FTD에서 NAT 풀 구성 및 NAT 풀 소모 문제 해결

목차

문제

NAT 풀이 필요한 모든 사용자 연결을 변환하기에 충분하지 않을 때 사용자는 FTD 트래픽에 대한 액세스 문제를 경험합니다. 많은 수의 연결을 처리할 수 있도록 충분한 NAT 리소스를 보장하려면 컨피그레이션을 수정해야 합니다.

환경

- Cisco Secure Firewall Firepower - 모든 FTD 및 ASA 모델 및 버전에 적용 가능
- 대용량 연결(100,000개 이상)

해결

대량의 연결에 대한 안정적인 변환을 확인하고 보장하려면 Cisco FTD에서 동적 변환용 NAT 풀을 확장합니다. 이는 동시 TCP 또는 UDP 변환 100,000개를 초과하는 연결 수를 다루는 데 필요합니다.

1. 확장의 필요성을 파악하기 위해 현재 NAT 풀 컨피그레이션 및 사용을 결정합니다.

출력 예:

```
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. 디바이스에서 원하는 수의 동시 TCP/UDP 연결을 지원하는 데 필요한 IP 주소/포트 변환 수를 추정합니다.

출력 예:

<#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. 디바이스에서 "nat-xlate-pool-exhausted"라는 이유로 패킷이 삭제되는지 확인합니다. PAT 풀의 각 IP 주소는 일반적으로 최대 128,000개(TCP 및 UDP 포트 결합) 변환을 지원할 수 있습니다. 그러나 특정 프로토콜에서 과도한 변환을 수행하려면 더 많은 IP 주소가 필요합니다. 예를 들어 디바이스에서 100,000개 이상의 고유한 TCP 포트 변환을 표시할 경우, 하나의 IP 주소에서 64,000개의 고유한 TCP 변환만 가능하므로 최소 2개의 IP 주소가 필요합니다.

출력 예:

<#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. 각 NAT에 대해 사용되고 있는 변환 수 및 주로 TCP 또는 UDP 변환에 사용되는 변환을 결정합니다. 자동 파서 또는 syslog/snmp 소프트웨어를 사용하여 "show xlate detail" 출력을 통해 구문 분석하고 상위 토커를 수집합니다.

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

AI 분석 후 출력 예:

```
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 인터페이스 트래픽에 대해 하나 이상의 IP 주소 풀을 추가하여 NAT 풀을 확장합니다. 필요에 따라 공식 문서를 참조하십시오. FTD에서 NAT 구성 및 확인

새 주소가 추가되었는지 확인합니다.

추가 후 출력 예:

```
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. 충분한 변환 리소스를 사용할 수 있도록 풀을 확장한 후 NAT 풀 사용을 모니터링합니다. 트래픽 오류를 확인하고 성공한 사용자 변환 확인

출력 예:

<#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

오류가 지속되거나 연결 제한에 도달할 경우 필요에 따라 NAT 풀에 주소를 더 추가합니다.

7. 단계별 지침 및 검증 절차에 대해서는 공식 Cisco Secure Firewall NAT 컨피그레이션 가이드를 참조하십시오. FTD에서 PAT 풀 구성

어떤 이유로든 특정 local-to-NAT 변환을 검토해야 하는 경우 `show conn`을 사용하여 로컬 또는 NAT IP 주소로 지정된 주소를 찾습니다. show `nat` 명령은 이 작업을 수행할 수 없습니다. show `conn detail` 출력은 분석을 위해 disk0(/mnt/disk0)으로 리디렉션될 수도 있습니다. 이는 VPN NAT 풀을 로컬 실제 소스 IP와 일치시킬 때 특히 유용합니다.

```
> 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
```

원인

이 문제는 동적 변환에 대한 NAT 풀이 부족하여 사용 가능한 포트 변환 및 IP 리소스가 소진되었기 때문에 발생합니다. 이렇게 하면 지원 가능한 동시 TCP/UDP 연결 수가 제한되므로 대용량 시나리오에서 트래픽 액세스 및 연결 문제가 발생합니다.

관련 콘텐츠

- FTD에서 PAT 풀 구성
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.