nube privada virtual

Descripción general del servicio

Edición 01

Fecha 2022-12-30

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

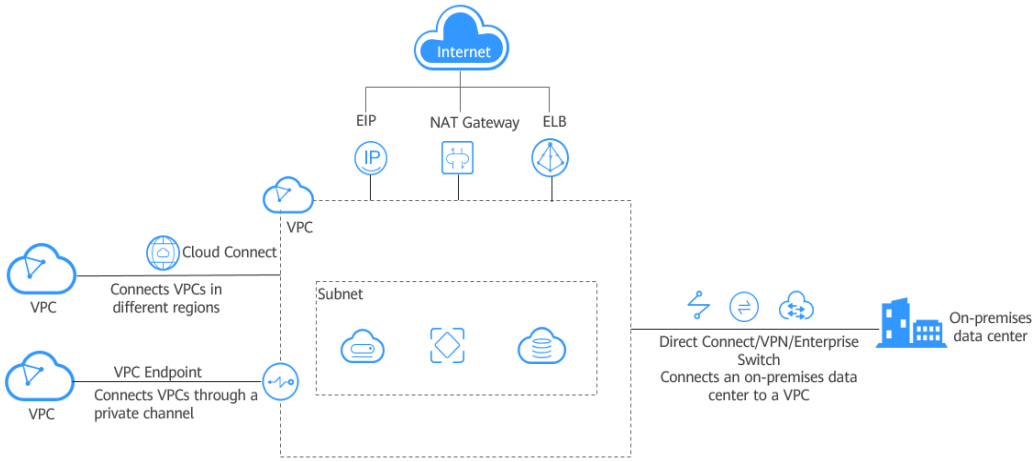
1 Descripción general del servicio de red....1
1.1 Descripción general del servicio de red....1
1.2 Planificación y diseño de la red....9
1.3 Seguridad de la red....15
1.4 Monitoreo de red....18
2 ¿Qué es Virtual Private Cloud?....20
3 Ventajas del producto....22
4 Escenarios de la aplicación....25
5 Funciones....30
6 Notas y restricciones....34
7 VPC y otros servicios....40
8 Facturación....42
9 Gestión de permisos....52
10 Conceptos básicos....57
10.1 Subred....57
10.2 Elastic IP....58
10.3 Tabla de rutas....58
10.4 Grupo de seguridad....61
10.5 Interconexión de VPC....63
10.6 ACL de red....65
10.7 Dirección IP virtual....67
10.8 Grupo de direcciones IP....69
10.9 Región y AZ....69

1 Descripción general del servicio de red

1.1 Descripción general del servicio de red

Huawei Cloud proporciona varios servicios de red para ayudarlo a construir las redes seguras y escalables en la nube, conectar redes en la nube y en las instalaciones de una manera confiable y de alta velocidad, y conectar su centro de datos en las instalaciones a Internet.

Figura 1-1 Servicios de red

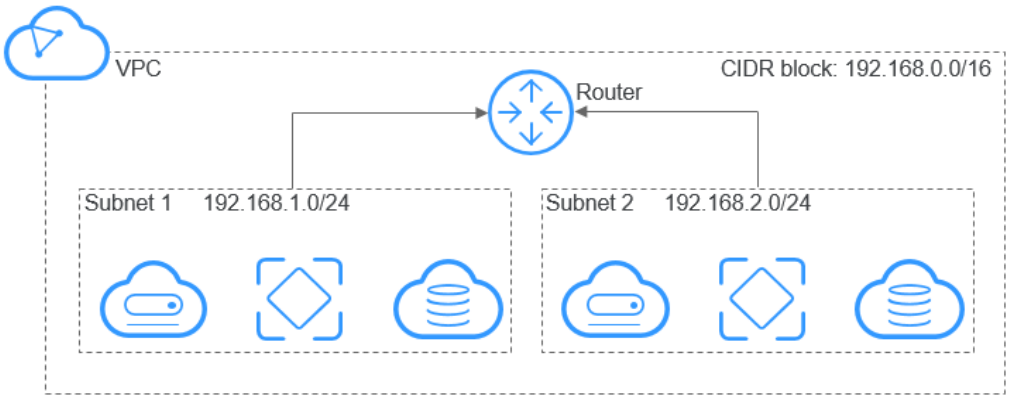


Virtual Private Cloud (VPC)

Una VPC es una red virtual lógicamente aislada, configurable y manejable para servidores en la nube, contenedores en la nube y bases de datos en la nube. Mejora la seguridad de los recursos y simplifica el despliegue de la red en la nube.

Cada VPC consta de un bloque CIDR privado, tablas de ruta y al menos una subred. Cuando crea una VPC, necesita especificar un bloque CIDR para la VPC y el sistema genera automáticamente una tabla de ruta predeterminada para la VPC. Todos los recursos de una VPC deben implementarse en las subredes. La tabla de ruta predeterminada asegura que todas las subredes de la VPC puedan comunicarse entre sí.

Figura 1-2 VPC



VPC puede trabajar junto con otros servicios de red para una conectividad de red más flexible.

- Conexión al Internet

  Los recursos de una VPC pueden comunicarse con Internet a través de **direcciones IP elásticas (EIP)**. También puede utilizar un gateway de NAT para permitir que los recursos de una VPC compartan una EIP.

- Conexión de una VPC y una red local

  Direct Connect, **VPN**, o **Enterprise Switch** se puede utilizar para conectar una VPC a un centro de datos local.

- Conexión de las VPC

  Una **interconexión de VPC** permite la comunicación entre dos VPC en la misma región.

  Cloud Connect permite una comunicación estable y de alta velocidad entre VPC en diferentes regiones.

Para obtener más información sobre la VPC, consulte **¿Qué es Virtual Private Cloud?**

Elastic IP (EIP)

El servicio EIP permite que los recursos en la nube se comuniquen con Internet mediante direcciones IP estáticas públicas y anchos de banda escalables. Las EIP se pueden vincular a o los ECS, los BMS, las direcciones IP virtuales, los balanceadores de carga y los gateway de NAT o desvincularse de ellos.

También puede comprar lo siguiente para sus EIP:

- Anchos de banda compartidos

  El ancho de banda compartido permite que los ECS, BMS y balanceadores de carga que están vinculados con las EIP en la misma región compartan el mismo ancho de banda.

- Paquete de datos compartidos

  Un paquete de datos compartido proporciona una cuota para el uso de datos. Los paquetes de datos compartidos entran en vigor inmediatamente después de su compra. Si se ha suscrito a las EIP de pago por uso facturados por tráfico en una región y compra un paquete de datos compartidos en la misma región, los EIP utilizarán el paquete de datos compartidos. Una vez que la cuota del paquete se agote o que el paquete venza, los EIP se seguirán facturando en modo de pago por uso.

- Paquete adicional de ancho de banda

  Un paquete adicional de ancho de banda se utiliza para aumentar temporalmente el ancho de banda máximo de una EIP anual/mensual.

Para obtener más información sobre la EIP, consulte **¿Qué son las EIP?**

Gateway de NAT

Gateway de NAT público

Los gateway de NAT públicos proporcionan la traducción de direcciones de red (NAT) con 10 Gbit/s de ancho de banda para servidores en una VPC, como ECS, Bare Metal Servers (BMS) y escritorios Workspace, o para servidores que se conectan a una VPC a través de Direct Connect o VPN en centros de datos locales, lo que permite que estos servidores compartan las EIP para acceder a Internet o para proporcionar servicios accesibles desde Internet.

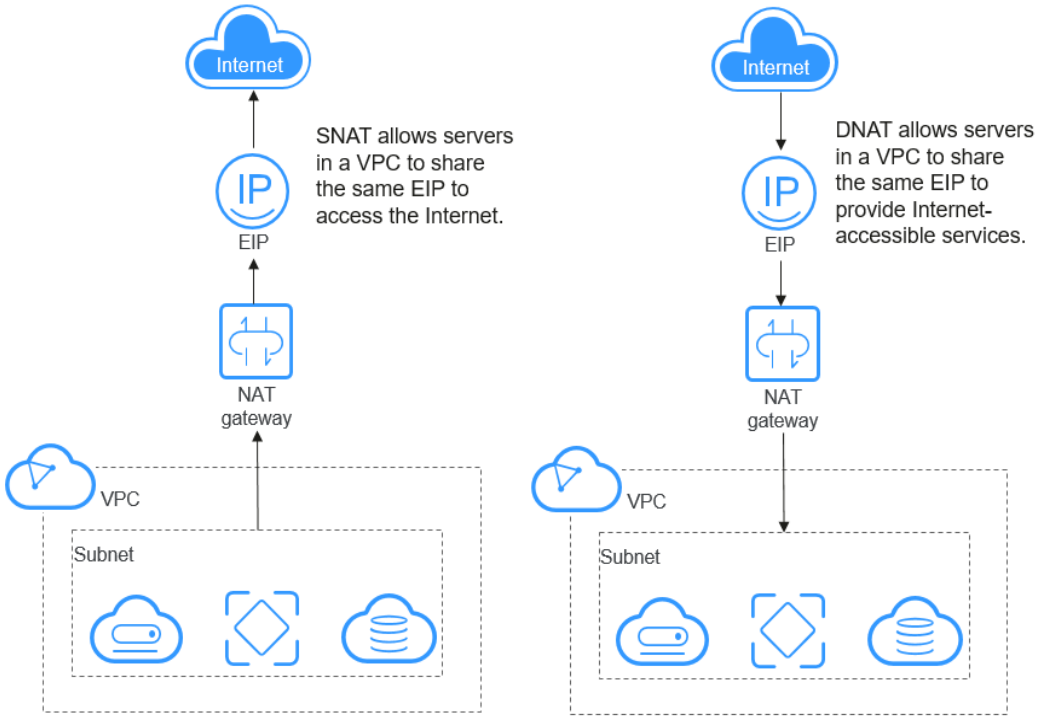
Los gateway de NAT proporcionan las funciones como NAT de origen y NAT de destino.

- NAT de origen (SNAT)

  SNAT traduce las direcciones IP privadas en las EIP, permitiendo a los servidores de una VPC compartir una EIP para acceder a Internet de una manera segura y eficiente.
- NAT de destino (DNAT)

  DNAT permite a los servidores de una VPC compartir una EIP para proporcionar servicios accesibles desde Internet a través de la asignación de direcciones IP o la asignación de puertos.

Figura 1-3 Gateway de NAT público



Gateway de NAT privado

Los gateway de NAT privados proporcionan la traducción de direcciones de red (NAT) para servidores, como ECS, BMS y escritorios Workspace, en una VPC, y permitir que varios

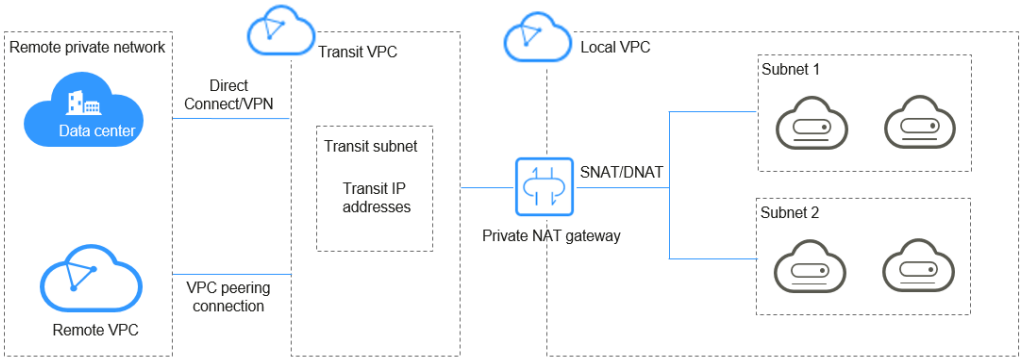
servidores compartan una dirección IP privada para acceder o proporcionar servicios accesibles desde un centro de datos local o una VPC remota.

Un gateway de NAT privado traduce las direcciones IP entre su VPC y su centro de datos local u otra VPC, lo que le permite mantener las redes heredadas sin cambios después de migrar algunas de sus cargas de trabajo a la nube.

Los gateway de NAT privados soportan SNAT y DNAT.

- SNAT permite que varios servidores de AZ en una VPC compartan la dirección IP de tránsito para acceder a un centro de datos local o a una VPC remota.
- DNAT permite que los servidores que comparten la misma dirección IP de tránsito en una VPC proporcionen servicios accesibles desde un centro de datos local o una VPC remota mediante la asignación de direcciones IP o puertos.

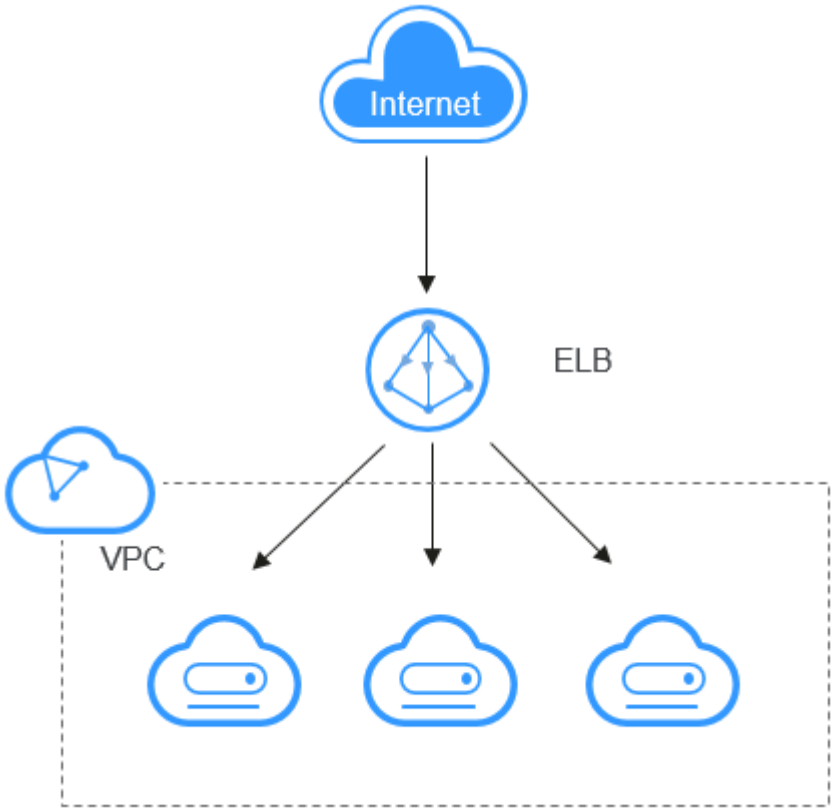
Figura 1-4 Gateway de NAT privado



Elastic Load Balance (ELB)

ELB distribuye automáticamente el tráfico entrante a través de varios servidores backend según las reglas de escucha configuradas. ELB amplía las capacidades de sus aplicaciones y mejora su disponibilidad al eliminar los puntos únicos de fallo (SPOF).

Figura 1-5 ELB

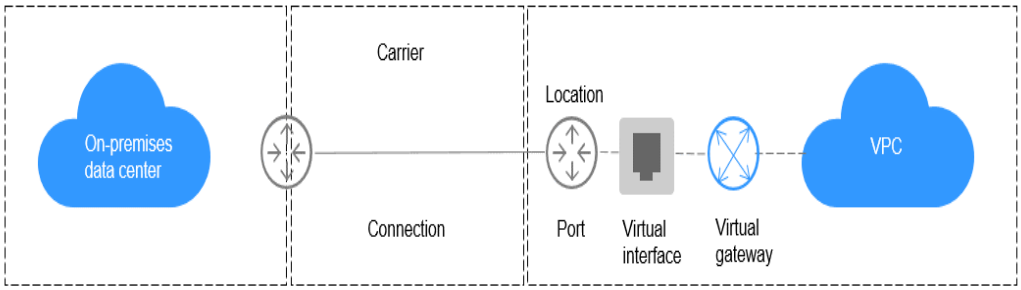


Direct Connect

Direct Connect le permite establecer una conexión de red dedicada entre su centro de datos local y una VPC. Con Direct Connect, puede crear fácilmente una nube híbrida segura y confiable.

Direct Connect establece una conexión dedicada y sus datos no se transferirán a través de Internet.

Figura 1-6 Direct Connect



Puede conectar su centro de datos a la nube utilizando cualquiera de los dos tipos de conexión:

- Conexión estándar

  Tiene más de una conexión terminada en diferentes ubicaciones. Estas conexiones funcionan como una copia de respaldo entre sí, mejorando la fiabilidad de las conexiones. Si solo puede seleccionar un operador debido a requisitos especiales, debe configurar diferentes rutas físicas.

  Una conexión estándar proporciona un puerto exclusivo. Puede crear las conexiones estándar en la consola de gestión.

- Conexión alojada

  Solicita una conexión a un socio que tiene una línea terminada en la ubicación de Direct Connect que está cerca de su centro de datos local.

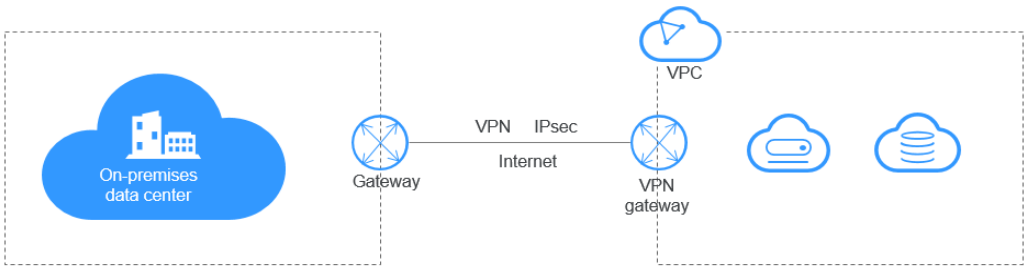
  Comparte el puerto con otros.

VPN

VPN establece un túnel de comunicación seguro y encriptado entre su centro de datos y su VPC. Con VPN, puede conectarse a una VPC y acceder a los recursos implementados allí.

A diferencia de Direct Connect, VPN establece un túnel cifrado que transfiere datos a través de Internet.

Figura 1-7 Topología de red



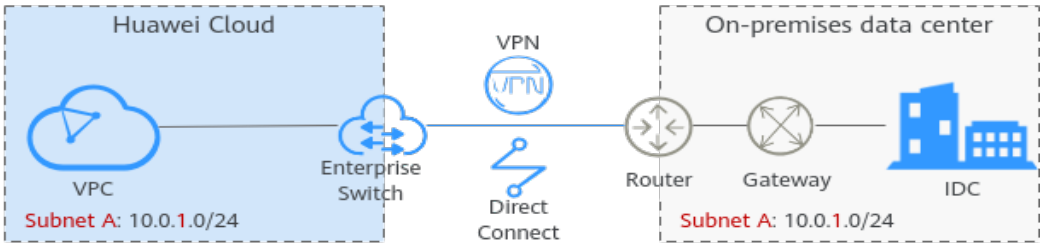
Conmutador empresarial

Los conmutadores empresariales habilitan las redes de nivel 2 para las VPC, lo que le ayuda a conectar redes en la nube y en las instalaciones que son altamente confiables, a gran escala y de alto rendimiento.

Actualmente, los conmutadores empresariales solo admiten los gateway de conexión de nivel 2 (L2CG). Un L2CG es un gateway de túnel virtual que puede trabajar con Direct Connect o VPN para establecer comunicaciones de red entre redes en la nube y en las instalaciones en la capa 2. El gateway le permite migrar cargas de trabajo en los centros de datos o las nubes privadas a la nube sin cambiar las subredes y direcciones IP.

Un conmutador empresarial es un gateway de túnel de una VPC y corresponde al gateway de túnel de su centro de datos. Puede funcionar junto con Direct Connect o VPN para habilitar las comunicaciones entre una VPC y su centro de datos en la capa 2. **Figura 1-8** muestra el diagrama de red. Debe conectar una subred de VPC al conmutador empresarial y especificar el conmutador empresarial para establecer una conexión con el gateway del túnel del centro de datos local para que la subred de VPC pueda comunicarse con la subred del centro de datos en la capa 2.

