Comportamento imprevisto di NAT dinamico con traffico non tracciabile

Sommario

Introduzione

Questo documento descrive il comportamento imprevisto di NAT (Network Address Translation) dinamico con traffico non tracciabile sui dispositivi IOS®.

Problema

Il traffico non modulare crea mezze voci nella tabella di traduzioni NAT in caso di NAT dinamico. Queste voci rappresentano un rischio per la sicurezza in quanto funzionano per il traffico da esterno a interno.

Configurazione NAT:

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

La metà delle voci viene creata in alcuni casi in cui è presente una mappatura interna -> esterna o quando il pacchetto viene avviato dall'interno -> dall'esterno.

Quando il router è configurato per il sovraccarico NAT (Port Address Translation, PAT) e il traffico non indirizzabile colpisce il router, vengono create voci di binding non indirizzabili per questo traffico. Il risultato è questo tipo di voce nella tabella NAT:

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

Questa voce di binding utilizza un intero indirizzo del pool. Nell'esempio, 10.10.10.1 è un indirizzo di un pool sovraccarico.

Ciò significa che un indirizzo IP locale interno viene associato all'IP globale esterno, simile al protocollo NAT statico. Per questo motivo, fino al timeout della voce corrente, i nuovi indirizzi IP locali interni non possono utilizzare questo indirizzo IP globale. Tutta la traduzione creata per questa associazione è una traduzione da 1 a 1 anziché un sovraccarico.

Soluzione

Per risolvere questo problema, è possibile utilizzare le route map con NAT dinamico. Con le route map, NAT non crea mezze voci o non utilizza il sovraccarico dell'interfaccia invece del sovraccarico del pool. I binding non associabili tramite patch non vengono creati in caso di sovraccarico dell'interfaccia.