NAT Gateway

Preguntas frecuentes

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 Gateway de NAT públicos

1.1 ¿Cuál es la relación entre una VPC, un gateway de NAT público, un ancho de banda de EIP y un ECS?

- Una VPC es un entorno de red seguro, aislado y lógico.
- Un gateway de NAT público permite que los ECS de una VPC accedan a Internet.
- EIP es un servicio que proporciona las direcciones IP estáticas válidas en Internet. El rendimiento de una VPC se determina por el ancho de banda de EIP.
- Un ECS es una instancia que se ejecuta en una VPC y utiliza un gateway de NAT público para acceder a Internet.

1.2 ¿Cómo ofrece un gateway de NAT público una alta disponibilidad?

El backend de un gateway de NAT público admite la recuperación automática de desastres con standby en modo activo y trabaja con Cloud Eye para informar alarmas, así reduciendo los riesgos y mejorando la disponibilidad.

1.3 ¿A qué puertos no se puede acceder?

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
UDP	135 a 139 1026 1027 1028 1068 1433 1434 4789 4790 5554 9996

1.4 ¿Cuáles son las diferencias entre el uso de un gateway de NAT público y el uso de una EIP para un ECS?

A Gateway NAT público proporciona SNAT y DNAT, por lo que múltiples ECS pueden compartir una EIP .

Un ECS también puede tener una EIP vinculada a él. La EIP no tiene que ser compartida.

Si tanto SNAT como EIP están configuradas para un ECS, los datos se reenviarán a través de la EIP .

Si tanto DNAT como EIP están configuradas para un ECS, el ECS tendrá dos EIP , una está directamente unida al ECS y otra está asociada con la regla de DNAT. Los datos entrantes serán reenviados por una de las dos EIP , que es determinada por el usuario cliente. Los datos salientes serán reenviados por la EIP directamente vinculada al ECS en prioridad. Si las dos EIP son diferentes, el reenvío de datos fallará.

No se recomienda configurar tanto un Gateway NAT público como una EIP para un ECS.

1.5 ¿Qué debo hacer si no puedo acceder a Internet a través de un gateway de NAT público?

Si su servidor no puede acceder a Internet con un Gateway NAT público, es posible que haya configurado incorrectamente la tabla de ruta de VPC. Realice los siguientes pasos para restablecer la tabla de ruta:

1. Localice la tabla de ruta asociada a la subred en la VPC.
2. Compruebe si la tabla de ruta contiene la ruta al gateway de NAT. Si no es así, agregue la ruta.
3. Asegúrese de que la dirección de destino de la ruta que se va a agregar contenga la dirección de destino.

1.6 ¿Puedo cambiar la VPC para un gateway de NAT público?

No.

La VPC que seleccionó cuando crear un Gateway NAT público no se puede cambiar después de crear el Gateway NAT público.

1.7 ¿El gateway de NAT público admite las direcciones IPv6?

No.

1.8 ¿Qué políticas de seguridad puedo configurar para desplegar el control de acceso si uso un gateway de NAT público?

Hay dos tipos de políticas de seguridad que puede configurar: grupos de seguridad y listas de control de acceso (ACL):

- 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. Después de crear un grupo de seguridad, puede crear varias reglas de acceso para el grupo de seguridad, y estas reglas se aplicarán a todos los ECS agregados a este grupo de seguridad.
- 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.

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.

Para obtener más información acerca de los grupos de seguridad y las ACL de red, consulte la sección "Seguridad" en la ***Guía de usuario de Virtual Private Cloud***.

1.9 ¿Qué puedo hacer si falla la conexión entre mis servidores e Internet después de agregar las reglas de SNAT y de DNAT?

Síntomas

Usted compró un Gateway NAT público y agregó las reglas de SNAT y de DNAT, pero sus servidores no pueden acceder a Internet ni proporcionar servicios accesibles desde Internet. Si la red configurada con un Gateway NAT público puede conectarse a Internet depende de la configuración de tabla de ruta, la configuración del grupo de seguridad y la configuración de ACL de red. Si se produce algún problema de configuración, la conexión de red fallará. Esta sección describe el proceso de localización de fallas después de configurar un Gateway NAT público.

Localización de fallas

Las siguientes causas de falla se enumeran en orden descendente de probabilidad de ocurrencia.

Si la falla persiste después de que se descarta una posible causa, baje la lista a las otras posibles causas.

