Configuración del conjunto NAT y solución de problemas de agotamiento del conjunto NAT en FTD

Contenido

Problema

Los usuarios experimentan problemas de acceso para el tráfico FTD cuando el conjunto NAT no es suficiente para traducir todas las conexiones de usuario necesarias. La modificación de la configuración es necesaria para garantizar suficientes recursos NAT para gestionar un gran número de conexiones.

Entorno

- Cisco Secure Firewall Firepower: aplicable a todos los modelos y versiones de FTD y ASA
- Conexiones de gran volumen (más de 100 000)

Resolución

Para resolver y garantizar una traducción confiable para grandes volúmenes de conexiones, expanda el conjunto NAT para la traducción dinámica en el FTD de Cisco. Esto es necesario para cubrir los recuentos de conexiones que exceden de 100,000 traducciones TCP o UDP simultáneas.

1. Determine la configuración y el uso actuales del conjunto NAT para identificar la necesidad de expansión.

Ejemplo de salida:

```
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. Calcule el número de traducciones de puertos/direcciones IP necesarias para admitir el número deseado de conexiones TCP/UDP simultáneas que se ven en el dispositivo.

Ejemplo de salida:

<#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 si los paquetes se descartan con la razón "nat-xlate-pool-exhausto" están aumentando en el dispositivo. Cada dirección IP de un grupo PAT suele admitir hasta 128 000 traducciones (puertos TCP y UDP combinados). Sin embargo, para traducciones excesivas en un protocolo determinado, se requieren más direcciones IP. Por ejemplo, si el dispositivo muestra más de 100.000 traducciones de puertos TCP únicas, se requieren al menos dos direcciones IP, ya que sólo 64.000 traducciones TCP únicas serían posibles en una dirección IP.

Ejemplo de salida:

<#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 cuántas traducciones se están utilizando para cada NAT y si son principalmente para traducciones TCP o UDP. Utilice un analizador automatizado o el software syslog/snmp para analizar la salida "show xlate detail" y reunir a los usuarios más activos.

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

Ejemplo de salida después del análisis 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 el conjunto NAT agregando uno o más conjuntos de direcciones IP para el tráfico de interfaz FTD. Consulte la documentación oficial según sea necesario: Configuración y verificación de NAT en FTD

Confirme que se ha agregado la nueva dirección.

Ejemplo de salida después de la adición:

```
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. Supervise el uso del conjunto NAT después de ampliar el conjunto para asegurarse de que haya suficientes recursos de traducción disponibles. Comprobar los errores de tráfico y validar las traducciones de usuario correctas

Ejemplo de salida:

<#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

Si persisten los errores o se alcanzan los límites de conexión, agregue más direcciones al conjunto NAT según sea necesario.

7. Para obtener instrucciones paso a paso y procedimientos de validación, consulte la guía de configuración oficial de NAT de Cisco Secure Firewall: Configuración del conjunto PAT en FTD

Si por alguna razón necesita revisar traducciones específicas de local a NAT, utilice `show conn` para localizar la dirección especificada por su dirección IP local o NAT. Los comandos `show nat` no pueden hacer esto. El resultado de `show conn detail` también se puede redirigir a disk0 (/mnt/disk0) para su análisis. Esto es especialmente útil para hacer coincidir los grupos de NAT de VPN con las IP de origen real locales.

```
> 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

Este problema es causado por un conjunto de NAT insuficiente para las traducciones dinámicas, lo que resulta en el agotamiento de las traducciones de puertos disponibles y los recursos IP. Esto limita el número de conexiones TCP/UDP simultáneas que se pueden admitir, lo que causa problemas de conectividad y acceso al tráfico en escenarios de gran volumen.

Contenido relacionado

- Configuración del conjunto PAT en FTD
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).