FTD(Firepower 위협 방어)를 통한 Traceroute 허용

목차

소개

이 문서에서는 Threat Service Policy를 통해 FTD(Firepower Threat Defense)를 통한 traceroute를 허용하는 컨피그레이션에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- FMC(Firepower Management Center)
- FTD(Firepower Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 이 문서는 모든 Firepower 플랫폼에 적용됩니다.
- 소프트웨어 버전 6.4.0을 실행하는 Cisco Firepower 위협 방어
- 소프트웨어 버전 6.4.0을 실행하는 Cisco Firepower Management Center Virtual

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

Traceroute - 패킷이 목적지로 이동하는 경로를 결정하는 데 도움이 됩니다. traceroute는 UDP(Unified Data Platform) 패킷을 잘못된 포트의 대상으로 전송하는 방식으로 작동합니다. 포트가 유효하지 않기 때문에, 목적지로 가는 동안 라우터는 ICMP(Internet Control Message Protocol) 시간 초과 메시지로 응답하고 ASA(Adaptive Security Appliance)에 오류를 보고합니다.

traceroute에는 전송된 각 프로브의 결과가 표시됩니다. 각 출력 행은 증가하는 순서의 TTL(Time to Live) 값에 해당합니다. 이 표에서는 출력 기호에 대해 설명합니다.

출력 기호	설명
*	시간 초과 기간 내에 프로브에 대한 응답을 받지 못했습니다.
nn msec	각 노드에 대해 지정된 프로브 수에 대한 왕복 시간(밀리초)입니다.
!네트워킹	ICMP 네트워크에 연결할 수 없습니다.
!H	ICMP 호스트에 연결할 수 없습니다.
!P	ICMP에 연결할 수 없습니다.
!A	관리상 ICMP가 금지되었습니다.
?	알 수 없는 ICMP 오류입니다.

기본적으로 ASA는 traceroute에 홉으로 나타나지 않습니다. ASA를 통과하는 패킷에서 TTL(Time-To-Live)을 줄이고 ICMP 도달 불가 메시지에 대한 속도 제한을 늘려야 나타납니다.

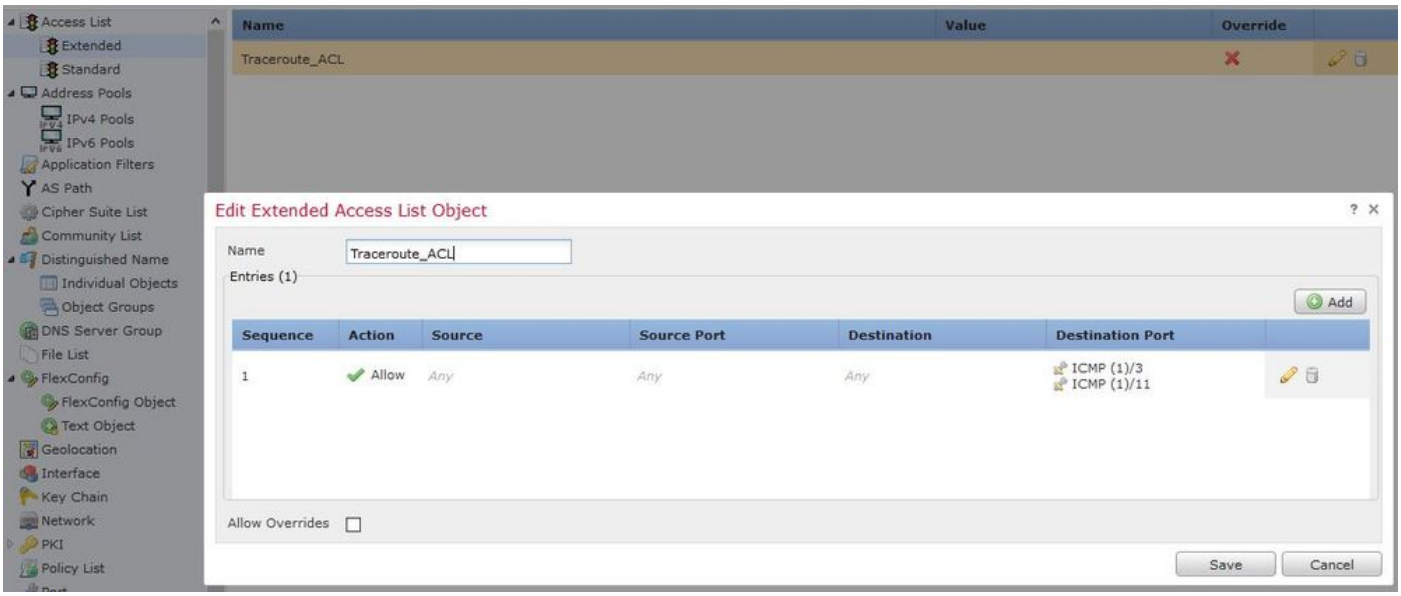
⚠ 주의: TTL이 1인 패킷은 삭제되지만, 연결에 TTL이 더 큰 패킷이 포함될 수 있다는 가정 하에 세션에 대한 연결이 열립니다. OSPF hello 패킷과 같은 일부 패킷은 TTL = 1로 전송되므로 TTL(Time To Live)이 감소하면 예기치 않은 결과가 발생할 수 있습니다. 트래픽 클래스를 정의할 때는 이러한 사항을 염두에 두어야 합니다.

