Configure NAT Pool and Troubleshoot NAT Pool Exhaustion in FTD

Contents

Issue

Users experience access issues for FTD traffic when the NAT pool is not sufficient to translate all necessary user connections. Configuration modification is required to ensure sufficient NAT resources for handling a large number of connections.

Environment

- Cisco Secure Firewall Firepower - applicable to all FTD and ASA models and versions
- High-volume connections (100,000+)

Resolution

To resolve and ensure reliable translation for large volumes of connections, expand the NAT pool for dynamic translation on the Cisco FTD. This is necessary to cover connection counts exceeding to 100,000 concurrent TCP or UDP translations.

1. Determine the current NAT pool configuration and usage to identify the need for expansion.

Example output:

```
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.Estimate the number of IP address/port translations required to support the desired number of concurrent TCP/UDP connections seen on the device.

Example output:

<#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.Determine if packets drops with reason "nat-xlate-pool-exhausted" are incrementing on the device. Each IP address in a PAT pool can typically support up to 128,000 (TCP and UDP ports combined) translations. However, for excessive translations on a certain protocol, more IP addresses are required. For example, if the device shows over 100,000 unique TCP port translations, at least two IP addresses are required as only 64,000 unique TCP translations would be possible on one IP address.

Example output:

<#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.Determine how many translations are being utilized for each NAT and if they are mainly for TCP or UDP translations. Use either an automated parser or syslog/snmp software to parse through the "show xlate detail" output and gather top talkers.

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

Example output after AI analysis:

```
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. Expand the NAT pool by adding one or more IP address pools for the FTD interface traffic. Refer to official documentation as needed: [Configure and Verify NAT on FTD]

Confirm the new address was added.

Example output after addition:

```
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.Monitor the NAT pool usage after expanding the pool to ensure sufficient translation resources are available. Check for traffic errors and validate successful user translations

Example output:

<#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

If errors persist or connection limits are approached, add more addresses to the NAT pool as necessary.

7.For step-by-step instructions and validation procedures, consult the official Cisco Secure Firewall NAT configuration guide: Configure PAT Pool on FTD

If for any reason you need to review specific local-to-NAT translations, use `show conn` to locate the specified address either by its local or NAT IP address. The `show nat` commands are not able to do this. The `show conn detail` output can be redirected to disk0 (/mnt/disk0) for analysis also. This is especially useful for matching VPN NAT pools to local real source IPs.

```
> 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
```

Cause

This issue is caused by an insufficient NAT pool for dynamic translations, resulting in exhaustion of available port translations and IP resources. This limits the number of concurrent TCP/UDP connections that can be supported, causing traffic access and connectivity issues for high-volume scenarios.

Related Content

- Configure PAT Pool on FTD
- Cisco Technical Support & Downloads