Virtual Private Network

Descripción general del servicio

Edición 01

Fecha 2023-01-11

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.

Índice

1 ¿Qué es Virtual Private Network?

Descripción general

Virtual Private Network (VPN) establece un túnel de comunicación cifrado basado en Internet entre su red y Virtual Private Cloud (VPC), para que pueda acceder a los recursos de la VPC de forma remota.

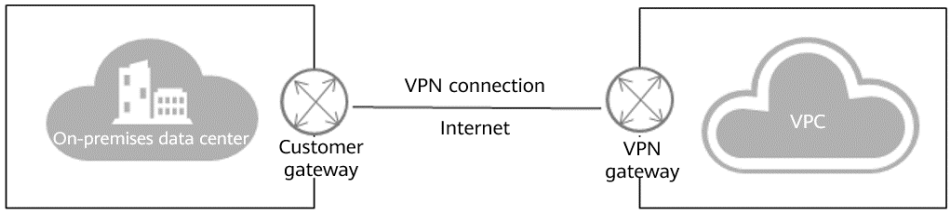
De forma predeterminada, los Elastic Cloud Servers (ECS) de una VPC no pueden comunicarse con dispositivos de su centro de datos local o red privada. Para habilitar la comunicación entre ellos, puede usar una VPN.

Una VPN consiste en una puerta de enlace VPN, una puerta de enlace de cliente y una o más conexiones VPN.

- Una puerta de enlace VPN proporciona una salida de Internet para que una VPC se conecte a una puerta de enlace de cliente en su centro de datos local.
- Una conexión VPN se cifra a través de Internet y vincula una puerta de enlace VPN a una puerta de enlace del cliente, lo que permite la comunicación entre una VPC y su centro de datos local. Esto ayuda a establecer rápidamente un entorno de nube híbrida seguro.

Figura 1-1 muestra la red de VPN.

Figura 1-1 Red de VPN



Componentes

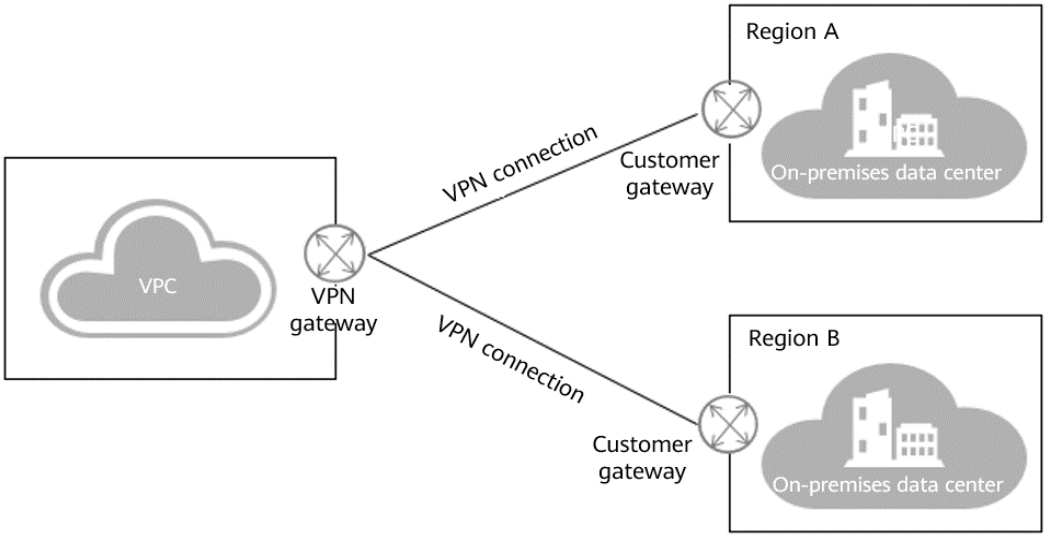
- **Puerta de enlace VPN**

  Una puerta de enlace de VPN es una puerta de enlace de salida para una VPC. Con una puerta de enlace 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 puerta de enlace de VPN funciona junto con una puerta de enlace de cliente en su centro de datos local. Se admiten conexiones VPN punto a punto y hub-and-spoke.

Figura 1-2 muestra la topología de las conexiones VPN de hub-and-spoke.

Figura 1-2 Topología de red



- **Puerta de enlace de cliente**

  Un dispositivo de puerta de enlace de cliente es un dispositivo físico o una aplicación de software en su lado de una conexión VPN. Una puerta de enlace de cliente es un recurso que se crea en la consola que representa un dispositivo de puerta de enlace de cliente y registra su información de configuración. Cuando crea una puerta de enlace de cliente, debe configurar su dirección IP pública, el tipo de enrutamiento, y protocolo de puerta de enlace de frontera (BGP) número de sistema autónomo (ASN).

- **Conexión de VPN**

  Una conexión VPN es un túnel de comunicación encriptada seguro y confiable de seguridad del protocolo de Internet (IPsec) establecido entre una puerta de enlace VPN y la puerta de enlace del cliente en un centro de datos local. Solo se admiten las VPN IPsec.

  Las conexiones VPN utilizan el Intercambio de claves de Internet (IKE) y los protocolos IPsec para cifrar de forma rentable y segura los datos transmitidos a través de Internet.

Acceso al servicio VPN

Puede acceder al servicio VPN a través de la consola de gestión basada en web.

- Si no tienes una cuenta, registra una cuenta en Huawei Cloud primero consultando a **Preparaciones**.

2 Ventajas del producto

VPN tiene las siguientes ventajas:

- **Seguridad de datos**

  El hardware propietario de Huawei utiliza IKE e IPsec para cifrar datos para proporcionar confiabilidad de clase operadora y garantizar una conexión VPN estable.
- **Escalamiento horizontal sin inconvenientes**

  Con VPN, puede conectar su centro de datos a su VPC y ampliar rápidamente los servicios desde el centro de datos a la nube, formando una nube híbrida.
- **Conexión de bajo costo**

  Las conexiones IPsec encriptadas por Internet brindan una alternativa rentable a las conexión Direct Connect.
- **Facilidad de uso**

  Puede crear una conexión VPN fácil de usar especificando parámetros en la consola y configurándolos en el centro de datos.

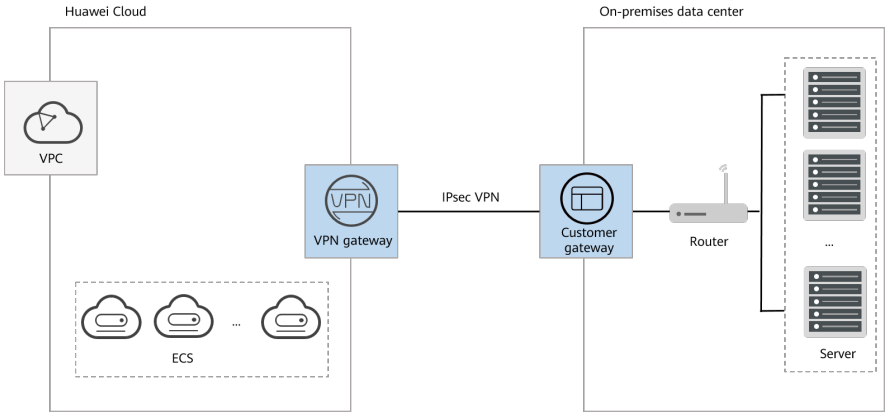
3 Escenarios de aplicación

Con una VPN entre una VPC y su centro de datos local, puede usar fácilmente recursos como ECS y almacenamiento en bloque en la nube. Sus aplicaciones locales se pueden migrar a la nube mientras sus datos principales se conservan en su centro de datos local. Sus servidores web se pueden escalar según sea necesario para cumplir con los requisitos informáticos siempre cambiantes, mientras que los costos de IT O&M se pueden reducir considerablemente.