구성

1단계. traceroute 보고를 활성화해야 하는 트래픽 클래스를 정의하는 확장 ACL을 생성합니다.

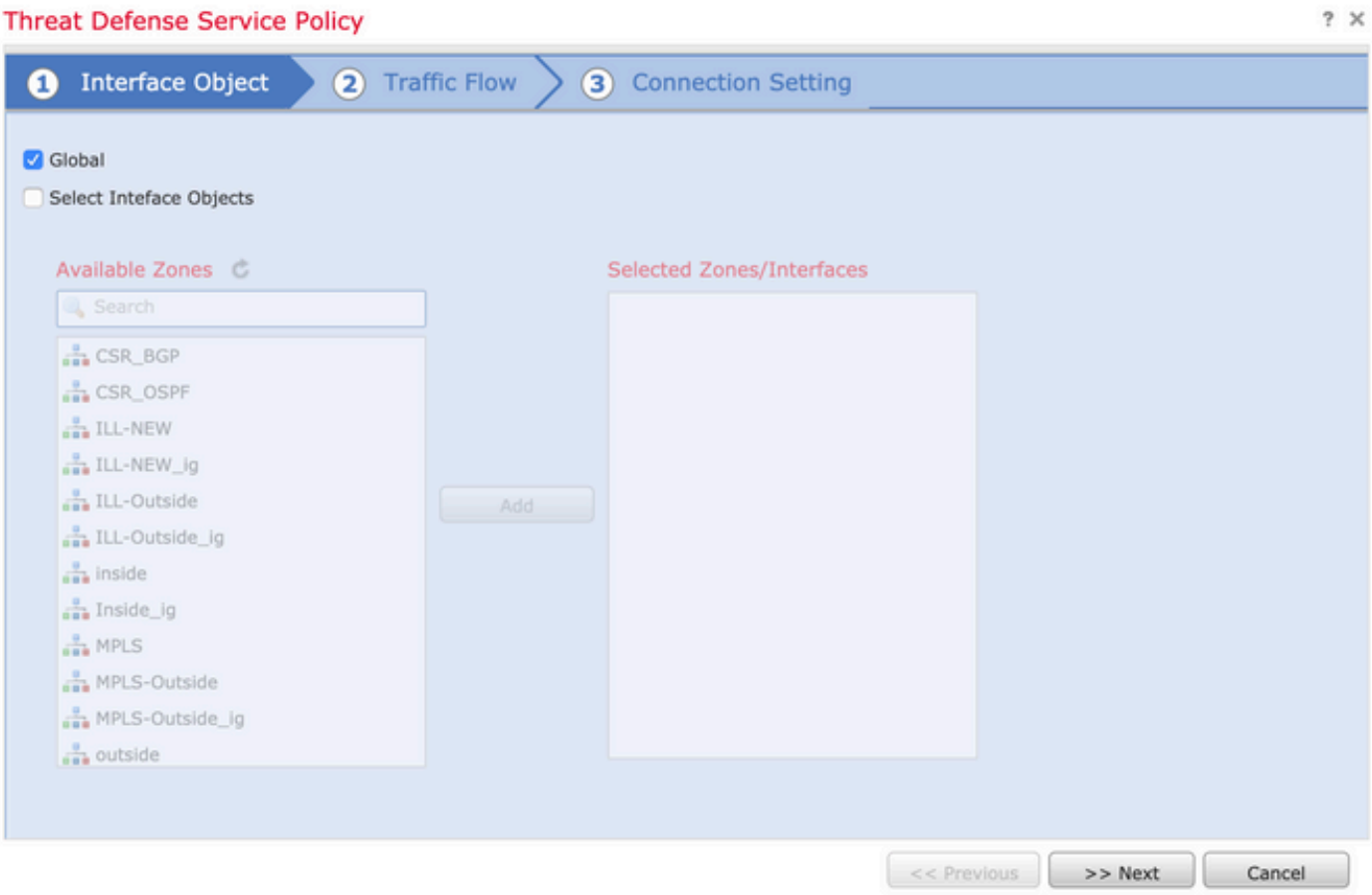
FMC GUI에 로그인하고 Objects(개체) > Object Management(개체 관리) > Access List(액세스 목록)로 이동합니다. 목차에서 Extended를 선택하고 새 Extended Access List를 추가합니다