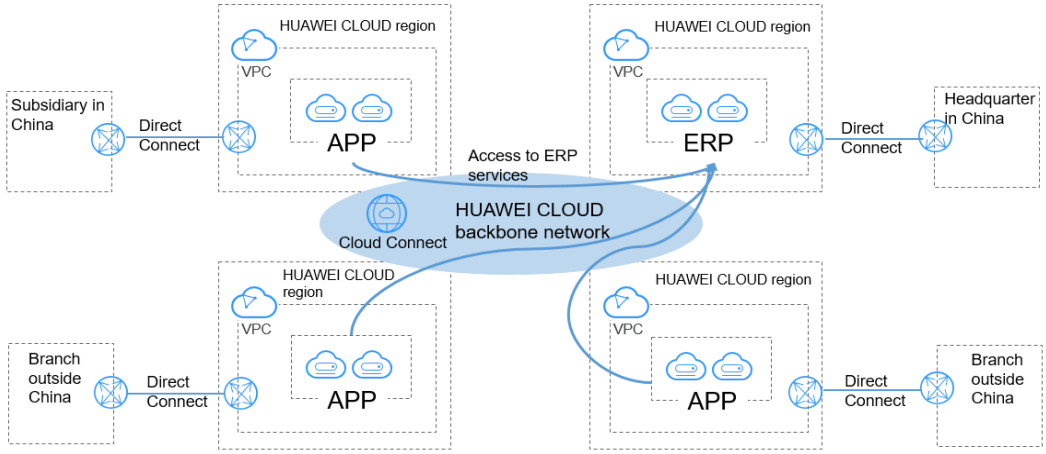
Figura 1-8 Redes de nivel 2



Cloud Connect

Cloud Connect le permite crear rápidamente las redes de alta calidad que pueden conectar VPC entre regiones y trabajar con Direct Connect para conectar las VPC y centros de datos locales. Con Cloud Connect, puede crear una red en la nube conectada globalmente con capacidades de comunicación y escalabilidad de clase empresarial.

Figura 1-9 Topología de red



Punto de conexión de VPC (VPCEP)

El servicio VPCEP proporciona los canales seguros y privados para conectar su VPC a los servicios de conexión (servicios en la nube o sus servicios privados) sin tener las EIP.

VPCEP se aplica a los siguientes escenarios:

- Acceso a sus servicios privados en una VPC a través de un servicio del punto de conexión de VPC

  Puede crear un servicio de punto de conexión de VPC para permitir que sus servicios proporcionados por ELB, ECS y BMS en una VPC sean accesibles.

  Un consumidor de servicios utiliza un punto de conexión de VPC para acceder al servicio de punto de conexión.

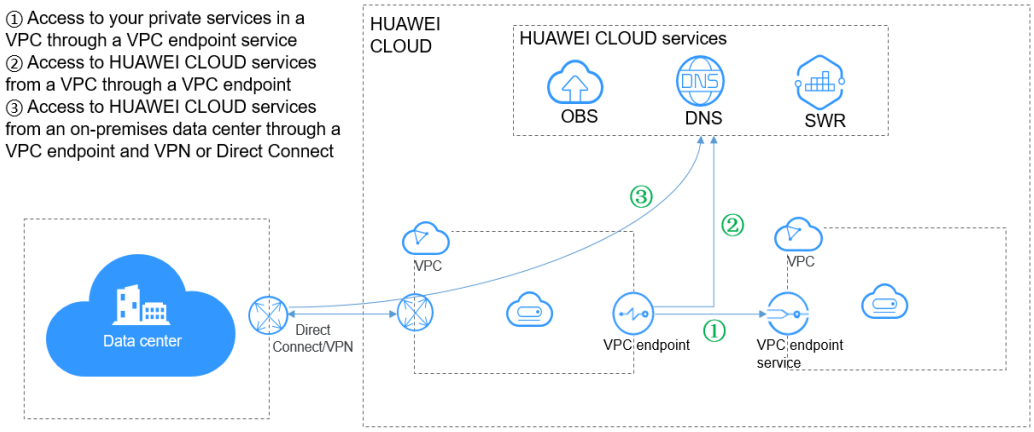
- Acceso a los servicios de Huawei Cloud desde una VPC a través de un punto de conexión de VPC

  Puede crear un punto de conexión de VPC para acceder a los servicios de punto de conexión de VPC.

- Acceso a los servicios de Huawei Cloud desde un centro de datos local a través de un punto de conexión de VPC y VPN o Direct Connect

  VPN o Direct Connect pueden trabajar junto con un punto de conexión de VPC para permitir el acceso a servicios en la nube, como OBS, DNS y SWR, desde un centro de datos local.

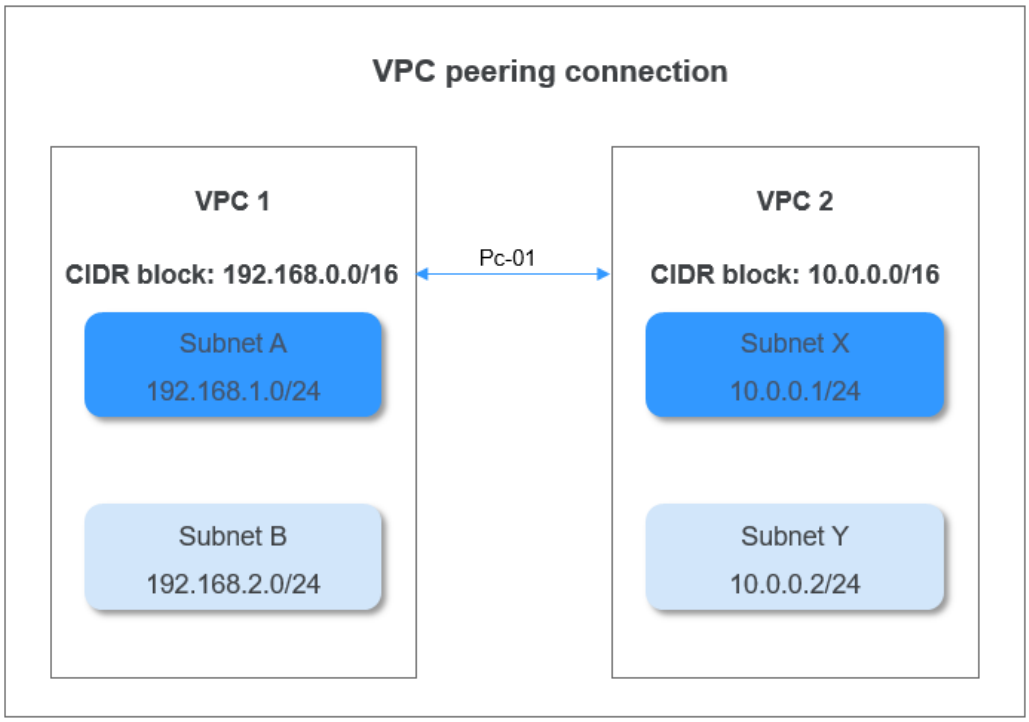
Figura 1-10 Punto de conexión de VPC



Interconexión de VPC

De forma predeterminada, las VPC no pueden comunicarse entre sí. Una interconexión de VPC permite que dos VPC de la misma región se comuniquen entre sí mediante las direcciones IP privadas como si estuvieran en la misma VPC. Puede crear una interconexión de VPC entre sus propias VPC o entre su VPC y una VPC de otra cuenta dentro de la misma región. Una interconexión de VPC entre las VPC en diferentes regiones no surtirá efecto.

Figura 1-11 Interconexión de VPC



1.2 Planificación y diseño de la red

Cuando implementa las cargas de trabajo en la nube, debe considerar el aislamiento, la escalabilidad y la conectividad de la red.

- **Aislamiento**

  El aislamiento es el requisito básico para la planificación y el diseño de redes. De forma predeterminada, las VPC están aisladas entre sí y no pueden comunicarse entre sí a través de una red privada sin importar si están en la misma región.

  En general, las diferentes cargas de trabajo se encuentran en las diferentes VPC. Los departamentos o entornos diferentes (como desarrollo, pruebas y producción) utilizan diferentes VPC.

  Puede crear varias subredes en una VPC para cargas de trabajo con diferentes requisitos y configurar las ACL de red para garantizar la seguridad entre subredes.

- **Escalabilidad**

  Considere la escalabilidad de la red desde los siguientes aspectos, ya que los requisitos de carga de trabajo cambian constantemente con el tiempo:

  - Reserve suficientes direcciones IP para ampliar la capacidad.
  - Cree las VPC para la **conectividad**.

- **Conectividad**

  La conectividad de red está estrechamente relacionada con el aislamiento y la escalabilidad de la red. Debe considerar la conectividad de red entre:

  - Una VPC y el Internet
  - Las VPC en la misma región y en diferentes regiones

- Un centro de datos local y una VPC

A continuación se describe la planificación y el diseño de redes en términos de planificación de VPC, planificación de subred, conectividad a Internet, conectividad entre VPC y entre un centro de datos local y una VPC.

Planificación de VPC

Cuando planifique las VPC:

1. Seleccione una región en la que se cree una VPC más cercana a sus servicios. Las VPC son específicas de la región. De forma predeterminada, las VPC no pueden comunicarse entre sí a través de una red privada sin importar si están en la misma región.
2. Determine el número de las VPC que necesita.
   - Si sus diferentes tipos de cargas de trabajo necesitan estar aisladas unas de otras, despliéguelas en diferentes VPC. Si solo hay un tipo de carga de trabajo, basta con una VPC.
   - Si necesita diferentes entornos para implementar sus cargas de trabajo, por ejemplo, entornos de desarrollo, pruebas y producción, debe crear varias VPC.
   - Si sus recursos tienen requisitos sobre la gestión de permisos, implemente en diferentes VPC para simplificar la gestión de permisos.
3. Seleccione un bloque CIDR de VPC.
   - Reserve suficientes direcciones IP para las cargas de trabajo para evitar el impacto de la expansión de la carga de trabajo en la red.
   - Evite conflictos de direcciones IP si necesita conectar una VPC a un centro de datos local o conectar dos VPC.

Tabla 1-1 Número de direcciones IP

Bloque CIDR de VPC	Rango de direcciones IP	Número máximo de direcciones IP
10.0.0.0/8-24	10.0.0.0-10.255.255.255	2^24-2=16777214
172.16.0.0/12-24	172.16.0.0-172.31.255.255	2^20-2=1048574
192.168.0.0/16-24	192.168.0.0-192.168.255.255	2^16-2=65534

Planificación de subred

Una subred es un rango de direcciones IP en una VPC. Todos los recursos de una VPC deben implementarse en subredes y las subredes de una VPC no pueden superponerse. Una vez creada una subred, su bloque CIDR no se puede modificar.

Las subredes utilizadas para implementar los recursos deben residir dentro del bloque CIDR de VPC, y las máscaras de subred utilizadas para definirlas pueden estar entre la máscara de red de su bloque CIDR de VPC y la máscara de red /29. VPC soporta los siguientes bloques CIDR.

- 10.0.0.0/8-24
- 172.16.0.0/12-24
- 192.168.0.0/16-24

Al planificar subredes:

- Le recomienda que cree diferentes subredes para diferentes módulos en una VPC. Por ejemplo, puede crear diferentes subredes para los servidores web, de aplicaciones y de bases de datos. Un servidor web está en una subred de acceso público, y los servidores de aplicaciones y de bases de datos están en las subredes de acceso no público. Puede aprovechar las ACL de red para ayudar a controlar el acceso a los servidores de cada subred.
- Si solo necesita planificar subredes para VPC, y la comunicación entre VPC y centros de datos locales no es necesaria, puede crear subredes dentro de cualquiera de los bloques CIDR enumerados anteriormente.
- Si su VPC necesita comunicarse con un centro de datos local a través de VPN o Direct Connect, el bloque CIDR de VPC no puede solaparse con el bloque CIDR del centro de datos local. Por lo tanto, al crear una VPC o subred, asegúrese de que su bloque CIDR no se superponga con ningún bloque CIDR en el centro de datos.
- Al determinar el tamaño de un bloque CIDR de VPC o subred, asegúrese de que el número de direcciones IP disponibles en el bloque CIDR cumpla con los requisitos de su carga de trabajo.

Enrutamiento

Una tabla de ruta contiene un conjunto de rutas que se utilizan para controlar dónde se reenvía el tráfico de subred entrante y saliente dentro de una VPC. Cuando crea una VPC, tiene automáticamente una tabla de rutas predeterminada, que permite la comunicación interna dentro de esa VPC.

- Si no necesita controlar explícitamente cómo cada subred enruta el tráfico entrante y saliente, puede utilizar la tabla de rutas predeterminada.
- Si necesita controlar explícitamente cómo cada subred enruta el tráfico entrante y saliente en una VPC, puede agregar rutas personalizadas a la tabla de rutas.

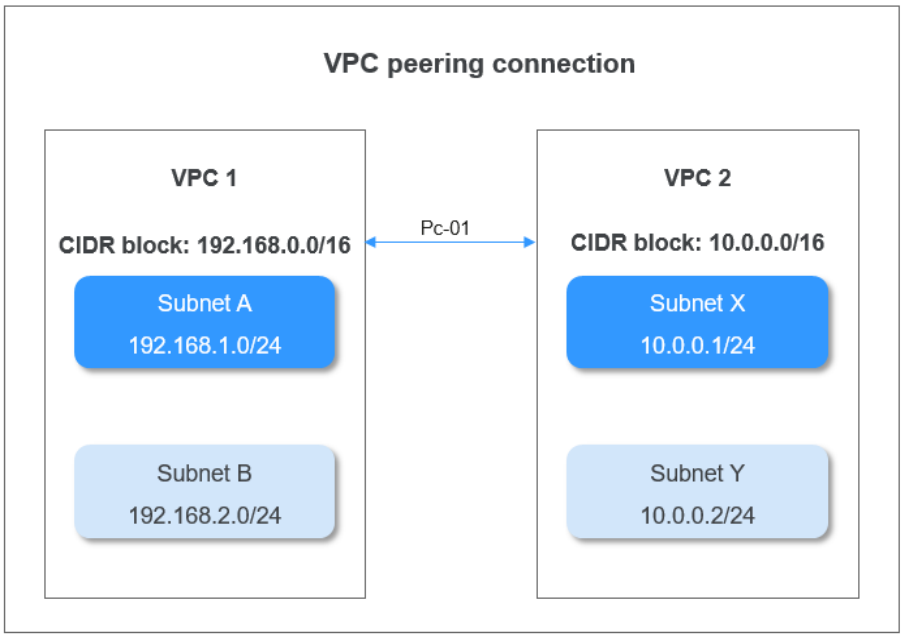
Conexión de las VPC

Puede utilizar lo siguiente para conectar dos VPC.

- **Interconexión de VPC**

  Puede crear una interconexión de VPC para conectar dos VPC en la misma región. Una interconexión de VPC utiliza direcciones IP privadas para enrutar el tráfico entre dos VPC. Los ECS de cualquiera de las VPC pueden comunicarse entre sí como si estuvieran en la misma VPC.

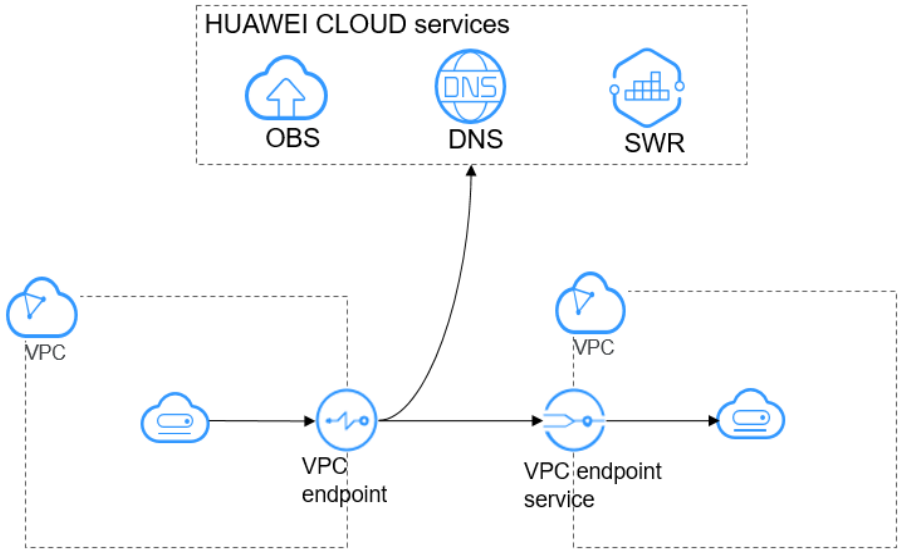
  Los bloques CIDR de dos VPC conectados por una interconexión de VPC no pueden solaparse. De lo contrario, la interconexión de VPC no tiene efecto.



- **Punto de conexión de VPC**

  El servicio de VPCEP proporciona los canales seguros y privados para permitir que sus recursos en una VPC sean accesibles desde otras VPC. Además, puede acceder a los servicios en Huawei Cloud, como OBS, SWR y DNS, a través de los puntos de conexión de VPC a través de la red privada.

  Figura 1-12 Uso del servicio VPCEP para acceder a los servicios a través de las VPC de una manera unidireccional

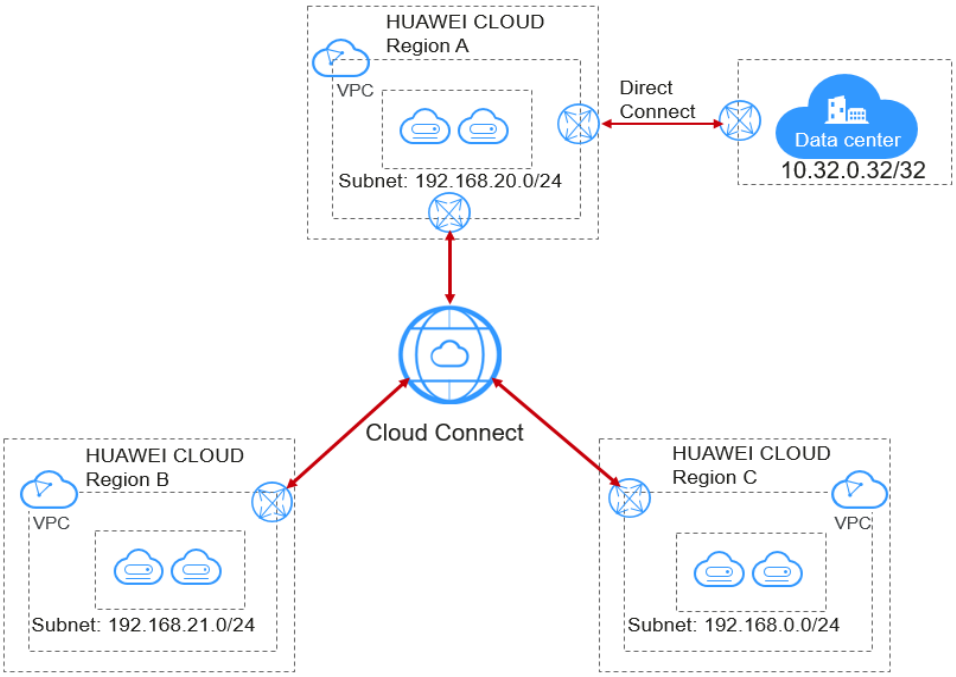


- **Cloud Connect**

  Cloud Connect le permite crear rápidamente las redes de alta calidad que pueden conectar VPC entre regiones y trabajar con Direct Connect para conectar las VPC y centros de datos locales. Con Cloud Connect, puede crear una red en la nube conectada globalmente con capacidades de comunicación y escalabilidad de clase empresarial.

Los bloques CIDR de VPC conectados por una conexión en la nube no pueden solaparse. De lo contrario, las comunicaciones de red fallarán.

Figura 1-13 Conexión de VPC en todas las regiones

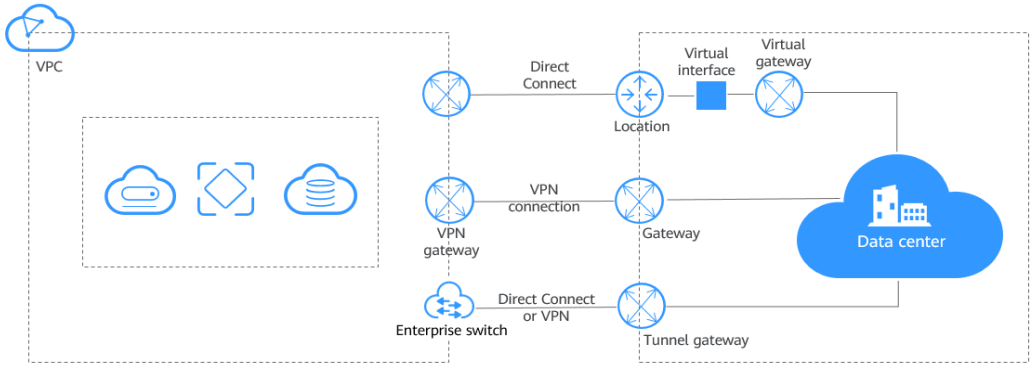


Conexión de una VPC a un centro de datos local

Si su VPC necesita comunicarse con su centro de datos local, puede usar Direct Connect o VPN junto con un L2CG.

