tanto, asegúrese de que las siguientes configuraciones de VPN son correctas para mantener las conexiones de VPN activas:

- En los dos extremos de la conexión de VPN, se invierten las configuraciones de subred local y remota.
- La configuración de la duración de la SA en ambos extremos de la conexión de VPN es la misma.
- DPD está habilitado en el dispositivo del gateway local y el número de veces de detección es de 3 o más.
- Los parámetros se modifican en ambos extremos de la conexión de VPN durante el uso de la conexión de VPN.
- Establezca TCP MAX-MSS en 1300 para el dispositivo del gateway local.
- El ancho de banda del dispositivo del gateway local es lo suficientemente grande para la conexión de VPN.

- La negociación de conexión de VPN se puede activar por ambos extremos y la negociación activa se ha habilitado en el dispositivo de gateway local.

13 Monitoreo

13.1 ¿Qué recursos de VPN se pueden monitorear?

VPN gateway

Se puede supervisar la siguiente información de ancho de banda de una dirección IP de gateway de VPN: tráfico entrante, ancho de banda entrante, tráfico saliente, ancho de banda saliente y uso de ancho de banda saliente.

Para ver la información de supervisión, haga clic en  en la columna **Gateway IP Address** de la lista de gateway de VPN.

VPN connection

Se puede supervisar la siguiente información sobre una conexión de VPN: estado de la conexión de 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 supervisar RTT de enlace promedio, RTT de enlace máximo, tasa de pérdida de paquetes de enlace, RTT de túnel promedio, RTT de túnel máximo y tasa de pérdida de paquetes de túnel, haga clic en el nombre de la conexión de VPN y haga clic en **Add** en el área **Health Check** de la página de fichas **Summary** para agregar elementos de comprobación de estado.

Para ver el estado de una conexión de VPN, haga clic en  en la columna **Monitoring** de la conexión de VPN.

13.2 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Para ver el estado de una conexión de VPN, haga clic en  en la columna **Monitoring** de la conexión de VPN.

13.3 ¿Puedo ver el tráfico de cada conexión de VPN?

No. El tráfico de VPN se monitoriza por gateway de VPN. Puede ver el tráfico entrante y saliente, así como los anchos de banda entrante y saliente de un gateway de VPN, pero no puede ver las estadísticas de tráfico de una conexión de VPN específica.

13.4 ¿Se me notificarán los resultados anormales del monitoreo de VPN?

Sí.

Puede configurar, en las consolas de Simple Message Notification (SMN) y de Cloud Eye, para recibir notificaciones si se producen resultados anormales de supervisión de VPN.

14 Ancho de banda y velocidad de red

14.1 ¿Cómo se prueba la velocidad de red de una conexión de VPN?

Entorno de prueba: Se ha creado una conexión de VPN. Se han creado ECS en las subredes locales de las VPC en los dos extremos de la conexión de VPN. Los ECS pueden hacer ping entre sí.

Cuando el ancho de banda de un gateway de VPN adquirido es de 200 Mbit/s:

1. Cuando los ECS en los dos extremos de la conexión de VPN ejecutan Windows, iPerf3 y FileZilla (una aplicación de FTP gratuita para cargar y descargar archivos) se utilizan para probar la velocidad de la red. El resultado de la prueba es de 180 Mbit/s, cumpliendo los requisitos.

   NOTA

   El protocolo FTP basado en TCP tiene un mecanismo de control de congestión, y el protocolo IPsec añade nuevas cabeceras a los paquetes originales. Como tal, es normal en la industria, tener una desviación de velocidad de red de aproximadamente el 10%.

   Figura 14-1 muestra el resultado de probar el ancho de banda de 200 Mbit/s en el cliente iPerf3.

Figura 14-1 Resultado de la prueba para 200 Mbit/s de ancho de banda (cliente de iPerf3)

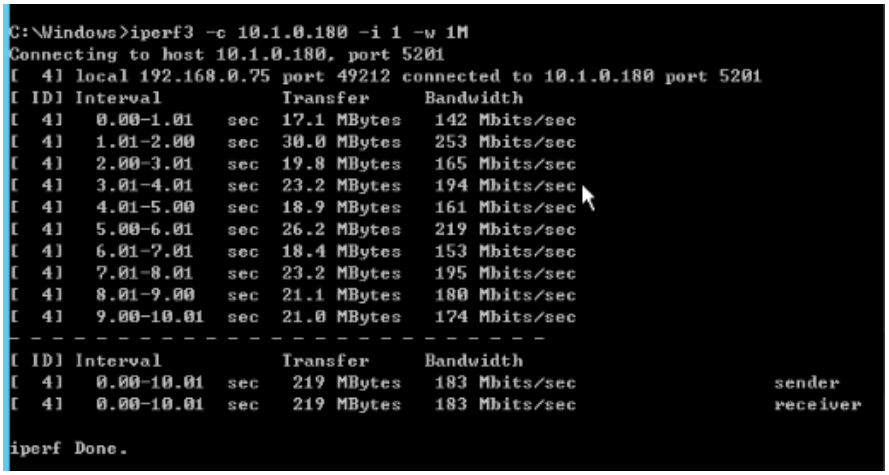
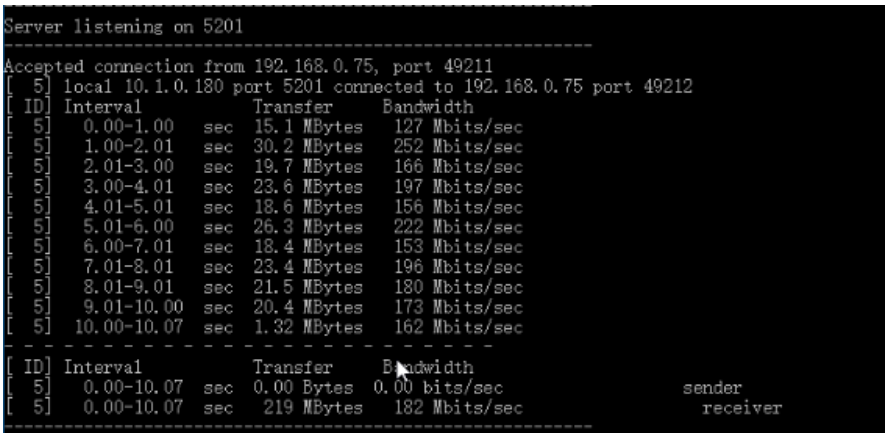


Figura 14-2 muestra el resultado de probar el ancho de banda de 200 Mbit/s en el servidor iPerf3.

Figura 14-2 Resultado de la prueba para un ancho de banda de 200 Mbit/s (servidor de iPerf3)

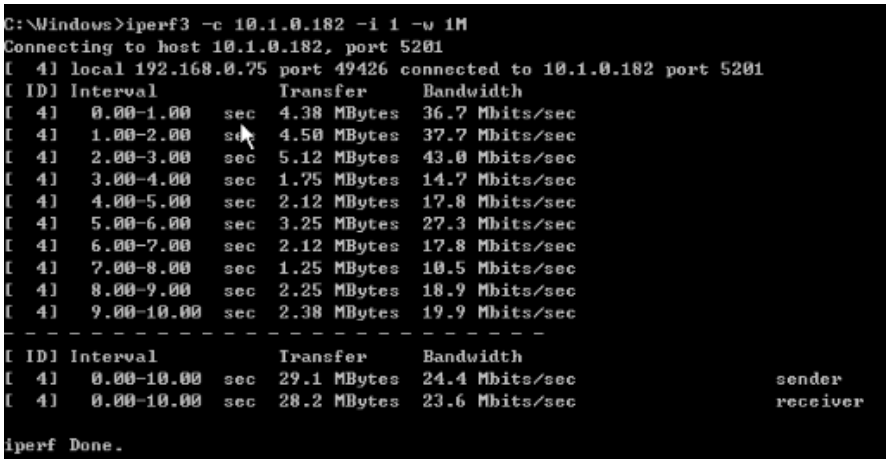


2. Cuando los ECS en los dos extremos de la conexión de VPN ejecutan CentOS 7, iPerf3 se utiliza para probar la velocidad de la red. El resultado de la prueba es de 180 Mbit/s, cumpliendo los requisitos.
3. Cuando el ECS que funciona como un servidor ejecuta CentOS 7 y el ECS que funciona como un cliente ejecuta Windows, iPerf3 y FileZilla se utilizan para probar la velocidad de la red. El resultado de la prueba es de 20 Mbit/s, no cumpliendo los requisitos.

   Esto se debe a que las implementaciones de TCP en Windows y Linux son diferentes.

   Figura 14-3 muestra el resultado del uso de iPerf3 para probar la velocidad de red entre dos ECS que ejecutan diferentes sistemas operativos.

Figura 14-3 Resultado de la prueba en iPerf3



Cuando el ancho de banda de un gateway de VPN adquirido es de 1000 Mbit/s:

NOTA

Algunas regiones admiten solo 300 Mbit/s de ancho de banda de forma predeterminada. Si se requiere un ancho de banda más alto, solicite un ancho de banda de 300 Mbit/s y luego **envíe un ticket de servicio** para ampliar la capacidad.

El ancho de banda del gateway de VPN es compartido por todas sus conexiones de VPN. Para utilizar plenamente el gran ancho de banda de 1000 Mbit/s, despliegar múltiples ECS con altas especificaciones ya que el rendimiento de reenvío de un solo ECS es limitado. Se recomiendan ECS con sus NICs que admitan un ancho de banda de 2 Gbit/s o superior.

Conclusiones: Según los resultados de las pruebas anteriores, los anchos de banda de los gateways de Huawei Cloud VPN cumplen los requisitos. Para aprovechar al máximo el ancho de banda adquirido, se recomienda utilizar servidores que ejecuten el mismo sistema operativo y NIC que cumplan determinados requisitos en los dos extremos de una conexión de VPN.

14.2 ¿En qué dirección está limitado el ancho de banda de VPN? ¿Cuál es la unidad de ancho de banda?

El ancho de banda del gateway de VPN comprado se aplica a la dirección de salida de Huawei Cloud. Para lograr un balanceo entre los anchos de banda en las direcciones de entrada y de salida, el ancho de banda en la dirección de entrada se limita de la siguiente manera:

- Si el ancho de banda adquirido es de 10 Mbit/s o menos, el ancho de banda en la dirección de entrada está limitado a 10 Mbit/s.
- Si el ancho de banda adquirido es mayor que 10 Mbit/s, el ancho de banda en la dirección de entrada es el mismo que el ancho de banda comprado.

La unidad de ancho de banda es Mbit/s y la del tráfico es GB.

14.3 ¿Cómo cambio el ancho de banda de la VPN?

1. En la lista de gateways de VPN, haga clic en el nombre de un gateway de VPN. Se muestra la página de detalles del gateway.

2. En el área **EIP**, haga clic en **Change** junto a **Bandwidth**.
3. Cambie el ancho de banda de EIP.

14.4 ¿Qué sucederá si el tráfico supera el ancho de banda de un gateway de VPN?

El ancho de banda del gateway de VPN se aplica al tráfico en la dirección de salida de una VPC. Si el tráfico saliente en la VPC excede el ancho de banda, se producirá una congestión de la red, no se podrá acceder a algunas subredes o incluso se interrumpirá la conexión de VPN debido al tiempo de espera de detección de VPN.

En este caso, se recomienda aumentar el ancho de banda del gateway de VPN.

NOTA

El ancho de banda máximo de una VPN es de 1000 Mbit/s.

14.5 ¿Por qué el cambio de ancho de banda de VPN no tiene efecto?

Hay un retraso para que el cambio de ancho de banda de VPN surta efecto.

Pruebe el ancho de banda 5 minutos después de cambiar el ancho de banda.

NOTA

El cambio del ancho de banda de VPN no interrumpirá los servicios en las redes.

14.6 ¿Cuáles son las diferencias entre el ancho de banda de una conexión de VPN y el de una conexión de Direct Connect?

Conceptos

- El ancho de banda de una conexión de Direct Connect es el ancho de banda de la conexión física creada por un usuario.
- El ancho de banda de una conexión de VPN se aplica a la dirección de salida de Huawei Cloud.

Ancho de banda máximo

- De forma predeterminada, el ancho de banda máximo de una conexión de Direct Connect es de 1000 Mbit/s. Cuando crea una conexión en la consola de gestión y establece **Port Type** en **10GE single-mode optical port** el ancho de banda máximo es de 10 Gbit/s.
- El ancho de banda máximo de una VPN es de 1000 Mbit/s.

Calidad de la red

- Un usuario de Direct Connect tiene una conexión dedicada con una alta calidad de red.
- Las conexiones de VPN comparten el ancho de banda de su gateway de VPN. Es decir, el ancho de banda total de las conexiones de VPN no puede exceder el ancho de banda del gateway de VPN correspondiente. La calidad de la red se verá afectada por la calidad de Internet.

14.7 ¿Cómo puedo determinar el ancho de banda de mi VPN?

Tenga en cuenta lo siguiente cuando determine el ancho de banda:

- Cantidad de datos transmitidos a través de un túnel de VPN en un período de tiempo (Reserve suficiente ancho de banda para evitar la congestión del enlace.)
- Ancho de banda de salida en los dos extremos de una conexión de VPN: El ancho de banda de salida en el lado de la nube debe ser menor que en el lado local.

15 Cuotas

15.1 ¿Qué cuotas tiene una VPN?

¿Qué es una cuota?

Las cuotas pueden limitar el número o la cantidad de recursos disponibles para los usuarios, como el número máximo de ECS o discos de EVS que se pueden crear.

Si la cuota de recursos existente no puede cumplir con los requisitos de servicio, puede solicitar una cuota más alta.

Tipos de recursos

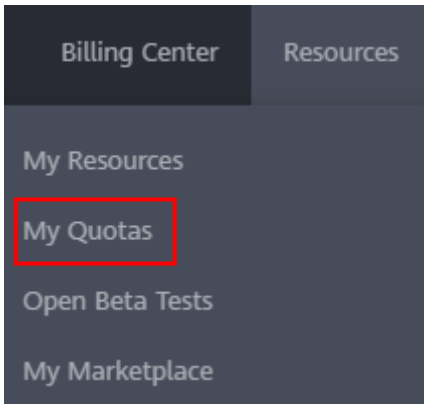
Los recursos de VPN incluyen gateways de VPN, conexiones de VPN y gateways de clientes. La cuota total de cada tipo de recurso varía según las regiones.

¿Cómo puedo ver mis cuotas?

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Elija **Resources** > **My Quotas** en la esquina superior derecha de la página.

   Se muestra la página **Service Quota**.

Figura 15-1 Mis cuotas

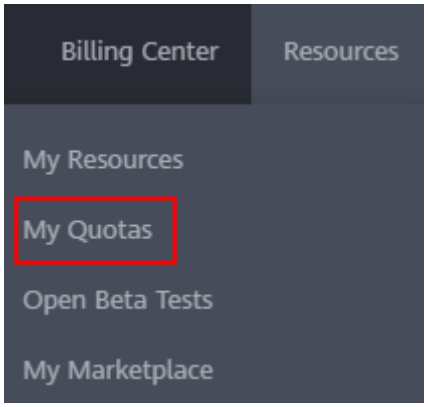


4. Vea la cuota usada y total de cada tipo de recursos en la página mostrada.
   Si una cuota no puede cumplir con los requisitos de servicio, solicite una cuota más alta.

¿Cómo solicito una cuota más alta?

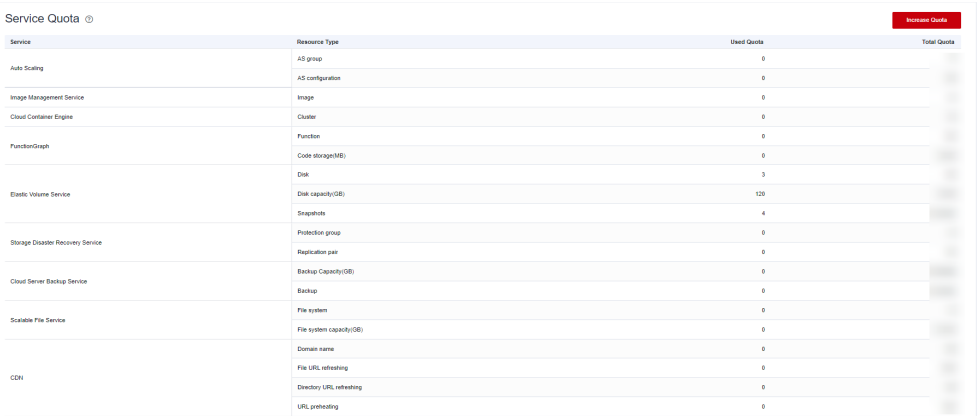
1. Inicie sesión en la consola de gestión.
2. Elija **Resources** > **My Quotas** en la esquina superior derecha de la página.
   Se muestra la página **Service Quota**.

Figura 15-2 Mis cuotas



3. Haga clic en **Increase Quota** en la esquina superior derecha de la página.

Figura 15-3 Solicitud de una cuota más alta



4. En la página **Create Service Ticket**, configure los parámetros según sea necesario.

   En el área **Problem Description**, introduzca la cuota requerida y el motivo del ajuste de cuota.

5. Seleccione el acuerdo y haga clic en **Submit**.

15.2 ¿Cuántos gateways y conexiones VPN puedo crear por defecto?

De forma predeterminada, cada usuario puede crear un máximo de 50 gateways de VPN y 100 gateways de cliente. Cada gateway de VPN puede tener un máximo de 100 grupos de conexión. Cuando dos EIP de un gateway de VPN están conectados a la misma dirección IP pública de un gateway de cliente, se utiliza un grupo de conexión de VPN. Cuando dos EIP de una gateway de VPN se conectan a dos gateway de cliente o a dos direcciones IP públicas del mismo gateway de cliente, se utilizan dos grupos de conexión de VPN.

Antes de comprar los gateway de VPN, compruebe su cuota disponible. Si la cuota es insuficiente, envíe **un ticket de servicio** para aumentar la cuota.

15.3 ¿Cómo cambio mi gateway de VPN y las cuotas de conexión?

1. Inicie sesión en la consola de gestión y seleccione **Service Tickets** > **Create Service Ticket** en la barra de menús.
2. En la página **Create Service Ticket**, haga clic en **Quotas** en el área **Services**.
3. Haga clic en **Quota Application** en **Issue Categories**.
4. Haga clic en **Create Now**.

   Ingrese la información requerida y haga clic en **Submit**.

15.4 ¿Cuántas VPN IPsec puedo tener?

De forma predeterminada, cada usuario puede crear un máximo de 50 gateways de VPN y 100 gateways de cliente. Cada gateway de VPN puede tener un máximo de 100 grupos de conexión. Cuando dos EIP de un gateway de VPN están conectados a la misma dirección IP pública de un gateway de cliente, se utiliza un grupo de conexión de VPN. Cuando dos EIP de una gateway de VPN se conectan a dos gateway de cliente o a dos direcciones IP públicas del mismo gateway de cliente, se utilizan dos grupos de conexión de VPN.

Antes de comprar los gateway de VPN, compruebe su cuota disponible. Si la cuota es insuficiente, envíe **un ticket de servicio** para aumentar la cuota.

16 Permisos de la cuenta

16.1 ¿Se requiere un nombre de usuario y contraseña para crear una conexión de VPN IPsec?

No. Huawei Cloud IPsec VPN utiliza una clave precompartida (PSK) para la autenticación. El PSK se configura en un gateway de VPN y se establecerá una conexión después de que se complete la negociación de VPN. Por lo tanto, no se requiere ningún nombre de usuario o contraseña para crear una conexión de VPN IPsec. En general, las VPN SSL, PPTP y L2TP usan nombres de usuario y contraseñas para la autenticación.

NOTA

IPsec XAUTH proporciona autenticación extendida para IPsec VPN. Requiere que los usuarios introduzcan sus nombres de usuario y contraseñas durante la negociación de VPN.

Huawei Cloud VPN no es compatible con IPsec XAUTH.

16.2 ¿Qué debo hacer si el sistema muestra un mensaje que indica que no tengo los permisos para crear una VPN?

- Compruebe si su cuenta es una cuenta IAM.
- Asegúrese de que su cuenta de IAM tiene los permisos **VPC Administrator**, **Tenant Guest** y **VPN Administrator**.

  Si su cuenta de IAM no tiene operaciones de operación de VPC, inicie sesión en la consola de IAM con una cuenta de Huawei Cloud y conceda los permisos a su cuenta de IAM. Para obtener más información, consulte **Crear un grupo de usuarios y asignar permisos** y **Agregar usuarios a o quitar usuarios de un grupo de usuarios**.

16.3 ¿Cómo puedo determinar que mi cuenta no puede crear una VPN debido a permisos insuficientes?

- Los gateway de VPN y las conexiones creadas por una cuenta de Huawei Cloud son invisibles para las cuentas de usuario de IAM.

- Se mostrará un mensaje indicando que el sistema está ocupado si crea un gateway o conexión de VPN con una cuenta de usuario IAM.

Para obtener más información sobre los permisos necesarios para crear una conexión de VPN, consulte **¿Qué debo hacer si el sistema muestra un mensaje que indica que no tengo los permisos para crear una VPN?**.

17 VPN clásico

17.1 Preguntas generales

17.1.1 ¿Qué dispositivos se pueden conectar a Huawei Cloud por una VPN?

Huawei Cloud VPN admite el protocolo IPsec estándar. Un dispositivo de su centro de datos local puede conectarse a Huawei Cloud si el dispositivo cumple los siguientes requisitos:

1. Soporta la VPN sobre IPsec.
2. Tiene una dirección IP pública fija, que se puede configurar estáticamente, o traducir con NAT en escenarios transversales de NAT (su dispositivo se despliega detrás de un gateway NAT).

La mayoría de los dispositivos son routers y firewalls. Para obtener más información sobre la configuración de la interconexión, consulte la **Guía del administrador**.

NOTA

- Los routers de banda ancha domésticos comunes, los hosts de Windows que proporcionan servicios VPN (como L2TP) y los terminales móviles personales no pueden conectarse a Huawei Cloud con una VPN.
- Los dispositivos que pueden interconectarse con el servicio Huawei Cloud VPN suelen ser de los siguientes:
  - Proveedores como Huawei (routers y firewalls), H3C (routers y firewalls), Cisco (routers y firewalls), Ruijie (routers y firewalls), ZTE, Sangfor, Fortinet, 360, Topsec, Hillstone, NetentSec, NSFOCUS, DELL, ZyXEL y Juniper
  - Proveedores de servicios en la nube como Alibaba Cloud, Tencent Cloud y Amazon Web Services
  - Proveedores de software como Openswan, strongSwan y TheGreenBow
- El protocolo IPsec es un protocolo de IETF estándar. Dispositivos compatibles con IPsec se pueden interconectar con Huawei Cloud.

  La mayoría de los routers y firewalls de clase empresarial admiten el protocolo de IPsec.
- Sin embargo, algunos dispositivos admiten IPsec de VPN solo después de comprar las licencias de software requeridas.

  Póngase en contacto con el administrador del centro de datos local para confirmar el modelo de dispositivo con el proveedor.

17.1.2 ¿Qué son los parámetros de negociación de VPN? ¿Cuáles son sus valores predeterminados?

Tabla 17-1 Parámetros de negociación de VPN

Política	Parámetro	Valor
IKE	Authentication Algorithm	• MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) • SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) • SHA2-256 (valor predeterminado) • SHA2-384 • SHA2-512
	Encryption Algorithm	• 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) • AES-256 • AES-192 • AES-128 (valor predeterminado)

Política	Parámetro	Valor
	DH Algorithm	● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 14 (valor predeterminado) ● Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 15 ● Grupo 16 ● Grupo 19 ● Grupo 20 ● Grupo 21 **NOTA** En algunas regiones, solo **Group 14**, **Group 2** y **Group 5** están disponibles.
	Version	● v1 (no recomendado debido a riesgos de seguridad) ● v2 (valor predeterminado)
	Lifecycle (s)	**86400** (predeterminado) Unidad: segundo Rango de valores: de **60** a **604800**
IPsec	Authentication Algorithm	● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.)

Política	Parámetro	Valor
	PFS	● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 14 (valor predeterminado) ● DH grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 15 ● DH grupo 16 ● DH grupo 19 ● DH grupo 20 ● DH grupo 21 ● Deshabilitar **NOTA** En algunas regiones, solo **DH group 14**, **DH group 2** y **DH group 5** están disponibles.
	Transfer Protocol	● ESP (valor predeterminado) ● AH ● AH-ESP
	Lifecycle (s)	**3600** (predeterminado) Unidad: segundo Rango de valores: de **480** a **604800**

NOTA

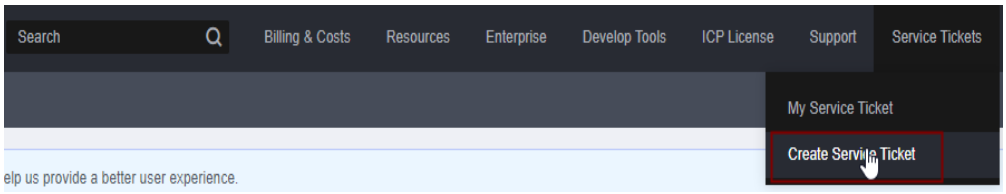
- Perfect Forward Secrecy (PFS) es una característica de seguridad.

  La negociación de IKE tiene dos fases, la fase 1 y la fase 2. La clave de la fase 2 (IPsec SA) se deriva de la clave generada en la fase 1. Una vez que se divulga la clave en la fase 1, la seguridad de la VPN IPsec puede verse afectada negativamente. Para mejorar la seguridad de la clave, IKE proporciona PFS. Después de configurar PFS, se realizará un intercambio de DH adicional durante la negociación de SA IPsec y se generará una nueva clave de SA IPsec, lo que mejorará la seguridad de SA IPsec.
- Para garantizar la seguridad, PFS está habilitado en Huawei Cloud de forma predeterminada. Asegúrese de que PFS también esté habilitado en el gateway local. De lo contrario, la negociación no funcionará.
- Para habilitar PFS, asegúrese de que las configuraciones en ambos extremos de una VPN son las mismas.
- La vida útil basada en el tráfico de IPsec SA en Huawei Cloud VPN es de 1,843,200 KB y no se puede cambiar. Esta duración no afecta al establecimiento de una SA IPsec.

17.1.3 ¿Cuáles son las categorías de los tickets de servicio de VPN? ¿Cómo puedo crear un ticket de servicio de VPN?

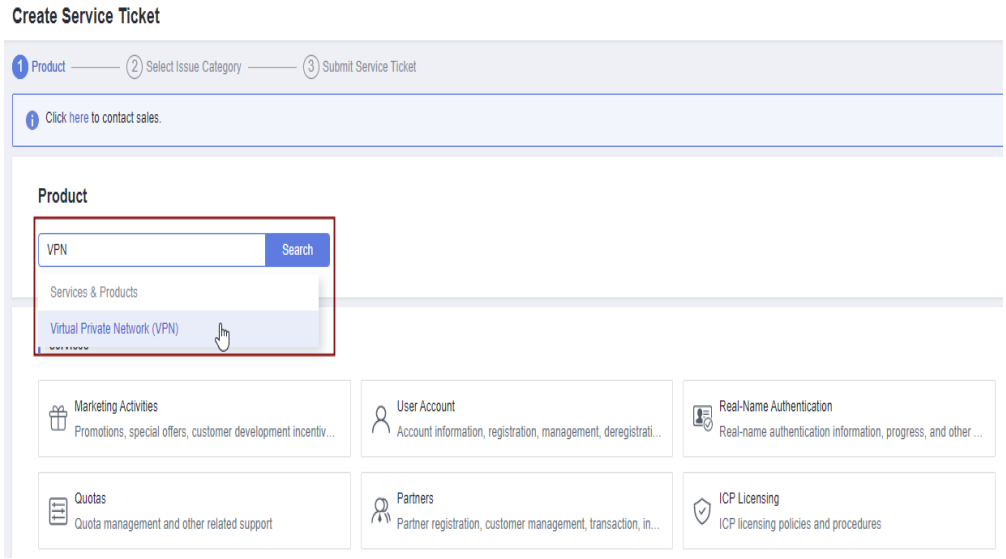
1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la consola de gestión, seleccione **Service Tickets** > **Create Service Ticket**.

