

Allow Traceroute through Firepower Threat Defense (FTD)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Configure](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

Introduction

This document describes the configuration to allow the traceroute through Firepower Threat Defense (FTD) via Threat Service Policy.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software and hardware versions:

- This article is applicable to all Firepower platforms.
- Cisco Firepower Threat Defense which runs software version 6.4.0.
- Cisco Firepower Management Center Virtual which runs software version 6.4.0.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information


Traceroute to help you determine the route that packets take to their destination. A traceroute works by sending Unified Data Platform (UDP) packets to a destination on an invalid port. Because the port is not valid, the routers along the way to the destination respond with an Internet Control Message Protocol

(ICMP) Time Exceeded Message and report that error to the Adaptive Security Appliance (ASA).

The traceroute shows the result of each probe sent. Every line of output corresponds to a Time to Live (TTL) value in increasing order. This table explains the output symbols.

Output Symbol	Description
*	No response was received for the probe within the timeout period.
nn msec	For each node, the round-trip time (in milliseconds) for the specified number of probes.
!N	ICMP network is unreachable.
!H	ICMP host is unreachable.
!P	ICMP is unreachable.
!A	ICMP administratively prohibited.
?	Unknown ICMP error.

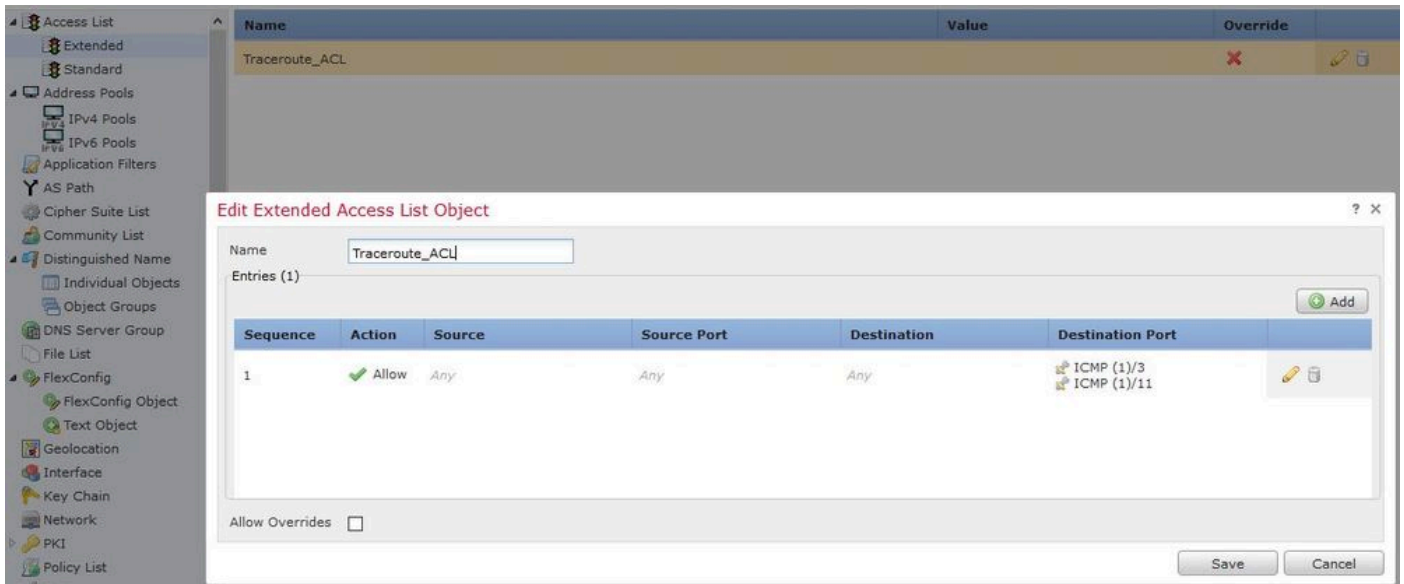
By default, the ASA does not appear on traceroutes as a hop. To make it appear, decrement the time-to-live on packets that pass through the ASA and increase the rate limit on ICMP unreachable messages.

 **Caution:** If you decrement time to live, packets with a TTL of 1 are dropped, but a connection is opened for the session on the assumption that the connection can contain packets with a greater TTL. Note that some packets, such as OSPF hello packets, are sent with TTL = 1, so decrementing time to live can have unexpected consequences. Keep these considerations in mind when you define your traffic class.

