تكوين تجمع NAT واستكشاف أخطاء تجميع NAT وإصلاحها في FTD

المحتويات

مسألة

يواجه المستخدمون مشاكل في الوصول لحركة مرور FTD عندما ال يكون تجمع NAT كافي لترجمة جميع إتصالات المستخدم الضرورية. يلزم تعديل التكوين لضمان وجود موارد كافية من NAT لمعالجة عدد كبير من الاتصالات.

البيئة

- ASA و FTD تارادصإلاو زرطلا عيمج ىلع قيبطتلل لباق - Cisco نم نمآلا ةيامحلا رادج
- (100000 نم رثكأ) مجحلا ريبك تالاصتإ

قرار

لحل وضمان الترجمة الموثوقة لوحدات التخزين الكبيرة من الاتصالات، قم بتوسيع تجمع NAT للترجمة الديناميكية على Cisco FTD. هذا ضروري لتغطية عدد الاتصالات التي تتجاوز 100000 ترجمة TCP أو UDP متزامنة.

1. تحديد تكوين تجمع NAT الحالي واستخدامه لتحديد الحاجة إلى التوسيع.

مثال الإخراج:

```
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
```

تالاصتإ نم بوغرملا ددعلا مءلد ةبولطملا IP ذفانم/نيوانع تامجرت ددع ريدقتب مق.2
زاهجلا ىلع اهتيؤر متي يتلا ةنمازتملا TCP/UDP.

جارخإلا لاثم:

<#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
```

نأ نكمي .زاهجلا ىلع ديازتي "nat-xlate-pool-exhausted" ببسل طقست مزحلا تناك اذإ ام ددح.3
UDP و TCP ذفانم) ةمجرت 128000 ىلإ لصي ام صاخ لكشب PAT عمجت يف IP ناونع لك مءدي
نيوانع نم ديزملا مزلي ،نيعم لوكوتورب ىلع ةدئازلا تامجرتلا نم ديزمل ،كلذ عمو .(ةعمتجم
مزلي ،TCP ذفنمل ةديرف ةمجرت 100000 نع ديزي ام زاهجلا رهظأ اذإ ،لاثملا ليبس ىلع .IP
ىلع ةديرف TCP ةمجرت 64000 ىوس ءارجإ نكمي ال هنأل ارظن IP ل لقألا ىلع نيناونع رفوت
دحاو IP ناونع.

جارخإلا لاثم:

<#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.حدد عدد الترجمات التي يتم إستخدامها لكل NAT وما إذا كانت تستخدم بشكل رئيسي لترجمات TCP أو UDP. أستخدم إما محلل آلي أو برنامج syslog/snmp لتحليل الإخراج "show xlate detail" وتجميع المتكاملات العليا.

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

مثال إخراج بعد تحليل 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. قم بتوسيع تجمع NAT عن طريق إضافة تجمع عنوان IP واحد أو أكثر لحركة مرور واجهة FTD. راجع الوثائق الرسمية حسب الحاجة: [تكوين NAT والتحقق من صحته على FTD]

تأكيد إضافة العنوان الجديد.

مثال إخراج بعد الإضافة:

```
                                                                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.مراقبة إستخدام تجمع NAT بعد توسيع التجمع لضمان توفر موارد ترجمة كافية. التحقق من أخطاء حركة المرور والتحقق من صحة ترجمات المستخدم الناجحة

مثال الإخراج:

<#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
```

إذا إستمرت الأخطاء أو اقتربت من حدود الاتصال، فقم بإضافة المزيد من العناوين إلى تجمع NAT حسب الضرورة.

7. للحصول على تعليمات خطوة بخطوة وإجراءات التحقق من الصحة، راجع دليل التكوين الرسمي ل Cisco Secure Firewall NAT: [تكوين تجمع PAT على FTD]

إن يحتاج أنت لأي سبب أن يراجع خاص محلي إلى nat ترجمة، استعملت عرض conn أن يعين عنوان إما بمحلي أو nat عنوان. يتعذر على أوامر show nat القيام بذلك. يمكن إعادة توجيه إخراج تفاصيل show conn إلى disk0 (/mnt/disk0) للتحليل أيضا. وهذا مفيد بشكل خاص لمطابقة

تجمعات NAT الخاصة بشبكة VPN إلى عناوين IP للمصدر الحقيقي المحلي.

```
                                                    > 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
```

السبب

يرجع هذا إلى إصدار إلى تجمع NAT غير كاف للترجمات الديناميكية، مما يؤدي إلى إستهلاك ترجمات المنفذ المتاحة ومواردIP. وهذا يحد من عدد إتصالات TCP/UDP المتزامنة التي يمكن دعمها، مما يتسبب في حدوث مشاكل في الوصول إلى حركة المرور والاتصال لسيناريوهات كبيرة الحجم.

المحتوى ذي الصلة

- تكوين تجمع PAT على FTD
- الدعم الفني والتنزيلات من Cisco

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).