Network Address Translation (NAT) FAQ

Contenido

Introducción

Este documento proporciona las respuestas a las preguntas frecuentes sobre el Network Address Translation (NAT).

NAT genérico

Q. ¿Qué es NAT?

A. El Network Address Translation (NAT) se diseña para la conservación de IP Address. Habilita las redes de IP privado que utilizan los IP Address no registrados para conectar con el Internet. El NAT actúa encendido a un router, generalmente conectando dos redes juntas, y traduce (no no global -) los direccionamientos únicos privados en la red interna a las direcciones legales, antes de que los paquetes se remitan a otra red.

Como parte de esta capacidad, el NAT se puede configurar para hacer publicidad de solamente un direccionamiento para toda la red al mundo exterior. Esto proporciona la seguridad complementaria con eficacia ocultando la red interna entera detrás de ese direccionamiento. El NAT ofrece las funciones duales de la Seguridad y de la conservación de dirección y se implementa típicamente en los entornos de acceso remoto.

Q. ¿Cómo el NAT trabaja?

A. Básicamente, el NAT permite que un único dispositivo, tal como un router, actúe como agente entre Internet (o red pública) y una red local (o red privada), así que significa que solamente un solo IP Address único está requerido para representar a un grupo completo de computadoras

cualquier cosa fuera de su red.

Q. ¿Cómo configuro el NAT?

A. Para configurar el NAT tradicional, usted necesita hacer por lo menos una interfaz en un router (NAT afuera) y otra interfaz en el router (NAT dentro) y un conjunto de reglas para traducir los IP Addresses en los encabezados de paquete (y las cargas útiles si está deseado) para necesitar ser configurado. Para configurar la interfaz virtual nacional (NVI), usted necesita por lo menos una interfaz configurada con el permiso NAT junto con el mismo conjunto de reglas como se mencionó anteriormente.

Para más información, refiera a la guía de configuración de los Servicios de direccionamiento IP del Cisco IOS o a configurar la interfaz virtual NAT.

Q. ¿Cuáles son las diferencias principales entre el Cisco IOS ® Software y las implementaciones del dispositivo de seguridad del Cisco PIX del NAT?

A. El Cisco IOS NAT basado en software no es fundamental diferente de la función NAT en el dispositivo de seguridad del Cisco PIX. Las diferencias principales incluyen los diversos tipos de tráfico soportados en las implementaciones. Refiera al Dispositivos de seguridad Cisco PIX de la serie 500 y a los ejemplos de la configuración del NAT para más información sobre la configuración del NAT en los dispositivos del Cisco PIX (incluye los tipos de tráfico soportados).

Q. ¿En qué Cisco que rutea el hardware está el Cisco IOS NAT disponible? ¿Cómo puede el hardware ser pedido?

A. La herramienta del Cisco Feature Navigator permite que los clientes identifiquen una característica (NAT) y que encuentren en cuál está disponibles la versión y la versión de hardware esta característica del Cisco IOS Software. Refiera al Cisco Feature Navigator para utilizar esta herramienta.

Q. ¿La NAT ocurre antes o después del ruteo?

A. La orden en la cual las transacciones se procesan usando el NAT se basa encendido si un paquete va de la red interna a la red externa o de la red externa a la red interna. El interior a la traducción exterior ocurre después de rutear, y el exterior a la traducción interior ocurre antes de rutear. Refiera al Orden NAT de funcionamiento para más información.

Q. ¿Se puede el NAT desplegar en un entorno público del Wireless LAN?

A. Sí. El NAT - IP estático la característica del soporte proporciona el soporte para los usuarios con los IP Address estáticos, habilitando a esos usuarios para establecer una sesión IP en un entorno público del Wireless LAN.

Q. ¿El NAT hace el balanceo de carga TCP para los servidores en la red interna?

A. Sí. Usando el NAT, usted puede establecer un host virtual en la red interna que coordina la carga a compartir entre los host reales. Refiera a evitar la sobrecarga del servidor usando el Equilibrio de carga TCP para más información.

Q. ¿Puede el límite de velocidad l el número de traducciones de NAT?

A. Sí. La característica de la traducción de NAT de la limitación de la tarifa proporciona la capacidad de limitar el número máximo de Funcionamientos de NAT simultáneos en un router. Además de dar a los usuarios más control sobre cómo se utilizan los direccionamientos NAT, la característica de la traducción de NAT de la limitación de la tarifa se puede utilizar para limitar los efectos de los virus, de los gusanos, y de los establecimientos de rechazo del servicio.

Q. ¿Cómo el rutear se aprende o se propaga para las subredes IP o los direccionamientos que son utilizados por el NAT?

A. La encaminamiento para los IP Addresses creados por el NAT es docta si:

- Derivan al agrupamiento de direcciones globales internas de la subred de un Next Hop Router.
- La entrada de Static Route se configura en el Next Hop Router y se redistribuye dentro de la red de la encaminamiento.

Cuando corresponden con a la dirección global interna con la interfaz local, el NAT instala un IP alias y una entrada ARP, en este caso el router **Proxy-arp** para estos direccionamientos. Si este comportamiento no se quiere, utilice la palabra clave del ninguno-*alias*.

Cuando configuran a un agrupamiento NAT, la opción de la agregar-*ruta* se puede utilizar para la inyección automática de la ruta.

Q. ¿Cuántas sesiones NAT simultáneas son admitidas en el NAT de Cisco IOS?

A. El límite de la sesión de NAT es limitado por la cantidad de DRAM disponible en el router. Cada traducción de NAT consume cerca de 312 bytes en el DRAM. Como consecuencia, 10,000 traducciones (más que sea dirigido generalmente en un único router) consumen sobre el 3 MB. Por lo tanto, el hardware típico de la encaminamiento tiene más que suficiente memoria para soportar miles de traducciones NAT.

Q. ¿Qué clase de funcionamiento de la encaminamiento puede ser esperado al usar el Cisco IOS NAT?

A. El Cisco IOS NAT soporta el Cisco Express Forwarding Switching, la transferencia rápida, y el process switching. Para la versión 12.4T y posterior, el trayecto de Switching rápido se soporta no más. Para la plataforma Cat6k, la orden de la transferencia es Netflow (trayecto de Switching HW), CEF, trayecto del proceso.

