排除FTD的Traceroute故障，即使成功執行ICMP Ping也不會顯示躍點資訊

問題

可以看到以下所有症狀：

- Traceroute失敗：當針對外部IP地址時，直接從思科防火牆威脅防禦(FTD)裝置發出的traceroute命令始終只返回* * *所有躍點。
- 成功的連線：對同一目標的ICMP Ping測試成功，並且在訪問控制策略中明確允許ICMP流量。

此行為可防止檢視來自FTD裝置的流量的路徑躍點，從而影響網路路徑疑難排解。

範例

對目標執行的Ping操作正在工作：

<#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
```

但traceroute不是：

<#root>

```
firepower#
```

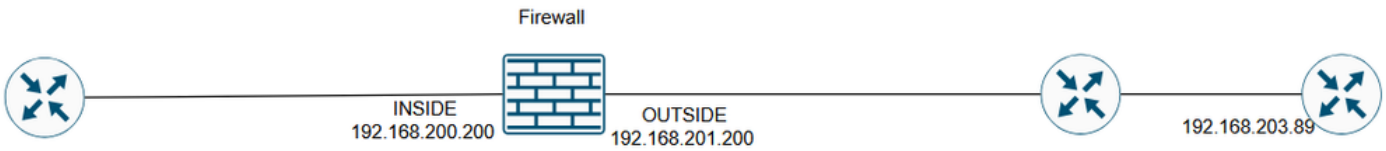
traceroute 192.168.203.89

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

環境

- 思科安全防火牆威脅防禦(FTD)。
- 首次觀測時間：7.4、7.4.2.3、7.6.2。其他版本也可能受到影響。
- 適用於管理的思科安全防火牆管理中心(FMC/cdFMC/FDM)。
- 正在使用靜態NAT規則，包括雙向配置。
- 從FTD CLI（Lina模式）執行traceroute命令。
- 訪問控制策略中允許的ICMP。

拓撲



inline_image_0.png

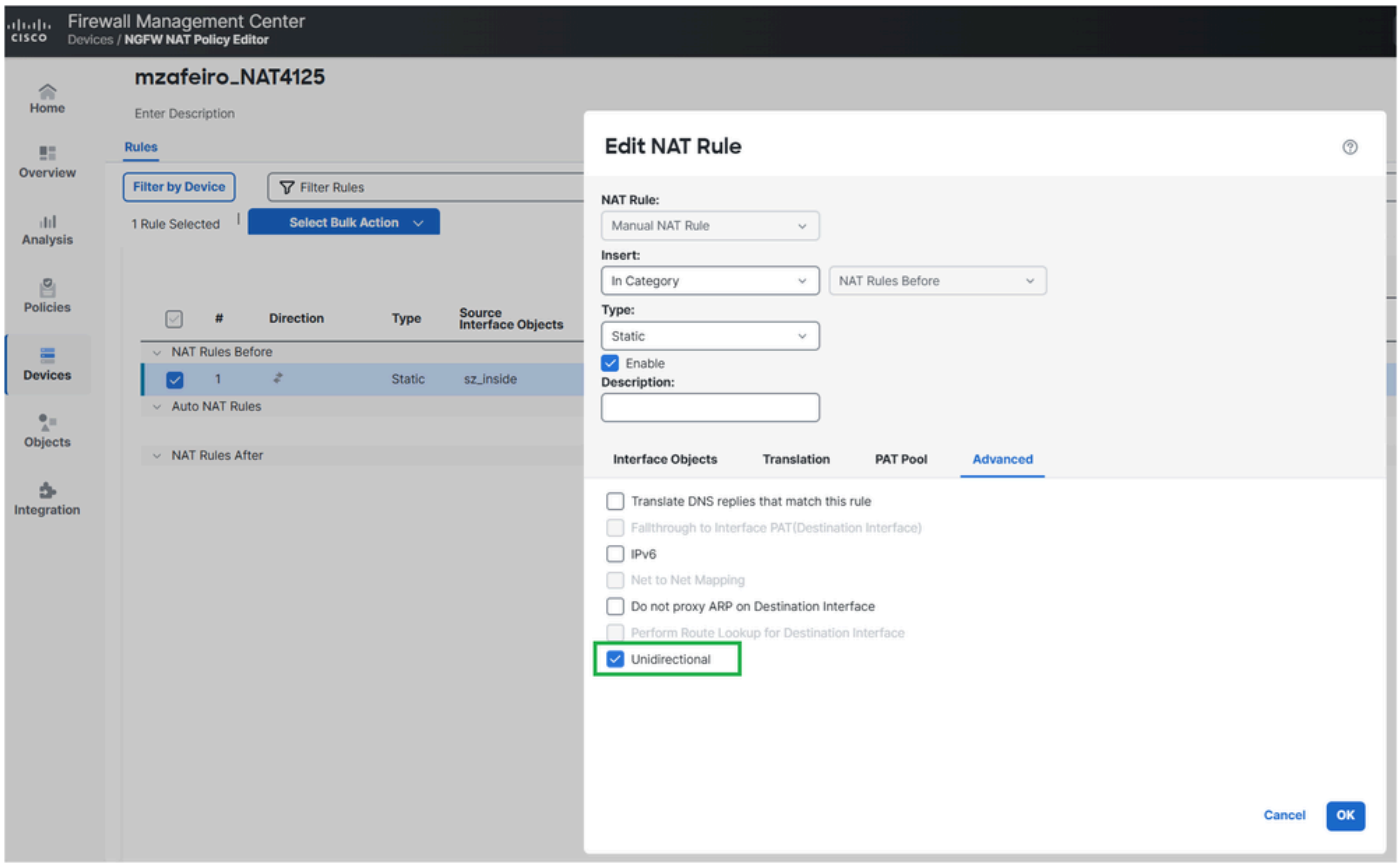
解析

可能的解決方案取決於配置的NAT規則的用途。

情境 1

如果目標是將內部伺服器IP僅轉換為出站訪問，則可以將NAT規則配置為單向。

在FMC上，可以通過NAT規則Advanced 選項完成此操作：



inline_image_0.png

部署的NAT配置：

<#root>