.Traceroute_ACL 아래에 객체의 이름을 입력하고 이미지에 표시된 대로 ICMP 유형 3 및 11을 허용하는 규칙을 추가합니다.

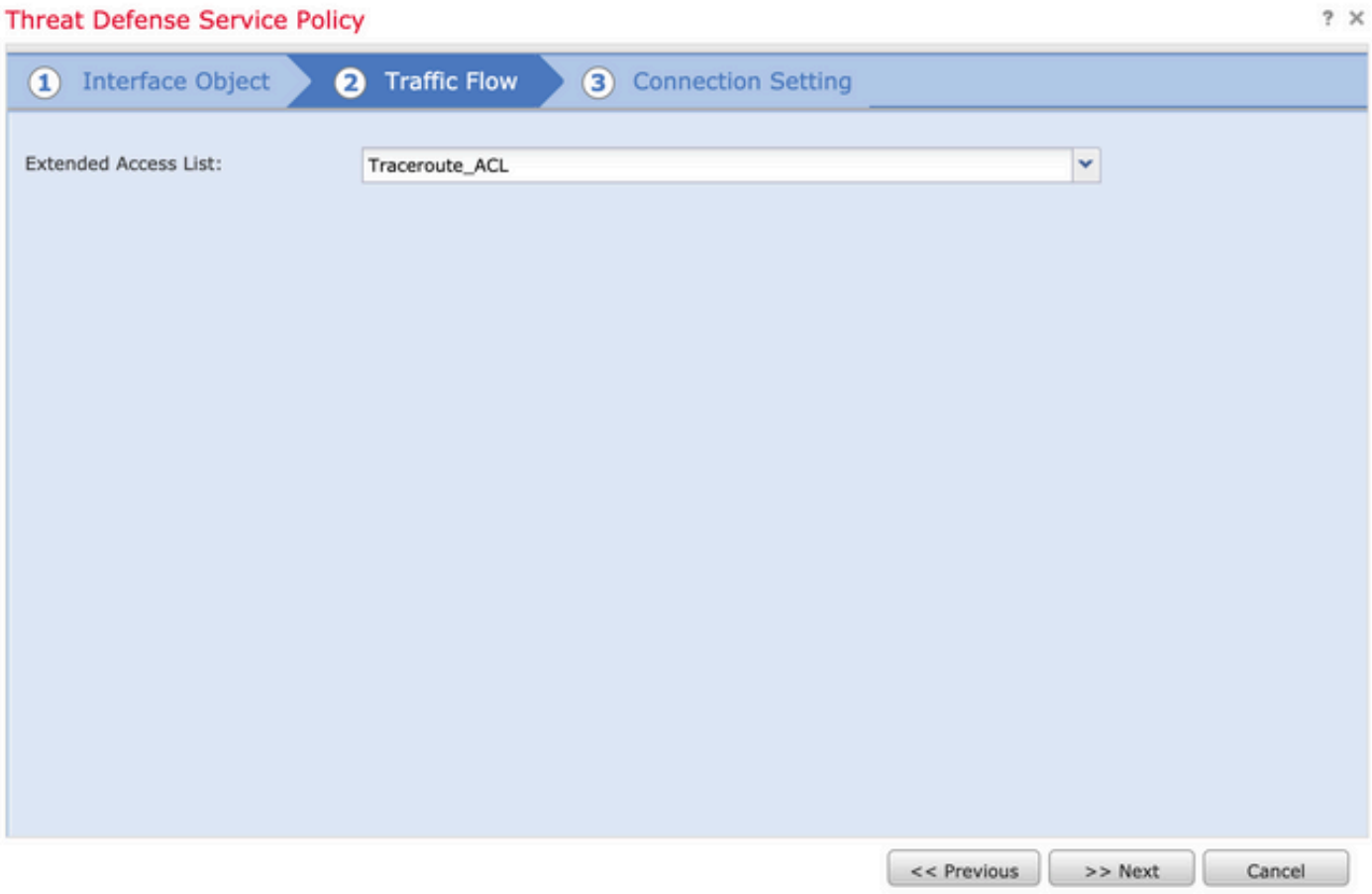


2단계. TTL(time-to-live) 값을 줄이는 서비스 정책 규칙을 구성합니다.

