Comment le mode NAT traite-t-il les fragments ICMP

Contenu

Introduction

Ce document explique comment le Traduction d'adresses de réseau (NAT) manipule des fragments de Protocole ICMP (Internet Control Message Protocol) quand vous configurez la surcharge NAT. Pour des informations sur la surcharge NAT, référez-vous à la Foire aux questions NAT.

La manipulation des fragments d'ICMP dépend de l'état de la table de traduction NAT, et la commande dans laquelle le routeur NAT reçoit l'ICMP fragmente. Nous regarderons trois cas différents, en lesquels nous envoyons deux pings de 172.16.0.1 à 172.17.1.2 avec une longueur de 3600 octets chacun (trois fragments IP).

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.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Affaire 1

Dans ce scénario nous voyons NAT pour créer entièrement une entrée de traduction étendue dans la table de traduction. Une fois que cela est fait, et il n'y a pas aucune autre adresse utilisable dans le groupe NAT, NAT relâche tous les fragments reçus avant que le premier fragment (fragment 0) d'un paquet.

Pendant que nous commençons, seulement une adresse dans le groupe exécute la surcharge ; la table de traduction NAT est vide ; et la configuration NAT apparaît en tant que :

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

Les regardons ce qui se produit pendant que les paquets commencent l'arrivée au routeur NAT.

1. Le fragment 0 du paquet 1 arrive, et NAT crée entièrement une entrée de traduction étendue. NAT se traduit alors et en avant le fragment 0 du paquet 1. La table de traduction apparaît maintenant en tant que :`Pro  Inside global  Inside local  Outside local  Outside global`
   `icmp  10.10.10.3:24320  172.16.0.1:24320  172.17.1.2:24320  172.17.1.2:24320`Notez le numéro 24320 dans la table de traduction ci-dessus. C'est la valeur d'ident d'ICMP incluse dans l'en-tête d'ICMP du datagramme IP. Seulement le fragment 0 du datagramme IP contient cette en-tête d'ICMP. Pour déterminer si les plusieurs fragments font partie du même paquet, les besoins NAT de dépister la valeur d'ident IP, trouvée dans l'en-tête IP de tous les fragments du datagramme IP d'origine. Si plusieurs fragments ont la même valeur d'ident IP comme fragmentent 0, qui a créé la traduction étendue, NAT traduit ces fragments utilisant la même entrée de traduction étendue. Référez-vous à RFC 791 pour plus d'informations sur le champ d'identification IP. Référez-vous à RFC 792 pour plus d'informations sur le champ d'identification d'ICMP.
2. Le fragment 2 du paquet 1 et le fragment 1 du paquet 1 arrivent. Puisque ces fragments font partie du même paquet qui contient le fragment 0 (qui a créé la traduction), NAT emploie l'entrée ci-dessus de traduction pour traduire et expédier ces fragments. Le périphérique de destination reçoit tous les fragments pour le paquet 1 et envoie une réponse.
3. Le fragment 1 du paquet 2 arrive. Puisque c'est un nouveau paquet, sa valeur d'ident IP n'apparie rien qui a été enregistré par NAT. Par conséquent NAT ne peut pas utiliser la traduction existante. Il ne peut pas également créer une nouvelle traduction puisqu'il a déjà entièrement une entrée de traduction étendue et il n'a pas l'ident d'ICMP pour créer un autre. Fragment NAT 1. du paquet 2 de baisses.
4. Le fragment 0 du paquet 2 arrive. NAT peut utiliser la traduction ci-dessus puisque l'ident d'ICMP s'assortit. (Tous les pings dans une série unique de pings utilisent le même nombre d'ident d'ICMP.) En ce moment, NAT enregistre l'ident IP de ce paquet. NAT se traduit et en avant le fragment 0 du paquet 2.
5. Le fragment 2 du paquet 2 arrive. NAT peut maintenant utiliser la traduction ci-dessus puisque sa valeur d'ident IP apparie l'un NAT enregistré dans l'étape précédente. NAT se traduit et en avant le fragment 2. du paquet 2. Le périphérique de destination reçoit seulement le fragment 0 et 2 (le fragment 1 manque), ainsi il n'envoie aucune réponse.

Affaire 2

Dans ce scénario, nous voyons que si les fragments autres que le premier fragment (fragment 0) arrivent en premier, NAT crée une traduction simple tant que il y a une adresse dans le groupe NAT qui n'a pas été déjà utilisé dans une traduction entièrement étendue.