Figura 1-1 Solución de problemas de desconexión de red

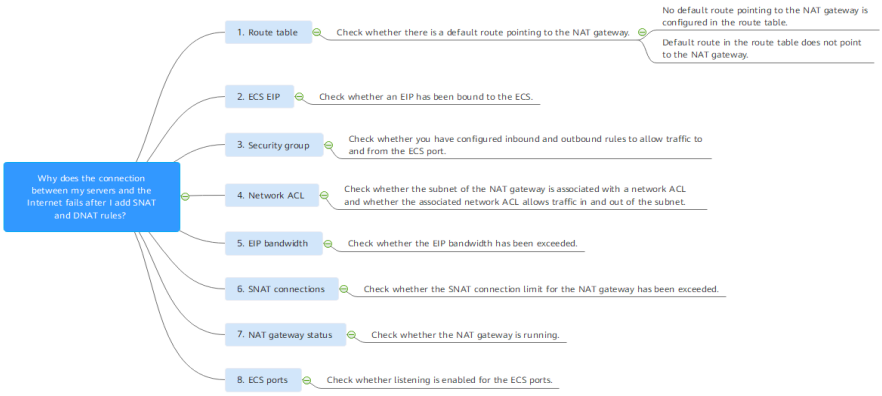


Tabla 1-1 Solución de problemas de desconexión de red

Causa posible	Solución
La tabla de ruta está configurada incorrectamente.	Agregue la ruta por defecto o una ruta que apunte al Gateway NAT público a la tabla de ruta. Para obtener más información, véase **Comprobación de si la ruta predeterminada que apunta al Gateway NAT público está configurada en la tabla de rutas**.
El ECS tiene una EIP vinculada.	Desvincule la EIP del ECS. Para obtener más información, véase **Comprobación de si el ECS tiene una EIP vinculada**.
Las reglas del grupo de seguridad están configuradas incorrectamente.	Configure las reglas del grupo de seguridad de ECS para permitir el tráfico hacia y desde el ECS. Para obtener más información, véase **Comprobación de si las reglas del grupo de seguridad permiten el tráfico hacia y desde el puerto de ECS**.
La ACL de red redestá configurada incorrectamente.	Agregue reglas de la ACL de red para permitir el tráfico dentro y fuera de la subred. Para obtener más información, véase **Comprobación de si las reglas de ACL de red permiten el tráfico dentro y fuera de la subred**.
El ancho de banda de la EIP excede el umbral.	Aumente el ancho de banda de EIP haciendo referencia a **Comprobación de si se ha superado el límite de ancho de banda de EIP**.
El volumen de servicio del Gateway NAT público excede el límite superior.	Aumente las especificaciones del Gateway NAT público. Para obtener más información, véase **Comprobación de si se ha superado el límite de conexión de SNAT para el Gateway NAT público**.
El estado de comprar es anormal.	Asegúrese de que el Gateway NAT público se está ejecutando. Para obtener más información, véase **Comprobar si el estado del Gateway NAT público es normal**.
No se escucha el puerto del ECS .	Vuelva a activar el puerto del ECS . Para obtener más información, véase **Comprobación de puertos de ECS**.

Comprobación de si la ruta predeterminada que apunta al Gateway NAT público está configurada en la tabla de rutas

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, elija **Route Tables**.
5. En la lista de tablas de ruta, haga clic en el nombre de la tabla de ruta asociada a la VPC al que pertenece el Gateway NAT público.
6. Compruebe si la ruta predeterminada (0.0.0.0/0) que apunta al Gateway NAT público está en la lista de rutas.
   - Si no, agregue la ruta por defecto que apunta al Gateway NAT público a la tabla de ruta.
     i. Haga clic en **Add Route** y configure los parámetros requeridos.

