NAT Gateway

Descripción general del servicio

Edición 01

Fecha 2022-07-27

HUAWEI TECHNOLOGIES CO., LTD.

Marcas y permisos


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

Aviso

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

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

Índice

1 ¿Qué es NAT Gateway?

NAT Gateway es un servicio de traducción de direcciones de red (NAT). Puede ser un gateway de NAT público o un gateway de NAT privado.

Gateway de NAT públicos

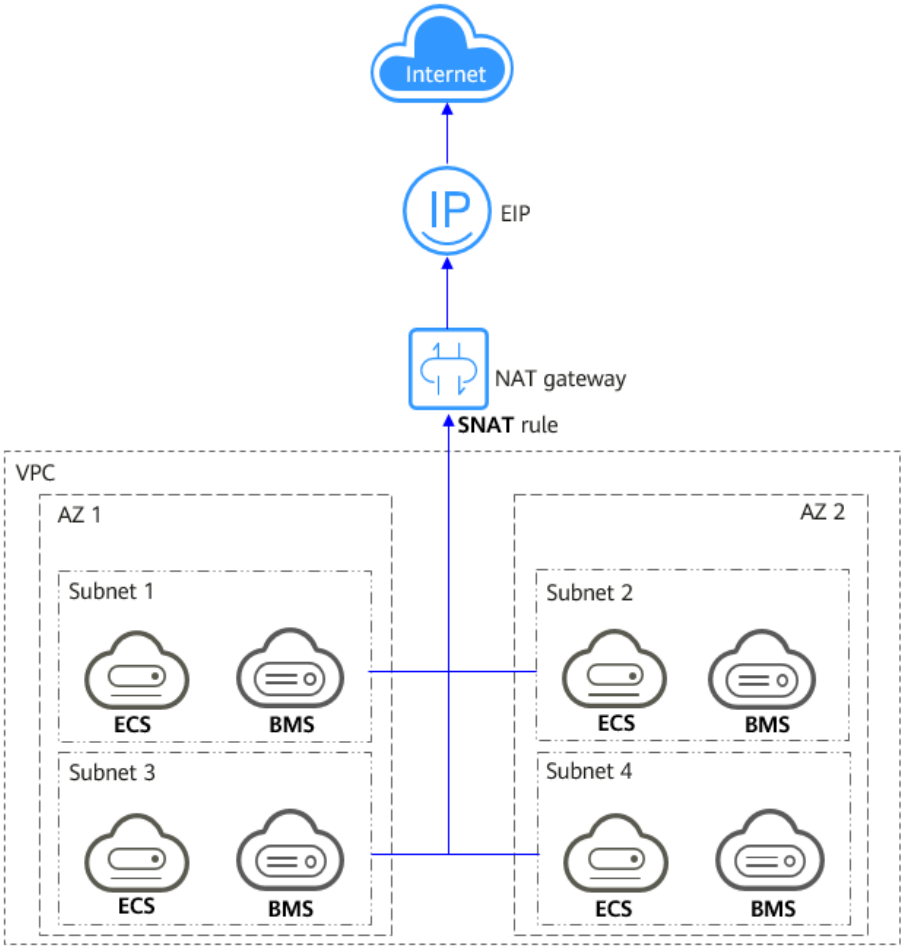
Un gateway de NAT público permite que los servidores locales y en la nube de una subred privada accedan a Internet o proporcionen servicios accesibles desde Internet. Los servidores en la nube son ECS y BMS en una VPC. Los servidores locales son servidores en centros de datos locales que se conectan a una VPC a través de Direct Connect o Virtual Private Network (VPN). Un gateway de NAT público admite hasta 20 Gbit/s de ancho de banda.

Los gateway de NAT públicos ofrecen NAT de origen (SNAT) y NAT de destino (DNAT).

- SNAT traduce direcciones IP privadas en direcciones IP elásticas (EIP), lo que permite que el tráfico de una red privada salga a Internet.

  Figura 1-1 muestra cómo funciona una regla de SNAT.

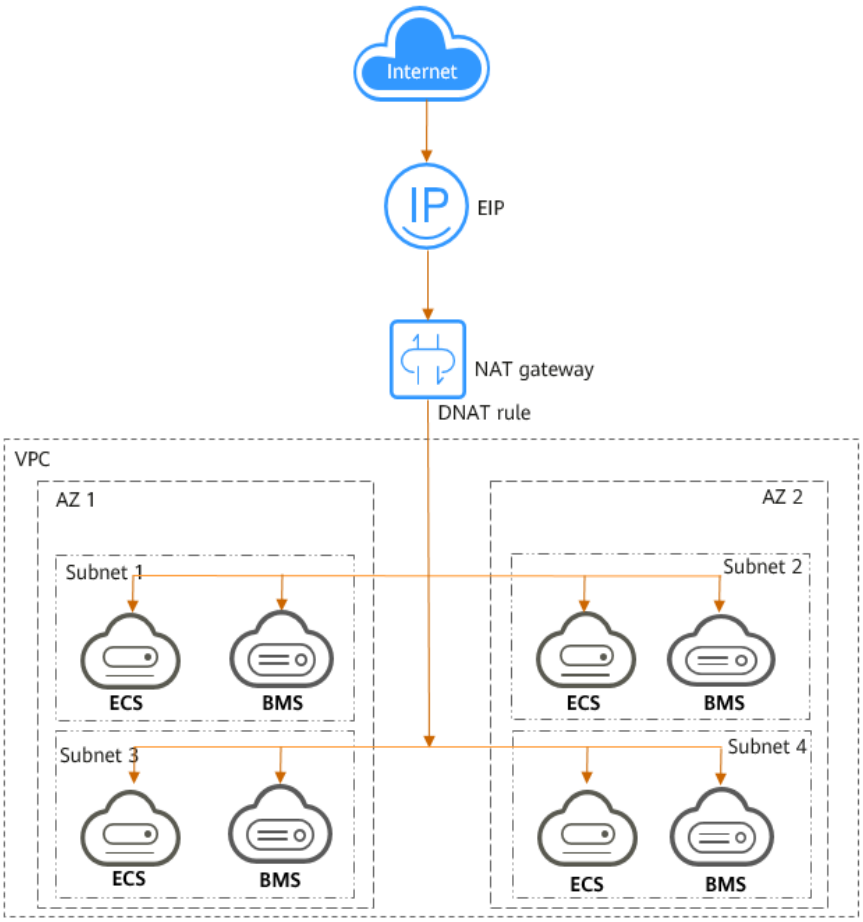
Figura 1-1 Gateway de NAT con una regla de SNAT



- DNAT permite que múltiples servidores dentro de una AZ o a través de múltiples AZ en una VPC compartan los EIP para proporcionar servicios accesibles desde Internet. Con un EIP, un gateway de NAT reenvía las solicitudes de Internet desde solo un puerto específico y a través de un protocolo específico a un puerto específico de un servidor, o puede reenviar todas las solicitudes al servidor independientemente del puerto en el que se originaron.

  Figura 1-2 muestra cómo funciona una regla de la DNAT.

