Comportamiento inesperado de NAT dinámica con tráfico no compatible

Contenido

Introducción

Este documento describe el comportamiento inesperado de la traducción dinámica de direcciones de red (NAT) con tráfico no compatible en dispositivos IOS®.

Problema

El tráfico no compatible crea semirentradas en la tabla de traducciones NAT en caso de NAT dinámica. Estas entradas suponen un riesgo para la seguridad, ya que trabajan para el tráfico exterior al interior.

Configuración de 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            ---                  ---
```

Se crean semirentradas en ciertos casos en los que hay una asignación de interna -> externa o cuando el paquete se inicia desde adentro -> externa.

Cuando el router está configurado para sobrecarga de NAT (Traducción de direcciones de puerto (PAT)) y el tráfico no patentable llega al router, se crean entradas de enlace no patentables para este tráfico. Esto lleva a este tipo de entrada en la tabla NAT:

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

Esta entrada de enlace consume una dirección completa del conjunto. En este ejemplo, 10.10.10.1 es una dirección de un conjunto sobrecargado.

Esto significa que una dirección IP local interna se enlaza a la IP global externa que es similar a la NAT estática. Debido a esto, hasta que se agote el tiempo de espera de la entrada actual, las nuevas direcciones IP locales internas no pueden utilizar esta dirección IP global. Toda la traducción creada para este enlace son traducciones de 1 a 1 en lugar de sobrecarga.

Solución

Para resolver este problema, puede utilizar route-maps con NAT dinámica. Con route-maps, NAT no creará semirentradas ni usará la sobrecarga de la interfaz en lugar de la sobrecarga del conjunto. No se crean vinculaciones no patentables en caso de sobrecarga de interfaz.