Configure

Step 1. Create the extended ACL that defines the traffic class for which traceroute reporting needs to be enabled.

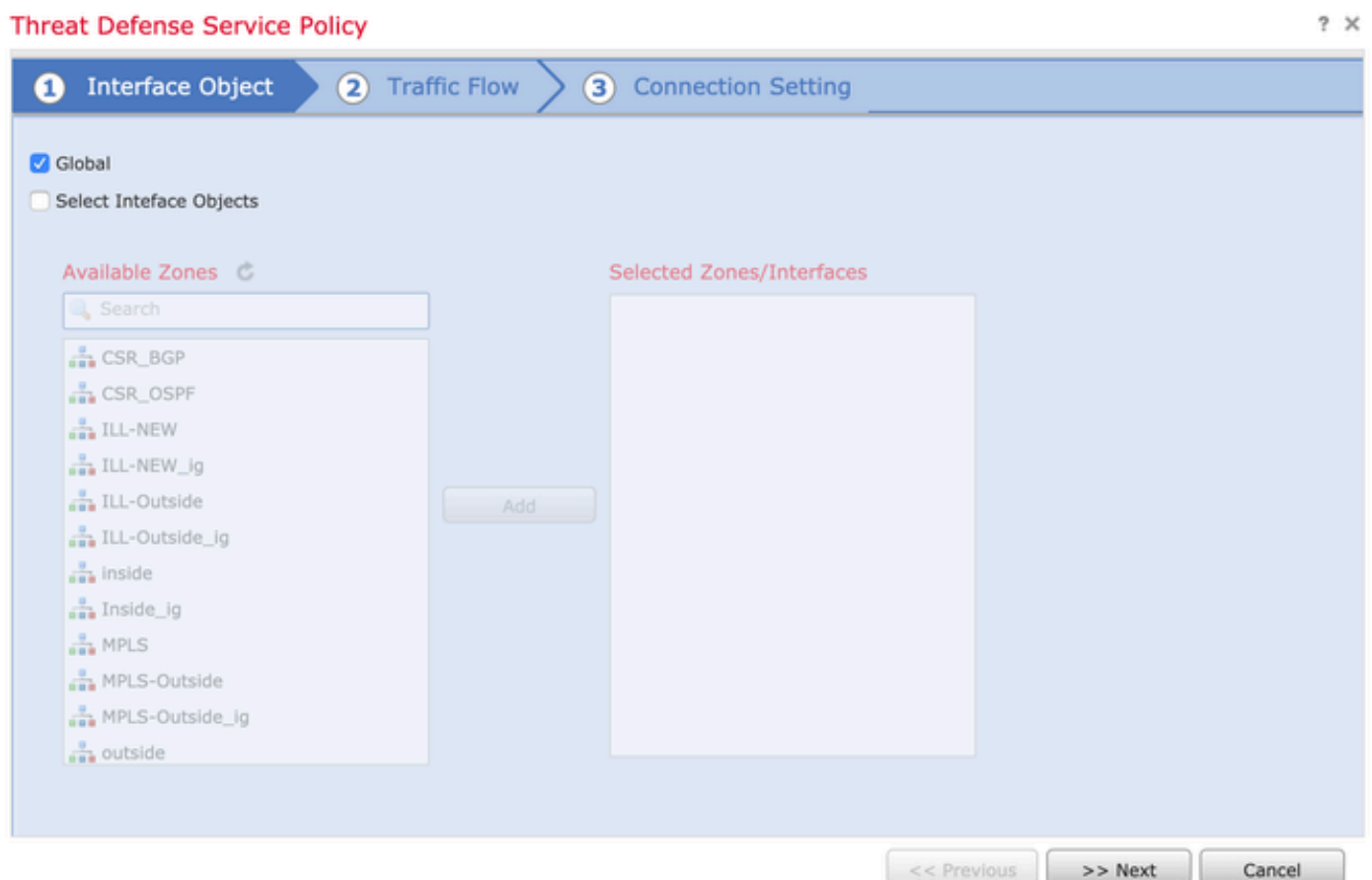
Log in to **FMC GUI** and navigate to **Objects > Object Management > Access List**. Select **Extended** from the table of contents and **Add** a new Extended Access List. Enter a Name for the object, for example, Under Traceroute_ACL, **Add** a rule to permit ICMP type 3 and 11 and **save** it, as shown in the image:



Step 2. Configure the service policy rule that decrements the time-to-live value.

