Comprensión de NAT para Habilitar la Comunicación Par-a-Par en Routers IOS e IOS XE

Contenido

Introducción

Este documento describe la necesidad de Utilidades transversales de sesión para servidores NAT (STUN), los tipos de configuraciones de Traducción de direcciones de red (NAT) con respecto a los servidores STUN, cómo NAT causa un problema en esta configuración y la solución.

Antecedentes

El objetivo principal de los dispositivos NAT es permitir que los dispositivos con direcciones IP privadas en una red de área local (LAN) se comuniquen con los dispositivos en espacios de direcciones públicas, como Internet. Sin embargo, aunque se supone que los dispositivos NAT permiten que los hosts internos se conecten con el espacio público, cuando se trata de aplicaciones punto a punto (P2P) como VoIP, juegos, WebRTC y uso compartido de archivos en las que los usuarios finales deben actuar como cliente y servidor para mantener una comunicación bidireccional de extremo a extremo, NAT ofrece dificultades para establecer esas conexiones UDP. Las técnicas transversales NAT suelen ser necesarias para que estas aplicaciones funcionen.

Necesidad de NAT Traversal

Comunicación de voz y vídeo en tiempo real en Internet son corriente principal hoy en día, con varias aplicaciones de mensajería instantánea (IM) populares que admiten llamadas VoIP. Un gran obstáculo en la adopción inicial de VoIP fue el hecho de que la mayoría de los PC u otros dispositivos se sientan detrás de firewalls y utilizan direcciones IP privadas. Un firewall asigna varias direcciones privadas (dirección IP y puerto) de la red a una única dirección pública con NAT. Pero el dispositivo final no conoce su dirección pública y, por lo tanto, no puede recibir tráfico de voz de la parte remota en la dirección privada que anuncia en su comunicación VoIP.

Unilateral Los procesos de corrección de direcciones propias (UNSAF) son procesos en los que algunos terminales de origen intentan determinar o corregir la dirección (y el puerto) por los que

otro terminal conoce la dirección (por ejemplo, para poder uUtilice los datos de dirección en el intercambio de protocolos o para anunciar una dirección pública desde la cual recibe conexiones.

Por lo tanto, las conexiones P2P que se están debatiendo son procesos de la UNSAF. Una forma habitual en que las aplicaciones P2P establecen sesiones de iguales y permanecen NAT-friendly es cuando utilizan un servidor de encuentro de dirección pública para fines de registro y detección de pares.

Utilidades transversales de sesión para NAT

Según RFC 5389, STUN proporciona una herramienta que se ocupa de las NAT. Proporciona un medio para que un terminal determine la dirección IP y el puerto asignados por un dispositivo NAT que corresponde a su puerto y dirección IP privada. También proporciona una manera para que un punto final mantenga activo un enlace NAT.

Tipos de Implementaciones de NAT

Se ha observado que el tratamiento NAT de UDP varía entre implementaciones. Los cuatro tratamientos observados en las implementaciones son:

Cono completo: un NAT de cono completo es uno en el que todas las solicitudes de la misma dirección IP interna y puerto se mapean a la misma dirección IP externa y puerto. Además, cualquier host externo puede enviar un paquete al host interno y envía un paquete a la dirección externa asignada.

Cono Restringido: Una NAT de cono restringido es aquella en la que todas las solicitudes de la misma dirección IP interna y puerto se asignan a la misma dirección IP externa y puerto. A diferencia de una NAT de cono completo, un host externo (con dirección IP X) puede enviar un paquete al host interno sólo si el host interno había enviado previamente un paquete a la dirección IP X.

Cono restringido de puerto: una NAT de cono restringido de puerto es como una NAT de cono restringido, pero la restricción incluye números de puerto. Específicamente, un host externo puede enviar un paquete, con la dirección IP de origen X y el puerto de origen P, al host interno sólo si el host interno había enviado previamente un paquete a la dirección IP X y al puerto P.