```
firepower#
```

show run nat

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

驗證

<#root>

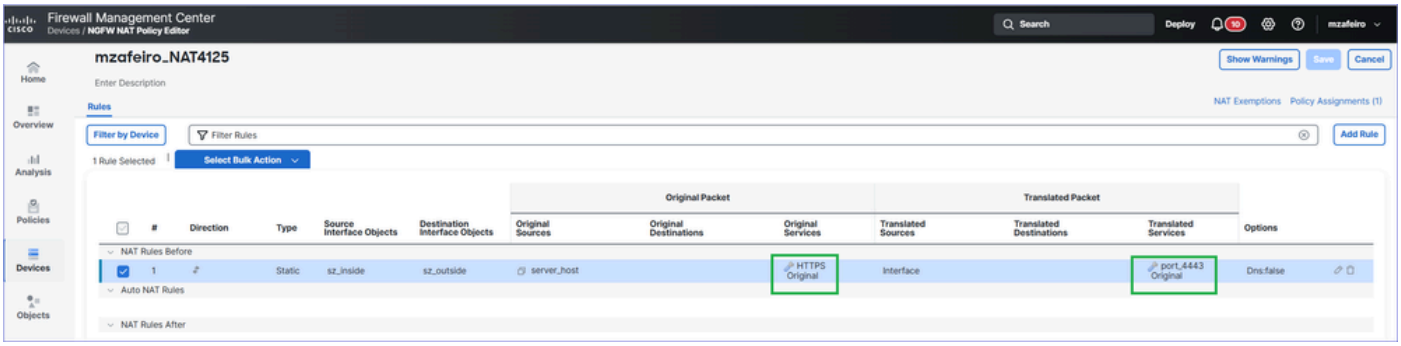
```
firepower#

 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
```

情境 2

如果目標是從外部訪問內部伺服器，則可以通過配置埠轉發使NAT規則更加具體：



inline_image_0.png

部署的NAT配置：

<#root>