- Direct Connect establece una conexión dedicada y sus datos no se transferirán a través de Internet.
- La VPN establece un túnel cifrado que transfiere datos a través del Internet.
- Los conmutadores empresariales solo admiten los gateway de conexión de nivel 2 (L2CG) ahora. Un L2CG es un gateway de túnel virtual que puede trabajar con Direct Connect o VPN para establecer comunicaciones de red entre redes en la nube y en las instalaciones en la capa 2. El gateway le permite migrar cargas de trabajo en los centros de datos o las nubes privadas a la nube sin cambiar las subredes y direcciones IP.

Figura 1-14 Conexión de una VPC a un centro de datos local



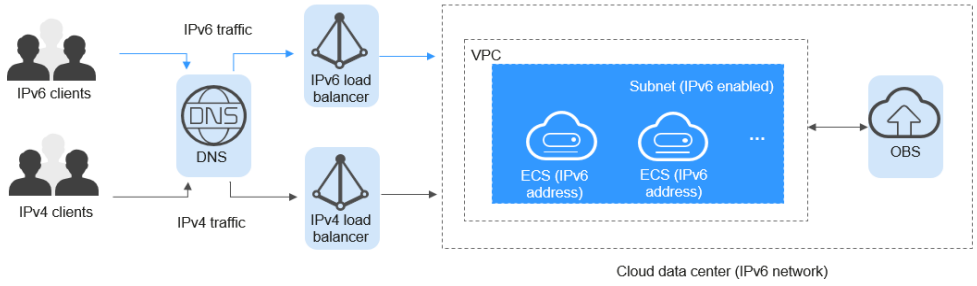
Conexión al Internet

- **Utilice los EIP para permitir que un pequeño número de ECS accedan a Internet.**

  Cuando solo unos ECS necesitan acceder a Internet, puede vincular las EIP a estos ECS. Esto les proporcionará acceso al Internet. También puede desvincular dinámicamente las EIP de los ECS y vincularlos a los gateway de NAT y los balanceadores de carga en su lugar, lo que también proporcionará acceso a Internet. El proceso no es complicado. Las EIP diferentes en la misma región pueden compartir un ancho de banda, lo que reduce sus costos de ancho de banda.

  Puede obtener las direcciones de IPv4 y de IPv6 para las comunicaciones privadas o por Internet si habilita las funciones IPv4 e IPv6 de doble pila o EIP de IPv6.

  Figura 1-15 Doble pila IPv4 e IPv6

- **Utilice un gateway de NAT para permitir que un gran número de ECS accedan a Internet.**

  Cuando un gran número de ECS necesita acceder a Internet, puede usar los gateway de NAT para sus ECS. Con los gateway de NAT, no es necesario asignar una EIP a cada ECS. Los gateway de NAT reducen los costos ya que no necesita tantas EIP. Los gateway de NAT ofrecen tanto SNAT como DNAT. SNAT permite que varios ECS en la misma VPC compartan uno o más EIP para acceder a Internet. SNAT evita que las EIP de ECS sean expuestas a Internet. DNAT puede implementar el reenvío de datos por puerto. Asigna puertos de EIP a puertos de ECS para que los ECS de una VPC puedan compartir la misma EIP y el mismo ancho de banda para proporcionar servicios accesibles a Internet.

- **Utilice ELB para si hay un gran número de solicitudes simultáneas.**

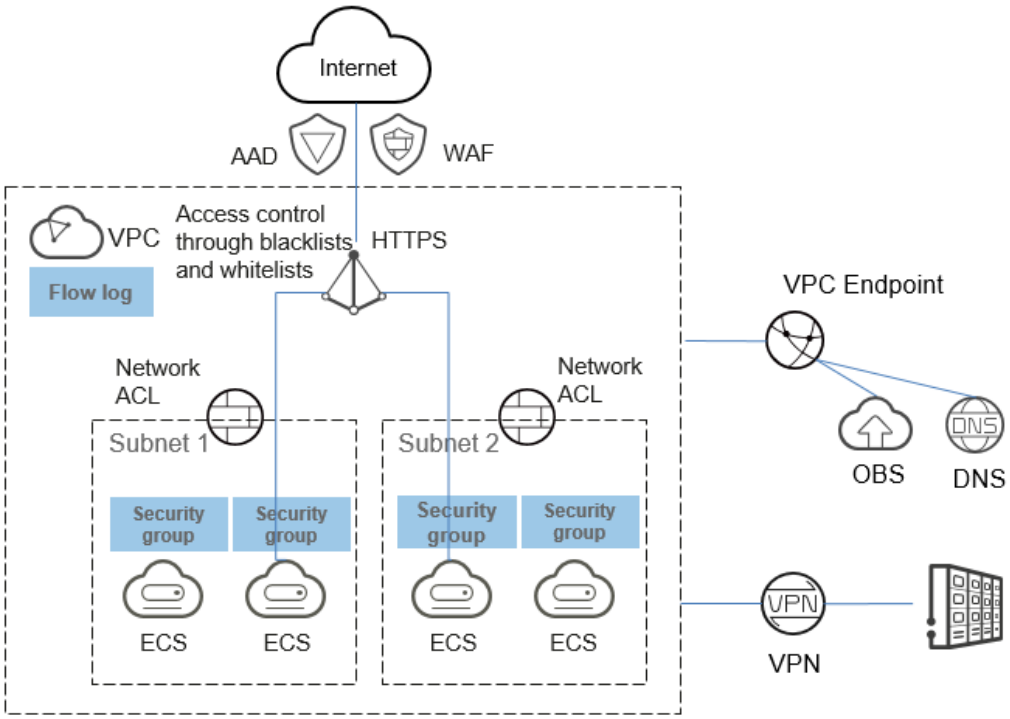
  En escenarios de alta simultaneidad, como el comercio electrónico, puede utilizar los balanceadores de carga proporcionados por el servicio de ELB para distribuir

uniformemente el tráfico entrante entre múltiples ECS, lo que permite que un gran número de usuarios accedan simultáneamente a su sistema o a la aplicación empresarial. ELB se implementa en el modo de clúster. Proporciona tolerancia a fallos para sus aplicaciones al equilibrar automáticamente el tráfico a través de múltiples AZ. ELB se integra profundamente con el servicio Auto Scaling (AS), que permite el ajuste automático basado en el tráfico de servicio y garantiza la estabilidad y fiabilidad del servicio.

1.3 Seguridad de la red

Huawei Cloud ofrece una amplia gama de servicios y funciones de seguridad para proteger sus recursos.

La siguiente figura muestra cómo los servicios y las funciones de seguridad protegen sus recursos.



Advanced Anti-DDoS (AAD) y Web Application Firewall (WAF)

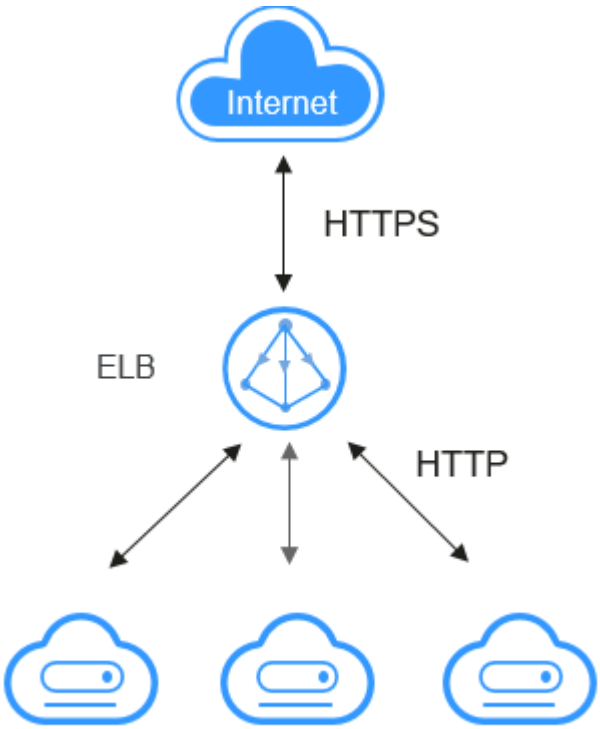
- AAD asegura la continuidad de importantes servicios empresariales. AAD ofrece direcciones IP de alta defensa para proporcionar servicios en lugar de las direcciones IP originales del servidor para sistemas externos. Los ataques maliciosos dirigidos a los servidores de origen se pueden desviar para su depuración para garantizar el funcionamiento estable de las cargas de trabajo de misión crítica. Este servicio se puede utilizar para proteger los servidores en Huawei Cloud, otras nubes y centros de datos locales.
- WAF mantiene los servicios web estables y seguros. Examina todas las solicitudes de HTTP y de HTTPS para detectar y bloquear los siguientes ataques: inyección de lenguaje de consulta estructurado (SQL), secuencias de comandos entre sitios (XSS), shells web, inyecciones de comandos y código, inclusión de archivos, acceso a archivos

confidenciales, vulnerabilidades de terceros, los ataques de Challenge Collapsar (CC), rastreadores maliciosos y falsificación de solicitudes entre sitios (CSRF).

ELB

ELB puede manejar las solicitudes de HTTPS y admitir los certificados de SSL e inicios de sesión de acceso en la capa 7. Además, puede configurar la lista negra y la lista blanca para gestionar los permisos de acceso.

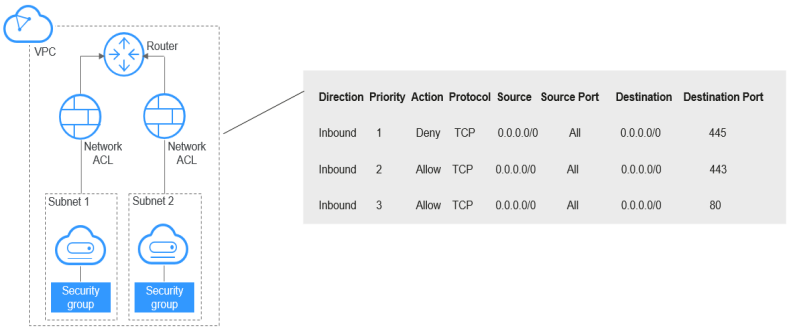
Figura 1-16 Solicitudes de HTTPS



ACL de red

Una ACL de red es una capa opcional de seguridad para las subredes. Puede asociar una o más subredes a una ACL de red para controlar el tráfico de entrada y salida de las subredes.

Figura 1-17 ACL de red

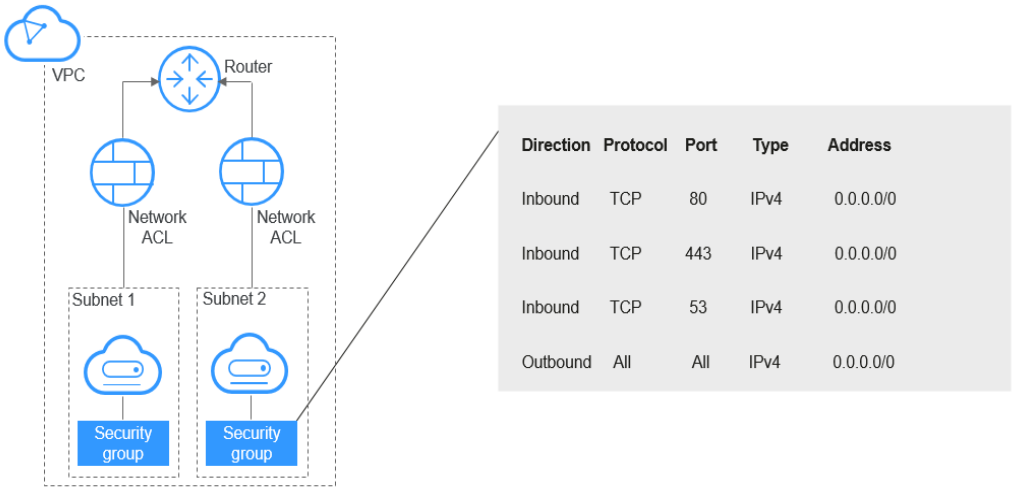


Grupo de seguridad

Un grupo de seguridad implementa el control de acceso para ECS que tienen los mismos requisitos de protección de seguridad en una VPC. Puede definir las reglas entrantes y las salientes para controlar el tráfico hacia y desde los ECS en un grupo de seguridad, haciendo que su VPC sea más segura.

Los grupos de seguridad operan a nivel de ECS, mientras que las ACL de red operan a nivel de subred. Puede utilizar las ACL de red junto con los grupos de seguridad para implementar un control de acceso completo y detallado.

Figura 1-18 Grupo de seguridad



Log de flujo de VPC

Un log de flujo de VPC registra información sobre el tráfico que va hacia y desde su VPC. Los registros de flujo de VPC le ayudan a supervisar el tráfico de red, analizar los ataques de red y determinar si las reglas de ACL de red y de grupos de seguridad requieren modificaciones.

Puede crear log de flujo para registrar información de tráfico sobre VPC, subredes o NIC para identificar el tráfico de ataques o el tráfico descartado por grupos de seguridad o ACL de red. Puede ver los registros de flujo en la consola de LTS o en los bucket de OBS. Estos logs de flujo se pueden analizar mediante herramientas de análisis de logs convencionales.

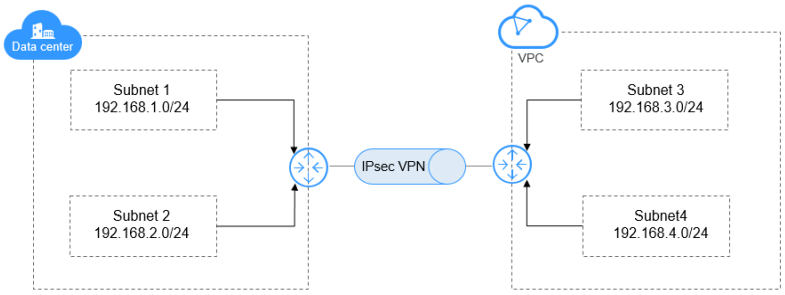
El siguiente es un registro de log de flujo de ejemplo:

```
<version> <project-id> <interface-id>  <srcaddr>      <dstaddr>       <srcport>
<dstport>   <protocol>  <packets>  <bytes>  <start>      <end>       <action>
<log-status>
1         *            *              192.168.0.59   192.168.0.218   22
39074       6           20         3997     1588743886   1588744486  ACCEPT     OK
1         *            *              192.168.0.59   192.168.0.218   22
39082       6           20         3997     1588743886   1588744486  ACCEPT     OK
1         *            *              192.168.0.218  192.168.0.59    39074
22          6           26         4033     1588743886   1588744486  ACCEPT     OK
1         *            *              192.168.0.218  192.168.0.59    39082
22          6           24         4117     1588743886   1588744486  ACCEPT     OK
```


VPN

VPN establece un túnel de comunicación seguro y encriptado entre su centro de datos local y su VPC, extendiendo rápidamente los recursos desde su centro de datos a la nube.

Figura 1-19 Establecimiento de un túnel de comunicación encriptado

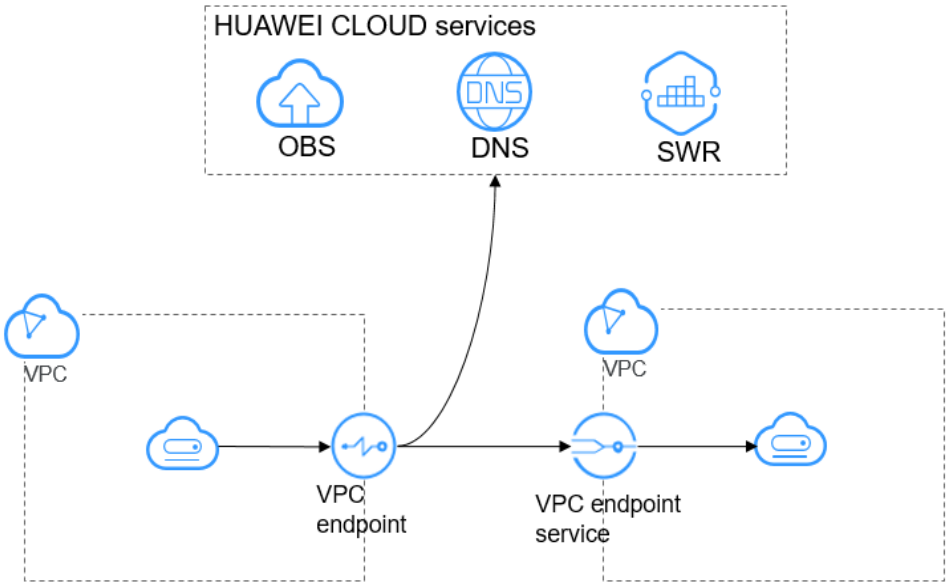


VPCEP

VPCEP proporciona los canales seguros y privados para conectar sus VPC a los servicios de conexión de VPC, incluidos los servicios en la nube o sus servicios privados, sin tener que utilizar las EIP.

El acceso es unidireccional.

Figura 1-20 Establecer un canal privado



1.4 Monitoreo de red

Huawei Cloud monitorea los siguientes recursos de red:

EIP y ancho de banda

Al monitorear el ancho de banda entrante, el ancho de banda saliente, el uso del ancho de banda, el tráfico entrante y el tráfico saliente, puede conocer la calidad de la EIP y el ancho de banda en tiempo real. Además, puede establecer reglas de alarma para generar alarmas automáticamente cuando una métrica excede el umbral, lo que garantiza la calidad de la red.

Tráfico en una VPC

Un log de flujo de VPC registra información sobre el tráfico que va hacia y desde su VPC. Los registros de flujo de VPC le ayudan a supervisar el tráfico de red, analizar los ataques de red y determinar si las reglas de ACL de red y de grupos de seguridad requieren modificaciones.

Puede crear log de flujo para registrar información de tráfico sobre VPC, subredes o NIC para identificar el tráfico de ataques o el tráfico descartado por grupos de seguridad o ACL de red. Puede ver los registros de flujo en la consola de LTS o en los bucket de OBS. Estos logs de flujo se pueden analizar mediante herramientas de análisis de logs convencionales.

El siguiente es un registro de log de flujo de ejemplo:

```
<version> <project-id> <interface-id>  <srcaddr>      <dstaddr>       <srcport>
<dstport>   <protocol>  <packets>  <bytes>  <start>      <end>       <action>
<log-status>
1         *            *              192.168.0.59   192.168.0.218   22
39074       6           20         3997     1588743886   1588744486  ACCEPT     OK
1         *            *              192.168.0.59   192.168.0.218   22
39082       6           20         3997     1588743886   1588744486  ACCEPT     OK
1         *            *              192.168.0.218  192.168.0.59    39074
22          6           26         4033     1588743886   1588744486  ACCEPT     OK
1         *            *              192.168.0.218  192.168.0.59    39082
22          6           24         4117     1588743886   1588744486  ACCEPT     OK
```


2 ¿Qué es Virtual Private Cloud?

Descripción general

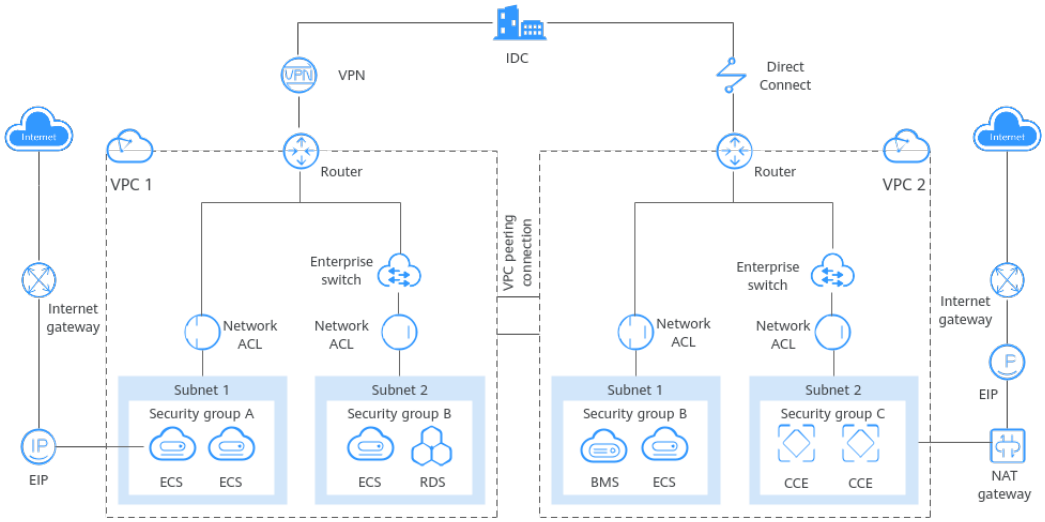
El servicio Virtual Private Cloud (VPC) le permite aprovisionar las redes virtuales aisladas y privadas lógicamente para recursos en la nube, como servidores en la nube, contenedores y bases de datos. Puede personalizar subredes, grupos de seguridad, ACL de red y asignar EIP y anchos de banda. Con Direct Connect o Virtual Private Network (VPN), puede conectar sus VPC a un centro de datos local.

