Utilisation du mode NAT dans les réseaux qui se chevauchent

Contenu

Introduction

Ce document explique comment vous pouvez utiliser la Traduction d'adresses de réseau (NAT) pour des réseaux en superposition. Les réseaux en superposition sont le résultat de l'attribution d'une adresse IP à un périphérique de votre réseau qui est déjà légalement attribuée à un autre périphérique sur Internet ou un réseau extérieur. Les réseaux en superposition se produisent également quand deux sociétés, qui utilisent chacune des adresses IP RFC 1918 dans leurs réseaux fusionnent. Ces deux réseaux doivent communiquer, de préférence sans devoir réadresser tous leurs périphériques.

Conditions préalables

Conditions requises

Une compréhension de base de l'adressage IP, du routage IP et du système de noms de domaine (DNS) est utile pour comprendre le contenu de ce document.

Components Used

La prise en charge de NAT a commencé dans le logiciel Cisco IOS® version 11.2. Pour plus d'informations sur la prise en charge de la plate-forme, reportez-vous à la Foire aux questions NAT.

Conventions

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

Configuration

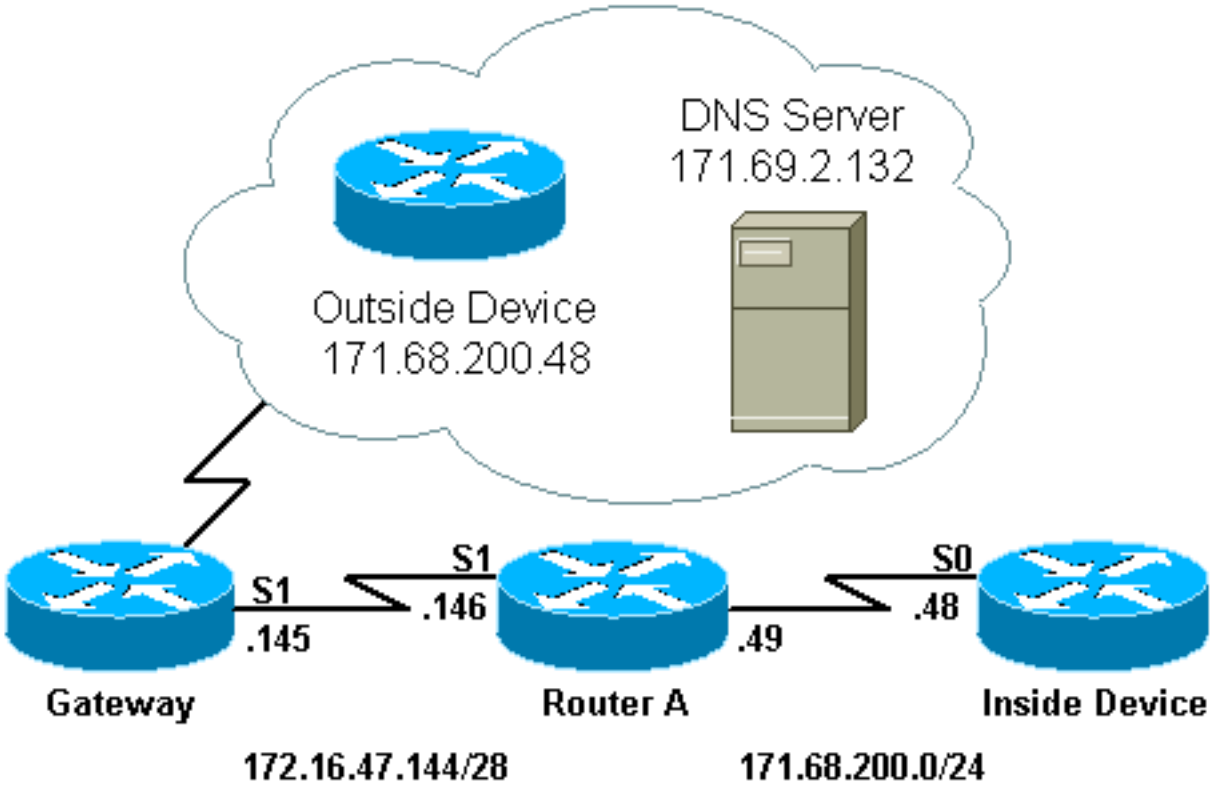
Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez l'outil de recherche de commandes (clients inscrits seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :

Notez que le périphérique interne a la même adresse IP que le périphérique externe avec lequel il souhaite communiquer.



