# firepower脅威対策(FTD)によるTracerouteの許可

## 内容



## はじめに

このドキュメントでは、Threat Service Policy(TSP)経由でFirepower Threat Defense(FTD)を介してtracerouteを許可するための設定について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

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

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- この記事は、すべてのFirepowerプラットフォームに適用されます。
- firepowerバージョン6.4.0が稼働するCisco Software Threat Defense(FTD)
- firepowerバージョン6.4.0が稼働するCisco Software Management Center Virtual(CIMC)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 背景説明

tracerouteを使用すると、パケットが宛先に到達するまでに経由するルートを特定できます。tracerouteは、Unified Data Platform(UDP)パケットを無効なポート上の宛先に送信することによって機能します。ポートが有効でないため、宛先までの経路にあるルータはインターネット制御メッセージプロトコル(ICMP)の「Time Exceeded」メッセージで応答し、そのエラーを適応型セキュリティアプライアンス(ASA)に報告します。

tracerouteは、送信された各プローブの結果を示します。出力の各行は、Time to Live（TTL；存続可能時間）値に昇順で対応しています。次の表に、出力シンボルの説明を示します。

| 出力シンボル | 説明 |
|---|---|
| * | タイムアウト期間内にプローブに対する応答が受信されませんでした。 |
| nn msec | 各ノードについて、指定されたプローブ数のラウンドトリップ時間（ミリ秒）。 |
| !N | ICMPネットワークに到達できません。 |
| !H | ICMPホストに到達できません。 |
| !P | ICMPに到達できません。 |
| !A | ICMPは管理上禁止されています。 |
| ? | 不明なICMPエラーです。 |

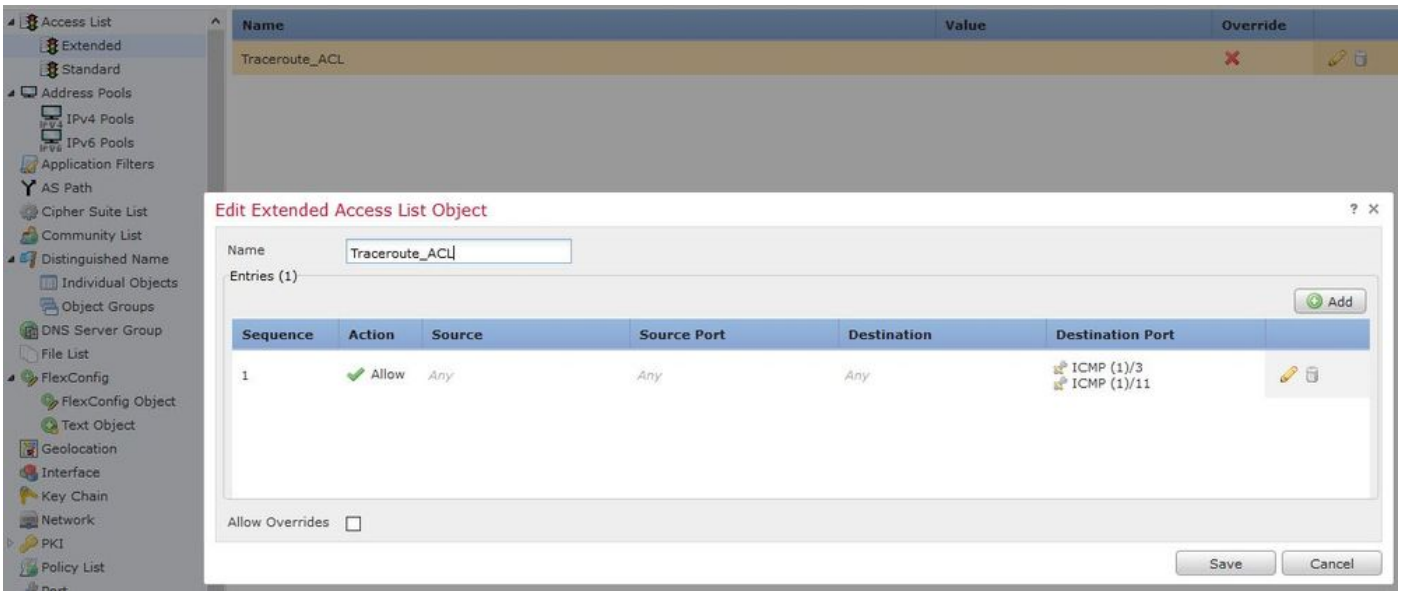
デフォルトでは、ASAはtracerouteにホップとして表示されません。これを表示するには、ASAを通過するパケットの存続可能時間(TTL)を減らし、ICMP到達不能メッセージのレート制限を増やす必要があります。