Implementación de la nube híbrida

Puede utilizar una VPN para conectar su centro de datos local a una VPC en la nube y utilizar las capacidades de escalado rápido y elástico de la nube para ampliar las capacidades de computación de aplicaciones. **Figura 3-1** muestra la implementación de la nube híbrida.

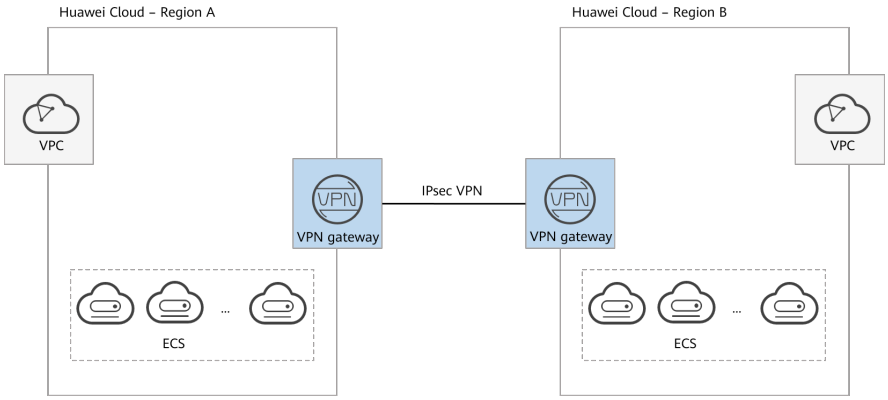
Figura 3-1 Implementación de nube híbrida



Interconexión entre regiones entre VPCs

Con las VPN, puede conectar VPC en diferentes regiones en Huawei Cloud para habilitar la conectividad entre los servicios de usuario en estas regiones, como se muestra en **Figura 3-2**.

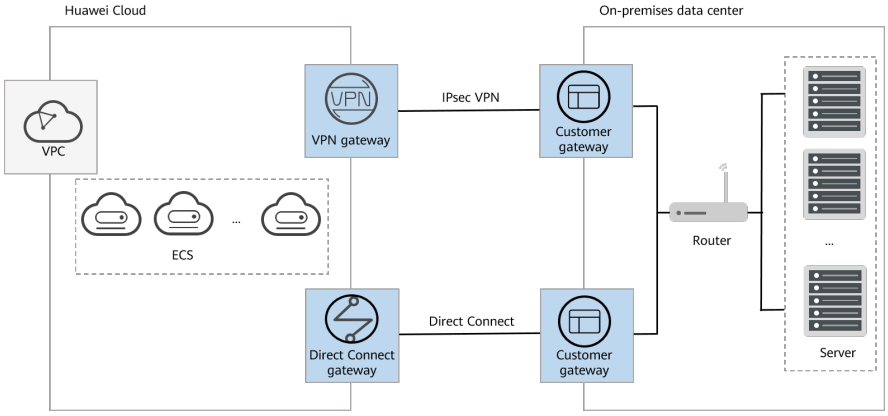
Figura 3-2 Interconexión entre regiones entre VPCs



Backup Between VPN and Direct Connect

For high reliability purposes, you can connect your on-premises data center to a VPC on the cloud through Direct Connect and VPN that back up each other, as shown in **Figura 3-3**.

Figura 3-3 Backup between VPN and Direct Connect



4 Differences Between VPN and Classic VPN

Tabla 4-1 Differences between VPN and Classic VPN

Item	VPN	Classic VPN
Deployment mode	Each tenant has exclusive use of VPN gateway instances that are isolated from each other. The performance of a VPN gateway instance is not affected by other VPN gateway instances. You can select gateway instances of different specifications based on your service requirements.	VPN gateway instances of multiple tenants are co-deployed on a hardware VPN gateway, but they are not isolated from each other. As a result, the performance of a VPN gateway instance is affected by other VPN gateway instances.
Reliability	Active-active gateways in different AZs	Active/Standby gateways
Routing mode	Policy-based and route-based modes are supported. In route-based mode, static routing and BGP routing are supported.	Only the policy-based mode is supported.
Interconnection with a VPC	Supported	Supported
Interconnection with an ER	Supported	Not supported
Multi-SKU of VPN gateways	Supported	Not supported
Number of VPN connections	10 to 100, which can be configured on the console.	10 by default. If you require more than 10 connections, submit a service ticket.

5 Notas y restricciones

Tabla 5-1 Notas y restricciones

Tipo de VPN	Recurso	Cuota por defecto	Cómo aumentar la cuota
Classic VPN	Puertas de enlace VPN por inquilino en cada región	2	**Enviar un ticket de servicio**.
	Conexiones VPN por inquilino en cada región	12	**Enviar un ticket de servicio**.
VPN	Puertas de enlace VPN por inquilino en cada región	50 Puede crear un máximo de 50 gateways VPN en una región.	**Enviar un ticket de servicio**.
	Puertas de enlace de clientes por inquilino en cada región	100	**Enviar un ticket de servicio**.
	Puertas de enlace de clientes que pueden conectarse a una única puerta de enlace VPN	100 Cuando se implementan puertas de enlace activos-activos, cada puerta de enlace de cliente tiene dos conexiones VPN.	Esta cuota no puede aumentarse.
	Subredes locales por puerta de enlace VPN	50	Esta cuota no puede aumentarse.
	Rutas basadas en políticas por conexión VPN	5	Esta cuota no puede aumentarse.
	Subredes de clientes por conexión VPN	50	Esta cuota no puede aumentarse.

6 Estándares y protocolos de referencia

Los siguientes estándares y protocolos están asociados con IPsec VPN:

- RFC 4301: Arquitectura de seguridad para el protocolo de Internet
- RFC 2403: El uso de HMAC-MD5-96 dentro de ESP y AH
- RFC 2409: Internet Key Exchange (IKE)
- RFC 2857: El uso de HMAC-RIPEMD-160-96 dentro de ESP y AH
- RFC 3566: El algoritmo AES-XCBC-MAC-96 y su uso con IPsec
- RFC 3625: Más grupos de More Modular Exponential (MODP) Diffie-Hellman para Internet Key Exchange (IKE)
- RFC 3664: El algoritmo AES-XCBC-PRF-128 para el protocolo de Internet Key Exchange (IKE)
- RFC 3706: Método basado en tráfico para detectar pares de Internet Key Exchange (IKE) muertos
- RFC 3748: Protocolo de autenticación extensible (EAP)
- RFC 3947: Negociación de NAT-Traversal en el IKE
- RFC 4109: Algoritmos para Internet Key Exchange (IKE) versión 1 (IKEv1)
- RFC 3948: Encapsulación UDP de paquetes IPsec ESP
- RFC 4305: Requisitos de implementación de algoritmos criptográficos para Encapsulating Security Payload (ESP) y Authentication Header (AH)
- RFC 4306: Protocolo de Internet Key Exchange (IKEv2)
- RFC 4307: Algoritmos criptográficos para su uso en el Internet Internet Key Exchange Version 2 (IKEv2)
- RFC 4322: Cifrado Oportunista mediante el Internet Key Exchange (IKE)
- RFC 4359: El uso de firmas RSA/SHA-1 dentro de Encapsulating Security Payload (ESP) y Authentication Header (AH)
- RFC 4434: El algoritmo AES-XCBC-PRF-128 para el protocolo de Internet Key Exchange Protocol (IKE)
- RFC 4478: Autenticación repetida en Internet Key Exchange Protocol (IKEv2)
- RFC 5996: Protocolo de Internet Key Exchange Protocol versión 2 (IKEv2)