Figura 1-2 Agregar la ruta

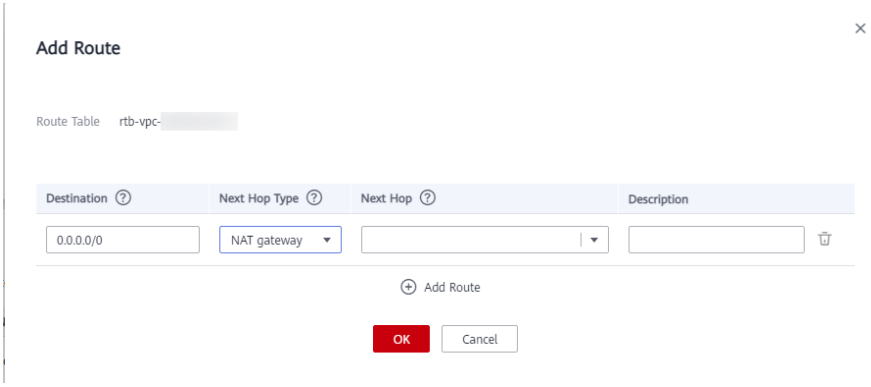


Tabla 1-2 Descripciones de parámetros

Parámetro	Descripción
Destination	El bloque CIDR de destino Póngalo a **0.0.0.0/0**.
Next Hop Type	Póngalo a **NAT gateway**.
Next Hop	Establezca el ID del Gateway NAT público que compró.
Descripción	(Opcional) Información complementaria sobre la ruta Ingrese hasta 255 caracteres. Los corchetes angulares (< o >) no están permitidos.

ii. Haga clic en **OK**.

- Si hay una ruta por defecto pero no apunta al Gateway NAT público, agregue una ruta que apunte al Gateway NAT público a la tabla de ruta existente. Alternativamente, cree una tabla de ruta y agregue una ruta predeterminada que apunte al Gateway NAT público a la nueva tabla de ruta.
  - Para agregar una ruta que apunte al Gateway NAT público a la tabla de ruta existente, realice los siguientes pasos:

    1) Haga clic en **Add Route** y configure los parámetros requeridos.

    Figura 1-3 Agregar la ruta

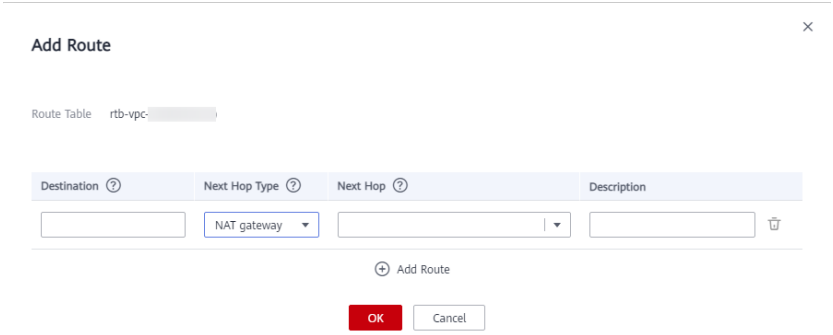
    

    Tabla 1-3 Descripciones de parámetros

Parámetro	Descripción
Destination	El bloque CIDR de destino
Next Hop Type	Póngalo a **NAT gateway**.
Next Hop	Establezca el ID del Gateway NAT público que compró.
Description	(Opcional) Información complementaria sobre la ruta Ingrese hasta 255 caracteres. Los corchetes angulares (< o >) no están permitidos.

    2) Haga clic en **OK**.

  - Cree una tabla de ruta y agregue una ruta por defecto que apunte al Gateway NAT público.

    NOTA

    Para crear una tabla de ruta, haga clic en **Increase Quota** en el cuadro de diálogo **Create Route Table** o elija **Service Tickets** > **Create Service Ticket** en la esquina superior derecha de la página **Route Tables** para aumentar primero su cuota de tabla de ruta. Para obtener más información, consulte **Creación de un ticket de servicio**.

    1) En la esquina superior derecha de la página **Route Tables**, haga clic en **Create Route Table** y configure los parámetros requeridos.

Tabla 1-4 Descripciones de parámetros

Parámetro	Descripción	Valor de ejemplo
Name	(Obligatorio) El nombre de la tabla de ruta Ingrese hasta 64 caracteres. Solo se permiten letras, dígitos, guiones bajos (_), guiones (-) y puntos (.). No se permiten espacios.	rtb-001
VPC	(Obligatorio) La VPC a la que pertenece la tabla de ruta	vpc-001
Descripción	(Opcional) Información complementaria sobre la tabla de ruta Ingrese hasta 255 caracteres. Los corchetes angulares (< o >) no están permitidos.	N/A
Route Settings	Información sobre rutas Puede hacer clic en **Add Route** para agregar más rutas. Establece **Destination** en **0.0.0.0/0**, **Next Hop Type** en **NAT gateway** y **Next Hop** en el Gateway NAT público que compraste.	N/A

2) Haga clic en **OK**.

   Aparece un cuadro de diálogo **Information** que indica que puede asociar la tabla de ruta a una subred ahora o más tarde.

3) Haga clic en **Associate Subnet**.

   Se muestra la ficha **Associated Subnets**.

4) Haga clic en **Associate Subnet** y seleccione la subred que desea asociar.

5) Haga clic en **OK**.