Configurations

Le routeur A est configuré pour NAT, de sorte qu'il traduit le périphérique interne en une adresse à partir de la « boucle de test » du pool et le périphérique externe en une adresse à partir du pool « tests-dns ». La table de configuration ci-dessous explique comment cette configuration peut être utile en cas de chevauchement.

Router A
! version 11.2

```
no service udp-small-servers
no service tcp-small-servers
!
hostname Router-A
!
!
ip domain-name cisco.com
ip name-server 171.69.2.132
!
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 nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat pool test-dns 172.16.47.177 172.16.47.180 prefix-
length 28
ip nat inside source list 7 pool test-loop
ip nat outside source list 7 pool test-dns
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
```

Pour que la configuration ci-dessus puisse permettre le chevauchement lorsque le périphérique interne communique avec le périphérique externe, il doit utiliser le nom de domaine du périphérique externe.

Le périphérique interne ne peut pas utiliser l'adresse IP du périphérique externe, car elle est identique à l'adresse qui lui est attribuée (le périphérique interne). Par conséquent, le périphérique interne envoie une requête DNS pour le nom de domaine du périphérique externe. L'adresse IP du périphérique interne sera la source de cette requête, et cette adresse sera traduite en adresse à partir du pool de « test-loop » parce que la commande **ip nat inside source list** est configurée.

Le serveur DNS répond à l'adresse qui provient du pool « test-loop » avec l'adresse IP associée au nom de domaine du périphérique externe dans la charge utile du paquet. L'adresse de

destination du paquet de réponse est traduite à nouveau vers l'adresse du périphérique interne, et l'adresse de la charge utile du paquet de réponse est ensuite traduite en adresse du pool « test-dns » en raison de la commande **ip nat outside source list**. Par conséquent, le périphérique interne apprend que l'adresse IP du périphérique externe est l'une des adresses du pool « test-dns », et il utilisera cette adresse lors de la communication avec le périphérique externe. À ce stade, le routeur exécutant NAT s'occupe des traductions.

Ce processus peut être vu en détail dans la section Dépannage. Les périphériques utilisant des adresses qui se chevauchent peuvent communiquer entre eux sans utiliser DNS, mais dans ce cas, la NAT statique doit être configurée. Voici un exemple de la façon dont cela pourrait être fait.

Router A

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

ip domain-name cisco.com
ip name-server 171.69.2.132
!
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 nat pool test-loop 172.16.47.161 172.16.47.165
prefix-length 28
ip nat inside source list 7 pool test-loop
ip nat outside source static 171.68.200.48 172.16.47.177
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.47.145
ip route 172.16.47.160 255.255.255.240 Serial0
!--- This line is necessary to make NAT work for return
traffic. !--- The router needs to have a route for the
pool to the inside !--- NAT interface so it knows that a
translation is needed. 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
```

Avec la configuration ci-dessus, lorsque le périphérique interne veut communiquer avec le périphérique externe, il peut maintenant utiliser l'adresse IP 172.16.47.177, et DNS n'est pas nécessaire. Comme indiqué ci-dessus, la traduction de l'adresse du périphérique interne est toujours effectuée de manière dynamique, ce qui signifie que le routeur doit obtenir des paquets du périphérique interne avant de créer une traduction. Pour cette raison, le périphérique interne doit initialiser toutes les connexions afin que le périphérique interne et le périphérique externe puissent communiquer. Si le périphérique externe doit établir des connexions au périphérique interne, l'adresse du périphérique interne doit également être configurée de manière statique.

Vérification

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Le processus par lequel le périphérique interne a utilisé DNS pour communiquer avec le périphérique externe, comme décrit ci-dessus, peut être vu en détail avec la procédure de dépannage suivante.

Actuellement, il n'y a aucune traduction dans la table de traduction qui peut être vue avec la commande **show ip nat translations**. Les exemples ci-dessous utilisent les commandes **debug ip packet** et **debug ip nat** à la place.

Remarque : Les commandes **debug** génèrent une quantité significative de sortie. Utilisez-la uniquement lorsque le trafic sur le réseau IP est faible, de sorte que les autres activités sur le système ne sont pas affectées.

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

Lorsque le périphérique interne envoie sa requête DNS au serveur DNS, qui réside en dehors du domaine NAT, l'adresse source de la requête DNS (l'adresse du périphérique interne) est traduite en raison des commandes **ip nat inside**. Ceci peut être vu dans la sortie de débogage ci-dessous.

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=6988, dst=53
```

Lorsque le serveur DNS envoie une réponse DNS, la charge utile de la réponse DNS est traduite en raison des commandes **ip nat outside**.