Figura 1-2 Gateway de NAT con una regla de DNAT



Gateway de NAT privados

Los gateway de NAT privados proporcionan traducción de direcciones de red, lo que permite que los ECS y BMS en una VPC se comuniquen con servidores en otras VPC o centros de datos locales. Puede configurar las reglas de SNAT y de DNAT para NAT Gateway para traducir las direcciones IP de origen y destino de los paquetes de origen en una dirección IP de tránsito.

Específicamente,

- SNAT permite a varios servidores dentro de una AZ o a través de múltiples AZ en una VPC compartir una dirección IP de tránsito para acceder a centros de datos locales u otras VPC.
- DNAT permite que los servidores que comparten la misma dirección IP de tránsito en una VPC proporcionen servicios accesibles desde centros de datos locales u otras VPC.

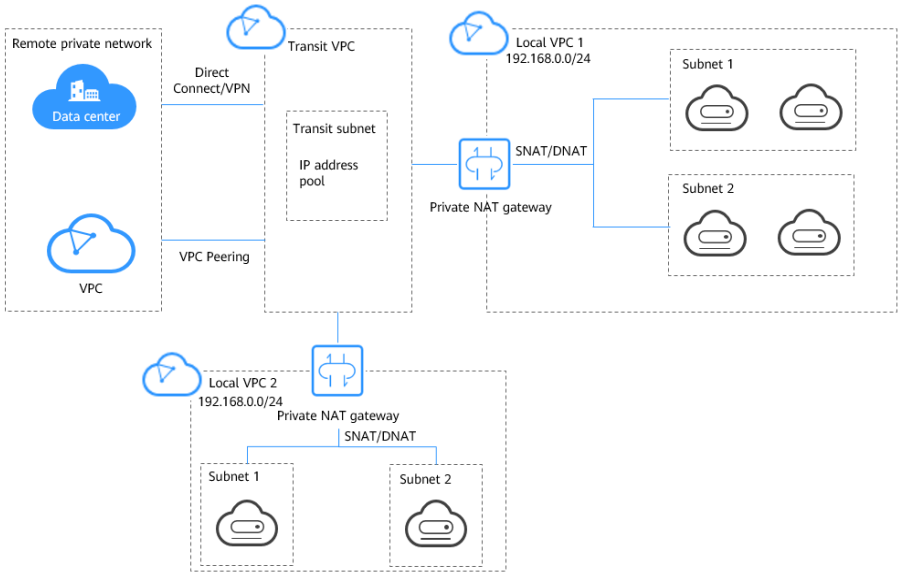
Transit Subnet

Una subred de tránsito es donde reside una dirección IP de tránsito.

Transit VPC

Una VPC de tránsito es donde reside una subred de tránsito.

Figura 1-3 Gateway de NAT privado



Un gateway de NAT privado se puede implementar para:

- Conectar las VPC con bloques CIDR superpuestos

  Puede implementar un gateway de NAT privado y configurar las reglas de SNAT y de DNAT para permitir que dos VPC con bloques CIDR superpuestos se comuniquen entre sí.

- Acceder a una red privada desde una dirección IP específica

  Un gateway de NAT privado le permite usar una dirección IP específica para acceder a un centro de datos local o a una VPC en una red privada remota. El centro de datos local se conecta a la VPC de tránsito a través de Direct Connect o VPN. La VPC remota se conecta a la VPC de tránsito a través de una conexión de emparejamiento de VPC. Como se muestra en la figura, se implementa un gateway de NAT privado y se configura una regla SNAT para que el gateway de NAT privado reemplace las direcciones IP privadas en la VPC 1 con una dirección IP específica de modo que la VPC 1 pueda comunicarse con la red privada a la izquierda a través de esta dirección IP específica.

- Los gateway de NAT privados son gratis por tiempo limitado en las siguientes regiones: CN East-Shanghai2, CN Southwest-Guiyang1, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg, and LA-Mexico City2.
- Los gateway de NAT privados se facturan en las siguientes regiones: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok y AP-Singapore.

¿Cómo accedo al servicio de NAT Gateway?

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

- Consola de gestión

  Inicie sesión en la consola de gestión y elija **NAT Gateway** en la lista de servicios para realizar operaciones en el gateway de NAT.

- API

  Utilice las API si necesita integrar NAT Gateway en su propia solución de sistema. Para obtener más información, consulta la **Referencia de la API de NAT Gateway**.

2 Ventajas del producto

Ventajas de los gateway de NAT públicos

- **Implementación flexible**

  Un gateway de NAT se puede compartir entre las subredes y AZs, de modo que incluso si una AZ falla, el gateway de NAT público todavía puede ejecutarse normalmente en otra AZ. El tipo y EIP de un gateway de NAT público se pueden cambiar en cualquier momento.

- **Facilidad de uso**

  Múltiples tipos de gateway de NAT están disponibles. La configuración del gateway de NAT público es simple, la operación & mantenimiento es fácil y se pueden aprovisionar rápidamente. Una vez aprovisionados, pueden funcionar de forma estable.

- **Rentabilidad**

  Múltiples servidores pueden compartir una EIP. Puede asociar uno o más EIP con un gateway de NAT público para permitir que varios servidores en una red privada se conecten a Internet a través de este EIP. Ya no es necesario configurar una EIP para cada servidor, lo que ahorra dinero en EIPs y ancho de banda.

Ventajas de los gateway de NAT privados

- **Planificación de red más fácil**

  Diferentes departamentos de una gran empresa pueden tener bloques CIDR superpuestos, por lo que la empresa tiene que volver a planificar su red antes de migrar sus cargas de trabajo a la nube. La replanificación lleva mucho tiempo y estresante. El gateway de NAT privado elimina la necesidad de volver a planificar la red para que los clientes puedan conservar su red original mientras migran a la nube.

- **Fácil operación & mantenimiento**

  Los departamentos de una gran empresa suelen tener redes jerárquicas para organizaciones jerárquicas, gestión basada en derechos y dominios y aislamiento de seguridad. Tales redes jerárquicas necesitan mapearse a una red a gran escala para permitir la comunicación entre ellas. Un gateway de NAT privado puede asignar el bloque CIDR de cada departamento al mismo bloque CIDR de VPC, lo que simplifica la gestión de redes complejas.

- **Seguridad fuerte**

  Los departamentos de una empresa pueden necesitar diferentes niveles de seguridad. Los gateway de NAT privados pueden exponer las direcciones IP y los puertos de solo

bloques CIDR especificados para cumplir con los requisitos de alta seguridad. Una delegación de regulación de la industria puede requerir que otras organizaciones usen una dirección IP específica para acceder a su sistema de regulación. Los gateway de NAT privados pueden ayudar a cumplir este requisito mediante la asignación de direcciones IP privadas a esa dirección IP especificada.

- **Cero conflictos de IP**

  Los servicios aislados de varios departamentos suelen utilizar direcciones IP del mismo bloque CIDR privado. Después de que la empresa migra las cargas de trabajo a la nube, se producen conflictos de direcciones IP. Gracias al mapeo de direcciones IP, los gateway de NAT privados permiten la comunicación entre bloques CIDR superpuestos.

