动态NAT意外行为与非Pattable流量的

目录

简介

本文描述意外行为动态网络地址转换(NAT)与在IOS®设备的非Pattable流量。

问题

非Pattable流量在动态NAT的情况下在NAT转换表里创建半条目。因为他们为外部到内部流量，工作这些条目摆在作为安全风险。

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            ---                   ---
```

半条目在某些情况下创建有里面映射- >外部或的地方，当数据包从里边启动-时>从外部。

当路由器为NAT超载(波尔特Addess转换(PAT))配置并且非pattable流量点击路由器，非pattable捆绑条目为此流量得到创建。它在NAT表里导致这种条目：

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

此捆绑条目消耗从池的一个整个地址。在本例中， 10.10.10.1是从一个被超载的池的一个地址。

那含义Inside local IP地址获得一定对类似于静态NAT的外网全局IP。因此，直到被计时的当前条目获得，新建的Inside local IP地址不能使用此全局IP地址。为此捆绑创建的所有转换是一对一转换而不是超载。

解决方案

为了解决此问题，您能以动态NAT使用route-map。 使用route-map， NAT不会创建半条目也不会使用接口超载而不是池超载。非pattable捆绑没有在接口超载的情况下创建。