Figura 17-1 Crear ticket de servicio



3. Busque **VPN** y seleccione **Virtual Private Network (VPN)**.

Figura 17-2 Selección de **Virtual Private Network (VPN)**



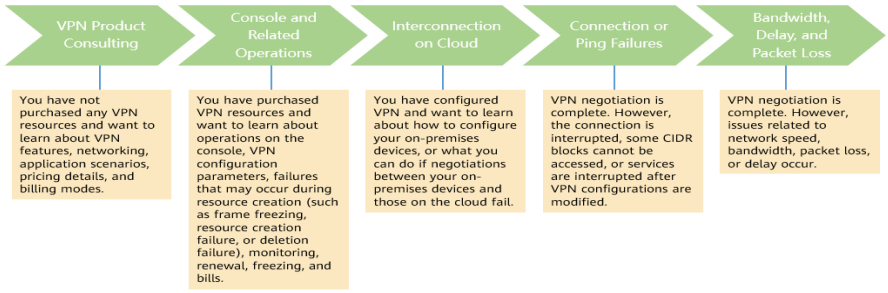
4. Seleccione una categoría de error.

Figura 17-3 Seleccionar categoría de problema

NOTA

Cuando **envía un ticket de servicio**, seleccione una categoría de problema para facilitar la gestión del problema.

Figura 17-4 Categoría de emisión y base de clasificación



17.1.4 ¿Puedo desplegar aplicaciones en la nube, bases de datos en un centro de datos local y luego conectarlas por una VPN?

VPN conecta una VPC y una red local.

Después de configurar correctamente la VPN, la VPC y la red local pueden comunicarse entre sí. En este caso, el servidor de aplicaciones que accede a la base de datos es exactamente lo mismo que acceder a otros servidores en la misma LAN.

Los servidores en la nube y los servidores locales pueden comunicarse entre sí.

AVISO

- Después de configurar una VPN, compruebe si la latencia de la red y la pérdida de paquetes afectan negativamente al funcionamiento del servicio.
- Se recomienda que ejecute el comando ping para comprobar la pérdida de paquetes y los detalles de latencia de red.

17.1.5 ¿Puedo visitar sitios web internacionales con una VPN?

No.

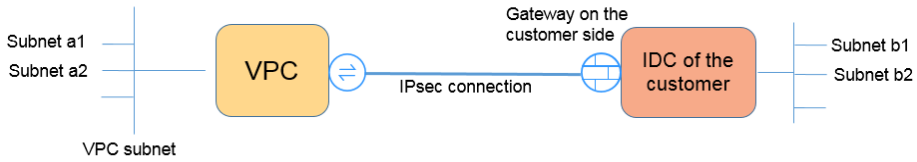
La VPN conecta una VPC y la red de un centro de datos local, es decir, una conexión sitio a sitio.

17.1.6 ¿Qué es una conexión de VPN? ¿Cómo configuro el número de conexiones de VPN al comprar un gateway de VPN?

Una conexión de VPN de Huawei Cloud es una conexión IPsec establecida entre un gateway de VPN en la nube y una dirección IP pública independiente de un centro de datos local. Puede configurar varias subredes locales (subredes VPC) y subredes remotas (subredes locales) para una conexión de VPN.

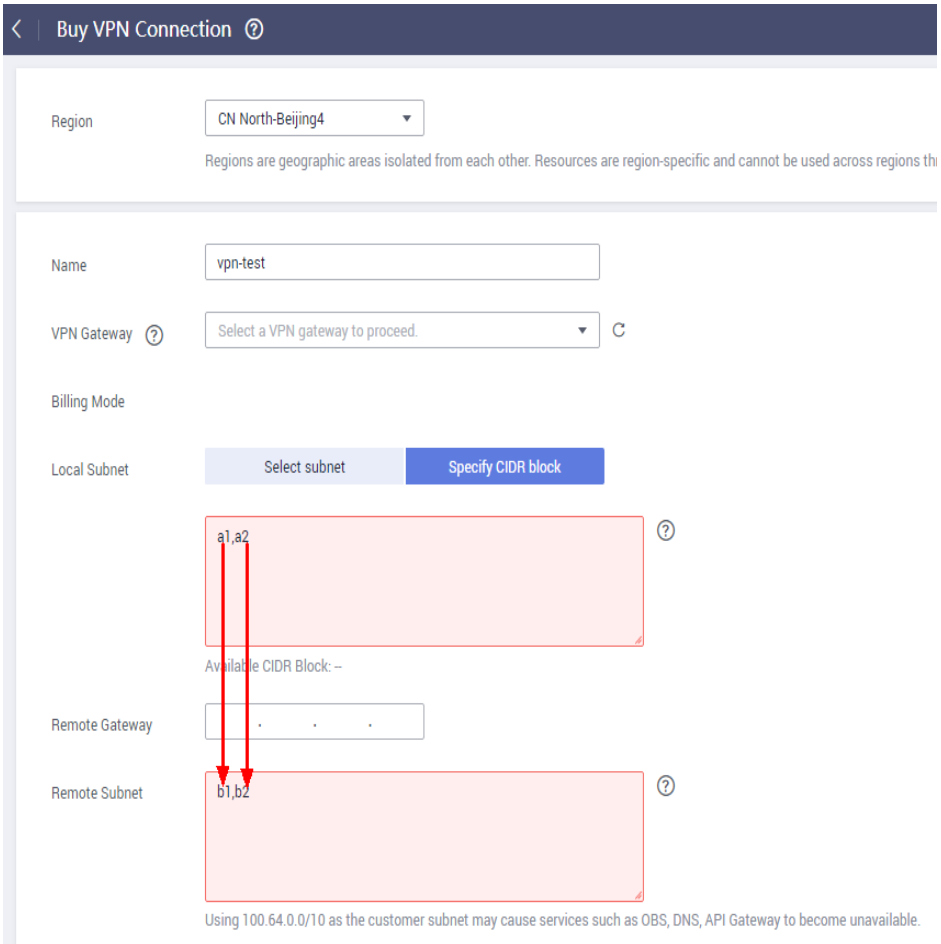
El número de conexiones de VPN que se van a crear viene determinado por el número de centros de datos locales. Cada conexión de VPN puede conectar una VPC a un solo centro de datos local.

Si elige comprar un gateway de VPN anual/mensual, establezca el número de conexiones de VPN en función del número de centros de datos locales que se conecten.



NOTA

En la figura anterior, si las subredes a1 y a2 en Huawei Cloud necesitan comunicarse con las subredes b1 y b2 en la red local, solo necesita crear una conexión de VPN, con los bloques CIDR de origen establecidos en a1 y a2 y los bloques CIDR de destino establecidos en b1 y b2. La siguiente figura muestra un ejemplo.

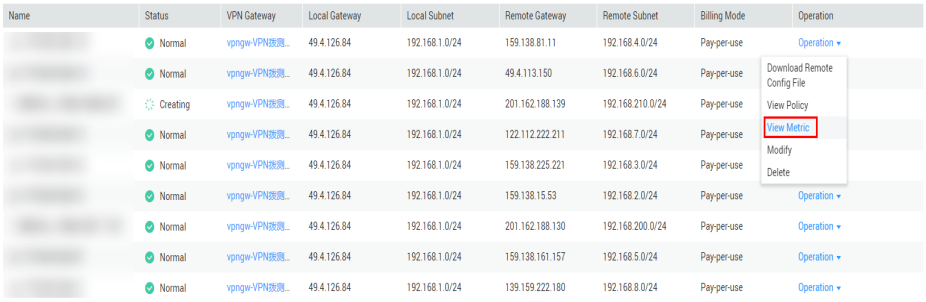


17.1.7 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía automáticamente notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Después de crear una conexión de VPN, puede localizar la fila que contiene la conexión de VPN y elegir **Operation** > **View Metric** para ver el estado de la conexión de VPN.

Figura 17-5 Ver métrica



17.1.8 ¿Se requiere un nombre de usuario y contraseña para crear una conexión de VPN IPsec?

No. Huawei Cloud IPsec VPN utiliza una clave precompartida (PSK) para la autenticación. La clave está configurada en un gateway de VPN. Se establecerá un túnel después de que se complete la negociación de VPN. Por lo tanto, no se requieren nombres de usuario y contraseñas.

En general, las VPN SSL, PPTP y L2TP usan nombres de usuario y contraseñas para la autenticación.

NOTA

IPsec XAUTH es una tecnología extendida de IPsec VPN. Indica a los usuarios que introduzcan sus nombres de usuario y contraseñas durante la negociación de VPN.

Huawei Cloud VPN no es compatible con IPsec XAUTH.

17.1.9 ¿Cuáles son las diferencias entre los escenarios de la aplicación y los modos de conexión de IPsec y SSL VPNs?

Escenarios

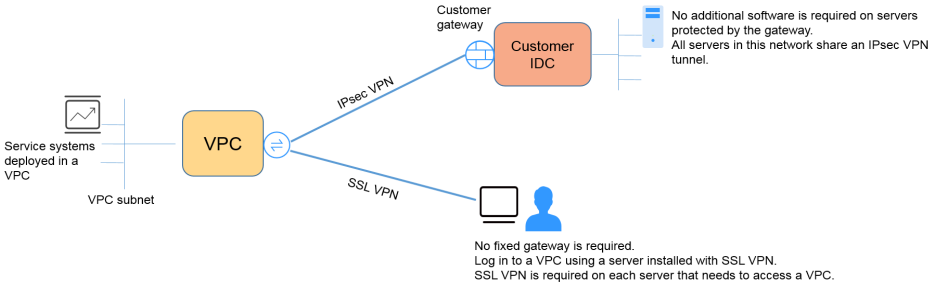
IPsec VPN conecta dos LAN, como una sucursal y su sede, o un centro de datos local y una VPC.

SSL VPN conecta un cliente a una LAN. Por ejemplo, el ordenador portátil de un empleado en un viaje de negocios accede a la red interna de la empresa.

Modos de conexión

IPsec VPN requiere gateway fijos, como firewalls o enrutadores, en ambos extremos. El administrador necesita configurar gateway en ambos extremos para completar la negociación de IPsec VPN.

SSL VPN necesita instalar un software cliente específico en el servidor, luego el servidor se conecta al dispositivo de SSL con el nombre de usuario y la contraseña.



NOTA

Huawei Cloud solo admite VPN IPsec.

17.1.10 ¿Se establecerá automáticamente una conexión de VPN IPsec?

Después de completar las configuraciones en ambos extremos de una conexión de VPN IPsec, la conexión de VPN no se establecerá automáticamente solo después de que los datos fluyan entre los dos extremos de la conexión. Si no hay flujo de datos entre la nube y el centro de datos local, la conexión de VPN siempre estará en el estado inactivo. Cualquier dato generado al acceder a servidores o hacer ping entre servidores puede desencadenar el establecimiento de una conexión de VPN.

El establecimiento de una conexión de VPN se puede activar en cualquiera de las dos condiciones siguientes: El gateway de VPN y el gateway remoto activan automáticamente la negociación. Los servidores en la nube y en las instalaciones se acceden entre sí a través de la conexión de VPN que se va a establecer.

Sin embargo, el establecimiento automático de una conexión de VPN no puede ser activado por un gateway de VPN en Huawei Cloud. Verifique que el establecimiento de su conexión de VPN pueda ser activado por los flujos de datos entre los dos extremos de la conexión de VPN. Es decir, compruebe si se puede establecer una conexión de VPN después de hacer ping a un servidor en la nube desde un servidor local, y si se puede establecer una conexión de VPN después de desconectar la conexión y hacer ping a un servidor local desde un servidor en la nube.

NOTA

Las direcciones de origen y destino de los paquetes de ping deben estar protegidas por la VPN.

Antes de establecer una conexión de VPN, las direcciones IP del gateway en ambos extremos se pueden hacer ping. Sin embargo, hacer ping a las direcciones IP del gateway no activa el establecimiento de la conexión de VPN.

17.1.11 ¿Qué me cobrarán por crear una VPN? ¿Se me cobrará por las direcciones IP de gateway de VPN?

Las VPN se facturan anualmente/mensualmente o de pago por uso. Debe pagar tanto por el ancho de banda del gateway de VPN o el precio del tráfico y el precio de la conexión de VPN.

Los gateway de VPN se pueden facturar por tráfico o ancho de banda.

- Un gateway de VPN anual/mensual solo se puede facturar por ancho de banda. El precio de un gateway de VPN anual/mensual incluye el precio de las conexiones de VPN que se pueden crear para el gateway y el precio del ancho de banda.
- El ciclo de facturación del modo de facturación de pago por uso es de una hora. Si elige un gateway de VPN de pago por uso, se debe comprar una conexión de VPN junto con el gateway de VPN. El precio incluye el ancho de banda del gateway de VPN o el precio del tráfico y el precio de la conexión de VPN creada junto con el gateway. Si crea otra conexión para el gateway, se le cobrará la conexión adicional.

  NOTA

  - La dirección IP del gateway de VPN no se facturará.
  - Un gateway de VPN no puede compartir un ancho de banda con una EIP vinculada a un ECS.

17.1.12 ¿Se puede retener una dirección IP de gateway de VPN después de que se elimine el gateway de VPN?

No. La dirección IP del gateway de VPN se liberará después de que se elimine el gateway de VPN.

Al eliminar un gateway de VPN también se eliminarán los recursos asociados con el gateway.

AVISO

La eliminación de la última conexión de un gateway de VPN de pago por uso también eliminará el gateway. Si desea conservar la dirección IP, no elimine la última conexión de VPN.

17.1.13 ¿Qué recursos de VPN se pueden monitorear?

VPN Gateway

La información de ancho de banda que se puede supervisar incluye el tráfico entrante, el ancho de banda entrante, el tráfico saliente, el ancho de banda saliente y el uso del ancho de banda saliente.

Para ver las métricas del gateway de VPN, localice el gateway de VPN de destino y haga clic en **View Metric** en la columna **Operation**.

VPN Connection

El estado de la conexión de VPN puede ser monitoreado.

El valor **1** indica que la conexión es normal.

El valor **0** indica que la conexión no está conectada.

Para ver el estado de la conexión de VPN, localice la conexión de VPN de destino y haga clic en **View Metric** en la columna **Operation**.

17.1.14 ¿Qué dirección del ancho de banda es limitado y cuál es la unidad del ancho de banda?

El ancho de banda del gateway de VPN comprado se utiliza en la dirección de salida. Para equilibrar el tráfico en las direcciones de entrada y salida, el ancho de banda en la dirección de entrada es limitado.

- Si el ancho de banda adquirido es de 10 Mbit/s o menos, el ancho de banda en la dirección de entrada está limitado a 10 Mbit/s.
- Si el ancho de banda adquirido es superior a 10 Mbit/s, el ancho de banda en la dirección de entrada es el mismo que el del ancho de banda adquirido.

La unidad de ancho de banda es Mbit/s y la del tráfico es GB.

17.1.15 ¿Cuál es la velocidad de red real de una conexión de VPN?

Se ha creado una conexión de VPN. Se han creado dos ECS con uno en el extremo local y el otro en el extremo remoto. Los dos ECS pueden hacer ping entre sí.

Realice los siguientes pasos para probar la velocidad de red de su gateway de VPN si el ancho de banda de su gateway de VPN es de 200 Mbit/s:

1. Si los ECS en los dos extremos de la VPN ejecutan Windows, use iPerf3 y FileZilla (una aplicación de FTP gratuita para cargar y descargar archivos) para probar la velocidad de la red.

   NOTA

   La prueba muestra que la velocidad media de red de la VPN es de 180 Mbit/s, y hay alrededor del 10% de desviación de velocidad de red. Los protocolos de TCP y de FTP tienen el mecanismo de control de congestión, y el protocolo de IPsec agrega un nuevo encabezado IP. Por lo tanto, aproximadamente un 10% de desviación de velocidad de red es normal para la red de VPN.

   Figura 17-6 muestra el resultado de la prueba.

   Figura 17-6 Resultado de la prueba para 200 Mbit/s de ancho de banda (cliente de iPerf3)

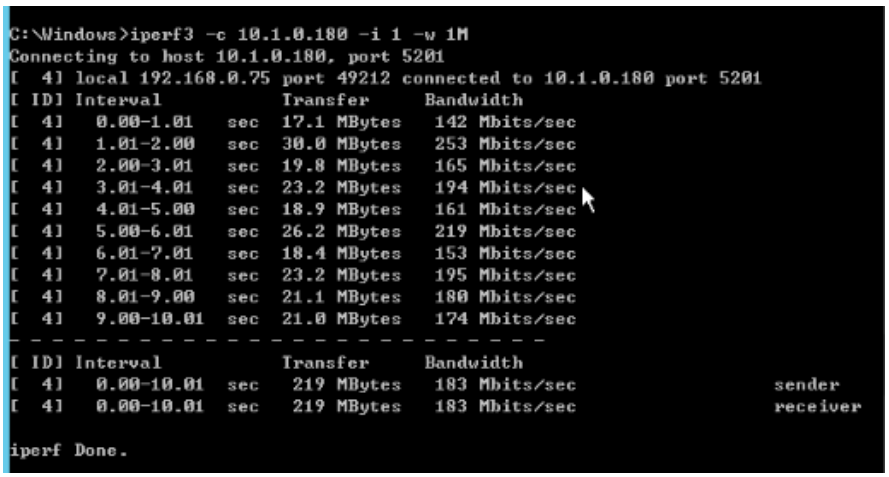
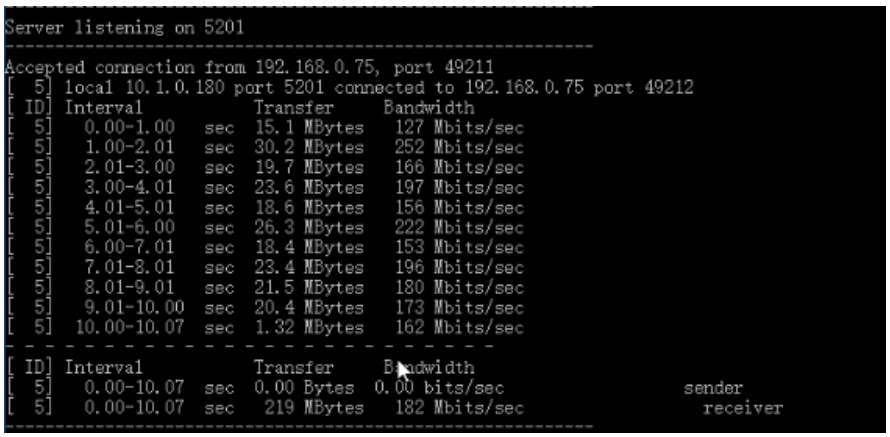
   

   Figura 17-7 muestra el resultado de la prueba.

Figura 17-7 Resultado de la prueba para un ancho de banda de 200 Mbit/s (servidor de iPerf3)

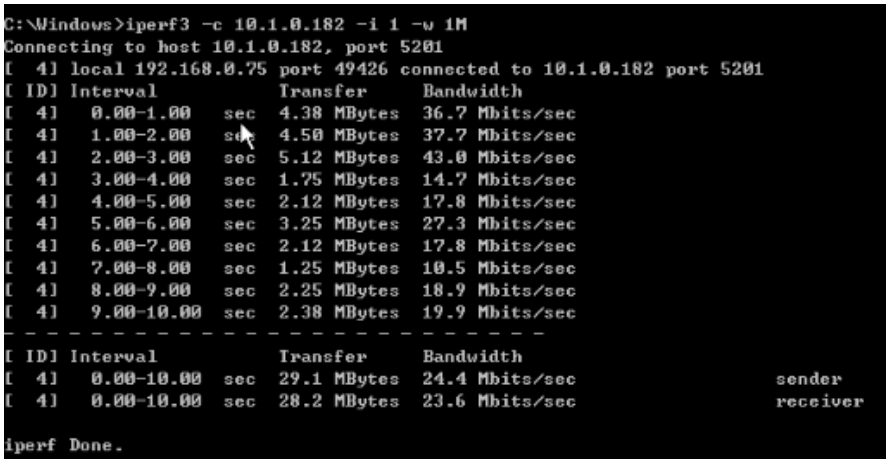


2. Si los ECS en los dos extremos de la VPN ejecutan CentOS 7, use iPerf3 para probar la velocidad de la red. La velocidad de la red puede alcanzar los 180 Mbit/s.
3. Si el ECS que funciona como el servidor ejecuta CentOS 7, y el ECS que funciona como el cliente ejecuta Windows, utilice iPerf3 y FileZilla para probar la velocidad de la red.

   La velocidad de red es de unos 20 Mbit/s, una velocidad de red lenta. Esto se debe a que las implementaciones TCP en Windows y en Linux son diferentes. Por lo tanto, si los ECS en los dos extremos de la VPN ejecutan diferentes sistemas operativos, la velocidad de red VPN no cumple con los requisitos de ancho de banda.

   Figura 17-8 muestra el resultado de la prueba.

Figura 17-8 Resultado de la prueba cuando los ECS en los dos extremos ejecutan diferentes sistemas operativos (iPerf3)



Realice los siguientes pasos para probar la velocidad de red de su gateway de VPN si el ancho de banda de su gateway de VPN es de 1,000 Mbit/s:

El ancho de banda del gateway de VPN es compartido por todas sus conexiones de VPN. Si el tamaño del ancho de banda es grande, se requieren múltiples ECS para probar el ancho de banda del gateway de VPN porque el rendimiento de reenvío de un ECS es limitado. Este escenario tiene altos requisitos en las especificaciones de ECS. Los ECS deben tener NIC que admitan el ancho de banda de 2 Gbit/s o superior.

Las pruebas muestran que la velocidad de red real de un gateway de VPN en Huawei Cloud está dentro del rango normal. Sin embargo, los servidores utilizados en ambos

extremos de la conexión de VPN deben ejecutar los sistemas operativos del mismo tipo y las NIC del servidor deben cumplir los requisitos de configuración.

17.1.16 ¿Puede una VPN facturada por tráfico usar un paquete de datos compartidos?

No.

El servicio VPN se factura de forma independiente y no puede usar paquetes de datos compartidos.

17.1.17 ¿Cuáles son las relaciones entre una VPC, un gateway de VPN y una conexión de VPN?

- Una VPC es una red privada en la nube. Se pueden crear múltiples VPC en la misma región mientras están aisladas entre sí. Una VPC se puede dividir en varias subredes.
- Se crea un gateway de VPN en una VPC y es el punto de acceso de una conexión de VPN. Una VPC en Huawei Cloud puede tener solo un gateway de VPN, mientras que un gateway de VPN puede tener múltiples conexiones de VPN.
- Se crea una conexión de VPN para un gateway de VPN y conecta una VPC a un centro de datos local (o una VPC en otra región).

  NOTA

  El número de conexiones de VPN es irrelevante para el número de subredes locales o el número de subredes remotas. Solo está relacionado con el número de centros de datos locales (o VPC en otras regiones) que se van a conectar a su VPC. Las conexiones de VPN creadas se muestran en la lista de conexiones de VPN. También puede ver el número de conexiones de VPN creadas para cada gateway de VPN.

17.1.18 ¿Qué es un gateway remoto y una subred remota en una conexión de VPN?

Al crear una conexión de VPN, una subred en Huawei Cloud VPC es la subred local y el gateway de VPN creada es el gateway local. La subred y el gateway conectadas en el centro de datos local es la subred remota y el gateway remoto.

Una dirección IP de gateway remota es una dirección IP pública.

17.1.19 ¿Cuántas conexiones de VPN necesito para conectarme a varios servidores locales?

Huawei Cloud IPsec VPN conecta una VPC en la nube y su centro de datos local. Por lo tanto, el número de conexiones de VPN es irrelevante para el número de servidores, pero para el número de centros de datos donde se encuentran los servidores.

En la mayoría de los casos, un centro de datos local tiene un gateway público. Todos los servidores se conectan a Internet con este gateway. Por lo tanto, solo necesita configurar una conexión de VPN para permitir las comunicaciones entre la VPC de Huawei Cloud y su centro de datos local.

17.1.20 ¿Una VPN permite comunicaciones entre dos VPC?

- Si las dos VPC se despliegan en la misma región, utilice una interconexión de VPC para conectarlas.
- Si las dos VPC se despliegan en diferentes regiones, utilice una conexión de VPN para conectarlas. A continuación, se detallan las operaciones:
  a. Cree un gateway de VPN para cada VPC y cree conexiones de VPN para los dos gateway de VPN.
  b. Establezca la dirección de gateway remota de cada conexión de VPN en la dirección IP de gateway del lado del otro extremo.
  c. Establezca las subredes remotas de cada conexión de VPN en las subredes de la VPC del mismo nivel.
  d. Las claves previamente compartidas y los parámetros de algoritmo de las dos conexiones de VPN deben ser los mismos.

17.1.21 ¿Cuáles son los impactos de una VPN en una red local? ¿Cuáles son los cambios en la ruta para acceder a un ECS?

Cuando configure una VPN, realice las siguientes operaciones en el gateway local:

1. Configure las políticas IKE e IPsec.
2. Especifique el tráfico interesante (reglas de ACL).
3. Compruebe la ruta del gateway local para asegurarse de que el tráfico destinado a la VPC de Huawei Cloud se enrute a la interfaz de salida correcta (la interfaz con la política de IPsec enlazada).

Una vez completada la configuración de VPN, solo el tráfico que coincide con las reglas de ACL entra en el túnel de VPN.

Por ejemplo, antes de crear una VPN, los usuarios locales acceden al ECS a través de la EIP vinculada al ECS. Después de crear la VPN, los flujos de datos que coinciden con las reglas de ACL acceden a la dirección IP privada del ECS a través del túnel de VPN.

17.1.22 ¿Puedo usar una red con dos salidas para establecer dos conexiones de VPN con la misma VPC?

No.

Cuando se crea una VPN en la nube, una subred local es una subred de VPC y una subred remota es una subred local. Si las dos conexiones usan la misma subred local y la misma subred remota, las conexiones de VPN fallarán.

17.1.23 ¿Cómo puedo evitar las desconexiones de VPN?

Las conexiones de VPN se renegocian cuando la vida útil de la SA IPsec está a punto de expirar o cuando los datos transmitidos con una conexión de VPN superan los 20 GB. Por lo general, la renegociación no interrumpe las conexiones de VPN.

La mayoría de las desconexiones se deben a configuraciones incorrectas en los dos extremos de la conexión de VPN o a fallos de renegociación debidos a excepciones de Internet.

Las causas comunes para las desconexiones son las siguientes:

- Las ACL de los dispositivos en ambos extremos de la conexión de VPN no coinciden.
- La configuración de la vida útil de SA en ambos extremos de la conexión de VPN es diferente.
- DPD no está configurado en su centro de datos local.
- La configuración se modifica cuando la conexión de VPN está en uso.
- Los paquetes están fragmentados porque el tamaño de los datos excede la MTU.
- La fluctuación se produce en la red del operador.

