Comportement inattendu de la NAT dynamique avec trafic non brevetable

Table des matières

Introduction

Problème

Solution

Introduction

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

Problème

Le trafic non brevetable crée des demi-entrées dans la table de traductions NAT en cas de NAT dynamique. Ces entrées posent un risque de sécurité, car elles fonctionnent pour le trafic de l'extérieur vers l'intérieur.

Configuration NAT :

<#root>

```
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            ---                   ---
```

Des demi-entrées sont créées dans certains cas où il existe un mappage de inside -> outside ou lorsque le paquet est lancé de inside -> outside.

Lorsque le routeur est configuré pour la surcharge NAT (traduction d'adresses de port (PAT)) et que le trafic non pattable atteint le routeur, des entrées de liaison non pattable 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 utilise une adresse complète 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. Par conséquent, tant que l'entrée actuelle n'a pas expiré, 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 route-maps avec NAT dynamique. Avec les route-maps, la NAT ne crée pas de demi-entrées et n'utilise pas la surcharge d'interface au lieu de la surcharge du pool. Les liaisons non brevetables ne sont pas créées en cas de surcharge d'interface.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.