3 Escenarios

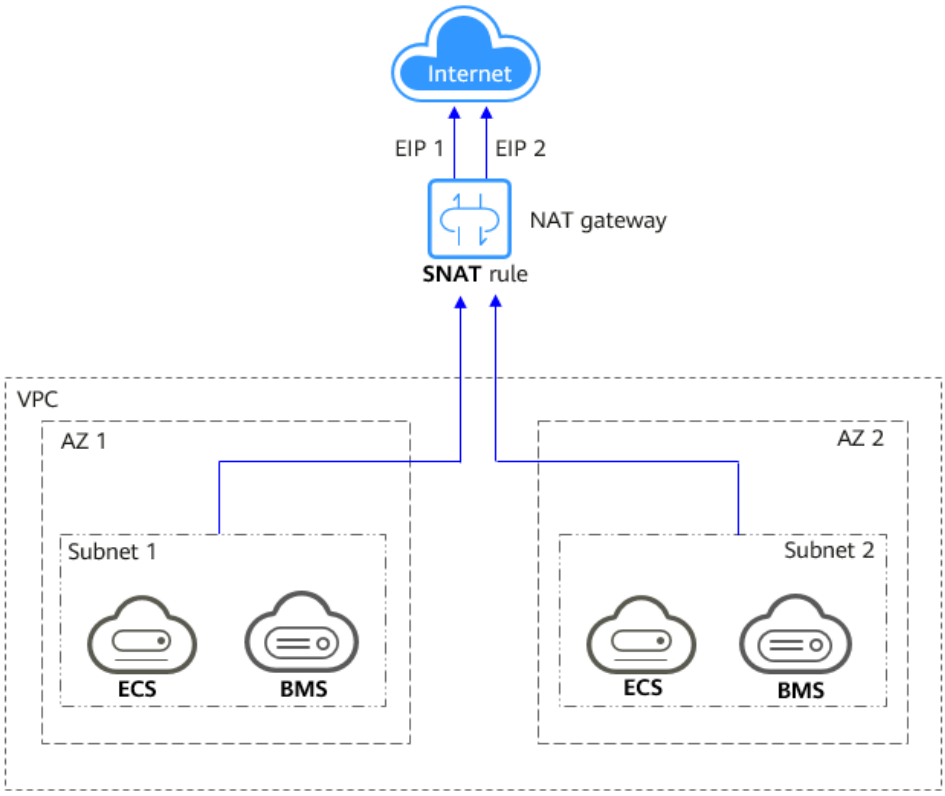
Gateway de NAT público

- **Permitir que una red privada acceda a Internet mediante SNAT**

  Si sus servidores en una VPC necesitan acceder a Internet, puede configurar reglas SNAT para permitir que estos servidores usen uno o más EIP para acceder a Internet sin exponer sus direcciones IP privadas. Solo puede configurar una regla de SNAT para cada subred en una VPC y seleccionar uno o más EIP para cada regla de SNAT. El gateway de NAT público proporciona diferentes números de conexiones y puede crear varias reglas de SNAT para satisfacer sus requisitos de servicio.

  Figura 3-1 muestra cómo los servidores de una VPC acceden a Internet mediante SNAT.

Figura 3-1 Uso de SNAT para permitir que los servidores de una VPC accedan a Internet



- **Permitir a los usuarios de Internet acceder a un servicio en una red privada mediante DNAT**

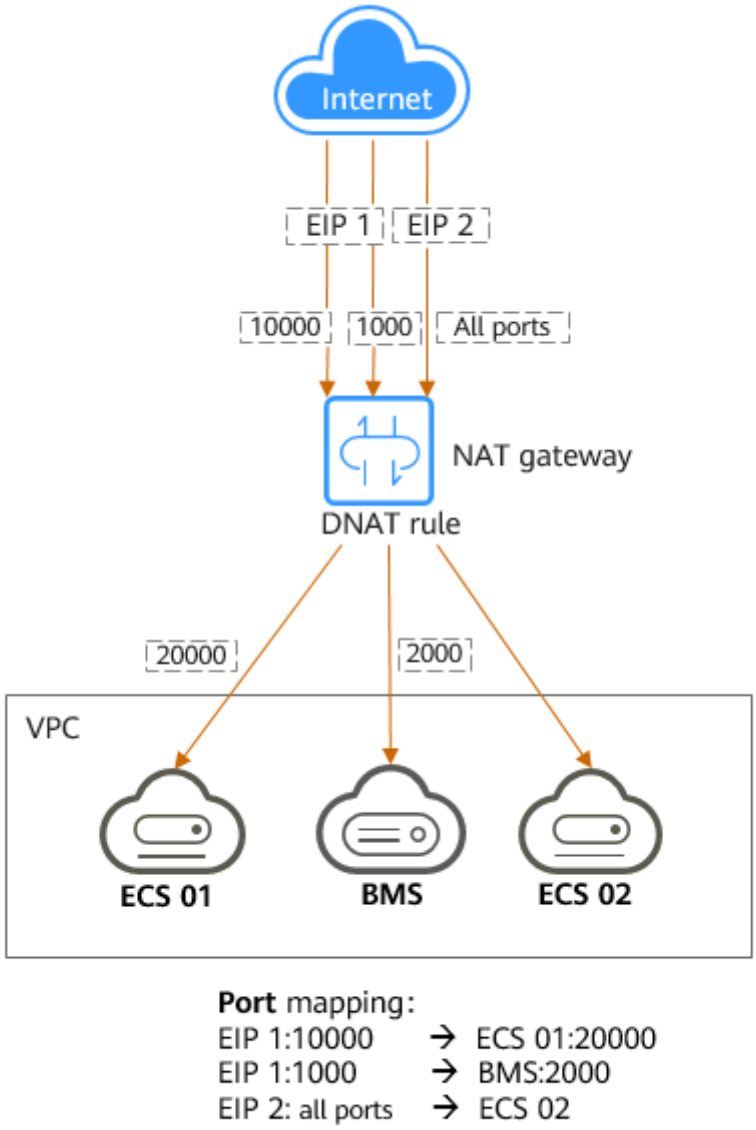
  Las reglas de DNAT permiten a los servidores de una VPC proporcionar servicios accesibles desde Internet.

  Después de recibir solicitudes desde un puerto específico a través de un protocolo específico, el gateway de NAT público puede reenviar las solicitudes a un puerto específico de un servidor a través de la asignación de puertos. El gateway de NAT público también puede reenviar todas las solicitudes destinadas a una EIP a un servidor específico a través de la asignación de direcciones IP.

  Se puede configurar una regla de DNAT para cada servidor. Si hay varios servidores, puede crear varias reglas de DNAT para asignar una o más EIP a las direcciones IP privadas de estos servidores.

  Figura 3-2 muestra cómo los servidores (ECSs o BMSs) en una VPC proporcionan servicios accesibles desde Internet mediante DNAT.