El funcionamiento depende de varios factores:

- El tipo de aplicación y su tipo de tráfico
- Si los IP Addresses están integrados
- Intercambio y examen de los mensajes múltiples
- Puerto de origen requerido
- El número de traducciones
- Otras aplicaciones que se ejecutan en ese entonces
- El tipo de hardware y procesador

Q. ¿Se puede el Cisco IOS NAT aplicar a las subinterfaces?

A. Sí. Las traducciones de la fuente y/o del NAT de destino se pueden aplicar a cualquier interfaz o subinterfaz que tiene una dirección IP (interfaces del dialer incluyendo). El NAT no se puede configurar con la interfaz virtual inalámbrica. La interfaz virtual inalámbrica no existe a la hora de la escritura al NVRAM. Así, después de la reinicialización, el router suelta la configuración del NAT en la interfaz virtual inalámbrica.

Q. ¿Se puede el Cisco IOS NAT utilizar con el Hot Standby Router Protocol (HSRP) para proporcionar los links redundantes a un ISP?

A. Sí. El NAT proporciona el HSRP redundante. Sin embargo, es diferente de SNAT (NAT stateful). El NAT con el HSRP es un sistema apátrida. No mantienen a la sesión en curso cuando ocurre el error. Durante la configuración NAT estática (cuando un paquete no hace juego ninguna configuración ESTÁTICA de la regla), el paquete se envía a través sin ninguna traducción.

Q. ¿El Cisco IOS NAT soporta las traducciones entrantes en una interfaz de Frame Relay? ¿Es compatible con las traducciones de salida en el lado Ethernet?

A. Sí. La encapsulación no importa para el NAT. El NAT puede ser hecho donde hay una dirección IP en una interfaz y la interfaz es NAT interior o NAT afuera. Debe haber un interior y un exterior para que el NAT funcione. Si usted utiliza NVI, debe haber por lo menos una interfaz habilitada NAT. ¿Vea cómo lo hago configuro el NAT? para más detalles.

Q. ¿Puede un solo router con NAT habilitado permitir que algunos usuarios utilicen el NAT y a otros usuarios en la misma interfaz de Ethernet para continuar utilizando sus propios IP Addresses?

A. Sí. Esto puede ser realizado con el uso de una lista de acceso que describe el conjunto de los host o de las redes que requieren el NAT. Todas las sesiones sobre el mismo host serán traducidas o pasarán a través del router y no serán traducidas.

Las Listas de acceso, las listas de acceso ampliadas, y los mapa del ruta se pueden utilizar para definir las *reglas* por las cuales los dispositivos IP consiguen traducidos. La dirección de red y la máscara de subred apropiada deben ser especificadas siempre. La palabra clave no se debe utilizar en lugar de la dirección de red o de la máscara de subred (véase NAT FAQ, mejores prácticas y Guía de despliegue para más detalle). Con la configuración NAT estática, cuando lo hace el paquete no correspondido con con cualquier configuración ESTÁTICA de la regla, el paquete será enviado a través sin ninguna traducción.

Q. ¿Al configurar para la PALMADITA (overloading (sobrecarga)), cuál es el número máximo de traducciones que se puedan crear por el IP Address global interior?

A. La PALMADITA (overloading (sobrecarga)) divide los puertos disponibles por el IP Address global en tres rangos: 0-511, 512-1023, y 1024-65535. La PALMADITA asigna un puerto de origen único para cada UDP o sesión TCP. Intenta asignar el valor de mismo puerto de la solicitud original, pero si el puerto de fuente original se ha utilizado ya, comienza a analizar desde el principio del rango de puerto determinado para encontrar el primer puerto disponible y lo asigna a la conversación. Hay una excepción para la base del código 12.2S. la base del código 12.2S

utiliza diversa lógica del puerto, y no hay reserva del puerto.

Q. ¿Cómo funciona PAT?

A. La PALMADITA trabaja con un IP Address global o las múltiples direcciones.

PALMADITA con una dirección IP

Condición	Descripción
1	El NAT/PAT examina el tráfico y lo hace juego a una regla de traducción.
2	Coincidencias de la regla a una configuración de la PALMADITA.
3	Si la PALMADITA sabe sobre el tipo de tráfico y si ese tipo de tráfico tiene “un conjunto de los puertos específicos o vira hacia el lado de babor él negocia” ese él utiliza, ACARICIE a los conjuntos ellos a un lado y no los afecta un aparato como Identificadores únicos.
4	Si una sesión sin los requisitos especiales del puerto intenta conectar hacia fuera, ACARICIE traduce el IP Source Address y marca la Disponibilidad del puerto de fuente originado (433, por ejemplo). **Nota:** Para el Transmission Control Protocol (TCP) y el User Datagram Protocol (UDP), los rangos son: 1-511, 512-1023, 1024-65535. Para el Internet Control Message Protocol (ICMP), el primer comienzo del grupo en 0.
5	Si el puerto de origen requerido está disponible, la PALMADITA asigna el puerto de origen, y la sesión continúa.
6	Si el puerto de origen requerido no está disponible, la PALMADITA comienza a buscar desde el principio del grupo relevante (comenzando en 1 para el TCP o las aplicaciones UDP, y a partir de la 0 para el ICMP).
7	Si un puerto está disponible se asigna, y la sesión continúa.
8	Si no hay puertos disponibles, el paquete se pierde.

PALMADITA con los IP Addresses múltiples

Condición	Descripción
1-7	Las primeras siete condiciones son lo mismo que

	con una sola dirección IP.
8	Si no hay puertos disponibles en el grupo relevante en la primera dirección IP, el NAT se mueve encendido a la dirección IP siguiente en el pool e intenta afectar un aparato el puerto de fuente original pedido.
9	Si el puerto de origen requerido está disponible, el NAT asigna el puerto de origen y la sesión continúa.
10	Si el puerto de origen requerido no está disponible, el NAT comienza a buscar desde el principio del grupo relevante (comenzando en 1 para el TCP o las aplicaciones UDP, y a partir de la 0 para el ICMP).
11	Si existe un puerto disponible, éste es asignado y la sesión prosigue.
12	Si no hay puertos disponibles, se cae el paquete, a menos que otra dirección IP esté disponible en el pool.