Por lo tanto, asegúrese de que las siguientes configuraciones de VPN son correctas para mantener las conexiones de VPN activas:

- Las subredes locales y remotas son pares coincidentes.
- La configuración de la duración de la SA en ambos extremos de la conexión de VPN es la misma.
- DPD está habilitado en el dispositivo del gateway local y el número de veces de detección es de 5 o más.
- Los parámetros se modifican en ambos extremos de la conexión de VPN durante el uso de la conexión de VPN.
- Establezca TCP MAX-MSS en 1300 para el dispositivo del gateway local.
- El ancho de banda del gateway local es lo suficientemente grande para ser utilizado por la conexión de VPN.
- La negociación de conexión de VPN se puede activar por ambos extremos y la negociación activa se ha habilitado en el gateway local.
- Hacer ping a las subredes en ambos extremos continuamente. El script es el siguiente:

```
#!/bin/sh
host=$1
if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi
log_name=$host".log"

while :; do
    result=`ping -W 1 -c 1 $host | grep 'bytes from '`
    if [ $? -gt 0 ]; then
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a
$log_name
    else
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo
$result | cut -d ':' -f 2`"| tee -a $log_name
    fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

NOTA

1. Utilice el editor vi para copiar el script anterior en el archivo **ping.sh**.
2. Ejecute el comando **chmod 777 ping.sh** para conceder permisos al archivo.
3. Ejecute el comando ping:

   ./ping.sh *x.x.x.x* **>>/dev/null &**

   x.x.x.x indica la dirección IP que se va a hacer ping.
4. Ejecute el siguiente comando:

   tail -f *x.x.x.x***.log**

   Puede ver el resultado de ping en tiempo real.

17.1.24 ¿Por qué se muestra Not Connected como el estado de una conexión de VPN creada correctamente?

Después de crear una conexión de VPN, su estado cambia a **Normal** solo después de que los servidores de ambos extremos de la conexión de VPN se comuniquen entre sí.

- IKE v1:

  Si no pasa tráfico con la conexión de VPN durante un período de tiempo, la conexión de VPN debe renegociarse. El tiempo de negociación depende del valor **Lifecycle (s)** en la política IPsec. Generalmente, **Lifecycle (s)** se establece en **3600** (1 hora), lo que indica que la negociación se iniciará en el minuto cincuenta y cuarto. Si la negociación es correcta, la conexión se mantiene hasta la siguiente ronda de negociación. Si la negociación falla, el estado de la conexión de VPN cambia a **Not Connected** en una hora. La conexión se puede restaurar solo después de que los dos extremos de la conexión de VPN se comuniquen entre sí. La desconexión se puede evitar usando una herramienta de monitorización de red, tal como IP SLA, para generar paquetes.
- IKE v2: si no pasa tráfico con la conexión de VPN durante un período de tiempo, la conexión de VPN permanece en el estado conectado.

17.1.25 ¿Qué puedo hacer si la configuración de la conexión de VPN falla?

1. Compruebe las políticas IKE e IPsec para ver si los modos de negociación y los algoritmos de encriptación en ambos extremos de la conexión de VPN son los mismos.
   a. Si la política IKE se ha configurado durante la fase uno y la política IPsec no se ha habilitado en la fase dos, las políticas IPsec en ambos extremos de la conexión de VPN pueden ser inconsistentes.
   b. Si utiliza un dispositivo físico de Cisco en su centro de datos local, se recomienda que utilice MD5 y establezca **Authentication Mode** en **MD5** al configurar la política IPsec para la conexión de VPN en la nube.
2. Compruebe si las reglas 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 para permitir la comunicación con las subredes de VPC. A continuación se proporciona un ejemplo de configuraciones de ACL:

   ```
   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
   ```
3. Compruebe si la conexión de VPN es normal haciendo ping al extremo local desde el extremo remoto y haciendo ping al extremo remoto desde el extremo local.

17.1.26 ¿Se puede usar una EIP como una dirección IP de gateway de VPN?

Sí para VPN, pero no para Classic VPN.

17.1.27 ¿Por qué la conexión de VPN siempre está en el estado no conectado incluso después de que se complete su configuración?

Asegúrese de que las claves previamente compartidas y la información de negociación en ambos extremos sean consistentes. Las subredes locales y el gateway de VPN en la nube son las subredes remotas y el gateway remoto en el centro de datos local. El gateway remotoy las subredes remotas en la nube son el gateway local y las subredes locales en el centro de datos local.

Asegúrese de que las rutas, NAT y las reglas de política de seguridad estén correctamente configuradas en su dispositivo de gateway local. A continuación, haga ping a los servidores en subredes en ambos extremos.

NOTA

La VPN se activa en función de los flujos de datos. Después de configurar VPN, haga ping a un dispositivo en la subred del par. Antes de ejecutar el comando ping, deshabilite la función de firewall en el dispositivo y permita paquetes ICMP entrantes en el grupo de seguridad en la nube.

Hacer ping a la dirección IP del gateway no puede activar la negociación de VPN. Hacer ping al servidor en la subred protegida por el gateway.

17.1.28 ¿Necesito configurar las reglas de ACL en la consola de gestión de Huawei Cloud después de configurar las reglas de ACL en el dispositivo de gateway local?

Necesita crear reglas de ACL dedicadas para su dispositivo de gateway local. Las políticas IPsec harán referencia a las reglas de ACL.

Cuando configura la VPN en la nube, las reglas de ACL se generarán automáticamente en función de las subredes locales y remotas introducidas en la consola de gestión y luego se entregarán al gateway de VPN.

(Huawei Cloud) El número de reglas de ACL = El número de subredes locales x El número de subredes remotas

17.2 Consulta sobre productos

17.2.1 ¿Cuáles son los escenarios típicos de IPsec VPN?

Una VPN es una conexión punto a punto que implementa el acceso a la red privada entre dos puntos.

- Casos de aplicación:
  - Cree una VPN entre diferentes regiones de Huawei Cloud para habilitar las comunicaciones de VPC entre regiones.
  - Cree una VPN entre Huawei Cloud y otra nube, por ejemplo, Alibaba Cloud.
  - Cree una VPN entre Huawei Cloud y su centro de datos local para permitir las comunicaciones entre una VPC de Huawei Cloud y una red local.
  - VPN HUB funciona junto con interconexiones de VPC y conexiones de Cloud Connect para permitir las comunicaciones entre un centro de datos local y varias VPC en la nube.

  - La VPN funciona con SNAT para acceder a direcciones IP específicas en las nubes.
- Escenarios no aplicables:
  - No utilice VPN para conectar VPCs en la misma región de Huawei Cloud. Se recomienda utilizar las interconexiones de VPC para habilitar las comunicaciones entre VPC en la misma región.
  - No establezca conexiones de VPN entre Huawei Cloud y su red doméstica que utiliza PPPoE dial-up.
  - No establezca las conexiones de VPN entre Huawei Cloud y routers (4G o 5G).
  - No establezca las conexiones de VPN entre Huawei Cloud y los terminales personales.

17.2.2 ¿Qué son una VPC, un gateway de VPN y una conexión de VPN?

VPC permite crear redes virtuales privadas y aisladas. Puede usar VPN para acceder de forma segura a ECS en VPC.

Un gateway VPN es un gateway de salida para una VPC. Con un gateway de VPN, puede crear una conexión segura, confiable y cifrada entre una VPC y un centro de datos local o entre dos VPC en diferentes regiones.

Una conexión de VPN es un túnel de comunicaciones cifrado IPsec seguro y confiable establecido entre un gateway de VPN y el gateway remoto en un centro de datos local.

Para crear una VPN en la nube, realice las siguientes operaciones:

1. Cree un gateway de VPN. Debe especificar la VPC que se va a conectar, así como el ancho de banda y las EIP del gateway de VPN.
2. Cree una conexión de VPN. Debe especificar la EIP de gateway utilizada para conectarse al gateway remoto, las subredes y las políticas de negociación.

17.2.3 ¿Cuáles son las relaciones entre una VPC, un gateway de VPN y una conexión de VPN?

- Una VPC es una red privada en la nube. Se pueden crear múltiples VPC en la misma región mientras están aisladas entre sí. Una VPC se puede dividir en varias subredes.
- Se crea un gateway de VPN en una VPC y es el punto de acceso de una conexión de VPN. Una VPC en Huawei Cloud puede tener solo un gateway de VPN, mientras que un gateway de VPN puede tener múltiples conexiones de VPN.
- Se crea una conexión de VPN para un gateway de VPN y conecta una VPC a un centro de datos local (o una VPC en otra región).

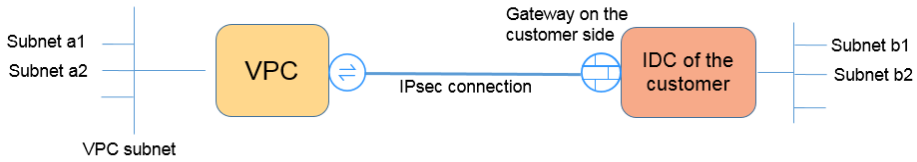
  NOTA

  El número de conexiones de VPN es irrelevante para el número de subredes locales o el número de subredes remotas. Solo está relacionado con el número de centros de datos locales (o VPC en otras regiones) que se van a conectar a su VPC. Las conexiones de VPN creadas se muestran en la lista de conexiones de VPN. También puede ver el número de conexiones de VPN creadas para cada gateway de VPN.

17.2.4 ¿Qué es una conexión de VPN? ¿Cómo configuro el número de conexiones de VPN al comprar un gateway de VPN?

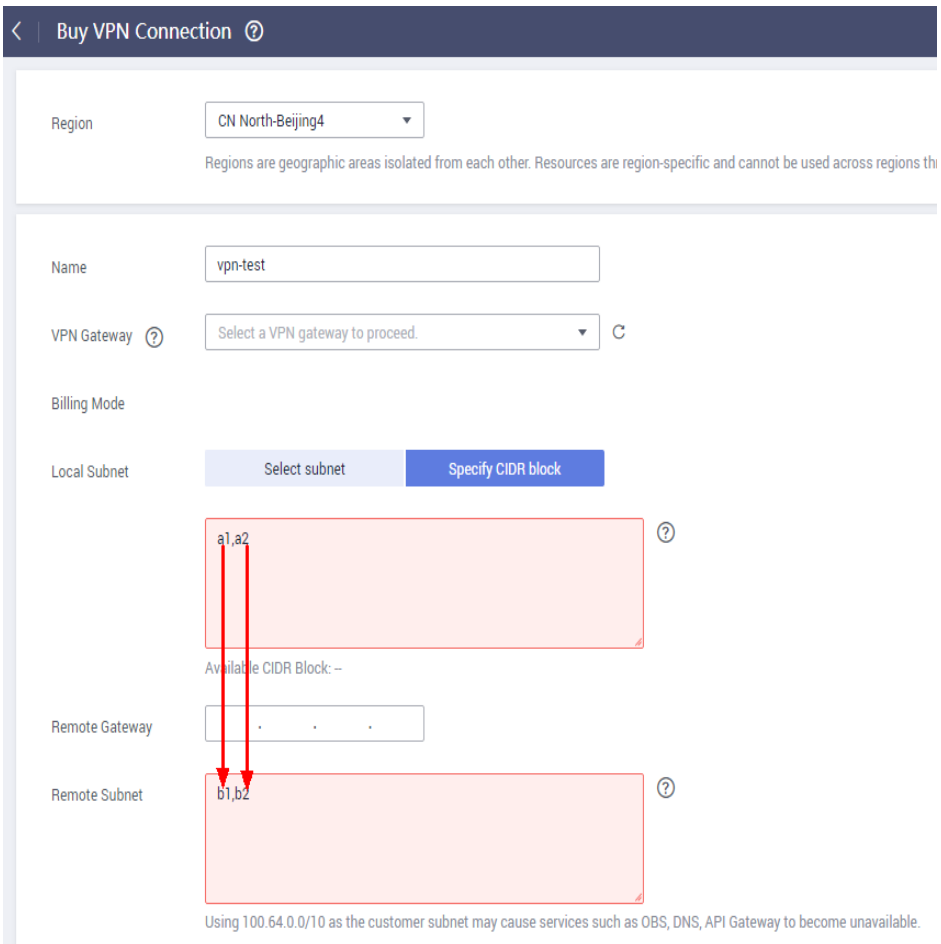
Una conexión de VPN de Huawei Cloud es una conexión IPsec establecida entre un gateway de VPN en la nube y una dirección IP pública independiente de un centro de datos local. Puede configurar varias subredes locales (subredes VPC) y subredes remotas (subredes locales) para una conexión de VPN.

El número de conexiones de VPN que se van a crear viene determinado por el número de centros de datos locales. Cada conexión de VPN puede conectar una VPC a un solo centro de datos local.



NOTA

En la figura anterior, si las subredes a1 y a2 en Huawei Cloud necesitan comunicarse con las subredes b1 y b2 en la red local, solo necesita crear una conexión de VPN, con los bloques CIDR de origen establecidos en a1 y a2 y los bloques CIDR de destino establecidos en b1 y b2. La siguiente figura muestra un ejemplo.



17.2.5 ¿Qué es un gateway remoto y una subred remota en una conexión de VPN?

Al crear una conexión de VPN, una subred en Huawei Cloud VPC es la subred local y el gateway de VPN creada es el gateway local. La subred y el gateway conectadas en el centro de datos local es la subred remota y el gateway remoto.

Una dirección IP de gateway remota es una dirección IP pública.

17.2.6 ¿Cómo planifico el bloque CIDR de una VPC a la que se accede por una conexión de VPN?

- El bloque CIDR de VPC no puede entrar en conflicto con el bloque CIDR local.
- Para evitar conflictos con 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.

17.2.7 ¿Se establecerá automáticamente una conexión de VPN IPsec?

Después de completar las configuraciones en ambos extremos de una conexión de VPN IPsec, la conexión de VPN no se establecerá automáticamente solo después de que los datos fluyan entre los dos extremos de la conexión. Si no hay flujo de datos entre la nube y el centro de datos local, la conexión de VPN siempre estará en el estado inactivo. Cualquier dato generado al acceder a servidores o hacer ping entre servidores puede desencadenar el establecimiento de una conexión de VPN.

El establecimiento de una conexión de VPN se puede activar en cualquiera de las dos condiciones siguientes: El gateway de VPN y el gateway remoto activan automáticamente la negociación. Los servidores en la nube y en las instalaciones se acceden entre sí a través de la conexión de VPN que se va a establecer.

Sin embargo, el establecimiento automático de una conexión de VPN no puede ser activado por un gateway de VPN en Huawei Cloud. Verifique que el establecimiento de su conexión de VPN pueda ser activado por los flujos de datos entre los dos extremos de la conexión de VPN. Es decir, compruebe si se puede establecer una conexión de VPN después de hacer ping a un servidor en la nube desde un servidor local, y si se puede establecer una conexión de VPN después de desconectar la conexión y hacer ping a un servidor local desde un servidor en la nube.

NOTA

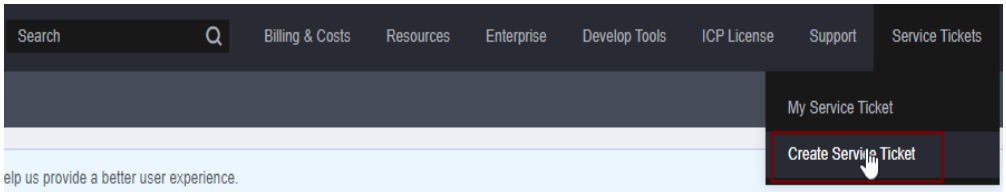
Las direcciones de origen y destino de los paquetes de ping deben estar protegidas por la VPN.

Antes de establecer una conexión de VPN, las direcciones IP del gateway en ambos extremos se pueden hacer ping. Sin embargo, hacer ping a las direcciones IP del gateway no activa el establecimiento de la conexión de VPN.

17.2.8 ¿Cuáles son las categorías de los tickets de servicio de VPN? ¿Cómo puedo crear un ticket de servicio de VPN?

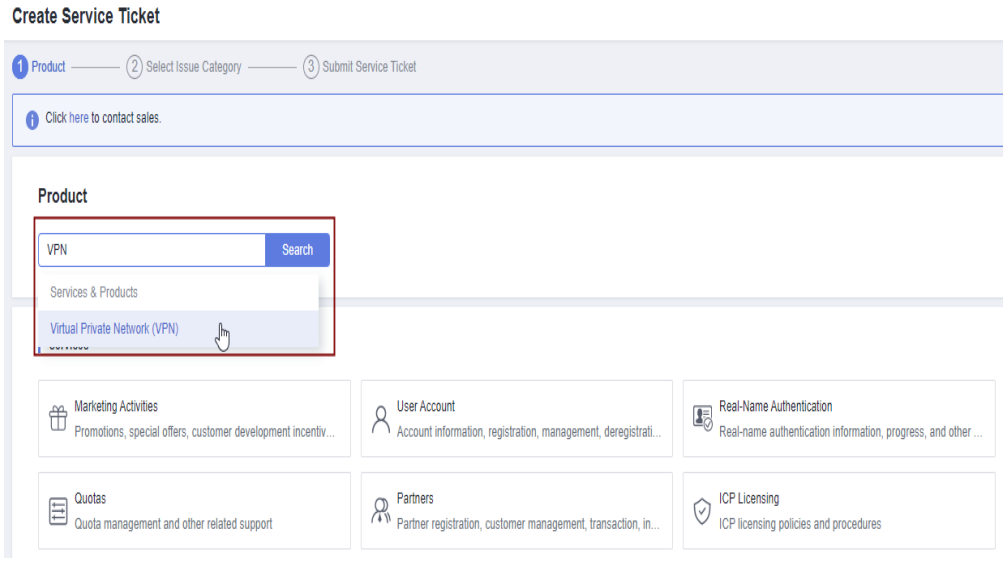
1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la consola de gestión, seleccione **Service Tickets** > **Create Service Ticket**.

Figura 17-9 Crear ticket de servicio



3. Busque **VPN** y seleccione **Virtual Private Network (VPN)**.

Figura 17-10 Selección de **Virtual Private Network (VPN)**



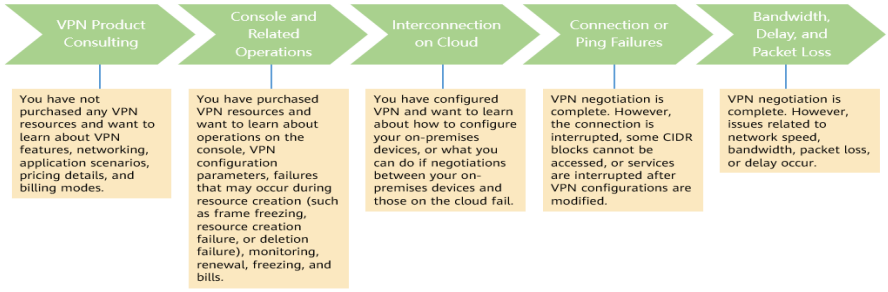
4. Seleccione una categoría de error.

Figura 17-11 Seleccionar categoría de problema

NOTA

Cuando **envía un ticket de servicio**, seleccione una categoría de problema para facilitar la gestión del problema.

Figura 17-12 Categoría de emisión y base de clasificación



17.2.9 ¿Qué son los parámetros de negociación de VPN? ¿Cuáles son sus valores predeterminados?

Tabla 17-2 Parámetros de negociación de VPN

Política	Parámetro	Valor
IKE	Authentication Algorithm	● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● AES-256 ● AES-192 ● AES-128 (valor predeterminado)

Política	Parámetro	Valor
	DH Algorithm	● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 14 (valor predeterminado) ● Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 15 ● Grupo 16 ● Grupo 19 ● Grupo 20 ● Grupo 21 **NOTA** En algunas regiones, solo **Group 14**, **Group 2** y **Group 5** están disponibles.
	Version	● v1 (no recomendado debido a riesgos de seguridad) ● v2 (valor predeterminado)
	Lifecycle (s)	**86400** (predeterminado) Unidad: segundo Rango de valores: de **60** a **604800**
IPsec	Authentication Algorithm	● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.)

Política	Parámetro	Valor
	PFS	● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 14 (valor predeterminado) ● DH grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 15 ● DH grupo 16 ● DH grupo 19 ● DH grupo 20 ● DH grupo 21 ● Deshabilitar **NOTA** En algunas regiones, solo **DH group 14**, **DH group 2** y **DH group 5** están disponibles.
	Transfer Protocol	● ESP (valor predeterminado) ● AH ● AH-ESP
	Lifecycle (s)	**3600** (predeterminado) Unidad: segundo Rango de valores: de **480** a **604800**

NOTA

- Perfect Forward Secrecy (PFS) es una característica de seguridad.

  La negociación de IKE tiene dos fases, la fase 1 y la fase 2. La clave de la fase 2 (IPsec SA) se deriva de la clave generada en la fase 1. Una vez que se divulga la clave en la fase 1, la seguridad de la VPN IPsec puede verse afectada negativamente. Para mejorar la seguridad de la clave, IKE proporciona PFS. Después de configurar PFS, se realizará un intercambio de DH adicional durante la negociación de SA IPsec y se generará una nueva clave de SA IPsec, lo que mejorará la seguridad de SA IPsec.
- Para garantizar la seguridad, PFS está habilitado en Huawei Cloud de forma predeterminada. Asegúrese de que PFS también esté habilitado en el gateway local. De lo contrario, la negociación no funcionará.
- Para habilitar PFS, asegúrese de que las configuraciones en ambos extremos de una VPN son las mismas.
- La vida útil basada en el tráfico de IPsec SA en Huawei Cloud VPN es de 1,843,200 KB y no se puede cambiar. Esta duración no afecta al establecimiento de una SA IPsec.

17.2.10 ¿Qué dispositivos se pueden conectar a Huawei Cloud por una VPN?

Huawei Cloud VPN admite el protocolo IPsec estándar. Un dispositivo de su centro de datos local puede conectarse a Huawei Cloud si el dispositivo cumple los siguientes requisitos:

1. Soporta la VPN sobre IPsec.
2. Tiene una dirección IP pública fija, que se puede configurar estáticamente, o traducir con NAT en escenarios transversales de NAT (su dispositivo se despliega detrás de un gateway NAT).

La mayoría de los dispositivos son routers y firewalls. Para obtener más información sobre la configuración de la interconexión, consulte la **Guía del administrador**.

NOTA

- Los routers de banda ancha domésticos comunes, los hosts de Windows que proporcionan servicios VPN (como L2TP) y los terminales móviles personales no pueden conectarse a Huawei Cloud con una VPN.
- Los siguientes productos pueden conectarse a Huawei Cloud con VPN:
  - Dispositivos: firewalls y enrutadores de acceso (AR) de Huawei, firewalls de Hillstone y firewalls de Check Point
  - Servicios en la nube: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) y Microsoft Azure
  - Software: strongSwan
- El protocolo IPsec es un protocolo de IETF estándar. Dispositivos compatibles con IPsec se pueden interconectar con Huawei Cloud.

  La mayoría de los routers y firewalls de clase empresarial admiten el protocolo de IPsec.
- Sin embargo, algunos dispositivos admiten IPsec de VPN solo después de comprar las licencias de software requeridas.

  Póngase en contacto con el administrador del centro de datos local para confirmar el modelo de dispositivo con el proveedor.

17.2.11 ¿Se requiere un nombre de usuario y contraseña para crear una conexión de VPN IPsec?

No. Huawei Cloud IPsec VPN utiliza una clave precompartida (PSK) para la autenticación. La clave está configurada en un gateway de VPN. Se establecerá un túnel después de que se complete la negociación de VPN. Por lo tanto, no se requieren nombres de usuario y contraseñas.

En general, las VPN SSL, PPTP y L2TP usan nombres de usuario y contraseñas para la autenticación.

NOTA

IPsec XAUTH es una tecnología extendida de IPsec VPN. Indica a los usuarios que introduzcan sus nombres de usuario y contraseñas durante la negociación de VPN.

Huawei Cloud VPN no es compatible con IPsec XAUTH.

17.2.12 ¿Cómo permito que servidores específicos accedan a una subred de VPC por una conexión de VPN creada?

Configuraciones en el centro de datos local

- Configurar reglas de denegación en dispositivos VPN.
- Configure las reglas de ACL en el router o switch.

Configuraciones en la nube

- Configurar reglas de grupo de seguridad para denegar el acceso desde direcciones IP específicas.
- Configurar reglas de ACL.

NOTA

Todas las reglas deben agregarse al dispositivo antes de que se establezca el túnel de VPN. No cambie la subred local y la subred remota para restringir el acceso.

17.2.13 ¿Qué recursos de VPN se pueden monitorear?

VPN Gateway

La información de ancho de banda que se puede supervisar incluye el tráfico entrante, el ancho de banda entrante, el tráfico saliente, el ancho de banda saliente y el uso del ancho de banda saliente.

Para ver las métricas del gateway de VPN, localice el gateway de VPN de destino y haga clic en **View Metric** en la columna **Operation**.

VPN Connection

El estado de la conexión de VPN puede ser monitoreado.

El valor **1** indica que la conexión es normal.

El valor **0** indica que la conexión no está conectada.

Para ver el estado de la conexión de VPN, localice la conexión de VPN de destino y haga clic en **View Metric** en la columna **Operation**.

17.2.14 ¿Se puede usar una EIP como una dirección IP de gateway de VPN?

No.

La dirección IP de un gateway de VPN tiene configuraciones preestablecidas y se asigna automáticamente cuando se crea el gateway de VPN. Una EIP no puede ser utilizada por un gateway de VPN.

17.2.15 ¿Necesito comprar las EIP para servidores que se comunican entre sí a través de una VPN?

Si su servidor local necesita acceder a un ECS en la nube con una VPN, no necesita comprar una EIP.

Si el ECS necesita proporcionar servicios accesibles desde Internet, se requiere una EIP.

17.2.16 ¿Se admiten las VPN SSL?

Las VPN SSL no son compatibles.

17.2.17 ¿Cuánto tiempo toma para que las configuraciones de VPN entregadas surtan efecto?

Las configuraciones de VPN tardan de 1 a 5 minutos en surtir efecto.

NOTA

Después de que las configuraciones de VPN entren en vigor, configure su gateway local para completar la negociación del túnel con el gateway de VPN en Huawei Cloud.

17.2.18 ¿Qué debo hacer si no puedo crear conexiones para un gateway de VPN que no tiene información de ancho de banda?

Si un gateway de VPN no tiene información de ancho de banda, la VPN es de la edición anterior. Este tipo de VPN ya no se puede crear en Huawei Cloud.

- Solo se puede crear una conexión de VPN para cada gateway de VPN de la edición anterior y su ancho de banda no está garantizado. Puede eliminar el gateway y crear una de las nuevas ediciones. Pero los servicios se verán afectados.
- También puede **enviar un ticket de servicio** para cambiar el gateway a una de la nueva edición y sus servicios no se verán afectados.

  De forma predeterminada, el ancho de banda de un gateway de VPN cambiada a la nueva edición es de 10 Mbit/s. Puede ajustar el ancho de banda según sea necesario. El ancho de banda de un gateway de VPN que se factura anualmente/mensualmente no se puede reducir.

17.2.19 ¿Huawei Cloud VPN admite direcciones de IPv6?

No.

Huawei Cloud VPN solo admite direcciones IPv4.

17.2.20 ¿Cómo puedo determinar el tamaño del ancho de banda de mi VPN?

Tenga en cuenta lo siguiente cuando determine el ancho de banda:

- Cantidad de datos transmitidos a través de un túnel de VPN en un período de tiempo (Reserve suficiente ancho de banda para evitar la congestión del enlace.)
- El ancho de banda de salida al final de la conexión de VPN en la nube debe ser menor que al final de la conexión de VPN en el centro de datos local.

17.2.21 ¿Una conexión de VPN es compatible con algoritmos de encriptación chinos?

No.

Utilice los algoritmos proporcionados en la consola de gestión de Huawei Cloud para la negociación. Asegúrese de que los algoritmos utilizados en ambos extremos sean los mismos.

17.2.22 ¿Qué versión de IKE debo seleccionar al crear una conexión de VPN?

Huawei Cloud recomienda IKEv2 para la negociación porque IKEv1 no es seguro. Además, IKEv2 funciona mejor que IKEv1 en términos de negociación y establecimiento de conexión, métodos de autenticación, tiempo de espera de DPD y tiempo de espera de SA.

Huawei Cloud no será compatible con IKEv1 pronto.

Introducción a IKEv1 e IKEv2

- La complejidad de IKEV1, un protocolo híbrido, trae inevitablemente algunos defectos de seguridad y rendimiento. Esto se ha convertido en el cuello de botella para el sistema IPsec actual.
- El protocolo IKEv2 reserva las funciones básicas de IKEv1 y supera algunos problemas traídos por IKEv1. Además, por simplicidad, eficiencia, seguridad y robustez, RFC 4306, un documento describe la versión 2 de IKE, combina el contenido de lo que eran documentos IKEv1 previamente separados. Al minimizar las funciones principales y los algoritmos de contraseña predeterminados, IKEv2 mejora en gran medida la capacidad de interoperación entre diferentes VPN IPsec.

Vulnerabilidades de seguridad de IKEv1

- Los algoritmos criptográficos soportados por IKEv1 no se han actualizado durante más de 10 años. Además, IKEv1 no admite algoritmos criptográficos fuertes como AES-GCM y ChaCha20-Poly1305. Para IKEv1, el bit E (Encryption) en la cabecera ISALMP especifica que las cargas útiles que siguen a la cabecera ISALMP están cifradas, pero cualquier verificación de integridad de datos de esas cargas útiles es manejada por una carga útil hash separada. Esta separación de la encriptación de la protección de la integridad de los datos impide el uso de encriptación autenticada (AES-GCM) con IKEv1.
- El protocolo IKEv1 es vulnerable a ataques de amplificación DoS. IKEv1 es vulnerable a conexiones semiabiertas.

  IKEv2 puede defenderse de ataques DoS.
- El modo agresivo IKEv1 no es lo suficientemente seguro. En modo agresivo, los paquetes de información no están cifrados. También hay ataques de fuerza bruta dirigidos al modo agresivo, como los ataque de intermediario.

Diferencias entre IKEv1 e IKEv2

- **Proceso de negociación**
  - La negociación IKEv1 SA consta de dos fases. IKEv1 es complejo y ocupa una gran cantidad de ancho de banda. La negociación IKEv1 fase 1 tiene como objetivo establecer la IKE SA. Este proceso soporta el modo principal y el modo agresivo. El modo principal utiliza seis mensajes ISAKMP para establecer el IKE SA, pero el modo agresivo utiliza solo tres. Por lo tanto, el modo agresivo es más rápido en el establecimiento de IKE SA. Sin embargo, el modo agresivo no proporciona protección de identidad de pares porque el intercambio de claves y la autenticación de identidad se realizan al mismo tiempo. La negociación de la fase 2 de IKEv1 tiene como objetivo establecer la SA IPsec para la transmisión de datos. Este proceso utiliza el modo de intercambio rápido (3 mensajes de ISAKMP) para completar la negociación.

- En comparación con IKEv1, IKEv2 simplifica el proceso de negociación de SA. IKEv2 utiliza dos intercambios (un total de 4 mensajes) para crear una SA IKE y un par de SA IPsec. Para crear varios pares de SA IPsec, solo se necesita un intercambio adicional para cada par adicional de SA.

  NOTA

  Para la negociación IKEv1, su modo principal requiere nueve (6+3) paquetes en total y su modo agresivo requiere 6 (3+3) paquetes. La negociación IKEv2 requiere solo 4 (2+2) paquetes.

- **Métodos de autenticación**
  - Solo IKEv1 (que requiere una tarjeta de encriptación) admite la autenticación de envolvente digital (HSS-DE).
  - IKEv2 admite la autenticación del Extensible Authentication Protocol (EAP). IKEv2 puede utilizar un servidor AAA para autenticar remotamente a los usuarios móviles y de PC y asignar direcciones IP privadas a estos usuarios. IKEv1 no proporciona esta función y debe usar L2TP para asignar direcciones IP privadas.
  - Solo IKEv2 admite algoritmos de integridad de IKE SA.
- **Timeout de DPD**
  - Solo IKEv1 admite el parámetro **retry-interval**. Si un dispositivo envía un paquete DPD pero no recibe respuesta dentro del intervalo de reintento especificado, el dispositivo registra un evento de fallo DPD. Cuando el número de eventos de error alcanza cinco, se eliminan tanto el SA IKE como el SA IPsec. La negociación IKE SA se iniciará de nuevo cuando el dispositivo tenga tráfico IPsec para manejar.
