排除FTD的Traceroute故障，即使成功执行ICMP Ping操作也不会显示跳信息

问题

可以看到以下所有症状：

- Traceroute故障：从思科防火墙威胁防御(FTD)设备直接发起的traceroute命令在针对外部IP地址时，始终只返回* * *所有跃点。
- 成功连接：对同一目标的ICMP ping测试成功，并且访问控制策略中明确允许ICMP流量。

此行为可防止对源自FTD设备的流量的路径跳数的可视性，从而影响网络路径故障排除工作。

示例

对目标执行ping操作成功：

<#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>

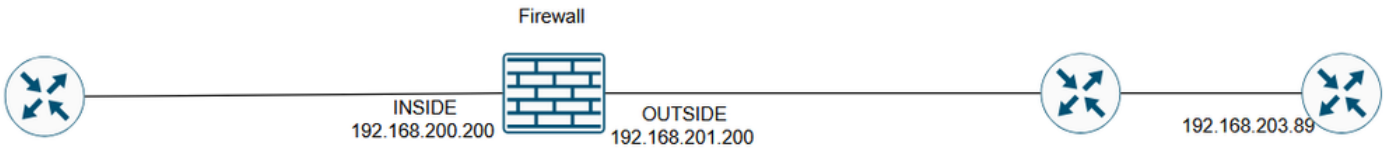
```
firepower#

traceroute 192.168.203.89

Type escape sequence to abort.
```

```
Tracing the route to 192.168.203.89
 1*  *  *
 2*  *  *
 3*  *  *
...
 30*  *  *
firepower#
```

环境

- 思科安全防火墙威胁防御(FTD)。
- 第一次观察时间：7.4、7.4.2.3、7.6.2。其他版本也可能受到影响。
- 用于管理的思科安全防火墙管理中心(FMC/cdFMC/FDM)。
- 使用的静态NAT规则，包括双向配置。
- 从FTD CLI（Lina模式）执行的traceroute命令。
- 访问控制策略中允许ICMP。