7 Facturación (VPN)

Artículos de facturación

Tabla 7-1 Artículos de facturación de VPN

Modo de facturación	Artículo 1	Artículo 2	Artículo 3	Fórmula de facturación
Anual/ Mensual	Puerta de enlace VPN	Conexión de VPN	Ancho de banda	Precio total = tarifa de puerta de enlace de VPN + tarifa de conexión VPN + tarifa de ancho de banda
Pago por uso	Puerta de enlace VPN (facturada por hora)	Conexión de VPN (facturada por hora)	● Ancho de banda Ancho de banda de la puerta de enlace de VPN (facturado por hora) ● Tráfico Tráfico de red pública	● Facturado por ancho de banda Precio total = tarifa de puerta de enlace de VPN + tarifa de conexión VPN + tarifa de ancho de banda de puerta de enlace de VPN ● Facturado por tráfico Precio total = tarifa de puerta de enlace de VPN + tarifa de conexión VPN + tarifa de tráfico de red pública

El servicio VPN se factura por los siguientes elementos:

- **VPN gateway**: Una puerta de enlace VPN está dedicada a un inquilino, asegurando su rendimiento de reenvío.

- **VPN connection**: De forma predeterminada, se incluyen 10 grupos de conexión VPN de forma gratuita con la compra de una puerta de enlace de VPN. Si es necesario, se pueden comprar grupos de conexiones VPN adicionales.

  Dos conexiones VPN entre una puerta de enlace VPN y una puerta de enlace de cliente se facturan como un grupo de conexiones VPN.
- **EIP bandwidth**: De forma predeterminada, una puerta de enlace VPN utiliza una dirección IP elástica (EIP) para proporcionar acceso a Internet. Se le cobrará por el ancho de banda utilizado por el EIP.

  El ancho de banda de una puerta de enlace VPN es compartido por todas las conexiones VPN creadas para la puerta de enlace VPN. Como tal, debe evaluar el ancho de banda requerido en función de la cantidad de datos transmitidos a través de todas las conexiones VPN.

  Para obtener más información sobre los precios de EIP, consulte **Detalles de precio de IP elástico**.

Para obtener más información sobre los precios de VPN, consulte **Detalles de precios del producto**.

Modos de facturación

Las puertas de enlace de VPN se facturan anualmente/mensualmente o de pago por uso.

Anual/Mensual

Se le factura por mes o año al crear una puerta de enlace de VPN.

- **Fórmula de facturación**: Precio total = tarifa de puerta de enlace de VPN (CNY/mes por puerta de enlace) + tarifa de grupo de conexión VPN (CNY/mes por 10 grupos de conexión) + tarifa de ancho de banda EIP (CNY/mes por Mbit/s)
- **Modo de facturación**: Se incluyen diez grupos de conexión VPN de forma gratuita con la compra de una puerta de enlace de VPN. Si se requieren más grupos de conexión VPN, debe comprarlos.

Pago por uso

Se le cobrará en función de la duración del uso. El ancho de banda EIP se puede facturar por ancho de banda o tráfico.

- **Facturado por ancho de banda**: Precio total = tarifa de puerta de enlace de VPN (CNY/hora por puerta de enlace) + tarifa de grupo de conexión VPN (CNY/hora por 10 grupos de conexión) + tarifa de ancho de banda EIP (CNY/hora por Mbit/s)
- **Facturado por tráfico**: Precio total = tarifa de puerta de enlace de VPN (CNY/hora por puerta de enlace) + tarifa de grupo de conexión VPN (CNY/hora por 10 grupos de conexión) + tarifa de tráfico EIP (CNY/GB por EIP)
- **Modo de facturación**: El ciclo de facturación es de 1 hora.

  Diez grupos de conexión VPN se incluyen de forma gratuita con la compra de una puerta de enlace de VPN. Si se requieren más grupos de conexión VPN, debe comprarlos.

Cambio del modo de facturación

Puede cambiar los modos de facturación de una puerta de enlace de VPN de la siguiente manera:

- Cambie el modo de facturación de una puerta de enlace de VPN de pago por uso a anual/mensual.

Cambiar el modo de facturación de pago por uso a anual/mensual

Prerrequisitos

- El modo de facturación de una puerta de enlace de VPN y los EIP vinculados solo pueden cambiarse a anual/mensual cuando los EIP se facturan actualmente por ancho de banda en modo de pago por uso.

Procedimiento

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. En la página principal de la consola, haga clic en **Service List** y elija **Networking** > **Virtual Private Network**.
4. En el panel de navegación de la izquierda, elija **Virtual Private Network** > **VPN Gateways**.
5. Localice una puerta de enlace de VPN de pago por uso y elija **More** > **Change Billing Mode** en la columna **Operation**.
6. En el cuadro de diálogo **Change Billing Mode**, haga clic en **OK**.

   Un grupo de conexiones consta de dos conexiones entre una puerta de enlace de cliente y una puerta de enlace VPN. De forma predeterminada, se incluyen 10 grupos de conexión VPN de forma gratuita con la compra de una puerta de enlace VPN.
7. Confirme la información de la puerta de enlace VPN y establezca una duración de renovación.
8. Haga clic en **Pay**.
9. En la página de pago, confirme la información del pedido, seleccione un cupón o descuento y seleccione el método de pago.
10. Haga clic en **Pay**.

    NOTA

    Cambiar el modo de facturación de una puerta de enlace de VPN de pago por uso a anual/mensual no afectará sus servicios.

Renovación

Para obtener más información, consulte **Gestión de renovación**.

Vencimiento y pago atrasado

Para obtener más información, consulte **Suspensión de servicio y liberación de recursos** y **Pago y reembolso**.

8 Facturación (Classic VPN)

Huawei Cloud Classic VPNs se pueden facturar por pago por uso (por hora). Usted paga solo por lo que usa, y durante el tiempo que lo usa. No se requieren previsiones y presupuestos complejos. Puede comprar una o más conexiones VPN y se facturará en función del número de conexiones VPN y la duración del uso.

Artículos de facturación

Tabla 8-1 Artículos de facturación de Classic VPNs

Modo de facturación	Artículo 1	Artículo 2	Artículo 3	Fórmula de facturación
Pago por uso	Puerta de enlace de Classic VPN	Conexión de VPN (facturada por hora)	• Ancho de banda Ancho de banda de la puerta de enlace de VPN (facturado por hora) • Tráfico Tráfico de red pública	• Facturado por ancho de banda Precio total = tarifa de puerta de enlace de VPN clásica + tarifa de conexión VPN + tarifa de ancho de banda de puerta de enlace de VPN • Facturado por tráfico Precio total = tarifa de puerta de enlace de Classic VPN + tarifa de conexión VPN + tarifa de tráfico de red pública

- Tarifa de puerta de enlace de VPN clásica: indica la tarifa por usar una puerta de enlace de VPN clásica.