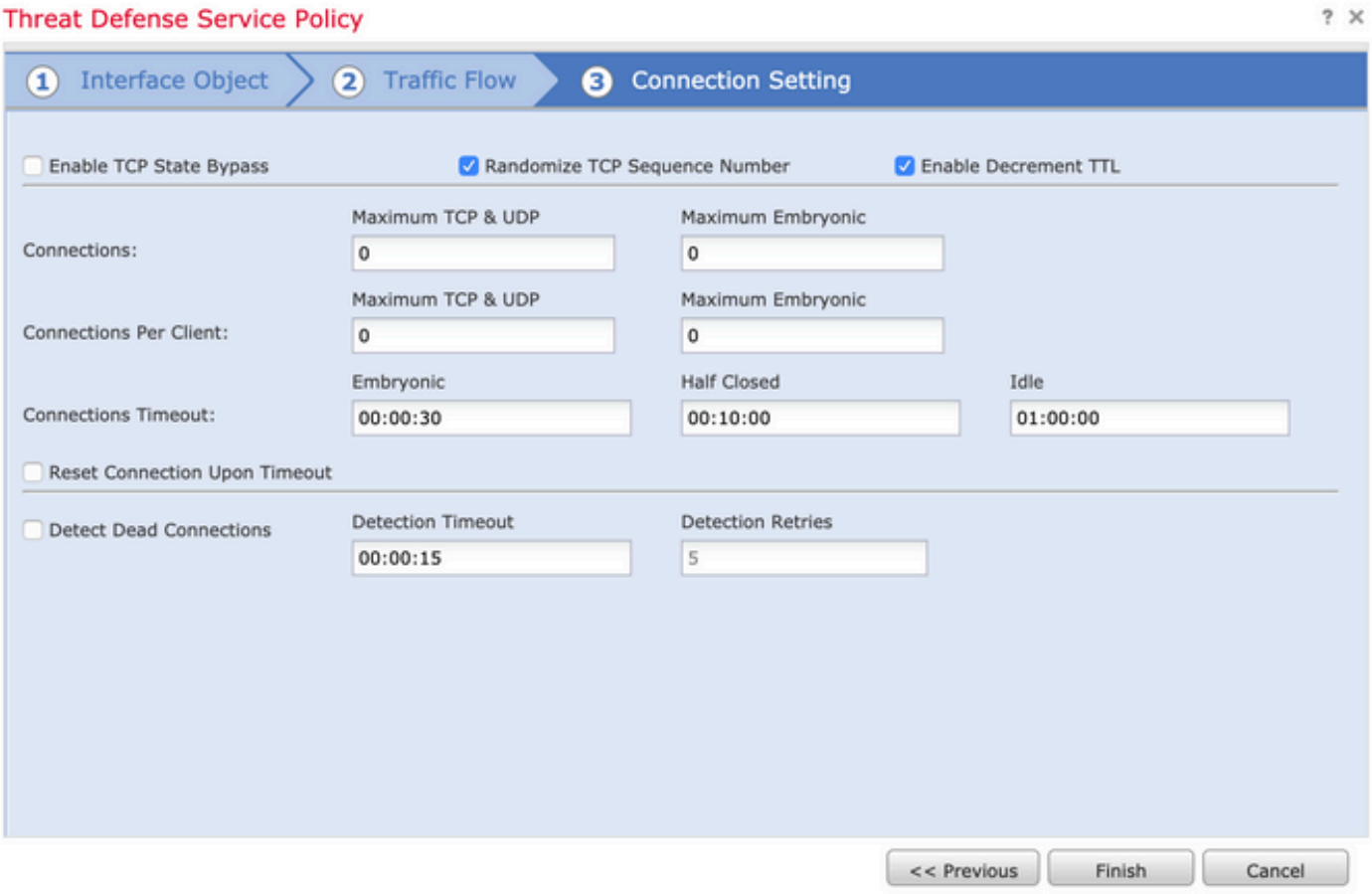
Policies(정책) > Access Control(액세스 제어)로 이동한 다음 디바이스에 할당된 정책을 수정합니다. Advanced(고급) 탭에서 Threat Defense Service Policy(위협 방어 서비스 정책)를 편집한 다음 Add Rule(규칙 추가) 탭에서 새 규칙을 추가한 다음 Global(전역) 확인란을 선택하여 전역으로 적용하고 Next(다음)를 클릭합니다.



Traffic Flow > Extended Access List(트래픽 흐름> 확장 액세스 목록)로 이동한 다음 이전 단계에서 만든 드롭다운 메뉴에서 Extended Access List Object(확장 액세스 목록 개체)를 선택합니다. 이제 다음을 클릭합니다.



Enable Decrement TTL(TTL 감소 활성화) 확인란을 선택하고 다른 연결 옵션을 수정합니다(선택 사항). 이제 Finish(마침)를 클릭하여 규칙을 추가한 다음 OK(확인)를 클릭하고 다음 그림과 같이 Threat defense 서비스 정책의 변경 사항을 저장합니다.