Q. ¿Cuáles son agrupaciones IP NAT?

A. Las agrupaciones IP NAT son un rango de los IP Addresses que se afectan un aparato para la traducción de NAT según las necesidades. Para definir un pool, utilizan al comando configuration:

ip nat pool <*name***> <***start-ip***> <***end-ip***> {netmask <***netmask***> | prefix-length <***prefix-length***>} [type {rotary}]**

Ejemplo 1

El siguiente ejemplo traduce entre los host interiores dirigidos de 192.168.1.0 o de la red de 192.168.2.0 global - a la red única 10.69.233.208/28:

```
ip nat pool net-208 10.69.233.208 10.69.233.223 prefix-length 28
ip nat inside source list 1 pool net-208
!
interface ethernet 0
ip address 10.69.232.182 255.255.255.240
ip nat outside
!
interface ethernet 1
ip address 192.168.1.94 255.255.255.0
ip nat inside
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.2.0 0.0.0.255
```

Ejemplo 2

En el siguiente ejemplo, la meta es definir a una dirección virtual, las conexiones a quien se distribuyen entre un conjunto de los host reales. El pool define los direccionamientos de los host reales. La lista de acceso define a la dirección virtual. Si no existe una traducción ya, los paquetes TCP de la interfaz serial 0 (la interfaz exterior) cuyo destino hace juego la lista de acceso se traducen a un direccionamiento del pool.

```
ip nat pool real-hosts 192.168.15.2 192.168.15.15 prefix-length 28 type rotary
ip nat inside destination list 2 pool real-hosts
!
interface serial 0
ip address 192.168.15.129 255.255.255.240
ip nat outside
!
interface ethernet 0
ip address 192.168.15.17 255.255.255.240
ip nat inside
!
access-list 2 permit 192.168.15.1
```

Q. ¿Cuál es el número máximo de agrupaciones IP configurables NAT (ip nat pool “nombre”)?

A. En el uso práctico, la cantidad de DRAM disponible en el router determinado limita al número máximo de agrupaciones IP configurables. (Cisco recomienda que usted configura un tamaño de pool de 255.) Cada pool debe ser no más que 16 bits. En 12.4(11)T y posterior, el IOS introduce CCE (motor de la clasificación típica). Esto ha limitado el NAT solamente para tener un máximo de 255 pools. En la base del código 12.2S, no hay restricción de los pools del máximo.

Q. ¿Cuál es la ventaja de usar el route-map contra el ACL en un agrupamiento NAT?

A. Un route-map está protegiendo a los usuarios externos indeseados para alcanzar a los usuarios/a los servidores interiores. También tiene la capacidad para asociar una sola dirección IP interior a diversas direcciones globales internas basadas en la regla. Refiera al soporte NAT para los agrupamientos múltiples que usan el Route Maps para más información.

Q. ¿Cuál es dirección IP “que solapa” en el contexto del NAT?

A. El solapar de la dirección IP refiere a una situación donde están ambas dos ubicaciones que quieren interconectar usando el mismo esquema de la dirección IP. Esto no es una ocurrencia poco frecuente; sucede a menudo cuando las compañías se combinan o se adquieren. Sin soporte especial, las dos ubicaciones no podrán conectarse y establecer sesiones. La dirección IP solapada puede ser una dirección pública asignada a otra compañía, una dirección privada asignada a otra compañía, o puede venir del rango de las direcciones privadas según lo definido en el RFC 1918 .

Los IP Address privados son unroutable y requieren las traducciones de NAT permitir las conexiones al mundo exterior. La solución implica el interceptar de las respuestas de la consulta de nombre del Domain Name System (DNS) del exterior al interior, configurando una traducción para la dirección externa, y reparando para arriba la respuesta de DNS antes de remitirla al host interior. Requieren a un servidor DNS ser implicado a ambos lados del dispositivo NAT para resolver a los usuarios que quieren tener conexión entre ambas redes.

El NAT puede examinar y realizar la traducción de la dirección en el contenido de los expedientes DNS *A* y *PTR*, tal y como se muestra en de usar el NAT en las redes superpuestas.

Q. ¿Cuáles son traducciones NAT estáticas?

A. Las traducciones NAT estáticas tienen mapeo uno a uno entre las direcciones local y global. Los usuarios pueden también configurar las traducciones de dirección estática al nivel del puerto,

y utilizan el resto de la dirección IP para otras traducciones. Esto ocurre típicamente donde usted está realizando el Port Address Translation (PAT).

El siguiente ejemplo muestra cómo configurar el routemap para permitir la traducción de afuera hacia adentro para el NAT estático:

```
ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127'
route-map R1 permit 10 match ip address ACL-A
```

Q. Qué es significada por la sobrecarga de NAT del término; ¿es esta PALMADITA?

A. Sí. La sobrecarga de NAT es la PALMADITA, que implica el usar de un pool con un rango de uno o más direccionamientos o el usar de una dirección IP de la interfaz conjuntamente con el puerto. Cuando usted sobrecarga, usted crea una traducción totalmente ampliada. Esto es una entrada de la tabla de traducción que contiene la dirección IP y la fuente/la información de puerto destino, que comúnmente se llama PAT o overloading (sobrecarga).

La PALMADITA (o overloading (sobrecarga)) es una característica del Cisco IOS NAT que se utiliza para traducir a las direcciones privadas *internas* (del Inside Local) a uno o más los IP Addresses del *exterior* (interior global, registrado generalmente). Para distinguir las conversaciones, se utilizan números de puerto de origen únicos en cada traducción.

Q. ¿Cuáles son traducciones NAT dinámicas?

A. En traducciones NAT dinámicas, los usuarios pueden establecer la correspondencia dinámica entre las direcciones local y global. La correspondencia dinámica es lograda definiendo las direcciones locales que se traducirán y la dirección IP de la agrupación de direcciones o de la interfaz de quienes afectar un aparato las direcciones globales y la asociación de los dos.

Q. ¿Cuál es ALG?

A. ALG es un gateway de capa de aplicación (ALG). El NAT realiza el servicio de traducción en cualquier tráfico del protocolo Protocolo de control de transmisión (TCP)/del protocolo UDP (TCP/UDP) que no lleve la fuente y/o los IP Address de destino en los datos de aplicación fluyen.