拓扑



inline_image_0.png

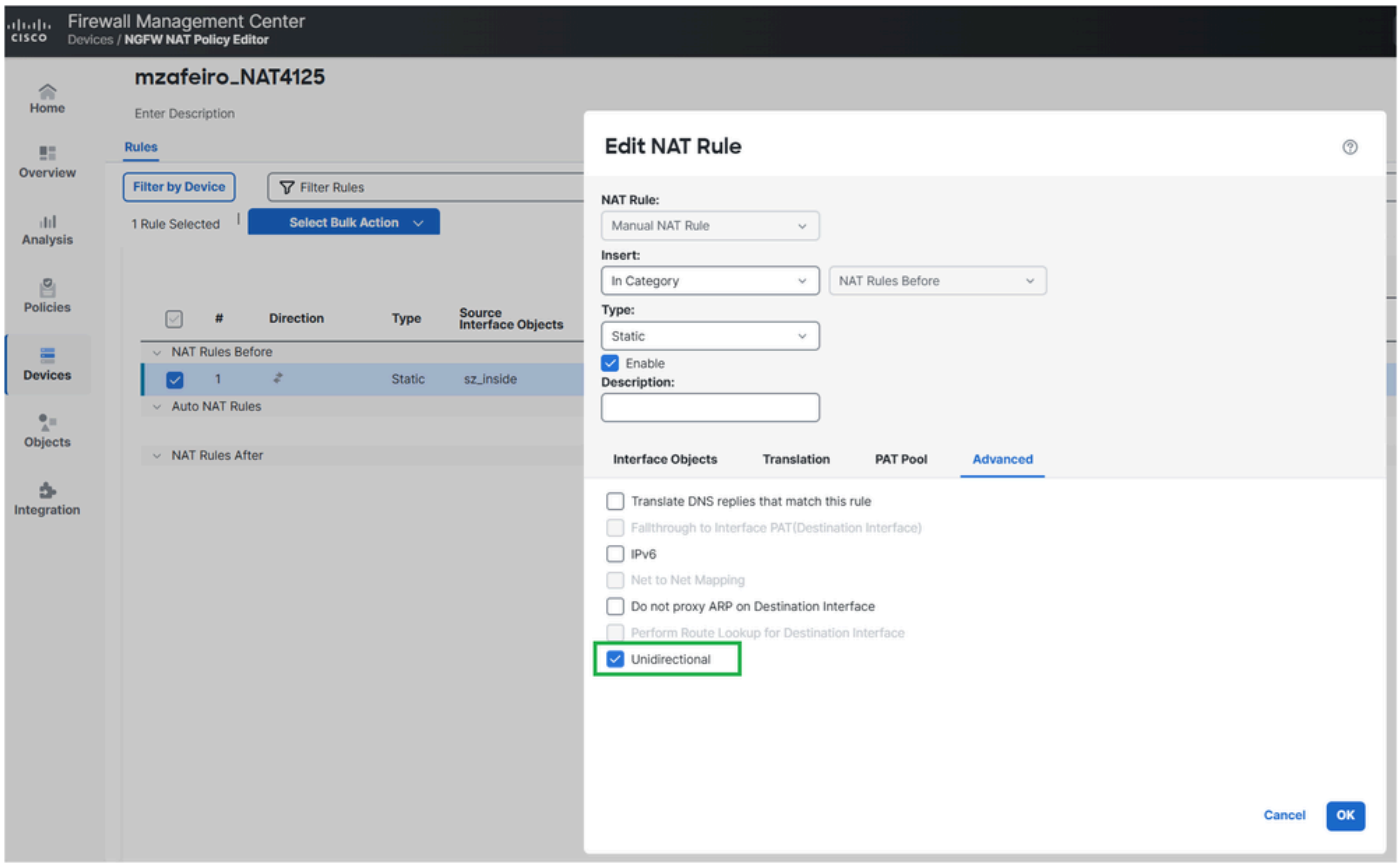
分辨率

可能的解决方案取决于配置的NAT规则的用途。

解决方案 1

如果目标是仅为出站访问转换内部服务器IP，则可以将NAT规则配置为单向规则。

在FMC上，可以通过NAT规则Advanced选项完成此操作：



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#
```

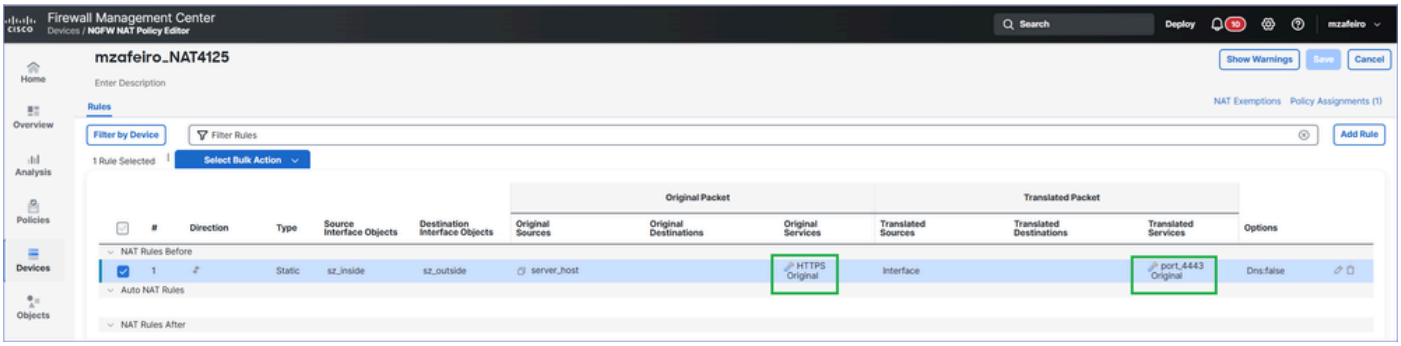
确认

<#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
```

解决方案 2

如果目标是从外部访问内部服务器，则可以通过配置端口转发使NAT规则更加具体：



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
```

确认

<#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
```

