Éviter les boucles de routage en mode NAT dynamique

Contenu

Introduction

Ce document décrit un scénario dans lequel les paquets font une boucle entre le routeur NAT et le routeur voisin sur l'interface extérieure en utilisant la traduction d'adresses de réseau dynamique (NAT) devant trafiquer destiné à un IP address inutilisé d'un groupe NAT et à la présence d'un default route sur le routeur NAT conduisant ces paquets de nouveau à l'extérieur.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Diagramme du réseau

La topologie suivante a été utilisée pour créer l'exemple de scénario.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Exemple de scénario

Dans la topologie ci-dessus, le routeur-Un est configuré avec NAT de sorte qu'il traduise des paquets originaires du réseau 171.68.200.0/24 à une plage d'adresses définie par le groupe NAT « test-boucle ». La configuration du Routeur-a est comme suit (tous autres Routeurs sont configurés avec les artères statiques afin d'obtenir la Connectivité) :

```
hostname Router-A
!
!
ip nat pool test-loop 172.16.47.161 172.16.47.165 prefix-length 28
ip nat inside source list 7 pool test-loop
!
interface Loopback0
 ip address 1.1.1.1 255.0.0.0
!
interface Ethernet0
 ip address 135.135.1.2 255.255.255.0
 shutdown
!
interface Serial0
 ip address 171.68.200.49 255.255.255.0
 ip nat inside
 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
 no ip mroute-cache
 no ip route-cache
!
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
access-list 7 permit 171.68.200.0 0.0.0.255
!
!
line con 0
 exec-timeout 0 0
line aux 0
line vty 0 4
 login
!
end
```

Utilisant l'élimination des imperfections de traduction NAT et les commandes de débogage de paquet IP, nous avons généré un ping du routeur sur le périphérique interne. Le ping fonctionné, et une entrée de table de traduction ont été générés. Dans la sortie ci-dessous, nous voyons que le paquet IP mettant au point et débogage d'IP NAT sont allumés, et qu'il n'y a aucune entrée dans la table de traduction à ce moment.

Remarque: Les commandes de **débogage** génèrent une importante quantité 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.

```
Router-A# show debug Generic IP: IP packet debugging is on (detailed) IP NAT debugging is on
Router-A# show ip nat translations Router-A#
```

Le routeur interne (périphérique interne) lance un paquet d'ICMP avec une adresse source de 171.68.200.48 et une adresse de destination de 171.68.191.1 (l'adresse du périphérique externe). La sortie de débogage suivante affiche un paquet IP avec une adresse IP source de 171.68.200.48 étant traduit à 172.16.47.161. Le paquet est livré dans l'interface Serial0 et est destiné l'interface Serial1.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [401]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

La sortie de débogage suivante affiche le paquet IP de retour avec une adresse IP de destination de 172.16.47.161 étant traduit de nouveau à 171.68.200.48. Le paquet est livré dans l'interface Serial1 et est destiné l'interface serial0.

```
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [401]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

La sortie de débogage affiche l'échange réussi de ping entre le périphérique interne et le périphérique externe :

```
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [402]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [402]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [403]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [403]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [404]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [404]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [405]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [405]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

Utilisant la commande de show ip nat translations, nous voyons une entrée dans la table de traduction pour le périphérique interne.

```
Router-A# show ip nat translations Pro Inside global Inside local Outside local Outside global -
-- 172.16.47.161 171.68.200.48 --- ---
```

Maintenant qu'une traduction pour le périphérique interne existe dans la table de traduction, nous pouvons avec succès cingler du périphérique externe à l'adresse globale du périphérique interne, suivant les indications de la sortie de débogage générée par le routeur-Un ci-dessous.

Remarque: Le paquet lancé par le périphérique externe a une adresse source de 171.68.191.1 et une adresse de destination de 172.16.47.161 (l'adresse globale interne dans la table de traduction).

```
Router-A#
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [108]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [108]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [109]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [109]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [110]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [110]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [111]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [111]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
NAT*: s=171.68.191.1, d=172.16.47.161->171.68.200.48 [112]
IP: s=171.68.191.1 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=8, code=0
NAT: s=171.68.200.48->172.16.47.161, d=171.68.191.1 [112]
IP: s=172.16.47.161 (Serial0), d=171.68.191.1 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=0, code=0
```

La sortie de débogage suivante explique ce qui peut se produire quand un périphérique externe essaye d'initier la transmission avec une adresse de destination qui est une adresse IP inutilisée dans le groupe de test-boucle. La commande de **clear ip nat translation** a été utilisée d'effacer la table de traduction et un ping a été envoyé à une adresse IP inutilisée dans le groupe de test-boucle.

Le périphérique externe envoie un paquet d'ICMP destiné pour l'adresse globale interne de 172.16.47.161. Cependant, l'interface de sortie est identique que l'interface d'entrée pour ce paquet.

```
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
```

```
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
IP: s=171.68.191.1 (Serial1), d=172.16.47.161 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

NAT traduit des paquets allant de l'externe vers interne avant de conduire le paquet. Dans ce cas, il n'y a aucune entrée dans la table de traduction, ainsi le routeur-Un peut seulement conduire le paquet. Le routeur-Un compte sur son default route pour conduire les paquets, envoyant les paquets soutiennent l'interface Serial1, qui entraîne une boucle qui pourrait par la suite réduire la ligne série.

Pour éviter ce genre de boucle de routage, ne lancez jamais les paquets des périphériques externes aux adresses globales internes. Cependant, puisqu'il est difficile imposer ce, vous pouvez ajouter une artère statique pour les adresses globales internes avec un prochain saut de null0 dans le routeur A. De cette façon, quand un périphérique externe envoie des paquets destinés pour une adresse globale interne, et là n'est aucune entrée dans la table de traduction, routeur-Un conduit le paquet à null0, évitant la boucle. Utilisant l'exemple ci-dessus, l'artère statique ressemble à ce qui suit :

```
ip route 172.16.47.160 255.255.255.252 null0.
```

Informations connexes

- Page de support NAT
- Page d'assistance pour les protocoles de routage IP
- Page de support pour le routage IP
- Support technique - Cisco Systems