Comprobación de si el ECS tiene una EIP vinculada

Si tanto SNAT como EIP están configurados para un ECS,, laEIP se usa preferentemente para el reenvío de datos.

Si tanto DNAT como EIP están configurados para un ECS, el ECS tendrá dos EIP, una que está unida al ECS y otra que está asociada con la regla de DNAT. Los datos entrantes serán reenviados por una de las dos EIP, que es determinada por el usuario del cliente. Los datos salientes serán transmitidos por la EIP vinculada al ECS en prioridad. Si las dos EIP son diferentes, el reenvío de datos fallará.

Si el ECS tiene una EIP vinculada, realice los siguientes pasos para desvincular la EIP .

1. Inicie sesión en la consola de gestión.

2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En **Computing**, haga click en **Elastic Cloud Server**.
4. En la lista, localice el ECS . En la columna **IP Address**, compruebe si el ECS tiene una EIP vinculada.
   - Si no, compruebe el siguiente elemento.
   - Si es así, desvincúlela.

     Para obtener más información sobre cómo desvincular una EIP de un ECS , consulte la sección **Desvinculación de una EIP**.

Comprobación de si las reglas del grupo de seguridad permiten el tráfico hacia y desde el puerto de ECS

Si se deniega el tráfico hacia y desde el puerto de ECS en el grupo de seguridad, agregue reglas al grupo de seguridad para permitir el tráfico del puerto.

1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. En **Computing**, haga click en **Elastic Cloud Server**.
4. En la página **Elastic Cloud Server**, haga clic en el nombre del ECS .
5. Haga clic en la ficha **Security Groups** y vea las reglas del grupo de seguridad.
6. Compruebe si ha configurado las reglas entrantes y salientes para permitir el tráfico hacia y desde el puerto del ECS .
   - En caso afirmativo, compruebe el siguiente elemento.
   - Si no, haga clic en **Manage Rule**.

     En la página de la ficha **Summary** del grupo de seguridad, haga clic en **Inbound Rules** u **Outbound Rules** para agregar una regla de entrada y una de salida que permiten el tráfico hacia y desde el puerto del ECS . Para obtener más información acerca de los parámetros de reglas entrantes y salientes, consulte **Adición de una regla de grupo de seguridad**.

Comprobación de si las reglas de ACL de red permiten el tráfico dentro y fuera de la subred

Compruebe si la subred de VPC está asociada a las reglas deACL de red. En caso afirmativo, compruebe las reglas deACL de red.

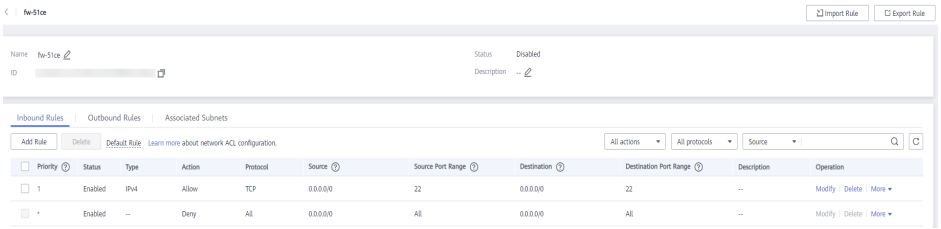
1. Inicie sesión en la consola de gestión.
2. Haga clic en  en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **Virtual Private Cloud**.
4. En el panel de navegación de la izquierda, haga clic en **Subnets**.
5. Compruebe si la subred del gateway de NAT está asociada con una ACL de red.

   El nombre específico de la ACL de red indica que la asociación tiene éxito.

Figura 1-4 ACL de red

6. Haga clic en el nombre de la ACL de red para ver los detalles.

Figura 1-5 Detalles de la ACL de red



7. Compruebe si se han agregado las reglas entrantes y salientes que permiten el tráfico dentro y fuera de la subred.

   Si no, agregue dichas reglas entrantes y salientes o disocie la ACL de red de la subred.

   Para obtener más información, consulte las secciones **Adición de una regla de ACL de red** y **Disociación de una subred de una ACL de red**.

   NOTA

   Las reglas de la ACL de red predeterminadas niegan todos los paquetes entrantes y salientes. Después de deshabilitar la ACL de red, las reglas predeterminadas siguen surtiendo efecto.

Comprobación de si se ha superado el límite de ancho de banda de EIP

Si una EIP está vinculada al Gateway NAT público, se utiliza el ancho de banda para proporcionar el tráfico de acceso entre la red pública y el Gateway NAT público.

