允许Traceroute通过Firepower威胁防御(FTD)

目录

简介

本文档介绍通过威胁服务策略允许traceroute通过Firepower威胁防御(FTD)的配置。

先决条件

要求

Cisco 建议您了解以下主题：

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

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 本文适用于所有Firepower平台。
- 运行软件版本6.4.0的Cisco Firepower威胁防御。
- 运行软件版本6.4.0的Cisco Firepower管理中心虚拟。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Traceroute，帮助您确定数据包通往目的地所采用的路由。traceroute的工作原理是将统一数据平台(UDP)数据包发送到无效端口上的目的地。由于端口无效，沿途的路由器会以Internet控制消息协议(ICMP)超时消息做出响应，并将该错误报告给自适应安全设备(ASA)。

traceroute显示发送的每个探测的结果。每行输出都对应一个生存时间(TTL)值（按递增顺序）。下表说明了输出符号。

输出符号	描述
*	在超时期限内未收到探测的响应。
nn msec	对于每个节点，指定数量的探测的往返时间（以毫秒为单位）。
!N	ICMP网络不可达。
!H	ICMP主机无法访问。
!P	ICMP不可达。
!A	ICMP管理性禁止。
?	未知的ICMP错误。

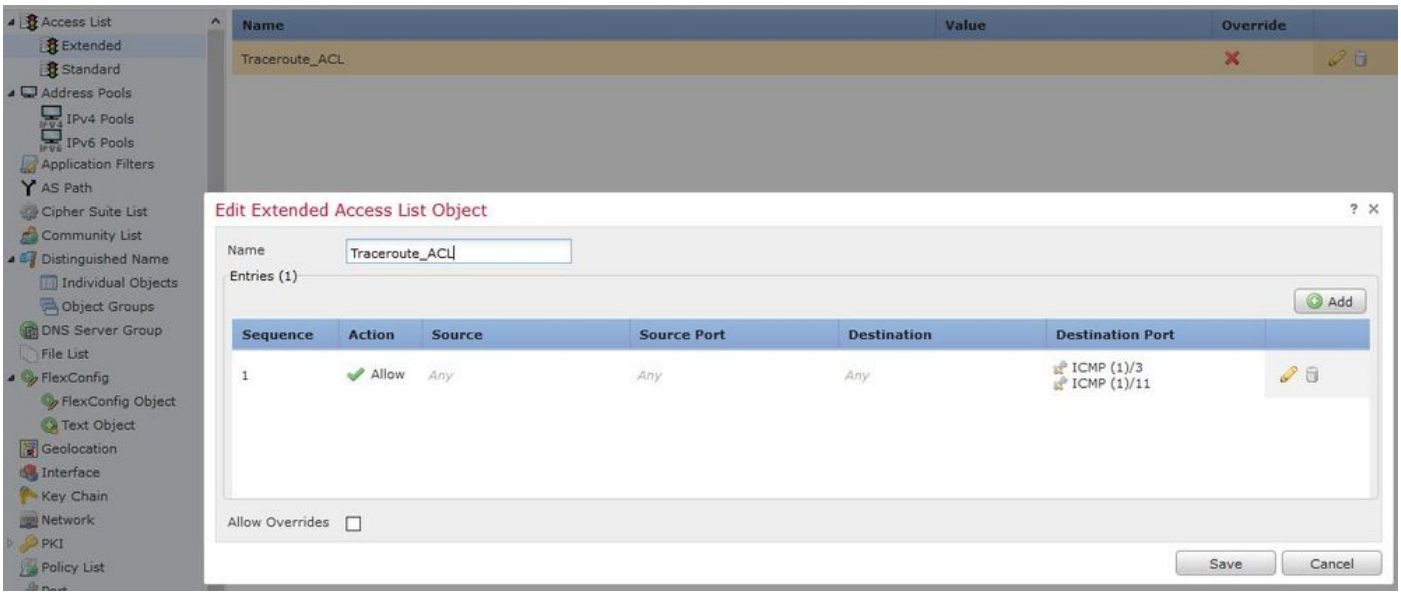
默认情况下，ASA在traceroute上不会显示为跃点。要使其显示，您需要缩短通过ASA的数据包的生存时间，并增加ICMP不可达消息的速率限制。

⚠ 注意：如果减少生存时间，则TTL为1的数据包将被丢弃，但会为会话打开一个连接，前提是该连接可以包含具有较大TTL的数据包。请注意，某些数据包（例如OSPF hello数据包）使用TTL = 1发送，因此缩短生存时间可能会产生意外的后果。在定义流量类时，请记住这些注意事项。

