أستكشاف أخطاء Traceroute من FTD التي ال تعرض معلومات النقلة رغم إختبار اتصال ICMP الناجح

مسألة

ك ل هذه االعراض تظهر:

- فشل Traceroute: ال تعود أوامر traceroute التي يتم بدء تشغيلها مباشرة من جهاز (FTD) من Cisco بشكل ثابت إال * * * لجميع التنقالت الدفاع عن تهديد جدار الحماية عنوانين IP الخارجية.
- إمكانية اتصال ناجحة: تكون إختبارات اتصال ICMP إلى الوجهة نفسها ناجحة، ويتم السماح بحركة مرور ICMP بشكل صريح في سياسة التحكم في الوصول.

FTD، يمنع هذا السلوك إمكانية الرؤية في نقالت المسار لحركة المرور التي تنشأ من جهاز مما يؤثر على جهود أستكشاف أخطاء مسار الشبكة وإصالحها.

مثال

إختبار االتصال إلى الوجهة يعمل:

```
<#root>

firepower#

ping 192.168.203.89

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.203.89, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

ولكن traceroute ليس:

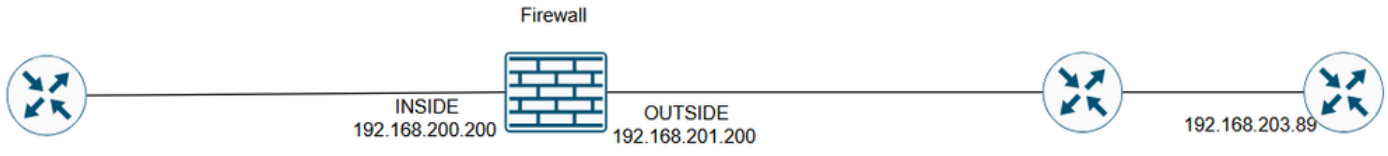
```
<#root>
```