El servicio VPC utiliza las tecnologías de virtualización de red, como redundancia de enlaces, clústeres de los gateway distribuidos e implementación de multi-AZ, para garantizar la seguridad, estabilidad y disponibilidad de la red.

Arquitectura del producto

La arquitectura del producto consta de componentes de VPC, características de seguridad y opciones de conectividad de VPC.

Figura 2-1 Arquitectura



Componentes de VPC

Cada VPC consta de un bloque CIDR privado, tablas de ruta y al menos una subred.

- Bloque de CIDR privado: Al crear una VPC, debe especificar el bloque de CIDR privado utilizado por la VPC. El servicio de VPC admite los siguientes bloques CIDR: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, y 192.168.0.0 – 192.168.255.255
- Subred: Los recursos de la nube, como servidores y bases de datos en la nube, deben implementarse en las subredes. Después de crear una VPC, divida la VPC en una o más subredes. Cada subred debe estar dentro de la VPC.
- Tabla de rutas: Cuando se crea una VPC, el sistema genera automáticamente una tabla de rutas predeterminada. La tabla de rutas garantiza que todas las subredes de la VPC puedan comunicarse entre sí. Si las rutas de la tabla de rutas predeterminada no pueden cumplir los requisitos de la aplicación, (por ejemplo, un ECS sin una dirección IP elástica (EIP) vinculada necesita acceder a Internet), puede crear una tabla de ruta personalizada.

Características de seguridad

Los grupos de seguridad y las ACL de red garantizan la seguridad de los recursos de nube implementados en una VPC. Un grupo de seguridad actúa como un firewall virtual para proporcionar reglas de acceso para instancias que tienen los mismos requisitos de seguridad y son de confianza mutua en una VPC. Una ACL de red se puede asociar a subredes que tienen los mismos requisitos de control de acceso. Puede agregar las reglas entrantes y las salientes para controlar con precisión el tráfico entrante y e saliente en el nivel de subred.

Conectividad de VPC

Huawei Cloud ofrece múltiples opciones de conectividad de VPC para satisfacer diversos requisitos.

- La interconexión de VPC permite que dos VPC de la misma región se comuniquen entre sí mediante direcciones IP privadas.
- Elastic IP o NAT Gateway permite que los ECS en una VPC se comuniquen con Internet.
- La red privada virtual (VPN), Cloud Connect o Direct Connect pueden conectar una VPC a su centro de datos.

Acceso al servicio de VPC

Puede acceder al servicio de VPC a través de la consola de gestión o mediante API basadas en HTTPS.

- Consola de gestión

  Puede utilizar la consola para realizar las operaciones directamente en los recursos de VPC. Para acceder al servicio de VPC, inicie sesión en la consola de gestión y seleccione **Virtual Private Cloud** en la página principal de la consola.

- API

  Si necesita integrar el servicio de VPC proporcionado por el sistema en la nube en un sistema de terceros para desarrollo secundario, puede usar las API para acceder al servicio de VPC.

3 Ventajas del producto

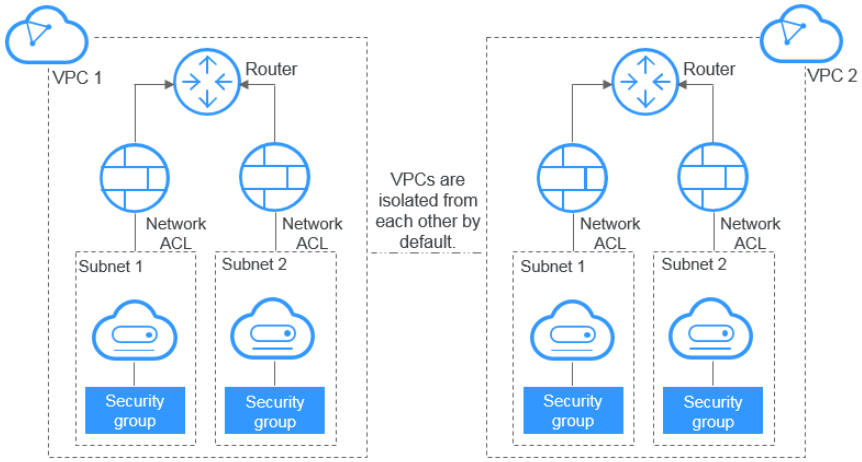
Configuración flexible

Puede crear VPC, agregar subredes, especificar intervalos de direcciones IP y configurar tablas de DHCP y de enrutamiento. Puede configurar la misma VPC para ECS que se encuentren en diferentes zonas de disponibilidad (AZ).

Segura y confiable

Cada VPC está aislada lógicamente de otras VPC utilizando la tecnología de túnel. De forma predeterminada, las VPC diferentes no pueden comunicarse entre sí. Puede utilizar ACL de red para proteger las subredes y utilizar los grupos de seguridad para proteger ECS. Agregan las capas adicionales de seguridad a sus VPCs, lo que hace que su red sea segura.

Figura 3-1 Segura y confiable



Interconectividad sin inconvenientes

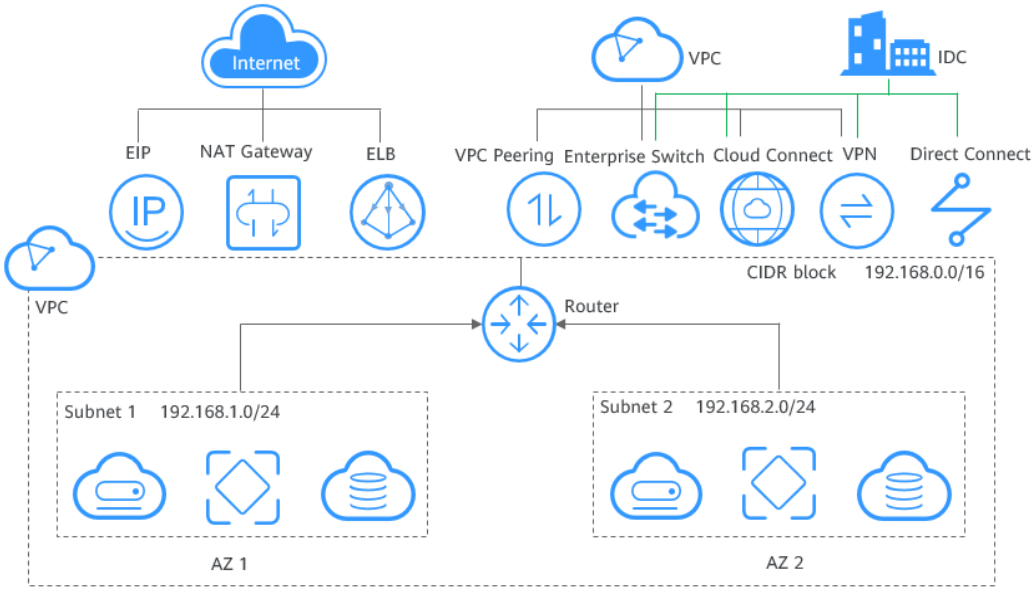
De forma predeterminada, las instancias de una VPC no pueden acceder a Internet. Puede aprovechar EIP, balanceadores de carga, gateways de NAT, conexiones de VPN y conexiones de Direct Connect para habilitar el acceso a o desde Internet.

Por defecto, las instancias en dos VPC no pueden comunicarse entre sí. Puede crear un interconexión de VPC para permitir que las instancias de las dos VPC de la misma región se comuniquen entre sí mediante direcciones IP privadas.

Puede utilizar un gateway de conexión de nivel 2 (L2CG) proporcionado por nuestro servicio Enterprise Switch para establecer la comunicación de red entre la nube y las redes locales, y migrar el centro de datos o los servicios de nube privada a la nube sin cambiar las subredes.

Se proporcionan múltiples opciones de conectividad para satisfacer diversos requisitos de servicio para la nube, lo que le permite implementar aplicaciones empresariales con facilidad y reducir los costos de operación y mantenimiento de TI empresarial (O&M).

Figura 3-2 Interconectividad



Acceso a alta velocidad

El BGP dinámico se utiliza para proporcionar acceso a varias redes portadoras. Puede establecer más de 20 conexiones BGP dinámicas a múltiples operadores. Las conexiones de BGP dinámicas permiten la conmutación por error en tiempo real basada en protocolos de enrutamiento preestablecidos, lo que garantiza una alta estabilidad de la red, una baja latencia de la red y un acceso fluido a los servicios en la nube.

Comparación de ventajas

Tabla 3-1 enumera las ventajas de una VPC sobre un IDC tradicional.

Tabla 3-1 Comparación entre una VPC y una IDC tradicional

Concepto	VPC	IDC tradicional
Ciclo de implementación	● No es necesario realizar una implementación de ingeniería compleja, incluida la planificación de ingeniería y el cableado. ● Puede determinar sus redes, subredes y rutas en Huawei Cloud en función de los requisitos de servicio.	Es necesario configurar redes y realizar pruebas. Todo el proceso toma mucho tiempo y requiere un soporte técnico profesional.
Costo total	Huawei Cloud ofrece modos de facturación flexibles para los servicios de red, para que pueda seleccionar el que mejor se adapte a sus necesidades empresariales. Además, debido a que no hay costos iniciales y costos de operación de red, el costo total de propiedad (TCO) se reduce significativamente.	Es necesario invertir mucho en salas de equipos, fuentes de alimentación, construcción y materiales de hardware. También necesita los equipos profesionales de O&M para garantizar la seguridad de la red. Los costos de gestión de activos aumentan con cualquier cambio en los requisitos del negocio.
Flexibilidad	Una variedad de servicios de red están disponibles para que usted pueda elegir. Si necesita más recursos de red (como ancho de banda), puede realizar rápidamente una expansión dinámica.	Debe cumplir estrictamente con el plan de red para completar la implementación del servicio. Si hay cambios en sus requisitos de servicio, es difícil ajustar dinámicamente la red.
Seguridad	Las VPC están aisladas lógicamente entre sí. Puede aprovechar las características de seguridad como las ACL de red y los grupos de seguridad, e incluso los servicios de seguridad como el Anti-DDoS avanzado (AAD) para proteger sus recursos en la nube.	La red es difícil de mantener y tiene una seguridad deficiente. Por lo tanto, necesita personal técnico profesional para garantizar la seguridad de la red.

4 Escenarios de la aplicación

Redes dedicadas en la nube

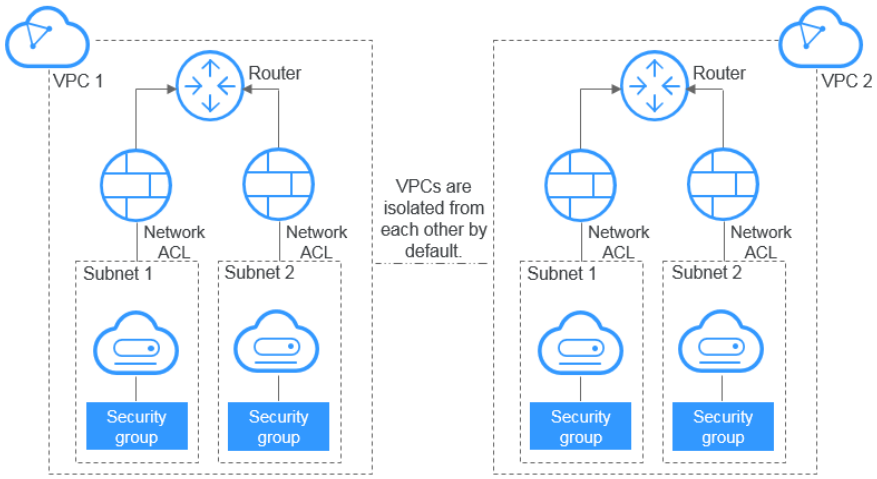
Caso

Cada VPC representa una red privada y está lógicamente aislada de otras VPC. Puede implementar su sistema de servicio en una VPC para crear un entorno de red privada en la nube. Si tiene varios sistemas de servicio, por ejemplo, un sistema de producción y un sistema de prueba, puede implementarlos en dos VPC diferentes para aislarlos. Si desea establecer comunicación entre estas dos VPC, puede crear una interconexión de VPC entre ellas.

Servicios Relacionados

ECS

Figura 4-1 Redes dedicadas en la nube



Alojamiento de sitios web o aplicaciones web

Caso

Puede alojar las aplicaciones de web y sitios web en una VPC y utilizar la VPC como una red normal. Con los gateway de EIP o de NAT, puede conectar los ECS que ejecutan sus aplicaciones web a Internet. Puede utilizar los balanceadores de carga proporcionados por el servicio de ELB para distribuir uniformemente el tráfico entre múltiples ECS.

Los recursos en la nube de una VPC pueden usar los siguientes servicios en la nube para conectarse a Internet.

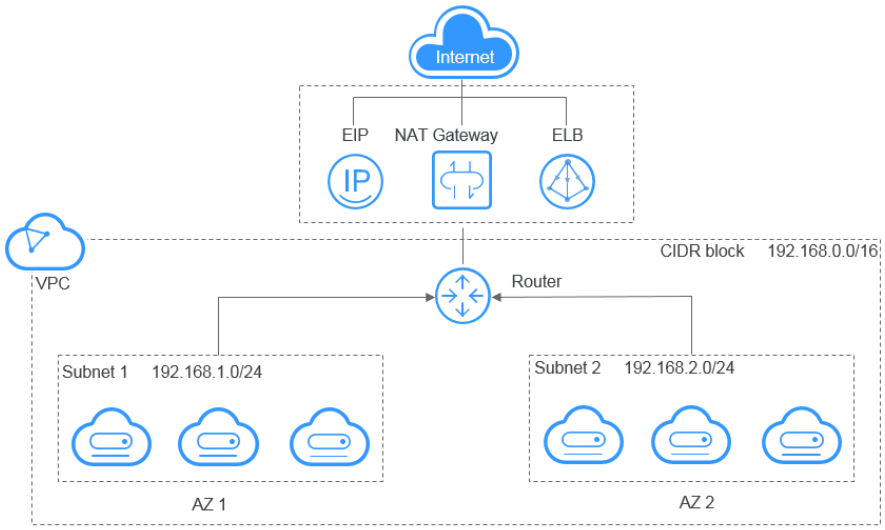
Tabla 4-1 Acceso a Internet

Servicio en la nube	Escenario de la aplicación	Descripción
EIP	Un solo ECS accede a Internet.	Puede asignar una EIP y vincularla a un ECS para que el ECS pueda acceder a Internet o proporcionar servicios accesibles desde Internet. Puede desvincular la EIP del ECS para desactivar el acceso en cualquier momento. Puede utilizar el ancho de banda compartido y los paquetes de datos compartidos para optimizar los costos.
NAT Gateway	Múltiples ECS comparten una EIP para acceder a Internet.	Un gateway de NAT ofrece tanto la traducción de direcciones de red de origen (SNAT) como la traducción de direcciones de red de destino (DNAT). SNAT permite que varios ECS en la misma VPC compartan las EIP para acceder a Internet. De esta manera, puede reducir los costes de gestión y evitar que las EIP de los ECS se expongan a Internet. DNAT implementa el reenvío de datos a nivel de puerto. Asigna puertos de EIP a puertos de ECS para que los ECS de una VPC puedan compartir la misma EIP y el mismo ancho de banda para proporcionar servicios accesibles a Internet. Sin embargo, DNAT no equilibra el tráfico.
ELB	Utilice los balanceadores de carga proporcionados por el servicio de ELB para distribuir uniformemente el tráfico entrante a través de múltiples ECS en escenarios de alta simultaneidad, como el comercio electrónico.	Los balanceadores de carga distribuyen el tráfico a través de múltiples ECS backend, equilibrando la carga de trabajo en cada ECS (en la capa 4 o la capa 7). Puede vincular las EIP a los ECS para permitir el acceso desde Internet. ELB amplía las capacidades de servicio de sus aplicaciones y mejora la disponibilidad al eliminar puntos únicos de fallas.

Servicios Relacionados

ECS, EIP, NAT Gateway y ELB

Figura 4-2 Alojamiento de sitios web o aplicaciones web



Control de acceso a aplicaciones web

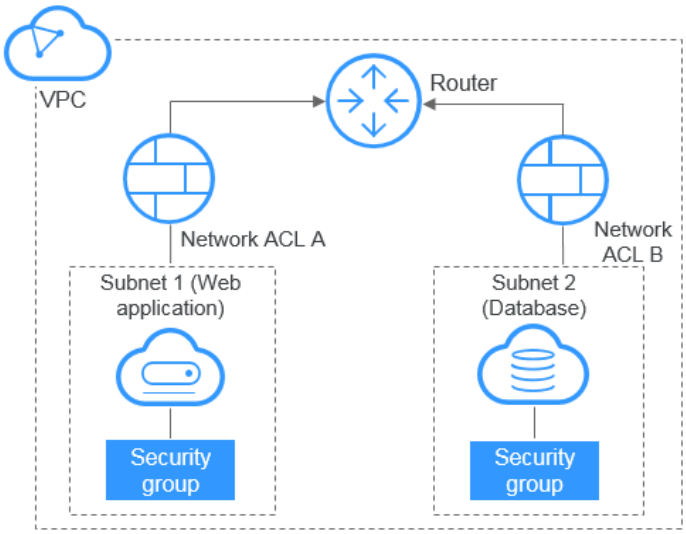
Caso

Puede crear una VPC y unos grupos de seguridad para alojar aplicaciones web de varios niveles en diferentes zonas de seguridad. Puede asociar servidores web y servidores de bases de datos con distintos grupos de seguridad, y configurar distintas reglas de control de acceso para los grupos de seguridad. Puede iniciar servidores Web en una subred de acceso público y también ejecutar servidores de base de datos en subredes que no son de acceso público. De esta manera, puede garantizar una alta seguridad.

Servicios Relacionados

ECS

Figura 4-3 Control de acceso a aplicaciones web



Opciones de conectividad de VPC

Caso

Puede utilizar los siguientes servicios en la nube para permitir que dos VPC se comuniquen entre sí.

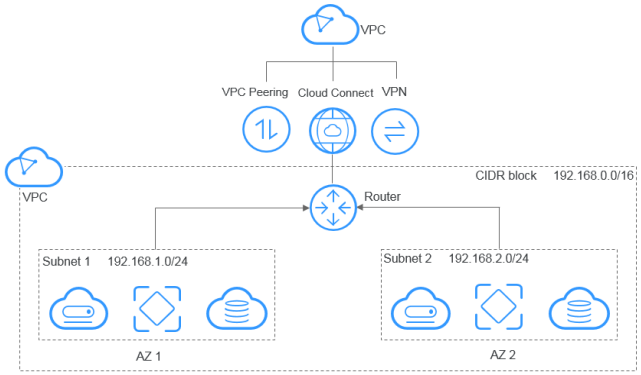
Tabla 4-2 Conexión de VPC

Servicio en la nube	Escenario de la aplicación	Descripción
VPC Peering	Conecte las VPC en la misma región.	Puede solicitar una interconexión de VPC con otra VPC en su cuenta o en otra cuenta, pero las dos VPC deben estar en la misma región. Las interconexión de VPC son gratis.
Cloud Connect	Conecte las VPC en diferentes regiones.	Cloud Connect le permite conectar dos VPC en la misma cuenta o en diferentes cuentas, incluso si se encuentran en diferentes regiones.
VPN	Utilice VPN para conectar las VPC en todas las regiones a un bajo costo.	La VPN utiliza un túnel de comunicaciones cifrado para conectar las VPC en las diferentes regiones y envía tráfico a través de Internet. Es barato, fácil de configurar y fácil de usar. Sin embargo, la calidad de las conexiones de VPN depende de la calidad de las conexiones a Internet.

Servicios Relacionados

ECS, Cloud Connect y VPN

Figura 4-4 Opciones de conectividad de VPC



Despliegue de la nube híbrida

Caso

Si tiene un centro de datos local y no desea migrar toda su empresa a la nube, puede crear una nube híbrida para que pueda mantener los datos principales en su centro de datos.