```
firepower#

show run nat

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

驗證

<#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
```

工作方式

工作方式

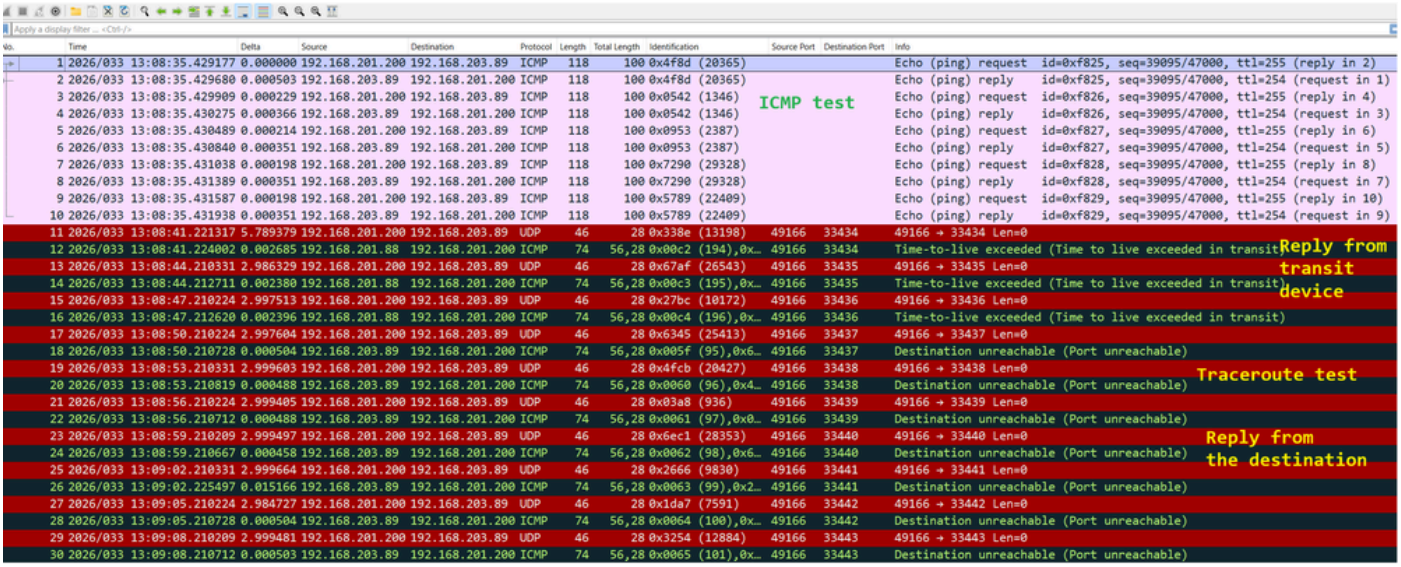
Ping

1. 防火牆傳送回應請求（ICMP型別8代碼0）訊息。
2. 為ICMP建立了新的防火牆連線。
3. 防火牆收到回應回覆(ICMP Type 0 Code 0)訊息。
4. 該消息與步驟2中建立的連線匹配。
5. 防火牆會使用回應回複訊息。

Traceroute

1. 防火牆將三個從連線埠、連線埠、連線埠和33434口開始33435UDP封33436傳送到使用TTL 1的目的地址。
2. 為UDP建立了新的防火牆連線。
3. 防火牆收到傳輸中超過ICMP TTL（型別11代碼0）或ICMP連線埠無法連線（型別3代碼3）。
4. 一旦ICMP資料包到達防火牆，它們將被視為與步驟2中的UDP資料包不同的連線。

這在Wireshark中可以看到：



inline_image_0.png

疑難排解

步驟 1

在防火牆輸出介面上啟用封包擷取（含追蹤軌跡），以檢視防火牆如何處理輸入封包：

<#root>

firepower#

capture CAPI trace interface OUTSIDE match ip host 192.168.203.89 host 192.168.201.100

步驟 2

使用ping測試:

<#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
```

然後使用traceroute進行測試：

<#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*  *  *
…
```

步驟 3

檢查捕獲內容：

- 封包1-10與ICMP ping 測試相關。
- 資料包11-16與traceroute相關。應答來自第一跳。
- 資料包17-28也與traceroute相關。應答來自目標端點。

<#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
```

步驟 4

從ping測試追蹤輸入ICMP封包。

Packet #2是在Packet #1中傳送的ICMP ping要求上的回。

<#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
```

跟蹤的關鍵點包括：

- 資料包與現有流匹配。
- 輸出介面是防火牆本身（身份介面）。

步驟 5

追蹤來自traceroute測試的輸入ICMP封包。

Packet #12是來自傳輸主機的回覆：

<#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-tr

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
```

- 資料包是新連線的一部分（它與現有流不匹配）。
- 資料包需要經過網路地址轉換（具體來說，UN-NAT表示目標NAT）。
- 此封包視為防火牆傳輸流量，並須接受存取控制原則(ACP)和Snort檢查。
- 輸出（輸出）介面是INSIDE。這是因為NAT轉換。

原因

在這種情況下，此靜態NAT規則會導致問題：

```
<#root>

firepower#

show run nat

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

相關內容

- 允許Traceroute通過Firepower威脅防禦(FTD)
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。