配置NAT地址池並排除FTD中的NAT地址池耗盡故障

目錄

問題

當NAT池不足以轉換所有必要的使用者連線時，使用者會遇到FTD流量的訪問問題。需要修改配置以確保有足夠的NAT資源來處理大量連線。

環境

- 思科安全防火牆Firepower — 適用於所有FTD和ASA型號和版本
- 大流量連線（100,000以上）

解析

要解決並確保大量連線的可靠轉換，請在Cisco FTD上展開用於動態轉換的NAT池。如果要覆蓋超過100,000個併發TCP或UDP轉換的連線計數，則必須進行此操作。

1.確定當前的NAT池配置和使用情況，確定擴展需求。

輸出示例：

```
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.估計支援裝置上可見的所需併發TCP/UDP連線數所需的IP地址/埠轉換數。

輸出示例：

<#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.確定裝置上的資料包丟棄原因是否為「nat-xlate-pool-expired」。PAT池中的每個IP地址通常可支援多達128,000個（TCP和UDP埠組合）轉換。但是，對於特定協定上的過度轉換，需要更多的IP地址。例如，如果裝置顯示超過100,000個唯一的TCP埠轉換，則至少需要兩個IP地址，因為一個IP地址上只能進行64,000個唯一的TCP轉換。

輸出示例：

<#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.確定每個NAT使用了多少轉換以及它們是否主要用於TCP或UDP轉換。使用自動分析器或syslog/snmp軟體來分析「show xlate detail」輸出並收集最大流量生成者。

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

AI分析後的輸出示例：

```
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.通過為FTD介面流量新增一個或多個IP地址池來擴展NAT池。請根據需要參閱官方文檔：[在FTD上設定和驗證NAT]

確認已新增新地址。

加法後的輸出示例：

```
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.在擴展池後監控NAT池使用情況，以確保有足夠的轉換資源可用。檢查通訊錯誤並驗證成功的使用者轉換

輸出示例：

<#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

如果錯誤持續或接近連線限制，請根據需要向NAT池中新增更多地址。

7.有關逐步說明和驗證過程，請參閱官方的Cisco安全防火牆NAT配置指南：在FTD上設定PAT池

如果出於任何原因，您需要檢視特定的本地到NAT轉換，請使用show conn按指定地址的本地或NAT IP地址查詢該地址。show nat命令無法執行此操作。show conn detail輸出還可以重定向到disk0(/mnt/disk0)進行分析。這對於將VPN NAT池與本地實際源IP匹配尤其有用。

```
> 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
```

原因

此問題是由用於動態轉換的NAT池不足導致可用埠轉換和IP資源耗盡引起的。這會限制可支援的併發TCP/UDP連線的數量，導致大流量場景中的流量訪問和連線問題。

相關內容

- 在FTD上設定PAT池
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。