Car nous commençons, il y a seulement une adresse dans le groupe NAT, la table de traduction NAT est vide, et la configuration apparaît en tant que :

```
ip nat pool POOL1 10.10.10.3 10.10.10.3 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

1. Le fragment 1 du paquet 1 arrive. NAT ne peut pas créer une traduction entièrement étendue dans la table de traduction puisqu'elle n'a pas les informations d'ident d'ICMP dans ce fragment. Cependant, puisqu'il n'y a pas aucune traduction entièrement étendue en place, NAT écrit une traduction simple. NAT se traduit alors et en avant le fragment 1. du paquet 1. L'entrée de traduction apparaît en tant que :
```
Pro    Inside global     Inside local
Outside local       Outside global
---    10.10.10.3        172.16.0.1            ---                 ---
```
2. Le fragment 0 du paquet 1 arrive. Puisque les informations d'ident d'ICMP sont incluses dans ce fragment, NAT écrit entièrement une entrée de traduction étendue :
```
Pro      Inside global
Inside local        Outside local       Outside global
---      10.10.10.3            172.16.0.1          ---                 ---
icmp     10.10.10.3:24321      172.16.0.1:24321    172.17.1.2:24321    172.17.1.2:24321
```
NAT enregistre alors les informations d'ident IP, et se traduit et en avant le fragment 0 du paquet 1.
3. Le fragment 2 du paquet 1 arrive. Puisque ce fragment a les mêmes informations d'ident IP que NAT enregistré dans l'étape 2, NAT emploie la traduction entièrement étendue pour traduire et pour expédier paquet à 1 fragment 2.Le périphérique de destination reçoit tous les fragments et réponses. En ce moment, tous les pings réussissent jusqu'à ce que la table de traduction NAT soit effacée ou chronomètre.

Affaire 3

Dans ce scénario, nous voyons que si les fragments autres que le premier fragment (fragment 0) arrivent en premier, NAT crée une traduction simple tant que il y a une adresse dans le groupe NAT qui n'a pas été déjà utilisé dans une traduction entièrement étendue. Si une traduction étendue dans la table NAT utilise déjà l'adresse, vous courez le risque de NAT traduisant chacune des adresses sources de fragment à une adresse différente.

Pendant que nous commençons, plus d'une adresse dans le groupe NAT exécute la surcharge, la table de traduction a déjà une traduction étendue, et la configuration est :

```
ip nat pool POOL1 10.10.10.3 10.10.10.5 prefix-length 24
ip nat inside source list 5 pool POOL1 overload
access-list 5 permit 172.16.0.0 0.0.0.31
```

La table de traduction apparaît en tant que :

```
Pro     Inside global         Inside local        Outside local       Outside global
icmp    10.10.10.3:24322      172.16.0.1:24322    172.17.1.2:24322    172.17.1.2:24322
```

1. Le fragment 1 du paquet 1 arrive. NAT ne peut pas créer une entrée de table entièrement étendue de traduction puisqu'elle n'a pas les informations d'ident d'ICMP dans ce fragment, et elle ne peut pas créer une entrée de traduction simple pour l'adresse 10.10.10.3, puisqu'il y a une entrée étendue existante pour cette adresse IP. NAT sélectionne la prochaine

adresse IP libre (10.10.10.4) et crée une traduction simple. NAT se traduit alors et en avant le fragment 1. du paquet 1. La table de traduction apparaît maintenant en tant que :Pro

```
Inside global         Inside local       Outside local      Outside global
---     10.10.10.4           172.16.0.1          ---                ---
icmp    10.10.10.3:24322     172.16.0.1:24322    172.17.1.2:24322   172.17.1.2:24322
```

2. Le fragment 0 du paquet 1 arrive. Puisque les informations d'ident d'ICMP sont incluses dans ce fragment, NAT écrit entièrement une entrée de traduction étendue pour l'adresse 10.10.10.3, et enregistre les informations d'ident IP pour ce paquet. NAT se traduit alors et en avant le fragment 0 du paquet 1. La table de traduction apparaît maintenant en tant que

```
:Pro     Inside global         Inside local       Outside local      Outside global
---     10.10.10.4           172.16.0.1          ---                ---
icmp    10.10.10.3:24322     172.16.0.1:24322    172.17.1.2:24322   172.17.1.2:24322
icmp    10.10.10.3:24323     172.16.0.1:24323    172.17.1.2:24323   172.17.1.2:24323
```

3. Le fragment 2 du paquet 1 arrive. Puisque ses informations d'ident IP apparient l'un NAT enregistré dans l'étape 2, NAT utilise la traduction entièrement étendue créée dans l'étape 2 pour traduire et pour expédier à paquet 1 fragment 2.En ce moment, le périphérique de destination reçoit tous les fragments du paquet 1, mais fragmente 0 et 2 ont fait traduire leur adresse source à 10.10.10.3 et le fragment 1 a été traduit à 10.10.10.4. Par conséquent, le périphérique de destination ne peut pas rassembler le paquet et n'envoie aucune réponse.
4. Le fragment 0 du paquet 2 arrive. NAT utilise la traduction entièrement étendue ci-dessus ou crée une nouvelle traduction entièrement étendue selon la valeur du champ d'ident d'ICMP de fragment. Dans l'un ou l'autre de cas, NAT enregistre les informations d'ident IP. NAT se traduit alors et en avant le fragment 0 du paquet 2.
5. Le fragment 2 du paquet 2 arrive. Ses informations d'ident IP apparient ce que NAT enregistré dans l'étape 4, si NAT utilise la deuxième traduction entièrement étendue créée dans l'étape 4. NAT se traduit et en avant fragment 2. du paquet 2.
6. Le fragment 1 du paquet 2 arrive. Ses informations d'ident IP apparient ce que NAT enregistré dans l'étape 4, si NAT utilise la deuxième traduction entièrement étendue créée dans l'étape 4. NAT se traduit et en avant fragment 1. du paquet 2.Le périphérique de destination reçoit chacun des trois fragments du paquet 2 de la même source (10.10.10.3), ainsi il rassemble le paquet et répond.

Résumé

Si les baisses NAT ou en avant un fragment d'ICMP dépend d'un certain nombre de choses, telles que la commande dans laquelle le routeur NAT reçoit les fragments, et l'état de la table de traduction à ce moment-là. Dans certaines conditions, NAT traduit les fragments différemment, qui le rend impossible pour que le périphérique de destination rassemble le paquet.

Informations connexes

- Page de support NAT
- Page de support pour le routage IP
- Support technique - Cisco Systems