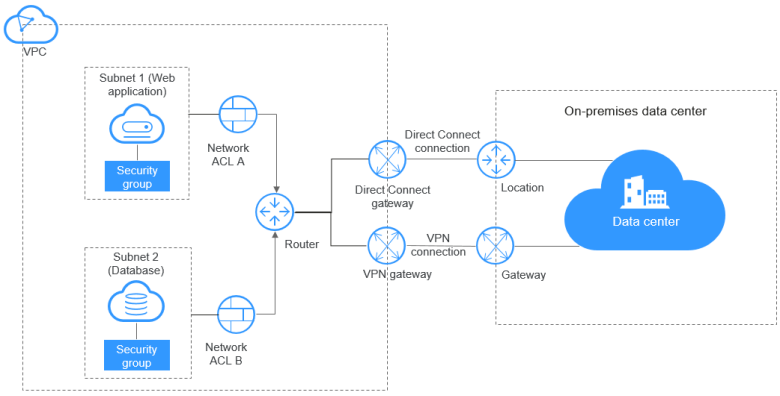
Tabla 4-3 Conexión a un centro de datos local

Servicio en la nube	Escenario de la aplicación	Descripción
VPN	Utilice una VPN para conectar una VPC a un centro de datos local a un bajo costo.	La VPN utiliza un túnel de comunicaciones cifrado para conectar una VPC en la nube a un centro de datos local y envía tráfico a través de Internet. Es barato, fácil de configurar y fácil de usar. Sin embargo, la calidad de las conexiones de VPN depende de la calidad de las conexiones a Internet.
Direct Connect	Utilice una conexión física para conectar una VPC a un centro de datos local.	Direct Connect proporciona las conexiones físicas entre las VPC y los centros de datos. Cuenta con baja latencia y es muy seguro. Direct Connect es una buena opción si tiene requisitos estrictos sobre la calidad de la transmisión de la red.

Servicios Relacionados

Cloud Connect, ECS, Direct Connect y VPN

Figura 4-5 Despliegue de la nube híbrida



5 Funciones

Tabla 5-1 enumera las funciones comunes de la VPC.

Antes de utilizar el servicio de VPC, puede familiarizarse con los conceptos básicos, como subredes, tablas de rutas, grupos de seguridad y EIP, para comprender mejor las funciones de VPC.

Tabla 5-1 Funciones comunes de VPC

Categoría	Función	Descripción
VPC y subred	VPC	Una VPC proporciona una red virtual aislada para sus recursos en la nube. Puede configurar y gestionar la red de forma flexible. Puede crear VPC, modificar información básica sobre VPC, agregar un bloque CIDR secundario a una VPC, eliminar un bloque CIDR secundario de una VPC, eliminar VPC y exportar la lista de VPC.
	Subred	Una subred es un bloque CIDR único con un rango de direcciones IP en su VPC. Todos los recursos de una VPC deben implementarse en las subredes. Puede crear subredes, modificar la información de subred y eliminar subredes.
	Tabla de rutas	Una tabla de rutas contiene las rutas que determinan a dónde se dirige el tráfico. Cuando se crea una VPC, el sistema crea automáticamente una tabla de ruta predeterminada. La tabla de rutas garantiza que todas las subredes de la VPC puedan comunicarse entre sí. También puede agregar las rutas personalizadas para controlar a dónde se dirige el tráfico. Puede agregar, consultar, modificar y eliminar rutas.

Categoría	Función	Descripción
	Dirección IP virtual	Una dirección IP virtual se puede compartir entre múltiples ECS. Puede configurar las direcciones IP privadas y virtuales para un ECS, y puede acceder al ECS a través de cualquiera de las direcciones IP. Una dirección IP virtual tiene la misma capacidad de acceso a la red que una dirección IP privada. Si necesita alta disponibilidad, puede utilizar las direcciones IP virtuales porque admiten la conmutación de ECS activa/en standby. Puede asignar y liberar las direcciones IP virtuales, vincular una dirección IP virtual a una EIP o un ECS y acceder a una dirección IP virtual a través de una EIP, una VPN, Direct Connect o la interconexión de VPC.
	Red de doble pila IPv4 e IPv6	La doble pila IPv4 e IPv6 permite que sus recursos utilicen las direcciones IPv4 e IPv6 para la comunicación de redes públicas y privadas. Huawei Cloud es compatible con la pila dual IPv4/IPv6. Puede crear una red de doble pila IPv4/IPv6 o agregar una subred IPv6 a una VPC para formar una red de doble pila.
	Log de flujo de VPC	Un log de flujo de VPC registra información sobre el tráfico que va hacia y desde una VPC. Los registros de flujo de VPC le ayudan a supervisar el tráfico de red, analizar los ataques de red y determinar si los grupos de seguridad y las reglas de la red de ACL requieren modificaciones. Puede crear, ver, habilitar, deshabilitar y eliminar logs de flujo de VPC.
Control de acceso	Grupo de seguridad	Un grupo de seguridad es una colección de reglas de control de acceso para ECS que tienen los mismos requisitos de protección de seguridad y son de confianza mutua dentro de una VPC. Puede crear un grupo de seguridad y definir diferentes reglas de acceso para proteger los ECS que contiene. Puede crear y eliminar grupos de seguridad, agregar, replicar, modificar, eliminar, importar o exportar reglas de grupos de seguridad, ver el grupo de seguridad de un ECS, cambiar el grupo de seguridad de un ECS y agregar recursos de nube o eliminarlos de un grupo de seguridad.

Categoría	Función	Descripción
	ACL de red	Una ACL de red es una capa opcional de seguridad para las subredes. Puede asociar una o más subredes a una ACL de red para controlar el tráfico de entrada y salida de las subredes. Puede crear, ver, modificar, eliminar, habilitar, deshabilitar las ACL de red, asociar subredes con las ACL de red o disociarlas de ellas, y agregar, modificar, cambiar la secuencia, habilitar, deshabilitar y eliminar reglas de ACL de red.
	Grupo de direcciones IP	Un grupo de direcciones IP es una colección de direcciones IP que utilizan la misma regla de grupo de seguridad. Un grupo de direcciones IP puede ser utilizado para gestionar direcciones IP que tengan los mismos requerimientos de seguridad o cuyos requerimientos de seguridad cambien de manera frecuente. Un grupo de direcciones IP le libera de modificar repetidamente las reglas del grupo de seguridad y simplifica la gestión de reglas. Puede crear un grupo de direcciones IP, asociar un grupo de direcciones IP a una regla de grupo de seguridad y modificar y eliminar un grupo de direcciones IP.
EIP y ancho de banda	EIP	El servicio Elastic IP (EIP) le permite utilizar direcciones IP públicas estáticas y anchos de banda escalables para conectar sus recursos de nube a Internet. Puede asignar las EIP, vincular las EIP a recursos en la nube, desvincular las EIP de recursos en la nube, liberar las EIP, modificar el ancho de banda de EIP y actualizar BGP estático a BGP dinámico.
	Anchos de banda compartidos	Un ancho de banda compartido permite que varias EIP compartan el mismo ancho de banda. Todos los ECS, BMS y balanceadores de carga que tienen EIP enlazados en la misma región pueden compartir un ancho de banda. Puede asignar, modificar, eliminar un ancho de banda compartido, agregar EIP a un ancho de banda compartido y eliminar EIP de un ancho de banda compartido.

Categoría	Función	Descripción
	Paquete de datos compartidos	Un paquete de datos compartido proporciona una cuota para el uso de datos. Tales envases son rentables y fáciles de usar. Los paquetes de datos compartidos entran en vigor inmediatamente después de su compra. Si se ha suscrito a EIP de pago por uso utilizando el ancho de banda facturado por tráfico en una región y compra un paquete de datos compartidos en la misma región, los EIP utilizarán el paquete de datos compartidos. Una vez que la cuota del paquete se agote o que el paquete venza, los EIP se seguirán facturando en modo de pago por uso.
Interconexión de recursos	Interconexión de VPC	Una interconexión de VPC es una conexión de red entre dos VPC. Una interconexión de VPC permite que dos VPC se comuniquen entre sí usando direcciones IP privadas como si estuvieran en la misma VPC. Puede crear una interconexión de VPC entre sus propias VPC o entre su VPC y una VPC de otra cuenta dentro de la misma región. Sin embargo, no puede crear una interconexión de VPC entre las VPC en diferentes regiones. Puede crear una interconexión de VPC con otra VPC en su cuenta o con una VPC en otra cuenta. También puede ver, modificar y eliminar interconexión de VPC.
Monitoreo	Consulta de métricas	Puede ver el ancho de banda y el uso de EIP del servicio de VPC a través de Cloud Eye, crear y establecer reglas de alarma, y personalizar los objetos monitoreados y las políticas de notificación sin agregar complementos.
Auditoría	Consulta de logs de auditoría	Con CTS, puede registrar las operaciones realizadas en el servicio de VPC para fines de consulta, auditoría y seguimiento posterior. Puede ver y exportar registros de operaciones de los últimos siete días en la consola CTS.
Etiqueta	Gestión de etiquetas	Las etiquetas le ayudan a identificar y gestionar recursos en la nube. Puede gestionar las etiquetas de VPC, las etiquetas de subred y las etiquetas en Huawei Cloud.
Permisos	Gestión de permisos	Puede utilizar Identity and Access Management (IAM) para implementar una gestión de permisos detallada para sus VPC, lo que permite a las empresas establecer diferentes permisos de acceso en función de las organizaciones y las responsabilidades. Puede crear un usuario de IAM, conceder permisos al usuario y crear políticas de VPC personalizadas.

6 Notas y restricciones

VPC

Tabla 6-1 enumera las cuotas de recursos de VPC por región para su cuenta.

Tabla 6-1 Cuotas de recurso de VPC

Recurso	Cuota por defecto	Cómo aumentar la cuota
VPC por cuenta	5	Envíe un ticket de servicio.
Subredes por cuenta	100	Envíe un ticket de servicio.
Grupos de seguridad por cuenta	100	Envíe un ticket de servicio.
Reglas de grupo de seguridad por cuenta	5000	Envíe un ticket de servicio.
Rutas por tabla de ruta	200	Esta cuota no puede aumentarse.
Tabla de rutas por defecto por VPC	1	Envíe un ticket de servicio.
Interconexión de VPC por región	50	Esta cuota no puede aumentarse.
ACL de red por cuenta	200	Envíe un ticket de servicio.
ECS que pueden enlazarse con una dirección IP virtual	10	Esta cuota no puede aumentarse.

- La cuota anterior se aplica a una sola cuenta.
- Se recomienda que un ACL de red no contenga más de 20 reglas en una dirección. De lo contrario, su rendimiento puede deteriorarse.

Grupo de seguridad

- De forma predeterminada, puede crear un máximo de 100 grupos de seguridad en su cuenta en la nube.
- De forma predeterminada, puede agregar hasta 50 reglas de grupo de seguridad a un grupo de seguridad.
- De forma predeterminada, no puede asociar más de cinco grupos de seguridad a cada ECS o NIC de extensión. En tal caso, las reglas de todos los grupos de seguridad seleccionados se agregan para que surtan efecto.
- Si un servidor en la nube o una NIC de extensión están asociados a varios grupos de seguridad, las reglas de grupo de seguridad se aplicarán según la siguiente secuencia: el primer grupo de seguridad asociado tendrá prioridad sobre los asociados más tarde, luego la regla con la prioridad más alta en ese grupo de seguridad se aplicará primero.
- Puede agregar un máximo de 20 instancias a un grupo de seguridad a la vez.
- No agregue más de 1000 instancias al mismo grupo de seguridad. De lo contrario, el rendimiento del grupo de seguridad puede verse afectado.
- Las reglas de grupo de seguridad con ciertas configuraciones no tienen efecto para los ECS de ciertas especificaciones. **Tabla 6-2** muestra los detalles.

Tabla 6-2 Escenarios en los que las reglas del grupo de seguridad no entran en vigor

Configuración de regla	Tipo de ECS
• **Action** se establece en **Deny**. • **Source** o **Destination** se establece en **IP address group**.	No se admiten los siguientes tipos de ECS x86: • Memoria optimizada (ECS M1) • Cómputo de alto rendimiento (ECS H1) • Intensivo de disco (ECS D1) • Acelerada por GPU (ECS G1 y G2) • Memoria grande (ECS E1, E2 y ET2)
Port se establece en puertos no consecutivos.	No se admiten los siguientes tipos de ECS x86: • Cómputo general (ECS S1, C1 y C2) • Memoria optimizada (ECS M1) • Cómputo de alto rendimiento (ECS H1) • Intensivo de disco (ECS D1) • Acelerada por GPU (ECS G1 y G2) • Memoria grande (ECS E1, E2 y ET2)
	No se admiten todos los ECS de Kunpeng.

ACL de red

- De forma predeterminada, puede crear un máximo de 200 ACL de red en su cuenta en la nube.
- Puede asociar una ACL de red con varias subredes. Sin embargo, una subred solo se puede asociar a una ACL de red a la vez.
- Se recomienda que una ACL de red no contenga más de 20 reglas en una dirección. De lo contrario, su rendimiento puede deteriorarse.

- Para un rendimiento óptimo, no importa más de 40 reglas de ACL de red a la vez. Las reglas existentes seguirán estando disponibles después de importar las reglas nuevas. Cada regla se puede importar solo una vez.

Tabla de rutas

- Cuando se crea una VPC, el sistema genera automáticamente una tabla de ruta predeterminada para la VPC.
- Se puede agregar un máximo de 200 rutas a cada tabla de rutas.
- No se puede eliminar la tabla de rutas predeterminada.
- La ruta del sistema no se puede modificar ni eliminar.
- Las rutas entregadas por los servicios VPN, Cloud Connect y Direct Connect a la tabla de rutas predeterminada no se pueden modificar ni eliminar.

Interconexión de VPC

- Si dos VPC conectadas por una interconexión de VPC se superponen entre sí, habrá conflictos de ruta y la interconexión de VPC puede no ser utilizable.

  Después de crear una interconexión de VPC, el comando ping puede usarse para comprobar si dos VPC pueden comunicarse entre sí, pero no puede usarse para comprobar si los gateway de la subred par están conectadas.
- Si dos VPC se superponen entre sí, solo puede crear una interconexión de VPC para habilitar la comunicación entre subredes específicas (no superpuestas) en las VPC. Asegúrese de que las subredes que se van a interconectar no se superpongan.
- Si hay tres VPC, A, B y C, y la VPC A está interconectada con VPC B y VPC C, pero VPC B y VPC C se superponen entre sí, no puede configurar rutas con los mismos destinos para la VPC A.
- No puede tener más de una interconexión de VPC entre las mismas dos VPC al mismo tiempo.
- Una interconexión de VPC entre las VPC en diferentes regiones no surtirá efecto.
  - Para permitir que las VPC de diferentes regiones se comuniquen entre sí, puede usar Cloud Connect.
- Si solicita una interconexión de VPC con una VPC de otra cuenta, la conexión solo se aplicará después de que la cuenta del mismo nivel acepte la solicitud. Si solicita una interconexión de VPC con un VPC propio, el sistema acepta automáticamente la solicitud y activa la conexión.
- Para garantizar la seguridad, no acepte la interconexión de VPC de las cuentas desconocidas.
- El propietario de una VPC en una interconexión puede eliminar la interconexión de VPC en cualquier momento. Si uno de sus propietarios elimina una interconexión de VPC, toda la información sobre esta conexión también se eliminará inmediatamente, incluidas las rutas agregadas para la interconexión de VPC.
- Después de establecer una interconexión de VPC, las cuentas local y de par deben agregar rutas a las tablas de ruta de las VPC local y de par para permitir la comunicación entre las dos VPC.
- No se puede eliminar una VPC que tiene rutas configuradas para una interconexión de VPC.

- Se puede crear una interconexión de VPC entre las VPC de la misma región incluso si uno se crea en la consola de Huawei Cloud China continental y otro en la consola internacional de Huawei Cloud.

Log de flujo de VPC

- Actualmente, solo los ECS S2, M2, Hc2, D2, Pi1, S3, C3, M3, H3, Ir3, I3, S6, E3, C3ne, M3ne, G5, P2v, C6, M6, Pi1, y H3 admiten logs de flujo de VPC.
- De forma predeterminada, puede crear un máximo de 10 logs de flujo de VPC.
- De forma predeterminada, se admite un máximo de 400,000 logs de flujo.

Dirección IP virtual

- Las direcciones IP virtuales no se recomiendan cuando se configuran varias NIC en la misma subred en un ECS. Es demasiado fácil que haya conflictos de ruta en el ECS, lo que causaría un fallo de comunicación usando la dirección IP virtual.
- Una dirección IP virtual solo puede enlazarse a ECS en la misma subred.
- Se recomienda que no más de ocho direcciones IP virtuales estén vinculadas a un ECS.
- Se recomienda que no más de 10 ECS estén vinculados a una dirección IP virtual.

EIP

Tenga en cuenta lo siguiente:

- Cada EIP puede estar vinculado a un solo recurso en la nube y debe estar en la misma región.
- Un EIP y su recurso en la nube enlazado pueden utilizar diferentes modos de facturación.
- El número de EIP que puede asignar varía según la región.
- Un EIP que ya ha estado vinculado a un recurso en la nube no puede vincularse a otro recurso sin antes estar desvinculado del recurso actual.
- Si un EIP se factura por ancho de banda, su ancho de banda máximo puede ser de 2000 Mbit/s (500 Mbit/s en la región **CN-Hong Kong**). Si necesita un mayor ancho de banda, envíe un ticket de servicio o póngase en contacto con su administrador de cuenta.
- Si un EIP es facturado por el tráfico, su ancho de banda máximo puede ser de 300 Mbit/s.
- Si una CIE se congela debido a atrasos en la cuenta o por razones de seguridad, la CIE no puede estar vinculada o sin consolidar.
- Si el ancho de banda de EIP usado excede el tamaño adquirido o es atacado (generalmente por ataques DDoS), el EIP será bloqueado pero puede ser vinculado o no.
- Su solicitud de aumento de cuota solo se aprobará si su cuenta tiene pedidos válidos y está utilizando continuamente recursos en la nube. Si ha liberado recursos inmediatamente después de suscribirse a ellos varias veces, se rechazará su solicitud de aumento de cuota.
- Solo puede liberar EIPs no unidos.
- El sistema le asigna preferentemente los EIP de aquellos que haya liberado, si los hubiera. Sin embargo, si alguno de estos EIP ya está asignado a otro usuario, no se puede reasignar a usted.
- El precio de un EIP de pago por uso incluye la tarifa de retención y el precio del ancho de banda. Si desvincula un EIP pero no lo libera, se le seguirá facturando y el precio

incluye la tarifa de retención y el precio del ancho de banda. En el momento en que vincula un EIP a una instancia, la tasa de retención ya no está incluida en el precio del EIP.

- Los EIP no se pueden transferir entre cuentas.

Solo el modo de facturación de pago por uso es compatible en las regiones de América Latina. El ancho de banda en las regiones **LA-Mexico City1** y **LA-Sao Paulo1** oscila entre 1 Mbit/s y 1000 Mbit/s.

Ancho de banda

- El tamaño mínimo de un ancho de banda compartido que se puede comprar es de 5 Mbit/s. Solo puede agregar EIP de pago por uso a un ancho de banda compartido.
- Cada cuenta puede tener un máximo de 5 anchos de banda compartidos. Si necesita más anchos de banda compartidos, envíe un ticket de servicio para solicitar un aumento de cuota.
- Dentro del período de validez de un ancho de banda utilizado por un EIP anual/mensual, solo puede aumentar el tamaño del ancho de banda. Si desea tener un tamaño de ancho de banda más pequeño, solo puede reducir el ancho de banda cuando renueve la suscripción.
- Si un EIP de pago por uso facturado por tráfico utiliza un ancho de banda dedicado, solo se facturará el ancho de banda utilizado en la dirección de salida.Si el ancho de banda saliente es mayor que 100 Mbit/s, el ancho de banda entrante será el mismo que el ancho de banda saliente.
- Un ancho de banda dedicado controla el límite de transferencia de datos en un único EIP. La velocidad de transferencia de datos en los EIP no se puede personalizar.
- Un ancho de banda compartido no puede controlar el límite de transferencia de datos en un único EIP. La velocidad de transferencia de datos en los EIP no se puede personalizar.
- Un ancho de banda compartido o un ancho de banda dedicado solo pueden ser utilizados por los recursos de su misma cuenta.

- El ancho de banda entrante se refiere al ancho de banda consumido cuando los datos se transfieren desde Internet a Huawei Cloud. El ancho de banda saliente se refiere al ancho de banda consumido cuando los datos se transfieren desde Huawei Cloud a Internet.
- Las reglas de límite para los anchos de banda públicos se cambiaron el 31 de julio de 2020, 00:00:00 GMT+08:00 en las regiones continentales de China, incluyendo CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1, y CN North-Ulanqab1.

  Las reglas de límite para anchos de banda públicos se cambiaron el 10 de diciembre de 2021, 00:00:00 GMT+08:00 en la región CN-Hong Kong.

