

# ICMP pingが成功したにもかかわらずホップ情報が表示されないFTDからのtracerouteのトラブルシューティング

## お問い合わせ内容

次の症状がすべて見られます。

- traceroute障害 : Cisco Firewall Threat Defense(FTD)デバイスから直接開始される tracerouteコマンドは、外部IPアドレスをターゲットとした場合、すべてのホップについて一貫して「\*\*」のみを返します。
- 正常な接続 : 同じ宛先へのICMP pingテストは成功し、ICMPトラフィックはアクセスコントロールポリシーで明示的に許可されます。

この動作により、FTDデバイスから発信されたトラフィックのパスホップが可視化されなくなり、ネットワークパスのトラブルシューティング作業に影響が及びます。

例

宛先へのpingは正常に動作しています。

```
<#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
```

ただし、tracerouteは有効ではありません。

```
<#root>
```

```
firepower#
```

```
traceroute 192.168.203.89
```

```
Type escape sequence to abort.
```

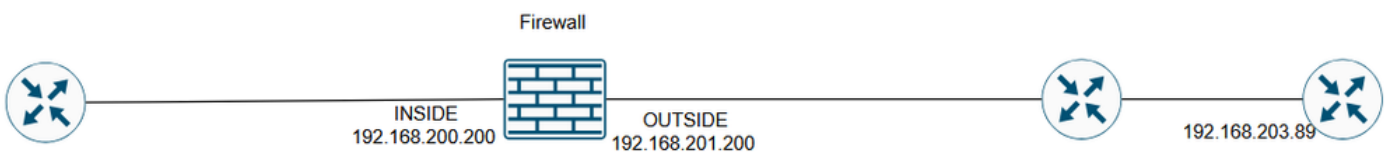
```
Tracing the route to 192.168.203.89
```

```
 1*  *  *  
 2*  *  *  
 3*  *  *  
...  
30* *  *  
firepower#
```

## 環境

- シスコセキュアファイアウォール脅威対策(FTD)
- 7.4、7.4.2.3、7.6.2での初回観測。他のバージョンも影響を受ける可能性があります。
- 管理用のCisco Secure Firewall Management Center(FMC / cdFMC / FDM)
- 双方向設定を含む、使用されているスタティックNATルール。
- FTD CLIからtracerouteコマンドを実行しました ( Linaモード )。
- アクセスコントロールポリシーでICMPが許可されました。

## トポロジ



inline\_image\_0.png ( インラインイメージ\_0.png )

