具有不可配置流量的動態NAT的意外行為

目錄

簡介

本檔案將說明IOS®裝置上使用不可路徑流量的動態網路位址轉譯(NAT)的意外行為。

問題

對於動態NAT，非可配置流量在NAT轉換表中建立半條目。這些條目會構成安全風險，因為它們適用於從外部到內部的流量。

NAT配置：

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

在某些情況下建立半條目，其中存在內部 — >外部對映，或者資料包從內部 — >外部發起。

當路由器配置為NAT過載(埠地址轉換(PAT))且不可配置流量到達路由器時，將為此流量建立不可配置繫結條目。它導致NAT表中的此類條目：

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

此繫結條目會使用池中的整個地址。在本示例中，10.10.10.1是來自超載池的地址。

這意味著內部本地IP地址繫結到類似於靜態NAT的外部全域性IP。因此，在當前條目超時之前，新的內部本地IP地址不能使用此全域性IP地址。為此繫結建立的所有轉換都是1對1轉換，而不是過載。

解決方案

為了解決此問題，您可以將路由對映與動態NAT結合使用。 使用路由對映時，NAT不會建立半條目或使用介面過載而不是池過載。如果介面過載，則不會建立不可模式繫結。