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。

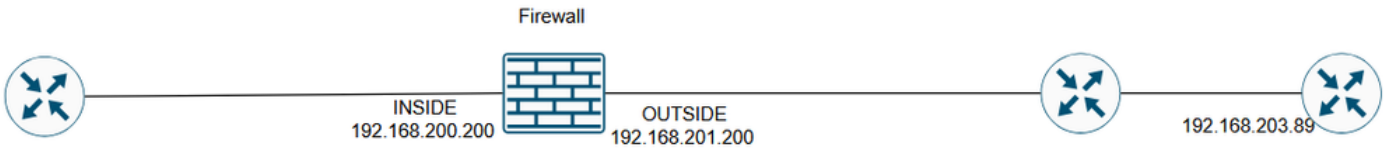
<#root>

```
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）

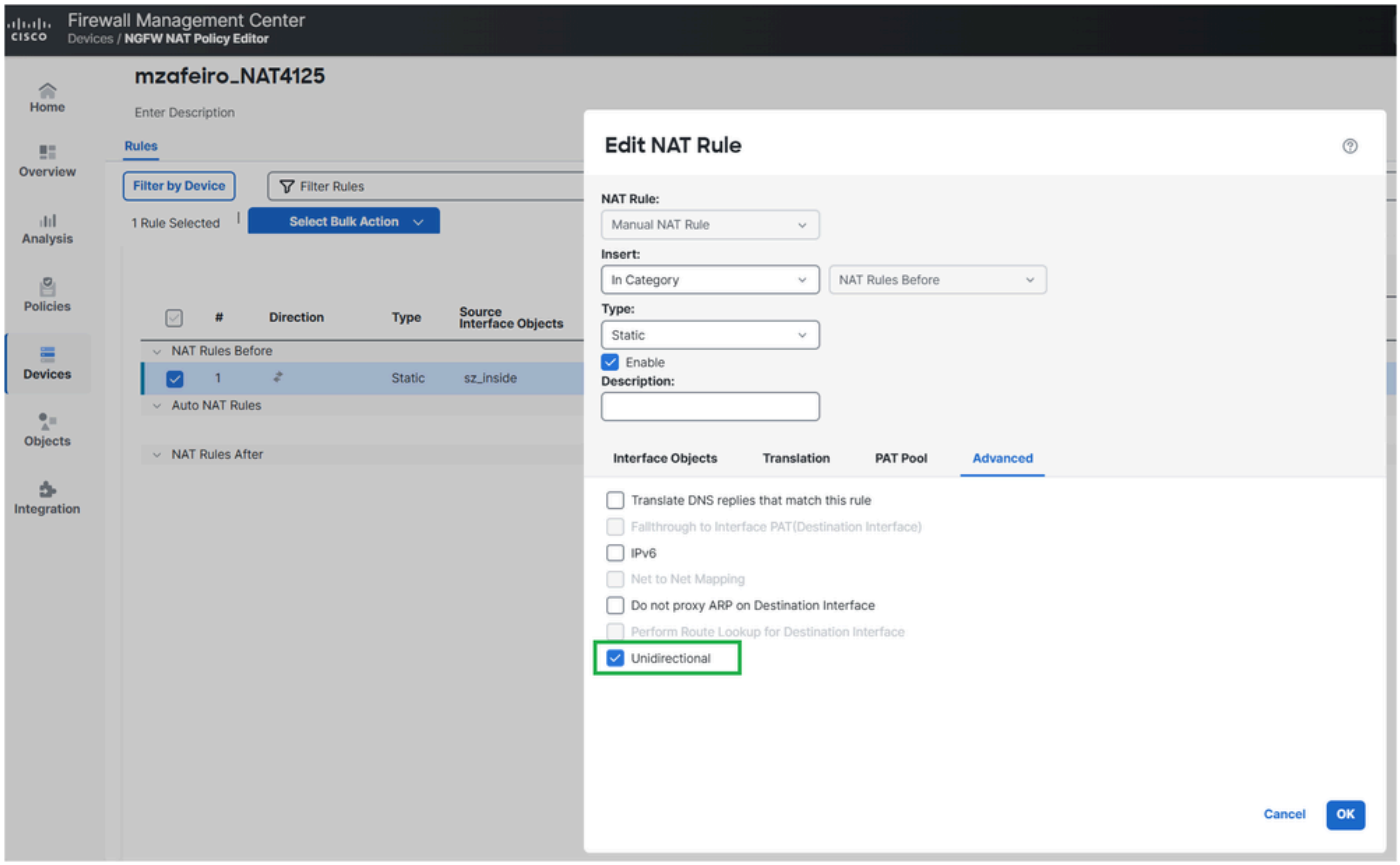
解決策

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#
```