⚠ 注意：存続可能時間(TTL)を減らすと、TTLが1のパケットはドロップされますが、接続がより大きなTTLのパケットを含むことができるという前提で、セッションに対して接続が開かれます。OSPF helloパケットなど、一部のパケットはTTL = 1で送信されるため、存続可能時間(TTL)を減らすと予期しない結果が生じる可能性があることに注意してください。トラフィッククラスを定義する際は、次の点に注意してください。

## 設定

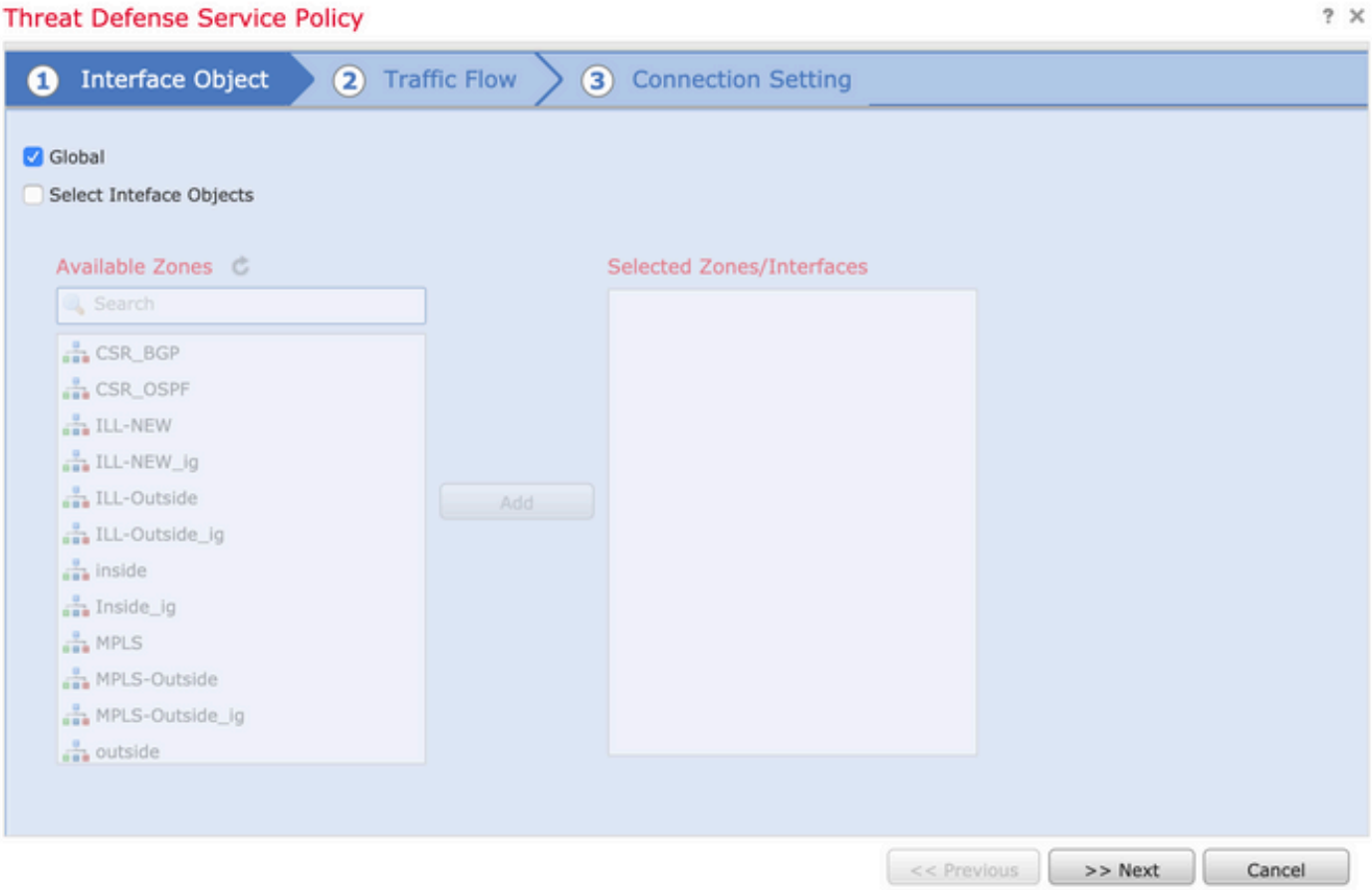
ステップ 1：traceroute レポートを有効にする必要があるトラフィッククラスを定義する拡張 ACL を作成します。