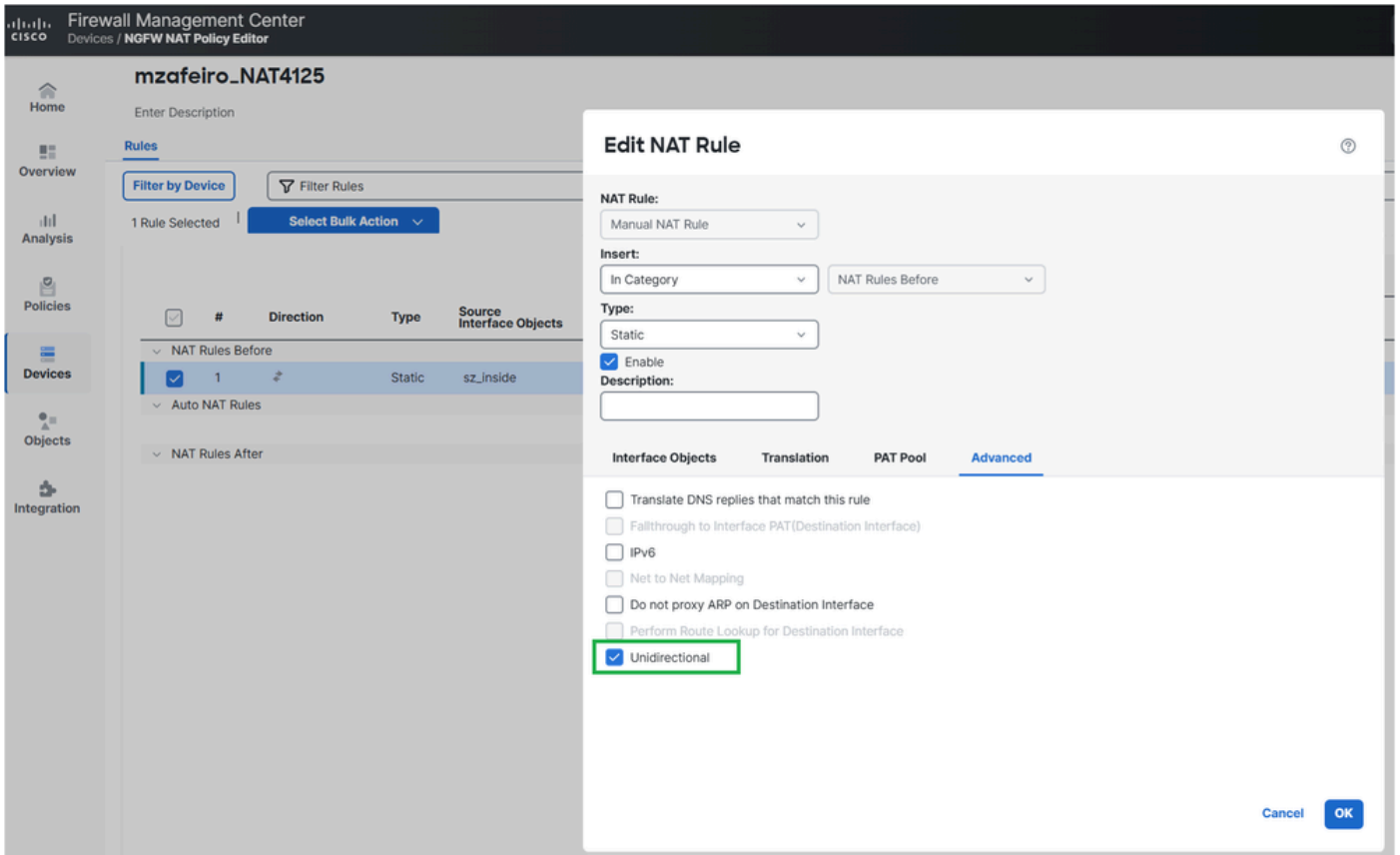
## 解決策

可能な解決策は、設定されたNATルールの目的によって異なります。

## 解決策 1

内部サーバのIPを発信アクセスのみに変換する場合は、NATルールを単方向に設定できます。

FMCでは、NATルールのAdvancedオプションから次の操作を実行できます。



inline\_image\_0.png ( インラインイメージ\_0.png )

導入されたNAT設定は次のとおりです。

```
<#root>
```

```
firepower#
```

```
show run nat
```

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

検証

```
<#root>
```

firepower#

```
traceroute 192.168.203.89
```

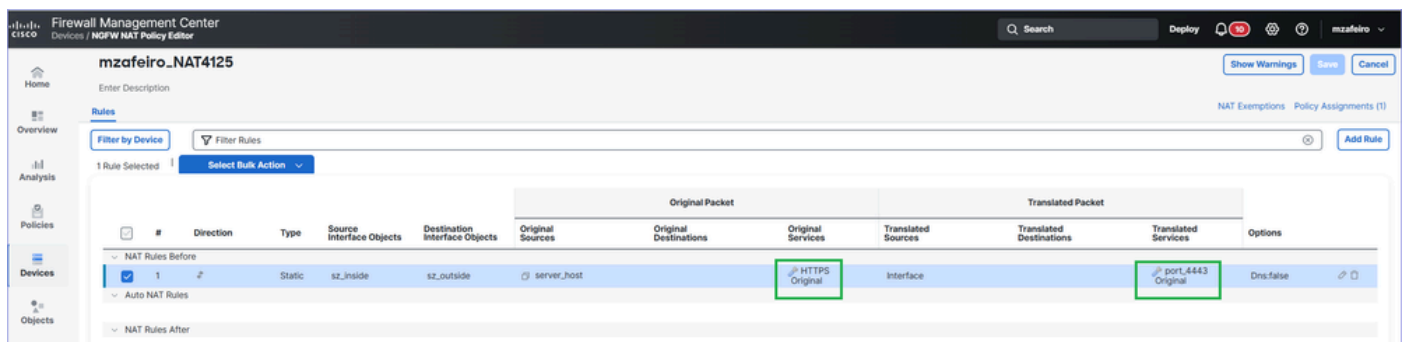
Type escape sequence to abort.