  Una puerta de enlace de VPN clásica admite un ancho de banda de reenvío máximo de 10 Mbit/s.
- Tarifa de conexión VPN: indica la tarifa que se cobra por las conexiones entre una puerta de enlace de VPN y una puerta de enlace de cliente.

  - Tarifa de conexión VPN = Precio unitario de conexión (CNY/hora) x Duración del uso (hora)
  - Las conexiones VPN se facturan en unidades de 10. El precio unitario de la conexión es el precio de 10 conexiones VPN.
  - En el modo de facturación anual/mensual, se admiten 10 conexiones VPN gratuitas de forma predeterminada.
- Tarifa de ancho de banda: Si une un EIP a una puerta de enlace de VPN, también se le cobrará por el ancho de banda utilizado por el EIP.

  Para obtener más información sobre los precios de EIP, consulte **Detalles de precios de IP elástica**.

Para obtener más información sobre los precios de Classic VPN, consulte **Detalles de precios del producto**.

Modos de facturación

Pago por uso

- **Facturado por ancho de banda**

  Si selecciona la facturación por ancho de banda, el ciclo de facturación es de una hora. La tarifa generada también varía dependiendo del tamaño del ancho de banda. El precio incluye el ancho de banda de la puerta de enlace de VPN o el precio del tráfico y el precio de la conexión VPN creada junto con la puerta de enlace. Si crea otra conexión para la puerta de enlace, se le cobrará la conexión adicional.

  Precio total = tarifa de ancho de banda de la puerta de enlace de VPN + tarifa de conexión VPN

  El ancho de banda que compró para una puerta de enlace VPN es el ancho de banda saliente, es decir, el ancho de banda de una VPC a su centro de datos local.

  - Si el ancho de banda saliente es de 10 Mbit/s o menos, el ancho de banda entrante se limita a 10 Mbit/s.
  - Si el ancho de banda saliente es más de 10 Mbit/s, el ancho de banda entrante es el mismo que el ancho de banda saliente.

  Por ejemplo, si el ancho de banda que compró es de 50 Mbit/s, utiliza la puerta de enlace VPN durante 5 horas y luego lo elimina, se le cobrará durante 5 horas en función del ancho de banda de 50 Mbit/s. Incluso si no transmite ningún dato durante esas cinco horas, todavía se le cobrará por el ancho de banda de 50 Mbit/s.
- **Facturado por tráfico**

  Si selecciona facturación por tráfico, se registrará el tráfico de cada hora y la unidad de facturación será de 1 GB. Si se utiliza menos de 1 GB, el precio varía (Precio total = Tráfico usado/1 GB x precio de 1 GB de tráfico). En este caso, modificar el tamaño del ancho de banda no cambia el precio del tráfico de red pública por GB. Solo se factura el tráfico en la dirección de salida.

  Precio total = Tarifa de tráfico de red pública + tarifa de conexión VPN

Cambio de los modos de facturación

Las puerta de enlace de VPN de pago por uso facturadas por ancho de banda se pueden cambiar a facturadas por tráfico o al revés.

Para cambiar una puerta de enlace de VPN de pago por uso facturada por tráfico para facturar por ancho de banda, realice las siguientes operaciones:

1. En la página **VPN Gateways**, busque la fila que contiene la puerta de enlace VPN que desea configurar.
2. Elija **More** > **Modify Bandwidth** en la columna **Operation**.
3. En la página **Modify Bandwidth**, establezca **Billed By** en **Bandwidth** en el área **Modify Specifications**.
4. Haga clic en **Submit**.

Renovación

Para obtener más información, consulte **Gestión de renovación**.

Vencimiento y pago atrasado

Para obtener más información, consulte **Suspensión de servicio y liberación de recursos** y **Pago y reembolso**.

9 Seguridad

9.1 Responsabilidad compartida

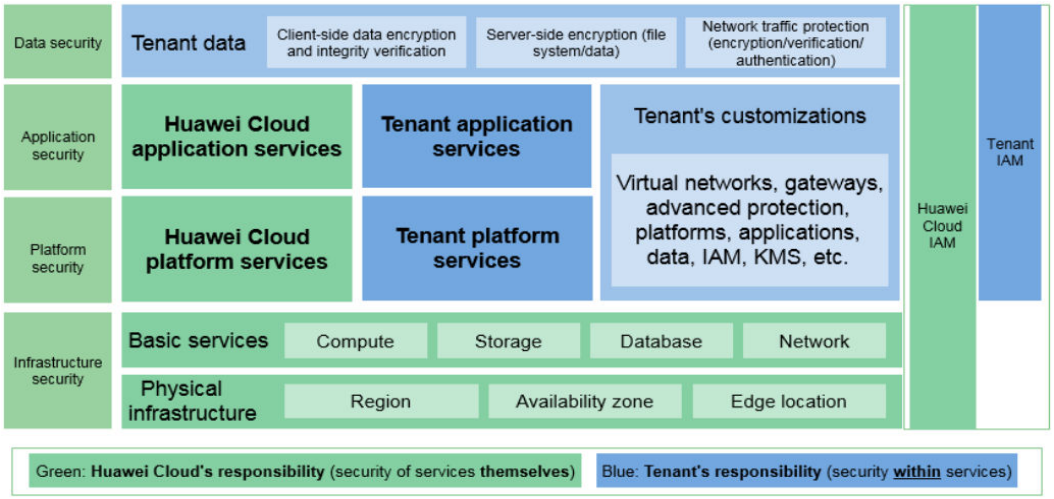
Huawei Cloud garantiza que su compromiso con la ciberseguridad nunca se verá compensado por la consideración de intereses comerciales. Para abordar los desafíos emergentes de la seguridad en la nube y las amenazas y ataques generalizados de seguridad en la nube, Huawei Cloud crea un sistema de seguridad integral que cumple con las leyes, regulaciones y estándares de la industria para servicios en la nube en diferentes regiones e industrias. aprovechando el ecosistema de seguridad de Huawei y las ventajas únicas en software y hardware.

Figura 9-1 muestra las responsabilidades compartidas por usted (los inquilinos) y Huawei Cloud.

- **Huawei Cloud**: Garantiza la seguridad de los servicios en la nube. Huawei Cloud es responsable de la seguridad de sus servicios en la nube IaaS, PaaS y SaaS, así como de los entornos físicos de los centros de datos de Huawei Cloud donde se implementan estos servicios. Huawei Cloud está comprometido no solo con la seguridad y el rendimiento de su infraestructura, servicios en la nube y tecnologías, sino también con la seguridad general de la nube O&M y, en términos más generales, el cumplimiento de la seguridad.
- **Tenants**: Garantice el uso seguro de los servicios en la nube. Su responsabilidad es utilizar los servicios en la nube de IaaS, PaaS y SaaS de forma segura, y gestionar eficazmente las configuraciones de seguridad que ha personalizado para firewalls virtuales, puertas de enlace de API, servicios de seguridad avanzados, servicios en la nube, datos de usuario, identidades y gestión de claves. y los sistemas operativos para redes virtuales, hosts virtuales y máquinas virtuales invitadas (VMs).