  - En el modo IKEv2, el intervalo de retransmisión aumenta de 1, 2, 4, 8, 16, 32 a 64 segundos. Si no se recibe ninguna respuesta dentro de ocho transmisiones consecutivas, el extremo par se considera muerto, y el SA IKE y el SA IPsec se eliminarán.
- **Procesamiento del tiempo de espera de IKE SA y del tiempo de espera de IPsec SA**

  En IKEv2, la vida útil suave de IKE SA es 9/10 de la vida útil dura de IKE SA más o menos un valor aleatorio para reducir la probabilidad de que dos extremos inicien la renegociación al mismo tiempo. Por lo tanto, la vida útil suave no requiere ajustes manuales en IKEv2.

Ventajas de IKEv2 sobre IKEv1

- Proceso de negociación de SA simplificado y mayor eficiencia de negociación.
- Se han cerrado muchas lagunas criptográficas, mejorando la seguridad.
- Admite la autenticación de EAP, lo que mejora la flexibilidad y la escalabilidad de la autenticación.
- EAP es un protocolo de autenticación que admite múltiples métodos de autenticación. La mayor ventaja de EAP es la escalabilidad. Es decir, se pueden agregar nuevos modos de autenticación sin cambiar el sistema de autenticación original. La autenticación EAP ha sido ampliamente utilizada en redes de acceso telefónico.
- IKEv2 emplea una carga útil cifrada que se basa en el diseño de ESP. La carga útil cifrada IKEv2 asocia la encriptación y la protección de la integridad de los datos de una manera que permite utilizar los algoritmos de encriptación autenticados. AES-GCM garantiza la confidencialidad, integridad y autenticación.

17.2.23 ¿Cuáles son los bits de los grupos DH utilizados por Huawei Cloud VPN?

Los grupos Diffie-Hellman (DH) determinan la fuerza de la clave utilizada en el proceso de intercambio de claves. Los números de grupo de DH más altos suelen ser más seguros, pero se requiere tiempo adicional para calcular la clave.

Tabla 17-3 enumera los bits correspondientes a los grupos DH usados por VPN.

Tabla 17-3 Bit correspondiente a cada grupo DH

Grupo DH	Módulo
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	ecp256 bits
20	ecp384 bits
21	ecp521 bits

NOTA

Los siguientes algoritmos de DH tienen riesgos de seguridad y no se recomiendan: DH grupo 1, DH grupo 2 y DH grupo 5.

17.2.24 ¿Puedo visitar sitios web internacionales con una VPN?

No.

La VPN conecta una VPC y la red de un centro de datos local, es decir, una conexión sitio a sitio.

17.2.25 ¿Puedo desplegar aplicaciones en la nube, bases de datos en un centro de datos local y luego conectarlas por una VPN?

VPN conecta una VPC y una red local.

Después de configurar correctamente la VPN, la VPC y la red local pueden comunicarse entre sí. En este caso, el servidor de aplicaciones que accede a la base de datos es exactamente lo mismo que acceder a otros servidores en la misma LAN.

Los servidores en la nube y los servidores locales pueden comunicarse entre sí.

AVISO

- Después de configurar una VPN, compruebe si la latencia de la red y la pérdida de paquetes afectan negativamente al funcionamiento del servicio.
- Se recomienda que ejecute el comando ping para comprobar la pérdida de paquetes y los detalles de latencia de red.

17.2.26 ¿Cuáles son las diferencias entre los escenarios de la aplicación y los modos de conexión de IPsec y SSL VPNs?

Escenarios

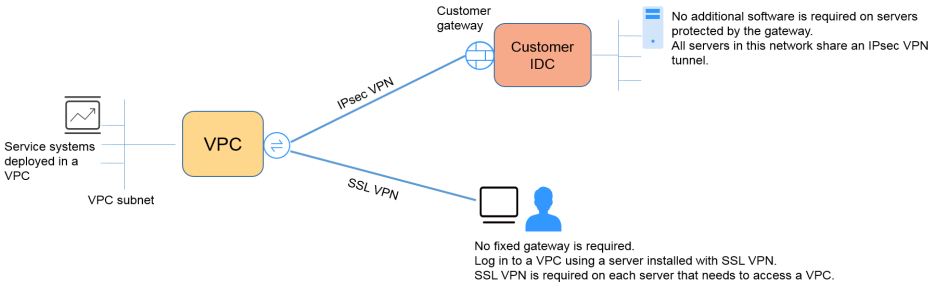
IPsec VPN conecta dos LAN, como una sucursal y su sede, o un centro de datos local y una VPC.

SSL VPN conecta un cliente a una LAN. Por ejemplo, el ordenador portátil de un empleado en un viaje de negocios accede a la red interna de la empresa.

Modos de conexión

IPsec VPN requiere gateway fijos, como firewalls o enrutadores, en ambos extremos. El administrador necesita configurar gateway en ambos extremos para completar la negociación de IPsec VPN.

SSL VPN necesita instalar un software cliente específico en el servidor, luego el servidor se conecta al dispositivo de SSL con el nombre de usuario y la contraseña.



NOTA

Huawei Cloud solo admite VPN IPsec.

17.2.27 ¿Qué me cobrarán por crear una VPN? ¿Se me cobrará por las direcciones IP de gateway de VPN?

Las VPN se facturan anualmente/mensualmente o de pago por uso. Debe pagar tanto por el ancho de banda del gateway de VPN o el precio del tráfico y el precio de la conexión de VPN.

Los gateway de VPN se pueden facturar por tráfico o ancho de banda.

1. Un gateway de VPN anual/mensual solo se puede facturar por ancho de banda. El precio de un gateway de VPN anual/mensual incluye el precio de las conexiones de VPN que se pueden crear para el gateway y el precio del ancho de banda.

2. El ciclo de facturación del modo de facturación de pago por uso es de una hora. Si elige un gateway de VPN de pago por uso, se debe comprar una conexión de VPN junto con el gateway de VPN. El precio incluye el ancho de banda del gateway de VPN o el precio del tráfico y el precio de la conexión de VPN creada junto con el gateway. Si crea otra conexión para el gateway, se le cobrará la conexión adicional.

   NOTA

   - La dirección IP del gateway de VPN no se facturará.
   - Un gateway de VPN no puede compartir un ancho de banda con una EIP vinculada a un ECS.

17.2.28 ¿Cuál es la diferencia entre la facturación de un gateway de VPN por ancho de banda y por tráfico?

Un gateway de VPN de pago por uso se puede facturar por ancho de banda o por tráfico.

Sus diferencias son las siguientes:

- Facturación por ancho de banda: El ciclo de facturación es de una hora. La tarifa generada depende del tamaño del ancho de banda.
- Facturado por tráfico: Se cobrarán las tarifas de tráfico generadas cada hora. La facturación se basa en el tráfico generado que sale de una VPC. El tamaño del ancho de banda no afecta al precio del tráfico público por GB.

17.2.29 ¿Puede una VPN facturada por tráfico usar un paquete de datos compartidos?

No.

El servicio VPN se factura de forma independiente y no puede usar paquetes de datos compartidos.

17.2.30 ¿Se puede retener una dirección IP de gateway de VPN después de que se elimine el gateway de VPN?

No. La dirección IP del gateway de VPN se liberará después de que se elimine el gateway de VPN.

Al eliminar un gateway de VPN también se eliminarán los recursos asociados con el gateway.

AVISO

La eliminación de la última conexión de un gateway de VPN de pago por uso también eliminará el gateway. Si desea conservar la dirección IP, no elimine la última conexión de VPN.

17.2.31 ¿Necesito comprar las EIP para servidores que se comunican entre sí a través de una VPN?

Si su servidor local necesita acceder a un ECS en la nube con una VPN, no necesita comprar una EIP.

Si el ECS necesita proporcionar servicios accesibles desde Internet, se requiere una EIP.

17.2.32 ¿Dónde puedo agregar rutas en la consola de VPN para llegar a las subredes remotas?

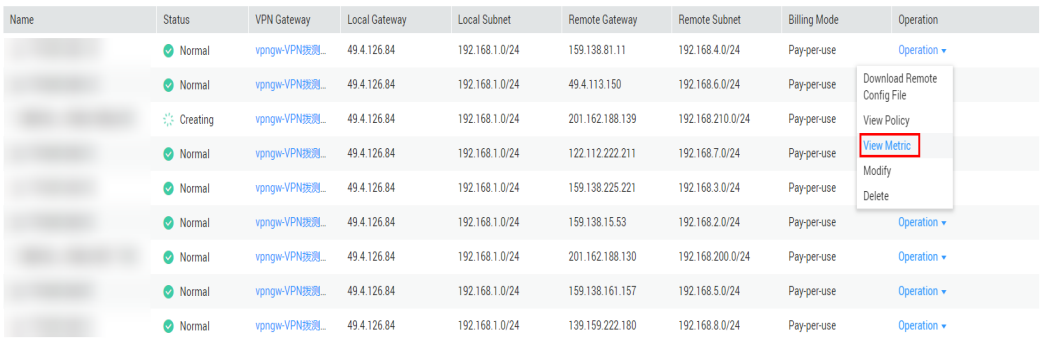
Cuando se crea una conexión de VPN, las rutas se entregan automáticamente para llegar a las subredes remotas.

17.2.33 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía automáticamente notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Después de crear una conexión de VPN, puede localizar la fila que contiene la conexión de VPN y elegir **Operation** > **View Metric** para ver el estado de la conexión de VPN.

Figura 17-13 Ver métrica



17.2.34 ¿Qué puedo hacer si la configuración de la conexión de VPN falla?

1. Compruebe las políticas IKE e IPsec para ver si los modos de negociación y los algoritmos de encriptación en ambos extremos de la conexión de VPN son los mismos.
   a. Si la política IKE se ha configurado durante la fase uno y la política IPsec no se ha habilitado en la fase dos, las políticas IPsec en ambos extremos de la conexión de VPN pueden ser inconsistentes.
   b. Si utiliza un dispositivo físico de Cisco en su centro de datos local, se recomienda que utilice MD5 y establezca **Authentication Mode** en **MD5** al configurar la política IPsec para la conexión de VPN en la nube.
2. Compruebe si las reglas 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 para permitir la comunicación con las subredes de VPC. A continuación se proporciona un ejemplo de configuraciones de ACL:

   ```
   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
```

3. Compruebe si la conexión de VPN es normal haciendo ping al extremo local desde el extremo remoto y haciendo ping al extremo remoto desde el extremo local.

17.2.35 ¿Qué dirección del ancho de banda es limitado y cuál es la unidad del ancho de banda?

El ancho de banda del gateway de VPN comprado se utiliza en la dirección de salida. Para equilibrar el tráfico en las direcciones de entrada y salida, el ancho de banda en la dirección de entrada es limitado.

- Si el ancho de banda adquirido es de 10 Mbit/s o menos, el ancho de banda en la dirección de entrada está limitado a 10 Mbit/s.
- Si el ancho de banda adquirido es superior a 10 Mbit/s, el ancho de banda en la dirección de entrada es el mismo que el del ancho de banda adquirido.

La unidad de ancho de banda es Mbit/s y la del tráfico es GB.

17.3 Escenarios de redes y aplicaciones

17.3.1 ¿Puedo visitar sitios web internacionales con una VPN?

No.

La VPN conecta una VPC y la red de un centro de datos local, es decir, una conexión sitio a sitio.

17.3.2 ¿Puedo desplegar aplicaciones en la nube, bases de datos en un centro de datos local y luego conectarlas por una VPN?

VPN conecta una VPC y una red local.

Después de configurar correctamente la VPN, la VPC y la red local pueden comunicarse entre sí. En este caso, el servidor de aplicaciones que accede a la base de datos es exactamente lo mismo que acceder a otros servidores en la misma LAN.

Los servidores en la nube y los servidores locales pueden comunicarse entre sí.

AVISO

- Después de configurar una VPN, compruebe si la latencia de la red y la pérdida de paquetes afectan negativamente al funcionamiento del servicio.
- Se recomienda que ejecute el comando ping para comprobar la pérdida de paquetes y los detalles de latencia de red.

17.3.3 ¿Cuántas conexiones de VPN necesito para conectarme a varios servidores locales?

Huawei Cloud IPsec VPN conecta una VPC en la nube y su centro de datos local. Por lo tanto, el número de conexiones de VPN es irrelevante para el número de servidores, pero para el número de centros de datos donde se encuentran los servidores.

En la mayoría de los casos, un centro de datos local tiene un gateway público. Todos los servidores se conectan a Internet con este gateway. Por lo tanto, solo necesita configurar una conexión de VPN para permitir las comunicaciones entre la VPC de Huawei Cloud y su centro de datos local.

17.3.4 ¿Necesito instalar el software IPsec en cada servidor que necesite acceder a un ECS para establecer una conexión de VPN?

No.

Huawei Cloud VPN conecta dos LAN. Varios servidores en el centro de datos local utilizan la misma dirección IP pública para acceder a la nube. Si instala el software IPsec en los servidores locales, el gateway de VPN en la nube recibirá paquetes de negociación de diferentes servidores y, a continuación, el sistema recibe una gran cantidad de información de negociación repetida, lo que causa excepciones de conexión o incluso falta de disponibilidad de conexión.

Se recomienda que utilice el firewall de salida para configurar una VPN para conectarse a la nube. Al crear una VPN, puede especificar varios bloques CIDR. Solo debe permitir que los servidores de desarrolladores accedan al ECS en la nube basándose en las reglas de grupo de seguridad en la nube o las reglas de seguridad del centro de datos local.

17.3.5 ¿Cuáles son las diferencias entre los escenarios de la aplicación y los modos de conexión de IPsec y SSL VPNs?

Escenarios

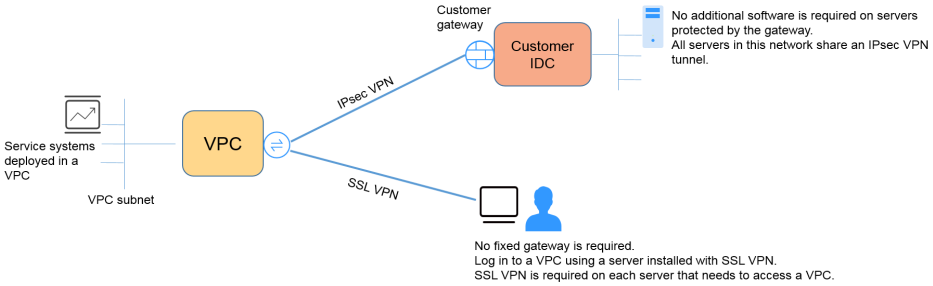
IPsec VPN conecta dos LAN, como una sucursal y su sede, o un centro de datos local y una VPC.

SSL VPN conecta un cliente a una LAN. Por ejemplo, el ordenador portátil de un empleado en un viaje de negocios accede a la red interna de la empresa.

Modos de conexión

IPsec VPN requiere gateway fijos, como firewalls o enrutadores, en ambos extremos. El administrador necesita configurar gateway en ambos extremos para completar la negociación de IPsec VPN.

SSL VPN necesita instalar un software cliente específico en el servidor, luego el servidor se conecta al dispositivo de SSL con el nombre de usuario y la contraseña.



NOTA

Huawei Cloud solo admite VPN IPsec.

17.3.6 ¿Una VPN permite comunicaciones entre dos VPC?

- Si las dos VPC se despliegan en la misma región, utilice una interconexión de VPC para conectarlas.
- Si las dos VPC se despliegan en diferentes regiones, utilice una conexión de VPN para conectarlas. A continuación, se detallan las operaciones:
  a. Cree un gateway de VPN para cada VPC y cree conexiones de VPN para los dos gateway de VPN.
  b. Establezca la dirección de gateway remota de cada conexión de VPN en la dirección IP de gateway del lado del otro extremo.
  c. Establezca las subredes remotas de cada conexión de VPN en las subredes de la VPC del mismo nivel.
  d. Las claves previamente compartidas y los parámetros de algoritmo de las dos conexiones de VPN deben ser los mismos.

17.3.7 ¿Cuáles son los impactos de una VPN en una red local? ¿Cuáles son los cambios en la ruta para acceder a un ECS?

Cuando configure una VPN, realice las siguientes operaciones en el gateway local:

1. Configure las políticas IKE e IPsec.
2. Especifique el tráfico interesante (reglas de ACL).
3. Compruebe la ruta del gateway local para asegurarse de que el tráfico destinado a la VPC de Huawei Cloud se enrute a la interfaz de salida correcta (la interfaz con la política de IPsec enlazada).

Una vez completada la configuración de VPN, solo el tráfico que coincide con las reglas de ACL entra en el túnel de VPN.

Por ejemplo, antes de crear una VPN, los usuarios locales acceden al ECS a través de la EIP vinculada al ECS. Después de crear la VPN, los flujos de datos que coinciden con las reglas de ACL acceden a la dirección IP privada del ECS a través del túnel de VPN.

17.3.8 ¿Qué configuraciones se requieren en ambos extremos de una VPN que conecta un centro de datos local a una VPC?

Para implementar la interconexión de VPN, cree una VPN en la nube y configure el dispositivo VPN en el centro de datos local.

- Creación de una VPN en la nube: Compre un gateway de VPN seleccionando el modo de facturación, la VPC y el ancho de banda. Compre una conexión de VPN especificando las direcciones IP del gateway, las subredes y las políticas de negociación en ambos extremos.
- Configuración del dispositivo de VPN local: Seleccione la dirección IP pública en el lado del centro de datos local, complete las configuraciones de las fases 1 y 2 de negociación de IPsec en el dispositivo que admite IPsec VPN y, a continuación, configure las rutas de red, NAT, y normas de seguridad.

17.3.9 ¿Puedo usar una red con dos salidas para establecer dos conexiones de VPN con la misma VPC?

No.

Cuando se crea una VPN en la nube, una subred local es una subred de VPC y una subred remota es una subred local. Si las dos conexiones usan la misma subred local y la misma subred remota, las conexiones de VPN fallarán.

17.3.10 ¿Puedo conectar dos VPC en la misma región a través de una VPN?

No.

Para dos VPC en la misma región, puede utilizar una conexión de peering de VPC o Cloud Connect para conectarlas.

17.3.11 ¿Cómo puedo conectar dos VPC en la misma región?

Se pueden conectar dos VPC en la misma región mediante una conexión de pares de VPC o de Cloud Connect. La interconexión de VPC solo puede conectar VPC en la misma región, y Cloud Connect también puede conectar VPC en diferentes regiones.

17.3.12 ¿Cómo puedo reemplazar una conexión de conexión directa con una VPN?

1. Asegúrese de que el gateway local admita IPsec VPN.
2. Cree un gateway de VPN y una conexión de VPN en Huawei Cloud. Seleccione la VPC a la que se utiliza la conexión de Direct Connect para el gateway de VPN.

AVISO

Cuando cree una conexión de VPN, configure su subred remota de la siguiente manera para evitar conflictos de enrutamiento.

- Elimine primero la interfaz virtual de la conexión de Direct Connect y, a continuación, configure la conexión de VPN.
- Divida la subred remota en dos subredes y configure la conexión de VPN. Una vez eliminada la conexión de Direct Connect, vuelva a configurar la conexión de VPN.

17.3.13 ¿Cómo puedo habilitar las comunicaciones entre dos VPC y una red local?

Topología de red

IDC-VPC 1-VPC 2

NOTA

IDC indica el centro de datos local. Se establece una conexión de VPN entre la VPC 1 y el IDC.

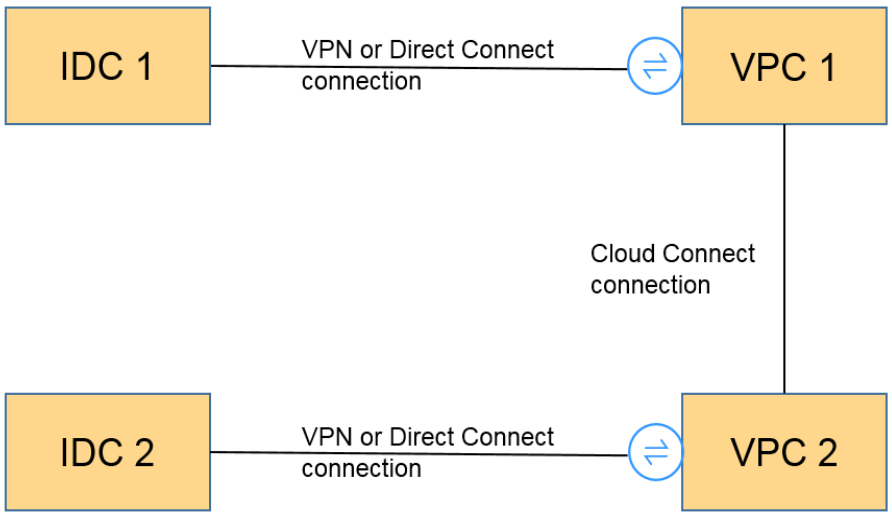
Procedimiento

1. Compruebe si las dos VPC están en la misma región.
   - Si las dos VPC están en la misma región, utilice una interconexión de VPC o conexión de Cloud Connect (gratuita) para conectarlas.
   - Si las dos VPC están en las regiones diferentes, utilice una conexión de Cloud Connect. (Tiene que pagar la tarifa de ancho de banda.)
2. Establezca una conexión de VPN entre el local y una VPC. En el centro de datos local, establezca la subred remota en las subredes de VPC 1 y VPC 2. La subred local de VPC 1 debe contener la subred conectada con una interconexión de VPC o una conexión de Cloud Connect. La ruta de subred de la interconexión de VPC o la conexión de Cloud Connect debe destinarse a la subred local.

17.3.14 ¿Cómo conecto cuatro subredes?

La **Figura 17-14** muestra la topología de red.

Figura 17-14 Topología de red



1. Utilice una conexión de VPN o de Direct Connect para conectar IDC 1 a VPC 1.
2. Utilice una conexión de Cloud Connect para conectar VPC 1 a VPC 2. (También puede utilizar una interconexión de VPC para habilitar las comunicaciones entre VPC 1 y VPC 2 si están en la misma región.)
3. Utilice una conexión de VPN o de Direct Connect para conectar IDC 2 a VPC 2.
4. Configure rutas para permitir que el tráfico vaya desde las cuatro subredes involucradas en las conexiones de VPN, de Cloud Connect y de Direct Connect.

17.3.15 ¿Necesito dos conexiones de VPN para conectar cuatro subredes de dos regiones si cada región tiene dos subredes?

No.

Solo se requiere una conexión de VPN entre dos regiones. Todas las subredes se pueden agregar a la conexión de VPN.

En este escenario, si intenta crear una segunda conexión de VPN, la consola de gestión muestra un mensaje que indica que se produce un conflicto porque las dos conexiones tienen la misma dirección de gateway remoto.

17.3.16 ¿Puedo acceder a OBS por una VPN?

Sí.

Con la ayuda del VPC Endpoint Service, usted accede a OBS con una VPN. Cree dos puntos de conexión de VPC para el servidor de DNS privado y OBS, respectivamente.

Configure el servidor de DNS privado y la ruta de Huawei Cloud en su centro de datos local.

17.3.17 ¿Cómo conecto mi computadora personal a la nube por una VPN?

Los routers de banda ancha domésticos comunes, terminales móviles personales y servicios VPN (como L2TP) proporcionados por hosts de Windows no pueden conectarse a ECS en VPC con Huawei Cloud VPN.

Para usar Huawei Cloud VPN, los dispositivos locales deben admitir el protocolo de IPsec estándar.

17.3.18 ¿Cómo accedo a los ECS de Huawei Cloud desde casa después de que mi red empresarial esté conectada a Huawei Cloud por una VPN?

Una VPN en Huawei Cloud conecta una VPC en la nube y una red de área local (LAN) local.

La red doméstica no forma 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 a la EIP del servicio en la nube o conectarse a la LAN de su empresa con SSL VPN (si su empresa admite el acceso SSL) y luego acceder a los recursos de VPC en la nube con la LAN.

17.3.19 ¿Cómo puedo crear una conexión de VPN temporalmente si no hay ningún dispositivo local que admita IPsec disponible después de comprar un gateway de Huawei Cloud VPN y una conexión de VPN?

Para establecer una conexión de VPN con Huawei Cloud, un dispositivo que admita IPsec estándar y una dirección IP pública fija debe estar disponible en la red local.

Para conectarse temporalmente a Huawei Cloud, instale software de terceros en el host.

El software IPsec de terceros recomendado incluye strongSwan, Openswan y GreenBow. Para obtener más información, consulte la **Guía del administrador de Virtual Private Network**.

17.3.20 ¿Cómo selecciono una región adecuada en la nube cuando estoy comprando un gateway de VPN?

Puede seleccionar una VPC en cualquier región cuando compre un gateway de VPN.

Sin embargo, se recomienda que seleccione la región donde se encuentra su centro de datos local para una menor latencia de red.

- Para varias VPC en la misma región, solo necesita crear un gateway de VPN porque las VPC se pueden conectar mediante las interconexiones de VPC (gratuitamente).
- Para conectarse a varias VPC en diferentes regiones, puede usar VPN y Cloud Connect.

17.4 Facturación y pagos

17.4.1 ¿Qué me cobrarán por crear una VPN? ¿Se me cobrará por las direcciones IP de gateway de VPN?

Las VPN se facturan anualmente/mensualmente o de pago por uso. Debe pagar tanto por el ancho de banda del gateway de VPN o el precio del tráfico y el precio de la conexión de VPN.

Los gateway de VPN se pueden facturar por tráfico o ancho de banda.

- Un gateway de VPN anual/mensual solo se puede facturar por ancho de banda. El precio de un gateway de VPN anual/mensual incluye el precio de las conexiones de VPN que se pueden crear para el gateway y el precio del ancho de banda.
- El ciclo de facturación del modo de facturación de pago por uso es de una hora. Si elige un gateway de VPN de pago por uso, se debe comprar una conexión de VPN junto con el gateway de VPN. El precio incluye el ancho de banda del gateway de VPN o el precio del tráfico y el precio de la conexión de VPN creada junto con el gateway. Si crea otra conexión para el gateway, se le cobrará la conexión adicional.

  NOTA

  - La dirección IP del gateway de VPN no se facturará.
  - Un gateway de VPN no puede compartir un ancho de banda con una EIP vinculada a un ECS.

17.4.2 ¿Cuál es la diferencia entre la facturación de un gateway de VPN por ancho de banda y por tráfico?

Un gateway de VPN de pago por uso se puede facturar por ancho de banda o por tráfico. Sus diferencias son las siguientes:

- Facturación por ancho de banda: El ciclo de facturación es de una hora. La tarifa generada depende del tamaño del ancho de banda.
- Facturado por tráfico: Se cobrarán las tarifas de tráfico generadas cada hora. La facturación se basa en el tráfico generado que sale de una VPC. El tamaño del ancho de banda no afecta al precio del tráfico público por GB.

17.4.3 ¿Puede una VPN facturada por tráfico usar un paquete de datos compartidos?

No.

El servicio VPN se factura de forma independiente y no puede usar paquetes de datos compartidos.

17.4.4 ¿Cuántas conexiones VPN se me cobrará para conectar VPCs en diferentes regiones?

Las VPN se pueden usar para conectar VPCs en diferentes regiones. El ancho de banda y las conexiones de VPN de cada región se facturarán de forma independiente. Por ejemplo:

En la Región A, establece una conexión de VPN con la Región B y otra conexión de VPN con la Región C, luego

- El gateway de VPN de la Región A tiene dos conexiones.
- El gateway de VPN de la Región B tiene una conexión.

- El gateway de VPN de la Región C tiene una conexión.

En este caso, se le cobrará por cuatro conexiones de VPN.

17.4.5 ¿Cuándo se congelarán mis recursos de VPN? ¿Cómo puedo descongelar los recursos de VPN?

- Si los recursos de VPN de pago por uso están atrasados, los recursos ingresan el período de gracia, durante el cual aún puede acceder y usar los recursos. Si el período de gracia finaliza y no ha pagado los atrasos, los recursos ingresan el período de retención, durante el cual se congelan los recursos. Los recursos congelados no están disponibles y no se pueden modificar ni eliminar. Si el período de retención finaliza y aún no ha recargado su cuenta y pagado los atrasos, los recursos se liberarán y no se podrán restaurar. Para asegurarse de que los recursos estén disponibles, recargue su cuenta y pague los atrasos antes de que expiren los recursos.
- Los recursos de VPN congelados estarán disponibles después de renovarlos o recargar su cuenta. Si una conexión de VPN está en el estado no conectado, inicie los flujos de datos para activar la conexión de VPN y deje que esté en el estado normal. Por ejemplo, puede hacer ping a hosts en diferentes subredes para activar flujos de datos.

17.5 Operaciones relacionadas en la consola

17.5.1 ¿Cuáles son las relaciones entre una VPC, un gateway de VPN y una conexión de VPN?

- Una VPC es una red privada en la nube. Se pueden crear múltiples VPC en la misma región mientras están aisladas entre sí. Una VPC se puede dividir en varias subredes.
- Se crea un gateway de VPN en una VPC y es el punto de acceso de una conexión de VPN. Una VPC en Huawei Cloud puede tener solo un gateway de VPN, mientras que un gateway de VPN puede tener múltiples conexiones de VPN.
- Se crea una conexión de VPN para un gateway de VPN y conecta una VPC a un centro de datos local (o una VPC en otra región).

  NOTA

  El número de conexiones de VPN es irrelevante para el número de subredes locales o el número de subredes remotas. Solo está relacionado con el número de centros de datos locales (o VPC en otras regiones) que se van a conectar a su VPC. Las conexiones de VPN creadas se muestran en la lista de conexiones de VPN. También puede ver el número de conexiones de VPN creadas para cada gateway de VPN.

17.5.2 ¿Cuánto tiempo toma para que las configuraciones de VPN entregadas surtan efecto?

Las configuraciones de VPN tardan de 1 a 5 minutos en surtir efecto.

NOTA

Después de que las configuraciones de VPN entren en vigor, configure su gateway local para completar la negociación del túnel con el gateway de VPN en Huawei Cloud.

17.5.3 ¿Por qué la conexión de VPN siempre está en el estado no conectado incluso después de que se complete su configuración?