Figura 3-2 Uso de DNAT para permitir que los servidores de una VPC proporcionen servicios accesibles desde Internet

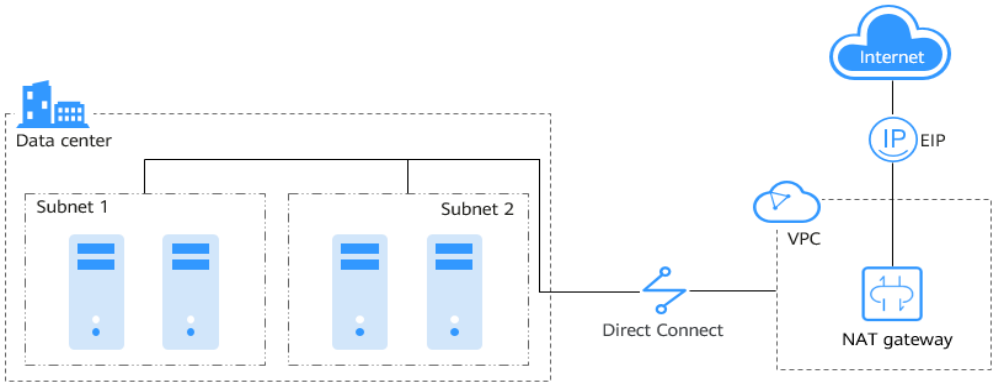


- **Permitir que los servidores de un centro de datos local accedan a Internet o sean accesibles desde Internet**

  En ciertos escenarios de Internet, juegos, comercio electrónico y financieros, un gran número de servidores en una nube privada están conectados a una VPC a través de Direct Connect o VPN. Si dichos servidores necesitan acceso seguro a Internet de alta velocidad o necesitan proporcionar servicios accesibles desde Internet, puede implementar un gateway de NAT y configurar las reglas SNAT y DNAT para cumplir con sus requisitos.

  Figura 3-3 muestra cómo utilizar SNAT y DNAT para proporcionar acceso a Internet de alta velocidad o proporcionar servicios accesibles desde Internet.

Figura 3-3 Uso de SNAT y DNAT para permitir la comunicación de alta velocidad con Internet



- **Configurar un sistema de alta disponibilidad mediante la adición de múltiples EIPs a una regla SNAT**

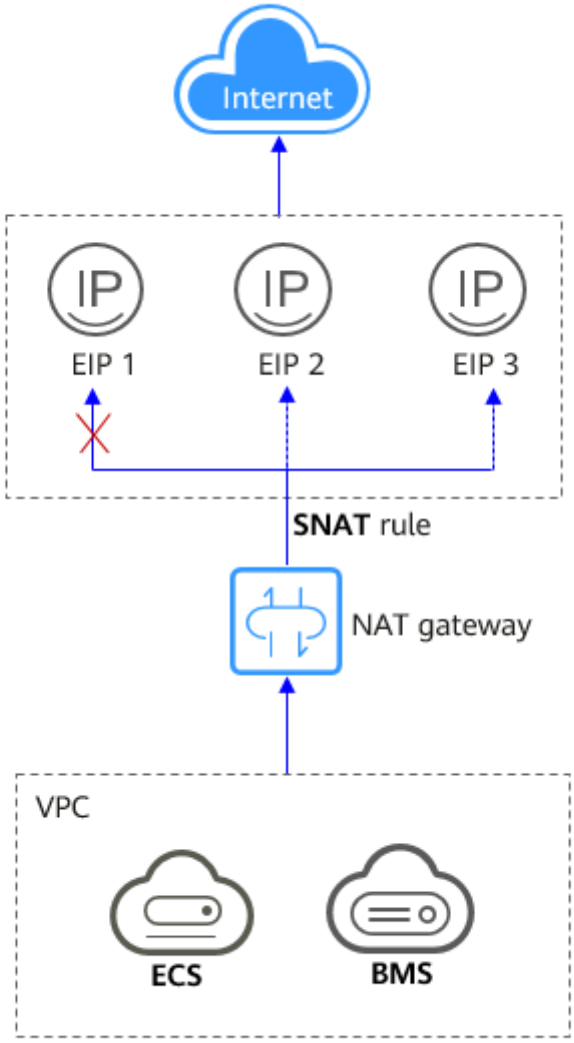
  Los EIP pueden ser atacados. Para mejorar la confiabilidad del sistema, puede vincular varias EIP a una regla SNAT de modo que si se ataca una EIP, otra EIP se puede utilizar para garantizar la continuidad del servicio.

  Cada regla SNAT puede tener hasta 20 EIP. Si una regla de SNAT tiene múltiples EIP, el sistema selecciona aleatoriamente un EIP para que los servidores utilicen para acceder a Internet.

  Si cualquier EIP está bloqueado o atacado, elimínelo manualmente del grupo EIP.

  Figura 3-4 muestra un sistema altamente disponible que usa una regla SNAT de un gateway de NAT público.

Figura 3-4 Uso de la regla SNAT de un gateway de NAT público para construir un sistema de alta disponibilidad



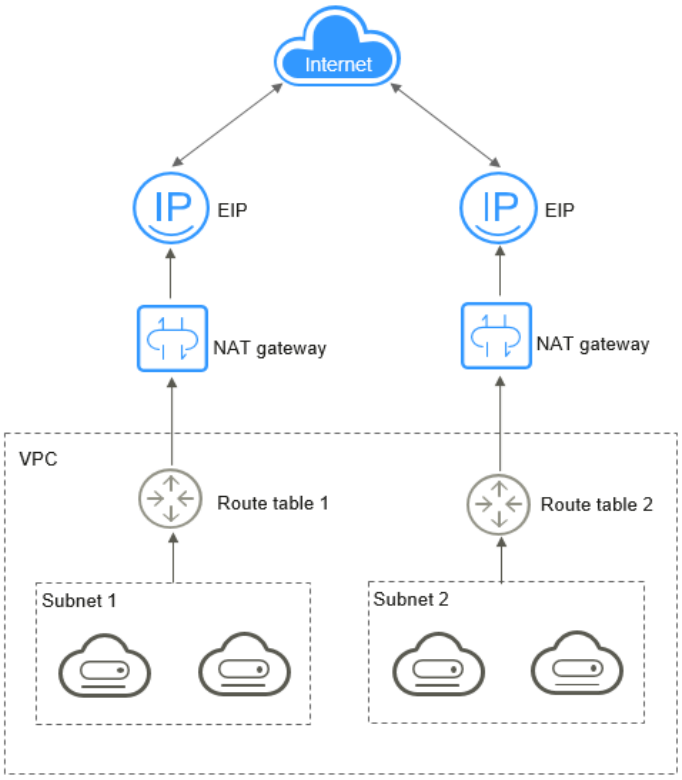
- **Usar múltiples gateways de NAT juntos**

  Si un solo gateway de NAT no puede cumplir con sus requisitos de rendimiento, por ejemplo, si hay más de un millón de conexiones SNAT, o si el ancho de banda máximo de 20 Gbit/s no puede cumplir con los requisitos de servicio, puede usar varios gateway de NAT juntos.

  Para utilizar varios gateway de NAT juntos, debe asociar las tablas de ruta de las subredes de VPC con estos gateway de NAT públicos.

  Figura 3-5 muestra cómo se utilizan varios gateway de NAT públicos para superar el cuello de botella de rendimiento.

Figura 3-5 Uso de múltiples gateways NAT públicos juntos



- El sistema no agrega una ruta predeterminada para un gateway de NAT público. Es necesario agregar una ruta que apunte al gateway de NAT público a la tabla de rutas correspondiente.
- Cada gateway NAT público tiene una tabla de rutas asociada. El número de gateway NAT públicos que se pueden crear en una VPC viene determinado por el número de tablas de ruta para la VPC.