FMC GUIにログインし、Objects > Object Management > Access Listの順に移動します。 目次からExtendedを選択し、新しい拡張アクセスリストを追加します。オブジェクトの名前を入力します。たとえば、次の図に示すように、Traceroute_ACLでICMPタイプ3と11を許可するルールを追加して保存します。

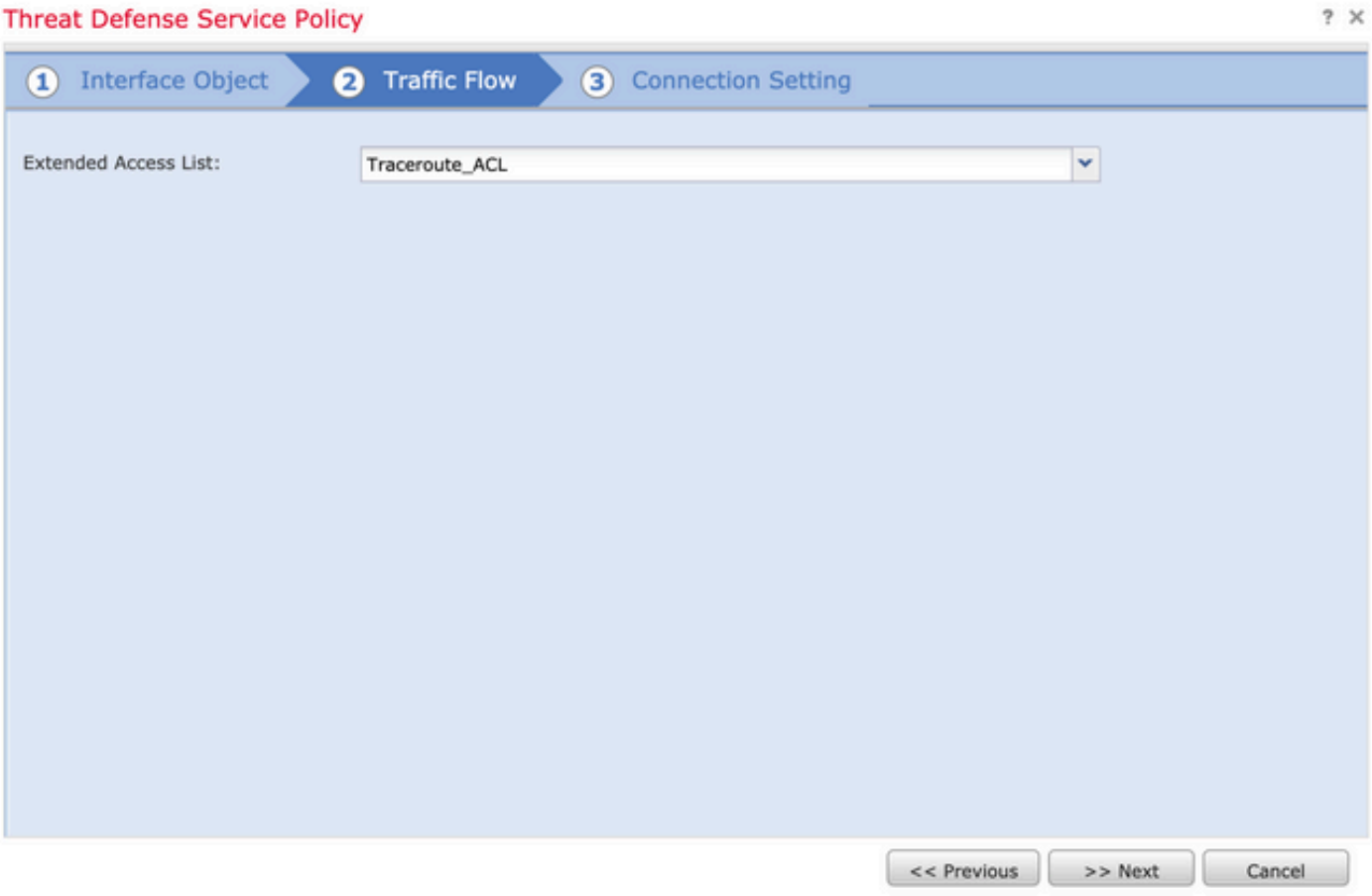



ステップ 2：存続可能時間(TTL)値を減らすサービスポリシールールを設定します。