Asegúrese de que las claves previamente compartidas y la información de negociación en ambos extremos sean consistentes. Las subredes locales y el gateway de VPN en la nube son las subredes remotas y el gateway remoto en el centro de datos local. El gateway remotoy las subredes remotas en la nube son el gateway local y las subredes locales en el centro de datos local.

Asegúrese de que las rutas, NAT y las reglas de política de seguridad estén correctamente configuradas en su dispositivo de gateway local. A continuación, haga ping a los servidores en subredes en ambos extremos.

NOTA

La VPN se activa en función de los flujos de datos. Después de configurar VPN, haga ping a un dispositivo en la subred del par. Antes de ejecutar el comando ping, deshabilite la función de firewall en el dispositivo y permita paquetes ICMP entrantes en el grupo de seguridad en la nube.

Hacer ping a la dirección IP del gateway no puede activar la negociación de VPN. Hacer ping al servidor en la subred protegida por el gateway.

17.5.4 ¿Se puede retener una dirección IP de gateway de VPN después de que se elimine el gateway de VPN?

No. La dirección IP del gateway de VPN se liberará después de que se elimine el gateway de VPN.

Al eliminar un gateway de VPN también se eliminarán los recursos asociados con el gateway.

AVISO

La eliminación de la última conexión de un gateway de VPN de pago por uso también eliminará el gateway. Si desea conservar la dirección IP, no elimine la última conexión de VPN.

17.5.5 ¿Necesito crear un gateway de VPN o una conexión de VPN para crear una VPN? ¿Qué información sobre una VPN creada puede ser modificada?

Prerrequisitos para crear una VPN

Cree una VPC y subredes de VPC. Las subredes de VPC no pueden entrar en conflicto con las subredes locales.

Para crear una VPN, necesita:

- Cree un gateway de VPN. Ponga a **Billing Mode**, **Region**, **Name**, **VPC**, **Billed By** y a **Bandwidth (Mbit/s)**. Se asignará una dirección IP al gateway de VPN después de crear el gateway. Solo las configuraciones para **Name** y **Bandwidth** se pueden modificar después de crear el gateway de VPN.
- Cree una conexión de VPN. Especifique el nombre de la conexión, el gateway de VPN asociada, las subredes locales, el gateway remoto, las subredes remotas, PSK y las

políticas de negociación. El nombre de la conexión, las subredes locales, PSK, el gateway remoto, las subredes remotas y las políticas de negociación se pueden modificar después de crear la conexión de VPN.

17.5.6 ¿Necesito configurar las reglas de ACL en la consola de gestión de Huawei Cloud después de configurar las reglas de ACL en el dispositivo de gateway local?

Necesita crear reglas de ACL dedicadas para su dispositivo de gateway local. Las políticas IPsec harán referencia a las reglas de ACL.

Cuando configura la VPN en la nube, las reglas de ACL se generarán automáticamente en función de las subredes locales y remotas introducidas en la consola de gestión y luego se entregarán al gateway de VPN.

(Huawei Cloud) El número de reglas de ACL = El número de subredes locales x El número de subredes remotas

17.5.7 ¿Qué hago si ocurre una excepción cuando agrego una subred remota durante la creación de una conexión VPN?

Compruebe si esta subred remota se ha utilizado como destino de una ruta de conexión de interconexión de VPC, de Cloud Connect o de Direct Connect, lo que provoca conflictos de ruta. Si es así, elimine la ruta y cree una nueva.

17.5.8 ¿Dónde puedo agregar rutas en la consola de VPN para llegar a las subredes remotas?

Cuando se crea una conexión de VPN, las rutas se entregan automáticamente para llegar a las subredes remotas.

17.5.9 ¿Puedo invocar a las API para gestionar los recursos de Huawei Cloud VPN?

La VPN requiere configuraciones complejas. Actualmente, los recursos VPN no se pueden crear, consultar o modificar con las API. Solo puede gestionar los recursos de VPN en la consola de VPN.

17.5.10 ¿Qué es un gateway remoto y una subred remota en una conexión de VPN?

Al crear una conexión de VPN, una subred en Huawei Cloud VPC es la subred local y el gateway de VPN creada es el gateway local. La subred y el gateway conectadas en el centro de datos local es la subred remota y el gateway remoto.

Una dirección IP de gateway remota es una dirección IP pública.

17.5.11 ¿Cómo desactivo PFS al crear una conexión de VPN?

Puede desactivar Perfect Forward Secrecy (PFS) en algunas regiones de Huawei Cloud. Se recomienda habilitar PFS en su centro de datos local, ya que mejora la seguridad de negociación de IKE en la fase 2.

De forma predeterminada, PFS está deshabilitado en los dispositivos de algunos proveedores. Consulte el manual de configuración del dispositivo para asegurarse de que PFS está habilitado.

NOTA

- PFS es una característica de seguridad.

  La negociación de IKE tiene dos fases, la fase 1 y la fase 2. La clave de la fase 2 (IPsec SA) se deriva de la clave generada en la fase 1. Una vez que se divulga la clave en la fase 1, la seguridad de la VPN IPsec puede verse afectada negativamente. Para mejorar la seguridad de la clave, IKE proporciona PFS. Después de configurar PFS, se realizará un intercambio de DH adicional durante la negociación de SA IPsec y se generará una nueva clave de SA IPsec, lo que mejorará la seguridad de SA IPsec.
- Para garantizar la seguridad, PFS está habilitado en Huawei Cloud de forma predeterminada. Asegúrese de que PFS también esté habilitado en el gateway local. De lo contrario, la negociación no funcionará.

17.5.12 ¿Cuántas subredes locales y remotas puedo agregar a una VPN? ¿Por qué se muestra un mensaje de error cuando actualizo la subred local especificando un bloque CIDR?

- Puede configurar hasta 5 subredes locales. El producto del número de subredes locales y el número de subredes remotas no puede exceder de 225.
- Una VPC proporciona rutas de subred de VPC basadas en las subredes remotas de la conexión de VPN, las subredes remotas de la conexión de Direct Connect y las subredes de la interconexión de VPC. Cada subred tiene una ruta de subred.
- El número de rutas de subred de VPC no puede exceder de 200. Es decir, el número total de subredes remotas de la conexión de VPN, subredes remotas de la conexión de Direct Connect, subredes de la interconexión de VPC y rutas personalizadas en una VPC no puede exceder de 200.

17.5.13 ¿Cuáles son las precauciones para configurar las subredes locales y remotas de una conexión VPN?

- Puede configurar hasta 5 subredes locales. El producto del número de subredes locales y el número de subredes remotas no puede exceder de 225. Si se supera la 225, considere la posibilidad de crear superredes en las subredes locales o remotas.
- La subred local no puede incluir el bloque CIDR de la subred remota. La subred remota puede incluir el bloque CIDR de la subred local.
- Hay rutas que apuntan a las subredes locales en la VPC donde reside el gateway de VPN.
- Si hay dos conexiones (conexión A y conexión B) creadas para un gateway de VPN, y la subred remota de la conexión A está dentro de la de la conexión B, cuando la red de destino a la que se va a acceder pertenece al bloque CIDR solapado, la conexión creada primero se hace coincidir primero. Independientemente del estado de la conexión. (La coincidencia de longitud de máscara no se utiliza para la VPN basada en políticas.)

17.5.14 ¿Por qué el estado de una conexión de VPN no está conectado en la consola de gestión cuando ya está disponible?

Hay una latencia para mostrar el estado más reciente de la conexión de VPN en la consola de gestión.

Si el acceso al servicio es normal, se establece la conexión de VPN. Después de varios minutos, el estado de la conexión de VPN será **Connected**.

17.5.15 ¿Qué puedo hacer si se muestra un mensaje que indica que la conexión de VPN no existe después de que se modifiquen las políticas de negociación?

Este problema se debe al intervalo de actualización de la página.

Cuando modifica la configuración avanzada, el sistema primero elimina la conexión de VPN y luego crea una. Si la página contiene el mensaje que indica que la conexión se está eliminando o que se está creando durante un corto período de tiempo, no cree la misma conexión (con la misma subred local, subred remota y gateway remoto) de nuevo.

Si la página permanece en el estado de eliminación o creación de conexión durante mucho tiempo, **envíe un ticket de servicio**.

17.5.16 ¿Qué debo hacer si no puedo crear conexiones para un gateway de VPN que no tiene información de ancho de banda?

Si un gateway de VPN no tiene información de ancho de banda, la VPN es de la edición anterior. Este tipo de VPN ya no se puede crear en Huawei Cloud.

- Solo se puede crear una conexión de VPN para cada gateway de VPN de la edición anterior y su ancho de banda no está garantizado. Puede eliminar el gateway y crear una de las nuevas ediciones. Pero los servicios se verán afectados.
- También puede **enviar un ticket de servicio** para cambiar el gateway a una de la nueva edición y sus servicios no se verán afectados.

  De forma predeterminada, el ancho de banda de un gateway de VPN cambiada a la nueva edición es de 10 Mbit/s. Puede ajustar el ancho de banda según sea necesario. El ancho de banda de un gateway de VPN que se factura anualmente/mensualmente no se puede reducir.

17.5.17 ¿Cómo puedo restablecer una conexión de VPN?

- Deshabilite la conexión de VPN en el dispositivo local. Después de que el estado de la conexión de VPN en la nube cambie a **Not connected**, habilite la conexión de VPN en el dispositivo local.
- Cambie la dirección IP del gateway remoto de la conexión de VPN en la nube a cualquier otra dirección IP. Después de que el estado de la conexión en el centro de datos local cambie a inactiva, cambie la dirección IP del gateway remoto en la nube a la dirección IP anterior.

17.5.18 ¿Cuál es el ancho de banda máximo admitido por un gateway de VPN?

El ancho de banda máximo soportado por un gateway de VPN es de 300 Mbit/s.

17.5.19 ¿Qué versión de IKE debo seleccionar al crear una conexión de VPN?

Huawei Cloud recomienda IKEv2 para la negociación porque IKEv1 no es seguro. Además, IKEv2 funciona mejor que IKEv1 en términos de negociación y establecimiento de conexión, métodos de autenticación, tiempo de espera de DPD y tiempo de espera de SA.

Huawei Cloud no será compatible con IKEv1 pronto.

Introducción a IKEv1 e IKEv2

- La complejidad de IKEV1, un protocolo híbrido, trae inevitablemente algunos defectos de seguridad y rendimiento. Esto se ha convertido en el cuello de botella para el sistema IPsec actual.
- El protocolo IKEv2 reserva las funciones básicas de IKEv1 y supera algunos problemas traídos por IKEv1. Además, por simplicidad, eficiencia, seguridad y robustez, RFC 4306, un documento describe la versión 2 de IKE, combina el contenido de lo que eran documentos IKEv1 previamente separados. Al minimizar las funciones principales y los algoritmos de contraseña predeterminados, IKEv2 mejora en gran medida la capacidad de interoperación entre diferentes VPN IPsec.

Vulnerabilidades de seguridad de IKEv1

- Los algoritmos criptográficos soportados por IKEv1 no se han actualizado durante más de 10 años. Además, IKEv1 no admite algoritmos criptográficos fuertes como AES-GCM y ChaCha20-Poly1305. Para IKEv1, el bit E (Encryption) en la cabecera ISALMP especifica que las cargas útiles que siguen a la cabecera ISALMP están cifradas, pero cualquier verificación de integridad de datos de esas cargas útiles es manejada por una carga útil hash separada. Esta separación de la encriptación de la protección de la integridad de los datos impide el uso de encriptación autenticada (AES-GCM) con IKEv1.
- El protocolo IKEv1 es vulnerable a ataques de amplificación DoS. IKEv1 es vulnerable a conexiones semiabiertas.

  IKEv2 puede defenderse de ataques DoS.
- El modo agresivo IKEv1 no es lo suficientemente seguro. En modo agresivo, los paquetes de información no están cifrados. También hay ataques de fuerza bruta dirigidos al modo agresivo, como los ataque de intermediario.

Diferencias entre IKEv1 e IKEv2

- **Proceso de negociación**
  - La negociación IKEv1 SA consta de dos fases. IKEv1 es complejo y ocupa una gran cantidad de ancho de banda. La negociación IKEv1 fase 1 tiene como objetivo establecer la IKE SA. Este proceso soporta el modo principal y el modo agresivo. El modo principal utiliza seis mensajes ISAKMP para establecer el IKE SA, pero el modo agresivo utiliza solo tres. Por lo tanto, el modo agresivo es más rápido en el establecimiento de IKE SA. Sin embargo, el modo agresivo no proporciona protección de identidad de pares porque el intercambio de claves y la autenticación de identidad se realizan al mismo tiempo. La negociación de la fase 2 de IKEv1 tiene como objetivo establecer la SA IPsec para la transmisión de datos. Este proceso utiliza el modo de intercambio rápido (3 mensajes de ISAKMP) para completar la negociación.

- En comparación con IKEv1, IKEv2 simplifica el proceso de negociación de SA. IKEv2 utiliza dos intercambios (un total de 4 mensajes) para crear una SA IKE y un par de SA IPsec. Para crear varios pares de SA IPsec, solo se necesita un intercambio adicional para cada par adicional de SA.

  NOTA

  Para la negociación IKEv1, su modo principal requiere nueve (6+3) paquetes en total y su modo agresivo requiere 6 (3+3) paquetes. La negociación IKEv2 requiere solo 4 (2+2) paquetes.

- **Métodos de autenticación**
  - Solo IKEv1 (que requiere una tarjeta de encriptación) admite la autenticación de envolvente digital (HSS-DE).
  - IKEv2 admite la autenticación del Extensible Authentication Protocol (EAP). IKEv2 puede utilizar un servidor AAA para autenticar remotamente a los usuarios móviles y de PC y asignar direcciones IP privadas a estos usuarios. IKEv1 no proporciona esta función y debe usar L2TP para asignar direcciones IP privadas.
  - Solo IKEv2 admite algoritmos de integridad de IKE SA.
- **Timeout de DPD**
  - Solo IKEv1 admite el parámetro **retry-interval**. Si un dispositivo envía un paquete DPD pero no recibe respuesta dentro del intervalo de reintento especificado, el dispositivo registra un evento de fallo de DPD. Cuando el número de eventos de error alcanza cinco, se eliminan tanto el SA IKE como el SA IPsec. La negociación IKE SA se iniciará de nuevo cuando el dispositivo tenga tráfico IPsec para manejar.
  - En el modo IKEv2, el intervalo de retransmisión aumenta de 1, 2, 4, 8, 16, 32 a 64 segundos. Si no se recibe ninguna respuesta dentro de ocho transmisiones consecutivas, el extremo par se considera muerto, y el SA IKE y el SA IPsec se eliminarán.
- **Procesamiento del tiempo de espera de IKE SA y del tiempo de espera de IPsec SA**

  En IKEv2, la vida útil suave de IKE SA es 9/10 de la vida útil dura de IKE SA más o menos un valor aleatorio para reducir la probabilidad de que dos extremos inicien la renegociación al mismo tiempo. Por lo tanto, la vida útil suave no requiere ajustes manuales en IKEv2.

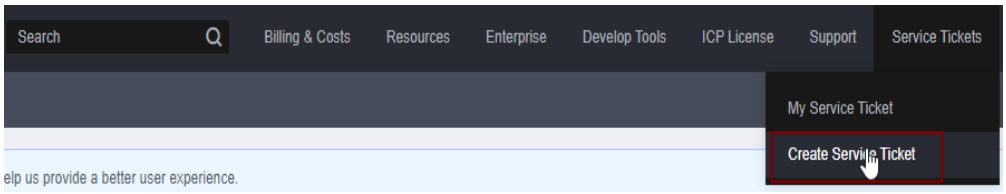
Ventajas de IKEv2 sobre IKEv1

- Proceso de negociación de SA simplificado y mayor eficiencia de negociación.
- Se han cerrado muchas lagunas criptográficas, mejorando la seguridad.
- Admite la autenticación de EAP, lo que mejora la flexibilidad y la escalabilidad de la autenticación.
- EAP es un protocolo de autenticación que admite múltiples métodos de autenticación. La mayor ventaja de EAP es la escalabilidad. Es decir, se pueden agregar nuevos modos de autenticación sin cambiar el sistema de autenticación original. La autenticación EAP ha sido ampliamente utilizada en redes de acceso telefónico.
- IKEv2 emplea una carga útil cifrada que se basa en el diseño de ESP. La carga útil cifrada IKEv2 asocia la encriptación y la protección de la integridad de los datos de una manera que permite utilizar los algoritmos de encriptación autenticados. AES-GCM garantiza la confidencialidad, integridad y autenticación.

17.5.20 ¿Cuáles son las categorías de los tickets de servicio de VPN? ¿Cómo puedo crear un ticket de servicio de VPN?

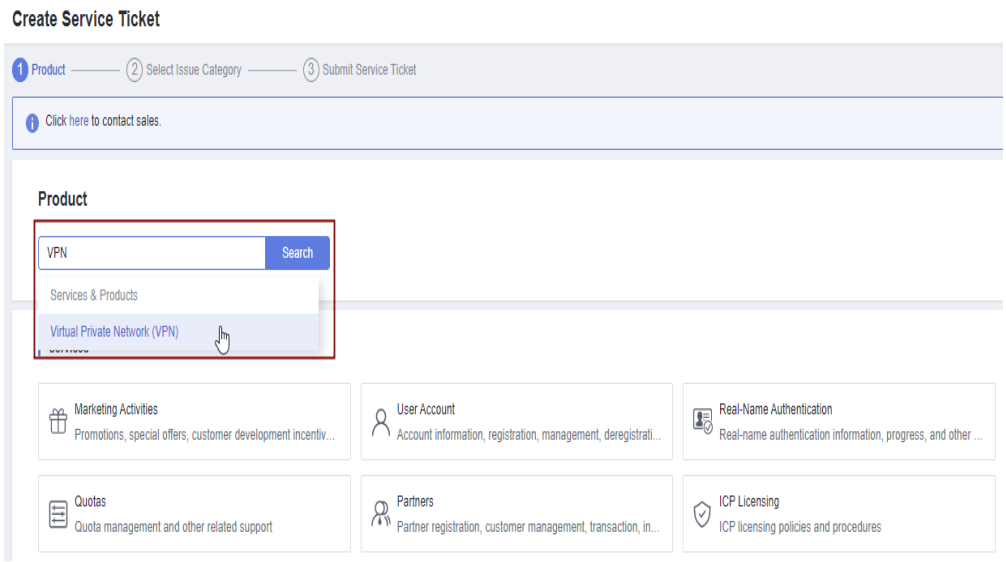
1. Inicie sesión en la consola de gestión.
2. En la esquina superior derecha de la consola de gestión, seleccione **Service Tickets** > **Create Service Ticket**.

Figura 17-15 Crear ticket de servicio



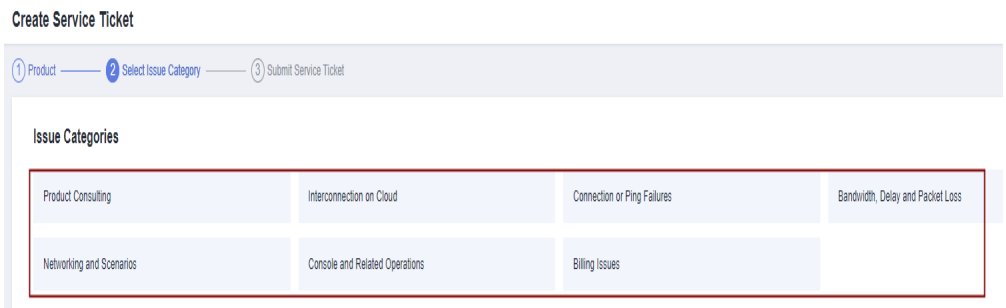
3. Busque **VPN** y seleccione **Virtual Private Network (VPN)**.

Figura 17-16 Selección de **Virtual Private Network (VPN)**



4. Seleccione una categoría de error.

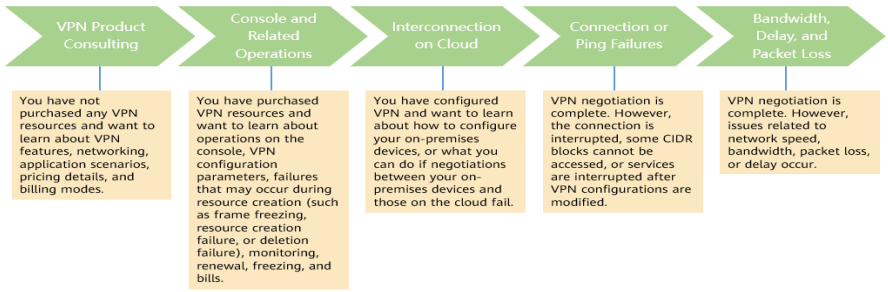
Figura 17-17 Seleccionar categoría de problema



NOTA

Cuando **envía un ticket de servicio**, seleccione una categoría de problema para facilitar la gestión del problema.

Figura 17-18 Categoría de emisión y base de clasificación



17.5.21 ¿Se requiere un nombre de usuario y contraseña para crear una conexión de VPN IPsec?

No. Huawei Cloud IPsec VPN utiliza una clave precompartida (PSK) para la autenticación. La clave está configurada en un gateway de VPN. Se establecerá un túnel después de que se complete la negociación de VPN. Por lo tanto, no se requieren nombres de usuario y contraseñas.

En general, las VPN SSL, PPTP y L2TP usan nombres de usuario y contraseñas para la autenticación.

NOTA

IPsec XAUTH es una tecnología extendida de IPsec VPN. Indica a los usuarios que introduzcan sus nombres de usuario y contraseñas durante la negociación de VPN.

Huawei Cloud VPN no es compatible con IPsec XAUTH.

17.5.22 ¿Qué recursos de VPN se pueden monitorear?

VPN Gateway

La información de ancho de banda que se puede supervisar incluye el tráfico entrante, el ancho de banda entrante, el tráfico saliente, el ancho de banda saliente y el uso del ancho de banda saliente.

Para ver las métricas del gateway de VPN, localice el gateway de VPN de destino y haga clic en **View Metric** en la columna **Operation**.

VPN Connection

El estado de la conexión de VPN puede ser monitoreado.

El valor **1** indica que la conexión es normal.

El valor **0** indica que la conexión no está conectada.

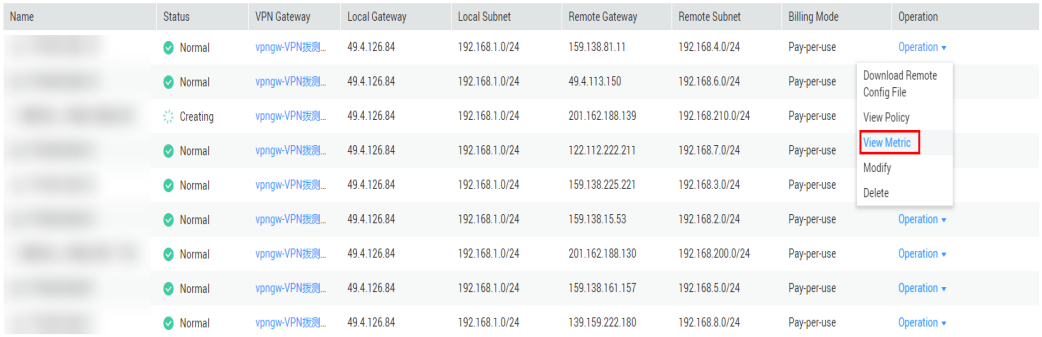
Para ver el estado de la conexión de VPN, localice la conexión de VPN de destino y haga clic en **View Metric** en la columna **Operation**.

17.5.23 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía automáticamente notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Después de crear una conexión de VPN, puede localizar la fila que contiene la conexión de VPN y elegir **Operation** > **View Metric** para ver el estado de la conexión de VPN.

Figura 17-19 Ver métrica



17.6 Negociación e interconexión de VPN

17.6.1 ¿Qué dispositivos se pueden conectar a Huawei Cloud por una VPN?

Huawei Cloud VPN admite el protocolo IPsec estándar. Un dispositivo de su centro de datos local puede conectarse a Huawei Cloud si el dispositivo cumple los siguientes requisitos:

1. Soporta la VPN sobre IPsec.
2. Tiene una dirección IP pública fija, que se puede configurar estáticamente, o traducir con NAT en escenarios transversales de NAT (su dispositivo se despliega detrás de un gateway NAT).

La mayoría de los dispositivos son routers y firewalls. Para obtener más información sobre la configuración de la interconexión, consulte la **Guía del administrador**.

NOTA

- Los routers de banda ancha domésticos comunes, los hosts de Windows que proporcionan servicios VPN (como L2TP) y los terminales móviles personales no pueden conectarse a Huawei Cloud con una VPN.
- Los siguientes productos pueden conectarse a Huawei Cloud con VPN:
  - Dispositivos: firewalls y enrutadores de acceso (AR) de Huawei, firewalls de Hillstone y firewalls de Check Point
  - Servicios en la nube: Alibaba Cloud, Tencent Cloud, Amazon Web Services (AWS) y Microsoft Azure
  - Software: strongSwan
- El protocolo IPsec es un protocolo de IETF estándar. Dispositivos compatibles con IPsec se pueden interconectar con Huawei Cloud.

  La mayoría de los routers y firewalls de clase empresarial admiten el protocolo de IPsec.
- Sin embargo, algunos dispositivos admiten IPsec de VPN solo después de comprar las licencias de software requeridas.

  Póngase en contacto con el administrador del centro de datos local para confirmar el modelo de dispositivo con el proveedor.

17.6.2 ¿Qué son los parámetros de negociación de VPN? ¿Cuáles son sus valores predeterminados?

Tabla 17-4 Parámetros de negociación de VPN

Política	Parámetro	Valor
IKE	Authentication Algorithm	● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● AES-256 ● AES-192 ● AES-128 (valor predeterminado)

Política	Parámetro	Valor
	DH Algorithm	● Grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 14 (valor predeterminado) ● Grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● Grupo 15 ● Grupo 16 ● Grupo 19 ● Grupo 20 ● Grupo 21 **NOTA** En algunas regiones, solo **Group 14**, **Group 2** y **Group 5** están disponibles.
	Version	● v1 (no recomendado debido a riesgos de seguridad) ● v2 (valor predeterminado)
	Lifecycle (s)	**86400** (predeterminado) Unidad: segundo Rango de valores: de **60** a **604800**
IPsec	Authentication Algorithm	● SHA1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● MD5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● SHA2-256 (valor predeterminado) ● SHA2-384 ● SHA2-512
	Encryption Algorithm	● AES-128 (valor predeterminado) ● AES-192 ● AES-256 ● 3DES (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.)

Política	Parámetro	Valor
	PFS	● DH grupo 5 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 2 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 14 (valor predeterminado) ● DH grupo 1 (Este algoritmo es inseguro. Tenga cuidado al usar este algoritmo.) ● DH grupo 15 ● DH grupo 16 ● DH grupo 19 ● DH grupo 20 ● DH grupo 21 ● Deshabilitar **NOTA** En algunas regiones, solo **DH group 14**, **DH group 2** y **DH group 5** están disponibles.
	Transfer Protocol	● ESP (valor predeterminado) ● AH ● AH-ESP
	Lifecycle (s)	**3600** (predeterminado) Unidad: segundo Rango de valores: de **480** a **604800**

NOTA

- Perfect Forward Secrecy (PFS) es una característica de seguridad.

  La negociación de IKE tiene dos fases, la fase 1 y la fase 2. La clave de la fase 2 (IPsec SA) se deriva de la clave generada en la fase 1. Una vez que se divulga la clave en la fase 1, la seguridad de la VPN IPsec puede verse afectada negativamente. Para mejorar la seguridad de la clave, IKE proporciona PFS. Después de configurar PFS, se realizará un intercambio de DH adicional durante la negociación de SA IPsec y se generará una nueva clave de SA IPsec, lo que mejorará la seguridad de SA IPsec.
- Para garantizar la seguridad, PFS está habilitado en Huawei Cloud de forma predeterminada. Asegúrese de que PFS también esté habilitado en el gateway local. De lo contrario, la negociación no funcionará.
- Para habilitar PFS, asegúrese de que las configuraciones en ambos extremos de una VPN son las mismas.
- La vida útil basada en el tráfico de IPsec SA en Huawei Cloud VPN es de 1,843,200 KB y no se puede cambiar. Esta duración no afecta al establecimiento de una SA IPsec.

17.6.3 ¿Se establecerá automáticamente una conexión de VPN IPsec?

Después de completar las configuraciones en ambos extremos de una conexión de VPN IPsec, la conexión de VPN no se establecerá automáticamente solo después de que los datos fluyan

entre los dos extremos de la conexión. Si no hay flujo de datos entre la nube y el centro de datos local, la conexión de VPN siempre estará en el estado inactivo. Cualquier dato generado al acceder a servidores o hacer ping entre servidores puede desencadenar el establecimiento de una conexión de VPN.

El establecimiento de una conexión de VPN se puede activar en cualquiera de las dos condiciones siguientes: El gateway de VPN y el gateway remoto activan automáticamente la negociación. Los servidores en la nube y en las instalaciones se acceden entre sí a través de la conexión de VPN que se va a establecer.

Sin embargo, el establecimiento automático de una conexión de VPN no puede ser activado por un gateway de VPN en Huawei Cloud. Verifique que el establecimiento de su conexión de VPN pueda ser activado por los flujos de datos entre los dos extremos de la conexión de VPN. Es decir, compruebe si se puede establecer una conexión de VPN después de hacer ping a un servidor en la nube desde un servidor local, y si se puede establecer una conexión de VPN después de desconectar la conexión y hacer ping a un servidor local desde un servidor en la nube.

NOTA

Las direcciones de origen y destino de los paquetes de ping deben estar protegidas por la VPN.

Antes de establecer una conexión de VPN, las direcciones IP del gateway en ambos extremos se pueden hacer ping. Sin embargo, hacer ping a las direcciones IP del gateway no activa el establecimiento de la conexión de VPN.

17.6.4 ¿Cómo configuro una VPN en un dispositivo local? (Configuración de la VPN en un firewall de Huawei de serie USG6600)

Debido a la simetría del túnel, los parámetros de VPN configurados en la nube deben ser los mismos que los configurados en su centro de datos local. Si son diferentes, no se puede establecer una VPN.

Para configurar una VPN, también debe configurar la VPN IPsec en su router o firewall local. El método de configuración puede variar según el dispositivo de red en uso. Para obtener más información, consulte la guía de configuración de su dispositivo de red.

El siguiente ejemplo utiliza un firewall de Huawei serie USG6600 que ejecuta V100R001C30SPC300 para describir cómo configurar una VPN en un dispositivo local.

Supongamos que las subredes locales son 192.168.3.0/24 y 192.168.4.0/24, las subredes de VPC son 192.168.1.0/24 y 192.168.2.0/24, y la dirección IP pública de la salida del túnel IPsec en la VPC es de *XXX.XXX.XX.XX*, que se puede obtener de los parámetros de gateway local de la VPN IPsec en la VPC.

Procedimiento

1. Inicie sesión en la CLI del firewall.
2. Compruebe la información de la versión del firewall.
   ```
   display version
   17:20:502017/03/09
   Huawei Versatile Security Platform Software
   Software Version: USG6600 V100R001C30SPC300 (VRP (R) Software, Version 5.30)
   ```
3. Cree una lista de control de acceso (ACL) y envíela a la instancia VPN de destino.
   ```
   acl number 3065 vpn-instance vpn64
   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
q
```

4. Cree una propuesta IKE.

