Comprender el orden de funcionamiento de NAT

Contenido

Introducción

Este documento describe que el orden en que se procesan las transacciones con NAT se basa en la dirección que un paquete viaja dentro o fuera de la red.

Prerequisites

Requirements

Cisco le recomienda que tenga conocimiento acerca de este tema:

- Traducción de direcciones de red (NAT, Network Address Translation). Para obtener más información sobre NAT, consulte Cómo funciona NAT.

Componentes Utilizados

La información de este documento se basa en la versión 12.2(27) del software del IOS® de Cisco.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

Este documento describe que el orden en que se procesan las transacciones con la Traducción

de direcciones de red (NAT) se basa en si un paquete va de la red interna a la red externa, o de la red externa a la red interna.

Descripción general de NAT

En esta tabla, cuando NAT realiza la traducción de global a local, o de local a global, la traducción es diferente en cada flujo.

De adentro hacia afuera

- Si IPSec, verifique la lista de acceso de entrada
- descifrado: para CET (Cisco Encryption Technology) o IPSec
- verificar lista de acceso de entrada
- revise los límites de velocidad de entrada
- contabilidad de entrada
- redirección al caché de la Web
- ruteo de política
- ruteo
- **NAT de adentro hacia afuera (traducción local a global)**
- crypto (mapa de control y marca para el encripción)
- control de lista de accesos de salida
- Inspeccionar (control de acceso basado en contexto (CBAC))
- Intercepción TCP
- cifrado
- cola

De afuera hacia adentro

- Si IPSec, verifique la lista de acceso de ent
- descifrado: para CET o IPSec
- verificar lista de acceso de entrada
- revise los límites de velocidad de entrada
- contabilidad de entrada
- redirección al caché de la Web
- **NAT de afuera hacia adentro (traducción de global a local)**
- ruteo de política
- ruteo
- crypto (mapa de control y marca para el encripción)
- control de lista de accesos de salida
- inspeccionar CBAC
- Intercepción TCP
- cifrado
- cola

Configuración y resultado de NAT

Este ejemplo demuestra cómo el orden de las operaciones puede afectar a NAT. En este caso, sólo se muestran NAT y ruteo.

En el ejemplo anterior, el Router-A está configurado para traducir la dirección local interna 172.31.200.48 a 172.16.47.150, como se muestra en esta configuración.

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
enable password ww
!
ip nat inside source static 172.31.200.48 172.16.47.150

!--- This command creates a static NAT translation
!--- between 172.31.200.48 and 172.16.47.150 ip domain-name cisco.com ip name-server
172.31.2.132 ! interface Ethernet0 no ip address shutdown ! interface Serial0 ip address
172.16.47.161 255.255.255.240 ip nat inside
```

```
!--- Configures Serial0 as the NAT inside interface no ip mroute-cache no ip route-cache no
fair-queue ! interface Serial1 ip address 172.16.47.146 255.255.255.240 ip nat outside

!--- Configures Serial1 as the NAT outside interface no ip mroute-cache no ip route-cache ! no
ip classless ip route 0.0.0.0 0.0.0.0 172.16.47.145

!--- Configures a default route to 172.16.47.145 ip route 172.31.200.0 255.255.255.0
172.16.47.162 ! ! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww login ! end
```

La tabla de traducción indica que existe la traducción deseada.

```
Router-A#show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

Esta salida se toma del Router-A con **debug ip packet detail** y **debug ip nat** habilitados, y un ping emitido desde el dispositivo 172.31.200.48 destinado a 172.16.47.142.

> **Nota**: Los comandos de depuración generan una cantidad significativa de resultados. Utilícelos sólo cuando el tráfico en la red del IP es lento, con el fin de que no se vea afectada negativamente otra actividad del sistema. Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.

```
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.31.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=172.31.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
```

Dado que no hay mensajes de depuración NAT en la salida anterior, no se utiliza la traducción estática actual y que el router no tiene una ruta para la dirección de destino (172.16.47.142) en su tabla de ruteo. El resultado del paquete no enrutable es un mensaje inalcanzable de ICMP, que se envía al dispositivo interno.

