NAT-pool configureren en problemen oplossen NAT-pool-uitputting in FTD

Inhoud

uitgeven

Gebruikers ondervinden toegangsproblemen voor FTD-verkeer wanneer de NAT-pool niet voldoende is om alle benodigde gebruikersverbindingen te vertalen. Configuratiewijziging is vereist om te zorgen voor voldoende NAT-bronnen voor het verwerken van een groot aantal verbindingen.

milieu

- Cisco Secure Firewall Firepower - toepasbaar op alle FTD- en ASA-modellen en -versies
- Aansluitingen voor grote volumes (100.000+)

resolutie

Om een betrouwbare vertaling voor grote volumes verbindingen op te lossen en te garanderen, breidt u de NAT-pool voor dynamische vertaling uit op de Cisco FTD. Dit is nodig om het aantal verbindingen te dekken dat meer dan 100.000 gelijktijdige TCP- of UDP-vertalingen bevat.

1. Bepaal de huidige configuratie en het gebruik van de NAT-pool om de behoefte aan uitbreiding te identificeren.

Voorbeeld van uitvoer:

```
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.Schat het aantal IP-adres/poortvertalingen dat nodig is om het gewenste aantal gelijktijdige TCP/UDP-verbindingen op het apparaat te ondersteunen.

Voorbeeld van uitvoer:

<#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.Bepaal of pakketten vallen met reden "nat-xlate-pool-uitgeput" worden verhoogd op het apparaat. Elk IP-adres in een PAT-pool kan doorgaans maximaal 128.000 (gecombineerde TCP- en UDP-poorten) vertalingen ondersteunen. Voor overtollige vertalingen op een bepaald protocol zijn echter meer IP-adressen nodig. Als het apparaat bijvoorbeeld meer dan 100.000 unieke TCP-poortvertalingen weergeeft, zijn ten minste twee IP-adressen vereist, aangezien slechts 64.000 unieke TCP-vertalingen mogelijk zouden zijn op één IP-adres.

Voorbeeld van uitvoer:

<#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.Bepaal hoeveel vertalingen er worden gebruikt voor elke NAT en of ze voornamelijk voor TCP- of UDP-vertalingen zijn. Gebruik een geautomatiseerde parser of syslog / snmp-software om door de uitvoer "Toon details" te parseren en toppraters te verzamelen.

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

Voorbeeld output na AI analyse:

```
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. Breid de NAT-pool uit door een of meer IP-adresgroepen voor het FTD-interfaceverkeer toe te voegen. Raadpleeg de officiële documentatie indien nodig: NAT configureren en verifiëren op FTD

Controleer of het nieuwe adres is toegevoegd.

Voorbeeld van uitvoer na toevoeging:

```
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.Controleer het gebruik van de NAT-pool na uitbreiding van de pool om ervoor te zorgen dat er voldoende vertaalbronnen beschikbaar zijn. Controleren op verkeersfouten en succesvolle gebruikersvertalingen valideren

Voorbeeld van uitvoer:

<#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

Als fouten blijven bestaan of verbindingslimieten worden benaderd, voegt u zo nodig meer adressen toe aan de NAT-pool.

7.Raadpleeg de officiële configuratiehandleiding van Cisco Secure Firewall NAT voor

stapsgewijze instructies en validatieprocedures: PAT Pool configureren op FTD

Als u om welke reden dan ook specifieke lokale-naar-NAT-vertalingen moet bekijken, gebruikt u `show conn` om het opgegeven adres te vinden op het lokale of NAT-IP-adres. De `show nat` commando's zijn niet in staat om dit te doen. De `show conn detail` output kan ook worden omgeleid naar disk0 (/mnt/disk0) voor analyse. Dit is vooral handig voor het matchen van VPN NAT-pools met lokale echte bron-IP's.

```
> 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
```

Oorzaak

Dit probleem wordt veroorzaakt door een ontoereikende NAT-pool voor dynamische vertalingen, waardoor de beschikbare poortvertalingen en IP-bronnen uitgeput raken. Dit beperkt het aantal gelijktijdige TCP/UDP-verbindingen dat kan worden ondersteund, wat leidt tot problemen met de toegang tot het verkeer en de connectiviteit voor scenario's met een hoog volume.

Verwante inhoud

- PAT-pool configureren voor FTD
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.