```
ike proposal 64
dh group5
authentication-algorithm sha1
integrity-algorithm hmac-sha2-256
sa duration 3600
q
```

5. Cree un par IKE y consulte la propuesta IKE creada. La dirección IP del par es 93.188.242.110.

```
ike peer vpnikepeer_64
pre-shared-key ******** (******** specifies the pre-shared key.)
ike-proposal 64
undo version 2
remote-address vpn-instance vpn64 93.188.242.110
sa binding vpn-instance vpn64
q
```

6. Crear un protocolo IPsec.

```
IPsec proposal IPsecpro64
encapsulation-mode tunnel
esp authentication-algorithm sha1
q
```

7. Cree una política IPsec y vincule la política IKE y la propuesta IPsec a ella.

```
IPsec policy vpnIPsec64 1 isakmp
security acl 3065
pfs dh-group5
ike-peer vpnikepeer_64
proposal IPsecpro64
local-address xx.xx.xx.xx
q
```

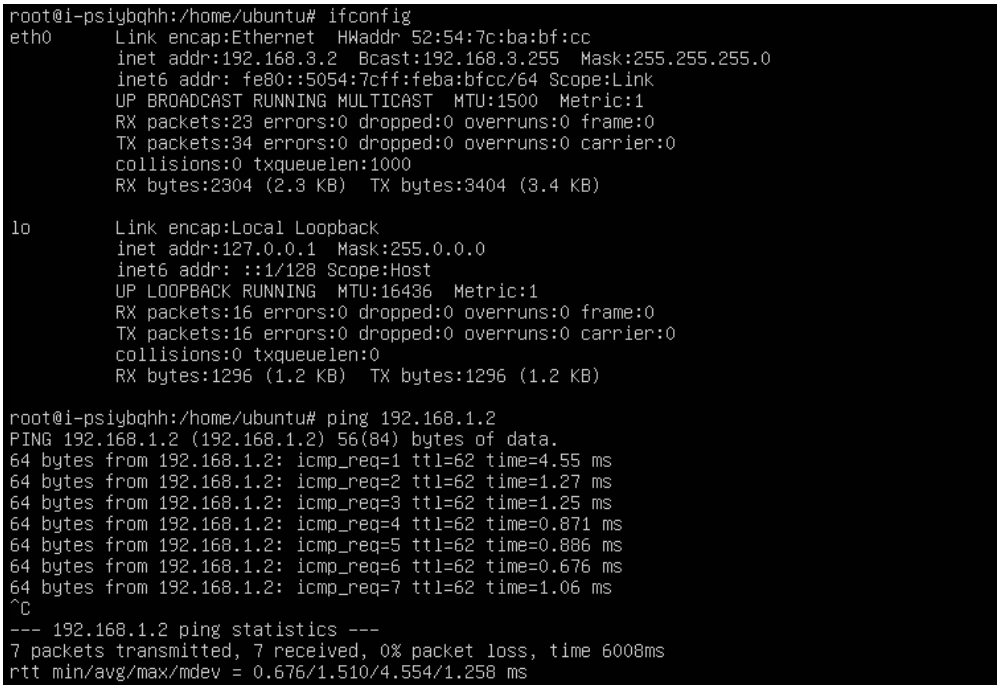
8. Aplique la política IPsec a la subinterfaz.

```
interface GigabitEthernet0/0/2.64
IPsec policy vpnIPsec64
q
```

9. Prueba de conectividad.

   Pruebe la conectividad entre sus ECS en la nube y los servidores en su centro de datos local, como se muestra en **Figura 17-20**.

Figura 17-20 Prueba de conectividad



17.6.5 ¿Cómo debo configurar un gateway local cuando uso una VPN para conectarme a la nube?

Determine las subredes locales, las subredes de VPC y las direcciones IP de gateway en ambos extremos.

Configure las políticas IPsec en el gateway local de acuerdo con las políticas IPsec configuradas en la nube. Agregue reglas al grupo de seguridad asociado con la VPC para permitir paquetes ICMP tanto en las direcciones entrantes como salientes.

- Configuración de ruta: agregue rutas que comiencen desde el gateway local y que destinen al gateway de VPN. El siguiente salto de la ruta en el gateway de VPN es la dirección IP del gateway pública en la dirección de salida.
- Configuración de NAT: En el gateway local, deshabilite NAT para las subredes locales que tendrán acceso a las subredes de VPC. Agregar reglas de grupo de seguridad para permitir el acceso mutuo entre las subredes locales y las subredes de VPC, y permitir el UDP 500, UDP 4500, Los paquetes ESP (protocolo IP 50) y AH (protocolo IP 51) desde y hacia las direcciones IP del gateway de VPN en la nube y el gateway local.

17.6.6 ¿Puede Huawei Cloud VPN conectarse a un gateway remoto a través de un nombre de dominio?

No. Una conexión de VPN solo puede conectarse a un gateway remota con la dirección IP pública del gateway.

17.6.7 ¿Cuántos túneles tiene mi conexión de VPN?

El número de túneles en una conexión de VPN = El número de subredes locales x El número de subredes remotas de la conexión de VPN

El estado de una conexión de VPN es normal siempre que uno de los túneles esté en el estado activo. Si necesita que cada túnel esté en el estado activo, los flujos de datos deben activarse entre cada dos subredes.

17.6.8 ¿Cómo permito que servidores específicos accedan a una subred de VPC por una conexión de VPN creada?

Configuraciones en el centro de datos local

- Configurar reglas de denegación en dispositivos VPN.
- Configure las reglas de ACL en el router o switch.

Configuraciones en la nube

- Configurar reglas de grupo de seguridad para denegar el acceso desde direcciones IP específicas.
- Configurar reglas de ACL.

NOTA

Todas las reglas deben agregarse al dispositivo antes de que se establezca el túnel de VPN. No cambie la subred local y la subred remota para restringir el acceso.

17.6.9 ¿Las VPN de Huawei Cloud tienen habilitado el mecanismo DPD?

Sí.

Las VPN en Huawei Cloud tienen el mecanismo DPD habilitado de forma predeterminada para detectar el estado del proceso IKE en el centro de datos local.

Después de tres fallos de detección consecutivos, Huawei Cloud considera que el proceso IKE en el centro de datos local es anormal. En este caso, Huawei Cloud elimina el túnel local para garantizar la sincronización del túnel entre los dos extremos.

El protocolo DPD no requiere que el extremo par esté configurado de forma síncrona, sino que requiere que el extremo par pueda responder a las detecciones DPD. Para asegurarse de que el estado del túnel de los dos extremos es consistente y evitar que un extremo tenga un túnel y el otro no, se recomienda que active el mecanismo DPD en su gateway local para detectar el estado del proceso IKE del servicio VPN en Huawei Cloud.

NOTA

Después de que el DPD falle, el túnel se eliminará sin afectar la estabilidad del servicio.

DPD puede detectar excepciones en el proceso IKE en el extremo del par en el tiempo y restablecer el túnel para garantizar la sincronización del túnel entre los dos extremos. Después de eliminar un túnel, si hay tráfico transmitido a través del túnel, el túnel se puede restablecer con la negociación.

17.6.10 ¿Cómo puedo usar grupos de seguridad para evitar que se acceda a ECS en una VPC a través de una VPN para implementar el aislamiento de seguridad?

Puede configurar grupos de seguridad para permitir el acceso solo a bloques CIDR o ECS específicos en una VPC con una VPN.

Ejemplo de configuración: Evite que los ECS de la subred 10.1.0.0/24 de VPC accedan a la subred local 192.168.1.0/24.

Procedimiento:

1. Cree los grupos de seguridad 1 y 2.
2. El grupo de seguridad 1 deniega el acceso desde la subred 192.168.1.0/24.
3. El grupo de seguridad 2 permite el acceso desde la subred 192.168.1.0/24.
4. Asociar ECS en la subred 10.1.0.0/24 con el grupo de seguridad 1 y asociar otros ECS en la VPC con el grupo de seguridad 2.

17.6.11 ¿Se restablecerá una conexión VPN después de que se modifique su configuración?

Una conexión de VPN consta de subredes locales, subredes remotas, gateway remoto, clave previamente compartida, políticas de negociación IKE y políticas de negociación IPsec. Una conexión de VPN se modifica si ocurre alguna de las siguientes situaciones:

- Si se modifican las subredes local y remota, el ID de conexión permanecerá sin cambios. Si no se actualizan todas las subredes, el túnel establecido entre las subredes no se restablecerá.
- Si se cambia la dirección IP del gateway remoto, incluso el ID de conexión permanecerá sin cambios, el extremo remoto ha cambiado. Por lo tanto, es necesario restablecer la conexión de VPN.
- Si solo se cambian las claves previamente compartidas de la conexión, el ID de conexión y el estado permanecerán sin cambios. Las claves se comprobarán de nuevo durante la renegociación. Si las claves no coinciden, la renegociación falla.
- Si se modifica la política de negociación (se requiere autenticación de clave previamente compartida), se cambiará el ID de conexión y se deberá restablecer la conexión.

17.6.12 ¿Por qué no puedo iniciar la negociación de Amazon Web Services con Huawei Cloud después de que estén interconectados?

Una vez establecida una conexión de VPN, Amazon Web Services (AWS) funciona en modo de respuesta y no inicia la negociación. Cuando un AWS EC2 accede a un Huawei Cloud ECS, la conexión de VPN no se activará para establecer una SA.

Según el documento de AWS, la negociación solo puede iniciarse desde el lado del cliente (en este caso, Huawei Cloud).

17.6.13 ¿Cómo configuro DPD para la interconexión con Huawei Cloud?

De forma predeterminada, DPD está habilitado en Huawei Cloud y no se puede deshabilitar.

Configure DPD de la siguiente manera:

- DPD-type: bajo demanda
- DPD idle-time: 30s

- DPD retransmit-interval: 15s
- DPD retry-limit: 3
- DPD msg: seq-hash-notify

El formato **DPD msg** en ambos extremos de la conexión de VPN debe ser el mismo, pero el tipo DPD, el tiempo de inactividad, el intervalo de retransmisión y el límite de reintentos pueden ser diferentes.

17.6.14 ¿Qué debo hacer si mi firewall no puede recibir paquetes de respuesta desde el gateway de Huawei Cloud VPN en la fase IKE?

1. Compruebe si las direcciones IP públicas de los dos extremos pueden comunicarse entre sí. Puede ejecutar el comando ping. De forma predeterminada, la dirección IP del gateway de VPN en Huawei Cloud se puede hacer ping.
2. El gateway local y el gateway de Huawei Cloud VPN pueden intercambiar paquetes en los puertos UDP 500 y 4500.
3. Asegúrese de que el número de puerto de origen no se traduce cuando la dirección IP pública local accede a la dirección IP del gateway en Huawei Cloud. Si existe NAT transversal, asegúrese de que el número de puerto no se cambiará después de NAT transversal.
4. La configuración del parámetro de negociación IKE en ambos extremos debe ser la misma. En el escenario NAT transversal, establezca el tipo de ID en el centro de datos local en IP y el ID local en Huawei Cloud en la dirección IP pública después de NAT.

17.6.15 ¿Qué debo hacer si mi firewall no puede recibir paquetes de respuesta de la subred VPN de Huawei Cloud?

1. Compruebe las rutas, las políticas de seguridad, la configuración de NAT, el tráfico interesante y las políticas de negociación para la negociación de la fase 2 en el dispositivo de gateway local.
   - Configuraciones de ruta: Enrute los datos para acceder a las subredes de la nube a los túneles.
   - Políticas de seguridad: permite el tráfico de subredes locales a subredes en la nube.
   - Políticas de NAT: no realice NAT cuando las subredes locales accedan a las subredes de la nube.
   - Tráfico interesante: el tráfico interesante en ambos extremos se configura de forma reflejada. El nombre del objeto de dirección no se puede utilizar para el tráfico interesante configurado con IKEv2.
   - Políticas de negociación: Garantizar que las políticas de negociación, especialmente las PFS, en ambos extremos sean las mismas.
2. Después de confirmar que tanto las negociaciones de la fase 1 como de la fase 2 son normales, asegúrese de que las reglas del grupo de seguridad en la nube permitan que las subredes locales accedan a las subredes de la nube mediante ICMP.

17.6.16 ¿Cuáles son los bits de los grupos DH utilizados por Huawei Cloud VPN?

Los grupos Diffie-Hellman (DH) determinan la fuerza de la clave utilizada en el proceso de intercambio de claves. Los números de grupo de DH más altos suelen ser más seguros, pero se requiere tiempo adicional para calcular la clave.

Tabla 17-5 enumera los bits correspondientes a los grupos DH usados por VPN.

Tabla 17-5 Bit correspondiente a cada grupo DH

Grupo DH	Módulo
1	768 bits
2	1024 bits
5	1536 bits
14	2048 bits
15	3072 bits
16	4096 bits
19	ecp256 bits
20	ecp384 bits
21	ecp521 bits

NOTA

Los siguientes algoritmos de DH tienen riesgos de seguridad y no se recomiendan: DH grupo 1, DH grupo 2 y DH grupo 5.

17.7 Error de conexión o de ping

17.7.1 ¿Por qué la conexión de VPN siempre está en el estado no conectado incluso después de que se complete su configuración?

Asegúrese de que las claves previamente compartidas y la información de negociación en ambos extremos sean consistentes. Las subredes locales y el gateway de VPN en la nube son las subredes remotas y el gateway remoto en el centro de datos local. El gateway remotoy las subredes remotas en la nube son el gateway local y las subredes locales en el centro de datos local.

Asegúrese de que las rutas, NAT y las reglas de política de seguridad estén correctamente configuradas en su dispositivo de gateway local. A continuación, haga ping a los servidores en subredes en ambos extremos.

NOTA

La VPN se activa en función de los flujos de datos. Después de configurar VPN, haga ping a un dispositivo en la subred del par. Antes de ejecutar el comando ping, deshabilite la función de firewall en el dispositivo y permita paquetes ICMP entrantes en el grupo de seguridad en la nube.

Hacer ping a la dirección IP del gateway no puede activar la negociación de VPN. Hacer ping al servidor en la subred protegida por el gateway.

17.7.2 ¿Cómo puedo evitar las desconexiones de VPN?

Las conexiones de VPN se renegocian cuando la vida útil de la SA IPsec está a punto de expirar o cuando los datos transmitidos con una conexión de VPN superan los 20 GB. Por lo general, la renegociación no interrumpe las conexiones de VPN.

La mayoría de las desconexiones se deben a configuraciones incorrectas en los dos extremos de la conexión de VPN o a fallos de renegociación debidos a excepciones de Internet.

Las causas comunes para las desconexiones son las siguientes:

- Las ACL de los dispositivos en ambos extremos de la conexión de VPN no coinciden.
- La configuración de la vida útil de SA en ambos extremos de la conexión de VPN es diferente.
- DPD no está configurado en su centro de datos local.
- La configuración se modifica cuando la conexión de VPN está en uso.
- Los paquetes están fragmentados porque el tamaño de los datos excede la MTU.
- La fluctuación se produce en la red del operador.

Por lo tanto, asegúrese de que las siguientes configuraciones de VPN son correctas para mantener las conexiones de VPN activas:

- Las subredes locales y remotas son pares coincidentes.
- La configuración de la duración de la SA en ambos extremos de la conexión de VPN es la misma.
- DPD está habilitado en el dispositivo del gateway local y el número de veces de detección es de 5 o más.
- Los parámetros se modifican en ambos extremos de la conexión de VPN durante el uso de la conexión de VPN.
- Establezca TCP MAX-MSS en 1300 para el dispositivo del gateway local.
- El ancho de banda del gateway local es lo suficientemente grande para ser utilizado por la conexión de VPN.
- La negociación de conexión de VPN se puede activar por ambos extremos y la negociación activa se ha habilitado en el gateway local.
- Hacer ping a las subredes en ambos extremos continuamente. El script es el siguiente:

```
#!/bin/sh
host=$1
if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi
log_name=$host".log"

while :; do
    result=`ping -W 1 -c 1 $host | grep 'bytes from '`
    if [ $? -gt 0 ]; then
```



```
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a
$log_name
    else
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo
$result | cut -d ':' -f 2`"| tee -a $log_name
    fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

NOTA

1. Utilice el editor vi para copiar el script anterior en el archivo **ping.sh**.
2. Ejecute el comando **chmod 777 ping.sh** para conceder permisos al archivo.
3. Ejecute el comando ping:

   ./ping.sh *x.x.x.x* **>>/dev/null &**

   x.x.x.x indica la dirección IP que se va a hacer ping.
4. Ejecute el siguiente comando:

   tail -f *x.x.x.x***.log**

   Puede ver el resultado de ping en tiempo real.

17.7.3 ¿Cómo puedo restaurar rápidamente una conexión VPN IPsec interrumpida?

1. Activar la negociación IPsec mediante flujos de datos de red privada. Por ejemplo, dos redes privadas en ambos extremos de la conexión de VPN hacen ping entre sí. Si el tráfico se puede activar correctamente, desplegar un script de ping continuo. Para obtener más información, véase **¿Cómo puedo evitar las desconexiones de VPN?**.
2. Si no se puede activar la negociación, compruebe la conectividad a Internet haciendo ping a la dirección IP del gateway de VPN y a la dirección IP del gateway remoto. De forma predeterminada, el gateway de Huawei Cloud VPN responde a los paquetes ICMP.
3. Si Internet es normal, compruebe si se produce un conmutador de enlace entre varios gateway. Es decir, el tráfico para acceder a la dirección IP del gateway de Huawei Cloud no fluye desde los puertos negociados.
4. Si no hay varios puertos o la ruta de puerto es normal, cambie las PSK en ambos extremos del túnel para activar la negociación de nuevo.
5. Si la negociación falla, compruebe si las políticas de negociación configuradas en ambos extremos son consistentes y si el tráfico interesante en ambos extremos se refleja mutuamente.
6. Si las políticas de negociación y la configuración de tráfico interesante son correctas, detenga la conexión de VPN en el dispositivo local. Después de que el estado de la conexión en Huawei Cloud cambie a **Not connected**, restablezca la conexión de VPN en el dispositivo local y active el flujo de datos.
7. Si aún no se puede activar la negociación, realice las siguientes operaciones:

   a. Registre la política de negociación, PSK, subredes locales, gateway remoto y subredes remotas de la conexión de Huawei Cloud VPN.

   b. Utilice el gateway de VPN existente para crear otra conexión de VPN. La política de negociación, PSK y las subredes locales son las mismas que las de la conexión de VPN original. Configure aleatoriamente el gateway remoto y las subredes remotas.

c. Después de crear la nueva conexión de VPN, elimine la conexión de VPN original y cambie el gateway remoto y las subredes remotas de la nueva conexión de VPN a la información registrada.

d. Active la negociación de nuevo.

