Unerwartetes Verhalten von dynamischer NAT bei nicht patentierbarem Datenverkehr

Inhalt

Einführung

In diesem Dokument wird das unerwartete Verhalten von dynamischer Network Address Translation (NAT) bei nicht patentiertem Datenverkehr auf IOS®-Geräten beschrieben.

Problem

Nicht-Pattable-Datenverkehr erstellt bei dynamischer NAT Halbeinträge in der NAT-Übersetzungstabelle. Diese Einträge stellen ein Sicherheitsrisiko dar, da sie für den Verkehr von außen nach innen wirken.

NAT-Konfiguration:

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

Die Hälfte der Einträge wird in bestimmten Fällen erstellt, in denen eine Zuordnung von innen -> außen oder von innen -> außen erfolgt.

Wenn der Router für NAT-Overload (Port Addess Translation (PAT)) und nicht patentierbaren Datenverkehr auf den Router konfiguriert ist, werden für diesen Datenverkehr nicht patentierbare Bindungseinträge erstellt. Diese Art von Eintrag führt zur NAT-Tabelle:

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

Dieser Bindungseintrag belegt eine gesamte Adresse aus dem Pool. In diesem Beispiel ist 10.10.10.1 eine Adresse aus einem überladenen Pool.

Das bedeutet, dass eine interne lokale IP-Adresse an die externe globale IP-Adresse gebunden wird, die der statischen NAT ähnelt. Daher können neue interne lokale IP-Adressen diese globale IP-Adresse nicht verwenden, bis der aktuelle Eintrag das Timeout erreicht hat. Bei der gesamten für diese Bindung erstellten Übersetzung handelt es sich um 1:1-Übersetzungen anstelle von Überlastung.

Lösung

Um dieses Problem zu beheben, können Sie route-maps mit dynamischer NAT verwenden. Bei Routing-Maps erstellt NAT keine Halbeinträge und verwendet keine Überlastung der Schnittstellen statt einer Überlastung des Pools. Im Falle einer Schnittstellenüberladung werden keine nicht patentierbaren Bindungen erstellt.