Estos protocolos incluyen el FTP, HTTP, FLACO, H232, DNS, RAS, SORBO, TFTP, telnet, archie, finger, NTP, NFS, rlogin, rsh, RCP. Los protocolos específicos que integran la información de la dirección IP dentro del payload requieren el soporte de un gateway del nivel de aplicación (ALG).

Refiérase con los gatewayes del nivel de aplicación con el NAT para más información.

Q. ¿Es posible crear una configuración con traducciones NAT estáticas y dinámicas?

A. Sí. Sin embargo, la misma dirección IP no se puede utilizar para la configuración estática NAT o en el pool para la configuración dinámica NAT. Todos los IP Address públicos necesitan ser únicos. Observe que no excluyen a las direcciones globales usadas en traducciones estáticas automáticamente con las agrupaciones dinámicas que contienen a esas mismas direcciones

globales. Las agrupaciones dinámicas deben ser creadas para excluir los direccionamientos asignados por las Entradas estáticas. Para más información, refiera a configurar el NAT estático y dinámico simultáneamente.

Q. ¿Cuando un traceroute se hace a través de un router NAT, debe el traceroute mostrar el direccionamiento NAT-global o debe él escaparse el direccionamiento NAT-local?

A. Traceroute del exterior debe volver siempre a la dirección global.

Q. ¿Cómo la PALMADITA afecta un aparato el puerto?

A. El NAT introduce las características adicionales del puerto: alcance total y port-map.

- El alcance total permite que el NAT utilice todos los puertos sin importar su rango del puerto predeterminado.
- El port-map permite que el NAT reserve a un usuario define el rango de puertos para la aplicación específica.

Refiera a los rangos definidos por el usario del puerto de origen para la PALMADITA para más información.

En 12.4(20)T2 hacia adelante, el NAT introduce la distribución aleatoria del puerto para L3/L4 y el simétrico-puerto.

- La distribución aleatoria del puerto permite que el NAT seleccione aleatoriamente cualquier puerto global para la petición del puerto de origen.
- el Simétrico-puerto permite que el NAT apoye a la *independiente del punto final*.

Refiera a la anatomía: Traductores de la mirada de un direccionamiento de red interna para más información.

Q. ¿Cuál es la diferencia en medio fragmentación de IP y segmentación TCP?

A. Fragmentación de IP ocurre en la capa 3 (IP); La segmentación TCP ocurre en el (TCP) de la capa 4. Fragmentación de IP ocurre cuando los paquetes que son más grandes que la Unidad máxima de transmisión (MTU) (MTU) de una interfaz se envían de esta interfaz. Estos paquetes tendrán que ser hechos fragmentos o ser desechados cuando se envían la interfaz. Si el bit del don't fragment (DF) no se fija en el encabezado IP del paquete, el paquete será hecho fragmentos. Si el bit DF se fija en el encabezado IP del paquete, se cae el paquete y un mensaje de error ICMP que indica el vlaue del Next-Hop MTU será devuelto al remitente. Todos los fragmentos de un paquete del IP llevan la misma identificación en el encabezado IP, que permite que el receptor final vuelva a montar los fragmentos en el paquete del IP original. Refiera a la resolución fragmentación de IP, los problemas MTU, MSS, y PMTUD con el GRE y IPSec para más información.

La segmentación TCP ocurre cuando una aplicación en una estación terminal está enviando los datos. Los datos de aplicación están rotos en lo que considera el TCP los pedazos mejor-clasificados enviar. Esta unidad de datos pasajeros del TCP al IP se llama un segmento. Los segmentos TCP se envían en los datagramas IP. Estos datagramas IP pueden entonces convertirse en fragmentos IP como pasan a través de los links del MTU inferior de la red y del encuentro que ellos pueden caber a través.

El TCP primero dividirá estos datos en segmentos en los segmentos TCP (basados en el valor TCP MSS) y agregará el encabezado TCP y pasará este segmento TCP al IP. Entonces el IP agregará un encabezado IP para enviar el paquete al host de extremo remoto. Si el paquete del IP con el segmento TCP es más grande que el IP MTU en una interfaz saliente en la trayectoria entre el IP de los host TCP entonces hará fragmentos del paquete IP/TCP para caber. Estos fragmentos del paquete del IP serán vueltos a montar en el host remoto por la capa IP y el segmento completo TCP (que fue enviado originalmente) será dado a la capa TCP. La capa TCP no tiene ninguna idea que el IP había hecho fragmentos del paquete durante transita.

El NAT soporta los fragmentos IP, pero no soporta los segmentos TCP.

Q. ¿El NAT soporta fuera de servicio para fragmentación de IP y la segmentación TCP?

A. El NAT soporta solamente los fragmentos IP fuera de servicio debido al virtual-**nuevo ensamble del IP**.

Q. ¿Cómo hacer el debug de fragmentación de IP y segmentación TCP?

A. El NAT utiliza el mismo debug CLI para ambos fragmentación de IP y la segmentación TCP: **frag nacional del IP del debug**.

Q. ¿Hay un NAT soportado MIB?

A. No. Allí en ningún NAT soportado MIB, incluyendo CISCO-IETF-NAT-MIB.

Q. ¿Cuál es *tiempo de espera agotado de TCP*, y cómo él se relaciona con el temporizador TCP NAT?

A. Si la entrada en contacto de tres vías no se completa y el NAT ve un paquete TCP, después el NAT comenzará un 60-segundo temporizador. Cuando se completa la entrada en contacto de tres vías, el NAT utiliza un temporizador de 24 horas para una entrada de NAT por abandono. Si un host extremo envía una RESTAURACIÓN, el NAT cambia el temporizador predeterminado a partir de 24 horas a 60 segundos. En el caso del FIN, el NAT cambia el temporizador predeterminado a partir de 24 horas a 60 segundos en que recibe el FIN y FIN-ACK.

Q. ¿Puedo cambiar la cantidad de tiempo que toma para que un tranlation NAT mida el tiempo hacia fuera de la tabla del tranlation NAT?

A. Sí. Usted puede cambiar los valores de agotamiento del tiempo NAT para todas las entradas o para diversos tipos de tranlations NAT (tales como UDP-descanso, dns-descanso, TCP-descanso, finrst-descanso, ICMP-descanso, PPTP-descanso, SYN-descanso, puerto-descanso y ARP-ping-descanso).