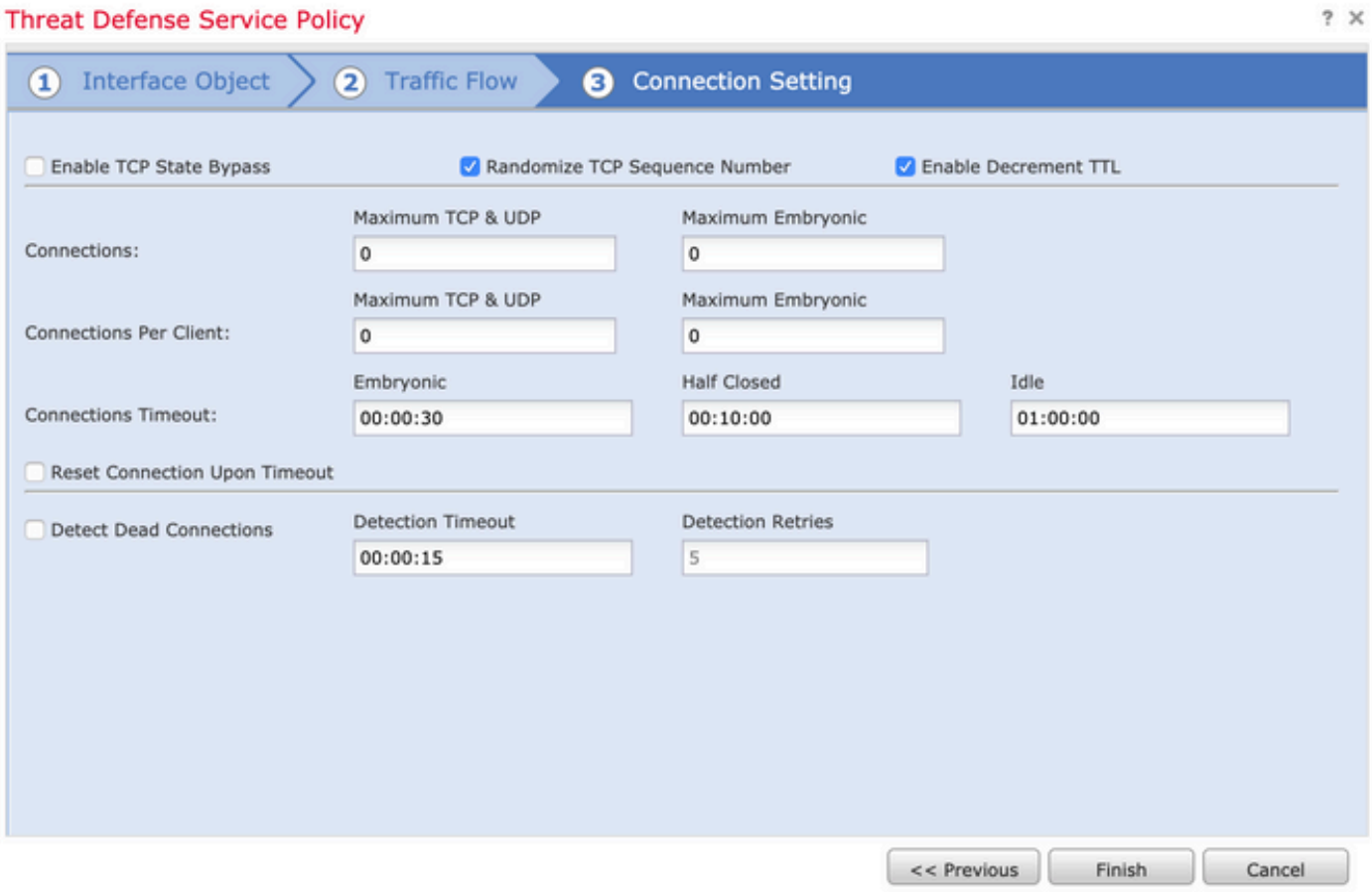
Policies > Access Controlの順に移動し、デバイスに割り当てられたポリシーをEditします。 Advancedタブで、Threat Defenseサービスポリシーを編集し、Add Ruleタブで新しいルールを追加し、Globalチェックボックスを選択してグローバルに適用し、次の図に示すようにNextをクリックします。




Traffic Flow > Extended Access Listの順に移動し、前の手順で作成したドロップダウンメニューからExtended Access List Objectを選択します。次の図に示すように、Nextをクリックします。



Enable Decrement TTLチェックボックスを選択し、他の接続オプションを変更します（オプション）。次の図に示すように、Finishをクリックしてルールを追加してから、OKをクリックし、Threat Defenseサービスポリシーへの変更をSaveします。