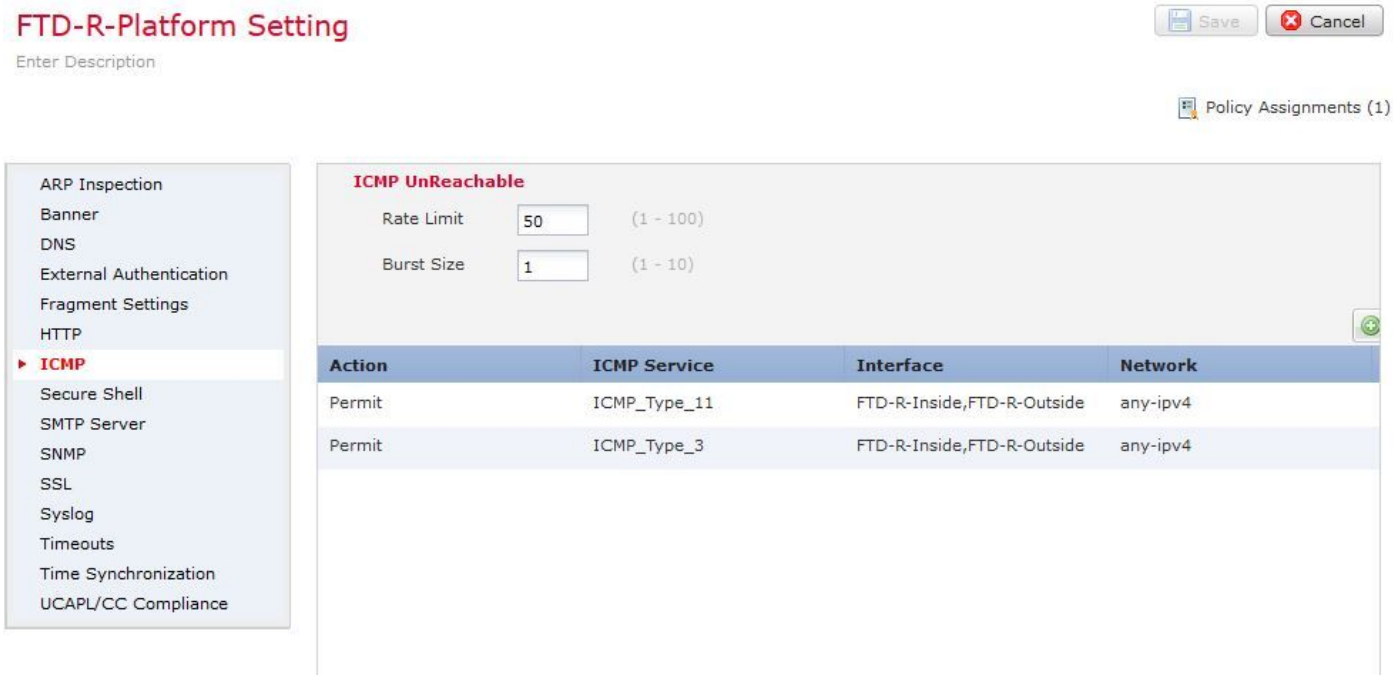


이전 단계가 완료되면 액세스 제어 정책을 저장합니다.

3단계. 내부 및 외부에서 ICMP를 허용하고 속도 제한을 50(선택 사항)으로 늘립니다.

Devices(디바이스) > Platform Settings(플랫폼 설정)로 이동한 다음 Edit(편집) 또는 Create a new Firepower Threat Defense 플랫폼 설정 정책을 수정하고 디바이스에 연결합니다. 콘텐츠 테이블에서 ICMP를 선택하고 Rate Limit(속도 제한)을 늘립니다. 예를 들어, 50까지(Burst Size(버스트 크기)를 무시할 수 있음)를 설정한 다음 Save(저장)를 클릭하고 이미지에 표시된 대로 Deploy the Policy to the device(디바이스에 정책 구축)로 진행합니다.

- Rate Limit(속도 제한) - 연결할 수 없는 메시지의 속도 제한을 설정합니다(초당 메시지 1~100개). 기본값은 초당 메시지 1개입니다.
- Burst Size(버스트 크기) - 버스트 속도를 1에서 10 사이로 설정합니다. 이 값은 현재 시스템에서 사용되지 않습니다.



⚠ 주의: ICMP Destination Unreachable(Type 3) 및 ICMP Time Exceeded(ICMP 시간 초과)(Type 11)가 ACL 정책 또는 사전 필터 정책의 Fastpath에서 Outside에서 Inside로 허용되는지 확인합니다.

다음을 확인합니다.

