De NAT-werkingsvolgorde begrijpen

Inhoud

Inleiding

Dit document beschrijft dat de ordertransacties worden verwerkt met NAT is gebaseerd op de richting waarin een pakket binnen of buiten het netwerk reist.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met dit onderwerp:

- in Cisco IOS®. Voor meer informatie over NAT, zie Hoe NAT werkt.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco IOS®-softwarerelease 12.2(27)S.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Conventies

Raadpleeg Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.

Achtergrondinformatie

Dit document beschrijft dat de volgorde waarin transacties met Network Address Translation (NAT) worden verwerkt, is gebaseerd op de vraag of een pakket van het binnennetwerk naar het

buitennetwerk of van het buitennetwerk naar het binnennetwerk gaat.

Overzicht van NAT

In deze tabel is wanneer NAT de wereldwijde naar lokale of lokale naar wereldwijde vertalingen uitvoert, de vertaling in elke stroom anders.

van binnen naar buiten	van buiten naar binnen
• Als IPSec vervolgens de invoertoegangslijst controleert • decryptie - voor CET (Cisco Encryption Technology) of IPSec • controle van invoertoegangslijst • controle van de invoersnelheidslimieten • inputboekhouding • doorsturen naar web cache • beleidsrouting • routing • **NAT binnen en buiten (lokale naar wereldwijde vertaling)** • crypto (controlekaart en teken voor encryptie) • toegangslijst voor uitvoer controleren • inspecteren (op context gebaseerde toegangscontrole (CBAC)) • TCP-onderschepping • encryptie • rij	• Als IPSec vervolgens de invoertoegangslij controleert • decryptie - voor CET of IPSec • controle van invoertoegangslijst • controle van de invoersnelheidslimieten • inputboekhouding • doorsturen naar web cache • **NAT buiten en binnen (wereldwijde naar lo vertaling)** • beleidsrouting • routing • crypto (controlekaart en teken voor encryp • toegangslijst voor uitvoer controleren • CBAC inspecteren • TCP-onderschepping • encryptie • rij

NAT-configuratie en -uitvoer

Dit voorbeeld toont aan hoe de orde van verrichtingen NAT kan uitvoeren. In dit geval worden alleen NAT en routing weergegeven.

In het vorige voorbeeld is router-A geconfigureerd om het lokale adres 172.31.200.48 naar 172.16.47.150 te vertalen, zoals in deze configuratie wordt getoond.

```
!
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
```

De vertaaltabel geeft aan dat de beoogde vertaling bestaat.

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

Deze output wordt genomen van router-A met **debug ip pakketdetail** en **debug ip nationaal** toegelaten, en pingelt uitgegeven van apparaat 172.31.200.48 dat voor 172.16.47.142 wordt bestemd.

> **Opmerking**: Debug commando's genereren een aanzienlijke hoeveelheid output. Gebruik ze alleen als er weinig verkeer op het IP-netwerk is, zodat andere activiteit op het systeem niet nadelig wordt beïnvloed. Voordat u debug-opdrachten uitgeeft, raadpleegt u Belangrijke informatie over debug-opdrachten.

```
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
```

Aangezien er geen NAT debug berichten in de vorige output zijn, wordt de huidige statische vertaling niet gebruikt, en dat de router geen route voor het bestemmingsadres (172.16.47.142) in zijn routeringstabel heeft. Het resultaat van het niet-routable pakket is een Onbereikbaar bericht ICMP , dat naar het binnenapparaat wordt verzonden.

Maar router-A heeft een standaardroute van 172.16.47.145, dus waarom wordt de route beschouwd als niet routable?

Router-A heeft **geen klasseloze IP-**configuratie, wat betekent dat als een pakket bestemd voor een "groot" netwerkadres (in dit geval 172.16.0.0) waarvoor subnetten in de routeringstabel bestaan, de router niet op de standaardroute vertrouwt. Met andere woorden, als u het **geen ip klasseloze** bevel uitgeeft, schakelt dit de capaciteit van de router uit om de route met de langste beetjekaart te zoeken. Om dit gedrag te veranderen moet u **IP klasseloos** op router-A vormen. De opdracht **klasseloze IP**-routing is standaard ingeschakeld op Cisco-routers met Cisco IOS-softwarereleases 11.3 en hoger.

```
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      ---                ---
```

Wanneer u de zelfde ping test herhaalt zoals eerder gedaan, ziet u dat het pakket vertaald wordt en ping succesvol is.

```
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
```

Het vorige voorbeeld toont aan dat wanneer een pakket binnen aan buitenkant oversteekt, een NAT router zijn routerlijst een route aan het buitenadres controleert alvorens het pakket blijft vertalen. Daarom is het belangrijk dat de NAT router een geldige route voor het buitennetwerk heeft. De route naar het doelnetwerk moet bekend zijn door een interface die buiten in de routerconfiguratie als NAT is gedefinieerd.

Het is belangrijk om op te merken dat de retourpakketten worden vertaald voordat ze worden verstuurd. Daarom moet de NAT router ook een geldige route voor het Binnen lokale adres in zijn routeringstabel hebben.

Gerelateerde informatie

- Netwerkadresomzetting configureren
- NAT-werking verifiëren en eenvoudige NAT-troubleshooting
- NAT: lokale en wereldwijde definities
- Hoe werkt Multicast NAT op Cisco-routers?
- Ondersteuningspagina voor NAT
- Cisco technische ondersteuning en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.