Si el estado del túnel IPsec sigue siendo anormal después de realizar las operaciones anteriores, **envíe un ticket de servicio** al servicio de atención al cliente de Huawei Cloud para obtener ayuda.

17.7.4 ¿Qué sucede si el ancho de banda de un gateway de VPN supera el tamaño que especifiqué cuando creo el gateway?

El ancho de banda del gateway de VPN se utiliza en la dirección de salida de una VPC. Si el ancho de banda excede el tamaño especificado, se producirá una congestión de la red, no se podrá acceder a algunas subredes o incluso se interrumpirá la conexión de VPN, ya que es posible que no se reciban los paquetes de detección de VPN.

En este caso, se recomienda aumentar el ancho de banda del gateway de VPN.

NOTA

El ancho de banda máximo de una conexión VPN es de 300 Mbit/s.

17.7.5 ¿Se establecerá automáticamente una conexión de VPN IPsec?

Después de completar las configuraciones en ambos extremos de una conexión de VPN IPsec, la conexión de VPN no se establecerá automáticamente solo después de que los datos fluyan entre los dos extremos de la conexión. Si no hay flujo de datos entre la nube y el centro de datos local, la conexión de VPN siempre estará en el estado inactivo. Cualquier dato generado al acceder a servidores o hacer ping entre servidores puede desencadenar el establecimiento de una conexión de VPN.

El establecimiento de una conexión de VPN se puede activar en cualquiera de las dos condiciones siguientes: El gateway de VPN y el gateway remoto activan automáticamente la negociación. Los servidores en la nube y en las instalaciones se acceden entre sí a través de la conexión de VPN que se va a establecer.

Sin embargo, el establecimiento automático de una conexión de VPN no puede ser activado por un gateway de VPN en Huawei Cloud. Verifique que el establecimiento de su conexión de VPN pueda ser activado por los flujos de datos entre los dos extremos de la conexión de VPN. Es decir, compruebe si se puede establecer una conexión de VPN después de hacer ping a un servidor en la nube desde un servidor local, y si se puede establecer una conexión de VPN después de desconectar la conexión y hacer ping a un servidor local desde un servidor en la nube.

NOTA

Las direcciones de origen y destino de los paquetes de ping deben estar protegidas por la VPN.

Antes de establecer una conexión de VPN, las direcciones IP del gateway en ambos extremos se pueden hacer ping. Sin embargo, hacer ping a las direcciones IP del gateway no activa el establecimiento de la conexión de VPN.

17.7.6 ¿Por qué los ECS en ambos extremos de una conexión VPN normal entre regiones no pueden acceder entre sí?

De forma predeterminada, un grupo de seguridad permite todo el tráfico saliente. Para permitir el tráfico entrante, agregue reglas entrantes al grupo de seguridad. Asegúrese de que el grupo de seguridad asociado con el ECS que necesita recibir paquetes de ping permita las solicitudes de ICMP entrantes.

17.7.7 ¿Por qué las subredes en ambos extremos de una conexión VPN normal no pueden acceder entre sí?

La conexión de VPN es normal, lo que indica que los parámetros de negociación en ambos extremos de la conexión de VPN son correctos. Debe realizar las siguientes operaciones:

- Verifique que las rutas al dispositivo de VPN en su centro de datos local estén correctamente configuradas.
- Compruebe que el intercambio de datos entre subred está permitido en el dispositivo de VPN.
- Compruebe que no se realiza NAT en las subredes locales que necesitan acceder a la nube.
- Verifique que se permita el acceso mutuo entre las direcciones IP públicas del gateway de VPN y el gateway del cliente.

17.7.8 ¿Qué hago si se interrumpe una conexión de VPN en uso y se muestra un mensaje que indica que el tráfico de direcciones IP no está en la lista blanca se genera?

Esto es causado generalmente por la falta de coincidencia de ACL entre los gateway local y remoto.

1. Compruebe si las subredes local y remota de la conexión de VPN son pares coincidentes. Asegúrese de que las reglas de ACL en ambos extremos de la conexión de VPN no entren en conflicto.
2. Utilice el formato de subred/máscara cuando configure tráfico interesante en su centro de datos local. No utilice el modo de objeto de dirección, ya que puede causar problemas de incompatibilidad.

17.7.9 ¿Qué hago si se interrumpe una conexión de VPN y se muestra un mensaje que indica que el DPD se agota?

Esto sucede porque no hay intercambio de datos a través de la conexión de VPN. Una vez finalizado el ciclo de vida de la SA, se eliminará la conexión de VPN si el extremo del mismo nivel no responde al DPD.

Solución

1. Habilite DPD en el dispositivo de gateway local y pruebe si los flujos de datos de ambos extremos pueden activar el establecimiento de conexión.
2. Despliegue el script de shell ping en los servidores en ambos extremos. También puede configurar el dispositivo de gateway local para mantener la conexión activa, por ejemplo, configurar NQA en dispositivos de Huawei o IP SLA en dispositivos de Cisco. Network

Quality Analysis (NQA) es una característica de Huawei que monitorea el rendimiento de la red en tiempo real y ayuda a diagnosticar fallas que ocurren en la red.

17.7.10 ¿Por qué el estado de una conexión de VPN no está conectado en la consola de gestión cuando ya está disponible?

Hay una latencia para mostrar el estado más reciente de la conexión de VPN en la consola de gestión.

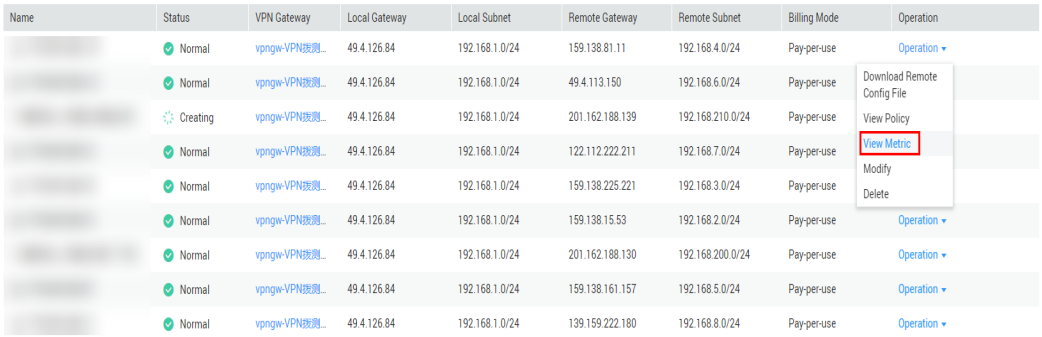
Si el acceso al servicio es normal, se establece la conexión de VPN.

17.7.11 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía automáticamente notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Después de crear una conexión de VPN, puede localizar la fila que contiene la conexión de VPN y elegir **Operation** > **View Metric** para ver el estado de la conexión de VPN.

Figura 17-21 Ver métrica



17.7.12 ¿Qué puedo hacer si la configuración de la conexión de VPN falla?

1. Compruebe las políticas IKE e IPsec para ver si los modos de negociación y los algoritmos de encriptación en ambos extremos de la conexión de VPN son los mismos.
   a. Si la política IKE se ha configurado durante la fase uno y la política IPsec no se ha habilitado en la fase dos, las políticas IPsec en ambos extremos de la conexión de VPN pueden ser inconsistentes.
   b. Si utiliza un dispositivo físico de Cisco en su centro de datos local, se recomienda que utilice MD5 y establezca **Authentication Mode** en **MD5** al configurar la política IPsec para la conexión de VPN en la nube.
2. Compruebe si las reglas 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 para permitir la comunicación con las subredes de VPC. A continuación se proporciona un ejemplo de configuraciones de ACL:

   ```
   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
```

3. Compruebe si la conexión de VPN es normal haciendo ping al extremo local desde el extremo remoto y haciendo ping al extremo remoto desde el extremo local.

17.7.13 ¿Qué debo hacer si no puedo acceder a los ECS en la nube desde mi centro de datos local o LAN después de que se haya configurado la conexión de VPN?

El grupo de seguridad deniega el acceso desde todos los orígenes de forma predeterminada. Si desea acceder a sus ECS, modifique las reglas del grupo de seguridad y permita el acceso desde las subredes locales.

17.7.14 ¿Por qué se muestra Not Connected como el estado de una conexión de VPN creada correctamente?

Después de crear una conexión de VPN, su estado cambia a **Normal** solo después de que los servidores de ambos extremos de la conexión de VPN se comuniquen entre sí.

- IKE v1:

  Si no pasa tráfico con la conexión de VPN durante un período de tiempo, la conexión de VPN debe renegociarse. El tiempo de negociación depende del valor **Lifecycle (s)** en la política IPsec. Generalmente, **Lifecycle (s)** se establece en **3600** (1 hora), lo que indica que la negociación se iniciará en el minuto cincuenta y cuarto. Si la negociación es correcta, la conexión se mantiene hasta la siguiente ronda de negociación. Si la negociación falla, el estado de la conexión de VPN cambia a **Not Connected** en una hora. La conexión se puede restaurar solo después de que los dos extremos de la conexión de VPN se comuniquen entre sí. La desconexión se puede evitar usando una herramienta de monitorización de red, tal como IP SLA, para generar paquetes.
- IKE v2: si no pasa tráfico con la conexión de VPN durante un período de tiempo, la conexión de VPN permanece en el estado conectado.

17.7.15 ¿Las VPN de Huawei Cloud tienen habilitado el mecanismo DPD?

Sí.

Las VPN en Huawei Cloud tienen el mecanismo DPD habilitado de forma predeterminada para detectar el estado del proceso IKE en el centro de datos local.

Después de tres fallos de detección consecutivos, Huawei Cloud considera que el proceso IKE en el centro de datos local es anormal. En este caso, Huawei Cloud elimina el túnel local para garantizar la sincronización del túnel entre los dos extremos.

El protocolo DPD no requiere que el extremo par esté configurado de forma síncrona, sino que requiere que el extremo par pueda responder a las detecciones DPD. Para asegurarse de que el estado del túnel de los dos extremos es consistente y evitar que un extremo tenga un túnel y el otro no, se recomienda que active el mecanismo DPD en su gateway local para detectar el estado del proceso IKE del servicio VPN en Huawei Cloud.

NOTA

Después de que el DPD falle, el túnel se eliminará sin afectar la estabilidad del servicio.

DPD puede detectar excepciones en el proceso IKE en el extremo del par en el tiempo y restablecer el túnel para garantizar la sincronización del túnel entre los dos extremos. Después de eliminar un túnel, si hay tráfico transmitido a través del túnel, el túnel se puede restablecer con la negociación.

17.8 EIP

17.8.1 ¿Se puede retener una dirección IP de gateway de VPN después de que se elimine el gateway de VPN?

No. La dirección IP del gateway de VPN se liberará después de que se elimine el gateway de VPN.

Al eliminar un gateway de VPN también se eliminarán los recursos asociados con el gateway.

AVISO

La eliminación de la última conexión de un gateway de VPN de pago por uso también eliminará el gateway. Si desea conservar la dirección IP, no elimine la última conexión de VPN.

17.8.2 ¿Se puede usar una EIP como una dirección IP de gateway de VPN?

No.

La dirección IP de un gateway de VPN tiene configuraciones preestablecidas y se asigna automáticamente cuando se crea el gateway de VPN. Una EIP no puede ser utilizada por un gateway de VPN.

17.8.3 ¿Necesito comprar las EIP para servidores que se comunican entre sí a través de una VPN?

Si su servidor local necesita acceder a un ECS en la nube con una VPN, no necesita comprar una EIP.

Si el ECS necesita proporcionar servicios accesibles desde Internet, se requiere una EIP.

17.8.4 ¿Por qué un ECS tiene información de acceso de EIP después de habilitar una VPN?

Esto ocurre porque el ECS tiene una EIP enlazada antes de que se use la VPN. Es decir, puede acceder al ECS con la VPN o la EIP.

Una vez establecida la VPN, el tráfico de los servidores que cumplen con las reglas de ACL puede entrar en el túnel para acceder a los ECS.

- Si una EIP está vinculada a un ECS, los dispositivos en una red que no sea VPN pueden acceder al ECS usando la EIP.
- Si solo se puede acceder al ECS con una VPN, desvincule la EIP del ECS después de que la conexión de VPN esté activa. Cuando un ECS necesita una EIP, puede usar reglas de ACL para especificar el tráfico que puede acceder al ECS a través de la EIP.

NOTA

Retener una EIP o no depende de sus servicios. Si se utiliza un ECS para acceder a un centro de datos local con una VPN, y también se utiliza para proporcionar servicios accesibles desde Internet, su EIP debe conservarse.

17.8.5 ¿Puede mi gateway local no tener una dirección IP pública fija?

No.

Para conectar su centro de datos local a Huawei Cloud con una VPN, su centro de datos local debe tener una dirección IP pública fija o una dirección IP pública fija después de NAT.

NOTA

Los routers de banda ancha domésticos comunes, los terminales móviles personales y los servicios de VPN (como L2TP) proporcionados por los hosts de Windows no pueden interconectarse con Huawei Cloud VPN.

17.9 Configuraciones de ruta

17.9.1 ¿Qué es un gateway remoto y una subred remota en una conexión de VPN?

Al crear una conexión de VPN, una subred en Huawei Cloud VPC es la subred local y el gateway de VPN creada es el gateway local. La subred y el gateway conectadas en el centro de datos local es la subred remota y el gateway remoto.

Una dirección IP de gateway remota es una dirección IP pública.

17.9.2 ¿Dónde puedo agregar rutas en la consola de VPN para llegar a las subredes remotas?

Cuando se crea una conexión de VPN, las rutas se entregan automáticamente para llegar a las subredes remotas.

17.9.3 ¿Necesito agregar una ruta para un ECS con varias NICs para llegar a la red local?

- Si se utiliza una NIC principal para establecer una VPN con la red local, no es necesario agregar ninguna ruta.
- Si se utiliza una NIC no primaria para establecer una VPN con la red local, agregue una ruta para llegar al gateway de la NIC no primaria.

17.10 Configuración de subred

17.10.1 ¿Cuáles son las precauciones para configurar las subredes locales y remotas de una conexión VPN?

- Puede configurar hasta 5 subredes locales. El producto del número de subredes locales y el número de subredes remotas no puede exceder de 225. Si se supera la 225, considere la posibilidad de crear superredes en las subredes locales o remotas.
- La subred local no puede incluir el bloque CIDR de la subred remota. La subred remota puede incluir el bloque CIDR de la subred local.
- Hay rutas que apuntan a las subredes locales en la VPC donde reside el gateway de VPN.
- Si hay dos conexiones (conexión A y conexión B) creadas para un gateway de VPN, y la subred remota de la conexión A está dentro de la de la conexión B, cuando la red de destino a la que se va a acceder pertenece al bloque CIDR solapado, la conexión creada primero se hace coincidir primero. Independientemente del estado de la conexión. (La coincidencia de longitud de máscara no se utiliza para la VPN basada en políticas.)

17.10.2 ¿Cuántas subredes locales y remotas puedo agregar a una VPN? ¿Por qué se muestra un mensaje de error cuando actualizo la subred local especificando un bloque CIDR?

- Puede configurar hasta 5 subredes locales. El producto del número de subredes locales y el número de subredes remotas no puede exceder de 225.
- Una VPC ofrece rutas de subred de VPC basadas en subredes remotas de una conexión de VPN, subredes remotas de una conexión de Direct Connect, subredes de una interconexión de VPC y subredes de una conexión de Cloud Connect. Cada subred tiene una ruta.
- El número de rutas de subred de VPC no puede exceder de 200. Es decir, en una VPC, el número total de subredes remotas de una conexión de VPN, subredes remotas de una conexión de Direct Connect, subredes de una interconexión de VPC y subredes de una conexión de Cloud Connect y rutas personalizadas no puede exceder de 200.

17.10.3 ¿Qué hago si ocurre una excepción cuando agrego una subred remota durante la creación de una conexión de VPN?

Compruebe si esta subred remota se ha utilizado como destino de una ruta de conexión de interconexión de VPC, de Cloud Connect o de Direct Connect, lo que provoca conflictos de ruta. Si es así, elimine la ruta y cree una nueva.

17.10.4 ¿Se puede retener una dirección IP de gateway de VPN después de que se elimine el gateway de VPN?

No. La dirección IP del gateway de VPN se liberará después de que se elimine el gateway de VPN.

Al eliminar un gateway de VPN también se eliminarán los recursos asociados con el gateway.

AVISO

La eliminación de la última conexión de un gateway de VPN de pago por uso también eliminará el gateway. Si desea conservar la dirección IP, no elimine la última conexión de VPN.

17.10.5 ¿Cómo planifico el bloque CIDR de una VPC a la que se accede por una conexión de VPN?

- El bloque CIDR de VPC no puede entrar en conflicto con el bloque CIDR local.
- Para evitar conflictos con 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.

17.10.6 ¿Cómo se asigna una dirección IP de gateway de VPN?

La dirección IP del gateway de VPN de Huawei Cloud es un grupo de direcciones IP planificadas antes de comprar los gateway de VPN. Estas direcciones IP están preestablecidas con las configuraciones de VPN.

Cuando compra un gateway de VPN, el sistema asigna aleatoriamente una dirección IP y la vincula a la VPC que seleccionó. Esta dirección IP solo puede estar vinculada a una VPC.

La dirección IP del gateway de VPN tiene datos preestablecidos. Por lo tanto, no es intercambiable con una EIP, y no puede especificar una EIP como la dirección IP del gateway de VPN cuando está comprando el gateway de VPN. La dirección IP del gateway de VPN solo se puede asignar aleatoriamente desde el grupo de direcciones IP VPN preestablecido. Cuando se elimina un gateway de VPN, se libera la relación de enlace entre la dirección IP de gateway y la VPC de gateway. Cuando se compra un nuevo gateway de VPN, el sistema asigna aleatoriamente una nueva dirección IP de gateway.

17.11 Tráfico interesante de VPN

17.11.1 ¿Necesito configurar las reglas de ACL en la consola de gestión de Huawei Cloud después de configurar las reglas de ACL en el dispositivo de gateway local?

Necesita crear reglas de ACL dedicadas para su dispositivo de gateway local. Las políticas IPsec harán referencia a las reglas de ACL.

Cuando configure la VPN en la nube, las reglas de ACL se generarán automáticamente en función de las subredes locales y remotas introducidas en la consola de gestión y luego se entregarán al gateway de VPN.

(Huawei Cloud) El número de reglas de ACL = El número de subredes locales x El número de subredes remotas

17.11.2 ¿Cómo configuro y modifico el tráfico interesante de una VPN en la nube?

El tráfico interesante se genera cuando la subred local y la subred remota se comunican entre sí mediante la topología de malla completa. Por ejemplo, hay dos subredes locales A y B, y

tres subredes remotas C, D y E. Las reglas de ACL para el tráfico interesante son las siguientes:

```
rule 1 permit ip source A destination C
rule 2 permit ip source A destination D
rule 3 permit ip source A destination E
rule 4 permit ip source B destination C
rule 5 permit ip source B destination D
rule 6 permit ip source B destination E
```

Si modifica la subred local y la subred remota en la consola de gestión, el tráfico interesante del dispositivo VPN se actualiza automáticamente. Es decir, se modifican las reglas de ACL en la nube.

17.12 Mantener la conexión de VPN activa

17.12.1 ¿Cómo puedo evitar las desconexiones de VPN?

Las conexiones de VPN se renegocian cuando la vida útil de la SA IPsec está a punto de expirar o cuando los datos transmitidos con una conexión de VPN superan los 20 GB. Por lo general, la renegociación no interrumpe las conexiones de VPN.

La mayoría de las desconexiones se deben a configuraciones incorrectas en los dos extremos de la conexión de VPN o a fallos de renegociación debidos a excepciones de Internet.

Las causas comunes para las desconexiones son las siguientes:

- Las ACL de los dispositivos en ambos extremos de la conexión de VPN no coinciden.
- La configuración de la vida útil de SA en ambos extremos de la conexión de VPN es diferente.
- DPD no está configurado en su centro de datos local.
- La configuración se modifica cuando la conexión de VPN está en uso.
- Los paquetes están fragmentados porque el tamaño de los datos excede la MTU.
- La fluctuación se produce en la red del operador.

Por lo tanto, asegúrese de que las siguientes configuraciones de VPN son correctas para mantener las conexiones de VPN activas:

- Las subredes locales y remotas son pares coincidentes.
- La configuración de la duración de la SA en ambos extremos de la conexión de VPN es la misma.
- DPD está habilitado en el dispositivo del gateway local y el número de veces de detección es de 5 o más.
- Los parámetros se modifican en ambos extremos de la conexión de VPN durante el uso de la conexión de VPN.
- Establezca TCP MAX-MSS en 1300 para el dispositivo del gateway local.
- El ancho de banda del gateway local es lo suficientemente grande para ser utilizado por la conexión de VPN.
- La negociación de conexión de VPN se puede activar por ambos extremos y la negociación activa se ha habilitado en el gateway local.
- Hacer ping a las subredes en ambos extremos continuamente. El script es el siguiente:


```
#!/bin/sh
host=$1
if [ -z $host ]; then
    echo "Usage: `basename $0` [HOST]"
    exit 1
fi
log_name=$host".log"

while :; do
    result=`ping -W 1 -c 1 $host | grep 'bytes from '`
    if [ $? -gt 0 ]; then
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is down"| tee -a
$log_name
    else
        echo -e "`date +'%Y/%m/%d %H:%M:%S'` - host $host is ok -`echo
$result | cut -d ':' -f 2`"| tee -a $log_name
    fi
sleep 5 # avoid ping rain
done
#./ping.sh x.x.x.x >>/dev/null &
```

NOTA

1. Utilice el editor vi para copiar el script anterior en el archivo **ping.sh**.
2. Ejecute el comando **chmod 777 ping.sh** para conceder permisos al archivo.
3. Ejecute el comando ping:

   ./ping.sh *x.x.x.x* **>>/dev/null &**

   x.x.x.x indica la dirección IP que se va a hacer ping.
4. Después de ejecutar el comando ping, se genera el archivo *x.x.x.x***.log**. Ejecute el siguiente comando:

   tail -f *x.x.x.x***.log**

   Puede ver el resultado de ping en tiempo real.

17.13 Monitoreo

17.13.1 ¿Qué recursos de VPN se pueden monitorear?

VPN Gateway

La información de ancho de banda que se puede supervisar incluye el tráfico entrante, el ancho de banda entrante, el tráfico saliente, el ancho de banda saliente y el uso del ancho de banda saliente.

Para ver las métricas del gateway de VPN, localice el gateway de VPN de destino y haga clic en **View Metric** en la columna **Operation**.

VPN Connection

El estado de la conexión de VPN puede ser monitoreado.

El valor **1** indica que la conexión es normal.

El valor **0** indica que la conexión no está conectada.

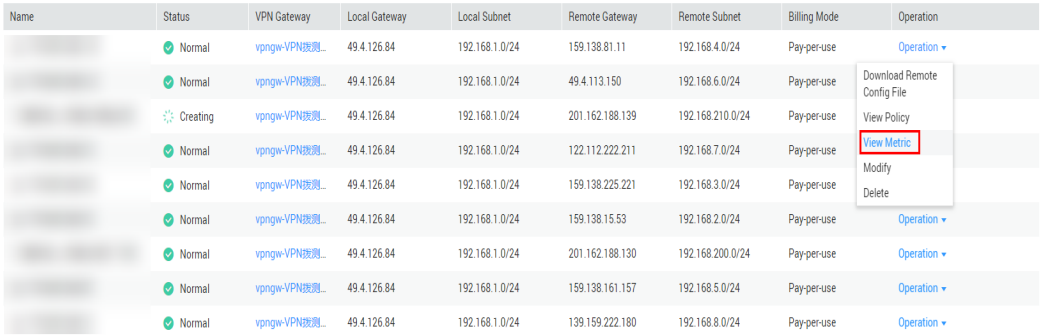
Para ver el estado de la conexión de VPN, localice la conexión de VPN de destino y haga clic en **View Metric** en la columna **Operation**.

17.13.2 ¿Se me notificará si se interrumpe una conexión de VPN?

El estado de la conexión de VPN puede ser monitoreado. Después de crear una conexión de VPN, el servicio VPN informa de la información del estado de la conexión a Cloud Eye, pero no le envía automáticamente notificaciones de alarma. Para recibir notificaciones, cree reglas de alarma y habilite **Alarm Notification** en la consola de Cloud Eye.

Después de crear una conexión de VPN, puede localizar la fila que contiene la conexión de VPN y elegir **Operation** > **View Metric** para ver el estado de la conexión de VPN.

Figura 17-22 Ver métrica



17.13.3 ¿Puedo ver el tráfico de cada conexión de VPN?

No. La monitorización del tráfico de VPN tiene que ver con el gateway de VPN. Puede ver el tráfico entrante y saliente, así como los anchos de banda entrante y saliente de un gateway de VPN, pero no puede ver el uso del tráfico de una conexión de VPN específica.

17.13.4 ¿Se me notificará cuando el resultado de monitoreo de VPN sea anormal?

Sí.

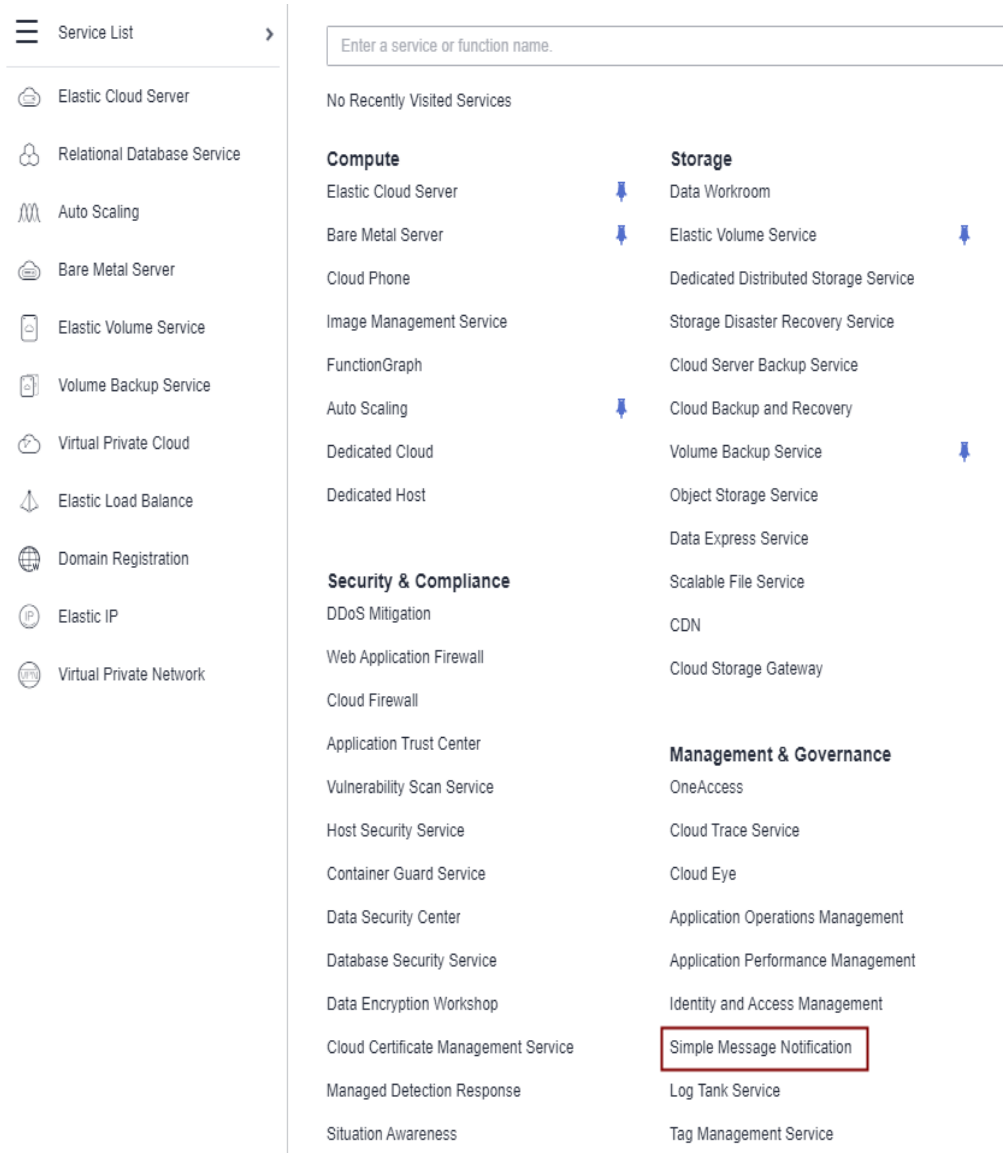
Puede configurar, en las consolas de Simple Message Notification (SMN) y de Cloud Eye, para recibir notificaciones si se producen resultados anormales de supervisión de VPN.