Si la red está desconectada, compruebe si el ancho de banda de EIP excede el límite.

Para obtener más información, consulte **¿Cómo sé si se ha superado el límite de ancho de banda de mi EIP?**

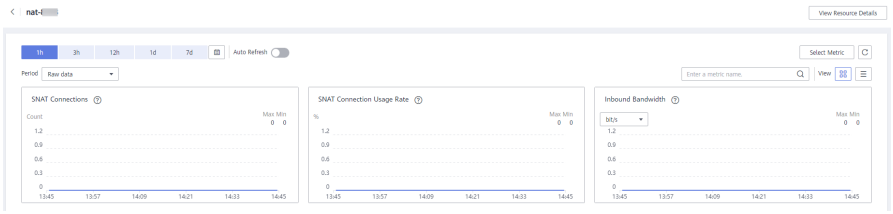
Para obtener instrucciones sobre cómo aumentar el ancho de banda, consulte **Cambio de un ancho de banda de EIP**.

Comprobación de si se ha superado el límite de conexión de SNAT para el Gateway NAT público

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Management & Governance**, seleccione **Cloud Eye**.

4. En el panel de navegación de la izquierda, elija **Cloud Service Monitoring** > **NAT Gateway**.
5. Busque la fila que contiene el Gateway NAT público que compró y haga clic en **View Metric** en la columna **Operation** para comprobar la supervisión detallada.

Figura 1-6 Detalles de la métrica del gateway de NAT



6. Compruebe si se ha superado el límite de conexión de SNAT para el Gateway NAT público.
   - Si no, compruebe el siguiente elemento.
   - Si el número de conexiones de SNAT excede el límite superior de las especificaciones del Gateway NAT público, aumente las especificaciones.

     Para obtener más información sobre cómo aumentar las especificaciones del Gateway NAT público, consulte **Modificación de un gateway de NAT público**.

Comprobar si el estado del Gateway NAT público es normal

1. Inicie sesión en la consola de gestión.
2. Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.
3. Haga clic en **Service List** en la esquina superior izquierda. En **Networking**, seleccione **NAT Gateway**.
4. En la lista de Gateway NAT público, localice el gateway de NAT y compruebe si su estado es **Running**.
   - En caso afirmativo, compruebe el siguiente elemento.
   - En caso negativo, las causas posibles son las siguientes:
     - El Gateway NAT público no se renueva a tiempo. Renueve la suscripción. Para obtener detalles sobre cómo renovar la suscripción, consulte **Realización de reembolso (clientes directos de pospago)**.
     - La cuenta o los recursos de su cuenta se congelan porque violó los requisitos de seguridad o las leyes y regulaciones relacionados al usar la plataforma en Huawei Cloud. Si completa la rectificación dentro del período requerido y cumple con los requisitos legales y de seguridad relacionados, su cuenta y recursos pueden ser descongelados. Si no completa la rectificación dentro del plazo requerido, se eliminarán sus recursos.

Comprobación de puertos de ECS

Asegúrese de que los puertos del ECS están en el estado **LISTEN**. **Tabla 1-5** enumera los estados comunes de TCP.

- Linux

Ejecute el comando **netstat -antp** para comprobar si el puerto de ECS está en el estado **LISTEN**.

Por ejemplo, ejecute **netstat -ntulp |grep 80**.

Figura 1-7 Comprobación del estado de escucha del puerto

```
[root@elb-mq02 ~]# netstat -antpu | grep sshd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      7178/sshd
```

Si no, habilite el puerto de ECS.

- Windows

  Realice las siguientes operaciones para comprobar la comunicación del puerto:

  a. Ejecute **cmd.exe**.

  b. Ejecute el comando **netstat -ano | findstr "***PID***"** para obtener el PID utilizado por el proceso.

     Por ejemplo, ejecute **netstat -ano | findstr "80"**.

     Figura 1-8 Comprobación del estado de escucha del puerto

```
C:\Users\Administrator>netstat -ano |findstr "80"
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       880
  TCP    [::]:80                [::]:0                 LISTENING       4
  TCP    [::]:49155             [::]:0                 LISTENING       880
  UDP    0.0.0.0:123            *:*                                    808
  UDP    [::]:123               *:*                                    808
```

     Si no, habilite el puerto de ECS.