  Después del cambio:

  - Si el ancho de banda adquirido o modificado es de hasta 10 Mbit/s, el ancho de banda entrante será de 10 Mbit/s, y el ancho de banda saliente será el mismo que el ancho de banda adquirido o modificado.
  - Si el ancho de banda adquirido o modificado es más de 10 Mbit/s, ambos anchos de banda en las direcciones entrantes y salientes serán los mismos que el ancho de banda comprado o modificado.

Paquetes de datos compartidos

- Un paquete de datos compartido solo tiene efecto para el ancho de banda facturado por el tráfico. Hay disponibles dos tipos de paquetes de datos compartidos: BGP estático (para ancho de banda BGP estático) y BGP dinámico (para ancho de banda BGP dinámico).
- Un paquete de datos compartido no puede surtir efecto para el ancho de banda de un EIP específico.
- Un paquete de datos compartido no puede tener efecto para un ancho de banda compartido.
- Los EIP del tipo BGP premium no pueden utilizar un paquete de datos compartido.
- No se puede cancelar la suscripción a un paquete de datos compartido.

7 VPC y otros servicios

Figura 7-1 muestra la relación entre VPC y otros servicios.

Figura 7-1 VPC y otros servicios

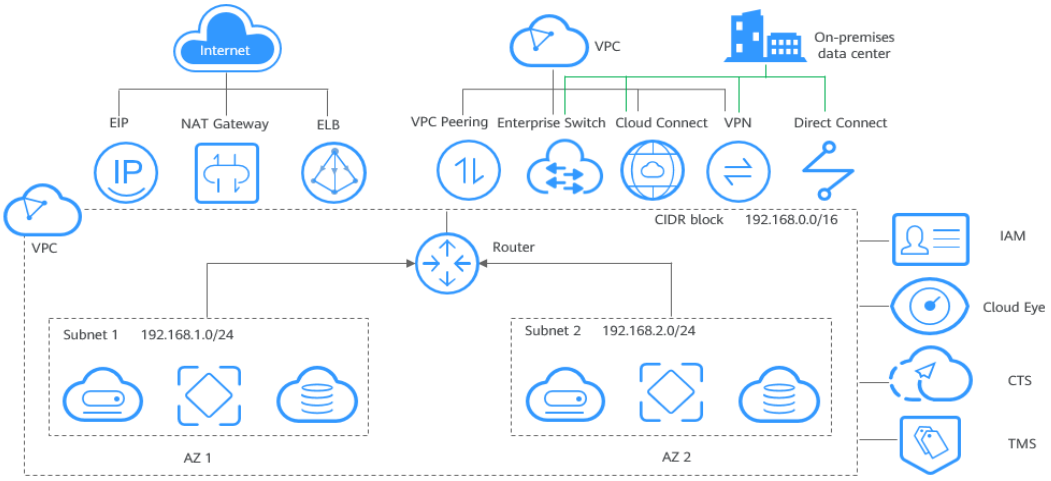


Tabla 7-1 Servicios relacionados

Función interactiva	Servicio
Redes seguras para ECS.	Elastic Cloud Server (ECS)
Conecte los ECS en una VPC a Internet.	Elastic IP (EIP)
	NAT Gateway
Conecte una VPC a un centro de datos local.	Virtual Private Network (VPN)
	Direct Connect
Distribuye el tráfico entrante a varios ECS en una VPC.	Elastic Load Balance (ELB)
Asigne diferentes permisos a los empleados de su empresa para acceder a sus recursos de VPC.	Identity and Access Management (IAM)

Función interactiva	Servicio
Comprueba el ancho de banda y el uso del tráfico.	Cloud Eye

8 Facturación

Conceptos de facturación:

El servicio de VPC es gratuito.

Tabla 8-1 Conceptos de facturación:

Concepto de facturación	Descripción
EIP	Las EIP son necesarias si sus recursos necesitan acceder a Internet.

El servicio de EIP ofrece varios modos de facturación para satisfacer sus necesidades.

- **Modos de facturación de EIP**
- **¿Qué opción de facturación es adecuada para mí?**
- **¿Cómo se me facturará si cambio el tamaño de mi ancho de banda?**
- **¿Cómo cambio el modo de facturación de EIP?**

Modos de facturación de EIP

EIP se puede facturar de forma anual/mensual o de pago por uso. Las opciones de facturación y los elementos de facturación varían según el modo de facturación.

- **Figura 8-1**
- **Tabla 8-2**

Figura 8-1 Facturación de EIP

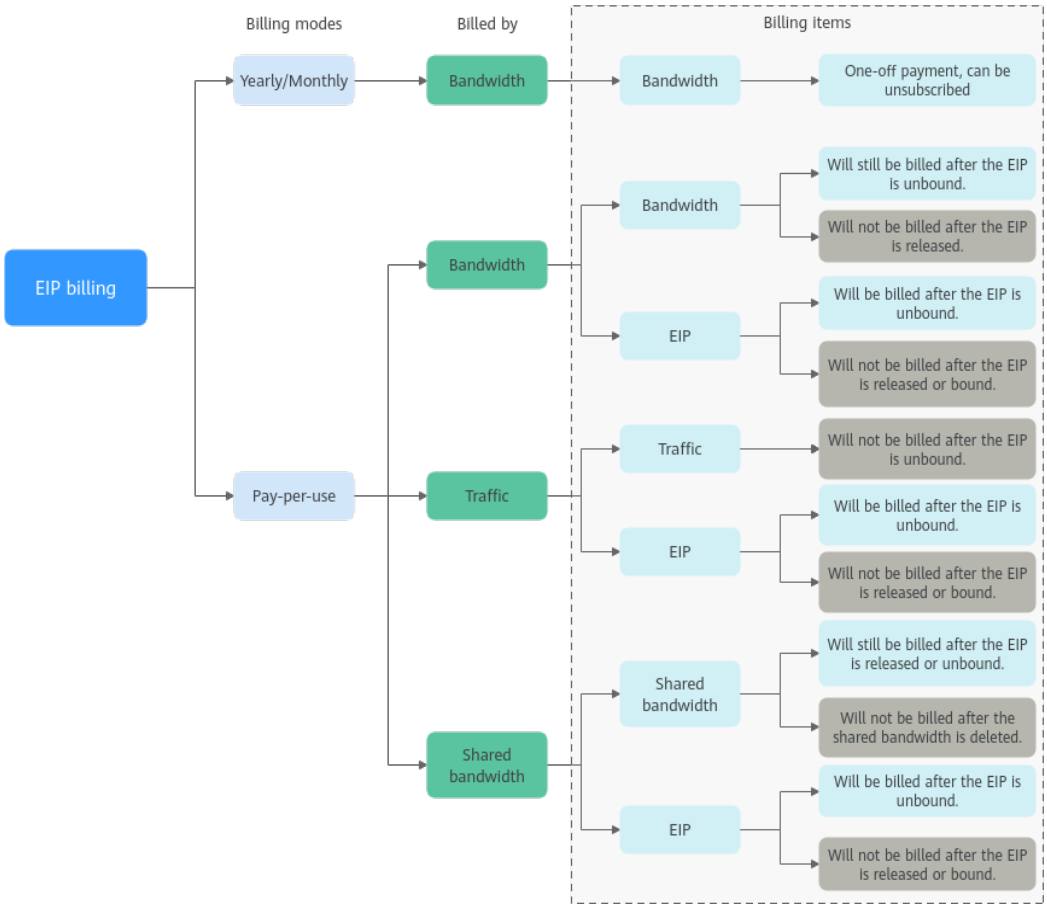


Tabla 8-2 Descripción de facturación de EIP

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación	Impacto de las operaciones de EIP en los artículos de facturación
Anual/Mensual	Ancho de banda	Ancho de banda	Si compra un EIP anual/mensual, solo tendrá que pagar por el ancho de banda incluido en la suscripción. Se le factura en función del tamaño de ancho de banda y la duración de uso especificados. No hay límite en su uso de tráfico.	Puede darse de baja de una suscripción anual/mensual. Su tarifa de uso real y algunas tarifas preferenciales se deducirán del monto del reembolso.

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación	Impacto de las operaciones de EIP en los artículos de facturación
Pago por uso	Ancho de banda	• Ancho de banda • EIP	Si un EIP de pago por uso se factura por ancho de banda: • Tarifa de ancho de banda: se le factura en función del tamaño de ancho de banda y la duración de uso especificados. No hay límite en el uso del tráfico. Después de comprar el EIP, puede cambiar el tamaño de ancho de banda especificado. El ancho de banda que utilice no excederá el ancho de banda especificado. • Tarifa de retención de EIP: la EIP se facturará si no está vinculada a ninguna instancia y no se libera.	Después de comprar un EIP: • Si el EIP no está vinculado a ninguna instancia, se facturará tanto el EIP como su ancho de banda. • Si el EIP está vinculado a una instancia, solo se facturará el ancho de banda. El ancho de banda se facturará sin importar si la instancia vinculada al EIP se está ejecutando o no. • Después de que el EIP se desvincule de una instancia, se seguirá facturando el ancho de banda. A menos que se publique, el EIP también se facturará. • Si se libera el EIP, tanto el EIP como su ancho de banda no se facturarán.

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación	Impacto de las operaciones de EIP en los artículos de facturación
	Tráfico	● Tráfico ● EIP	Si un EIP de pago por uso es facturado por tráfico: ● Tarifa de tráfico: se le factura en función de su tipo de EIP y el tráfico total utilizado que sale de la nube. El tamaño de ancho de banda que establezca solo se utiliza para limitar la velocidad máxima de transferencia de datos. Para evitar altas tarifas causadas por el tráfico de ráfagas, especifique un tamaño de ancho de banda adecuado cuando compre un EIP. ● Tarifa de retención de EIP: la EIP se facturará si no está vinculada a ninguna instancia y no se libera.	Después de comprar un EIP: ● Si el EIP no está vinculado a ninguna instancia, solo se facturará al EIP. ● Si el EIP está vinculado a una instancia, solo se facturará el tráfico utilizado. Si la instancia vinculada al EIP deja de funcionar y no se genera tráfico, no habrá tráfico ni tarifas de EIP. ● Después de que el EIP se desvincule de una instancia, el tráfico no se facturará, pero el EIP se facturará. ● Si se libera el EIP, el EIP no se facturará.

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación	Impacto de las operaciones de EIP en los artículos de facturación
	Anchos de banda compartidos	● Anchos de banda compartidos ● EIP	Si se agrega un EIP de pago por uso a un ancho de banda compartido: ● Tarifa de ancho de banda compartido: Solo se facturará el ancho de banda compartido. No habrá costes adicionales de ancho de banda o tráfico para los EIP añadidos al ancho de banda compartido. ● Tarifa de retención de EIP: la EIP se facturará si no está vinculada a ninguna instancia y no se libera.	Después de comprar un EIP: ● Anchos de banda compartidos – Cualquier operación en el EIP no afecta a la facturación del ancho de banda compartido. Por ejemplo, si ha liberado el EIP pero no ha eliminado el ancho de banda compartido, el ancho de banda compartido todavía se facturará. – Después de eliminar un ancho de banda compartido, ya no se facturará. ● EIP – Si el EIP no está vinculado a ninguna instancia, se facturará al EIP. – Si el EIP no está vinculado de una instancia, se facturará al EIP para mantenerlo asignado a su cuenta a menos que se libere. – Si el EIP se libera o se vincula a una instancia, el EIP no se facturará.

Puede agregar varios EIP en la misma región a un ancho de banda compartido para reducir los costos. Un ancho de banda compartido se puede facturar anual/mensual o de pago por uso.

Para obtener más información, consulte **Tabla 8-3**. Actualmente, solo se pueden agregar EIP de pago por uso a un ancho de banda compartido.

- Puede agregar un EIP a un ancho de banda compartido al comprar el EIP.
- También puede agregar un EIP existente a un ancho de banda compartido. Después de agregar el EIP a un ancho de banda compartido, no habrá ancho de banda adicional ni costes de tráfico, y solo se facturará el ancho de banda compartido.

Tabla 8-3 Detalles de facturación de ancho de banda compartido

Modo de facturación	Facturación por	Artículo de facturación	Descripción del artículo de facturación
Anual/ Mensual	Ancho de banda	Ancho de banda	Si compra un ancho de banda compartido anual/ mensual, se le factura en función del tamaño de ancho de banda y la duración de uso especificados. No hay límite en el uso del tráfico.
Pago por uso	Ancho de banda	Ancho de banda	Se le factura en función del tamaño de ancho de banda y la duración de uso especificados. No hay límite en el uso del tráfico. Después de comprar un ancho de banda compartido, puede cambiar el tamaño de ancho de banda especificado. El ancho de banda que utilice no excederá el ancho de banda especificado.

- El precio del ancho de banda, tráfico y EIP varía según la región.
- **Detalles de precios de EIP**
- El ancho de banda de EIP se refiere al ancho de banda saliente que se consume cuando se transfieren datos de Huawei Cloud a Internet. Por ejemplo, cuando los ECS proporcionan servicios accesibles desde Internet y los usuarios externos descargan recursos de los ECS, eso consume ancho de banda saliente. Solo se facturará el ancho de banda saliente.
  - Si el ancho de banda adquirido o modificado es de hasta 10 Mbit/s, el ancho de banda entrante será de 10 Mbit/s, y el ancho de banda saliente será el mismo que el ancho de banda adquirido o modificado.
  - Si el ancho de banda adquirido o modificado es más de 10 Mbit/s, ambos anchos de banda en las direcciones entrantes y salientes serán los mismos que el ancho de banda comprado o modificado.

¿Qué opción de facturación es adecuada para mí?

Los EIP se pueden facturar por ancho de banda o tráfico. **Tabla 8-4** muestra los escenarios de aplicación de diferentes opciones de facturación.

Cloud Eye supervisa las métricas de su red, como el ancho de banda y el tráfico. Según el uso del ancho de banda, puede determinar qué opción de facturación (por ancho de banda o por tráfico) es más rentable. Aquí hay algunas sugerencias para su referencia:

- Si el tamaño de ancho de banda requerido es inferior a 5 Mbit/s, configure su EIP para que se le facture por ancho de banda y elija el modo de facturación anual/mensual o de pago por uso en función de la duración de su uso.
- Si el tamaño de ancho de banda requerido es superior a 5 Mbit/s y el uso de ancho de banda es superior al 20%, configure su EIP para que se le cobre por ancho de banda.

Para obtener más información, consulte **Consulta de métricas**.

Tabla 8-4 Escenarios de aplicación de las opciones de facturación EIP

Modo de facturación	Facturación por	Caso
Anual/ Mensual	Ancho de banda	Para tráfico pesado o estable
Pago por uso	Ancho de banda	Para tráfico pesado o estable
	Tráfico	Para tráfico ligero o con fuertes fluctuaciones
	Anchos de banda compartidos	Para tráfico escalonado

¿Cómo se me facturará si cambio el tamaño de mi ancho de banda?

Si no se agrega un EIP a un ancho de banda compartido, el EIP utiliza el ancho de banda dedicado sin importar si se factura por el ancho de banda o el tráfico. Después de agregar un EIP a un ancho de banda compartido, solo se factura el ancho de banda compartido.

- **Modificación del tamaño de ancho de banda dedicado**
- **Modificación del tamaño del ancho de banda compartido**

Cuando se cambia el tamaño del ancho de banda, el precio y el tiempo efectivo del ancho de banda varían según el modo de facturación, que se aplica a los anchos de banda dedicados y compartidos. Para más detalles, consulte **Tabla 8-5**.

Tabla 8-5 Impacto en la facturación después de un cambio de tamaño de ancho de banda

Modo de facturación	Facturación por	Cambio	Impacto
Anual/ Mensual	Ancho de banda	Aumentar el ancho de banda	El cambio entrará en vigor inmediatamente. El aumento del ancho de banda se facturará en consecuencia.

Modo de facturación	Facturación por	Cambio	Impacto
	Ancho de banda	Disminuir el ancho de banda al renovarse	El cambio no entrará en vigor inmediatamente. Debe seleccionar un nuevo tamaño de ancho de banda y una duración de renovación. El cambio entrará en vigor en el primer ciclo de facturación después de una renovación exitosa. ● La orden se puede cancelar antes de que el ancho de banda surta efecto. ● El ancho de banda no se puede modificar en el primer ciclo de facturación.
Pago por uso	Ancho de banda	Aumentar o disminuir el ancho de banda	El cambio entrará en vigor inmediatamente.
	Tráfico	Aumentar o disminuir el ancho de banda	El cambio entrará en vigor inmediatamente. El tamaño de ancho de banda que establezca solo se utiliza para limitar la velocidad máxima.

¿Cómo cambio el modo de facturación de EIP?

El servicio EIP proporciona varios modos de facturación para que seleccione. Puede cambiar el modo de facturación de EIP durante el período de uso de EIP si es necesario.

- **Tabla 8-6**
- **Cambio de facturación de ancho de banda**

El cambio en el modo de facturación no cambia los EIP ni interrumpe el uso de los EIP.

Figura 8-2 Cambio del modo de facturación EIP

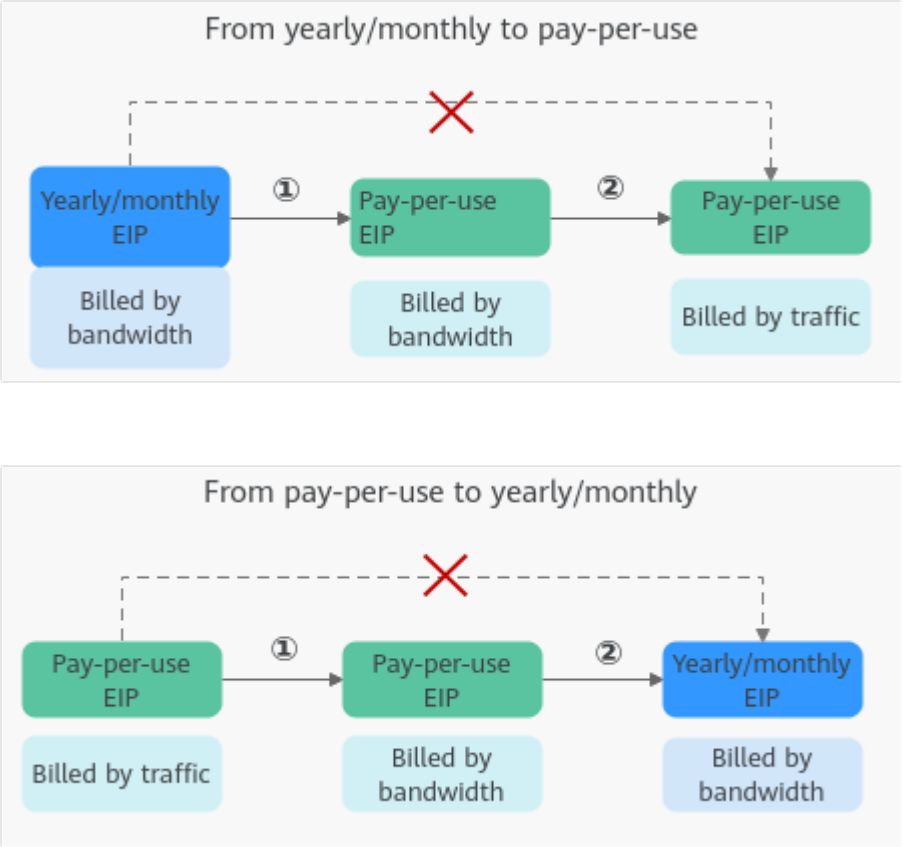


Tabla 8-6 Descripción de cambio del modo de facturación EIP

Cambio	Descripción
De anual/mensual a pago por uso	● Un EIP facturado sobre una base anual/mensual se puede cambiar directamente para ser facturado por ancho de banda sobre una base de pago por uso al vencimiento. ● Un EIP facturado sobre una base anual/mensual no se puede cambiar directamente para ser facturado por el tráfico sobre una base de pago por uso. Para cambiar esto: 1. En primer lugar, cambie el EIP facturado sobre una base anual/mensual para ser facturado por ancho de banda sobre una base de pago por uso. 2. A continuación, cambie el EIP facturado por ancho de banda sobre una base de pago por uso para ser facturado por tráfico sobre una base de pago por uso. El nuevo modo de facturación solo entra en vigor después de que expire la facturación anual/mensual.

