FTDでのNATプールの設定とNATプール枯渇のトラブルシューティング

内容

お問い合わせ内容

必要なユーザ接続をすべて変換するのにNATプールでは不十分な場合、FTDトラフィックのアクセスの問題が発生します。多数の接続を処理するために十分なNATリソースを確保するには、設定の変更が必要です。

環境

- Cisco Secure Firewall Firepower：すべてのFTDおよびASAモデルとバージョンに適用可能
- 大容量接続（100,000以上）

解決策

大量の接続を解決し、信頼性の高い変換を実現するには、Cisco FTDでダイナミック変換のNATプールを拡張します。これは、同時TCPまたはUDP変換が100,000を超える接続カウントをカバーするために必要です。

1. 現在のNATプールの設定と使用状況を確認して、拡張の必要性を特定します。

出力例：

```
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. デバイスで認識されるTCP/UDP同時接続の希望数をサポートするために必要なIPアドレス/ポート変換の数を見積もります。

出力例：

<#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. デバイスで「nat-xlate-pool-exhausted」の理由によるパケットドロップが増加しているかどうかを判別します。PATプールの各IPアドレスは、通常、最大128,000の変換（TCPポートとUDPポートを組み合わせたもの）をサポートできます。ただし、特定のプロトコルでの過剰な変換には、より多くのIPアドレスが必要です。たとえば、デバイスに100,000を超える一意のTCPポート変換が表示されている場合、1つのIPアドレスで64,000個の一意のTCP変換が可能であるため、少なくとも2つのIPアドレスが必要です。

出力例：

<#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. 各NATで使用されている変換の数と、主にTCPまたはUDPの変換に使用されている変換の数を確認します。自動パーサーまたはsyslog/snmpソフトウェアを使用して、「show xlate detail」出力を解析し、トップトーカーを収集します。

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

AI解析後の出力例：

```
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. FTDインターフェイストラフィック用の1つ以上のIPアドレスプールを追加して、NATプールを拡張します。必要に応じて、公式ドキュメント「FTDでのNATの設定と確認」を参照してください。

新しい住所が追加されたことを確認します。

追加後の出力例：

```
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. プールを拡張した後にNATプールの使用状況を監視し、十分な変換リソースが使用可能であることを確認します。トラフィックエラーを確認し、正常なユーザ変換を検証する

出力例：

<#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

エラーが続く場合、または接続制限に近づく場合は、必要に応じてNATプールにアドレスを追加します。

7. 詳細手順と検証手順については、公式の『Cisco Secure Firewall NAT configuration guide: Configure PAT Pool on FTD』を参照してください。

何らかの理由で、特定のローカルからNATへの変換を確認する必要がある場合は、`show conn`を使用して、ローカルまたはNAT IPアドレスによって指定のアドレスを見つけます。`show nat`コマン

ドでは、この設定は行えません。show conn detailの出力も、分析のためにdisk0(/mnt/disk0)にリダイレクトできます。これは、VPN NATプールをローカルの実際の送信元のIPと一致させる場合に特に便利です。

```
> 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

この問題は、ダイナミック変換のためのNATプールが不十分で、使用可能なポート変換とIPリソースの枯渇が原因で発生します。これにより、同時にサポート可能なTCP/UDP接続数が制限され、大量のシナリオでトラフィックアクセスと接続の問題が発生します。

関連コンテンツ

- FTDでのPATプールの設定
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。