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
```

## 解決策 2

内部サーバが外部から到達可能であることが目標である場合は、ポートフォワーディングを設定してNATルールをより具体的にすることができます。



inline\_image\_0.png ( インラインイメージ\_0.png )

導入されたNAT設定は次のとおりです。

<#root>

firepower#

```
show run nat
```

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

## 検証

<#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
```

## 仕組み

### ping

1. ファイアウォールはエコー要求(ICMP Type 8 Code 0)メッセージを送信します。
2. ICMP用の新しいファイアウォール接続が作成されます。
3. ファイアウォールがエコー応答(ICMP Type 0 Code 0)メッセージを受信します。
4. このメッセージは、ステップ2で作成した接続と一致します。
5. エコー応答メッセージはファイアウォールによって使用されます。

### トレースルート

1. ファイアウォールは、ポート33434、33435、および33436から宛先に向けて、TTL 1で3つのUDPパケットを送信します。
2. UDP用の新しいファイアウォール接続が作成されます。
3. ファイアウォールは、転送中のICMP TTL超過 (タイプ11コード0) またはICMPポート到達不能 (タイプ3コード3) を受信します。
4. ICMPパケットがファイアウォールに到着すると、それらはステップ2のUDPパケットとは異なる接続として扱われます。

これはWiresharkで確認できます。

| No. | Time                    | Delta    | Source          | Destination     | Protocol | Length | Total Length | Identification        | Source Port | Destination Port | Info  |
|-----|-------------------------|----------|-----------------|-----------------|----------|--------|--------------|-----------------------|-------------|------------------|---|
| 1   | 2026/03/13:08:35.429177 | 0.000000 | 192.168.201.200 | 192.168.203.89  | ICMP     | 118    | 100          | 0x4f8d (20365)        |             |                  | Echo (ping) request id=0xf825, seq=39095/47000, ttl=255 (reply in 2)  |
| 2   | 2026/03/13:08:35.429600 | 0.000503 | 192.168.203.89  | 192.168.201.200 | ICMP     | 118    | 100          | 0x4f8d (20365)        |             |                  | Echo (ping) reply id=0xf825, seq=39095/47000, ttl=254 (request in 1)  |
| 3   | 2026/03/13:08:35.429909 | 0.000229 | 192.168.201.200 | 192.168.203.89  | ICMP     | 118    | 100          | 0x0542 (1346)         |             |                  | Echo (ping) request id=0xf826, seq=39095/47000, ttl=255 (reply in 4)  |
| 4   | 2026/03/13:08:35.430275 | 0.000366 | 192.168.203.89  | 192.168.201.200 | ICMP     | 118    | 100          | 0x0542 (1346)         |             |                  | Echo (ping) reply id=0xf826, seq=39095/47000, ttl=254 (request in 3)  |
| 5   | 2026/03/13:08:35.430489 | 0.000214 | 192.168.201.200 | 192.168.203.89  | ICMP     | 118    | 100          | 0x0953 (2387)         |             |                  | Echo (ping) request id=0xf827, seq=39095/47000, ttl=255 (reply in 6)  |
| 6   | 2026/03/13:08:35.430840 | 0.000351 | 192.168.203.89  | 192.168.201.200 | ICMP     | 118    | 100          | 0x0953 (2387)         |             |                  | Echo (ping) reply id=0xf827, seq=39095/47000, ttl=254 (request in 5)  |
| 7   | 2026/03/13:08:35.431038 | 0.000198 | 192.168.201.200 | 192.168.203.89  | ICMP     | 118    | 100          | 0x7290 (29328)        |             |                  | Echo (ping) request id=0xf828, seq=39095/47000, ttl=255 (reply in 8)  |
| 8   | 2026/03/13:08:35.431389 | 0.000351 | 192.168.203.89  | 192.168.201.200 | ICMP     | 118    | 100          | 0x7290 (29328)        |             |                  | Echo (ping) reply id=0xf828, seq=39095/47000, ttl=254 (request in 7)  |
| 9   | 2026/03/13:08:35.431587 | 0.000198 | 192.168.201.200 | 192.168.203.89  | ICMP     | 118    | 100          | 0x5789 (22409)        |             |                  | Echo (ping) request id=0xf829, seq=39095/47000, ttl=255 (reply in 10) |
| 10  | 2026/03/13:08:35.431938 | 0.000351 | 192.168.203.89  | 192.168.201.200 | ICMP     | 118    | 100          | 0x5789 (22409)        |             |                  | Echo (ping) reply id=0xf829, seq=39095/47000, ttl=254 (request in 9)  |
| 11  | 2026/03/13:08:41.221317 | 5.789379 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x338e (13198)        | 49166       | 33434            | 49166 → 33434 Len=0   |
