

Replay a Packet Using Packet Tracer Tool in FMC

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Replay the packet using packet tracer tool available on FMC](#)

[Replay the packets using PCAP file](#)

[Limitations of using this option](#)

[Related Documents](#)

Introduction

This document describes how you can replay a packet in your FTD device using FMC GUI Packet Tracer tool.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of Firepower technology
- Knowledge of Packet flow through the Firewall

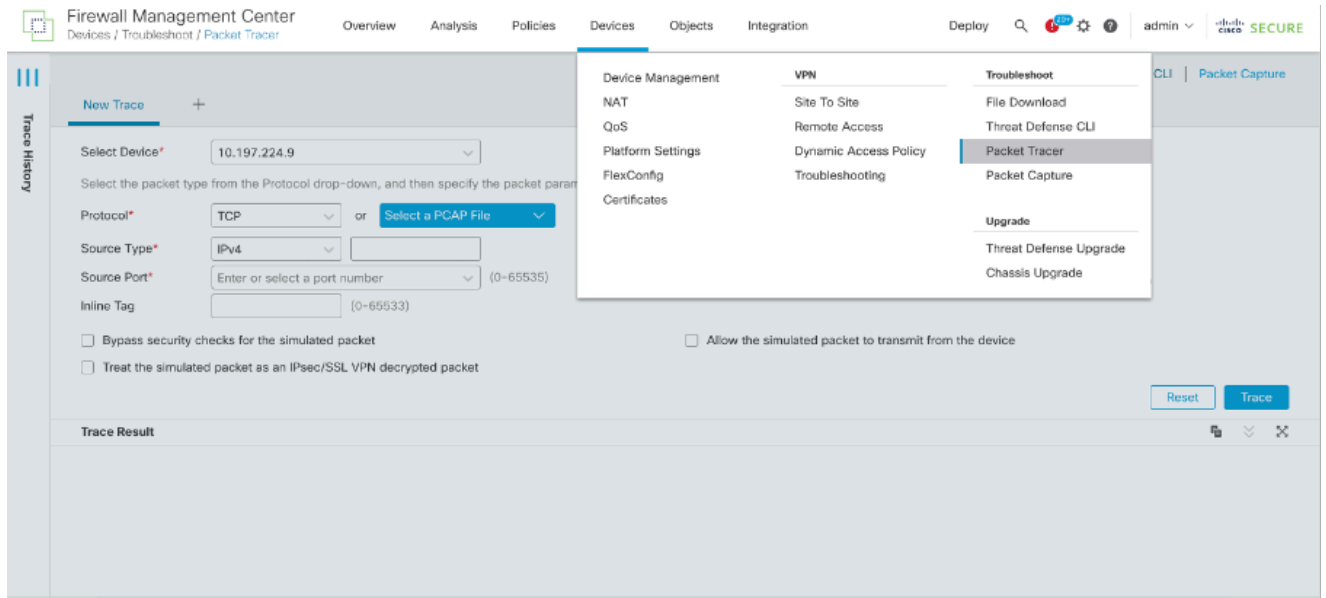
Components Used

- Cisco Secure Firewall Management Center (FMC) and Cisco Firewall Threat Defense (FTD) version 7.1 or later.
- Packet capture files in pcap format

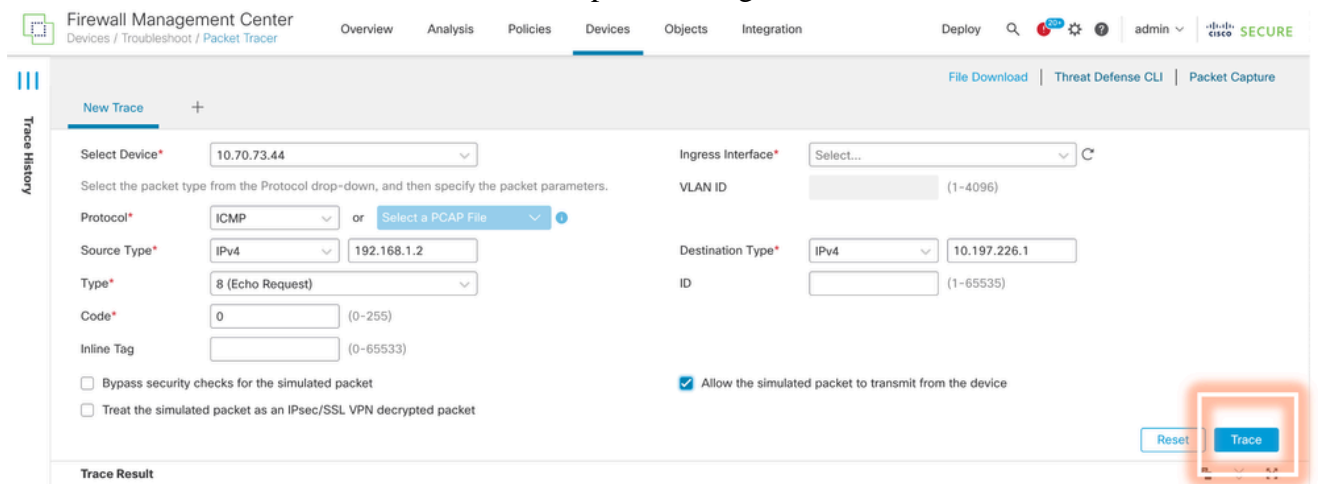
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Replay the packet using packet tracer tool available on FMC