配置

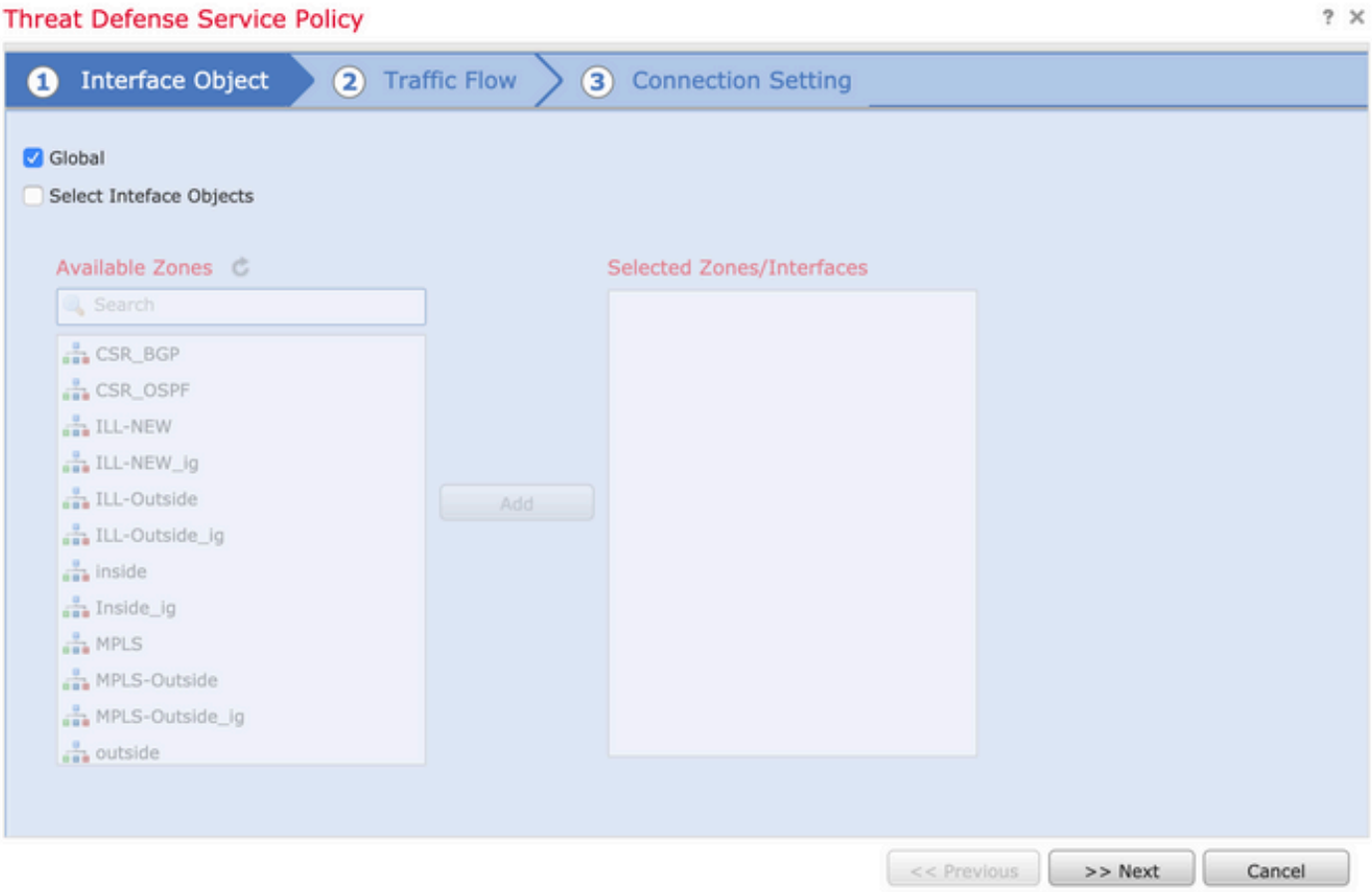
步骤1:创建扩展ACL，定义需要为其启用traceroute报告的流量类。

登录到FMC GUI，然后导航到对象(Objects)>对象管理(Object Management)>访问列表(Access List)。 从目录中选择Extended,Add a new Extended Access List。输入对象的名称，例如，在Traceroute_ACL下，Add规则允许ICMP类型3和11并保存，如图所示：