```
firepower#

traceroute 192.168.203.89

Type escape sequence to abort.
Tracing the route to 192.168.203.89
  1*  *  *
  2*  *  *
  3*  *  *
  ...
 30*  *  *
firepower#
```

البيئة

- الدفاع الآمن عن تهديد جدار الحماية (FTD) من Cisco.
- ولوحظ أول مرة في: 7-4 و 7-4-2-3 و 7-6-2، ويمكن أن تتأثر أيضا نسخ أخرى.
- مركز إدارة جدار الحماية الآمن من Cisco (FMC / CDfmc / FDM) للإدارة.
- قواعد NAT الثابتة قيد الاستخدام، بما في ذلك التكوينات ثنائية الإتجاه.
- تم تنفيذ أوامر traceroute من FTD CLI (وضع Lina).
- ICMP المسموح به في سياسة التحكم في الوصول.

المخطط



inline_image_0.png

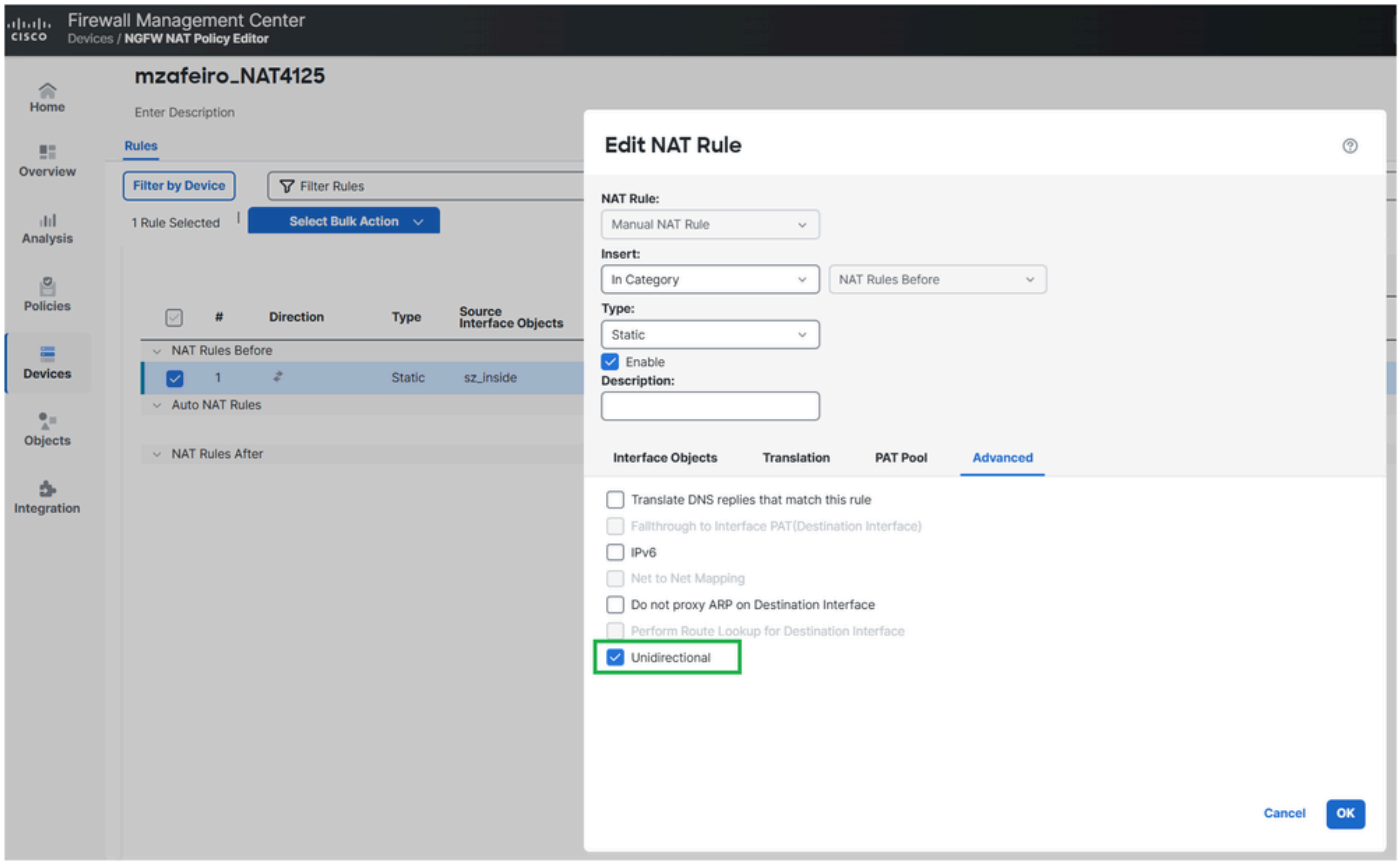
قرار

تعتمد الحلول الممكنة على الغرض من قاعدة NAT التي تم تكوينها.

الحل 1

إن كان الهدف أن يترجم الداخلي نادل ip فقط ل وصول خارج أنت يستطيع شكلت ال nat قاعدة بما أن أحادي إتجاه.

على FMC، يمكن القيام بذلك من الخيارات المتقدمة لقاعدة NAT:



inline_image_0.png

تكوين NAT المنشور:

<#root>

```
firepower#

show run nat

nat (INSIDE,OUTSIDE) source static server_host interface unidirectional
firepower#
```

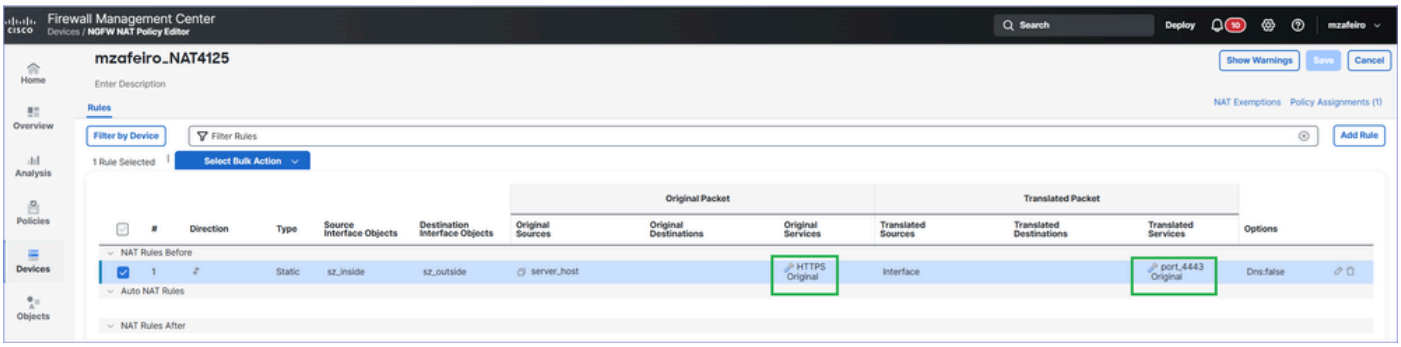
التحقق

<#root>