Huawei Cloud Security White Paper detalla las ideas y medidas para construir el sistema de seguridad en la nube de Huawei, incluidas las estrategias de seguridad en la nube, el modelo de responsabilidad compartida, el cumplimiento de la seguridad y la protección de la privacidad, la organización de la seguridad y el personal, la seguridad de la infraestructura, los servicios y la seguridad del inquilino, la seguridad de la ingeniería, seguridad de O&M y seguridad del ecosistema.

Figura 9-1 Modelo de responsabilidad compartida de Huawei Cloud

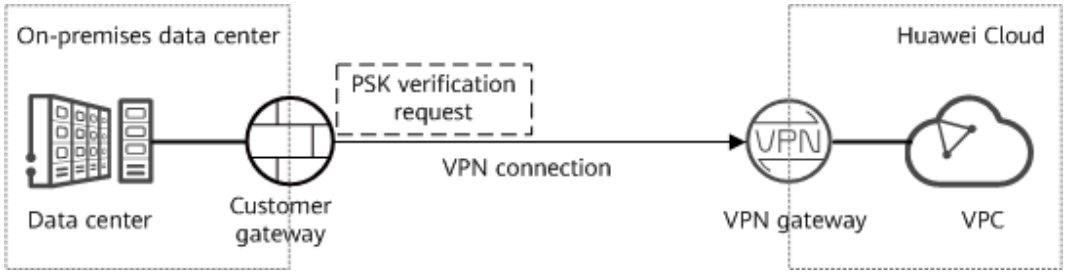


9.2 Autenticación de identidad y control de acceso

Una conexión VPN admite la autenticación de una puerta de enlace de cliente mediante una clave precompartida (PSK), lo que impide el acceso no autorizado.

La autenticación de identidad se realiza correctamente y la conexión VPN solo se puede configurar cuando la PSK configurada en la puerta de enlace del cliente es la misma que la configurada para la conexión VPN.

Figura 9-2 Gestión de identidades y acceso



9.3 Tecnologías de protección de datos

- La capacidad de VPN IPsec de sitio a sitio se proporciona para admitir la transmisión cifrada del tráfico de datos entre su red local y una VPC en la nube, asegurando su acceso a la nube.

  IPsec VPN es una tecnología de túnel que proporciona seguridad de capa IP mediante el conjunto de protocolos IKE/IPsec. Garantiza la confidencialidad y la integridad de los paquetes de datos IP y evita que sean interceptados, divulgados o manipulados en redes inseguras (como Internet).

- Al crear una conexión VPN IPsec, puede configurar los algoritmos de encriptación y autenticación para el tráfico de datos en una política IPsec.

  Se soportan algoritmos criptográficos comerciales comunes. Los algoritmos recomendados se enumeran de la siguiente manera en orden descendente de seguridad:

- Algoritmos de encriptación:
  - AES-256-GCM-16 (soportado solo por VPN)
  - AES-128-GCM-16 (soportado solo por VPN)
  - AES-256
  - AES-192
  - AES-128
- Algoritmos de autenticación:
  - SHA2-512
  - SHA2-384
  - SHA2-256

PFS

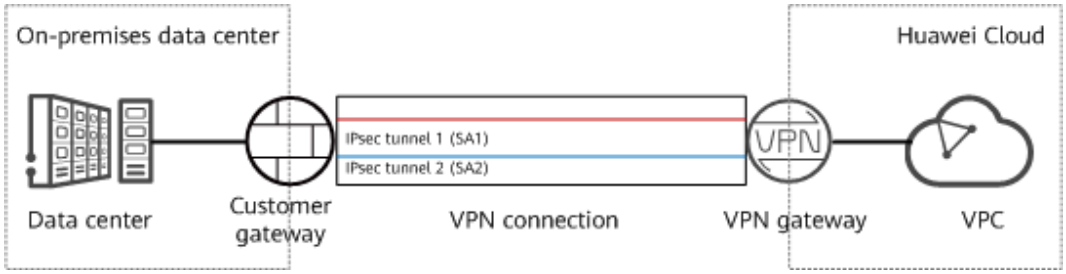
Perfect Forward Secrecy (PFS) asegura que el compromiso de las claves de un túnel IPsec no afecta la seguridad de otros túneles al aprovechar que las claves de estos túneles son irrelevantes entre sí. De forma predeterminada, PFS está habilitado para el servicio VPN.

Cada conexión IPsec VPN consiste en al menos un túnel IPsec, cada uno de los cuales utiliza un conjunto independiente de claves para proteger el tráfico de usuario.

Se soportan algoritmos PFS comunes. Los algoritmos recomendados son los siguientes:

- DH group 14
- DH group 15
- DH group 16
- DH group 19
- DH group 20
- DH group 21

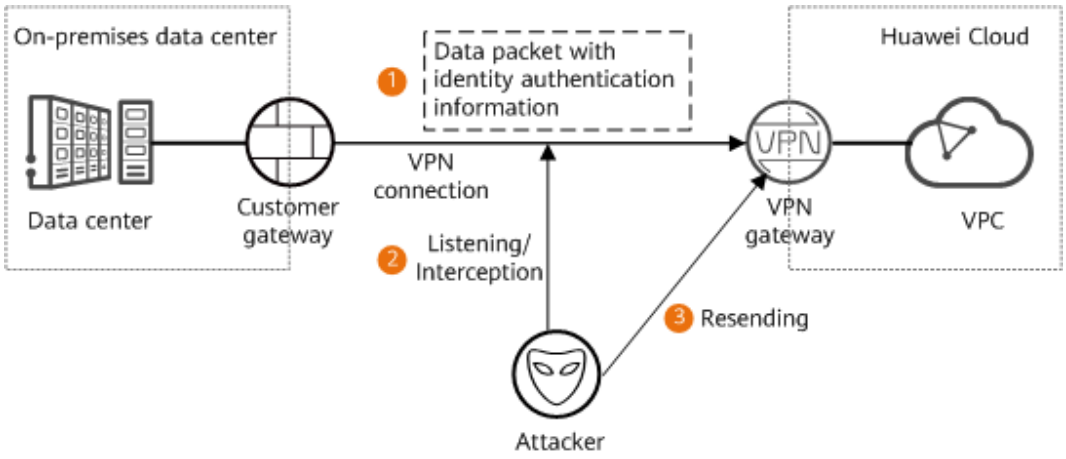
Figura 9-3 PFS



Anti-replay

Anti-replay utiliza números de secuencia para proteger los paquetes cifrados IPsec contra ataques de repetición, que se inician enviando repetidamente paquetes de datos interceptados. De forma predeterminada, la función anti-replay está habilitada para el servicio VPN.

