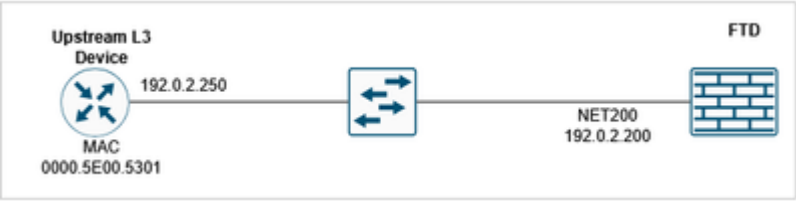
FTD 문제 해결 ARP 항목이 있어도 업스트림 디바이스를 Ping할 수 없음

목차

문제

방화벽이 업스트림 IP 주소에 대한 ARP 항목을 관찰할 수 있음에도 불구하고, FTD(Firewall Threat Defense)에서 업스트림 디바이스 IP 주소를 ping할 수 없습니다. ARP 테이블에는 예상 항목이 표시되어, 레이어 2 연결이 작동하지만 레이어 3 ping 트래픽이 차단되고 있음을 나타냅니다.

토폴로지



FTD CLI 증상

업스트림 IP 주소에 대한 Ping이 실패했습니다.

```
<#root>

device#

ping 192.0.2.250


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

업스트림 IP 주소에 대한 ARP 항목이 있습니다.

```
<#root>
device#

show arp



NET200 192.0.2.250 0000.5e00.5301

 47
```

FTD 인터페이스에서 추적을 사용하여 캡처를 활성화합니다.

```
<#root>
device#

capture CAPI interface NET200 trace match icmp host 192.0.2.200 host 192.0.2.250
```

ping 테스트 중 FTD LINA syslog:

```
<#root>
device#

show log | include 192.0.2.250


May 15 2026 09:46:26: %FTD-6-302020: Built outbound ICMP connection for faddr 192.0.2.250/0 gaddr 192.0
May 15 2026 09:46:26: %FTD-3-313001:

Denied ICMP type=0, code=0 from 192.0.2.250 on interface NET200


May 15 2026 09:46:26: %FTD-6-302021: Teardown ICMP connection for faddr 192.0.2.250/0 gaddr 192.0.2.200
...
```

패킷 캡처는 ICMP 에코 응답이 도착하는 것을 보여줍니다.

<#root>

device#

show capture CAPI

10 packets captured
   1: 09:46:26.649456   802.1Q vlan#200 P0 192.0.2.200 > 192.0.2.250 icmp: echo request
   2: 09:46:26.649883   802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply

   3: 09:46:28.642621   802.1Q vlan#200 P0 192.0.2.200 > 192.0.2.250 icmp: echo request
   4: 09:46:28.643002   802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply

...

ICMP 에코 응답의 패킷 추적은 패킷이 기존 연결과 예상대로 일치하며 출력 인터페이스가 FTD 인터페이스(NP Identity Ifc)임을 보여줍니다.

<#root>

device#

show capture CAPI packet-number 2 trace

10 packets captured
   2: 09:46:26.649883   802.1Q vlan#200 P0 192.0.2.250 > 192.0.2.200 icmp:

echo reply

...
Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 4096 ns
Config:
Additional Information:

Found flow with id 1400, using existing flow

```
...

Result:
input-interface: NET200(vrfid:0)
input-status: up
input-line-status: up

output-interface: NP Identity Ifc


Action: allow
Time Taken: 28672 ns
```

Debug ICMP trace(디버그 ICMP 추적)는 ICMP 에코 응답이 거부되고 있음을 보여줍니다.

<#root>

```
FTD220-5#

debug icmp trace


debug icmp trace enabled at level 1

FTD220-5#

ping 192.0.2.250


Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
ICMP echo request from self:192.0.2.200 to NET200:192.0.2.250 ID=49503 seq=15001 len=72