Q. ¿Cómo paro el Lightweight Directory Access Protocol (LDAP) de asociar los bytes adicionales a cada paquete de respuesta LDAP?

A. Las configuraciones LDAP agregan los bytes adicionales (resultados de la búsqueda LDAP) mientras que procesan los mensajes de la Búsqueda-RES-entrada del tipo. El LDAP asocia 10

bytes de los resultados de la búsqueda a cada uno del paquete de respuesta LDAP. En caso que este 10 bytes de dato adicionales den lugar al paquete que excede la Unidad máxima de transmisión (MTU) (MTU) en una red, se cae el paquete. En este caso, Cisco recomienda que usted apaga este comportamiento LDAP usando el comando de la añadir-ldap-búsqueda-**RES del servicio del no ip nat** CLI para que los paquetes sean enviados y reciban.

Q. ¿Cuál es la recomendación de la ruta para el interior global/el IP Address local del exterior en el cuadro NAT?

A. Una ruta tiene que ser especificada en el cuadro configurado NAT para el IP Address global interior para las características tales como NAT-NVI. Semejantemente, una ruta se debe también especificar en el cuadro NAT para el IP Address local exterior. En este caso, cualquier paquete del en hacia fuera a la dirección usando la regla estática del exterior requerirá esta clase de ruta. En tales escenarios, mientras que proporciona a la ruta para IG/OL, el IP Address de Next Hop debe también ser configurado. Si la configuración del salto siguiente falta, esto se considera un Error de configuración y dará lugar al comportamiento indefinido.

NVI-NAT está presente en la trayectoria de la función de resultados solamente. Si usted tiene directamente la subred conectada con NAT-NVI o la regla exterior de la traducción de NAT configurada en el cuadro, después en esos escenarios, usted necesita proporcionar un IP Address de Next Hop simulado y también un ARP asociado para el salto siguiente. Esto es necesario para que la infraestructura subyacente dé el paquete al NAT para la traducción.

Q. ¿El Cisco IOS NAT soporta los ACL con una palabra clave del “registro”?

A. Cuando usted configura el Cisco IOS NAT para la traducción NAT dinámica, un ACL se utiliza para identificar los paquetes que pueden ser traducidos. La arquitectura NAT actual no soporta los ACL con una palabra clave del “registro”.

VOZ-NAT

Q. ¿El NAT soporta el protocolo skinny client control (SCCP) v17 que se envía con el administrador de las Comunicaciones unificadas de Cisco (CUCM) V7?

A. CUCM 7 y todas las cargas del teléfono del valor por defecto para CUCM 7 soportan SCCPv17. La versión del SCCP usada es determinada por la versión común más alta entre CUCM y el teléfono cuando el teléfono se registra.

El NAT todavía no soporta el SCCP v17. Hasta que el soporte NAT para el SCCP v17 se implemente, el firmware se debe retroceder a la versión 8-3-5 o anterior para negociar el SCCP v16. CUCM6 no encontrará el problema del NAT con ninguna carga del teléfono mientras utilice el SCCP v16. El Cisco IOS no soporta actualmente la versión 17 del SCCP.

Q. ¿Qué versiones de la carga CUCM /SCCP/firmware son soportadas por el NAT?

A. El NAT soporta las versiones de la versión 6.x y anterior CUCM. Estas versiones CUCM se liberan con la carga del firmware del teléfono del valor por defecto 8.3.x (o anterior) que soportan el SCCP v15 (o anterior).

El NAT no soporta las versiones 7.x CUCM o versiones posteriores. La versión estos CUCM se

libera con la carga del firmware del teléfono del valor por defecto 8.4.x que soporta el SCCP v17 (o más adelante).

Si CUCM se utiliza 7.x o más adelante, una más vieja carga del firmware se debe instalar en el servidor TFTP CUCM de modo que los teléfonos utilicen una carga del firmware con el SCCP v15 o para soportar anterior por el NAT.

El link abajo confirma que la carga del firmware 8.3.x contiene el SCCP v15 o anterior y trabajará con el NAT y que la carga del firmware 8.4.x contiene el SCCP v17 y no trabajará con el NAT.

http://third-gen-phones.gforge.cisco.com/twiki/prod/bin/view/Thirdgenphones/CCMLoadNumberAndCodeNameDecoderRing

Q. ¿Cuál es mejora de la asignación del puerto de la PALMADITA del proveedor de servicio para el RTP y el RTCP?

A. La mejora de la asignación del puerto de la PALMADITA del proveedor de servicio para la característica RTP y RTCP asegura eso para el SORBO, H.323, y las llamadas de voz flacas. Los números del puerto usados para las secuencias RTP son números del puerto uniformes, y las secuencias RTCP son el número del puerto impar subsiguiente siguiente. El número del puerto se traduce a un número dentro del rango especificado conforme al RFC-1889. Una llamada con un número del puerto dentro del rango dará lugar a una traducción de la PALMADITA a otro número del puerto dentro de este rango. Asimismo, una traducción de la PALMADITA para un número del puerto fuera de este rango no dará lugar a una traducción a un número dentro del rango dado.

Refiera a la mejora de la asignación del puerto de la PALMADITA del proveedor de servicio para el RTP y el RTCP para más información.

Q. ¿Cuál es Session Initiation Protocol (SIP) y puede SORBER los paquetes sea NATted?

A. El Session Initiation Protocol (SIP) es un Control Protocol ASCII-basado, de la capa de la aplicación que se puede utilizar para establecer, para mantener, y para terminar las llamadas entre dos o más puntos finales. El SIP es un protocolo alternativo desarrollado por la Fuerza de tareas de ingeniería en Internet (IETF) (IETF) para la Conferencia de los multimedia sobre el IP. La implementación del SIP de Cisco permite a las Plataformas de Cisco soportadas para señalar la configuración de la Voz y las multimedias llaman sobre las redes del IP.

Los paquetes del SORBO pueden ser NATted.

Q. ¿Cuál es soporte recibido del Traversal NAT para el regulador de la frontera de la sesión (SBC)?

A. El Traversal recibido Cisco IOS NAT para la característica SBC permite a un router del gateway del nivel de la aplicación del SORBO del Cisco IOS NAT (ALG) para actuar como SBC en un gateway multiservicio de Cisco IP-to-IP, que ayuda a asegurar la salida lisa de los servicios de la voz sobre IP (VoIP).