Navigate to **Policies > Access Control** and then **Edit** the policy assigned to the device.

Under the Advanced tab, **Edit** the Threat Defense Service Policy, and then **Add** a new rule from **Add Rule** tab, then choose the **Global** checkbox to apply it globally, and click **Next**, as shown in the image:



Navigate to **Traffic Flow > Extended Access List** and then choose **Extended Access List Object** from the Dropdown menu which was created in previous steps. Now click **Next**, as shown in the image:

The screenshot shows a configuration window titled "Threat Defense Service Policy" with three tabs: "1 Interface Object", "2 Traffic Flow", and "3 Connection Setting". The "3 Connection Setting" tab is active. Below the tabs, there is a label "Extended Access List:" followed by a dropdown menu containing the text "Traceroute_ACL". At the bottom right of the window, there are three buttons: "<< Previous", ">> Next", and "Cancel".

Choose the **Enable Decrement TTL** checkbox and modify the other connection options (Optional). Now, click **Finish** to add the rule, then click **OK**, and **Save** the changes to the Threat defence service policy, as shown in the image:

The screenshot shows the 'Connection Setting' tab of the Threat Defense Service Policy configuration. The interface includes a breadcrumb trail with three steps: 1. Interface Object, 2. Traffic Flow, and 3. Connection Setting. The configuration area contains several sections:

- Global Settings:**
 - Enable TCP State Bypass
 - Randomize TCP Sequence Number
 - Enable Decrement TTL
- Connections:**
 - Maximum TCP & UDP:
 - Maximum Embryonic:
- Connections Per Client:**
 - Maximum TCP & UDP:
 - Maximum Embryonic:
- Connections Timeout:**
 - Embryonic:
 - Half Closed:
 - Idle:
- Reset Connection Upon Timeout
- Detect Dead Connections
 - Detection Timeout:
 - Detection Retries:

At the bottom right, there are three buttons: '<< Previous', 'Finish', and 'Cancel'.

Once the previous steps are completed, **save** the Access Control Policy.

Step 3. Permit ICMP on Inside and Outside, and Increase the Rate Limit to 50 (optional).

Navigate to **Devices > Platform Settings** and then **Edit** or **Create** a new Firepower Threat Defense platform settings policy and associate it to the device. Choose **ICMP** from the table of content and Increase the Rate Limit. For example, to 50 (You can ignore the Burst Size) and then click **Save**, and proceed to **Deploy** the Policy to the device, as shown in the image:

- **Rate Limit**—Sets the rate limit of unreachable messages, between 1 and 100 messages per second. The default is 1 message per second.
- **Burst Size**—Sets the burst rate, between 1 and 10. This value is not currently used by the system.

FTD-R-Platform Setting

Enter Description

Save Cancel

Policy Assignments (1)

- ARP Inspection
- Banner
- DNS
- External Authentication
- Fragment Settings
- HTTP
- ICMP**
- Secure Shell
- SMTP Server
- SNMP
- SSL
- Syslog
- Timeouts
- Time Synchronization
- UCAPL/CC Compliance

ICMP UnReachable

Rate Limit (1 - 100)

Burst Size (1 - 10)

Action	ICMP Service	Interface	Network
Permit	ICMP_Type_11	FTD-R-Inside,FTD-R-Outside	any-ipv4
Permit	ICMP_Type_3	FTD-R-Inside,FTD-R-Outside	any-ipv4

⚠ Caution: Ensure **ICMP Destination Unreachable (Type 3)** and **ICMP Time Exceeded (Type 11)** are allowed from Outside to Inside in the ACL policy or via Fastpath in Pre-filter policy.

Verify

Check the configuration from FTD CLI once policy deployment is complete:

```
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#
```

Troubleshoot

You can take captures on FTD Ingress and Egress interfaces for the interesting traffic to further troubleshoot the issue.

Packet capture on Lina, while traceroute is performed, can show as this for each hop on the route until it reaches the target 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 unreachable
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
```

A more detailed output can be obtained on Lina CLI if you perform traceroute with "-I" and "-n" switches as listed.

```
[ 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 is

```
[ 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.

 **Tip:** Cisco bug ID [CSCvq79913](#). ICMP error packets are dropped for Null pdts_info. Make sure to use the prefilter for ICMP, preferably for the type 3 and 11 return traffic.

Related Information

[Technical Support & Documentation - Cisco Systems](#)