| 12  | 2026/03/13:08:41.224002 | 0.002685 | 192.168.201.88  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x00c2 (194),0x... | 49166       | 33434            | Time-to-live exceeded (Time to live exceeded in transit)              |
| 13  | 2026/03/13:08:44.210331 | 2.986329 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x67af (26543)        | 49166       | 33435            | 49166 → 33435 Len=0   |
| 14  | 2026/03/13:08:44.212711 | 0.002380 | 192.168.201.88  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x00c3 (195),0x... | 49166       | 33435            | Time-to-live exceeded (Time to live exceeded in transit)              |
| 15  | 2026/03/13:08:47.210224 | 2.997513 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x27bc (10172)        | 49166       | 33436            | 49166 → 33436 Len=0   |
| 16  | 2026/03/13:08:47.212620 | 0.002396 | 192.168.201.88  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x00c4 (196),0x... | 49166       | 33436            | Time-to-live exceeded (Time to live exceeded in transit)              |
| 17  | 2026/03/13:08:50.210224 | 2.997604 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x6345 (25413)        | 49166       | 33437            | 49166 → 33437 Len=0   |
| 18  | 2026/03/13:08:50.210728 | 0.000504 | 192.168.203.89  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x005f (95),0x6... | 49166       | 33437            | Destination unreachable (Port unreachable)                            |
| 19  | 2026/03/13:08:53.210331 | 2.999603 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x4fcb (20427)        | 49166       | 33438            | 49166 → 33438 Len=0   |
| 20  | 2026/03/13:08:53.210819 | 0.000488 | 192.168.203.89  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x0060 (96),0x4... | 49166       | 33438            | Destination unreachable (Port unreachable)                            |
| 21  | 2026/03/13:08:56.210224 | 2.999405 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x03a8 (936)          | 49166       | 33439            | 49166 → 33439 Len=0   |
| 22  | 2026/03/13:08:56.210712 | 0.000488 | 192.168.203.89  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x0061 (97),0x0... | 49166       | 33439            | Destination unreachable (Port unreachable)                            |
| 23  | 2026/03/13:08:59.210209 | 2.999497 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x6ec1 (28353)        | 49166       | 33440            | 49166 → 33440 Len=0   |
| 24  | 2026/03/13:08:59.210657 | 0.000458 | 192.168.203.89  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x0062 (98),0x6... | 49166       | 33440            | Destination unreachable (Port unreachable)                            |
| 25  | 2026/03/13:09:02.210331 | 2.999664 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x2666 (9830)         | 49166       | 33441            | 49166 → 33441 Len=0   |
| 26  | 2026/03/13:09:02.225497 | 0.015166 | 192.168.203.89  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x0063 (99),0x2... | 49166       | 33441            | Destination unreachable (Port unreachable)                            |
| 27  | 2026/03/13:09:05.210224 | 2.984727 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x1da7 (7591)         | 49166       | 33442            | 49166 → 33442 Len=0   |
| 28  | 2026/03/13:09:05.210728 | 0.000504 | 192.168.203.89  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x0064 (100),0x... | 49166       | 33442            | Destination unreachable (Port unreachable)                            |
| 29  | 2026/03/13:09:08.210209 | 2.999481 | 192.168.201.200 | 192.168.203.89  | UDP      | 46     | 28           | 0x3254 (12884)        | 49166       | 33443            | 49166 → 33443 Len=0   |
| 30  | 2026/03/13:09:08.210712 | 0.000503 | 192.168.203.89  | 192.168.201.200 | ICMP     | 74     | 56           | 28 0x0065 (101),0x... | 49166       | 33443            | Destination unreachable (Port unreachable)                            |