Tabla 1-5 Estados comunes de TCP

Estado de TCP	Descripción	Escenario
LISTEN	Escucha las solicitudes de conexión de red desde un puerto de TCP remoto.	El servidor de TCP se está ejecutando.
ESTABLISHED	Se ha establecido una conexión.	Una conexión de TCP está correctamente configurada.
TIME-WAIT	Espera hasta que el servidor de TCP remoto reciba el acuse de recibo después de enviar una solicitud de desconexión.	La conexión de TCP está rota y este estado se borra en 1 minuto.
CLOSE-WAIT	Espera una solicitud de desconexión enviada por un usuario local.	Un error del programa resultó en un socket abierto. Este estado se muestra después de desconectar la red, lo que indica que un proceso está en un bucle infinito o esperando que se cumplan ciertos requisitos. Para resolver este problema, reinicie el proceso afectado.

Estado de TCP	Descripción	Escenario
FIN-WAIT-2	Espera la solicitud de desconexión de red desde un servidor de TCP remoto.	La red se ha desconectado y requiere 12 minutos para recuperarse automáticamente.
SYN-SENT	Espera la solicitud de conexión de red coincidente después de enviar una solicitud de conexión de red.	Falló la solicitud de conexión de TCP, que generalmente se debe a la demora en el manejo del uso alto de CPU en el servidor o por un ataque DDoS.
FIN-WAIT-1	Espera la solicitud de desconexión de TCP remota o el acuse de recibo de una solicitud de desconexión anterior.	Si la red se ha desconectado, es posible que este estado no se recupere automáticamente después de 15 minutos. Si el puerto permanece ocupado durante un largo período de tiempo, reinicie el sistema operativo para resolver el problema.

2 Gateway de NAT privados

2.1 ¿Cómo soluciono problemas de una falla de red después de configurar un gateway de NAT privado?

Comprobación de reglas de grupo de seguridad

Si se deniega el tráfico hacia y desde el puerto de ECS en el grupo de seguridad, agregue reglas al grupo de seguridad para permitir el tráfico del puerto.

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.

Paso 3 En **Compute**, seleccione **Elastic Cloud Server**.

Paso 4 En la lista de ECS, haga clic en el nombre del ECS para el que comprobará las reglas del grupo de seguridad.

Paso 5 Haga clic en la ficha **Security Groups** y vea las reglas del grupo de seguridad.

Paso 6 Compruebe si ha configurado las reglas entrantes y salientes para permitir el tráfico hacia y desde el puerto de ECS.

- En caso afirmativo, vaya a **Comprobación de si la ruta predeterminada que apunta al gateway de NAT privado está configurado en la tabla de rutas**.
- En caso negativo, vaya a **Paso 7**.

Paso 7 Haga clic en **Manage Rule**. En la página mostrada, haga clic en **Inbound Rules** u **Outbound Rules** para agregar una regla de entrada y una regla de salida que permitan el tráfico hacia y desde el puerto de ECS.

----Fin

Comprobación de si la ruta predeterminada que apunta al gateway de NAT privado está configurado en la tabla de rutas

Paso 1 Inicie sesión en la consola de gestión.

Paso 2 Haga clic en en la esquina superior izquierda y seleccione la región y el proyecto deseados.

Paso 3 En **Networking**, haga clic en **Virtual Private Cloud**.

Paso 4 En el panel de navegación de la izquierda, elija **Route Tables**.

Paso 5 En la lista de tablas de ruta, haga clic en el nombre de la tabla de ruta asociada a la VPC a la que pertenece el gateway de NAT privado.

Paso 6 Compruebe si la ruta que apunta al gateway de NAT privado está configurado en la lista de rutas.

----Fin

2.2 ¿Cuántos gateway de NAT privados puedo Comprar en una VPC?

Puede crear un máximo de 10 gateway de NAT privados en una VPC.

2.3 ¿Puedo aumentar el número de reglas de SNAT y de DNAT admitidas por un gateway de NAT privado?

Puede **crear un ticket de servicio** para solucionar este problema.

2.4 ¿Puede una regla de SNAT y de DNAT de un gateway de NAT privado compartir la misma dirección IP de tránsito?

No.

2.5 ¿Pueden los gateway de NAT privados traducir las direcciones IP locales conectadas a la nube por la conexión directa?

Sí. Al crear una regla de DNAT y seleccionar **Custom** para **Instance Type**, puede agregar una dirección IP local.

2.6 ¿Cuáles son las diferencias entre los gateway de NAT privados y los gateway de NAT públicos?