Cambio	Descripción
De pago por uso a anual/mensual	● Un EIP que se factura por ancho de banda sobre una base de pago por uso puede cambiarse directamente para ser facturado sobre una base anual/mensual. ● Un EIP que es facturado por el tráfico sobre una base de pago por uso no se puede cambiar directamente para ser facturado sobre una base anual/mensual. Para cambiar esto: 1. Primero, cambie el EIP facturado por tráfico en una base de pago por uso para ser facturado por ancho de banda en una base de pago por uso. 2. A continuación, cambie el EIP facturado por ancho de banda sobre una base de pago por uso para ser facturado sobre una base anual/mensual. Una vez que se realiza el cambio, el nuevo modo de facturación se aplica inmediatamente.
● From billing by traffic (pay-per-use) to billing by bandwidth (pay-per-use) ● From billing by bandwidth (pay-per-use) to billing by traffic (pay-per-use)	● Un EIP facturado por tráfico sobre una base de pago por uso puede cambiarse directamente para ser facturado por ancho de banda sobre una base de pago por uso. ● Un EIP facturado por ancho de banda sobre una base de pago por uso puede cambiarse directamente para ser facturado por tráfico sobre una base de pago por uso. Una vez que se realiza el cambio, el nuevo modo de facturación se aplica inmediatamente.

9 Gestión de permisos

Si necesita asignar diferentes permisos a los empleados de su empresa para acceder a sus recursos de VPC, 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, puedes usar tu 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 VPC, pero no deben poder eliminarlos ni realizar ninguna otra operación de alto riesgo. En este escenario, puede crear usuarios de IAM para los desarrolladores de software y concederles solo los permisos necesarios para usar los recursos de VPC.

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

IAM se puede utilizar de forma gratuita. Solo paga por los recursos de su cuenta. Para obtener más información acerca de IAM, consulte **Descripción general del servicio IAM**.

Permisos de VPC

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

VPC es un servicio a nivel de proyecto implementado y accedido en regiones físicas específicas. Para asignar permisos de VPC a un grupo de usuarios, especifique el ámbito como proyectos específicos de la región, por ejemplo, **ap-southeast-1** para **CN-Hong Kong** 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 la VPC, los usuarios deben cambiar a una región en la que se les haya autorizado a usar la VPC.

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Tipo de mecanismo de autorización de grano grueso que define permisos relacionados con las responsabilidades del usuario. Este mecanismo proporciona solo un número limitado de roles de nivel de servicio para la autorización. Al usar roles para conceder permisos, también debe asignar otros roles de los que dependen los permisos

para que surtan efecto. 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 VPC únicamente los permisos para administrar un determinado tipo de recursos. La mayoría de las políticas definen permisos basados en API. Para ver las acciones de API compatibles con VPC, consulte **Políticas de permisos y acciones compatibles**.

Tabla 9-1 enumera todas las roles definidos por el sistema y políticas admitidas por VPC.

Tabla 9-1 Roles definidos por el sistema y políticas admitidas por VPC

Nombre de la política	Descripción	Tipo de política	Dependencias
VPC FullAccess	Todas las operaciones en VPC.	Política definida por el sistema	No hay
VPC ReadOnlyAccess	Permisos de sólo lectura en VPC.	Política definida por el sistema	No hay
VPC Administrator	La mayoría de los permisos en VPC, excluyendo la creación, modificación, eliminación y visualización de grupos de seguridad y reglas de grupos de seguridad. Para obtener este permiso, los usuarios también deben tener el permiso de **Tenant Guest**.	Rol definido por el sistema	Depende de la política de **Tenant Guest**.

Tabla 9-2 enumera las operaciones comunes soportadas por cada política o rol definido por el sistema de VPC. Seleccione las políticas según sea necesario.

Tabla 9-2 Operaciones comunes soportadas por cada política o función definida por el sistema de VPC

Operación	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Creación de una VPC.	x	√	√
Modificación de una VPC	x	√	√

Operación	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Eliminación de una VPC	x	√	√
Consulta de información de VPC	√	√	√
Creación de una subred	x	√	√
Consulta de información de subred	√	√	√
Modificación de una subred	x	√	√
Supresión de una subred	x	√	√
Creación de un grupo de seguridad	x	x	√
Consulta de la información del grupo de seguridad	√	x	√
Modificación de un grupo de seguridad	x	x	√
Eliminación de un grupo de seguridad	x	x	√
Adición de una regla de grupo de seguridad	x	x	√
Consulta de una regla de grupo de seguridad	√	x	√
Modificación de una regla de grupo de seguridad	x	x	√

Operación	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Eliminación de una regla de grupo de seguridad	x	x	√
Creación de una ACL de red	x	√	√
Consulta de una ACL de red	√	√	√
Modificación de una ACL de red	x	√	√
Eliminación de una ACL de red	x	√	√
Adición de una regla de ACL de red	x	√	√
Modificación de una regla de ACL de red	x	√	√
Eliminación de una regla de ACL de red	x	√	√
Creación de una interconexión de VPC	x	√	√
Modificación de una interconexión de VPC	x	√	√
Eliminación de una interconexión de VPC	x	√	√
Creación de una tabla de rutas	x	√	√

Operación	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Supresión de una tabla de ruta	x	√	√
Adición de una ruta	x	√	√
Modificación de una ruta	x	√	√
Eliminación de una ruta	x	√	√

Enlaces útiles

- **¿Qué es IAM?**
- **Creación de un usuario y concesión de permisos de VPC**
- **Políticas de permisos y acciones admitidas**

10 Conceptos básicos

10.1 Subred

Una subred es un bloque CIDR único con un rango de las direcciones IP en una VPC. Todos los recursos de una VPC deben implementarse en las subredes.

- De forma predeterminada, los ECS de todas las subredes de la misma VPC pueden comunicarse entre sí, pero los ECS de las diferentes VPC no pueden.

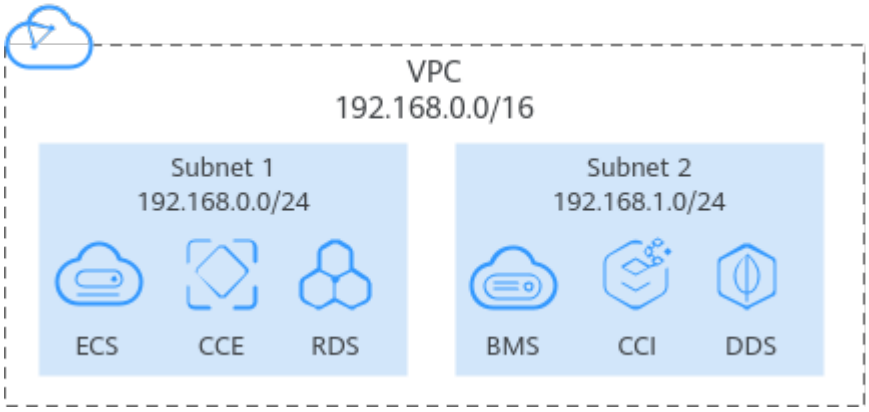
  Puede crear interconexión de VPC para habilitar ECS en diferentes VPC pero en la misma región para comunicarse entre sí.
- Después de que se crea una subred, su CIDR no se puede modificar.

  Las subredes utilizadas para implementar sus recursos deben residir dentro de su VPC, y las máscaras de subred utilizadas para definirlas pueden estar entre la máscara de red de su bloque CIDR de VPC y /28 Máscara de red.
  - 10.0.0.0 - 10.255.255.255
  - 172.16.0.0 - 172.31.255.255
  - 192.168.0.0 - 192.168.255.255

  Una máscara de subred puede estar entre la máscara de red de su bloque CIDR de VPC y la máscara de red /28. Si un bloque CIDR de VPC es 192.168.0.0/16, su máscara de subred puede estar entre 16 y 28.

Figura 10-1 Subred

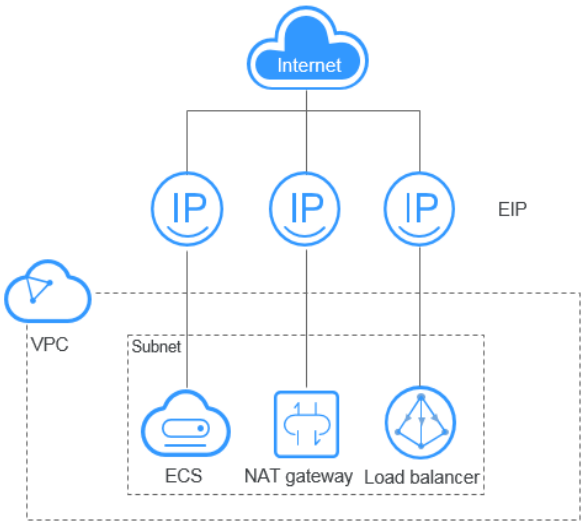


10.2 Elastic IP

El servicio Elastic IP (EIP) permite que los recursos en la nube se comuniquen con Internet mediante direcciones IP estáticas públicas y anchos de banda escalables. Los EIP pueden estar vinculados o independientes de ECS, BMS, direcciones IP virtuales, gateways NAT o balanceadores de carga.

Cada EIP solo puede ser usado por un recurso en la nube a la vez.

Figura 10-2 Acceso a Internet con un EIP



10.3 Tabla de rutas

Tabla de rutas

Una tabla de rutas contiene un conjunto de las rutas que se utilizan para determinar a dónde se dirige el tráfico de red de las subredes en una VPC. Cada subred debe estar asociada a una tabla de rutas. Puede asociar una subred a una sola tabla de rutas a la vez, pero puede asociar varias subredes a la misma tabla de rutas.

Se admiten las rutas IPv4 e IPv6.

Figura 10-3 Tabla de rutas

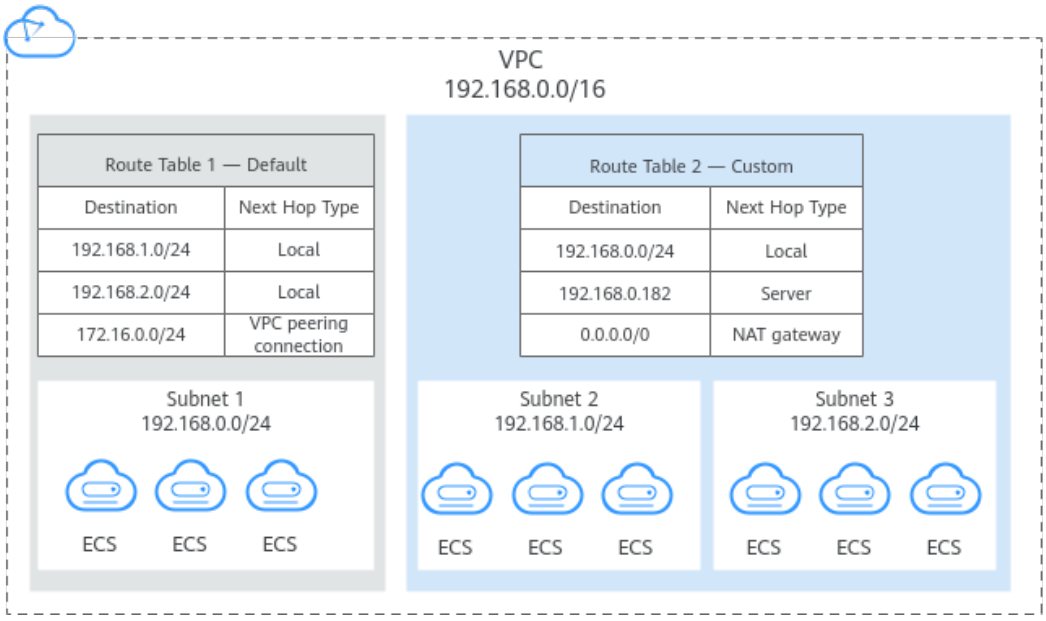


Tabla de rutas predeterminada y tabla de rutas personalizadas

Cuando se crea una VPC, el sistema genera automáticamente una tabla de ruta predeterminada para la VPC. Si crea una subred en la VPC, la subred se asocia automáticamente a la tabla de rutas predeterminada.

- Puede agregar rutas a, eliminar rutas de y modificar rutas en la tabla de rutas predeterminada, pero no puede eliminar la tabla.
- Cuando creas una conexión de VPN, de Cloud Connect, o de Direct Connect, la tabla de rutas predeterminada entrega automáticamente una ruta que no se puede eliminar ni modificar.

Si no desea utilizar la tabla de rutas predeterminada, ahora puede crear una tabla de rutas personalizada y asociarla a la subred. Las tablas de ruta personalizadas se pueden eliminar si ya no son necesarias.

Para utilizar una tabla de rutas personalizada, debe enviar un ticket de servicio. Debe hacer clic en **Increase quota** en la página **Create Route Table** o elegir **More** > **Service Tickets** > **Create Service Ticket** en la esquina superior derecha de la página. Para obtener más información, consulte **Enviar un ticket de servicio**.

Ruta

Una ruta se configura con el destino, el tipo de salto siguiente y el salto siguiente para determinar a dónde se dirige el tráfico de red. Las rutas se clasifican en las rutas del sistema y las rutas personalizadas.

- Rutas del sistema: Estas rutas son agregadas automáticamente por el sistema y no se pueden modificar o eliminar.

Después de crear una tabla de rutas, el sistema agrega automáticamente las siguientes rutas de sistema a la tabla de rutas, para que las instancias de una VPC puedan comunicarse entre sí.

- Rutas cuyo destino es 100.64.0.0/10 o 198.19.128.0/20.
- Rutas cuyo destino son los bloques CIDR IPv4 e IPv6 de subredes en la VPC.

  Si habilita IPv6 al crear una subred, el sistema asigna automáticamente un bloque CIDR IPv6 a la subred. A continuación, puede ver las rutas IPv6 en su tabla de rutas. Ejemplos de destinos de bloques CIDR de subred son los siguientes:

  - IPv4: 192.168.2.0/24
  - IPv6: 2407:c080:802:be7::/64

  Además de las rutas del sistema anteriores, el sistema agrega automáticamente una ruta cuyo destino es 127.0.0.0/8. Esta es la dirección de bucle de retorno local.

- Rutas personalizadas: Estas son rutas que puede agregar, modificar y eliminar. El destino de una ruta personalizada no se puede superponer al de una ruta de sistema.

  Puede agregar una ruta personalizada y configurar el destino, el tipo de salto siguiente y el salto siguiente en la ruta para determinar a dónde se dirige el tráfico de red. **Tabla 10-1** enumera los tipos admitidos de saltos siguientes.

Tabla 10-1 Tipo del próximo salto

Tipo del próximo salto	Descripción	Tabla de rutas admitida
Servidor	El tráfico dirigido hacia el destino es reenviado a un ECS en la VPC.	• Tabla de rutas predeterminada • Tabla de rutas personalizada
NIC de extensión	El tráfico dirigido hacia el destino es reenviado a una NIC de extensión de un ECS en la VPC.	• Tabla de rutas predeterminada • Tabla de rutas personalizada
Red definida por el usuario de BMS	El tráfico destinado al destino se reenvía a una red de BMS definida por el usuario.	• Tabla de rutas predeterminada • Tabla de rutas personalizada
Gateway de la VPN	El tráfico dirigido hacia el destino es reenviado a un VPN Gateway.	Tabla de rutas personalizada
Gateway de Direct Connect	El tráfico dirigido hacia el destino es reenviado a un Direct Connect Gateway.	Tabla de rutas personalizada
Cloud connection	Traffic intended for the destination is forwarded to a cloud connection.	Tabla de rutas personalizada

Tipo del próximo salto	Descripción	Tabla de rutas admitida
Interfaz de red suplementaria	El tráfico dirigido hacia el destino se reenvía a la interfaz de red suplementaria de un ECS en la VPC.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Gateway de NAT	El tráfico dirigido hacia el destino es reenviado a un NAT Gateway.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Interconexión de VPC	El tráfico dirigido hacia el destino es reenviado a una interconexión de VPC.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Dirección IP virtual	El tráfico dirigido hacia el destino se reenvía a una dirección IP virtual y luego es enviado a los ECS activos y en standby a los que está vinculada la dirección IP virtual.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Enrutador empresarial	El tráfico destinado al destino se reenvía a un enrutador empresarial.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada
Firewall en la nube	El tráfico destinado al destino se reenvía a un firewall en la nube.	● Tabla de rutas predeterminada ● Tabla de rutas personalizada

Si especifica el destino al crear un recurso, se entrega una ruta del sistema. Si no especifica un destino al crear un recurso, se entrega una ruta personalizada que se puede modificar o eliminar.

Por ejemplo, cuando se crea un gateway de NAT, el sistema entrega automáticamente una ruta personalizada sin un destino específico (0.0.0.0/0 se utiliza de forma predeterminada). En este caso, puede cambiar el destino. Sin embargo, cuando crea un gateway de VPN, debe especificar la subred remota, es decir, el destino de una ruta. En este caso, el sistema entrega esta ruta del sistema. No modifique el destino de la ruta en la página **Route Tables**. Si lo hace, el destino no será coherente con la subred remota configurada. Para modificar el destino de la ruta, vaya a la página de recursos específica y modifique la subred remota, a continuación, el destino de la ruta se cambiará en consecuencia.

10.4 Grupo de seguridad

Un grupo de seguridad es una colección de reglas de control de acceso para recursos en la nube, como servidores en la nube, contenedores y bases de datos, que tienen los mismos

requisitos de protección de seguridad y que son de confianza mutua dentro de una VPC. Después de crear un grupo de seguridad, puede crear varias reglas de acceso para el grupo de seguridad, estas reglas se aplicarán a todos los recursos de nube agregados a este grupo de seguridad.

Su cuenta viene automáticamente con un grupo de seguridad predeterminado (**Sys-default**). El grupo de seguridad predeterminado permite todo el tráfico saliente, niega todo el tráfico entrante y permite todo el tráfico entre los recursos de nube del grupo. Sus recursos en la nube de este grupo de seguridad ya pueden comunicarse entre sí sin agregar reglas adicionales.

Figura 10-4 ilustra cómo funciona el grupo de seguridad predeterminado.

Figura 10-4 Grupo de seguridad predeterminado

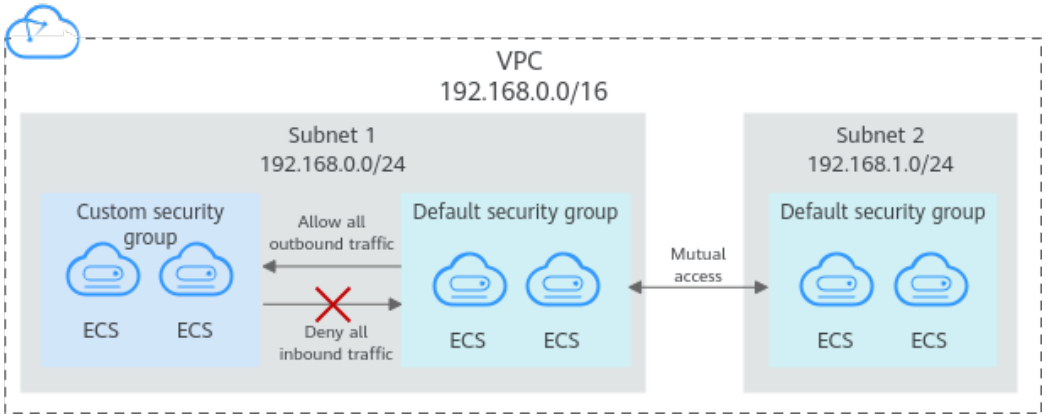


Tabla 10-2 describe las reglas predeterminadas para el grupo de seguridad predeterminado.

Tabla 10-2 Reglas en el grupo de seguridad predeterminado (**Sys-default**)

Dirección	Prioridad	Acción	Protocolo	Puerto/Rango	Origen/Destino	Descripción
Saliente	100	Permitir	Todos	Todos	Destino: 0.0.0.0/0	Permite todo el tráfico de salida.
Entrante	100	Permitir	Todos	Todos	Origen: el grupo de seguridad actual, por ejemplo, **Sys-default**	Permite las comunicaciones entre ECS dentro del mismo grupo de seguridad en cualquier puerto.
Entrante	100	Permitir	TCP	22	Origen: 0.0.0.0/0	Permite que todas las direcciones IP accedan a los ECS Linux mediante SSH.
Entrante	100	Permitir	TCP	3389	Origen: 0.0.0.0/0	Permite que todas las direcciones IP accedan a ECS de Windows a través de RDP.

También puede crear los grupos de seguridad personalizados y las reglas según sea necesario.

Si dos ECS están en el mismo grupo de seguridad pero en las VPC diferentes, los ECS no pueden comunicarse entre sí. Para habilitar las comunicaciones entre los ECS, utilice un interconexión de VPC para conectar los dos VPC.