Refiera a configurar el Traversal recibido Cisco IOS NAT para el regulador de la frontera de la sesión y el Traversal recibido SP NAT para las llamadas del SORBO usando el regulador de la

frontera de la sesión del Cisco IOS para más información.

Q. ¿Cuántos SORBEN, flaco, y las llamadas H323 pueden una memoria del Routers y un CPU dirigir con el NAT?

A. El número de llamadas manejadas por un router NAT es contingente en la cantidad de memoria disponible en el cuadro y la potencia de procesamiento del CPU.

Q. ¿Un router NAT soporta la segmentación TCP de flaco y de los paquetes H323?

A. Segmentación del soporte TCP IOS-NAT para el H323 en el Mainline 12.4 y el soporte de la segmentación TCP para FLACO de 12.4(6)T hacia adelante.

Q. ¿Hay advertencias a tener cuidado para al usar una configuración de la sobrecarga NAT en un despliegue de la Voz?

A. Sí. Cuando usted tiene el configs de la sobrecarga NAT y un despliegue de la Voz, usted necesita el mensaje de inscripción pasar con el NAT y crear una asociación para que el out->in alcance este dispositivo interno. El dispositivo interno envía este registro en una moda periódica y el NAT pone al día este agujerito/asociación de la información como en el mensaje de señalización.

Q. ¿Hay problemas conocidos causados publicando el transporte nacional del IP claro * ordene o el comando forzado transporte nacional del IP claro en un despliegue de la Voz?

A. En las implementaciones de la Voz cuando usted isssue un **transporte nacional del IP claro *** ordene o un comando **forzado transporte nacional del IP claro** y tenga NAT dinámico, usted limpiará hacia fuera el agujerito/la asociación y debe esperar el ciclo siguiente del registro del dispositivo interno a re-establish esto. Cisco recomienda que usted no utiliza estos comandos clear en un despliegue de la Voz.

Q. ¿El soporte NAT expresa la solución colocalizada?

A. No. La solución colocalizada no se soporta actualmente. El despliegue siguiente con el NAT (en el mismo cuadro) se considera una solución colocalizada: CME/DSP-Farm/SCCP/H323.

Q. ¿NVI soporta ALG flaco, el SORBO ALG H323 ALG, y TCP?

A. No. Observe que el SORBO ALG UDP (usado por la mayoría de las implementaciones) no está afectado.

NAT con VRF/MPLS

Q. ¿Un router NAT soportará nunca NATting el mismo espacio de la dirección en un VRF que está siendo NATted en un espacio de dirección global? Actualmente, recibo esta advertencia: *"% de la Entrada estática similar (1.1.1.1 ---> 22.2.2.2) existe ya"* cuando intento configurar el siguiente: `72UUT(config)#ip nat inside source`

```
static 1.1.1.1 22.2.2.2 72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED
```

A. Soportes de la herencia NAT overloapping los config del direccionamiento sobre diversos VRF. Usted tendría que configurar solapar en la regla con la opción coincidencia-en-*VRF* y configurar el **interior nacional del IP/afuera** en el mismo VRF para el tráfico sobre ese VRF específico. El soporte que solapa no incluye la tabla de Global Routing.

Usted debe agregar la palabra clave coincidencia-en-*VRF* para las entradas NAT estáticas VRF que solapan para diversos VRF. Sin embargo, no es posible solapar los direccionamientos globales y del vrf NAT.

```
72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf 72UUT(config)#ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf
```

Q. ¿La herencia NAT soporta VRF-Lite (NATting de un VRF a un diverso VRF)?

A. No. Usted debe utilizar NVI para NATting entre diversos VRF. Usted puede utilizar la herencia NAT para hacer el NAT del VRF a global o el NAT dentro del mismo VRF.

NAT NVI

Q. ¿Cuál es NAT NVI?

A. Interfaz virtual de la significa NAT NVI. Permite que el NAT traduzca entre dos diversos VRF. Esta solución se debe utilizar en lugar de la traducción de dirección de red en un solo sentido.

Q. ¿Se debe el NAT NVI utilizar cuando NATting entre una interfaz en global y una interfaz en un VRF?

A. Cisco recomienda que usted utiliza la herencia NAT para el VRF a NAT global (interior nacional del IP/hacia fuera) y entre las interfaces en el mismo VRF. NVI se utiliza para el NAT entre diversos VRF.

Q. ¿La segmentación TCP para NAT-NVI se soporta?

A. No hay soporte para la segmentación TCP para NAT-NVI.

Q. ¿NVI soporta ALG flaco, el SORBO ALG H323 ALG, y TCP?

A. No. Observe que el SORBO ALG UDP (usado por la mayoría de las implementaciones) no está afectado.

Q. ¿Hace la segmentación TCP soportada con el SNAT?

A. El SNAT no soporta ningún TCP ALGs (por ejemplo, SORBO, FLACO, H323, o DNS). Por lo tanto, la segmentación TCP no se soporta. Sin embargo, se soportan el SORBO UDP y el DNS.

SNAT

Q. ¿Cuál es NAT stateful (SNAT)?

A. El SNAT permite que dos o más traductores de dirección de red funcionen como un grupo de la traducción. Un miembro del grupo de la traducción maneja el tráfico que requiere la traducción de información de la dirección IP. Además, informa al traductor de reserva los flujos activos mientras que ocurren. El traductor de reserva puede entonces utilizar la información del traductor activo para preparar las entradas de la tabla de traducción duplicados. Por lo tanto, si a una falla crítica obstaculiza al traductor activo, el tráfico se puede conmutar rápidamente al respaldo. El flujo de tráfico continúa puesto que se utilizan las mismas traducciones de dirección de red y el estado de esas traducciones se ha definido previamente. Refiera a la elasticidad del IP mejorado usando Cisco NAT stateful para más información.

Q. ¿La segmentación TCP se soporta con el SNAT?

A. El SNAT no soporta ningún TCP ALGs (por ejemplo, SORBO, FLACO, H323, o DNS). Por lo tanto, la segmentación TCP no se soporta. Sin embargo, se soportan el SORBO UDP y el DNS.