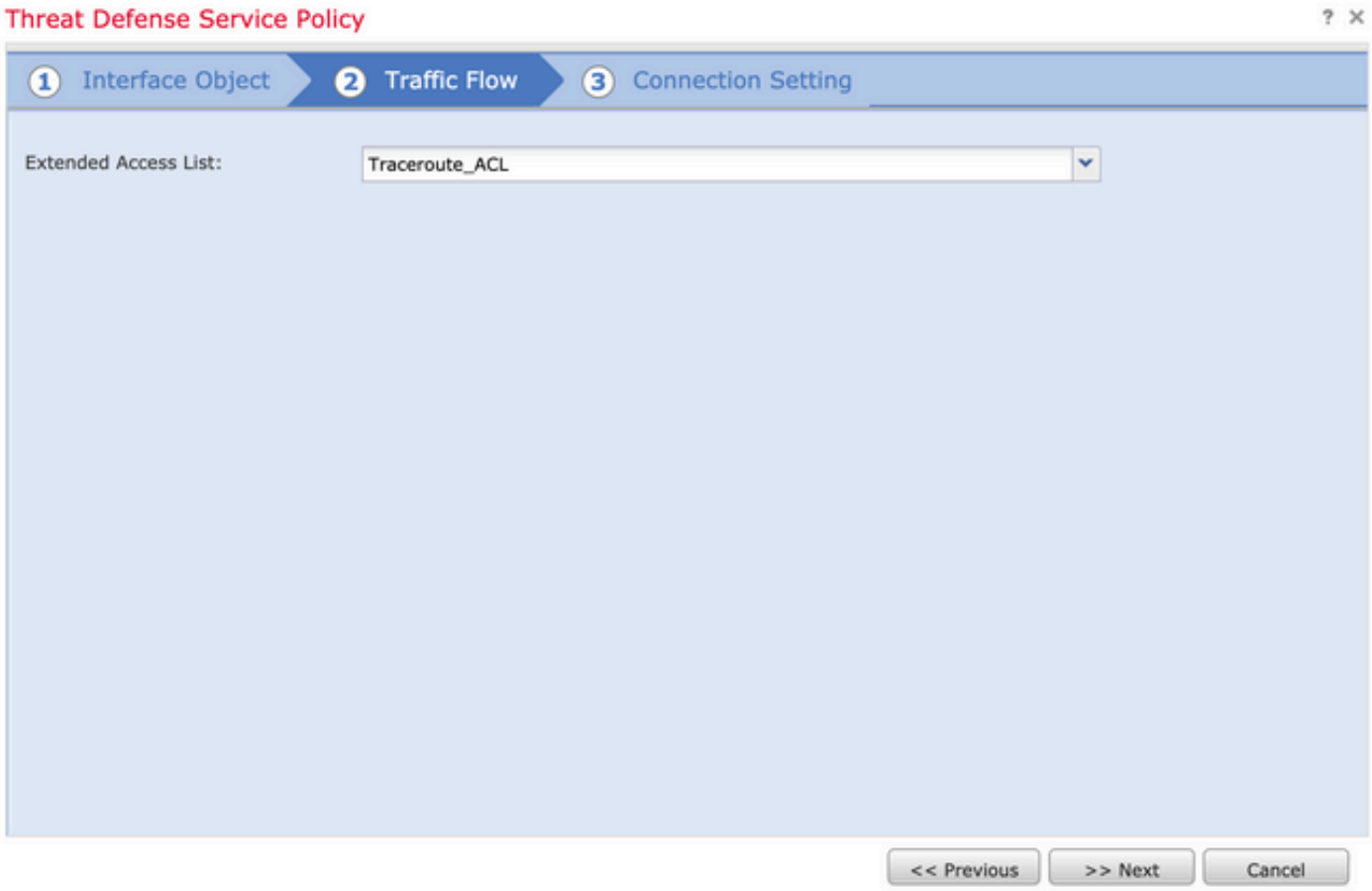


第二步：配置减少生存时间值的服务策略规则。

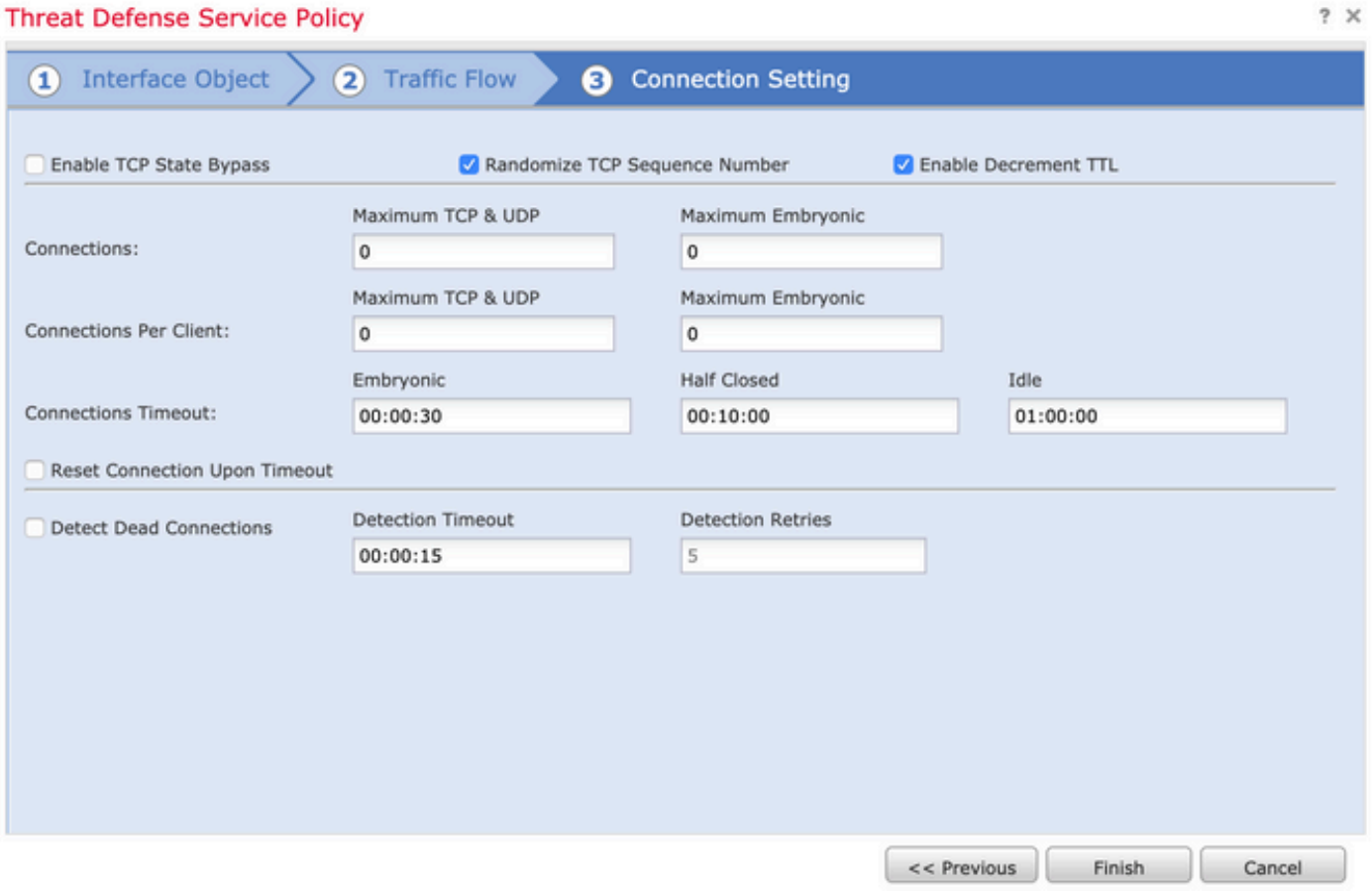
导航到Policies > Access Control ，然后单击Edit分配给设备的策略。在Advanced选项卡下，编辑Threat Defense Service Policy，然后从Add Rule选项卡中添加新规则，然后选中Global复选框以全局应用该规则，然后单击Next，如下图所示：



导航到Traffic Flow > Extended Access List，然后从在先前步骤中创建的下拉菜单中选择Extended Access List Object。现在单击下一步，如图所示：



选中Enable Decrement TTL复选框并修改其他连接选项（可选）。现在，单击Finish添加规则，然后单击OK，然后单击Save保存对威胁防御服务策略的更改，如图所示：