정책 구축이 완료되면 FTD CLI에서 컨피그레이션을 확인합니다.

```
FTD# show run policy-map
!
policy-map type inspect dns preset_dns_map
---Output omitted---

class class_map_Traceroute_ACL
set connection timeout idle 1:00:00
set connection decrement-ttl
class class-default
!

FTD# show run class-map
!
class-map inspection_default

---Output omitted---

class-map class_map_Traceroute_ACL
match access-list Traceroute_ACL
!

FTD# show run access-l Traceroute_ACL
access-list Traceroute_ACL extended permit object-group ProxySG_ExtendedACL_30064773500 any any log
FTD#
```

문제 해결

FTD 인그레스 및 이그레스 인터페이스에서 캡처하여 흥미로운 트래픽으로 문제를 더 자세히 해결할 수 있습니다.

Lina의 패킷 캡처는 traceroute가 수행되는 동안 대상 IP에 도달할 때까지 경로의 각 희망에 대해 이와 같이 표시될 수 있습니다.

```
ftd64# capture icmp interface inside real-time match icmp any any

Warning: using this option with a slow console connection may
         result in an excessive amount of non-displayed packets
         due to performance limitations.

Use ctrl-c to terminate real-time capture


   1: 00:22:04.192800       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   2: 00:22:04.194432       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   3: 00:22:04.194447       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   4: 00:22:04.194981       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   5: 00:22:04.194997       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   6: 00:22:04.201130       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   7: 00:22:04.201146       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   8: 00:22:04.201161       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   9: 00:22:04.201375       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  10: 00:22:04.201420       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  11: 00:22:04.202336       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
  12: 00:22:04.202519       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  13: 00:22:04.216022       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  14: 00:22:04.216038       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
  15: 00:22:04.216038       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  16: 00:22:04.216053       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
  17: 00:22:04.216297       172.18.127.245 > 10.10.10.11 icmp: 172.18.127.245 udp port 33452 unreachabl
  18: 00:22:04.216312       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
  19: 00:22:04.216327       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
```

