Configurazione del pool NAT e risoluzione dei problemi di esaurimento del pool NAT in FTD

Sommario

Problema

Gli utenti riscontrano problemi di accesso per il traffico FTD quando il pool NAT non è sufficiente per tradurre tutte le connessioni utente necessarie. La modifica della configurazione è necessaria per garantire risorse NAT sufficienti per la gestione di un numero elevato di connessioni.

Ambiente

- Cisco Secure Firewall Firepower - applicabile a tutti i modelli e le versioni FTD e ASA
- Connessioni con volumi elevati (oltre 100.000)

Risoluzione

Per risolvere e garantire una traduzione affidabile per grandi volumi di connessioni, espandere il pool NAT per la traduzione dinamica sull'FTD Cisco. Questa operazione è necessaria per coprire un numero di connessioni superiore a 100.000 conversioni TCP o UDP simultanee.

1. Determinare la configurazione e l'utilizzo correnti del pool NAT per identificare la necessità di espansione.

Output di esempio:

```
device# show run nat
nat (inside,outside) source dynamic PROXY-OUT-10.X.X.2-5 pat-pool PROXY-PAT-203.X.X.1-4
nat (inside,outside) source static BlueCoat3Inside-10.X.X.X BlueCoat1Outside-203.X.X.5
```

```
nat (inside,outside) source static BluecoatInside-10.X.X.X BlueCoat2Outside-203.X.X.6
nat (inside,outside) source static BluecoatOutside_10.X.X.X BlueCoatNATOutside_203.X.X.7 description VM
nat (inside,outside) source static BluecoatOutside_10.X.X.X BlueCoatNATOutside_203.X.X.8 description VM
!
nat (inside,outside) after-auto source dynamic any interface
```

2. Stimare il numero di conversioni di indirizzi IP/porte richieste per supportare il numero desiderato di connessioni TCP/UDP simultanee rilevate sul dispositivo.

Output di esempio:

<#root>

```
device# show conn count
device# show xlate count
103388 in use, 106915 most used
...
device# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source dynamic PROXY-OUT-10.X.X.2-5 pat-pool PROXY-PAT-203.X.X.1-4
```

translate_hits = 1668081470, untranslate_hits = 207827918

```
2 (inside) to (outside) source static BlueCoat3Inside-10.X.X.X BlueCoat1Outside-203.X.X.5
 translate_hits = 0, untranslate_hits = 0
3 (inside) to (outside) source static BluecoatInside-10.X.X.X BlueCoat2Outside-203.X.X.6
 translate_hits = 0, untranslate_hits = 0
4 (inside) to (outside) source static BluecoatOutside_10.X.X.X BlueCoatNATOutside_203.X.X.7 description
 translate_hits = 212, untranslate_hits = 903609
5 (inside) to (outside) source static BluecoatOutside_10.X.X.X BlueCoatNATOutside_203.X.X.8 description
 translate_hits = 221, untranslate_hits = 900629
...
Manual NAT Policies (Section 3)
1 (inside) to (outside) source dynamic any interface
```

translate_hits = 1655085476, untranslate_hits = 65319288

3.Determinare se i pacchetti scendono con il motivo "nat-xlate-pool-exceeded" (nat-xlate-pool-scaricato) sono in aumento sul dispositivo. Ogni indirizzo IP in un pool PAT in genere supporta fino a 128.000 conversioni (porte TCP e UDP combinate). Tuttavia, per traduzioni eccessive su un certo protocollo, sono necessari più indirizzi IP. Ad esempio, se il dispositivo mostra oltre 100.000 conversioni univoche della porta TCP, sono necessari almeno due indirizzi IP in quanto su un indirizzo IP sarebbero possibili solo 64.000 conversioni TCP univoche.

Output di esempio:

<#root>

```
firepower# show asp drop
Frame drop:
 Flow is denied by configured rule (acl-drop) 22233
 First TCP packet not SYN (tcp-not-syn) 645
 TCP failed 3 way handshake (tcp-3whs-failed) 122
 TCP RST/FIN out of order (tcp-rstfin-ooo) 2835
 TCP SEQ in SYN/SYNACK invalid (tcp-seq-syn-diff) 2
 TCP SYNACK on established conn (tcp-synack-ooo) 4
 TCP packet SEQ past window (tcp-seq-past-win) 169
 TCP invalid ACK (tcp-invalid-ack) 5
 TCP RST/SYN in window (tcp-rst-syn-in-win) 4
```

NAT failed due to pool exhaustion (nat-xlate-pool-exhausted) 26448

```
 Connection to PAT address without pre-existing xlate (nat-no-xlate-to-pat-pool) 168
 Blocked or blacklisted by the firewall preprocessor (firewall) 1780
 Blocked or blacklisted by the reputation preprocessor (reputation) 3
 Packet is blacklisted by snort (snort-blacklist) 17848
 Modifies fixed length of data (snort-replace-data-pkt) 51
```