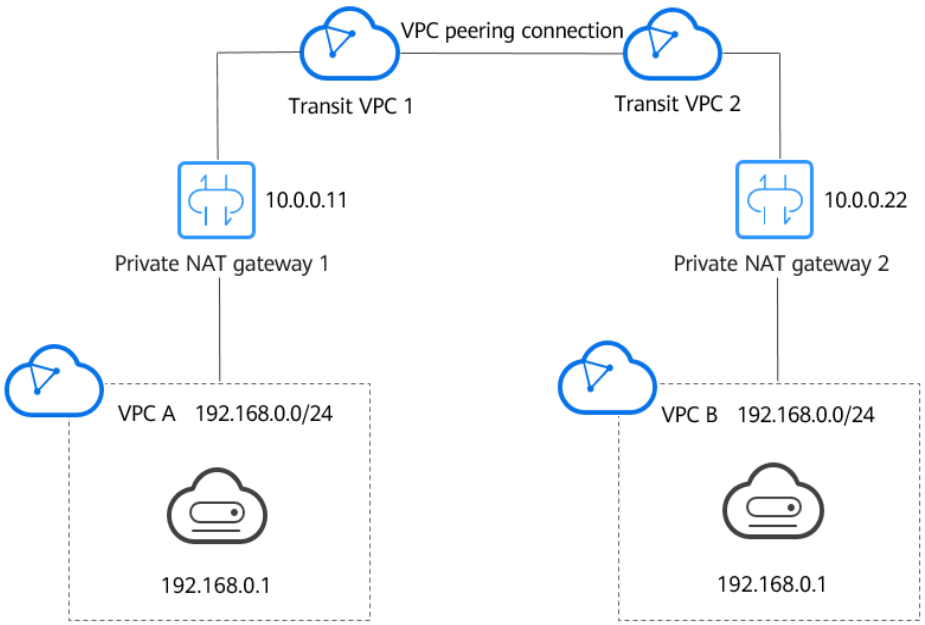
Gateway de NAT privado

- **Conectar las VPC con bloques CIDR superpuestos**

  Puede configurar dos gateway de NAT privados para dos VPC con bloques CIDR superpuestos y, a continuación, agregar reglas SNAT y DNAT en los dos gateway de NAT privados para permitir que los servidores en las dos VPC usen las direcciones IP de tránsito para comunicarse entre sí.

  En la siguiente figura, hay dos VPCs de tránsito y dos gateway de NAT privados. La dirección 192.168.0.1 en la VPC A se traduce a 10.0.0.11, y la dirección IP 192.168.0.1 en la VPC B se traduce a 10.0.0.22. Entonces se puede establecer un interconexión de VPC entre las dos VPC de tránsito para permitir la comunicación entre ellas.

Figura 3-6 Conexión de VPC con bloques CIDR superpuestos

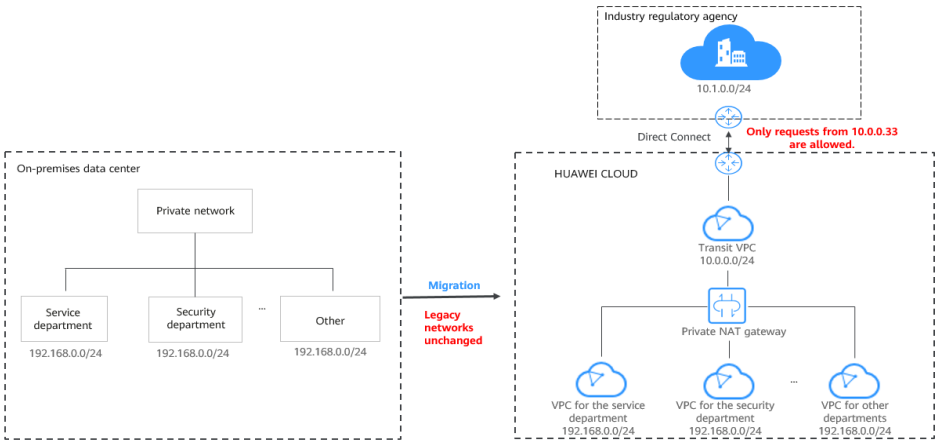


- **Migrar cargas de trabajo a la nube sin cambiar la topología de la red ni acceder a las agencias reguladoras desde direcciones IP específicas**

  Es posible que las organizaciones quieran migrar sus cargas de trabajo a la nube sin realizar ningún cambio en su topología de red existente. También pueden tener que acceder a las agencias reguladoras desde direcciones IP específicas según lo requieran estas agencias. Un gateway de NAT privado es una buena opción.

  La siguiente figura representa una red de empresa donde las subredes de diferentes departamentos se superponen. Un gateway de NAT privado permite a la empresa mantener la topología de red existente sin cambios mientras migra sus cargas de trabajo a la nube. En este ejemplo, el gateway de NAT privado asigna la dirección IP de cada departamento a 10.0.0.33 para que cada departamento pueda usar 10.0.0.33 para acceder de forma segura a la delegación reguladora.

Figura 3-7 Migrar cargas de trabajo a la nube sin cambiar la topología de la red ni acceder a las agencias reguladoras desde direcciones IP específicas



4 Especificaciones del gateway de NAT

El rendimiento del gateway NAT está determinado por el número máximo de conexiones SNAT admitidas.

Gateway de NAT público

Una conexión SNAT consiste en una dirección IP de origen, un puerto de origen, una dirección IP de destino, un puerto de destino y un protocolo de capa de transmisión. La dirección IP de origen es la EIP, y el puerto de origen es el puerto EIP. Una conexión SNAT identifica de forma única una sesión.

El rendimiento es el ancho de banda total de todos los EIP en las reglas de la DNAT. Por ejemplo, un gateway NAT público tiene dos reglas de DNAT. El ancho de banda de EIP en la primera regla de DNAT es de 10 Mbit/s, y el de la segunda regla de DNAT es de 5 Mbit/s. El rendimiento del gateway NAT público será de 15 Mbit/s.

Un gateway de NAT público admite hasta 20 Gbit/s de ancho de banda.

El tiempo de espera predeterminado de una conexión SNAT a través de TCP es de 900 segundos.

El tiempo de espera predeterminado de una conexión SNAT a través de UDP es de 300 segundos.

Seleccione una gateway NAT pública en función de sus requisitos de servicio. **Tabla 4-1** enumera las especificaciones del gateway de NAT público.

