ICMP Ping에 성공해도 홉 정보가 표시되지 않는 FTD의 Traceroute 문제 해결

문제

이러한 모든 증상이 나타납니다.

- Traceroute 오류: Cisco FTD(Firewall Threat Defense) 디바이스에서 직접 시작되는 Traceroute 명령은 외부 IP 주소를 대상으로 할 때 모든 홉에 대해 * * *만 일관성 있게 반환합니다.
- 성공한 연결: 동일한 대상에 대한 ICMP ping 테스트에 성공했으며 ICMP 트래픽은 액세스 제어 정책에서 명시적으로 허용됩니다.

이러한 동작으로 인해 FTD 디바이스에서 시작되는 트래픽에 대한 경로 홉에 대한 가시성이 차단되어 네트워크 경로 트러블슈팅 작업에 영향을 줍니다.

예

대상에 대한 Ping이 작동 중입니다.

<#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
```

그러나 traceroute는

<#root>

```
firepower#
```

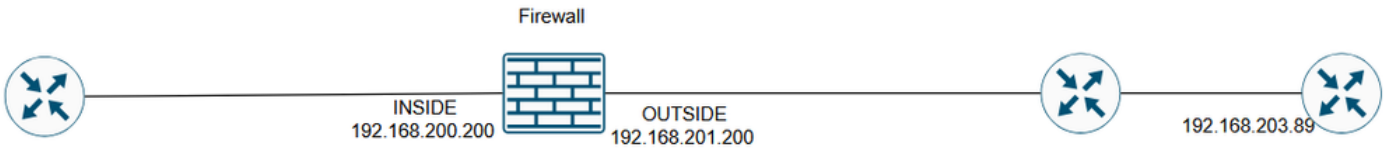
```
traceroute 192.168.203.89

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

환경

- Cisco FTD(Secure Firewall Threat Defense).
- 7.4, 7.4.2.3, 7.6.2에서 처음 관찰되었습니다. 다른 버전도 영향을 받을 수 있습니다.
- 관리용 Cisco Secure Firewall Management Center(FMC/cdFMC/FDM).
- 양방향 컨피그레이션을 포함하여 사용 중인 고정 NAT 규칙
- FTD CLI(Lina 모드)에서 실행되는 Traceroute 명령입니다.
- 액세스 제어 정책에서 허용되는 ICMP입니다.

