Onverwacht gedrag van Dynamisch NAT met niet-opvraagbaar verkeer

Inhoud

Inleiding

Dit document beschrijft het onverwachte gedrag van Dynamic Network adresomzetting (NAT) met niet-Pattable verkeer op IOS® apparaten.

Probleem

Niet-Pattable verkeer creëert halve ingangen in de vertaaltabel NAT in het geval van dynamische NAT. Deze inzendingen vormen een veiligheidsrisico omdat ze werken voor buitengebruik verkeer.

NAT-configuratie:

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

Halve items worden gecreëerd in bepaalde gevallen waar er een afbeelding van binnenuit is -> buitenkant of wanneer pakket van binnenuit wordt geïnitieerd -> buitenkant.

Wanneer de router is geconfigureerd voor NAT-overload (Port Adess Translation (PAT) en niet-plattable verkeer de router bereikt, worden niet-Pattable JECT-items gecreëerd voor dit verkeer. Dit leidt tot dit soort vermelding in de NAT-tabel:

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

Dit bindt inzending verbruikt een volledig adres uit de pool. In dit voorbeeld is 10.10.10.1 een adres uit een overbelast bassin.

Dat betekent dat een binnen lokaal IP adres gebonden wordt aan het buiten globale IP dat gelijkend is op statische NAT. Daarom kunnen nieuwe interne lokale IP-adressen niet dit globale IP-adres gebruiken totdat het huidige adres is uitgeschakeld. Alle vertalingen die hiervoor gemaakt worden, zijn 1-tot-1 vertalingen in plaats van overbelasting.

Oplossing

Om dit probleem op te lossen, kunt u routekaarten gebruiken met dynamische NAT. Met routekaarten zal NAT geen halve ingangen maken of interface-overbelasting in plaats van pooloverbelasting gebruiken. Niet-Pattable bindings worden niet gecreëerd in geval van interface overload.