Figura 9-4 Replay attack

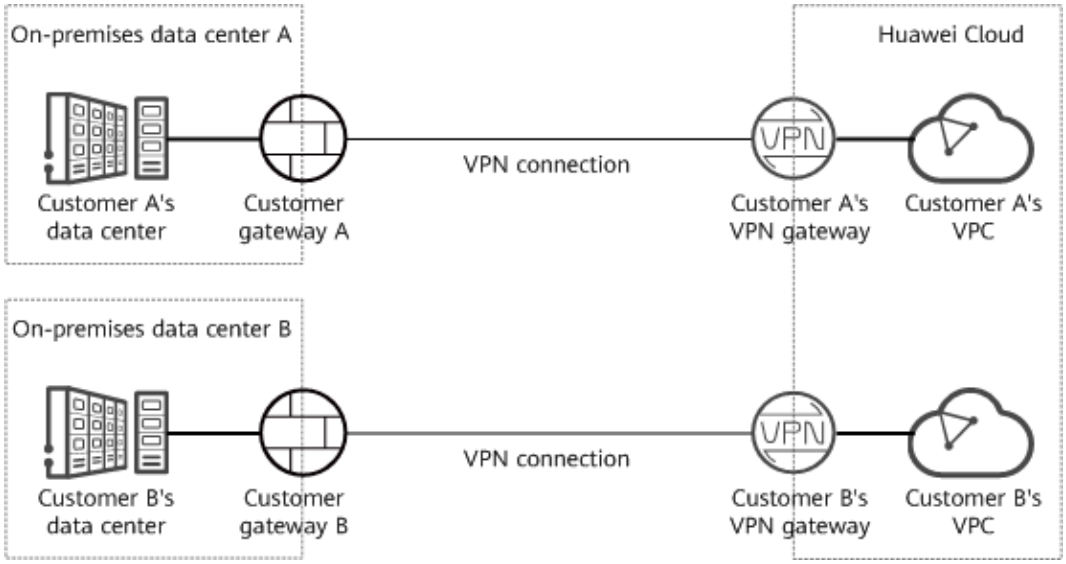


Aislamiento de datos

Una puerta de enlace de VPN es exclusiva para un inquilino. Como tal, los inquilinos están aislados de cada uno, lo que garantiza la seguridad de los datos.

El aislamiento de datos solo es compatible con VPN, pero no con Classic VPN.

Figura 9-5 Aislamiento de datos

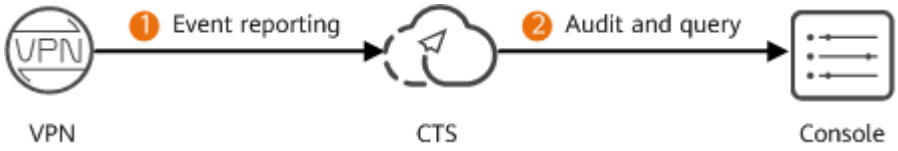


Como se muestra en la figura, un fallo de la puerta de enlace VPN del cliente A no tiene impacto en la puerta de enlace VPN del cliente B.

9.4 Auditoría y Logs

La VPN registra todas las llamadas a la API, las operaciones realizadas en los recursos, y los eventos relacionados iniciados por su cuenta, y las envía a Cloud Trace Service (CTS) en archivos de registro para consultas, auditorías y seguimiento de fuentes.

Figura 9-6 Logs de auditoría de seguridad

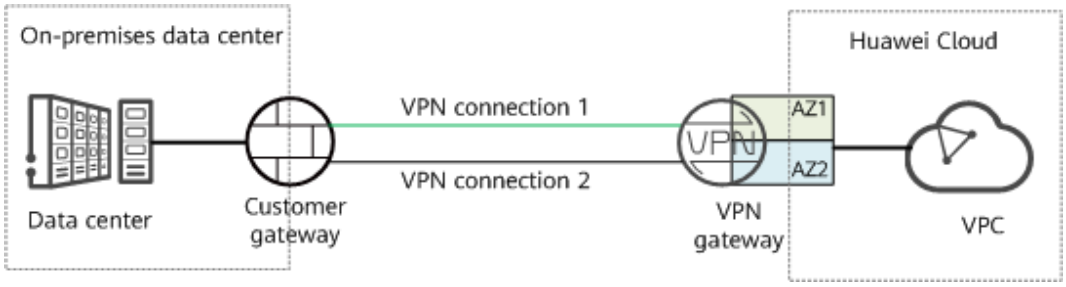


9.5 Resiliencia del servicio

VPN proporciona la función de recuperación ante desastres de dual-AZ. Puede crear una puerta de enlace VPN en dos Zonas de disponibilidad en la misma región, y crear una conexión VPN entre la puerta de enlace del cliente y cada zona de disponibilidad.

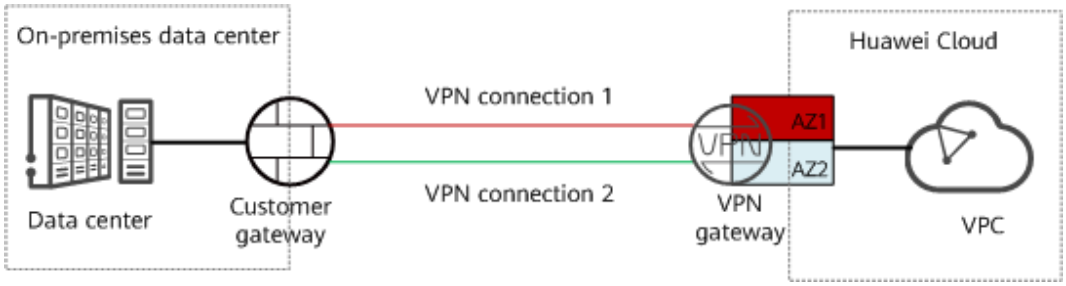
La recuperación ante desastres Dual-AZ solo es compatible con VPN, pero no con Classic VPN.

Figura 9-7 Escenario en el que los servicios se ejecutan correctamente



Si la puerta de enlace VPN o la conexión VPN en un zona de disponibilidad es defectuosa, el tráfico se conmuta automáticamente a la otra conexión VPN, lo que garantiza el funcionamiento normal del servicio.

Figura 9-8 Escenario de migración por falla



10 Gestión de permisos

Si necesita asignar diferentes permisos a los empleados de su empresa para acceder a sus recursos de VPN, Identity and Access Management (IAM) es una buena opción para la gestión de permisos detallada. IAM proporciona autenticación de identidad, gestión de permisos y control de acceso, lo que le ayuda a gestionar de forma segura el acceso a sus recursos de Huawei Cloud.

Con IAM, puede usar su cuenta de Huawei Cloud para crear usuarios de IAM y asignar permisos a los usuarios para controlar su acceso a recursos específicos. Por ejemplo, algunos desarrolladores de software de su empresa necesitan usar recursos de VPN, pero no deben poder eliminarlos ni realizar operaciones de alto riesgo. En este escenario, puede crear usuarios de IAM para los desarrolladores de software y concederles solo los permisos necesarios para usar recursos VPN.

Si su cuenta de Huawei Cloud no necesita usuarios individuales de IAM para la gestión de permisos, puede omitir este tema.

IAM es gratis. Solo paga por los recursos de su cuenta. Para obtener más información acerca de IAM, consulte **Descripción general del servicio IAM**.

Permisos de VPN

De forma predeterminada, los nuevos usuarios de IAM no tienen permisos asignados. Debe agregar un usuario a uno o más grupos y adjuntar directivas o roles de permisos a estos grupos. Los usuarios heredan permisos de los grupos a los que se agregan y pueden realizar operaciones específicas a servicios en la nube según los permisos.

VPN es un servicio a nivel de proyecto implementado en regiones físicas específicas. Para asignar permisos VPN a un grupo de usuarios, especifique el ámbito como proyectos específicos de la región y seleccione proyectos para que los permisos surtan efecto. Si se selecciona **All projects**, los permisos surtirán efecto para el grupo de usuarios en todos los proyectos específicos de la región. Al acceder a VPN, los usuarios deben cambiar a una región en la que se les haya autorizado a usar este servicio.