나열된 "-I" 및 "-n" 스위치로 traceroute를 수행하는 경우 Lina CLI에서 보다 자세한 출력을 얻을 수 있습니다.

```
[ On the Client PC ]

# traceroute 10.18.127.245 -I -n

Note: You may not observe any difference between traceroute with or without -I switch. The difference i


[ On FTD Lina CLI ]

ftd64# capture icmp interface inside real-time match icmp any any

Warning: using this option with a slow console connection may
```

```
        result in an excessive amount of non-displayed packets
        due to performance limitations.

Use ctrl-c to terminate real-time capture


    1: 18:37:33.517307       10.10.10.11 > 172.18.127.245 icmp: echo request
    2: 18:37:33.517642       10.10.10.11 > 172.18.127.245 icmp: echo request
    3: 18:37:33.517658       10.10.10.11 > 172.18.127.245 icmp: echo request
    4: 18:37:33.517658       10.10.10.11 > 172.18.127.245 icmp: echo request
    5: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
    6: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
    7: 18:37:33.517673       10.10.10.11 > 172.18.127.245 icmp: echo request
    8: 18:37:33.517749       10.10.10.11 > 172.18.127.245 icmp: echo request
    9: 18:37:33.517749       10.10.10.11 > 172.18.127.245 icmp: echo request
   10: 18:37:33.517764       10.10.10.11 > 172.18.127.245 icmp: echo request
   11: 18:37:33.517764       10.10.10.11 > 172.18.127.245 icmp: echo request
   12: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
   13: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
   14: 18:37:33.517826       10.10.10.11 > 172.18.127.245 icmp: echo request
   15: 18:37:33.517932       10.10.10.11 > 172.18.127.245 icmp: echo request
   16: 18:37:33.517932       10.10.10.11 > 172.18.127.245 icmp: echo request
   17: 18:37:33.522464       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   18: 18:37:33.522510       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   19: 18:37:33.522510       10.0.0.1 > 10.10.10.11 icmp: time exceeded in-transit
   20: 18:37:33.522632       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   21: 18:37:33.522647       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   22: 18:37:33.522647       172.16.1.1 > 10.10.10.11 icmp: time exceeded in-transit
   23: 18:37:33.523852       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
   24: 18:37:33.523929       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
   25: 18:37:33.523944       10.0.114.197 > 10.10.10.11 icmp: time exceeded in-transit
   26: 18:37:33.524066       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
   27: 18:37:33.524127       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
   28: 18:37:33.524127       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
   29: 18:37:33.524142       10.0.127.113 > 10.10.10.11 icmp: time exceeded in-transit