Simétrico: una NAT simétrica es aquella en la que todas las solicitudes de la misma dirección IP interna y del mismo puerto a una dirección IP de destino específica y a un puerto, se asignan a la misma dirección IP externa y al mismo puerto. Si el mismo host envía un paquete con la misma dirección de origen y puerto, pero a un destino diferente, se utiliza una asignación diferente. Además, sólo el host externo que recibe un paquete puede enviar un paquete UDP de vuelta al host interno.

Considere una topología en la que el origen (A, Pa) (donde A es la dirección IP y Pa es el puerto de origen) se comunica con el destino (B, Pb) y (C, PC) a través de un dispositivo NAT.

Tipo de implementación de NAT	Público origen cuando destinado a (B, Pb)	Origen público cuando está destinado a (C, Pc)	Puede destino (por ejemplo: (B, Pb)) enviar tráfico a (A, Pa)?
Cono completo	(X1,Px1)	(X1,Px1)	Yes
Cono Restringido	(X1,Px1)	(X1,Px1)	Sólo si (A, Pa) había enviado primero el tráfico a B

Cono restringido de puerto	(X1,Px1)	(X1,Px1)	Sólo si (A, Pa) había enviado primero el tráfico a (B, Pb)
Simétrico	(X1,Px1)	(X2,Px2)	Sólo si (A, Pa) había enviado primero el tráfico a (B, Pb)

Problemas con NAT transversal y NAT simétrica

Los servidores STUN responden a las solicitudes de enlace STUN enviadas por los clientes STUN y proporcionan la IP/puerto público del cliente. Ahora, esta dirección/puerto es utilizada por el cliente STUN en su comunicación peer-to-peer señalización. Sin embargo, ahora que el endhost utiliza la misma dirección/puerto privado (supongamos que límite a la IP/puerto público proporcionado en la respuesta STUN) el dispositivo NAT lo traduce a la misma IP pero a un puerto diferente si NAT simétrica sencilloyoanotación se utiliza. Esto interrumpe la comunicación UDP porque el señalización había establecido la conexión basada en la ppuerto anterior.

Cisco IOS® routers' NAT sencilloyoanotación cuando realiza PAT es simétrico por defecto. Allíedelantero, se espera que vea problemas de conexión UDP con estos routers que realizan NAT.

Sin embargo, la implementación NAT de los routers Cisco IOS-XE cuando realizan PAT no es simétrica. Cuando envía dos mensajes diferentes transmite con la misma IP de origen y el mismo puerto, pero a diferentes destinos, el origen se NATED a la misma IP global interna y al mismo puerto.

La solución al problema

A partir de esta descripción, está claro que la problema se puede resolver si realiza Independiente del terminal mapeo.

Según RCFC 4787: Con Asignación independiente del terminal (EIM), la NAT reutiliza la asignación de puertos para los paquetes posteriores enviados desde la misma dirección IP interna y el mismo puerto (X:x) a cualquier puerto y dirección IP externos.

Desde un cliente, cuando el endhost ejecuta los comandos **nc -p 23456 10.0.0.4 40000** y **nc -p 23456 10.0.0.5 5000**, en dos ventanas de terminal diferentes, aquí están los resultados de las traducciones NAT si utiliza EIM:

```
Pro Inside global       Inside local            Outside local       Outside global

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.4:40000 10.0.0.4:40000

tcp 10.0.0.1:23456   192.168.0.2:23456  10.0.0.5:50000 10.0.0.5:50000
```

Aquí puede ver que diferentes flujos de tráfico que tienen la misma dirección de origen y el mismo puerto se traducen a la misma dirección/puerto independientemente del puerto/dirección de destino.

En los routers Cisco IOS, puede habilitar la Asignación de puertos independiente del terminal con el comando **ip nat service enable-sym-puerto.**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-

book/iadnat-fpg-port-alloc.html

Summary

La implementación NAT de Cisco IOS es simétrica de forma predeterminada cuando se utiliza la Traducción de direcciones de puerto (PAT) y puede causar problemas cuando pasa el tráfico UDP P2P que requiere servidores como STUN para NAT traversal. Debe configurar explícitamente EIM en el dispositivo NAT para que esto funcione.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).