在FTD中配置NAT池并排除NAT池耗尽故障

目录

问题

当NAT池不足以转换所有必需的用户连接时，用户会遇到FTD流量的访问问题。需要修改配置，以确保有足够的NAT资源用于处理大量连接。

环境

- 思科安全防火墙Firepower — 适用于所有FTD和ASA型号和版本
- 大容量连接（100,000以上）

分辨率

要解决并确保大量连接的可靠转换，请在Cisco FTD上展开用于动态转换的NAT池。为了将连接计数超过100,000个并发TCP或UDP转换，必须执行此操作。

1.确定当前的NAT池配置和使用情况，确定扩展需求。

示例输出：

```
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.估计为支持设备上可见的所需并发TCP/UDP连接数所需的IP地址/端口转换数。

示例输出：

<#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.确定数据包丢弃原因为“nat-xlate-pool-exhausted”是否在设备上增加。PAT池中的每个IP地址通常可支持多达128,000个（TCP和UDP端口组合）转换。但是，对于特定协议上的过度转换，需要更多IP地址。例如，如果设备显示超过100,000个唯一的TCP端口转换，则至少需要两个IP地址，因为一个IP地址上只能进行64,000个唯一的TCP转换。

示例输出：

<#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.确定每个NAT使用了多少转换，以及它们主要用于TCP还是UDP转换。使用自动解析器或syslog/snmp软件来解析整个“show xlate detail”输出并收集最大流量生成者。

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

AI分析后的输出示例：

```
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.通过为FTD接口流量添加一个或多个IP地址池来扩展NAT池。请根据需要参阅官方文档：[在 FTD 上配置和验证 NAT]

确认已添加新地址。

加法后的输出示例：

```
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.在扩展池后监控NAT池使用情况，以确保有足够的转换资源可用。检查流量错误并验证成功的用户转换

示例输出：

<#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
```

如果错误持续或接近连接限制，请根据需要向NAT池添加更多地址。

7.有关分步说明和验证过程，请参阅官方的Cisco安全防火墙NAT配置指南：在FTD上配置PAT池

如果出于任何原因需要查看特定的本地到NAT转换，请使用show conn通过指定地址的本地或NAT IP地址查找该地址。show nat命令无法执行此操作。show conn detail输出也可以重定向到disk0(/mnt/disk0)进行分析。这对于将VPN NAT池与本地实际源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

此问题是由用于动态转换的NAT池不足导致可用端口转换和IP资源耗尽引起的。这会限制可支持的并发TCP/UDP连接的数量，导致大量场景出现流量访问和连接问题。

相关内容

- 在FTD上配置PAT池
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。