4.Determina quante traduzioni vengono utilizzate per ogni NAT e se sono principalmente per le traduzioni TCP o UDP. Usare un parser automatico o un software syslog/snmp per analizzare l'output "show xlate detail" e raccogliere i top talker.

```
device# show xlate detail | redirect disk0:/show.xlate.detail.txt
```

Output di esempio dopo l'analisi AI:

```
Top Protocols
+-------------------------+---------+---------+
| (Dynamic NAT and PAT)   | Count   | %       |
+=========================+=========+=========+
| TCP                     | 96047   | 92.941% |
+-------------------------+---------+---------+
| UDP                     | 7286    | 7.05%   |
+-------------------------+---------+---------+
| ICMP                    | 9       | 0.009%  |
+-------------------------+---------+---------+
 Top Translated (Mapped) Source IPs
+---------------------------------------+---------+---------+
| (Dynamic NAT and PAT)                 | Count   | %       |
+=======================================+=========+=========+
| 203.X.X.9                             | 71585   | 69.27%  |
+---------------------------------------+---------+---------+
| 203.X.X.6                             | 31434   | 30.417% |
+---------------------------------------+---------+---------+
| 203.X.X.10                            | 323     | 0.313%  |
```

```
+----------------------------------------+---------+---------+
```

5. Espandere il pool NAT aggiungendo uno o più pool di indirizzi IP per il traffico dell'interfaccia FTD. Consultare la documentazione ufficiale, se necessario: Configurazione e verifica di NAT su FTD

Confermare che il nuovo indirizzo è stato aggiunto.

Output di esempio dopo l'aggiunta:

```
device# show run nat
nat (inside,outside) source dynamic PROXY-OUT-10.X.X.2-5 pat-pool PROXY-PAT-203.X.X.1-4
nat (inside,outside) source static BlueCoat3Inside-10.X.X.X BlueCoat1Outside-203.X.X.5
nat (inside,outside) source static BluecoatInside-10.X.X.X BlueCoat2Outside-203.X.X.6
nat (inside,outside) source static BluecoatOutside_10.X.X.X BlueCoatNATOutside_203.X.X.7 description VM
nat (inside,outside) source static BluecoatOutside_10.X.X.X BlueCoatNATOutside_203.X.X.8 description VM
nat (inside,outside) source dynamic 10-Network pat-pool 203.X.X.10 destination static Cloud-1 Cloud-1
!
nat (inside,outside) after-auto source dynamic any interface
```

6.Monitorare l'utilizzo del pool NAT dopo l'espansione del pool per garantire la disponibilità di risorse di traduzione sufficienti. Verifica la presenza di errori di traffico e convalida traduzioni utente riuscite

Output di esempio:

<#root>

```
device# show conn
device# show nat
...
Manual NAT Policies (Section 1)
...
6 (inside) to (outside) source dynamic 10-Network pat-pool 203.X.X.10 destination static Cloud-1 Cloud-
```

translate_hits = 134315, untranslate_hits = 136136

Se gli errori persistono o i limiti delle connessioni vengono raggiunti, aggiungere altri indirizzi al pool NAT in base alle esigenze.

7. Per istruzioni dettagliate e procedure di convalida, consultare la guida ufficiale alla configurazione di Cisco Secure Firewall NAT: Configura pool PAT su FTD

Se per un qualsiasi motivo è necessario rivedere traduzioni da locale a NAT specifiche, utilizzare `show conn` per individuare l'indirizzo specificato in base all'indirizzo IP locale o NAT. I comandi `show nat` non sono in grado di eseguire questa operazione. L'output `show conn detail` può essere reindirizzato su disco0 (/mnt/disk0) anche per l'analisi. Ciò è particolarmente utile per abbinare i pool VPN NAT a IP reali locali.

```
> show conn | include 10.239.27.176
TCP management_static_vti_1  10.238.x.176(10.239.x.176):55140 CH01FTD02-inside  10.x.x.161:22, idle 0:0
TCP management_static_vti_1  10.238.x.176(10.239.x.176):9125 CH01FTD02-inside  10.x.x.162:22, idle 0:00
TCP management_static_vti_1  10.238.x.176(10.239.x.176):51681 CH01FTD02-inside  10.x.x.17:7000, idle 0:
                            Source NAT IP(Source Local IP)                      (Destination IP)
---
show conn detail | redirect disk0:/show.conn.detail.txt
```

Causa

Il problema è causato da un pool NAT insufficiente per le traduzioni dinamiche, che ha causato l'esaurimento delle traduzioni delle porte e delle risorse IP disponibili. Ciò limita il numero di connessioni TCP/UDP simultanee che possono essere supportate, causando problemi di accesso al traffico e di connettività per scenari con volumi elevati.

Contenuto correlato

- Configura pool PAT su FTD
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).