Los gateway de NAT privados realizan NAT entre direcciones IP privadas y resuelven los siguientes problemas:

- Conflictos de las direcciones IP privadas
- Acceso desde las direcciones especificadas

Los gateway de NAT públicos realizan NAT entre las direcciones IP privadas y las direcciones IP públicas y tienen las siguientes ventajas:

- Seguro: Solo las EIP compartidas, en lugar de todas las EIP de los servidores, están expuestas a Internet.
- Rentable: las EIP y el ancho de banda son compartidos, lo que ahorra costes de infraestructura de red.

2.7 ¿Cómo se factura el gateway de NAT privado?

Los gateway de NAT privados están en forma gratuita en algunas regiones durante un período limitado de tiempo y se facturan en otras regiones. Para saber cómo se facturan los gateway de NAT privados, consulte la **Facturación (gateway de NAT privado)**.

NOTA

- 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.

2.8 ¿Se puede usar un gateway de NAT privado entre las cuentas?

Los gateway de NAT privados no se pueden usar entre las cuentas. Sin embargo, puede utilizar una **interconexión de VPC** para conectar las VPC de tránsito de las dos cuentas. De esta manera, las dos VPC donde se despliegan los gateway de NAT privados de las dos cuentas pueden comunicarse entre sí.

3 Regla de SNAT

3.1 ¿Por qué necesito SNAT?

Gateway de NAT público: Además de requerir los servicios proporcionados por el sistema, algunos ECS también necesitan acceder al Internet para obtener información o descargar software. Sin embargo, la asignación de una dirección IP pública a cada ECS consume las direcciones IPv4 ya limitadas, conlleva los costes adicionales y puede aumentar la superficie de ataque en un entorno virtual. Es preferible y más práctico que varios ECS compartan una dirección IP pública. Esto se puede hacer usando SNAT.

Private NAT gateways: Los departamentos diferentes de una gran empresa pueden tener un gran número de bloques CIDR superpuestos. Después de que la empresa migre sus cargas de trabajo a la nube, esos departamentos no podrán comunicarse entre sí. En este caso, SNAT se puede utilizar para traducir las direcciones IP de múltiples ECS en un departamento en una dirección IP de tránsito para acceder a otros departamentos. En otros escenarios en los que se requiere alta seguridad, una delegación de regulación de la industria puede requerir que otras organizaciones usen una dirección IP especificada para acceder al sistema de regulación. En este caso, SNAT puede traducir las direcciones IP de varios servidores en una organización a una dirección IP de tránsito, es decir, la dirección IP especificada.

3.2 ¿Qué son las conexiones de SNAT?

Una conexión de 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 transporte. Una conexión de SNAT identifica de forma única una sesión. La dirección IP de origen y el puerto de origen se refieren a la dirección IP y el puerto después de NAT.

SNAT soporta tres protocolos: TCP, UDP e ICMP. Un gateway de NAT admite hasta 55,000 conexiones simultáneas a cada dirección IP y puerto de destino. Si cambia cualquiera de la dirección IP de destino, el número de puerto y el protocolo (TCP, UDP o ICMP), puede crear otras conexiones de 55,000. El número de conexiones que consulta en un ECS puede ser diferente del número real de conexiones de SNAT. (Puede ejecutar el comando **netstat** para consultar el número de conexiones.) Supongamos que un ECS crea 100 conexiones a un destino fijo cada segundo. Las 55,000 conexiones se agotarán en unos 10 minutos sin tener en cuenta las conexiones inactivas caídas. Como resultado, no se pueden establecer las nuevas conexiones.

Si no hay ningún paquete de datos que pase con la conexión de SNAT durante mucho tiempo, la conexión se agotará el tiempo de espera. Para evitar la interrupción de la conexión, inicie más paquetes de datos o utilice TCP para mantener las conexiones. Además, para evitar la interrupción del servicio causada por las conexiones insuficientes, utilice Cloud Eye para controlar el número de conexiones de SNAT y establecer las reglas de alarma adecuadas.

3.3 ¿Cuál es el ancho de banda de un gateway de NAT público utilizado por un servidor para acceder al Internet? ¿Cómo configuro el ancho de banda?

SNAT del gateway de NAT público traduce las direcciones IP privadas de servidores a las EIP. El ancho de banda de un gateway de NAT público utilizado por un servidor para acceder al Internet depende de la EIP que haya comprado.

Para obtener más información sobre cómo ajustar un ancho de banda, consulte la **Modificación del ancho de banda de EIP**.

3.4 ¿Cómo resuelvo las pérdidas de paquetes o las fallas de conexión al usar un gateway de NAT?