Remarque : NAT ne regarde pas la charge utile de la réponse DNS, sauf si la traduction se produit sur l'en-tête IP du paquet de réponse. Reportez-vous à la commande **ip nat outside source list 7 pool** dans la configuration du routeur ci-dessus.

Le premier message NAT de la sortie de débogage ci-dessous montre que le routeur reconnaît la réponse DNS et traduit l'adresse IP dans la charge utile en 172.16.47.177. Le deuxième message NAT indique que le routeur traduit la destination de la réponse DNS afin de pouvoir renvoyer une réponse au périphérique interne qui a exécuté la requête DNS initiale. La partie de destination de l'en-tête, l'adresse globale interne, est traduite en adresse locale interne.

La charge utile de la réponse DNS est traduite :

```
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
```

La partie de destination de l'en-tête IP dans le paquet de réponse DNS est traduite :

```
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65371]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=6988
```

Examinons une autre requête et une autre réponse DNS :

```
NAT: s=171.68.200.48->172.16.47.161, d=171.69.2.132 [0]
IP: s=172.16.47.161 (Serial0), d=171.69.2.132 (Serial1), g=172.16.47.145, len 66, forward
    UDP src=7419, dst=53
NAT: DNS resource record 171.68.200.48 -> 172.16.47.177
NAT: s=171.69.2.132, d=172.16.47.161->171.68.200.48 [65388]
IP: s=171.69.2.132 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 315, forward
    UDP src=53, dst=7419
```

Maintenant que la charge utile du DNS a été traduite, notre table de traduction a une entrée pour les adresses locales et globales externes du périphérique externe. Avec ces entrées dans la table, nous pouvons maintenant traduire entièrement l'en-tête des paquets ICMP échangés entre le périphérique interne et le périphérique externe. Examinons cet échange dans la sortie de débogage ci-dessous.

Le résultat suivant indique l'adresse source (adresse du périphérique interne) en cours de traduction.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [406]
```

Ici, l'adresse de destination (adresse locale externe du périphérique) est traduite.

```
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [406]
```

Après traduction, le paquet IP ressemble à ceci :

```
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
```

Le résultat suivant indique l'adresse source (adresse du périphérique externe) traduite sur le paquet de retour.

```
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16259]
```

L'adresse de destination (adresse globale du périphérique interne) du paquet de retour est désormais traduite.

```
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16259]
```

Après traduction, le paquet de retour ressemble à ceci :

```
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

L'échange de paquets se poursuit entre le périphérique interne et le périphérique externe.

```
NAT: s=171.68.200.48->172.16.47.161, d=172.16.47.177 [407]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [407]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16262]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16262]
IP: s=172.16.47.177 (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=172.16.47.177 [408]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [408]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16267]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16267]
IP: s=172.16.47.177 (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=172.16.47.177 [409]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [409]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16273]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16273]
IP: s=172.16.47.177 (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=172.16.47.177 [410]
NAT: s=172.16.47.161, d=172.16.47.177->171.68.200.48 [410]
IP: s=172.16.47.161 (Serial0), d=171.68.200.48 (Serial1), g=172.16.47.145, len 100, forward
    ICMP type=8, code=0
NAT*: s=171.68.200.48->172.16.47.177, d=172.16.47.161 [16277]
NAT*: s=172.16.47.177, d=172.16.47.161->171.68.200.48 [16277]
IP: s=172.16.47.177 (Serial1), d=171.68.200.48 (Serial0), g=171.68.200.48, len 100, forward
    ICMP type=0, code=0
```

Une fois l'échange de paquets entre l'extérieur et l'intérieur terminé, nous pouvons regarder la table de traduction, qui a trois entrées. La première entrée a été créée lorsque le périphérique interne a envoyé une requête DNS. La deuxième entrée a été créée lorsque la charge utile de la réponse DNS a été traduite. La troisième entrée a été créée lorsque la requête ping a été échangée entre le périphérique interne et le périphérique externe. La troisième entrée est un résumé des deux premières entrées, et est utilisée pour des traductions plus efficaces.

```
Router-A# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 172.16.47.161      171.68.200.48      ---                ---
--- ---                ---                172.16.47.177      171.68.200.48
--- 172.16.47.161      171.68.200.48      172.16.47.177      171.68.200.48
```

Il est important de noter que lorsque vous essayez d'établir la connectivité entre deux réseaux qui

se chevauchent en exécutant la NAT dynamique sur un seul routeur Cisco, vous devez utiliser DNS pour créer une traduction globale externe locale à externe. Si vous n'utilisez pas DNS, la connectivité peut être établie avec la NAT statique, mais il est plus difficile à gérer.

Informations connexes

- Page de support NAT
- Support technique - Cisco Systems