```
firepower#

traceroute 192.168.203.89


Type escape sequence to abort.
Tracing the route to 192.168.203.89
1  192.168.201.88 2 msec 2 msec 2 msec
 2  192.168.203.89 1 msec *  1 msec
```

الحل 2

إن يكون الهدف لنادل داخلي أن يكون reachable من الخارج بعد ذلك أنت يستطيع جعلت الـ nat قاعدة أكثر تحديدا ب يشكل ميناء forwarding:



inline_image_0.png

تكوين NAT المنشور:

<#root>

```
firepower#

show run nat


nat (INSIDE,OUTSIDE) source static server_host interface service SVC_25769850586 SVC_25769850587
```

التحقق

```
<#root>

firepower#

traceroute 192.168.203.89

Type escape sequence to abort.
Tracing the route to 192.168.203.89
1  192.168.201.88 2 msec 2 msec 2 msec
2  192.168.203.89 1 msec *  1 msec
```

كيف يعمل

كيف يعمل

بينغ

1. يرسل جدار الحماية رسالة طلب صدى (ICMP النوع 8 الرمز 0).
2. يتم إنشاء اتصال جدار حماية جديد ل ICMP
3. يستلم جدار الحماية رسالة رد على الارتداد (رمز ICMP من النوع 0)
4. تطابق الرسالة الاتصال الذي تم إنشاؤه في الخطوة 2
5. رسالة الرد على الارتداد مستهلكة بواسطة جدار الحماية

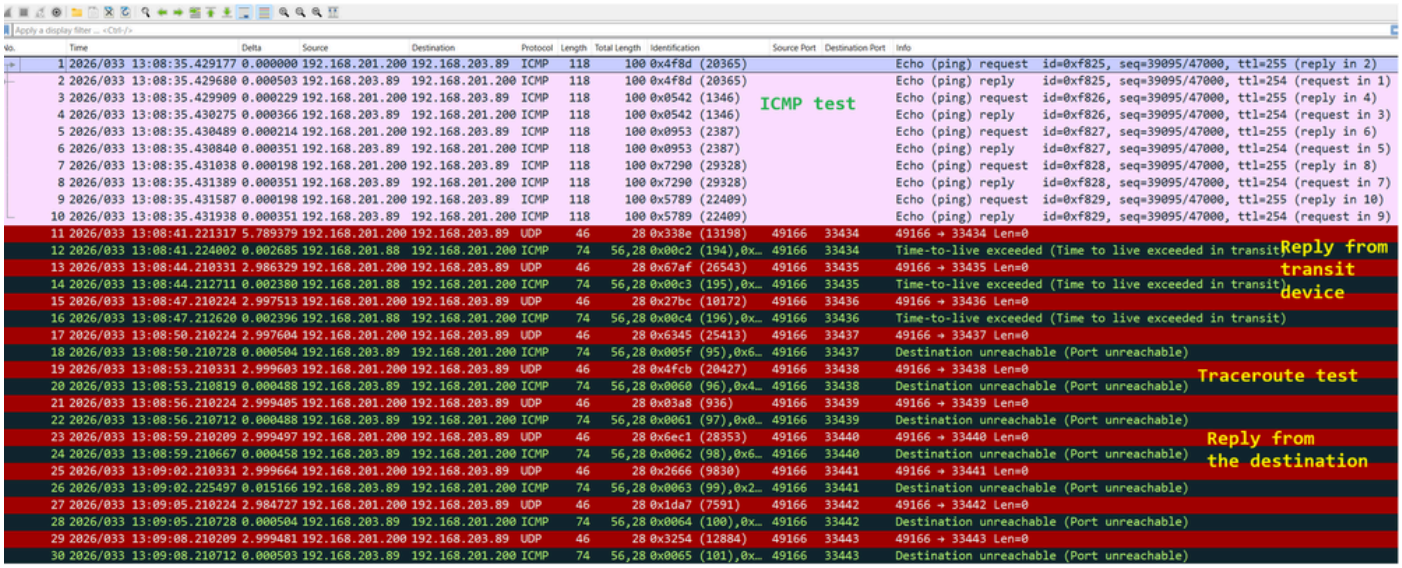
traceroute

1. يرسل جدار الحماية ثلاث حزم UDP بدءا من المنفذ، 33434 و 33435 و 33436 نحو الوجهة مع TTL 1.
2. يتم إنشاء اتصال جدار حماية جديد ل UDP

3. أو (النوع 11 الرمز 0) ICMP TTL الذي تم تجاوزه أثناء النقل يستقبل جدار الحماية إما منفذ ICMP الذي يتعذر الوصول إليه (النوع 3 الرمز 3).

4. بمجرد وصول حزم ICMP إلى جدار الحماية، يتم معالجتها كإتصالات مختلفة عن حزم UDP من الخطوة 2.

وبوسعنا أن نرى هذا في ويريشارك:



inline_image_0.png

استكشاف الأخطاء وإصلاحها

الخطوة 1

مكنت ربط على جدار مانع للحريق مخرج قارن مع تتبع أن يرى كيف جدار الحماية يعالج المدخل ربط:

<#root>

firepower#

capture CAPI trace interface OUTSIDE match ip host 192.168.203.89 host 192.168.201.100

الخطوة 2

الاختبار باستخدام إختبار الاتصال:

```
<#root>

                                                                firepower#

                                                          ping 192.168.203.89


                                                  Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.203.89, timeout is 2 seconds:
                                                                      !!!!!
   Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ثم اختبر مع traceroute:

```
<#root>

                                                                firepower#

                                                       traceroute 192.168.203.89


                                                  Type escape sequence to abort.
                                               Tracing the route to 192.168.203.89
                                                                     1*  *  *
                                                                     2*  *  *
                                                                     3*  *  *
                                                                     4*  *  *
                                                                     5*  *  *
                                                                     6*  *  *
                                                                     7*  *  *
                                                                        …
```

الخطوة 3

تحقق من محتويات الالتقاط:

- تتصل الحزم 1-10 باختبار إختبار اتصال ICMP.
- الرابط 11-16 مرتبطة ب traceroute. الردود من الخطوة الأولى.

- ربط ربط 17-28 أيضا traceroute. الردود من الغاية نهاية نقطة.

```
<#root>

                                                                firepower#

                                                      show capture CAPI

                                                                190 packets captured
  1: 13:50:27.345471       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
    2: 13:50:27.345975       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
  3: 13:50:27.346219       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
    4: 13:50:27.346600       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
  5: 13:50:27.346814       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
    6: 13:50:27.347165       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
  7: 13:50:27.347378       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
    8: 13:50:27.347714       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
  9: 13:50:27.347928       802.1Q vlan#201 P0 192.168.201.200 > 192.168.203.89 icmp: echo request
   10: 13:50:27.348279       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
11: 13:50:33.229724       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33434:  udp 0
12: 13:50:33.232562       802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tra
13: 13:50:36.220279       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33435:  udp 0
14: 13:50:36.222827       802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tra
15: 13:50:39.220172       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33436:  udp 0
16: 13:50:39.222675       802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tra
17: 13:50:42.220157       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33437:  udp 0
18: 13:50:42.220737       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
19: 13:50:45.220264       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33438:  udp 0
20: 13:50:45.220752       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
21: 13:50:48.220157       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33439:  udp 0
22: 13:50:48.220645       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
23: 13:50:51.220157       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33440:  udp 0
24: 13:50:51.220645       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
25: 13:50:54.220264       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33441:  udp 0
26: 13:50:54.220752       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
27: 13:50:57.220157       802.1Q vlan#201 P0 192.168.201.200.49168 > 192.168.203.89.33442:  udp 0
28: 13:50:57.220645       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: 192.168.203.89 udp
```

الخطوة 4

قم بتتبع حزم ICMP الخاصة بالمدخل من إختبار الاتصال.