Puede conceder permisos mediante roles o políticas.

- Roles: Un tipo de mecanismo de autorización de grano grueso que define permisos relacionados con las responsabilidades del usuario. Solo hay un número limitado de roles para conceder permisos a los usuarios. Algunos roles dependen de otros roles para que surtan efecto. Cuando asigne dichos roles a los usuarios, recuerde asignar los roles de los

que dependen. Sin embargo, los roles no son una opción ideal para la autorización detallada y el control de acceso seguro.

- Políticas: Un tipo de mecanismo de autorización detallado que define los permisos necesarios para realizar operaciones en recursos de nube específicos bajo ciertas condiciones. Este mecanismo permite una autorización más flexible basada en políticas, cumpliendo los requisitos para un control de acceso seguro. Por ejemplo, puede conceder a los usuarios de VPN solo los permisos necesarios para administrar un cierto tipo de ECS.

Tabla 10-1 enumera todos los roles y permisos definidos por el sistema admitidos por VPN.

Tabla 10-1 Funciones y permisos definidos por el sistema VPN

Nombre de rol/política del sistema	Descripción	Dependencias
VPN Administrator	Todas las operaciones en recursos VPN. Para obtener este permiso, los usuarios también deben tener los permisos **Tenant Guest** y **VPC Administrator**.	**Tenant Guest** y **VPC Administrator** ● **VPC Administrator**: política a nivel de proyecto, que debe asignarse en el mismo proyecto que el **VPC Administrator** ● **Tenant Guest**: política a nivel de proyecto, que debe asignarse en el mismo proyecto que el **VPC Administrator**
VPN FullAccess	Permisos completos para VPN.	N/A
VPN ReadOnlyAccess	Permisos de sólo lectura para los recursos VPN. Los usuarios que tienen estos permisos solo pueden ver información acerca de los recursos VPN.	N/A

Tabla 10-2 enumera las operaciones comunes admitidas por cada política definida por el sistema de VPN. Seleccione los permisos necesarios.

Tabla 10-2 Operaciones comunes soportadas por el **VPN Administrator**

Operación	VPN Administrator	VPN FullAccess	VPN ReadOnlyAccess
Creación de una VPN gateway	Soportado	√	×

Operación	VPN Administrator	VPN FullAccess	VPN ReadOnlyAccess
Visualización de un gateway de VPN	Soportado	√	√
Modificación de una puerta de enlace de VPN	Soportado	√	×
Eliminación de una puerta de enlace VPN	Soportado	√	×
Creación de una conexión VPN	Soportado	√	×
Visualización de una conexión de VPN	Soportado	√	√
Modificación de una conexión de VPN	Soportado	√	×
Eliminación de una conexión de VPN	Soportado	√	×

Enlaces útiles

- **¿Qué es IAM?**
- **Creación de un usuario y concesión de permisos de VPN**

11 VPN y otros servicios

Figura 11-1 muestra los servicios relacionados con VPN.

Figura 11-1 VPN y servicios relacionados

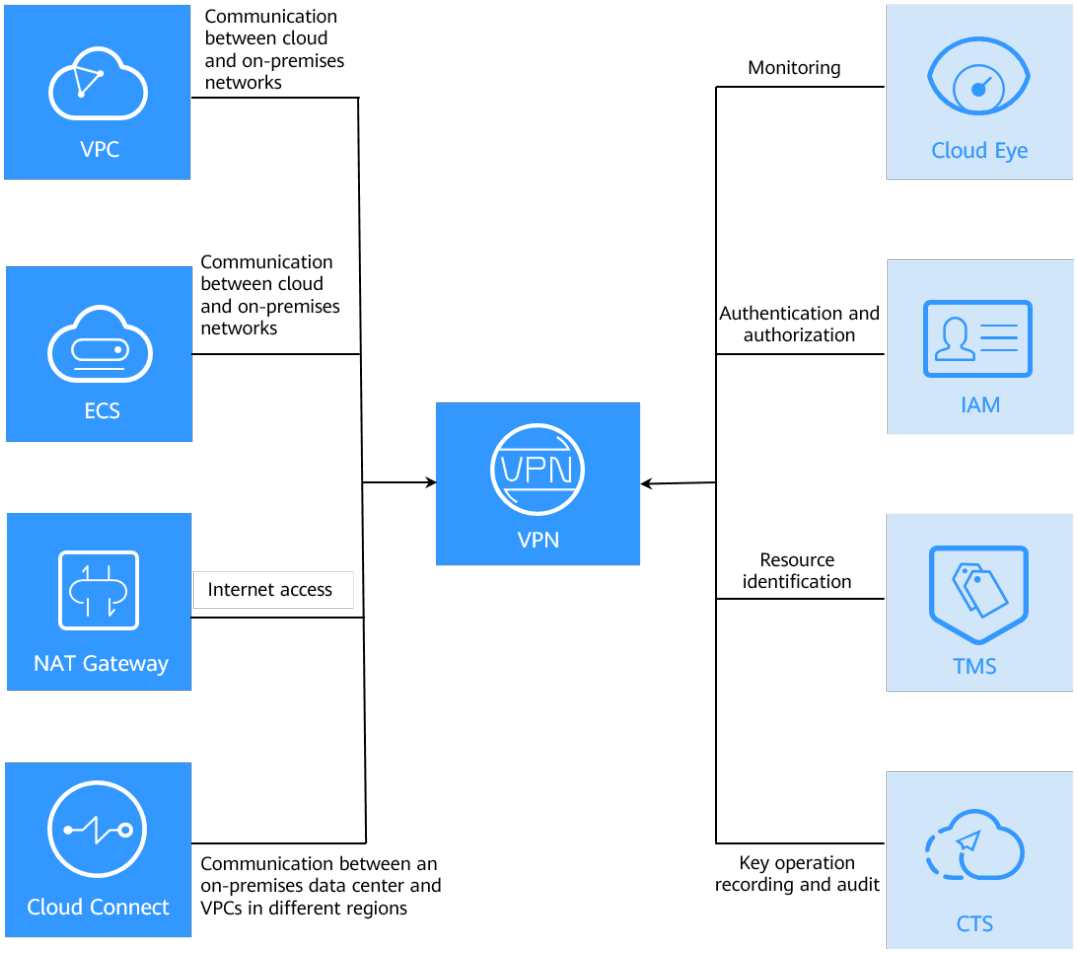


Tabla 11-1 Servicios relacionados

Servicios relacionados	Función	Referencia
Virtual Private Cloud (VPC)	Le permite crear una nube privada virtual a la que se pueda conectar su centro de datos local.	**VPC**
Elastic Cloud Server (ECS)	Le permite crear grupos de seguridad, agregar reglas de grupo de seguridad y agregar ECS a los grupos de seguridad, lo que mejora la seguridad del acceso a ECS.	**ECS**
Network address translation (NAT) gateway	Permite a los servidores de un centro de datos local que se conectan a una VPC mediante VPN compartir EIPs para acceder a Internet o proporcionar servicios a los que se puede acceder desde Internet.	**Puerta de enlace NAT**
Cloud Connect	Funciona junto con VPN para permitir comunicaciones de red estables entre su centro de datos local y las VPC en diferentes regiones.	**Cloud Connect**
Cloud Eye	Supervisa los recursos de VPN y le permite ver métricas.	**Cloud Eye**
Identity and Access Management (IAM)	Permite asignar diferentes permisos a diferentes usuarios. Permite un control de grano fino sobre sus recursos VPN.	**Identity and Access Management**
Tag Management Service (TMS)	Identifica las VPN para facilitar la clasificación y la búsqueda.	**Tag Management Service**
Cloud Trace Service (CTS)	Registra las operaciones realizadas en VPN.	**Cloud Trace Service**