ICMP echo reply




from NET200:192.0.2.250 to self:192.0.2.200


 ID=49503 seq=15001 len=72

Denied ICMP type = 0, code = 0 from 192.0.2.250on interface 4


?
...
Success rate is 0 percent (0/5)
```

⚠ 주의: 디버그를 신중하게 사용하십시오!

ICMP 디버그를 끄려면

<#root>

device#

no debug icmp trace

debug icmp trace disabled.

환경

FTD 10.x 다른 소프트웨어 버전도 영향을 받습니다.

해결

ping 트래픽을 거부하던 플랫폼 설정에서 ICMP 규칙 컨피그레이션을 식별하고 수정하여 문제가 해결되었습니다. 해결책에는 다음 단계가 포함됩니다.

1단계. ARP 테이블 항목 확인

업스트림 IP 주소에 대한 ARP 항목이 방화벽의 ARP 테이블에 표시되는지 확인합니다. 이는 레이어 2 연결이 제대로 작동하고 있음을 나타냅니다.

<#root>

device#

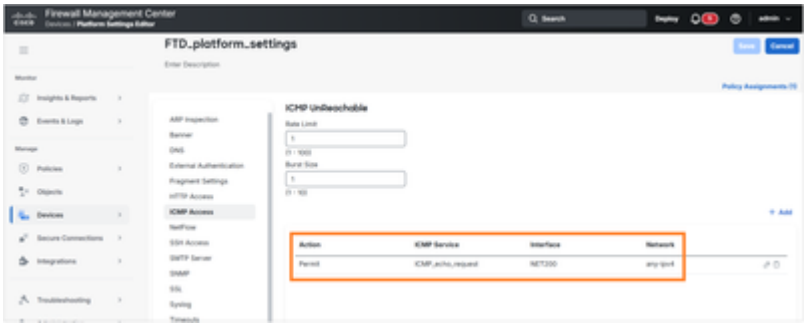
```
show arp
```

2단계. ICMP 규칙에 대한 플랫폼 설정 확인

플랫폼 설정 컨피그레이션으로 이동하여 ping 트래픽에 영향을 줄 수 있는 ICMP 규칙 정책을 검사합니다. 특히 ICMP 에코 요청/응답 패킷을 차단하거나 거부할 수 있는 규칙을 찾습니다.

3단계. 차단 ICMP 규칙 식별 및 수정

Ping 트래픽을 거부하도록 구성된 플랫폼 설정에서 ICMP 규칙을 찾습니다.



이 예에서 ICMP 규칙은 FTD 인터페이스에서 ICMP 에코 요청만 수락하도록 허용합니다.

FTD CLI 확인:

```
<#root>
device#

show run icmp


icmp unreachable rate-limit 1 burst-size 1

icmp permit any echo NET200
```

4단계. ICMP 규칙 컨피그레이션 업데이트

확인된 ICMP 규칙을 수정하여 ping 트래픽을 허용하거나, 네트워크 보안 요구 사항 및 운영 요구에 맞게 차단 컨피그레이션을 제거합니다.

결과 ICMP 규칙:

<#root>

```
device#
```

show run icmp

```
icmp unreachable rate-limit 1 burst-size 1
icmp permit any echo NET200
```

icmp permit 192.0.2.0 255.255.255.0 echo-reply NET200

5단계. 연결 테스트

컨피그레이션을 변경한 후 업스트림 IP 주소에 대한 ping 연결을 테스트하여 문제가 해결되었으며 ICMP 트래픽이 현재 제대로 흐르고 있는지 확인합니다.

<#root>

```
device#
```

ping 192.0.2.250

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.250, timeout is 2 seconds:
!!!!!
```

Success rate is 100 percent (5/5)

```
, round-trip min/avg/max = 1/1/1 ms
```

원인

이 문제의 근본 원인은 ICMP 에코 응답 트래픽을 명시적으로 거부하는 플랫폼 설정에 구성된 ICMP 규칙입니다. 방화벽이 적절한 레이어 2 연결을 유지했지만(표시되는 ARP 항목에서 나타남), 플랫폼 레벨 ICMP 규칙은 레이어 3 ICMP 에코 응답 패킷을 차단하여 업스트림 IP 주소에 대한 성공적인 ping 작업을 방지했습니다. 이러한 컨피그레이션 유형은 보안 정책이 ICMP 트래픽을 제한하기 위해 구현되지만, 실수로 합법적인 네트워크 연결 테스트 및 모니터링에 영향을 미칠 수 있는 경우 발생할 수 있습니다.

관련 콘텐츠

- https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/100/management-center-device-config-10-0/interfaces-settings-platform.html#task_42BBA666CD604517ADA18B32CA162F62
- https://www.cisco.com/c/en/us/td/docs/security/asa/asa-cli-reference/I-R/asa-command-ref-I-R/ia-inr-commands.html#wp1366339900
- 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.