Tabla 4-1 Especificaciones del gateway de NAT público

Tipo	Número máximo de conexiones SNAT	Ancho de banda	Paquetes por segundo (PPS)
Small (pequeño)	10,000	20 Gbit/s	2,000,000
Medium (mediano)	50,000	20 Gbit/s	2,000,000
Large (grande)	200,000	20 Gbit/s	2,000,000

Tipo	Número máximo de conexiones SNAT	Ancho de banda	Paquetes por segundo (PPS)
Extra-large (extragrande)	1,000,000	20 Gbit/s	2,000,000

- El PPS de cada tipo de gateway NAT es 2,000,000 tanto en direcciones entrantes como en las salientes.
- Si el número de solicitudes excede el máximo de conexiones permitidas de un gateway de NAT público, los servicios se verán afectados negativamente. Para evitar esta situación, cree reglas de alarma en la consola de Cloud Eye para controlar el número de conexiones SNAT.
- Las reglas de DNAT de un gateway de NAT público son irrelevantes para el tipo de gateway NAT. Se pueden agregar hasta 200 reglas de DNAT a un gateway de NAT público. Para aumentar el número de reglas de la DNAT, **envíe un ticket de servicio**

Gateway de NAT privado

Una conexión SNAT consiste en una dirección IP de origen, un puerto de origen, una dirección IP de destino, un puerto de destino y un protocolo de capa de transmisión. La dirección IP de origen es la dirección IP de tránsito, y el puerto de origen es el puerto de la dirección IP de tránsito.

Seleccione un gateway de NAT privado en función de sus requisitos de servicio. **Tabla 4-2** enumera las especificaciones del gateway NAT privado.

Tabla 4-2 Especificaciones del gateway NAT privado

Tipo	Número máximo de conexiones SNAT	Ancho de banda	PPS	Número de reglas de NAT (reglas de SNAT +reglas de DNAT)
Small (pequeño)	2000	200 Mbit/s	20,000	20
Medium (mediano)	5000	500 Mbit/s	50,000	50
Large (grande)	20,000	2 Gbit/s	200,000	200
Extra-large (extragrande)	50,000	5 Gbit/s	500,000	500

Si el número de solicitudes excede el máximo de conexiones permitidas de un gateway NAT privado, los servicios se verán afectados negativamente. Para evitar esta situación, cree reglas de alarma en la consola de Cloud Eye para controlar el número de conexiones SNAT.

5 Notas y restricciones

Gateway de NAT público

When using a public NAT gateway:

- Múltiples reglas para un gateway de NAT público pueden usar el mismo EIP, pero las reglas para diferentes gateway de NAT deben usar diferentes EIP.
- Cada VPC puede asociarse con múltiples gateway de NAT públicos.
- Solo se puede agregar una regla SNAT para cada subred de VPC.
- SNAT y DNAT pueden compartir una EIP para ahorrar recursos de la EIP. Sin embargo, una regla SNAT no puede compartir una EIP con una regla DNAT cuyo **Port Type** se establece en **All ports**.
- Si tanto una EIP como un gateway de NAT público están configurados para un servidor, los datos se reenviarán a través de la EIP.
- Si la regla se utiliza en el escenario de Direct Connect, el bloque CIDR personalizado debe ser un bloque CIDR de una conexión Direct Connect y no puede superponerse con las subredes VPC del gateway de NAT.
- Después de realizar operaciones en los recursos subyacentes de un ECS, por ejemplo, cambiando sus especificaciones, las reglas de gateway NAT configuradas no serán válidas. Elimine las reglas y vuelva a crearlas para las nuevas especificaciones.
- Solo se puede configurar una regla de DNAT para cada puerto de un servidor. Un puerto puede asignarse a un solo EIP.
- Las direcciones IP privadas utilizadas por los balanceadores de carga no se pueden configurar cuando se agregan reglas de DNAT en los gateway de NAT públicos para comunicaciones por Internet.
- Se pueden agregar hasta 200 reglas de DNAT a un gateway de NAT público. El número de reglas SNAT que se pueden agregar a un gateway de NAT público no está limitado.
- Algunos operadores bloquearán los siguientes puertos por razones de seguridad. Se recomienda que no utilice los siguientes puertos.

Protocolo	Puerto
TCP	42 135 137 138 139 444 445 593 1025 1068 1434 3127 3128 3129 3130 4444 4789 4790 5554 5800 5900 9996

Protocolo	Puerto
UDP	135 to 139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

Gateway de NAT privado

Cuando se utiliza un gateway NAT privado:

- Agregue manualmente rutas en la VPC para conectarla a la red privada remota a través de un interconexión de VPC, conexión directa o conexión VPN.
- Solo se puede agregar una regla SNAT para cada subred de VPC.
- Las reglas de SNAT y de DNAT no pueden compartir una dirección IP de tránsito.
- Una regla DNAT con **Port Type** establecido en **All ports** no puede compartir la misma dirección IP de tránsito con una regla de DNAT con **Port Type** establecido en **Specific port**.
- El número total de reglas de DNAT y SNAT que se pueden agregar a un gateway de NAT privado varía con el tipo del gateway de NAT privado.
  - Pequeño: 20 o menos
  - Mediano: 50 o menos
  - Grande: 200 o menos
  - Extragrande: 500 o menos

- Los gateway de NAT privados son gratis por tiempo limitado en las siguientes regiones: CN East-Shanghai2, CN Southwest-Guiyang1, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg, and LA-Mexico City2.
- Los gateway de NAT privados se facturan en las siguientes regiones: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok y AP-Singapore.

6 Uso de NAT Gateway con otros servicios

Figura 6-1 muestra la relación entre NAT Gateway y otros servicios.