토폴로지



inline_image_0.png

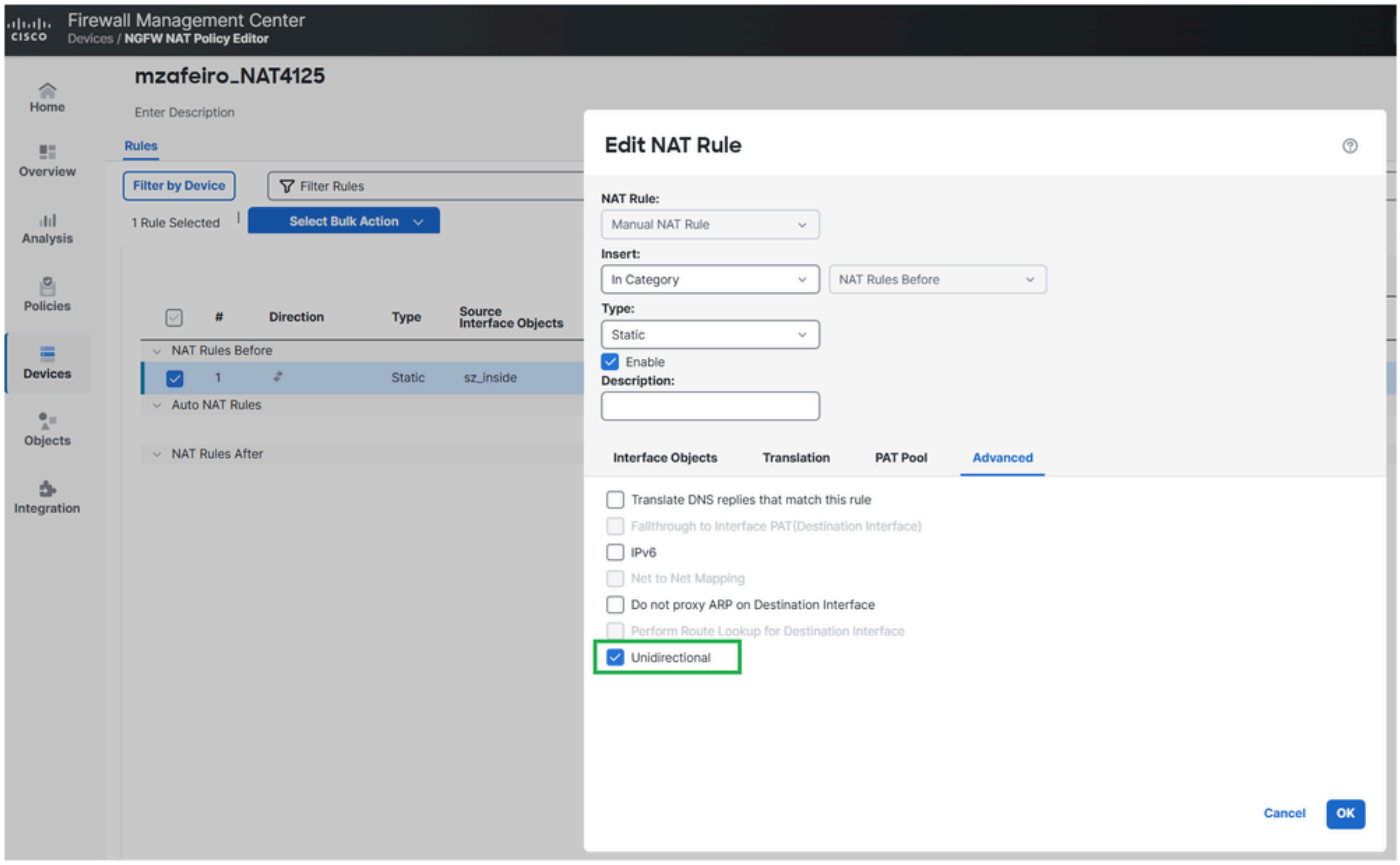
해결

가능한 솔루션은 구성된 NAT 규칙의 목적에 따라 다릅니다.

해결 방법 1

아웃바운드 액세스에 대해서만 내부 서버 IP를 변환하는 것이 목표인 경우 NAT 규칙을 단방향으로 구성할 수 있습니다.

FMC에서는 NAT 규칙 Advanced 옵션에서 이 작업을 수행할 수 있습니다.



inline_image_0.png

구축된 NAT 컨피그레이션:

```
<#root>

firepower#

show run nat

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

확인

<#root>

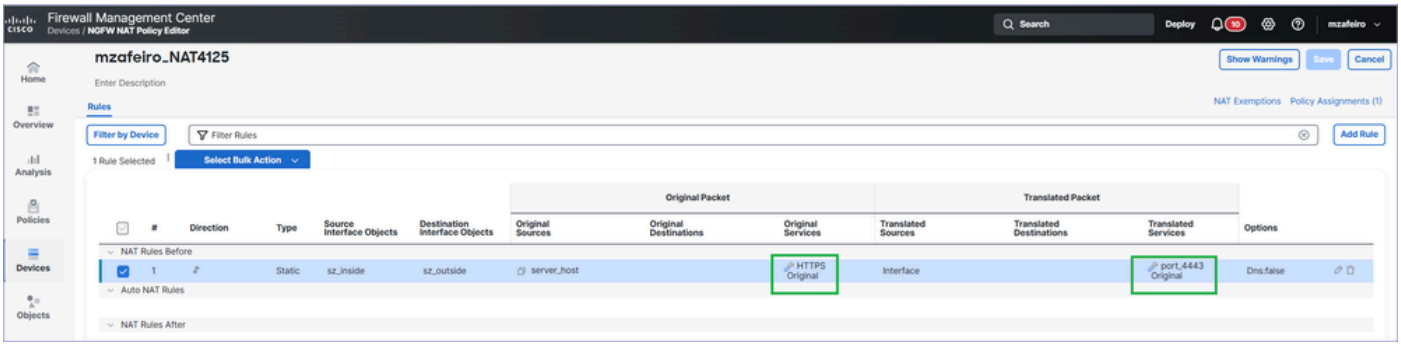
```
firepower#
```

```
 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
```

해결 방법 2

외부에서 내부 서버에 연결할 수 있는 것이 목표인 경우 포트 전달을 구성하여 NAT 규칙을 더 구체적으로 지정할 수 있습니다.



inline_image_0.png

구축된 NAT 컨피그레이션:

<#root>

```
firepower#
```

```
show run nat
```

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

확인

<#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
```

운영 방식

운영 방식

핑

1. 방화벽은 에코 요청(ICMP Type 8 Code 0) 메시지를 전송합니다.
2. ICMP에 대한 새 방화벽 연결이 생성됩니다.
3. 방화벽은 에코 응답(ICMP Type 0 Code 0) 메시지를 수신합니다.
4. 메시지는 2단계에서 생성한 연결과 일치합니다.
5. 에코 응답 메시지는 방화벽에서 사용됩니다.