inline\_image\_0.png ( インラインイメージ\_0.png )

## トラブルシューティング

### ステップ 1

トレースを使用してファイアウォール出カインターフェイスでのパケットキャプチャを有効にし、ファイアウォールによる入カパケットの処理方法を確認します。

```
<#root>
```

```
firepower#
```

```
capture CAPI trace interface OUTSIDE match ip host 192.168.203.89 host 192.168.201.100
```

### ステップ 2

pingを使用してテストします。

```
<#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

次に、tracertを使用してテストします。

```
<#root>
```

```
firepower#
```

```
tracert 192.168.203.89
```

```
Type escape sequence to abort.
```

```
Tracing the route to 192.168.203.89
```

```
 1*  *  *
```

```
 2*  *  *
```

```
 3*  *  *
```

```
 4*  *  *
```

```
 5*  *  *
```

```
 6*  *  *
```

```
 7*  *  *
```

```
...
```

### 手順 3

キャプチャの内容を確認します。

- パケット1 ~ 10は、ICMP pingテストに関連しています。
- パケット11 ~ 16はtracertに関連しています。 応答は最初のホップからのものです。
- パケット17 ~ 28もtracertに関連しています。 応答は宛先エンドポイントからのものです。

```
<#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-tr
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-tr
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-tr
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
```

## ステップ 4

pingテストから入力ICMPパケットをトレースします。

Packet #2は、Packet #1で送信されたICMP ping要求に対する応答です。

```
<#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
```

トレースのキーポイントは次のとおりです。

- パケットは既存のフローに一致しました。
- 出カインターフェイスは、ファイアウォール自体 (アイデンティティインターフェイス) です。

ステップ 5 :

tracerouteテストから入力ICMPパケットをトレースします。

パケット#12は中継ホストからの応答です。

<#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, loc
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
```

- パケットは新しい接続の一部です ( 既存のフローと一致しませんでした )。
- パケットはネットワークアドレス変換(NAT)の対象になります ( 具体的には、UN-NATは「宛先NAT」を意味します )。
- パケットはファイアウォール中継トラフィックとして扱われ、アクセスコントロールポリシー(ACP)とSnortの検査の対象となります。
- 出カインターフェイスはINSIDEです。これはNAT変換によるものです。

## 原因

この場合、問題の原因は次のスタティックNATルールにあります。

<#root>

```
firepower#
```

```
show run nat
```

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

## 関連コンテンツ

- [Firepower Threat Defense\(FTD\)を介したtracerouteの許可](#)
- [シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。