NAT-Pool konfigurieren und Fehlerbehebung bei NAT-Pool-Erschöpfung in FTD durchführen

Inhalt

Problem

Bei Benutzern treten Zugriffsprobleme für FTD-Datenverkehr auf, wenn der NAT-Pool nicht ausreicht, um alle erforderlichen Benutzerverbindungen zu übersetzen. Eine Konfigurationsänderung ist erforderlich, um ausreichende NAT-Ressourcen für die Verarbeitung einer großen Anzahl von Verbindungen sicherzustellen.

Umwelt

- Cisco Secure Firewall Firepower - anwendbar auf alle FTD- und ASA-Modelle und -Versionen
- Hochvolumige Verbindungen (über 100.000)

Auflösung

Erweitern Sie den NAT-Pool für dynamische Übersetzungen auf dem Cisco FTD, um bei großen Verbindungsvolumen eine zuverlässige Übersetzung zu gewährleisten. Dies ist erforderlich, um die Anzahl der Verbindungen zu erfassen, die 100.000 gleichzeitige TCP- oder UDP-Übersetzungen übersteigt.

1. Bestimmen Sie die aktuelle Konfiguration und Nutzung des NAT-Pools, um den Erweiterungsbedarf zu ermitteln.

Beispiel:

```
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. Schätzen Sie die Anzahl der IP-Adressen/Port-Umwandlungen, die erforderlich sind, um die gewünschte Anzahl gleichzeitiger TCP/UDP-Verbindungen auf dem Gerät zu unterstützen.

Beispiel:

<#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. Stellen Sie fest, ob Pakete aufgrund der Inkrementierung von "nat-xlate-pool-ausgelaugt" auf dem Gerät verworfen werden. Jede IP-Adresse in einem PAT-Pool kann in der Regel bis zu 128.000 Übersetzungen unterstützen (TCP- und UDP-Ports zusammen). Für übermäßige Übersetzungen in einem bestimmten Protokoll sind jedoch mehr IP-Adressen erforderlich. Zeigt das Gerät beispielsweise mehr als 100.000 eindeutige TCP-Portübersetzungen an, sind mindestens zwei IP-Adressen erforderlich, da nur 64.000 eindeutige TCP-Übersetzungen für eine IP-Adresse möglich wären.

Beispiel:

<#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. Bestimmen Sie, wie viele Übersetzungen für jede NAT verwendet werden und ob diese hauptsächlich für TCP- oder UDP-Übersetzungen verwendet werden. Verwenden Sie entweder einen automatisierten Parser oder eine Syslog-/SNMP-Software, um die Ausgabe von "show xlate detail" zu analysieren und Top-Talkers zu sammeln.

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

Beispielausgabe nach 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. Erweitern Sie den NAT-Pool, indem Sie einen oder mehrere IP-Adresspools für den FTD-Schnittstellenverkehr hinzufügen. Lesen Sie bei Bedarf die offizielle Dokumentation: Konfigurieren und Überprüfen von NAT auf FTD

Bestätigen Sie, dass die neue Adresse hinzugefügt wurde.

Beispielausgabe nach der 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. Überwachen Sie die Nutzung des NAT-Pools, nachdem Sie den Pool erweitert haben, um sicherzustellen, dass ausreichende Übersetzungsressourcen zur Verfügung stehen. Auf Datenverkehrsfehler prüfen und erfolgreiche Benutzerübersetzungen validieren

Beispiel:

<#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

Wenn weiterhin Fehler auftreten oder Verbindungslimits erreicht werden, fügen Sie dem NAT-Pool nach Bedarf weitere Adressen hinzu.

7. Schrittweise Anleitungen und Validierungsverfahren finden Sie im offiziellen Cisco Secure Firewall NAT-Konfigurationsleitfaden: PAT-Pool auf FTD konfigurieren

Wenn Sie aus irgendeinem Grund spezifische Übersetzungen von local-to-NAT überprüfen müssen, verwenden Sie `show conn`, um die angegebene Adresse entweder anhand der lokalen oder der NAT-IP-Adresse zu suchen. Die Befehle `show nat` können dies nicht. Die Ausgabe von `show conn detail` kann zur Analyse auch auf disk0 (/mnt/disk0) umgeleitet werden. Dies ist besonders beim Abgleich von VPN NAT-Pools mit lokalen echten Quell-IPs nützlich.

```
> 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
```

Ursache

Dieses Problem wird durch einen unzureichenden NAT-Pool für dynamische Übersetzungen verursacht, was dazu führt, dass die verfügbaren Portübersetzungen und IP-Ressourcen erschöpft sind. Dies schränkt die Anzahl der gleichzeitig unterstützten TCP/UDP-Verbindungen ein und verursacht bei Szenarien mit hohem Datenverkehrsvolumen Zugriffs- und Verbindungsprobleme.

Verwandte Inhalte

- PAT-Pool auf FTD konfigurieren
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.