具有不可路由流量的动态NAT的意外行为

目录

简介

本文档介绍IOS®设备上具有不可路径流量的动态网络地址转换(NAT)的意外行为。

问题

非可路径流量在NAT转换表中创建半个条目，以防动态NAT。由于这些条目适用于从外部到内部的流量，因此会带来安全风险。

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            ---                   ---
```

在存在内部 — >外部映射或从内部 — >外部发起数据包时，会创建一半条目。

当路由器配置为NAT过载(端口地址转换(PAT))且不可路径流量到达路由器时，将为此流量创建不可路径绑定条目。它导致NAT表中出现以下条目：

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

此绑定条目使用池中的整个地址。在本例中，10.10.10.1是来自过载池的地址。

这意味着内部本地IP地址绑定到与静态NAT类似的外部全局IP。因此，在当前条目超时之前，新的内部本地IP地址无法使用此全局IP地址。为此绑定创建的所有转换都是1对1转换，而不是过载。

解决方案

要解决此问题，可以将路由映射与动态NAT配合使用。 使用路由映射时，NAT不会创建半个条目或使用接口过载而不是池过载。接口过载时不会创建非路径绑定。