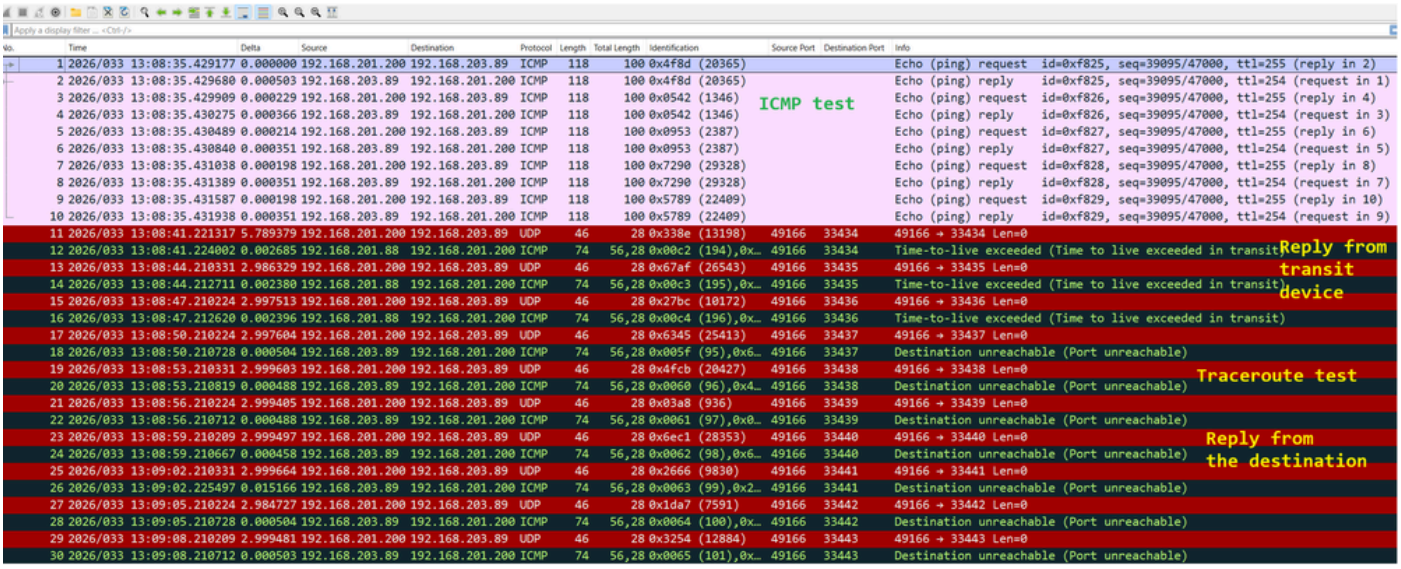
트레이스라우트

1. 방화벽은 TTL 1을 사용하여 포트, 33434, 33435 및 33436에서 대상으로 3개의 UDP 패킷을 전송합니다.
2. UDP에 대한 새 방화벽 연결이 생성됩니다.

3. 방화벽은 전송 중에 초과된 ICMP TTL(Type 11 Code 0) 또는 ICMP Port unreachable(Type 3 Code 3)을 수신합니다.

4. ICMP 패킷이 방화벽에 도착하면 2단계의 UDP 패킷과 다른 연결로 처리됩니다.

이는 Wireshark에서 확인할 수 있습니다.



inline_image_0.png

문제 해결

1단계

방화벽이 인그레스 패킷을 처리하는 방법을 보려면 추적을 사용하여 방화벽 이그레스 인터페이스의 패킷 캡처를 활성화합니다.

<#root>

```
firepower#

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

2단계

ping을 사용하여 테스트:

<#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
```

그런 다음 traceroute로 테스트합니다.

<#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*  *  *
…
```

3단계

캡처 내용을 확인합니다.

- 패킷 1-10은 ICMP ping 테스트와 관련됩니다.
- 패킷 11-16은 traceroute와 관련됩니다. 응답은 첫 번째 홉에서 옵니다.
- 패킷 17-28도 traceroute와 관련됩니다. 응답은 대상 끝점에서 옵니다.

<#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
```

4단계

ping 테스트에서 인그레스 ICMP 패킷을 추적합니다.

패킷 #2는 패킷 모드에서 보낸 ICMP ping 요청에 대한 #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
```

추적의 핵심 사항은 다음과 같습니다.

- 패킷이 기존 흐름과 일치합니다.
- 출력 인터페이스는 방화벽 자체(ID 인터페이스)입니다.

5단계

traceroute 테스트에서 인그레스 ICMP 패킷을 추적합니다.

패킷 #12은 트랜짓 호스트의 응답입니다.

<#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
```

- 패킷이 새 연결의 일부입니다(기존 흐름과 일치하지 않음).
- 패킷은 네트워크 주소 변환(특히 UN-NAT는 목적지 NAT를 의미함)의 적용을 받습니다.
- 패킷은 방화벽 통과 트래픽으로 처리되며 ACP(Access Control Policy) 및 Snort 검사의 대상

이 됩니다.

- 출력(이그레스) 인터페이스가 INSIDE입니다. NAT 변환 때문입니다.

원인

이 경우 다음과 같은 고정 NAT 규칙으로 인해 문제가 발생합니다.

```
<#root>

firepower#

show run nat

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

관련 콘텐츠

- FTD(Firepower 위협 방어)를 통한 Traceroute 허용
- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.