Comportamento inesperado de NAT dinâmico com tráfego não-pagável

Contents

[Introduction](#)
[Problema](#)
[Solução](#)

Introduction

Este documento descreve o comportamento inesperado da Network Address Translation (NAT) dinâmica com tráfego Não Pattável em dispositivos IOS®.

Problema

O tráfego que não pode ser transportado cria meia entrada na tabela de conversões NAT no caso de NAT dinâmico. Essas entradas representam um risco à segurança, já que funcionam para o tráfego de fora para dentro.

Configuração do 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            ---                  ---
```

Metade das entradas são criadas em certos casos em que há um mapeamento de dentro -> externo ou quando o pacote é iniciado de dentro -> externo.

Quando o roteador é configurado para sobrecarga de NAT (Port Addess Translation (PAT)) e o tráfego não patível atinge o roteador, entradas de vinculação não patáveis são criadas para esse tráfego. Isso leva a esse tipo de entrada na tabela NAT:

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

Essa entrada de associação consome um endereço inteiro do pool. Neste exemplo, 10.10.10.1 é um endereço de um pool sobrecarregado.

Isso significa que um endereço IP local interno é vinculado ao IP global externo, que é semelhante ao NAT estático. Por causa disso, até que a entrada atual tenha expirado, os novos endereços IP locais internos não poderão usar esse endereço IP global. Toda a conversão criada para esta associação é de 1 para 1 em vez de sobrecarga.

Solução

Para resolver esse problema, você pode usar mapas de rota com NAT dinâmico. Com mapas de rota, o NAT não criará meia entrada nem usará sobrecarga de interface em vez de sobrecarga de pool. As associações não patáveis não são criadas em caso de sobrecarga da interface.