Figura 6-1 Relación entre NAT Gateway y otros servicios

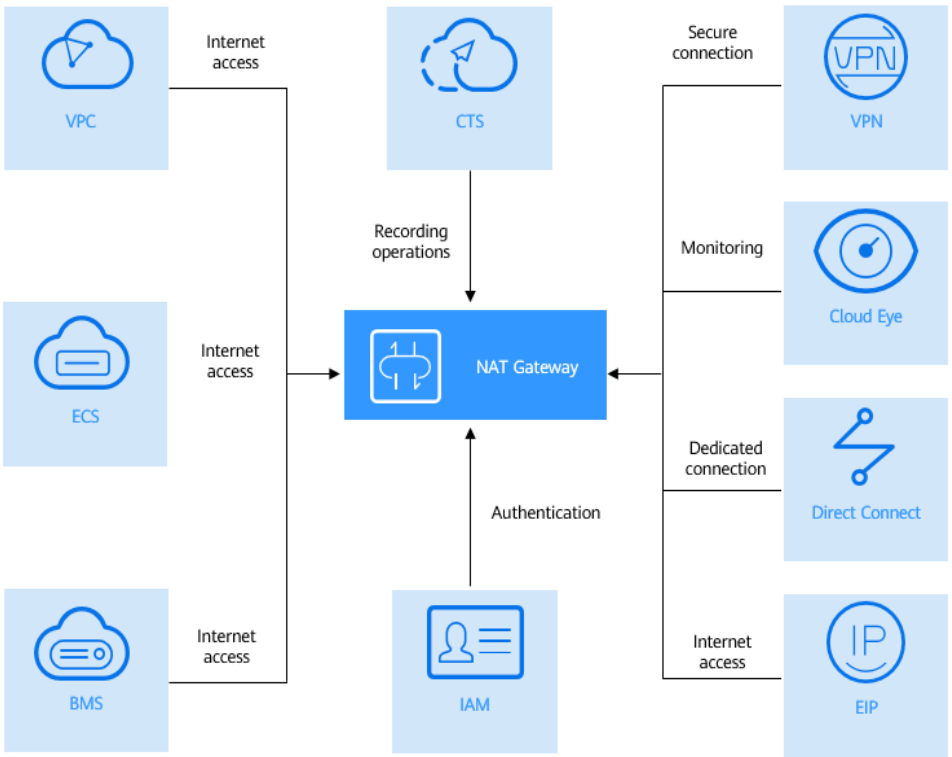


Tabla 6-1 Servicios relacionados

Servicio en la nube	Interacción	Referencia
Direct Connect	Los servidores locales conectados a una VPC a través de Direct Connect pueden usar un gateway de NAT público para acceder a Internet o proporcionar servicios accesibles desde Internet.	**Configuración de reglas de SNAT y de DNAT para permitir que los servidores locales se comuniquen con Internet a alta velocidad**
Virtual Private Network (VPN)	Una VPN establece un túnel de comunicación cifrado basado en Internet entre su red local y una VPC. Esto garantiza un acceso seguro a Internet a través de un gateway de NAT público.	**Configuración de reglas de SNAT y de DNAT para permitir que los servidores locales se comuniquen con Internet a alta velocidad**
ECS and BMS	Los ECS y BMS pueden utilizar un gateway de NAT público para acceder a Internet o proporcionar servicios accesibles desde Internet.	**Configuración de reglas de SNAT para permitir que los servidores accedan a Internet** **Configuración de reglas de DNAT para permitir que los servidores proporcionen servicios accesibles desde Internet**
VPC	Los ECS de una VPC pueden conectarse a Internet.	**Configuración de reglas de SNAT para permitir que los servidores accedan a Internet**
Elastic IP (EIP)	Con un gateway de NAT público, los servidores de una VPC pueden compartir una EIP para acceder a Internet o proporcionar servicios accesibles a Internet.	**Uso de SNAT para permitir que los servidores accedan a Internet** **Configuración de reglas de DNAT para permitir que los servidores proporcionen servicios accesibles desde Internet**
Cloud Eye	Puede ver los datos de supervisión del gateway de NAT en la consola de Cloud Eye.	**Consulta de métricas**

Servicio en la nube	Interacción	Referencia
Identity and Access Management (IAM)	Si necesita asignar diferentes permisos a los empleados de su empresa para controlar su acceso a sus recursos de NAT Gateway, IAM es una buena opción para la gestión de permisos detallada.	**Identity and Access Management**
Cloud Trace Service (CTS)	Con CTS, puede grabar operaciones en NAT Gateway para realizar consultas, auditorías y seguimiento posterior.	**Cloud Trace Service**

7 Facturación (gateway de NAT público)

Conceptos de facturación:

Los gateway de NAT públicos se facturan en función del tipo del gateway de NAT público y la duración del uso.

Hay disponibles cuatro tipos de gateway de NAT públicos: pequeños, medianos, grandes y extragrandes.

Para obtener detalles de precios, consulte **Calculadora de precios de NAT Gateway**.

Modos de facturación

Los gateway de NAT públicos se facturan por día.

Cambios de configuración

Si se cambia el tipo del gateway de NAT, el gateway de NAT con especificaciones más altas se facturará ese día.

cancelación de suscripción

Para darse de baja de un gateway de NAT público de pago por uso, solo tiene que **eliminarlo**.

8 Facturación (gateway de NAT privado)

Los gateway de NAT privados comenzaron a cobrarse a partir del 1 de junio de 2022.

Esta sección describe los detalles de facturación sobre los gateway de NAT privados.

Conceptos de facturación:

Los gateway de NAT privados se facturan según el tipo del gateway de NAT privado y la duración del uso.

Hay disponibles cuatro tipos de gateways de NAT privados: pequeños, medianos, grandes y extragrandes.

Modos de facturación

Los gateway de NAT privados se facturan por hora.

- Los gateway de NAT privados son gratis por tiempo limitado en las siguientes regiones: CN East-Shanghai2, CN Southwest-Guiyang1, CN-Hong Kong, LA-Sao Paulo1, AF-Johannesburg, and LA-Mexico City2.
- Los gateway de NAT privados se facturan en las siguientes regiones: CN South-Guangzhou, CN East-Shanghai1, CN North-Beijing4, AP-Bangkok y AP-Singapore.

Tabla 8-1 Precios unitarios del gateway de NAT privado de las diferentes especificaciones

Región	Small (pequeño)	Medium (mediano)	Large (grande)	Extra-large (extragrande)
CN South-Guangzhou	$0.076/ Gateway/Hora	$0.146/ Gateway/Hora	$0.286/ Gateway/Hora	$0.508/ Gateway/Hora
CN East-Shanghai1				
CN North-Beijing4				

Cambios de configuración

Las nuevas especificaciones entran en vigor inmediatamente tras el cambio. A continuación, se le cobrará según las nuevas especificaciones.

cancelación de suscripción

Para darse de baja de una pasarela NAT privada de pago por uso, solo tiene que **eliminarlo**.

9 Gestión de permisos

Puede utilizar Identity and Access Management (IAM) para gestionar los permisos de NAT Gateway y controlar el acceso a sus recursos. IAM proporciona la autenticación de identidad, la gestión de permisos y el control de acceso.

Puede crear usuarios de IAM para sus empleados y asignar permisos a estos usuarios sobre la base del principio de privilegio mínimo (PoLP) para controlar su acceso a tipos de recursos específicos. Por ejemplo, puede crear usuarios de IAM para desarrolladores de software y asignar permisos específicos para permitirles usar recursos de NAT Gateway pero evitar que puedan eliminar recursos o realizar operaciones de alto riesgo.

Si su cuenta de Huawei Cloudcuenta no requiere usuarios individuales de IAM para la gestión de permisos, omita 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 ¿Qué es IAM?**https://support.huaweicloud.com/intl/es-us/productdesc-iam/iam_01_0026.html**What Is IAM?What Is IAM?What Is IAM? What Is IAM?What Is IAM?What Is IAM?

Permisos de NAT Gateway

De forma predeterminada, los nuevos usuarios de IAM no tienen ningún permiso asignado. Para asignar permisos a estos nuevos usuarios, el administrador de cuentas debe agregarlos a uno o más grupos y adjuntar políticas o roles de permisos a estos grupos.

NAT Gateway es un servicio a nivel de proyecto implementado y accedido en regiones físicas específicas. Al asignar permisos de NAT Gateway a un grupo de usuarios, especifique los proyectos específicos de la región donde los permisos tendrán efecto. Si selecciona **All projects**, los permisos se otorgarán para todos los proyectos específicos de la región. Al acceder a NAT Gateway, los usuarios deben cambiar a una región donde se les haya autorizado a usar este servicio.

Puede conceder permisos a los usuarios mediante roles y políticas.

- Roles: Un tipo de mecanismo de autorización de granularidad gruesa que proporciona solo una cantidad limitada de roles de nivel de servicio. Al usar roles para conceder permisos, también debe asignar roles de dependencia. 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 para un control de acceso más seguro. Por ejemplo, el administrador de cuentas puede conceder a los usuarios de NAT Gateway solo los permisos para gestionar un cierto tipo de gateways NAT y reglas SNAT. La mayoría de las políticas definen permisos basados en API. Para ver las acciones de API admitidas por NAT Gateway, consulte **Políticas de permisos y acciones admitidas**.