.#1 الحزمة في المرسل ICMP اتصال إختبار على طلب الرد هي #2 الحزمة

```
<#root>

                                                                firepower#

                                                      show capture CAPI packet-number 2 trace
```

```
                                                                190 packets captured
   2: 13:50:27.345975       802.1Q vlan#201 P0 192.168.203.89 > 192.168.201.200 icmp: echo reply
                                                                                …
                                                                         Phase: 4
                                                                Type: FLOW-LOOKUP
                                                                         Subtype:
                                                                Result: ALLOW
                                                            Elapsed time: 488 ns
                                                                         Config:
                                                            Additional Information:
                                                Found flow with id 143799, using existing flow
                                                                                …
                                                                         Phase: 6
                                                            Type: ADJACENCY-LOOKUP
                                                Subtype: Resolve Nexthop IP address to MAC
                                                                Result: ALLOW
                                                            Elapsed time: 1952 ns
                                                                         Config:
                                                            Additional Information:
                                    Found adjacency entry for Next-hop 0.0.0.0 on interface  identity
                                                                Adjacency :Active
                                    MAC address 0000.0000.0000 hits 483359 reference 2

                                                                         Result:
                                                        input-interface: OUTSIDE(vrfid:0)
                                                                input-status: up
                                                            input-line-status: up
                                                        output-interface: NP Identity Ifc
                                                                Action: allow
                                                            Time Taken: 18056 ns
                                                                  1 packet shown
```

النقاط الرئيسية للتتبع هي:

- تطابق الحزمة تدفق موجود.
- واجهة الإخراج هي جدار الحماية نفسه (واجهة الهوية).

الخطوة 5

قم بتتبع حزم ICMP الخاصة بالمدخل من إختبار traceroute.

الحزمة #12 هي الرد من مضيف النقل:

```
<#root>

                                                                firepower#

                                                  show capture CAPI packet-number 12 trace
```

```
                                                                190 packets captured
12: 13:50:33.232562       802.1Q vlan#201 P0 192.168.201.88 > 192.168.201.200 icmp: time exceeded in-tra

                                                                        Phase: 3
                                                                     Type: UN-NAT
                                                                  Subtype: static
                                                                    Result: ALLOW
                                                               Elapsed time: 6344 ns
                                                                       Config:
                                                 nat (INSIDE,OUTSIDE) source static server_host interface
                                                                Additional Information:
                                                      NAT divert to egress interface INSIDE(vrfid:0)
                                                Untranslate 192.168.201.200/49168 to 192.168.200.50/49168

                                                                        Phase: 7
                                                                   Type: ACCESS-LIST
                                                                       Subtype:
                                                                    Result: ALLOW
                                                               Elapsed time: 97 ns
                                                                       Config:
                                                          access-group CSM_FW_ACL_ global
                                       access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268436480
                          access-list CSM_FW_ACL_ remark rule-id 268436480: ACCESS POLICY: mzafeiro_empty - Default
                                     access-list CSM_FW_ACL_ remark rule-id 268436480: L4 RULE: DEFAULT ACTION RULE
                                                                Additional Information:
          This packet will be sent to snort for additional processing where a verdict will be reached
                                                                                ...
                                                                        Phase: 18
                                                                   Type: FLOW-CREATION
                                                                       Subtype:
                                                                    Result: ALLOW
                                                               Elapsed time: 16104 ns
                                                                       Config:
                                                                Additional Information:
                                                 New flow created with id 143805, packet dispatched to next module
                                                                                ...
                                                                        Phase: 20
                                                                     Type: SNORT
                                                                  Subtype: identity
                                                                    Result: ALLOW
                                                               Elapsed time: 39496 ns
                                                                       Config:
                                                                Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

                                                                        Result:
                                                          input-interface: OUTSIDE(vrfid:0)
                                                                  input-status: up
                                                               input-line-status: up
                                                          output-interface: INSIDE(vrfid:0)
                                                                 output-status: up
                                                              output-line-status: up
                                                                       Action: allow
                                                                Time Taken: 158341 ns
```

- الحزمة جزء من توصيل جديد (لم تتطابق مع تدفق موجود).
- تخضع الحزمة لترجمة عنوان الشبكة (على وجه التحديد، UN-NAT يعني غاية NAT).

- يتم التعامل مع الحزمة كحركة مرور عبور لجدار الحماية وتخضع لنهج التحكم في الوصول (ACP) وفحص الشظايا.
- الإنتاج (مخرج) قارن داخلي. هذا يرجع إلى ال nat ترجمة.

السبب

في هذه الحالة، المشكلة سببها هذا ساكن إستاتيكي nat قاعدة:

<#root>

```
firepower#
```

show run nat

```
nat (INSIDE,OUTSIDE) source static server_host interface
```

المحتوى ذي الصلة

- السماح ب Traceroute من خلال الدفاع ضد تهديد الطاقة النارية (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).