Sin embargo, el Router-A tiene una ruta predeterminada de 172.16.47.145, así que ¿por qué se considera que la ruta no es enrutable?

El Router-A **no** tiene **ninguna ip sin clase** configurada, lo que significa que si un paquete destinado a una dirección de red "principal" (en este caso, 172.16.0.0) para la cual existen subredes en la tabla de ruteo, el router no depende de la ruta predeterminada. En otras palabras, si ejecuta el comando **no ip classless**, esto desactiva la capacidad del router para buscar la ruta con la coincidencia de bit más larga. Para cambiar este comportamiento, debe configurar **ip classless** en el Router-A. El comando **ip classless** se habilita de forma predeterminada en los routers Cisco con Cisco IOS Software Releases 11.3 y versiones posteriores.

```
Router-A#configure terminal
Enter configuration commands, one per line.  End with CTRL/Z.
Router-A(config)#ip classless
Router-A(config)#end

Router-A#show ip nat translation
%SYS-5-CONFIG_I: Configured from console by console nat tr
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.150      172.31.200.48      ---                ---
```

Cuando repite la misma prueba de ping que hizo anteriormente, verá que el paquete se traduce y el ping es exitoso.

```
Ping Response on device 172.31.200.48

D:\>ping 172.16.47.142
Pinging 172.16.47.142 with 32 bytes of data:

Reply from 172.16.47.142: bytes=32 time=10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255
Reply from 172.16.47.142: bytes=32 time<10ms TTL=255

Ping statistics for 172.16.47.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0%)
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum =  10ms, Average =  2ms

Debug messages on Router A indicating that the packets generated by device
172.31.200.48 are getting translated by NAT.

Router-A#
*Mar 28 03:34:28: IP: tableid=0, s=172.31.200.48 (Serial0), d=172.16.47.142
(Serial1), routed via RIB
*Mar 28 03:34:28: NAT: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [160]
*Mar 28 03:34:28: IP: s=172.16.47.150 (Serial0), d=172.16.47.142 (Serial1),
 g=172.16.47.145, len 100, forward
*Mar 28 03:34:28: ICMP type=8, code=0
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [160]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [161]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [161]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [162]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [162]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [163]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [163]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
```

```
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0
*Mar 28 03:34:28: NAT*: s=172.31.200.48->172.16.47.150, d=172.16.47.142 [164]
*Mar 28 03:34:28: NAT*: s=172.16.47.142, d=172.16.47.150->172.31.200.48 [164]
*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=172.31.200.48
(Serial0), routed via RIB
*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=172.31.200.48 (Serial0),
g=172.16.47.162, len 100, forward
*Mar 28 03:34:28: ICMP type=0, code=0

Router-A#undebug all
All possible debugging has been turned off
```

El ejemplo anterior muestra que cuando un paquete atraviesa de adentro hacia afuera, un router NAT verifica su tabla de ruteo para una ruta a la dirección externa antes de continuar traduciendo el paquete. Por lo tanto, es importante que el router NAT tenga una ruta válida para la red externa. La ruta a la red de destino debe conocerse a través de una interfaz definida como NAT externa en la configuración del router.

Es importante tener en cuenta que los paquetes de retorno se traducen antes de enrutarse. Por lo tanto, el router NAT también debe tener una ruta válida para la dirección local interna en su tabla de ruteo.

Información Relacionada

- Configuración de Network Address Translation
- Verificación del funcionamiento de NAT y resolución de problemas básicos de NAT
- NAT: definiciones locales y globales
- ¿Cómo Funciona Multicast NAT en los Routers de Cisco?
- Página de Soporte de NAT
- Asistencia técnica y descargas de Cisco

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).