10.5 Interconexión de VPC

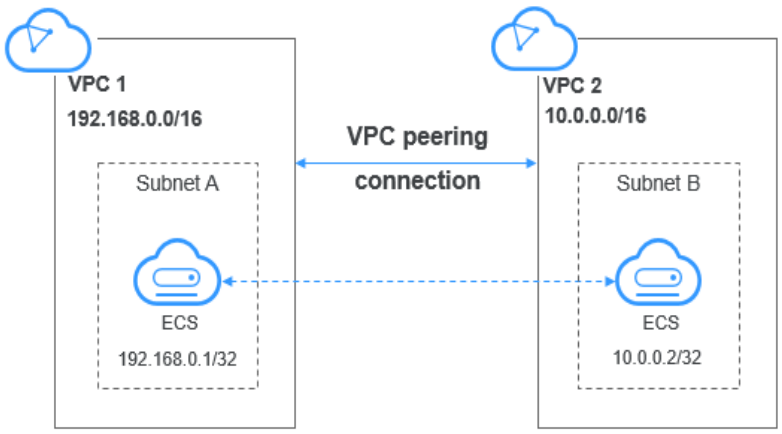
Una interconexión de VPC es una conexión de red entre dos VPC en una región que le permite enrutar el tráfico entre ellos mediante las direcciones IP privadas. Los ECS en cualquiera de las VPC pueden comunicarse entre sí como si estuvieran en la misma región. Puede crear una interconexión de VPC entre sus propias VPC, o entre su VPC y la de otra cuenta dentro de la misma región. Sin embargo, no puede crear una interconexión de VPC entre las VPC en diferentes regiones.

Cada cuenta puede tener un máximo de 50 interconexión de VPC en cada región de forma predeterminada.

- La interconexión de VPC entre las VPC de la misma cuenta: Cada cuenta puede crear un máximo de 50 interconexión de VPC en una región.
- La interconexión de VPC entre las VPC de diferentes cuentas: Las interconexión de VPC aceptadas usan las cuotas de ambas cuentas. Las interconexión de VPC que deben aceptarse solo usan las cuotas de cuentas que solicitan las conexiones.

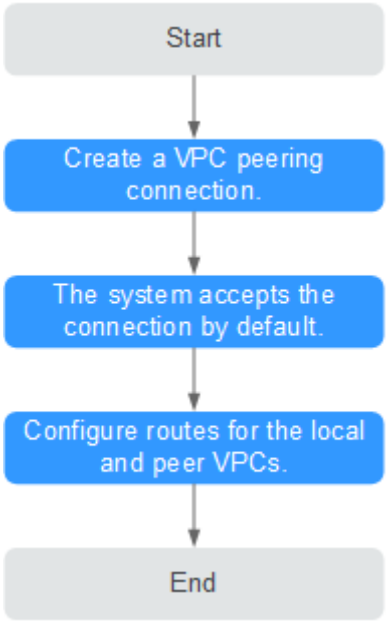
  Una cuenta puede crear interconexiones de VPC con diferentes cuentas si la cuenta tiene suficiente cuota.

Figura 10-5 Interconexión de VPC



- Creación de una interconexión de VPC entre las VPC de su cuenta

Figura 10-6 Creación de una interconexión de VPC entre las VPC de su cuenta

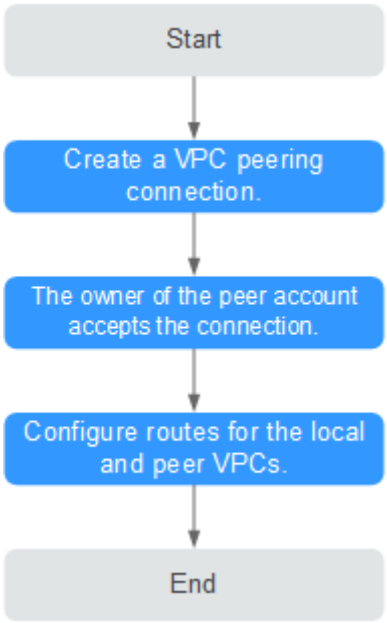


Si crea una interconexión de VPC entre dos VPC en la misma cuenta, el sistema acepta la conexión de forma predeterminada. Es necesario agregar rutas a las tablas de rutas de las VPC local y del mismo nivel para permitir la comunicación entre ellas.

Para obtener más información, consulte **Creación de una interconexión de VPC con otra VPC en su cuenta**.

- Creación de una interconexión de VPC con una VPC de otra cuenta

Figura 10-7 Creación de una interconexión de VPC con una VPC de otra cuenta



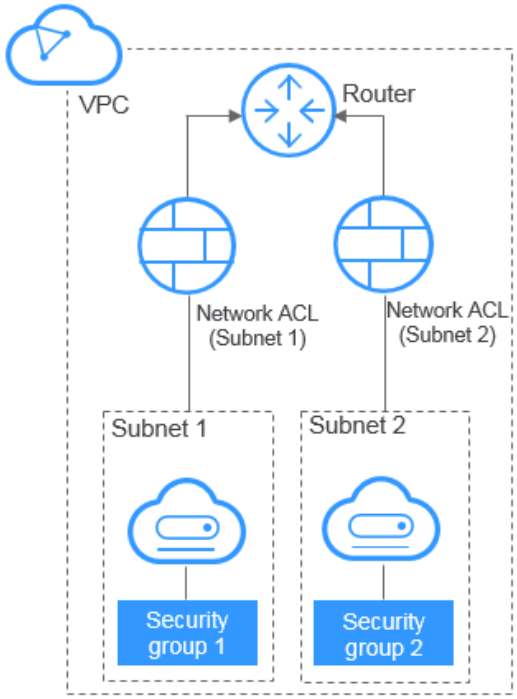
a. Si crea una interconexión de VPC entre su VPC y una VPC que está en otra cuenta, la interconexión de VPC estará en el estado **Awaiting acceptance**.

b. Después de que el propietario de la cuenta del mismo nivel acepte la conexión, el estado de la conexión cambia a **Accepted**. Los propietarios de las cuentas local y de pares deben agregar rutas a las tablas de rutas de las VPC conectadas por la interconexión de VPC para permitir la comunicación entre las dos VPC.

10.6 ACL de red

Una ACL de red es una capa opcional de seguridad para sus subredes. Después de asociar una o más subredes a una ACL de red, puede controlar el tráfico de entrada y salida de las subredes.

Figura 10-8 Grupos de seguridad y ACL de red



Similar a los grupos de seguridad, las ACL de red controlan el acceso a las subredes y agregan una capa adicional de defensa a las subredes. Los grupos de seguridad solo tienen las reglas de "allow", pero las ACL de red tiene ambas reglas de "allow" y "deny". Puede utilizar las ACL de red junto con los grupos de seguridad para implementar un control de acceso completo y detallado. Puede utilizar las ACL de red junto con los grupos de seguridad para implementar un control de acceso completo y detallado.

Conceptos básicos de la ACL de red

- Su VPC no viene con una ACL de red, pero puede crear una ACL de red y asociarla con una subred de VPC si es necesaria. De forma predeterminada, cada ACL de red deniega todo el tráfico entrante y saliente de la subred asociada hasta que agregue reglas.
- Puede asociar una ACL de red con varias subredes. Sin embargo, una subred solo se puede asociar a una ACL de red a la vez.
- Cada ACL de red recién creada se encuentra en el estado **Inactive** hasta que se asocien las subredes.

- Las ACL de red son de estado. Si envía una solicitud desde su instancia y se permite el tráfico saliente, se permite que el tráfico de respuesta para esa solicitud fluya independientemente de las reglas entrantes de ACL de red. De manera similar, si se permite el tráfico entrante, se permite que las respuestas al tráfico entrante permitido fluyan hacia fuera, independientemente de las reglas salientes.

  El periodo de tiempo de espera del seguimiento de la conexión varía según el protocolo. El periodo de tiempo de espera de una conexión TCP en el estado establecido es 600s, y el periodo de tiempo de espera de una conexión ICMP es 30s. Para otros protocolos, si se reciben paquetes en ambas direcciones, el periodo de tiempo de espera de seguimiento de conexión es de 180 segundos. Si se reciben uno o más paquetes en una dirección pero no se recibe ningún paquete en la otra dirección, el período de tiempo de espera de seguimiento de conexión es de 30 segundos. Para los protocolos distintos de TCP, UDP e ICMP, solo se realiza un seguimiento de la dirección IP y el número de protocolo.

Reglas por defecto de ACL de red

De forma predeterminada, cada ACL de red tiene reglas preestablecidas que permiten los siguientes paquetes:

- Paquetes cuyo origen y destino están en la misma subred
- Paquetes de difusión con el destino 255.255.255.255/32, que se utiliza para configurar la información de inicio del host.
- Paquetes de multidifusión con el destino 224.0.0.0/24, que es utilizado por los protocolos de enrutamiento.
- Paquetes de metadatos con el destino 169.254.169.254/32 y el puerto TCP número 80, que se utiliza para obtener metadatos.
- Paquetes de bloques CIDR reservados para servicios públicos (por ejemplo, paquetes con el destino 100.125.0.0/16)
- Una ACL de red niega todo el tráfico de entrada y salida de una subred, excepto los anteriores. **Tabla 10-3** muestra las reglas predeterminadas de ACL de red. No puede modificar ni eliminar las reglas predeterminadas.

Tabla 10-3 Reglas predeterminadas de ACL de red

Dirección	Prioridad	Acción	Protocolo	Fuente	Destino	Descripción
Entrante	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Deniega todo el tráfico entrante.
Saliente	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Deniega todo el tráfico saliente.

Prioridades de las reglas

- Cada regla de ACL de red tiene un valor de prioridad donde un valor más pequeño corresponde a una prioridad más alta. Cada vez que dos reglas entran en conflicto, la regla con la prioridad más alta es la que se aplica. La regla cuyo valor de prioridad es un asterisco (*) tiene la prioridad más baja.

- Si varias reglas de ACL de red entran en conflicto, solo la regla con la prioridad más alta tiene efecto. Si necesita que una regla surta efecto antes o después de una regla específica, puede insertar esa regla antes o después de la regla específica.

Escenarios de aplicación

- Si la capa de aplicación necesita proporcionar servicios a los usuarios, se debe permitir que el tráfico llegue a la capa de aplicación desde todas las direcciones IP. Sin embargo, también debe evitar el acceso ilegal de usuarios maliciosos.

  Solución: puede agregar reglas de ACL de red para denegar el acceso desde direcciones IP sospechosas.
- ¿Cómo puedo aislar puertos con vulnerabilidades identificadas? Por ejemplo, ¿cómo puedo aislar el puerto 445 que puede ser explotado por el gusano WannaCry?

  Solución: puede agregar reglas de ACL de red para denegar el tráfico de acceso desde un puerto y protocolo específicos, por ejemplo, el puerto TCP 445.
- No se requiere defensa para la comunicación dentro de una subred, pero se requiere control de acceso para la comunicación entre subredes.

  Solución: puede agregar reglas de ACL de red para controlar el tráfico entre subredes.
- Para las aplicaciones a las que se accede con frecuencia, es posible que sea necesario ajustar una secuencia de reglas de seguridad para mejorar el rendimiento.

  Solución: Una ACL de red le permite ajustar la secuencia de reglas para que las reglas usadas con frecuencia se apliquen antes que otras reglas.

10.7 Dirección IP virtual

Una dirección IP virtual se puede compartir entre múltiples ECS. Un ECS puede tener direcciones IP privadas y virtuales, y puede acceder al ECS a través de cualquiera de las direcciones IP. Una dirección IP virtual tiene las mismas capacidades de acceso a la red que una dirección IP privada, incluida la comunicación de capa 2 y capa 3 en VPC, el acceso entre VPC mediante las interconexiones de VPC, así como el acceso a través de las EIP, las conexiones de VPN y las conexiones de Direct Connect.

Puede vincular ECS implementados en modo activo/en standby con la misma dirección IP virtual y, a continuación, vincular una EIP a la dirección IP virtual. Las direcciones IP virtuales pueden trabajar junto con Keepalived para garantizar una alta disponibilidad y recuperación ante desastres. Si el ECS activo es defectuoso, el ECS en standby toma automáticamente los servicios del activo.

Redes

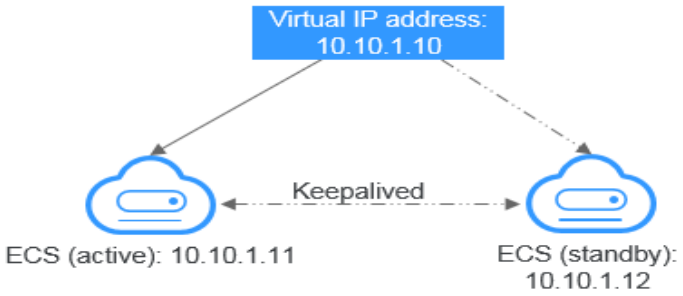
Las direcciones IP virtuales se utilizan para una alta disponibilidad y pueden trabajar junto con Keepalived para hacer posible la conmutación activa/en standby del ECS. De esta manera, si un ECS se cae por alguna razón, el otro puede hacerse cargo y los servicios continúan ininterrumpidos. Los ECS se pueden configurar para HA o como clústeres de equilibrio de carga.

- **Networking mode 1**: HA

  Si desea mejorar la disponibilidad del servicio y evitar puntos únicos de error, puede implementar los ECS en el modo activo/en standby o implementar un ECS activo y varios ECS en standby. En esta disposición, todos los ECS usan la misma dirección IP

virtual. Si el ECS activo se vuelve defectuoso, un ECS en standby se hace cargo de los servicios del ECS activo y los servicios continúan sin interrupciones.

Figura 10-9 Diagrama de red del modo de HA

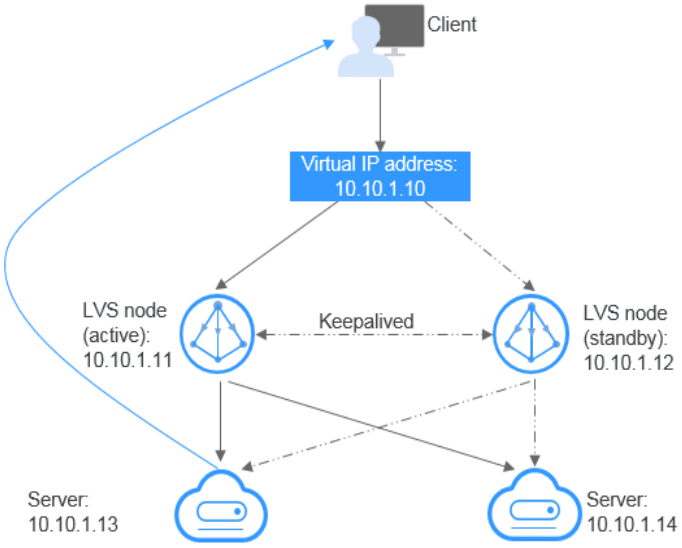


- En esta configuración, una única dirección IP virtual está vinculada a dos ECS en la misma subred.
- A continuación, Keepalived se utiliza para configurar los dos ECS para que funcionen en el modo activo/en standby. Siga los estándares de la industria para configurar Keepalived. Los detalles no están incluidos aquí.

- **Networking mode 2**: clúster de equilibrio de carga HA

  Si desea crear un clúster de equilibrio de carga de alta disponibilidad, utilice Keepalived y configure los nodos de LVS como los enrutadores directos.

Figura 10-10 clúster de equilibrio de carga de HA



- Vincule una única dirección IP virtual a dos ECS.
- Configure los dos ECS como nodos de LVS que funcionan como enrutadores directos y use Keepalived para configurar los nodos en el modo activo/en standby. Los dos ECS reenviarán uniformemente las solicitudes a diferentes servidores backend.

- Configure dos ECS más como servidores de backend.
- Deshabilite la comprobación de origen/destino de los dos servidores backend.

Siga los estándares de la industria para configurar Keepalived. Los detalles no están incluidos aquí.

Escenarios de aplicación

- Acceso a la dirección IP virtual a través de una EIP.

  Si su aplicación tiene requisitos de alta disponibilidad y necesita proporcionar servicios a través de Internet, se recomienda vincular una EIP a una dirección IP virtual.

- Uso de una VPN, Direct Connect o la interconexión de VPC para acceder a una dirección IP virtual

  Para garantizar una alta disponibilidad y acceso a Internet, utilice una VPN para la seguridad y Direct Connect para una conexión estable. La interconexión de VPC es necesaria para que las VPC en la misma región puedan comunicarse entre sí.

10.8 Grupo de direcciones IP

Un grupo de direcciones IP es una colección de direcciones IP que pueden usar la misma regla del grupo de seguridad. Un grupo de direcciones IP puede ser utilizado para gestionar direcciones IP que tengan los mismos requerimientos de seguridad o cuyos requerimientos de seguridad cambien de manera frecuente.

Puede crear un grupo de direcciones IP y agregar direcciones IP que deben gestionarse de manera unificada al grupo. A continuación, puede seleccionar este grupo de direcciones IP al configurar una regla del grupo de seguridad. La regla entrará en vigor para todas las direcciones IP del grupo de direcciones IP.

10.9 Región y AZ

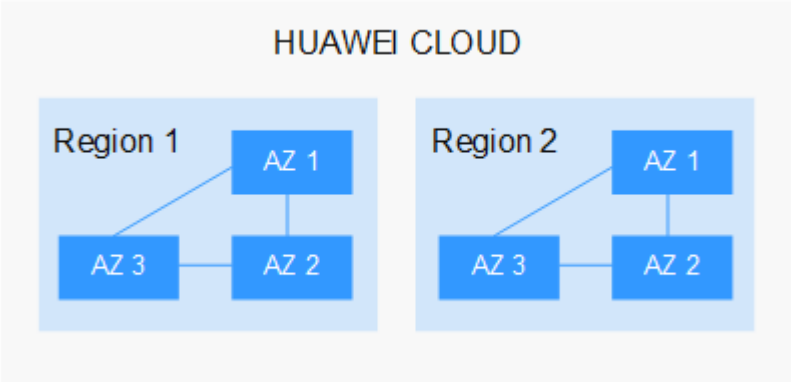
Concepto

Una región y una zona de disponibilidad (AZ) identifican la ubicación de un centro de datos. Puede crear recursos en una región específica y AZ.

- Las regiones se dividen en función de la ubicación geográfica y la latencia de la red. Los servicios públicos, como Elastic Cloud Server (ECS), Elastic Volume Service (EVS), Object Storage Service (OBS), Virtual Private Cloud (VPC), Elastic IP (EIP) y Image Management Service (IMS), se comparten dentro de la misma región. Las regiones se clasifican en regiones universales y regiones dedicadas. Una región universal proporciona servicios en la nube universales para los tenants estándares. Una región dedicada proporciona servicios específicos para tenants específicos.
- Una AZ contiene uno o más centros de datos físicos. Cada AZ cuenta con instalaciones independientes de electricidad, de refrigeración, de extinción de incendios y a prueba de humedad. Dentro de una AZ, los recursos de computación, red, almacenamiento y otros se dividen de forma lógica en múltiples clústeres. Las AZ dentro de una región están interconectadas usando fibras ópticas de alta velocidad, para soportar sistemas de alta disponibilidad entre las AZ.

Figura 10-11 muestra la relación entre regiones y AZ.

Figura 10-11 Las regiones y las AZ



Huawei Cloud ofrece servicios en muchas regiones de todo el mundo. Seleccione una región y AZ según los requisitos. Para obtener más información, consulte **Regiones globales de Huawei Cloud**.

Selección de una región

Al seleccionar una región, tenga en cuenta los siguientes factores:

- Localización

  Se recomienda seleccionar la región más cercana para una menor latencia de red y un acceso rápido. Las regiones dentro de China continental proporcionan la misma infraestructura, calidad de red BGP, así como operaciones de recursos y configuraciones. Por lo tanto, si sus usuarios objetivo están en China continental, no es necesario tener en cuenta las diferencias de latencia de la red al seleccionar una región.

  - Si sus usuarios objetivo se encuentran en Asia Pacífico (excepto China continental), seleccione la región **CN-Hong Kong**, **AP-Bangkok**, or **AP-Singapore**.
  - Si sus usuarios objetivo se encuentran en África, seleccione la región **AF-Johannesburg**.
  - Si sus usuarios objetivo están en América Latina, seleccione la región **LA-Santiago**.

    La región **LA-Santiago** se encuentra en Chile.

- Precio del recurso

  Los precios de los recursos pueden variar en diferentes regiones. Para obtener más información, consulte **Detalles de precios del producto**.

Selección de una AZ

Al implementar recursos, tenga en cuenta los requisitos de las aplicaciones en cuanto a la recuperación ante desastres (DR) y la latencia de la red.

- Para una alta capacidad de DR, implemente recursos en diferentes AZ dentro de la misma región.
- Para una menor latencia de red, implemente recursos en la misma AZ.

Regiones y endpoint

Antes de usar una API para llamar a recursos, especifique su región y endpoint. Para regiones y endpoints, consulte **Regiones y endpoint**.