Si se producen las fallas de conexión o pérdidas de paquetes en un servidor que utiliza el gateway de NAT para acceder al Internet, puede comprobar las conexiones de SNAT en la consola de Cloud Eye. Si el número de conexiones de SNAT excede el soporte de las especificaciones del gateway de NAT, habrá pérdidas de paquetes o fallas de conexión.If the number of connections exceeds the upper limit, change the NAT gateway specifications.

3.5 ¿Qué debo hacer si mi ECS no puede acceder a un servidor en la red pública por el gateway de NAT público?

La conexión de TCP puede fallar cuando un ECS accede a un servidor de la red pública con una regla de SNAT. Realice los siguientes pasos para localizar la causa del error:

1. Ejecute el siguiente comando para comprobar si **tcp_tw_recycle** está habilitado en el servidor remoto:

   sysctl -a|grep tcp_tw_recycle

   Si **tcp_tw_recycle** está establecido en **1**, **tcp_tw_recycle** está habilitado.
2. Ejecute el siguiente comando para comprobar el número de paquetes perdidos del servidor remoto:

   cat /proc/net/netstat | awk '/TcpExt/ { print $21,$22 }'

   Si **ListenDrops** no se establece en **0**, se produce una pérdida de paquetes, es decir, la red está defectuosa.

Solución de problemas

Método 1: Modificación del parámetro del kernel del servidor remoto

- Ejecute el siguiente comando para modificar temporalmente los parámetros (la modificación no es válida después de reiniciar el servidor):

sysctl -w net.ipv4.tcp_tw_recycle=0

- Realice las operaciones siguientes para modificar permanentemente los parámetros:
  a. Modifique el archivo **/etc/sysctl.conf**:
     vi /etc/sysctl.conf
     Agregue el siguiente contenido al archivo:
     net.ipv4.tcp_tw_recycle=0
  b. Presione **Esc**, escriba **:wq!**, guarde el archivo y salga.
  c. Ejecute el siguiente comando para hacer que la modificación surta efecto:
     sysctl -p

Método 2: Modificación del parámetro del kernel del cliente local

- Para modificar temporalmente los parámetros (la configuración no es válida después de reiniciar el cliente local), configure el parámetro de la siguiente manera:
  sysctl -w net.ipv4.tcp_timestamps=0
- Realice las operaciones siguientes para modificar permanentemente los parámetros:
  a. Modifique el archivo **/etc/sysctl.conf**:
     vi /etc/sysctl.conf
     Agregue el siguiente contenido al archivo:
     net.ipv4.tcp_timestamps=0
  b. Presione **Esc**, escriba **:wq!**, guarde el archivo y salga.
  c. Ejecute el siguiente comando para hacer que la modificación surta efecto:
     sysctl -p

3.6 ¿Cuáles son las relaciones y diferencias entre los bloques CIDR en un gateway de NAT y en una regla de SNAT?

Al crear un gateway de NAT, debe especificar la VPC y el bloque CIDR de subred para el gateway de NAT. Este bloque CIDR solo puede ser utilizado por el sistema.

Cuando cree una regla de SNAT y establezca **Scenario** en **VPC**, seleccione una subred en la VPC de destino. De esta manera, los servidores de la subred pueden acceder a Internet con la regla de SNAT.

Cuando cree una regla de SNAT y establezca **Scenario** en **Direct Connect/Cloud Connect**, ingrese un bloque CIDR de un centro de datos local u otra VPC. Con esto, los servidores locales o servidores en la nube en el bloque CIDR pueden acceder a Internet con la regla de SNAT.

4 Reglas de DNAT

4.1 ¿Por qué necesito DNAT?

En un gateway de NAT público, DNAT permite a los servidores de una VPC compartir una EIP para proporcionar los servicios accesibles desde Internet. Con una EIP, un gateway de NAT público 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. Para obtener más información, consulte **Adición de una regla de DNAT**.

En un gateway de NAT privado, DNAT permite que los servidores que comparten la misma dirección IP de tránsito en una VPC proporcionen los servicios accesibles desde los centros de datos locales u otras VPC. Para obtener más información, consulte **Adición de una regla de DNAT**.

4.2 ¿Puedo modificar las reglas de DNAT?

Puede modificar las reglas de DNAT. Para los gateway de NAT públicos y privados, las reglas de DNAT pueden modificarse.

4.3 ¿Qué debo hacer si las reglas de gateway de NAT se vuelven inválidas después de que se cambien las especificaciones de ECS?

Si se cambian las especificaciones de ECS, las reglas del gateway de NAT configuradas no serán válidas. Tendrá que eliminar las reglas y crear nuevas reglas.