Creación de temas y adición de suscripciones en la consola de SMN

1. Inicie sesión en la consola de gestión.

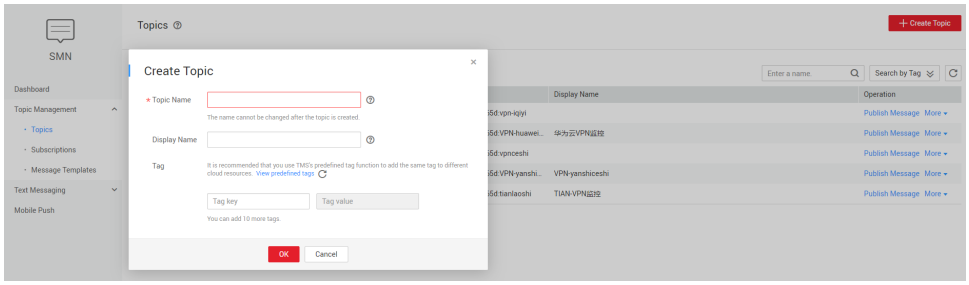
   En **Management & Governance**, seleccione **Simple Message Notification**.

Figura 17-23 Simple Message Notification



2. Elija **Topic Management** > **Topics** y haga clic en **Create Topic** para crear un tema, por ejemplo, **VPN-huaweicloud**.

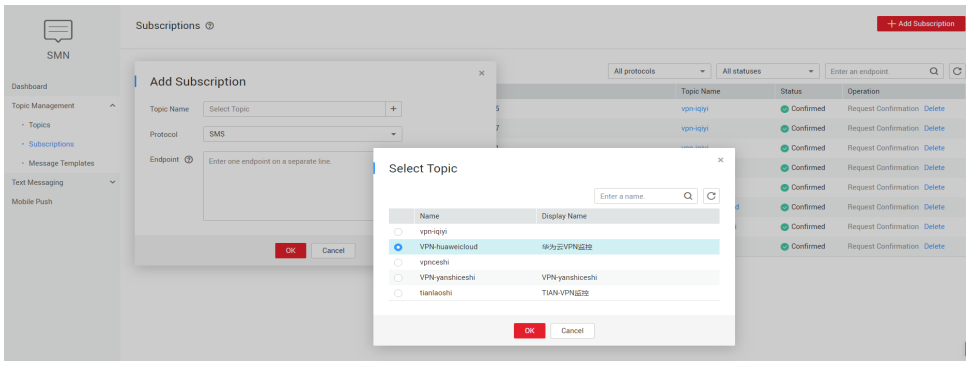
Figura 17-24 Crear tema



3. Elija **Topic Management** > **Subscriptions** y haga clic en **Add Subscription**.

   Seleccione un tema, establezca **Protocol** en **Email** e introduzca una dirección de correo electrónico para recibir notificaciones de alarma en el cuadro **Endpoint**.

Figura 17-25 Agregar suscripción



NOTA

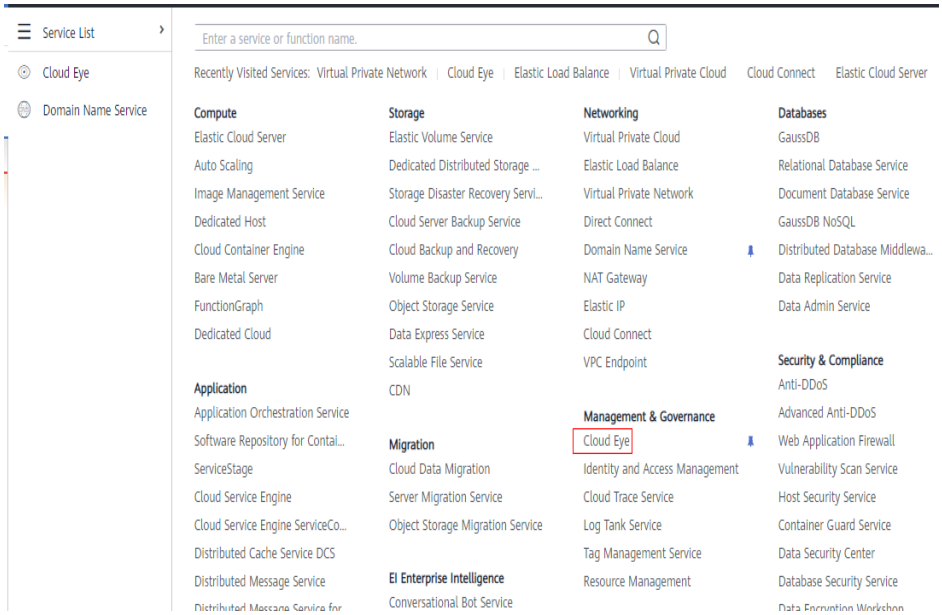
Después de agregar la suscripción, el sistema enviará un correo electrónico de confirmación a su dirección de correo electrónico. Confirme la suscripción en su correo electrónico.

Creación de reglas de alarma de VPN en la consola de Cloud Eye

1. Inicie sesión en la consola de gestión.

   En **Management & Governance**, seleccione **Cloud Eye**.

Figura 17-26 Cloud Eye



2. Cree una regla de alarma para supervisar el uso del ancho de banda de un gateway de VPN.

   Introduzca un nombre de regla de alarma, seleccione **Elastic IP and Bandwidth** para **Resource Type**, establezca **Dimension** en **Bandwidths**, **Monitoring Scope** en **Specific resources** y seleccione el gateway de VPN de destino, establezca **Method** en **Create manually** y **Alarm Policy** en **Outbound Bandwidth Usage**, **5 consecutive periods**, **>** y **90**. Establezca **Notification Object** en un tema SMN y utilice la configuración predeterminada para otros parámetros.

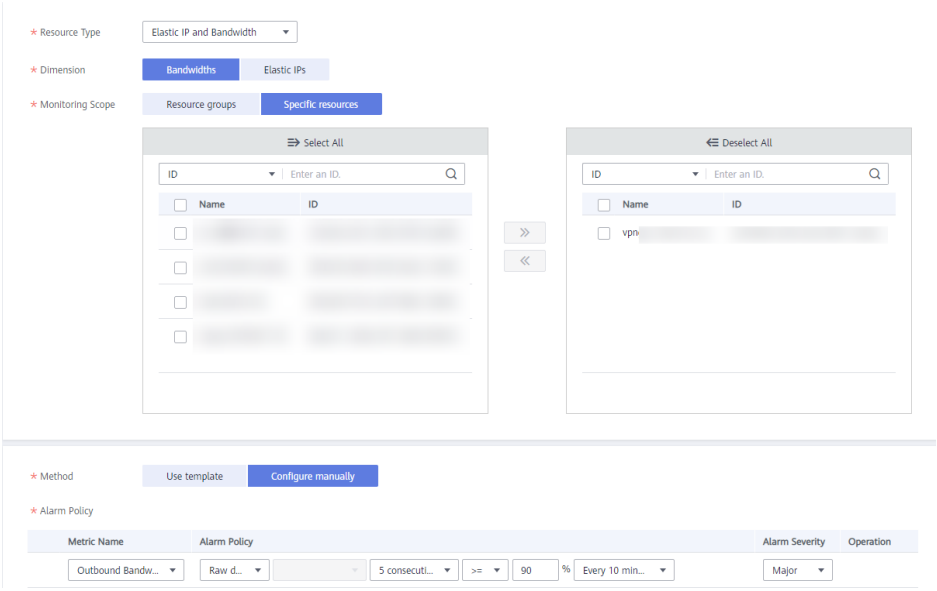
3. Cree una regla de alarma para supervisar el estado de la conexión de VPN.

   El proceso de creación es similar al del ancho de banda. Seleccione **Virtual Private Network** para **Resource Type**, establezca **Dimension** en **VPN connections**, **Monitoring Scope** en **Specific resources** y seleccione la conexión de VPN de destino, establezca **Method** en **Create manually** y **Alarm Policy** en **VPN Connection Status**, **<** y **1**. Establezca **Notification Object** en un tema SMN y utilice la configuración predeterminada para otros parámetros.

4. Cree una regla de alarma para supervisar sus vínculos locales.

   Cree una tarea de supervisión de sitios web, establezca **Type** en **PING**, **URL** a la dirección IP del gateway de su centro de datos local y conserve la configuración predeterminada para otros parámetros. Cree una regla de alarma, seleccione **Website Monitoring** para **Resource Type**, establezca **Monitoring Scope** en **Specific resources** y seleccione la tarea de supervisión del sitio web de destino, establezca **Method** en **Create manually**, y **Alarm Policy** en **Available Monitoring Location Count** y configure otro parámetro según sea necesario. Establezca **Notification Object** en un tema SMN y utilice la configuración predeterminada para otros parámetros.

Figura 17-27 Creación de una regla de alarma



17.14 Ancho de banda y velocidad de red

17.14.1 ¿Cuál es la velocidad de red real de una conexión de VPN?

Se ha creado una conexión de VPN. Se han creado dos ECS con uno en el extremo local y el otro en el extremo remoto. Los dos ECS pueden hacer ping entre sí.

Realice los siguientes pasos para probar la velocidad de red de su gateway de VPN si el ancho de banda de su gateway de VPN es de 200 Mbit/s:

1. Si los ECS en los dos extremos de la VPN ejecutan Windows, use iPerf3 y FileZilla (una aplicación de FTP gratuita para cargar y descargar archivos) para probar la velocidad de la red.

> **NOTA**
>
> La prueba muestra que la velocidad media de red de la VPN es de 180 Mbit/s, y hay alrededor del 10% de desviación de velocidad de red. Los protocolos de TCP y de FTP tienen el mecanismo de control de congestión, y el protocolo de IPsec agrega un nuevo encabezado IP. Por lo tanto, aproximadamente un 10% de desviación de velocidad de red es normal para la red de VPN.

Figura 17-28 muestra el resultado de la prueba.

Figura 17-28 Resultado de la prueba para 200 Mbit/s de ancho de banda (cliente de iPerf3)

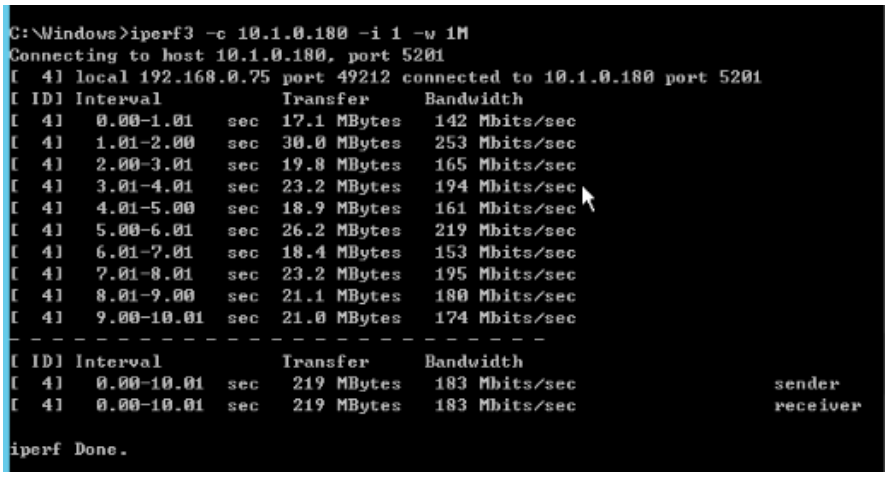
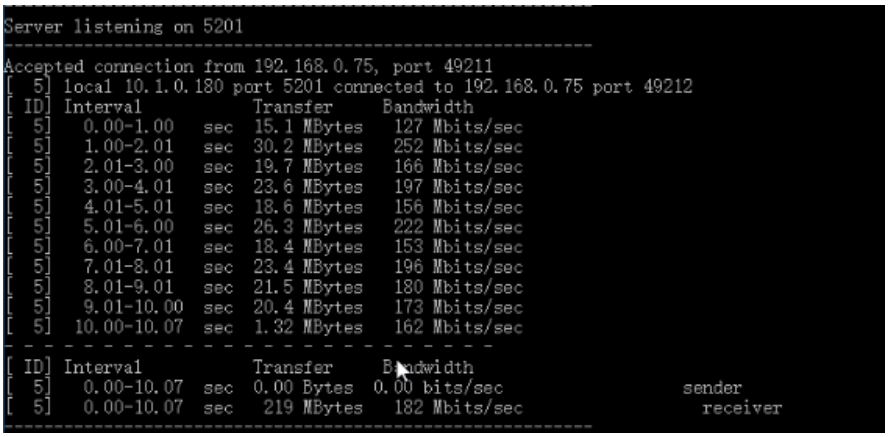


Figura 17-29 muestra el resultado de la prueba.

Figura 17-29 Resultado de la prueba para un ancho de banda de 200 Mbit/s (servidor de iPerf3)

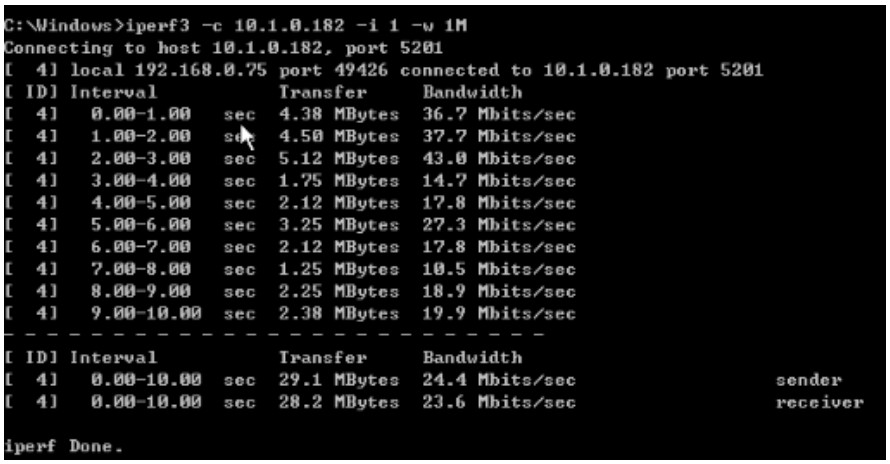


2. Si los ECS en los dos extremos de la VPN ejecutan CentOS 7, use iPerf3 para probar la velocidad de la red. La velocidad de la red puede alcanzar los 180 Mbit/s.
3. Si el ECS que funciona como el servidor ejecuta CentOS 7, y el ECS que funciona como el cliente ejecuta Windows, utilice iPerf3 y FileZilla para probar la velocidad de la red.

   La velocidad de red es de unos 20 Mbit/s, una velocidad de red lenta. Esto se debe a que las implementaciones TCP en Windows y en Linux son diferentes. Por lo tanto, si los ECS en los dos extremos de la VPN ejecutan diferentes sistemas operativos, la velocidad de red VPN no cumple con los requisitos de ancho de banda.

   Figura 17-30 muestra el resultado de la prueba.

Figura 17-30 Resultado de la prueba cuando los ECS en los dos extremos ejecutan diferentes sistemas operativos (iPerf3)



Realice los siguientes pasos para probar la velocidad de red de su gateway de VPN si el ancho de banda de su gateway de VPN es de 1,000 Mbit/s:

El ancho de banda del gateway de VPN es compartido por todas sus conexiones de VPN. Si el tamaño del ancho de banda es grande, se requieren múltiples ECS para probar el ancho de banda del gateway de VPN porque el rendimiento de reenvío de un ECS es limitado. Este escenario tiene altos requisitos en las especificaciones de ECS. Los ECS deben tener NIC que admitan el ancho de banda de 2 Gbit/s o superior.

Las pruebas muestran que la velocidad de red real de un gateway de VPN en Huawei Cloud está dentro del rango normal. Sin embargo, los servidores utilizados en ambos extremos de la conexión de VPN deben ejecutar los sistemas operativos del mismo tipo y las NIC del servidor deben cumplir los requisitos de configuración.

17.14.2 ¿Qué dirección del ancho de banda es limitado y cuál es la unidad del ancho de banda?

El ancho de banda del gateway de VPN comprado se utiliza en la dirección de salida. Para equilibrar el tráfico en las direcciones de entrada y salida, el ancho de banda en la dirección de entrada es limitado.

- Si el ancho de banda adquirido es de 10 Mbit/s o menos, el ancho de banda en la dirección de entrada está limitado a 10 Mbit/s.
- Si el ancho de banda adquirido es superior a 10 Mbit/s, el ancho de banda en la dirección de entrada es el mismo que el del ancho de banda adquirido.

La unidad de ancho de banda es Mbit/s y la del tráfico es GB.

17.14.3 ¿Cómo cambio el tamaño del ancho de banda de la VPN?

1. En la página **VPN Gateways**, busque la fila que contiene el gateway de VPN de destino y elija **More** > **Modify Bandwidth** en la columna **Operation**.
2. En la página **Modify Bandwidth**, seleccione el tamaño de ancho de banda requerido.
3. Haga clic en **Submit**.

17.14.4 ¿Qué sucede si el ancho de banda de un gateway de VPN supera el tamaño que especifiqué?

El ancho de banda del gateway de VPN se utiliza en la dirección de salida de una VPC. Si el ancho de banda excede el tamaño especificado, se producirá una congestión de la red, no se podrá acceder a algunas subredes o incluso se interrumpirá la conexión de VPN, ya que es posible que no se reciban los paquetes de detección de VPN.

En este caso, se recomienda aumentar el ancho de banda del gateway de VPN.

NOTA

El ancho de banda máximo de una conexión VPN es de 300 Mbit/s.

17.14.5 ¿Por qué el cambio de ancho de banda de VPN no tiene efecto?

Hay una latencia para que el cambio de ancho de banda de VPN surta efecto.

Pruebe el ancho de banda 5 minutos después de cambiar el ancho de banda.

NOTA

El cambio del ancho de banda de VPN no interrumpirá la ejecución de la carga de trabajo y las redes.

17.14.6 ¿Puede una VPN compartir ancho de banda con una EIP?

No.

Actualmente, una dirección IP pública se genera automáticamente y su ancho de banda se establece cuando se crea un gateway de VPN. La VPN no puede compartir ancho de banda con una EIP.

17.14.7 ¿Cuáles son las diferencias entre el ancho de banda de una conexión de VPN y el de una conexión de Direct Connect?

Conceptos

- El ancho de banda de una conexión de Direct Connect es el ancho de banda de la conexión creada por un usuario.
- El ancho de banda de conexión de VPN se refiere al ancho de banda en la dirección de salida.

Tamaño del ancho de banda

- El ancho de banda máximo predeterminado de una conexión de Direct Connect es Mbit/s de 1,000. Cuando crea una conexión en la consola de gestión y establece **Port Type** en **10GE single-mode optical port** el ancho de banda máximo es de 10 Gbit/s.
- El ancho de banda máximo de una conexión VPN es de 300 Mbit/s.

Calidad de la red

- Un usuario de Direct Connect tiene una conexión dedicada con una alta calidad de red.

- Las conexiones de VPN compartían el ancho de banda de su gateway de VPN. El ancho de banda total de las conexiones de VPN no puede exceder el ancho de banda de su gateway. La calidad de la red se verá afectada por la calidad de Internet.

17.14.8 ¿Cómo puedo determinar el tamaño del ancho de banda de mi VPN?

Tenga en cuenta lo siguiente cuando determine el ancho de banda:

- Cantidad de datos transmitidos a través de un túnel de VPN en un período de tiempo (Reserve suficiente ancho de banda para evitar la congestión del enlace.)
- El ancho de banda de salida al final de la conexión de VPN en la nube debe ser menor que al final de la conexión de VPN en el centro de datos local.

17.15 Cuotas

17.15.1 ¿Qué es la cuota de VPN?

¿Qué es una cuota?

Las cuotas pueden limitar el número o la cantidad de recursos disponibles para los usuarios, como el número máximo de ECS o discos de EVS que se pueden crear.

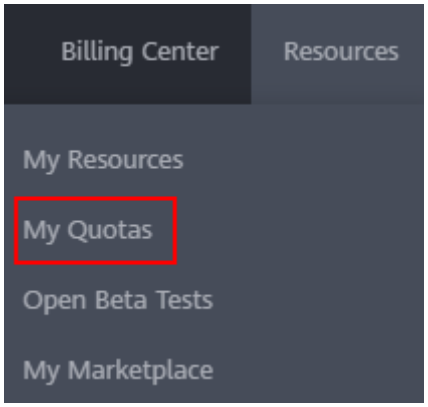
Si la cuota de recursos existente no puede cumplir con los requisitos de servicio, puede solicitar una cuota más alta.

¿Cómo puedo ver mi cuota?

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Elija **Resources** > **My Quotas** en la esquina superior derecha de la página.

   Se muestra la página **Service Quota**.

   Figura 17-31 Mis cuotas

4. Vea la cuota usada y total de cada tipo de recursos en la página mostrada.

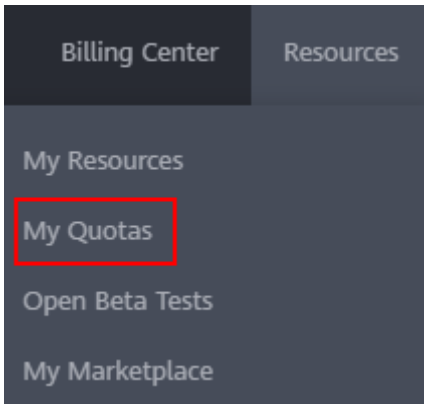
Si una cuota no puede cumplir con los requisitos de servicio, solicite una cuota más alta.

¿Cómo solicito una cuota más alta?

1. Inicie sesión en la consola de gestión.
2. Elija **Resources** > **My Quotas** en la esquina superior derecha de la página.

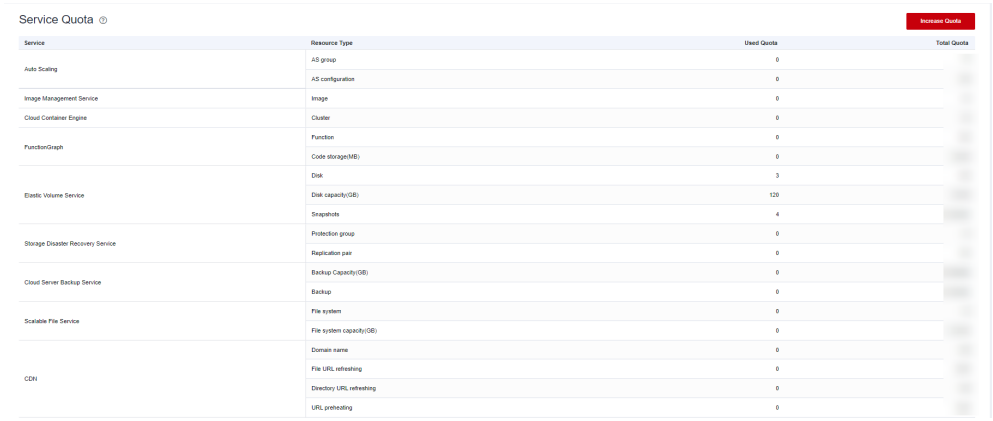
   Se muestra la página **Service Quota**.

   Figura 17-32 Mis cuotas

3. Haga clic en **Increase Quota** en la esquina superior derecha de la página.

   Figura 17-33 Solicitud de una cuota más alta

4. En la página **Create Service Ticket**, configure los parámetros según sea necesario.

   En el área **Problem Description**, introduzca la cuota requerida y el motivo del ajuste de cuota.
5. Seleccione el acuerdo y haga clic en **Submit**.

17.15.2 ¿Cuántos gateways y conexiones VPN puedo crear por defecto?

- VPN: De forma predeterminada, cada usuario puede crear hasta 50 gateways de VPN y 100 gateways remotos. Antes de comprar los gateway de VPN, compruebe su cuota restante. Si se ha alcanzado la cuota, **envíe un ticket de servicio** para solicitar un aumento de cuota.

- VPN clásica: De forma predeterminada, cada usuario puede crear dos gateway de VPN y 12 conexiones de VPN. Antes de comprar los gateway de VPN, compruebe su cuota restante. Si se ha alcanzado la cuota, **envíe un ticket de servicio** para solicitar un aumento de cuota.

17.15.3 ¿Cómo cambio mi gateway de VPN y las cuotas de conexión?

1. Inicie sesión en la consola de gestión. En la esquina superior derecha de la página, elija **Service Tickets** > **Create Service Ticket**.
2. En la página **Create Service Ticket**, haga clic en **Quotas** en el área **Services**.
3. Elija **Quota Application** en la sección **Issue Categories**.
4. Haga clic en **Create Now**.

   Ingrese la información requerida y haga clic en **Submit**.

17.15.4 ¿Cuántas VPN IPsec puedo tener?

De forma predeterminada, un usuario puede tener un máximo de cinco VPN IPsec. Si la cuota no puede cumplir con sus requisitos de servicio, solicite un aumento de cuota.

17.16 Permisos de la cuenta

17.16.1 ¿Se requiere un nombre de usuario y contraseña para crear una conexión de VPN IPsec?

No. Huawei Cloud IPsec VPN utiliza una clave precompartida (PSK) para la autenticación. La clave está configurada en un gateway de VPN. Se establecerá un túnel después de que se complete la negociación de VPN. Por lo tanto, no se requieren nombres de usuario y contraseñas.

En general, las VPN de Secure Sockets Layer (SSL), Point to Point Tunneling Protocol (PPTP) y Layer 2 Tunneling Protocol (L2TP) usan nombres de usuario y contraseñas para la autenticación.

NOTA

IPsec XAUTH es una tecnología extendida de IPsec VPN. Indica a los usuarios que introduzcan sus nombres de usuario y contraseñas durante la negociación de VPN.

Huawei Cloud VPN no es compatible con IPsec XAUTH.

17.16.2 ¿Qué debo hacer si el sistema muestra un mensaje que indica que no tengo los permisos para crear una VPN?

Compruebe si su cuenta es una cuenta de usuario de IAM. En caso afirmativo, realice operaciones en la consola de IAM como usuario de la cuenta de Huawei Cloud para autorizarle los permisos de operación de VPC. Asegúrese de que su cuenta tiene los permisos **VPC Administrator**, **Tenant Guest** y **VPN Administrator**.

17.16.3 ¿Cómo puedo determinar si mi cuenta no puede crear una VPN debido a permisos insuficientes?

- Los gateway de VPN y las conexiones creadas por la cuenta de Huawei Cloud son invisibles para las cuentas de usuario de IAM.
- Se mostrará un mensaje indicando que el sistema está ocupado si crea un gateway o conexión de VPN con una cuenta de usuario IAM.

Para obtener más información sobre los permisos necesarios para crear una conexión de VPN, consulte **¿Qué debo hacer si el sistema muestra un mensaje que indica que no tengo los permisos para crear una VPN?**.