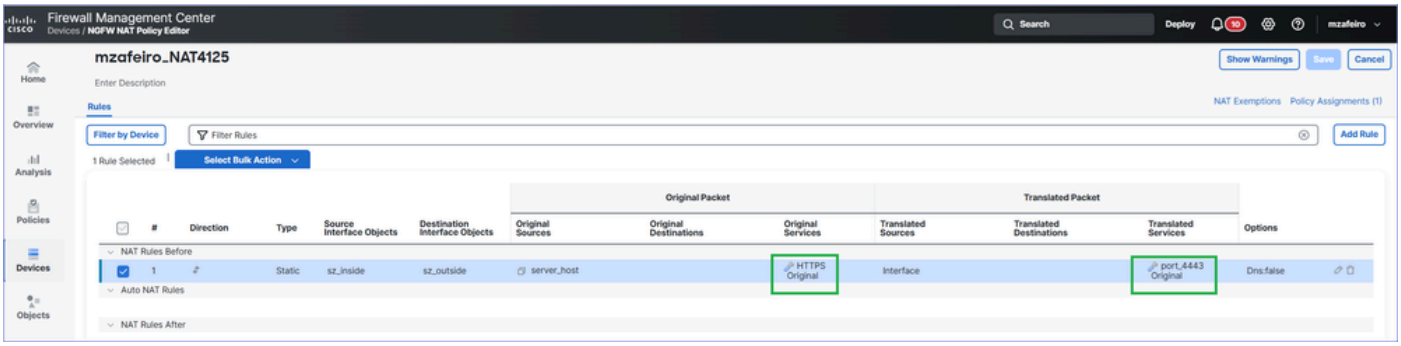
検証

```
<#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

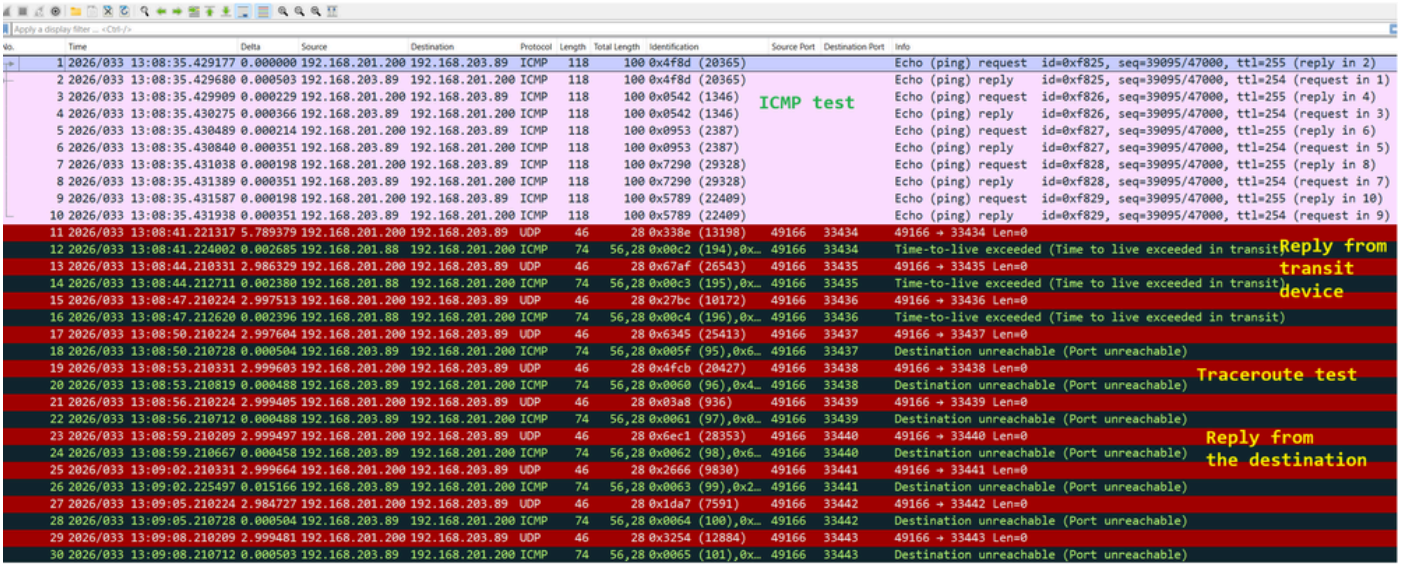
ping

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。



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力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力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、tracerouteを使用してテストします。

<#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*  *  *
…
```

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traceroute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traceroute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-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 p
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 p
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 p
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 p
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 p
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 p
```

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。
- 出力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 :

tracerout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, 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
```

- 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。
- 出力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。