Comportement inhabituel de NAT dynamique avec le trafic de Non-Pattable

Contenu

Introduction

Ce document décrit le comportement inhabituel de la traduction d'adresses de réseau dynamique (NAT) avec le trafic de Non-Pattable sur des périphériques de ® IOS.

Problème

Le trafic de Non-Pattable crée des moitié-entrées dans la table de traductions NAT en cas de NAT dynamique. Ces entrées posent comme risque de sécurité puisqu'elles fonctionnent pour le trafic de l'extérieur vers l'intérieur.

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            ---                  ---
```

De demi entrées sont créées dans certains cas où il y a un mappage de l'intérieur - > extérieur ou quand le paquet est initié de l'intérieur - > dehors.

Quand le routeur est configuré pour la surcharge NAT (traduction d'Addess de port (PAT)) et le trafic non-pattable frappe le routeur, les entrées non-pattable de grippage obtiennent créé pour ce trafic. Il mène à ce genre d'entrée dans la table 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            ---                  ---
```

Cette entrée de grippage consomme une adresse entière du groupe. Dans cet exemple, 10.10.10.1 est une adresse d'un groupe surchargé.

Cela signifie qu'une adresse IP d'interne local obtient la limite à l'IP global d'extérieur qui est semblable à NAT statique. Pour cette raison, jusqu'à ce que l'entrée en cours obtienne chronométré, les nouvelles adresses IP d'interne local ne peuvent pas utiliser cette adresse IP globale. Toute la traduction créée pour ce grippage est les traductions 1 à 1 au lieu de la surcharge.

Solution

Afin de résoudre ce problème, vous pouvez utiliser des route-map avec NAT dynamique. Avec des route-map, NAT ne créera pas des moitié-entrées ou utilisera la surcharge d'interface au lieu de la surcharge de groupe. Des attaches de Non-pattable ne sont pas créées en cas de surcharge d'interface.