Configurar o pool NAT e solucionar problemas de esgotamento do pool NAT no FTD

Contents

Problema

Os usuários experimentam problemas de acesso para o tráfego de FTD quando o pool de NAT não é suficiente para converter todas as conexões de usuário necessárias. A modificação da configuração é necessária para garantir recursos NAT suficientes para lidar com um grande número de conexões.

Ambiente

- Cisco Secure Firewall Firepower - aplicável a todos os modelos e versões de FTD e ASA
- Conexões de alto volume (mais de 100.000)

Resolução

Para resolver e garantir a conversão confiável para grandes volumes de conexões, expanda o pool NAT para conversão dinâmica no Cisco FTD. Isso é necessário para cobrir as contagens de conexões que excedem 100.000 conversões simultâneas de TCP ou UDP.

1. Determine a configuração e o uso atuais do pool NAT para identificar a necessidade de expansão.

Saída de exemplo:

```
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. Estime o número de conversões de endereço IP/porta necessárias para suportar o número desejado de conexões TCP/UDP simultâneas vistas no dispositivo.

Saída de exemplo:

<#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. Determine se os pacotes caem com o motivo "nat-xlate-pool-excluded" estão aumentando no dispositivo. Cada endereço IP em um pool PAT pode suportar até 128.000 conversões (portas TCP e UDP combinadas). No entanto, para conversões excessivas em um determinado protocolo, são necessários mais endereços IP. Por exemplo, se o dispositivo mostrar mais de 100.000 conversões de porta TCP exclusivas, pelo menos dois endereços IP serão necessários, pois somente 64.000 conversões TCP exclusivas seriam possíveis em um endereço IP.

Saída de exemplo:

<#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. Determine quantas conversões estão sendo utilizadas para cada NAT e se elas são principalmente para conversões TCP ou UDP. Use um analisador automatizado ou um software syslog/snmp para analisar a saída "show xlate detail" e reunir os principais locutores.

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

Exemplo de saída após a análise de IA:

```
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. Expanda o pool NAT adicionando um ou mais pools de endereços IP para o tráfego da interface FTD. Consulte a documentação oficial conforme necessário: Configurar e verificar o NAT no FTD

Confirme se o novo endereço foi adicionado.

Exemplo de saída após adição:

```
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. Monitore o uso do pool de NAT depois de expandir o pool para garantir que recursos de conversão suficientes estejam disponíveis. Verificar erros de tráfego e validar conversões de usuário bem-sucedidas

Saída de exemplo:

<#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

Se os erros persistirem ou os limites de conexão forem abordados, adicione mais endereços ao pool NAT conforme necessário.

7. Para obter instruções passo a passo e procedimentos de validação, consulte o guia de configuração oficial do Cisco Secure Firewall NAT: Configurar o pool PAT no FTD

Se, por algum motivo, você precisar revisar conversões locais para NAT específicas, use `show conn` para localizar o endereço especificado pelo endereço IP local ou NAT. Os comandos `show nat` não podem fazer isso. A saída de `show conn detail` também pode ser redirecionada para disk0 (/mnt/disk0) para análise. Isso é especialmente útil para combinar pools de NAT de VPN com IPs de origem real locais.

```
> 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
```

Causa

Esse problema é causado por um pool de NAT insuficiente para conversões dinâmicas, resultando no esgotamento das conversões de porta disponíveis e dos recursos IP. Isso limita o número de conexões TCP/UDP simultâneas que podem ser suportadas, causando problemas de conectividade e acesso ao tráfego para cenários de alto volume.

Conteúdo relacionado

- Configurar o pool PAT no FTD
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.