Q. ¿Está el soporte SNAT para la encaminamiento asymetric?

A. Soportes de ruteo NAT del Asymetric habilitando como Datos en espera. Por abandono, la como-espera es permiso. Sin embargo, de 12.4(24)T hacia adelante, los como-Datos en espera se soportan no más. Los clientes deben aseegurarse los paquetes se rutean correctamente y el retardo apropiado se agrega para que el Asymmetric Routing trabaje correctamente.

NAT-PT (v6 a v4)

Q. ¿Cuál es NAT-PT?

A. El NAT-PT es v4 a la traducción v6 para el NAT. La Traducción de protocolo (NAT-PT) es un mecanismo de la traducción IPv6-IPv4, según lo definido en el RFC 2765 y el RFC 2766 , permitiendo que los dispositivos IPv6-only comuniquen con los dispositivos IPv4-only y vice versa. Refiera a implementar el NAT-PT para el IPv6 para más información sobre esta característica

Q. ¿El NAT-PT se soporta en la trayectoria del Cisco Express Forwarding (CEF)?

A. El NAT-PT no se soporta en la trayectoria CEF.

Q. ¿Qué ALGs se soporta en el NAT-PT?

A. Soportes TFTP/FTP y DNS del NAT-PT. No hay soporte para la Voz y el SNAT en el NAT-PT.

Q. ¿El ASR 1004 soporta el NAT-PT?

A. El Routers de los servicios de la agregación (ASR) utiliza NAT64. Para más información sobre configurar NAT64, refiera a configurar una red de la encaminamiento para NAT64 apátrida.

Dependiente de la plataforma Cisco 7300/7600/6k

Q. ¿Está el NAT stateful (SNAT) disponible en el Catalyst 6500 en el tren SX?

A. El SNAT no está disponible en el Catalyst 6500 en el tren SX.

Q. ¿El NAT que reconoce VRF se soporta en hardware en el 6k?

A. El NAT que reconoce VRF no se soporta en hardware en esta plataforma.

Q. ¿Los 7600 y el Cat6000 soportan el NAT que reconoce VRF?

A. En la plataforma 65xx/76xx, el NAT que reconoce VRF no se soporta, y se bloquean los CLI.

Nota: Usted puede implementar un diseño leveraging un FWSM que se ejecute en el modo transparente virtual del contexto.

Dependiente de la plataforma Cisco 850

Q. ¿Cisco 850 soporta NAT flaco ALG en la versión 12.4T?

A. No. No hay soporte para NAT flaco ALG en 12.4T en las 850 Series.

Despliegue NAT

Q. ¿Cómo implemento el NAT?

A. El NAT permite al internetworks del IP privado esos IP Addresses nonregistered del uso para conectar con Internet. El NAT traduce el direccionamiento privado (del RFC1918) en la red interna a las direcciones enrutables legales antes de que los paquetes se remitan sobre otra red.

Para más información sobre implementar el NAT, refiera a configurar el NAT para la conservación de IP Address.

Q. ¿Cómo implemento el NAT con la Voz?

A. El soporte NAT para las características de la voz permite los mensajes integrados SORBO que pasan a través de un router configurado con el Network Address Translation (NAT) que se traducirán de nuevo al paquete. Un gateway de capa de aplicación (ALG) se utiliza con el NAT para traducir los paquetes de voz.

Para más información sobre implementar el NAT con la Voz, refiera al soporte NAT para ALGs.

Q. ¿Cómo hace la integración NAT I con el MPLS VPNs?

A. La integración NAT con la característica del MPLS VPNs permite que el MPLS VPNs múltiple sea configurado en un único dispositivo para trabajar junta. El NAT puede distinguir de qué MPLS VPN recibe el tráfico IP incluso si el MPLS VPNS todo utiliza el mismo esquema de IP Addressing. Esta mejora permite a los clientes múltiples del MPLS VPN para compartir los servicios mientras que se asegura de que cada MPLS VPN está totalmente a parte del otro.

Q. ¿La correlación estática NAT soporta el HSRP para la Alta disponibilidad?

A. Cuando una interrogación del Address Resolution Protocol (ARP) se acciona para un direccionamiento que se configure con la correlación estática del Network Address Translation (NAT) y sea poseído por el router, el NAT responde con la dirección MAC BIA en la interfaz a la cual el ARP está señalando. Dos Routers actúa como HSRP activo y espera. Sus interfaces interiores NAT se deben habilitar y configurar para pertenecer a un grupo.

Q. ¿Cómo hace el implemet NAT NVI I?

A. La característica de la interfaz virtual NAT (NVI) quita el requisito de configurar una interfaz como el NAT interior o NAT afuera. Para más información sobre NAT NVI, refiera a configurar la interfaz virtual NAT.

Q. ¿Cómo implemento el Equilibrio de carga con el NAT?

A. Hay dos clases de Equilibrio de carga que se pueden hacer con el NAT: usted puede cargar la balanza entrante a un conjunto de los servidores para distribuir la carga en los servidores, y usted puede cargar la balanza su tráfico de usuarios a Internet sobre dos o más ISP.

Para más información sobre el Equilibrio de carga entrante, refiera a evitar la sobrecarga del servidor usando el Equilibrio de carga TCP.

Para más información sobre la carga saliente que equilibra, refiera al balanceo de carga IOS NAT para dos Conexiones ISP.

Q. ¿Cómo implemento el NAT en el conjucntion con el IPSec?

A. Hay soporte para el Encapsulating Security Payload (ESP) de la seguridad IP (IPSec) a través de NAT y de Transparencia IPSec NAT.

El IPSec ESP a través de la función NAT proporciona la capacidad de soportar los túneles o las conexiones simultáneos múltiples del IPSec ESP a través de un dispositivo NAT del Cisco IOS configurado en la sobrecarga o el modo del Port Address Translation (PAT).

La característica de la Transparencia IPSec NAT introduce el soporte para que el tráfico IPSec viaje a través de las puntas NAT o de la PALMADITA en la red dirigiendo muchas incompatibilidades sabidas entre el NAT y el IPSec.

Q. ¿Cómo implemento el NAT-PT?

A. El NAT-PT (Traducción del protocolo de traducción de dirección de red) es un mecanismo de la traducción IPv6-IPv4, según lo definido en el RFC 2765 y el RFC 2766 , que permite que los dispositivos IPv6-only comuniquen con los dispositivos IPv4-only y vice versa.

