Comportement inattendu de la NAT dynamique avec trafic non réparable

Contenu

Introduction

Ce document décrit le comportement inattendu de la traduction d'adresses de réseau dynamique (NAT) avec le trafic non réparable sur les périphériques IOS®.

Problème

Le trafic non réparable crée des demi-entrées dans la table des traductions NAT en cas de NAT dynamique. Ces entrées représentent un risque pour la sécurité car elles fonctionnent pour le trafic externe à interne.

Configuration NAT :

```
ip nat pool ATT_FIBER 10.10.10.1 10.10.10.6 netmask  255.255.255.248
ip nat inside source list GUEST_SUBNET pool ATT_FIBER overload
ip nat inside source list OFFICE_SUBNETS pool ATT_FIBER overload

ip access-list extended OFFICE_SUBNETS
 deny   ip 172.16.26.0 0.0.0.127 any
 permit ip 172.16.8.0 0.0.1.255 any

ip access-list extended GUEST_SUBNET
 permit ip 172.16.26.0 0.0.0.127 any
```

```
udp 10.10.10.1:49370    172.16.9.9:49370      192.168.1.1:53      192.168.1.1:53
udp 10.10.10.1:49535    172.16.9.9:49535      192.168.2.2:53    192.168.2.2:53
tcp 10.10.10.1:53133    172.16.9.9:53133      192.168.3.3:80     192.168.3.3:80
tcp 10.10.10.1:56311    172.16.9.9:56311      192.168.4.4:5816    192.168.4.4:5816
--- 10.10.10.1         172.16.9.9            ---                  ---
```

Les demi-entrées sont créées dans certains cas où il existe un mappage interne -> externe ou lorsque le paquet est initié de l'intérieur -> externe.

Lorsque le routeur est configuré pour la surcharge NAT (traduction d'adresses de port (PAT)) et que le trafic non réparable atteint le routeur, des entrées de liaison non remplaçables sont créées pour ce trafic. Il mène à ce type d'entrée dans la table NAT :

```
--- 10.10.10.1        172.16.9.9           ---                  ---
```

Cette entrée de liaison consomme une adresse complète à partir du pool. Dans cet exemple, 10.10.10.1 est une adresse d'un pool surchargé.

Cela signifie qu'une adresse IP locale interne est liée à l'adresse IP globale externe qui est similaire à la NAT statique. C'est pourquoi, tant que l'entrée actuelle n'est pas arrivée à expiration, les nouvelles adresses IP locales internes ne peuvent pas utiliser cette adresse IP globale. Toutes les traductions créées pour cette liaison sont des traductions de 1 à 1 au lieu d'une surcharge.

Solution

Afin de résoudre ce problème, vous pouvez utiliser des routes-maps avec NAT dynamique. Avec les routes-maps, NAT ne crée pas de demi-entrées ou n'utilise pas la surcharge d'interface au lieu de la surcharge de pool. Les liaisons non remplaçables ne sont pas créées en cas de surcharge d'interface.