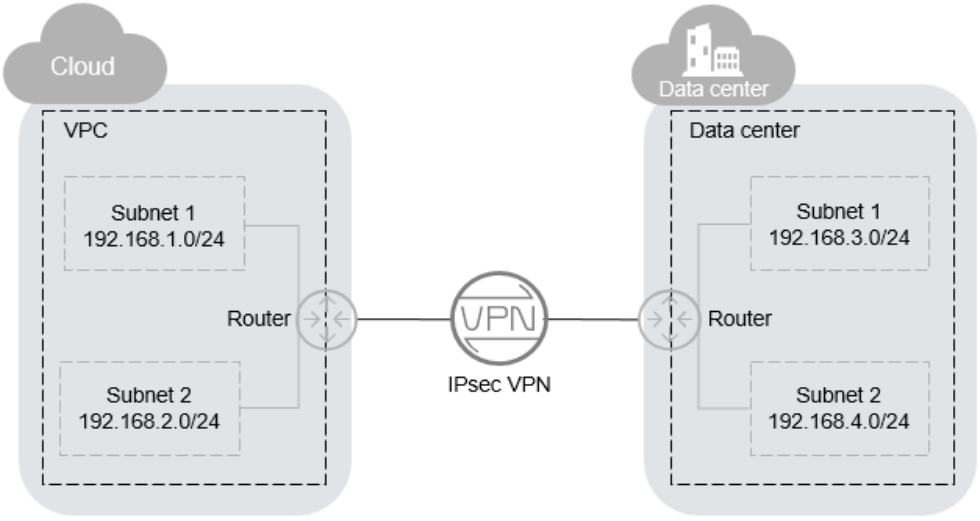
12 Conceptos Básicos

12.1 IPsec VPN

Internet Protocol Security (IPsec) VPN utiliza un conjunto de protocolos de red seguro que autentica y cifra los paquetes de datos para proporcionar una comunicación cifrada segura entre diferentes redes.

En **Figura 12-1**, la VPC tiene subredes 192.168.1.0/24 y 192.168.2.0/24. Su centro de datos local tiene subredes 192.168.3.0/24 y 192.168.4.0/24. Puede usar VPN para permitir que las subredes de la VPC se comuniquen con las de su centro de datos.

Figura 12-1 IPsec VPN



Huawei Cloud admite VPN sitio a sitio para permitir las comunicaciones entre subredes de VPC y subredes locales. Antes de establecer una VPN IPsec, asegúrese de que el centro de datos local donde se va a establecer la VPN cumple las siguientes condiciones:

- Los dispositivos locales que admiten IPsec estándar están disponibles.

- Los dispositivos locales se han asignado con direcciones IP públicas independientes (o direcciones IP traducidas por NAT).
- Las subredes locales no entran en conflicto con las subredes de VPC y son accesibles a los dispositivos locales.

Si se cumplen las condiciones anteriores, asegúrese de que las políticas IKE y IPsec en ambos extremos sean consistentes y que las subredes en ambos extremos sean pares coincidentes al configurar IPsec VPN.

Una vez completada la configuración, la negociación VPN debe ser activada por flujos de datos de red privada.

12.2 Puerta de enlace VPN

Una puerta de enlace de VPN es una puerta de enlace de salida para una VPC. Con una puerta de enlace 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 puerta de enlace VPN funciona junto con una puerta de enlace del cliente en un centro de datos local. Cada centro de datos tiene una puerta de enlace de cliente, y cada VPC tiene una puerta de enlace VPN. Una puerta de enlace de VPN puede conectarse a una o más puertas de enlace de clientes, lo que permite conexiones VPN punto a punto y hub-and-spoke.

12.3 Conexión de VPN

Una conexión VPN es un túnel de comunicación cifrado IPsec seguro y confiable establecido entre una puerta de enlace VPN y la puerta de enlace del cliente en un centro de datos local. Solo se admiten las VPN IPsec.

Las conexiones VPN utilizan protocolos IKE e IPsec para cifrar de forma rentable y segura los datos transmitidos a través de Internet.

12.4 Ancho de banda de puerta de enlace de VPN

El ancho de banda que compró para una puerta de enlace VPN es el ancho de banda saliente, es decir, el ancho de banda de una VPC a su centro de datos local.

- Si el ancho de banda saliente es de 10 Mbit/s o menos, el ancho de banda entrante se limita a 10 Mbit/s.
- Si el ancho de banda saliente es más de 10 Mbit/s, el ancho de banda entrante es el mismo que el ancho de banda saliente.

Si su puerta de enlace VPN se factura por el tráfico en una base de pago por uso, el tamaño de ancho de banda de la puerta de enlace VPN no afecta el precio total. Pero se recomienda que establezca el tamaño del ancho de banda en función de los requisitos reales para evitar una gran cantidad de tráfico causado por errores del programa o acceso malicioso.

12.5 Subred local

Las subredes locales son subredes de VPC que necesitan comunicarse con una red local a través de VPN. Cuando compras una conexión VPN, puedes configurar **Local Subnet** en cualquiera de las siguientes opciones:

- **Select subnet**: seleccione subredes de la lista desplegable. Esto se recomienda si todas las subredes que requieren comunicación VPN están en la VPC.
- **Specify CIDR block**: Introduzca las subredes mediante la notación CIDR (ejemplo: 192.168.0.0/16), y con cada entrada separada por una coma. Esto se recomienda si los bloques CIDR que requieren comunicación VPN no están en la VPC de la puerta de enlace VPN. Los bloques de CIDR de otra VPC se pueden conectar a esta VPC usando Interconexión de VPC.

12.6 Customer Gateway

Una puerta de enlace de cliente se encuentra en un centro de datos local y debe tener una dirección IP pública fija. No se puede utilizar una dirección IP pública dinámica para las comunicaciones IPsec VPN con Huawei Cloud. Si se cambia la dirección IP pública, cámbiela en Huawei Cloud lo antes posible. De lo contrario, la conexión VPN fallará.

12.7 Subred del cliente

Las subredes de clientes son subredes en un centro de datos local que acceden a una VPC a través de una VPN. Es necesario introducir subredes mediante notación CIDR (ejemplo: 192.168.0.0/16), y con cada entrada separada por una coma.

Después de configurar una subred de cliente, no es necesario agregar una ruta para ella. El servicio VPN entregará automáticamente rutas que apuntan a la subred del cliente.

NOTA

No se puede establecer una subred de cliente en una dirección IP de Class D o Class E o una dirección IP que comience por 127.

12.8 PSK

Un pre-shared key (PSK) es una clave configurada para una conexión VPN en la nube. Se utiliza para la negociación IKE entre dispositivos VPN en ambos extremos de una conexión VPN. Asegúrese de que las configuraciones de PSK en ambos extremos de la conexión VPN son las mismas. De lo contrario, la negociación IKE fallará.

Enlace de referencia:

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