1. Login to FMC GUI. Go to Devices > Troubleshoot > Packet Tracer.

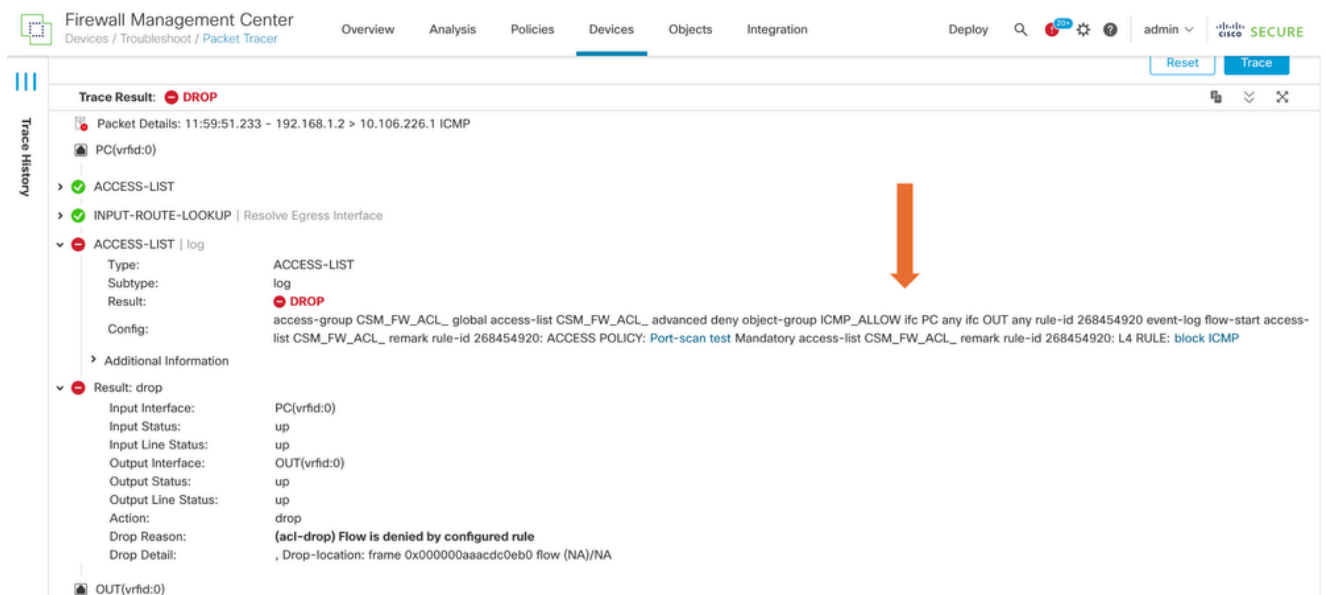


2. Provide the details of the source, destination, protocol, ingress interface. Click Trace.



3. Use the option of Allow the simulated packet to transmit from the device to replay this packet from the device.

4. Observe that the packet was dropped because there is a configured rule in Access control policy to drop ICMP packets.



5. This packet tracer with TCP packets the final result of the trace (as shown).

The screenshot shows the Firewall Management Center Packet Tracer interface. The 'New Trace' form is filled with the following details: Select Device: 10.70.73.44; Protocol: TCP; Source Type: IPv4; Source Port: 1234; Ingress Interface: PC - Ethernet1/1; Destination Type: IPv4; Destination Port: 443. The 'Trace Result' section shows a green checkmark and the word 'ALLOW' in green, with an orange arrow pointing to it. Below the result, the packet details are listed: 12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP. The trace steps are: INPUT-ROUTE-LOOKUP | Resolve Egress Interface, ACCESS-LIST | log, and CONN-SETTINGS.

Replay the packets using PCAP file

You can upload the pcap file using the Select a PCAP File button. Then select the Ingress interface and click on Trace.

The screenshot shows the Firewall Management Center Packet Tracer interface. The 'New Trace 3' form is filled with the following details: Select Device: 10.197.224.9; Protocol: TCP; Source Type: IPv4; Source Port: Enter or select a port number; Ingress Interface: outside - GigabitEthernet0/1; Destination Type: IPv4; Destination Port: Enter or select a port number. The 'Select a PCAP File' button is highlighted with a red box. The 'Trace Result' section is empty.

Limitations of using this option

1. We can only simulate TCP/UDP packets.
2. The maximum number of packets supported in a PCAP file is 100.
3. Pcap file size must be less than 1 MB.

4. The PCAP file name must not exceed 64 characters (extension included) and must only contain alphanumeric, special characters (“.”, “-“, “_”), or both.
5. Only a single flow packets are supported currently.

The Trace 3 is showing drop reason as invalid ip header

The screenshot shows the Cisco Firewall Management Center (FMC) Packet Tracer interface. The configuration for the packet capture is as follows:

- Protocol: UDP or single2.pcap
- Source Type: IPv4, 192.168.29.58
- Source Port: 60376 (0-65535)
- Destination Type: IPv4, 192.168.29.160
- Destination Port: 161 (0-65535)
- Inline Tag: (0-65533)

Options for the simulated packet:

- Bypass security checks for the simulated packet
- Allow the simulated packet to transmit from the device
- Treat the simulated packet as an IPsec/SSL VPN decrypted packet

Trace Result: **Error: Some packets from the PCAP file were not replayed.**

Packet 1: 11:58:21.875534

Packet Details: 11:58:21.875534 192.168.29.58:60376 > 192.168.29.160:161 udp 80

inside(vrfid:0)

Result: drop

Input Interface:	inside(vrfid:0)
Input Status:	up
Input Line Status:	up
Output Interface:	NP Identity Ifc
Action:	drop
Time Taken:	0 ns
Drop Reason:	(invalid-ip-header) Invalid IP header
Drop Detail:	Drop-location: frame 0x000055f7cfb1b71b flow (NA)/NA

NP Identity Ifc

Related Documents

For more information on Packet captures and tracers, please refer [Cisco Live Document](#).