Ordre des opérations NAT

Contenu

Introduction

Ce document montre que l'ordre dans lequel les transactions sont traitées à l'aide de la traduction d'adresses réseau (NAT) est basé sur le fait qu'un paquet va du réseau interne vers le réseau externe, ou du réseau externe vers le réseau interne.

Conditions préalables

Conditions requises

Les lecteurs de ce document doivent avoir des connaissances sur le sujet suivant :

- Traduction d'adresses réseau (NAT). Pour plus d'informations sur NAT, consultez Comment fonctionne NAT.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Remarque: Les informations de ce document sont basées sur le logiciel Cisco IOS® Version 12.2(27)

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Présentation de NAT

Dans ce tableau, quand NAT s'effectue de global en local, ou de local en global, la traduction est différente dans chaque flux.

De l'intérieur vers l'extérieur	De l'extérieur vers l'intérieur
• Si IPSec, contrôler la liste d'accès en entrée • Déchiffrement - pour CET (technologie de chiffrement Cisco) ou IPSec • contrôler la liste d'accès en entrée • contrôler les limites du débit en entrée • suivi en entrée • rediriger vers le cache Web • routage de stratégie • acheminement • **NAT de l'intérieur vers l'extérieur (traduction de local en global)** • chiffrement (vérifier le mappage et marquer pour le chiffrement) • contrôler la liste d'accès en sortie • inspecter (Contrôle d'accès basé sur contexte (CBAC)) • Interception TCP • cryptage • Queue	• Si IPSec, contrôler la liste d'accès en entrée • déchiffrement - pour CET ou IPSec • contrôler la liste d'accès en entrée • contrôler les limites du débit en entrée • suivi en entrée • rediriger vers le cache Web • **NAT de l'extérieur vers l'intérieur (traduction de global en local)** • routage de stratégie • acheminement • chiffrement (vérifier le mappage et marquer pour le chiffrement) • contrôler la liste d'accès en sortie • inspecter CBAC • Interception TCP • cryptage • Queue

Configuration et sortie NAT

Cet exemple explique comment l'ordre des opérations peut affecter NAT. Dans ce cas, seuls NAT et le routage sont montrés.

Dans l'exemple précédent, le Routeur A est configuré pour traduire l'adresse locale intérieure 171.68.200.48 en 172.16.47.150, comme le montre cette configuration.

```
!
version 11.2
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
```

```
!
enable password ww
!
ip nat inside source static 171.68.200.48 172.16.47.150 !--- This command creates a static NAT
translation !--- between 171.68.200.48 and 172.16.47.150 ip domain-name cisco.com ip name-server
171.69.2.132 ! 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 171.68.200.0 255.255.255.0 172.16.47.162 !
! line con 0 exec-timeout 0 0 line aux 0 line vty 0 4 password ww login ! end
```

La table de traduction indique que la traduction voulue existe.

```
Router-A#show ip nat translation Pro Inside global Inside local Outside local Outside global ---
172.16.47.150 171.68.200.48 --- ---
```

Cette sortie est prise du Routeur A avec debug ip packet detail et debug ip nat activés, et un ping est émis du périphérique 171.68.200.48 destiné à 172.16.47.142.

Remarque: Les commandes de débogage produisent une quantité importante de sortie. Utilisez-les seulement quand le trafic sur le réseau IP est faible, afin que le reste de l'activité sur le système ne soit pas affectée. Avant d'émettre des commandes **debug**, reportez-vous à Informations importantes sur les commandes de débogage.

```
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=171.68.200.48 (Serial0), d=172.16.47.142, len 100, unroutable
    ICMP type=8, code=0
IP: s=172.16.47.161 (local), d=171.68.200.48 (Serial0), len 56, sending
    ICMP type=3, code=1
```

Puisqu'il n'y a aucun message de débogage NAT dans la sortie précédente, vous savez que la traduction statique existante n'est pas utilisée et que le routeur n'a pas de route pour l'adresse de destination (172.16.47.142) dans sa table de routage. Le résultat du paquet non routable est un message d'ICMP inaccessible , qui est envoyé au périphérique interne.

Mais le Routeur A a la route par défaut 172.16.47.145 ; donc pourquoi la route est-elle considérée comme non routable ?

Le Routeur A a **no ip classless** configuré, ce qui signifie que si un paquet destiné pour une adresse réseau « principale » (dans ce cas, 172.16.0.0) pour laquelle il existe des sous-réseaux dans la table de routage, le routeur ne se base pas sur la route par défaut. En d'autres termes, si vous émettez la commande **no ip classless**, cela arrête la capacité du routeur de rechercher la route ayant la correspondance de bits la plus longue. Afin de changer ce comportement, vous devez configurer **ip classless** sur le Routeur A. La commande **ip classless** est activée par défaut sur les routeurs Cisco avec le logiciel Cisco IOS Versions 11.3 et ultérieures.

```
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 --- 172.16.47.150 171.68.200.48 --- ---
```

Quand vous répétez le même test ping comme fait précédemment, vous voyez que le paquet est traduit et que le ping est réussi.

```
Ping Response on device 171.68.200.48

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
171.68.200.48 are getting translated by NAT.

Router-A#
```

```
**\*Mar 28 03:34:28: IP: tableid=0, s=171.68.200.48 (Serial0), d=172.16.47.142 (Serial1), routed
via RIB \*Mar 28 03:34:28: NAT: s=171.68.200.48->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->171.68.200.48 [160] \*Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1),
d=171.68.200.48 (Serial0), routed via RIB \*Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1),
d=171.68.200.48 (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=171.68.200.48->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->171.68.200.48 [161] *Mar 28 03:34:28: IP:
tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0), routed via RIB *Mar 28
03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (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=171.68.200.48-
>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-
>171.68.200.48 [162] *Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48
(Serial0), routed via RIB *Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48
(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=171.68.200.48->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->171.68.200.48 [163] *Mar 28 03:34:28: IP: tableid=0,
s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0), routed via RIB *Mar 28 03:34:28: IP:
s=172.16.47.142 (Serial1), d=171.68.200.48 (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=171.68.200.48->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->171.68.200.48
[164] *Mar 28 03:34:28: IP: tableid=0, s=172.16.47.142 (Serial1), d=171.68.200.48 (Serial0),
routed via RIB *Mar 28 03:34:28: IP: s=172.16.47.142 (Serial1), d=171.68.200.48 (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
```

L'exemple précédent montre que quand un paquet passe de l'intérieur vers l'extérieur, un routeur NAT examine sa table de routage pour rechercher une route vers l'adresse externe avant de continuer à traduire le paquet. Par conséquent, il est important que le routeur NAT ait une route valide pour le réseau externe. La route vers le réseau de destination doit être connue via une interface qui est définie en tant que NAT externe dans la configuration du routeur.

Il est important de noter que les paquets de retour sont traduits avant d'être routés. Par conséquent, le routeur NAT doit également avoir une route valide pour l'adresse locale interne dans sa table de routage.

Informations connexes

- Configuration de la traduction d'adresses réseau : Pour commencer
- Vérification de l'opération NAT et dépannage NAT de base
- NAT : Définitions locales et globales
- Comment la traduction d'adresse de réseau (NAT) multidiffusion fonctionne-t-elle sur les routeurs Cisco ?
- Page de support NAT
- Support et documentation techniques - Cisco Systems