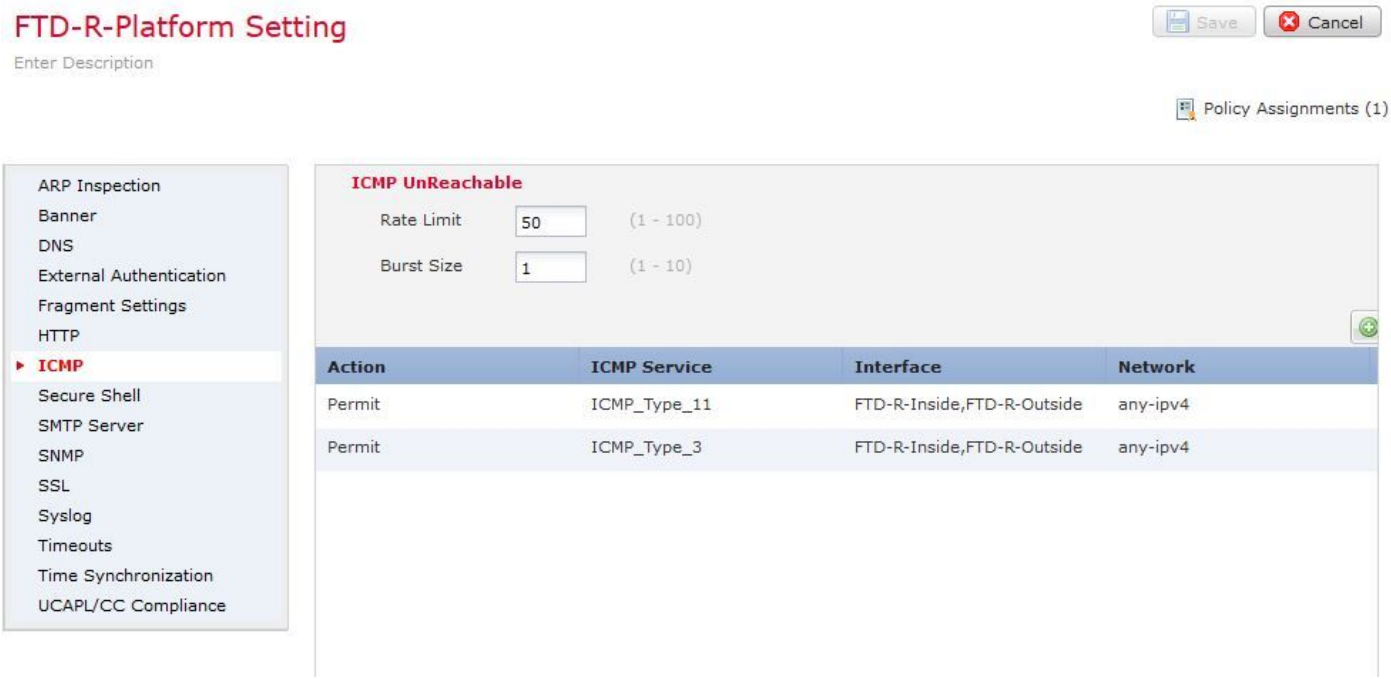


完成上述步骤后，请保存访问控制策略。

第三步：允许内部和外部的ICMP，并将速率限制增加到50（可选）。

导航到设备>平台设置，然后依次导航到编辑或创建新的Firepower威胁防御平台设置策略，并将其与设备关联。从内容表中选择ICMP并增大速率限制。例如，设置为50（您可以忽略突发大小），然后单击Save，然后继续Deploy策略到设备，如图所示：

- Rate Limit — 设置不可达消息的速率限制，该值为每秒1到100条消息。默认为每秒1条消息。
- Burst Size — 设置突发速率，介于1和10之间。系统当前未使用此值。



⚠ 注意：确保ACL策略中允许从外部到内部或预过滤器策略中允许的ICMP目标无法到达（类型3）和ICMP超时（类型11）。

验证

完成策略部署后，从FTD CLI检查配置：

```
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#
```

故障排除

您可以在FTD入口和出口接口上捕获相关流量，以进一步排除问题。

在Lina上捕获数据包时，在执行traceroute时，可以针对路由上的每个希望显示此数据包，直到它到达目标IP。

```
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
```

如果您使用列出的“ — I”和“ — n”交换机执行traceroute，则可以在Lina CLI上获取更详细的输出。

[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.
```

提示：Cisco Bug ID CSCvq79913。对于Null pdts_info，会丢弃ICMP错误数据包。确保对ICMP使用预过滤器，最好是对3类和11类返回流量使用预过滤器。

相关信息

技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。