运行原理

工作原理

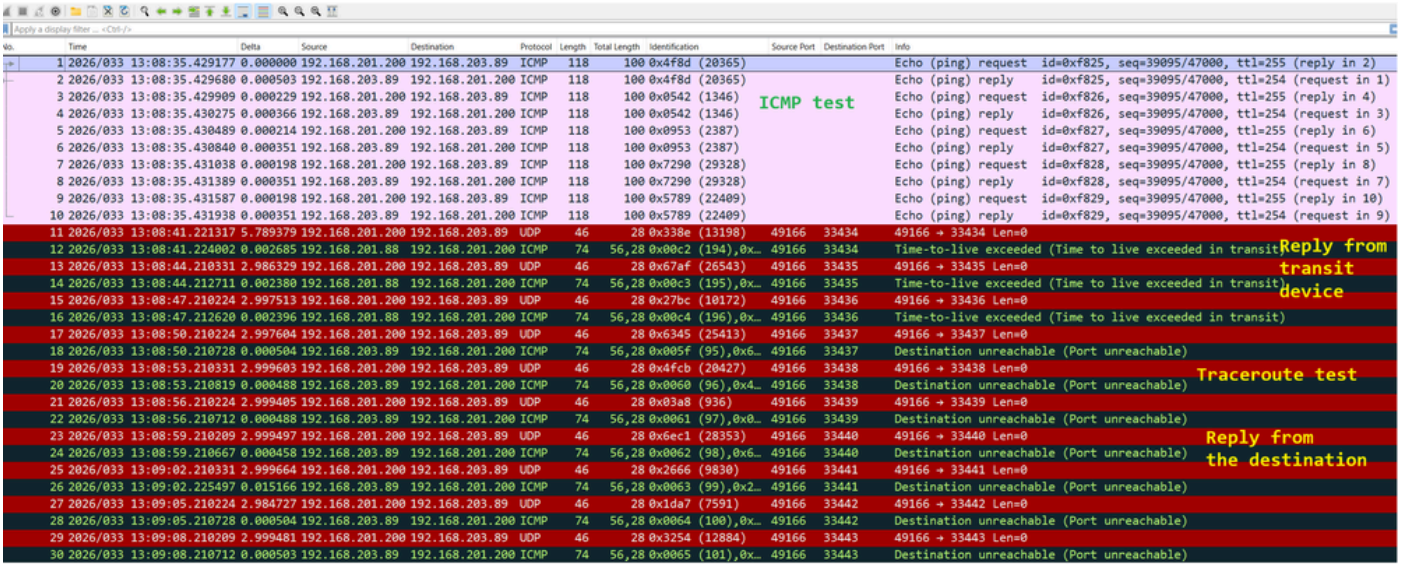
ping

1. 防火墙发送回应请求（ICMP类型8代码0）消息。
2. 为ICMP创建新的防火墙连接。
3. 防火墙收到应答（ICMP类型0代码0）消息。
4. 该消息与步骤2中创建的连接匹配。
5. 回应应答消息被防火墙占用。

Traceroute

1. 防火墙将三个UDP数据包从端口33434、33435和33436发往使用TTL 1的目的地。
2. 为UDP创建了新的防火墙连接。
3. 防火墙接收传输过程中超出的ICMP TTL（类型11代码0）或无法到达的ICMP端口（类型3代码3）。
4. 一旦ICMP数据包到达防火墙，它们将被视为不同于步骤2中的UDP数据包的连接。

这在Wireshark中可以看到：



inline_image_0.png

故障排除

第 1 步

使用trace在防火墙出口接口上启用数据包捕获，以查看防火墙如何处理入口数据包：

<#root>

firepower#

capture CAPI trace interface OUTSIDE match ip host 192.168.203.89 host 192.168.201.100

步骤 2

使用ping测试:

<#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
```

然后使用traceroute进行测试：

<#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*  *  *
…
```

步骤 3

检查捕获内容：

- 数据包1-10与ICMP ping测试相关。
- 数据包11-16与traceroute相关。应答来自第一跳。
- 数据包17-28也与traceroute相关。应答来自目标端点。

<#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
```

步骤 4

通过ping测试跟踪入口ICMP数据包。

Packet #2是对Packet Tracer中发送的ICMP ping请求的回#1。

<#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
```

跟踪的关键点包括：

- 数据包与现有流匹配。
- 输出接口是防火墙本身（身份接口）。

步骤 5

跟踪来自traceroute测试的入口ICMP数据包。

数据包#12是来自传输主机的应答：

<#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
```

- 数据包是新连接的一部分（它与现有流不匹配）。
- 数据包需要经过网络地址转换（具体而言，UN-NAT表示目标NAT）。
- 该数据包被视为防火墙中转流量，并受到访问控制策略(ACP)和Snort检测。
- 输出（出口）接口为INSIDE。这是因为NAT转换。

原因

在这种情况下，此静态NAT规则会导致问题：

```
<#root>

firepower#

show run nat

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

相关内容

- 允许Traceroute通过Firepower威胁防御(FTD)
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。