Configurer le pool NAT et dépanner l'épuisement du pool NAT dans FTD

Table des matières

Problème

Les utilisateurs rencontrent des problèmes d'accès pour le trafic FTD lorsque le pool NAT n'est pas suffisant pour traduire toutes les connexions utilisateur nécessaires. Une modification de la configuration est nécessaire pour garantir des ressources NAT suffisantes pour gérer un grand nombre de connexions.

Environnement

- Cisco Secure Firewall Firepower - applicable à tous les modèles et versions FTD et ASA
- Connexions à grand volume (plus de 100 000)

Résolution

Pour résoudre et assurer une traduction fiable pour de grands volumes de connexions, étendez le pool NAT pour la traduction dynamique sur le FTD Cisco. Cela est nécessaire pour couvrir les nombres de connexions dépassant 100 000 traductions TCP ou UDP simultanées.

1. Déterminez la configuration et l’utilisation actuelles du pool NAT afin d’identifier le besoin d’extension.

Exemple de rapport :

```
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.Estimez le nombre de traductions d'adresses IP/ports nécessaires pour prendre en charge le nombre souhaité de connexions TCP/UDP simultanées sur le périphérique.

Exemple de rapport :

<#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. Déterminez si les abandons de paquets avec la raison « nat-xlate-pool-used » sont incrémentés sur le périphérique. Chaque adresse IP d'un pool PAT peut généralement prendre en charge jusqu'à 128 000 traductions (ports TCP et UDP combinés). Cependant, pour des traductions excessives sur un certain protocole, plus d'adresses IP sont nécessaires. Par exemple, si le périphérique affiche plus de 100 000 traductions de ports TCP uniques, au moins deux adresses IP sont requises, car seules 64 000 traductions TCP uniques sont possibles sur une adresse IP.

Exemple de rapport :

<#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. Déterminez le nombre de traductions utilisées pour chaque NAT et si elles concernent principalement les traductions TCP ou UDP. Utilisez un analyseur automatique ou un logiciel syslog/snmp pour analyser la sortie « show xlate detail » et rassembler les principaux locuteurs.

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

Exemple de résultat après analyse AI :

```
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. Développez le pool NAT en ajoutant un ou plusieurs pools d'adresses IP pour le trafic d'interface FTD. Reportez-vous à la documentation officielle si nécessaire : Configuration et vérification de la fonction NAT sur FTD

Confirmez que la nouvelle adresse a été ajoutée.

Exemple de sortie après addition :

```
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. Surveillez l'utilisation du pool NAT après avoir étendu le pool pour vous assurer que des ressources de traduction suffisantes sont disponibles. Vérifier les erreurs de trafic et valider les traductions utilisateur réussies

Exemple de rapport :

<#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 des erreurs persistent ou si des limites de connexion sont approchées, ajoutez d'autres adresses au pool NAT, si nécessaire.

7.Pour obtenir des instructions détaillées et des procédures de validation, consultez le guide de configuration officiel de la fonction NAT de Cisco Secure Firewall : Configurer le pool PAT sur FTD

Si, pour une raison quelconque, vous avez besoin de réviser des traductions locales-NAT spécifiques, utilisez `show conn` pour localiser l'adresse spécifiée soit par son adresse IP locale ou NAT. Les commandes `show nat` ne peuvent pas faire cela. La sortie `show conn detail` peut être redirigée vers disk0 (/mnt/disk0) pour analyse également. Cela est particulièrement utile pour faire correspondre des pools NAT VPN à des adresses IP source réelles 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
```

Motif

Ce problème est dû à un pool NAT insuffisant pour les traductions dynamiques, ce qui entraîne l'épuisement des traductions de port et des ressources IP disponibles. Cela limite le nombre de connexions TCP/UDP simultanées pouvant être prises en charge, ce qui entraîne des problèmes d'accès au trafic et de connectivité pour les scénarios à volume élevé.

Autres informations utiles

- Configurer le pool PAT sur FTD
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.