Tabla 9-1 enumera todas las funciones y políticas definidas por el sistema admitidas por NAT Gateway.

Tabla 9-1 Funciones y políticas definidas por el sistema compatibles con NAT Gateway

Nombre de la política	Descripción	Tipo	Dependencia
NATFullAccess	Todas las operaciones en recursos de NAT Gateway.	Política definida por el sistema	N/A
NATReadOnlyAccess	Permisos de sólo lectura para todos los recursos de NAT Gateway.	Política definida por el sistema	N/A
NAT Administrator	Todas las operaciones en recursos de NAT Gateway.	Rol definido por el sistema	Para obtener este permiso, los usuarios también deben tener el permiso de **Tenant Guest**.

Tabla 9-2 enumera las operaciones comunes admitidas por cada política o rol del sistema de NAT Gateway. Seleccione las políticas según sea necesario.

Tabla 9-2 Operaciones comunes admitidas por cada política o función definida por el sistema de NAT Gateway

Operación	NATFullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Creación de un gateway de NAT	√	x	√
Consulta de gateways de NAT	√	√	√
Consulta de detalles del gateway de NAT	√	√	√

Operación	NATFullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Actualización de un gateway de NAT	√	x	√
Eliminación de un gateway de NAT	√	x	√
Adición de una regla SNAT	√	x	√
Consulta de una regla SNAT	√	√	√
Modificación de una regla SNAT	√	x	√
Eliminación de una regla SNAT	√	x	√
Adición de una regla de DNAT	√	x	√
Consulta de una regla de DNAT	√	√	√
Modificación de una regla de la DNAT	√	x	√
Eliminación de una regla de DNAT	√	x	√
Eliminación de reglas de DNAT por lotes	√	x	√
Importación de reglas de DNAT mediante plantillas	√	x	√
Exportación de reglas de DNAT mediante plantillas	√	√	√
Creación de una subred de tránsito	√	x	√

Operación	NATFullAccess	NAT ReadOnlyAccess	NAT Gateway Administrator
Consulta de subredes de tránsito	√	√	√
Consulta de detalles acerca de una subred de tránsito	√	√	√
Modificación de una subred de tránsito	√	x	√
Supresión de una subred de tránsito	√	x	√
Asignación de una dirección IP de tránsito	√	x	√
Consulta de una dirección IP de tránsito	√	√	√
Liberación de una dirección IP de tránsito	√	x	√

Para agregar o modificar una regla de DNAT, su cuenta debe tener el permiso **NAT FullAccess** o permiso detallado **nat:dnatRules:create/nat:dnatRules:update**. Después de configurar una regla de DNAT, agregue una regla de grupo de seguridad para permitir que Internet acceda a los servidores para los que está configurada la regla de DNAT. De lo contrario, la regla de la DNAT no puede tener efecto. Por lo tanto, se requiere el permiso **VPC FullAccess** o permiso detallado **vpc:securityGroups:create**.

Enlaces útiles

- **¿Qué es IAM?**
- **Creación de un usuario y concesión de permisos de NAT Gateway**
- **Políticas de permisos y acciones compatibles**

10 Región y AZ

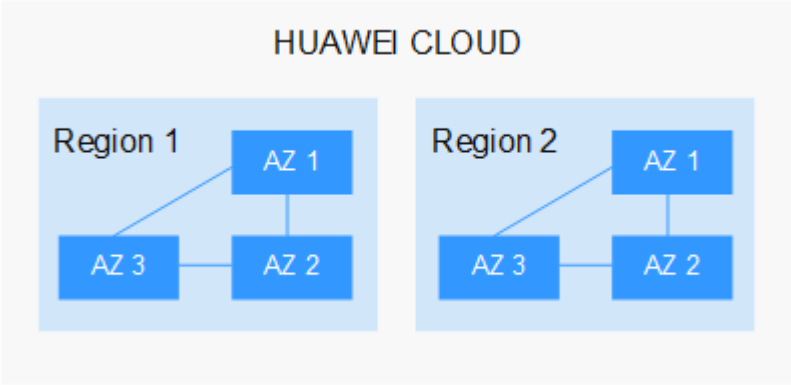
Concepto

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 10-1 muestra la relación entre regiones y AZ.

Figura 10-1 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**.

11 Conceptos básicos

EIP

EIP es una dirección IP pública estática.

Se puede acceder directamente a una EIP a través de Internet. Una dirección IP privada es una dirección IP en una red de área local (LAN) y no se puede enrutar a través de Internet.

Puede vincular un EIP a un ECS en su subred para permitir que el ECS se comunique con Internet.

Cada EIP puede ser utilizado por solo un ECS a la vez. Si desea que varios ECS en la misma VPC compartan una EIP, debe usar un gateway de NAT. Para obtener más información, consulte la **Guía del usuario de NAT Gateway**.

Conexiones SNAT

Una conexión SNAT consiste en una dirección IP de origen, un puerto de origen, una dirección IP de destino, un puerto de destino y un protocolo de capa de transmisión. La dirección IP de origen es la EIP, y el puerto de origen es el puerto EIP. Una conexión SNAT identifica de forma única una sesión.

Conexiones de DNAT

Las conexiones de DNAT permiten a los servidores de una VPC compartir una EIP para proporcionar servicios accesibles desde Internet.

12 Historial de revisiones

Lanzado en	Descripción
2022-07-27	Esta es la decimotercera versión oficial, que incorpora el siguiente cambio: Agregado el método de aumentar el número de reglas de DNAT para un gateway de NAT público en **Especificaciones del gateway de NAT**.
2022-06-15	Esta edición es el décimo lanzamiento oficial, que incorpora el siguiente cambio: Facturación modificada de los gateway de NAT privados desde que finaliza la OBT de los gateway de NAT privados.
2022-06-01	Esta edición es la novena versión oficial, que incorpora el siguiente cambio: Agregado **Facturación (gateway de NAT privado)**.
2022-02-18	Este edición es el octavo lanzamiento oficial, que incorpora el siguiente cambio: Agregado Infografía de NAT Gateway.
2021-12-23	Esta edición es el séptimo lanzamiento oficial, que incorpora los siguientes cambios: ● Agregado **Ventajas de los gateway de NAT privados**. ● Actualizado **Historial de revisiones**.
2021-11-12	Esta edición es el sexto lanzamiento oficial, que incorpora el siguiente cambio: Agregado CTS en **Uso de NAT Gateway con otros servicios**.
2021-10-28	Este número es el quinto lanzamiento oficial, que incorpora el siguiente cambio: Agregado **Gestión de permisos**.

Lanzado en	Descripción
2020-03-30	Esta edición es el cuarto lanzamiento oficial, que incorpora el siguiente cambio: Agregada la sección "Detalles de precios".
2019-11-05	Esta edición es la tercera versión oficial, que incorpora el siguiente cambio: Agregado el escenario SNAT HA.
2019-02-26	Esta edición es el segundo lanzamiento oficial, que incorpora el siguiente cambio: Agregado **Uso de NAT Gateway con otros servicios**.
2018-11-16	Esta edición es el primer lanzamiento oficial.