Para más información sobre implementar y configurar el NAT-PT, refiera a implementar el NAT-PT para el IPv6.

Q. ¿Cómo implemento el Multicast NAT?

A. Es posible al NAT el IP de la fuente para una secuencia de multidifusión. Un route-map no puede ser utilizado al hacer el NAT dinámico para el Multicast, sólo una lista de acceso se soporta para esto.

Para más información, refiérase a cómo hace el trabajo del Multicast NAT sobre los routeres Cisco. El grupo de la multidifusión de destino es NATted usando una solución de la reflexión del servicio de multidifusión.

Q. ¿Cómo implemento NAT stateful (SNAT)?

A. El SNAT habilita el servicio continuo para las sesiones de NAT dinámicamente asociadas. Las sesiones que se definen estáticamente reciben la ventaja de la Redundancia sin la necesidad del SNAT. En ausencia del SNAT, las sesiones que utilizan las asignaciones dinámicas NAT serían separadas en caso de falla crítica y tendrían que ser restablecidas. Solamente se soporta la configuración mínima SNAT. Las implementaciones futuras deben ser realizadas solamente después que hablan con su equipo de cuenta de Cisco para validar las restricciones actuales en relación con del diseño.

El SNAT se recomienda para los escenarios siguientes:

- Modo del HSRP según lo descrito en el White Paper SNAT: Elasticidad del IP mejorado usando Cisco NAT stateful.
- Primario/respaldo no es un modo recomendado puesto que hay falta de algunas características comparada al HSRP.
- Para fracaso-sobre los escenarios y para la configuración 2-router. Es decir, si los desperfectos del router uno, el otro router asumen el control el seamlessly. (La arquitectura SNAT no se diseña para manejar las Interfaz-aletas.)
- se soporta el escenario NON-asimétrico de la encaminamiento. El Asymmetric Routing se puede manejar solamente si el tiempo de espera en el paquete de respuesta es más alto que eso entre 2 Routers SNAT para intercambiar los mensajes SNAT.

La arquitectura SNAT no se diseña actualmente para manejar la robustez; por lo tanto, no se espera que estas pruebas tengan éxito:

- Borrar las entradas de NAT mientras que hay tráfico.
- Cambio de los parámetros de la interfaz (como el cambio de la dirección IP, el shut/no shut, el etc.) mientras que hay tráfico.
- No se espera que **claros** específicos o a los **comandos show** SNAT ejecuten correctamente y no recomendado.Algo del SNAT se relacionó **claramente** y los **comandos show** son como sigue:
  clear ip snat sessions * clear ip snat sessions <ip address of the peer> clear ip snat translation distributed * clear ip snat translation peer < IP address of SNAT peer> sh ip snat distributed verbose sh ip snat peer < IP address of peer>
- Si el usuario quiere borrar las entradas, el **transporte nacional del IP forzado** o **claro transporte nacional del IP claro * los** comandos puede ser utilizado.Si el usuario quiere ver las entradas, **mostrar a IP la traducción nacional**, **mostrar IP las traducciones nacionales prolijas**, y a **IP de la demostración los** comandos **nacionales stats** pueden ser utilizados. Si el *servicio interno* se configura, mostrará a SNAT la información específica también.
- Borrar las traducciones de NAT en el router de reserva no se recomienda. Siempre claro las entradas de NAT en el router primario SNAT.
- El SNAT no es HA; por lo tanto, las configuraciones en ambo Routers deben ser lo mismo.

Ambo Routers debe tener el mismo funcionamiento de la imagen. También aseegurese que la plataforma subyacente usada para ambo el Routers SNAT es lo mismo.

Mejores prácticas NAT

Q. ¿Hay mejores prácticas NAT?

A. Sí. Éstas son las mejores prácticas NAT:

1. Cuando el usar dinámico y NAT estática, el ACL que fija la regla para el NAT dinámico debe excluir los host locales estáticos tan no hay coincidencia.
2. Guárdese de usar el ACL para el NAT con el **IP del permiso cualquier** como usted puede conseguir los resultados no predecibles. Después de que 12.4(20)T NAT traduzca el HSRP y los paquetes del Routing Protocol localmente generados si él se envía la interfaz exterior, así como localmente los paquetes encriptados que corresponden con la regla NAT.
3. Cuando usted tiene redes superpuestas para el NAT, utilice la palabra clave coincidencia-en-**VRF**.Usted debe agregar la palabra clave coincidencia-en-**VRF** para las entradas NAT estáticas VRF que solapan para diversos VRF, pero no es posible solapar los direccionamientos globales y del vrf NAT.`Router(config)#`**`ip nat inside source static 1.1.1.1 22.2.2.2 vrf RED match-in-vrf`** `Router(config)#`**`ip nat inside source static 1.1.1.1 22.2.2.2 vrf BLUE match-in-vrf`**
4. Los agrupamientos NAT con el mismo intervalo de direcciones no pueden ser utilizados en diversos VRF a menos que se utilice la palabra clave coincidencia-en-**VRF**.Por ejemplo: **`ip nat pool poolA 171.1.1.1 171.1.1.10 prefix-length 24 ip nat pool poolB 171.1.1.1 171.1.1.10 prefix-length 24 ip nat inside source list 1 poolA vrf A match-in-vrf ip nat inside source list 2 poolB vrf B match-in-vrf`** **Nota:** Wven aunque la configuración CLI es válida, sin la palabra clave coincidencia-en-**VRF la** configuración no se soporta.
5. Al desplegar el Equilibrio de carga ISP con la sobrecarga de la interfaz NAT, la mejor práctica es utilizar el route-map con la coincidencia de la interfaz sobre corresponder con ACL.
6. Al usar el pool que asocia, usted no debe utilizar diversa asignación dos (ACL o route-map) para compartir el mismo direccionamiento del agrupamiento NAT.
7. Al desplegar el mismo NAT gobierna en dos diverso Routers en el escenario de falla, usted debe utilizar la Redundancia del HSRP.
8. No defina la misma dirección global interna en el NAT estático y a una agrupación dinámica. Esta acción puede llevar a los resultados no deseables.

Información Relacionada

- Soporte de tecnología del Routing IP
- Soporte Técnico y Documentación - Cisco Systems