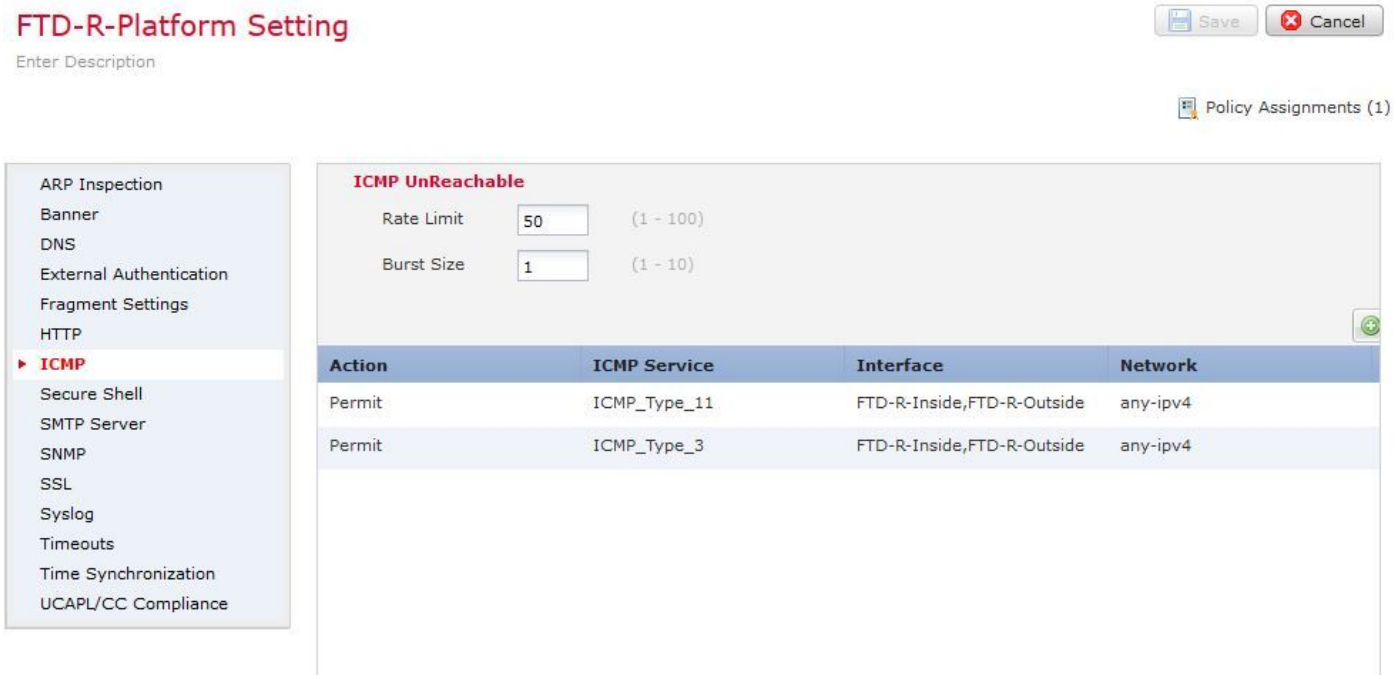



前の手順が完了したら、アクセスコントロールポリシーを保存します。

ステップ 3：InsideとOutsideでICMPを許可し、レート制限を50に設定します（オプション）。

Devices > Platform Settingsの順に移動し、EditまたはCreate a new device Threat Defense platform settings policyを選択して、Firepowerに関連付けます。目次からICMPを選択し、レート制限を大きくします。たとえば、50（バーストサイズは無視できます）に設定してからSaveをクリックし、次の図に示すようにポリシーをデバイスに展開します。

- Rate Limit:到達不能メッセージのレート制限を1秒あたり1 ~ 100メッセージの間で設定します。デフォルトは1秒あたり1メッセージです。
- バーストサイズ:バーストレートを1 ~ 10の間で設定します。現在、この値はシステムで使用されていません。




⚠ 注意:ICMP宛先到達不能（タイプ3）およびICMP時間超過（タイプ11）が、ACLポリシーのOutsideからInsideまたはプレフィルタポリシーのFastpathで許可されていることを確認してください。

## 確認

ポリシーの導入が完了したら、FTD CLIから設定を確認します。

```
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#
```

# トラブルシュート

問題をさらにトラブルシューティングするために、対象トラフィックのFTDの入力インターフェイスと出力インターフェイスでキャプチャを取得できます。

tracerouteが実行されている間のLinaのパケットキャプチャは、ターゲットIPに到達するまで、ルート上の各希望のためにこのように表示できます。

```
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
```

上記の「－I」および「－n」スイッチを使用してtracerouteを実行すると、Lina CLIでより詳細な出力を取得できます。

```
[ 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.
```

ヒント:Cisco Bug ID CSCvq79913。ICMPエラーパケットはNull pdts_infoに対してドロップされます。ICMPには必ずプレフィルタを使用してください。できればタイプ3および11リターントラフィックに使用します。

## 関連情報

テクニカル サポートとドキュメント - Cisco Systems

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。