   30: 18:37:33.526767       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   31: 18:37:33.526843       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   32: 18:37:33.526843       10.122.149.1 > 10.10.10.11 icmp: time exceeded in-transit
   33: 18:37:33.527652       10.10.10.11 > 172.18.127.245 icmp: echo request
   34: 18:37:33.527697       10.10.10.11 > 172.18.127.245 icmp: echo request
   35: 18:37:33.527713       10.10.10.11 > 172.18.127.245 icmp: echo request
   36: 18:37:33.527728       10.10.10.11 > 172.18.127.245 icmp: echo request
   37: 18:37:33.527987       10.10.10.11 > 172.18.127.245 icmp: echo request
   38: 18:37:33.528033       10.10.10.11 > 172.18.127.245 icmp: echo request
   39: 18:37:33.528048       10.10.10.11 > 172.18.127.245 icmp: echo request
   40: 18:37:33.528048       10.10.10.11 > 172.18.127.245 icmp: echo request
   41: 18:37:33.528064       10.10.10.11 > 172.18.127.245 icmp: echo request
   42: 18:37:33.528064       10.10.10.11 > 172.18.127.245 icmp: echo request
   43: 18:37:33.528079       10.10.10.11 > 172.18.127.245 icmp: echo request
   44: 18:37:33.528094       10.10.10.11 > 172.18.127.245 icmp: echo request
   45: 18:37:33.528094       10.10.10.11 > 172.18.127.245 icmp: echo request
   46: 18:37:33.532870       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
   47: 18:37:33.532885       10.0.254.225 > 10.10.10.11 icmp: time exceeded in-transit
   48: 18:37:33.533679       172.18.127.245 > 10.10.10.11 icmp: echo reply
   49: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
   50: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
   51: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
   52: 18:37:33.533694       172.18.127.245 > 10.10.10.11 icmp: echo reply
   53: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
   54: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
   55: 18:37:33.533724       172.18.127.245 > 10.10.10.11 icmp: echo reply
   56: 18:37:33.533740       10.10.10.11 > 172.18.127.245 icmp: echo request
```

```
  57: 18:37:33.533816       10.10.10.11 > 172.18.127.245 icmp: echo request
  58: 18:37:33.533831       10.10.10.11 > 172.18.127.245 icmp: echo request
  59: 18:37:33.537066       172.18.127.245 > 10.10.10.11 icmp: echo reply
  60: 18:37:33.537081       172.18.127.245 > 10.10.10.11 icmp: echo reply
  61: 18:37:33.537081       172.18.127.245 > 10.10.10.11 icmp: echo reply
  62: 18:37:33.538500       172.18.127.245 > 10.10.10.11 icmp: echo reply
  63: 18:37:33.538500       172.18.127.245 > 10.10.10.11 icmp: echo reply
  64: 18:37:33.539217       172.18.127.245 > 10.10.10.11 icmp: echo reply
64 packets shown.
0 packets not shown due to performance limitations.
```

팁: Cisco 버그 ID CSCvq79913. ICMP 오류 패킷은 Null pdts_info에 대해 삭제됩니다. ICMP의 경우 프리필터를 사용하고, 3 및 11 반환 트래픽의 경우 프리필터를 사용하는 것이 좋습니다.

관련 정보

기술 지원 및 문서 – Cisco Systems

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.