Replay a Packet Using Packet Tracer Tool in FMC

Contents

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

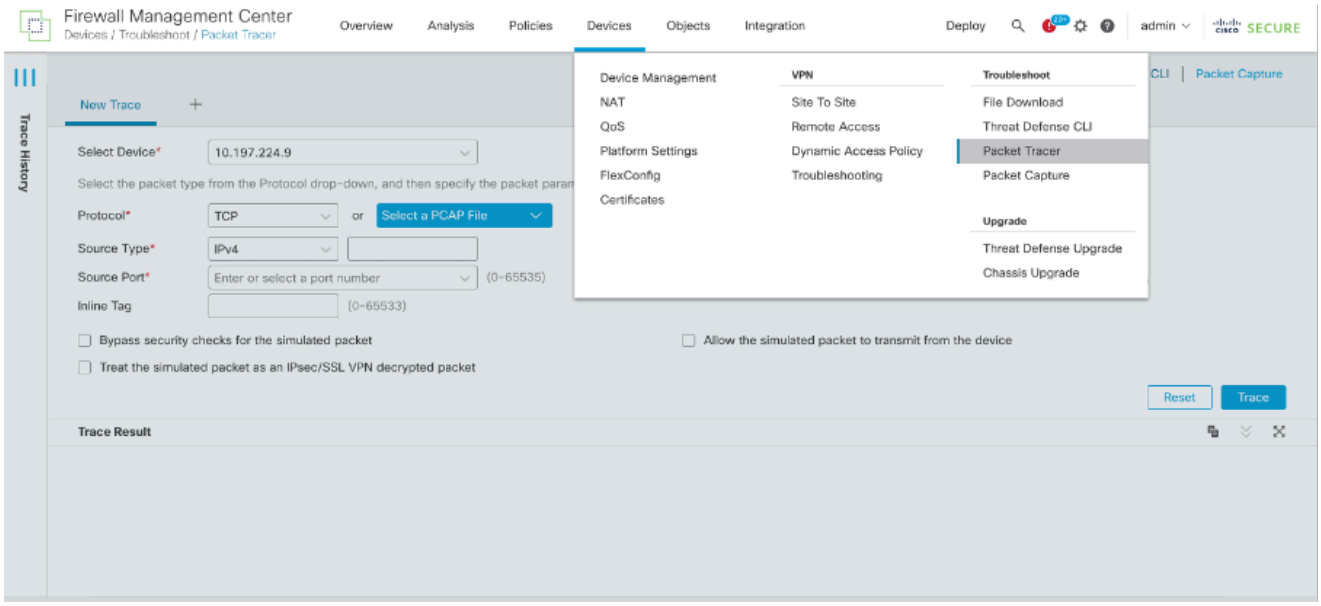
Components Used

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

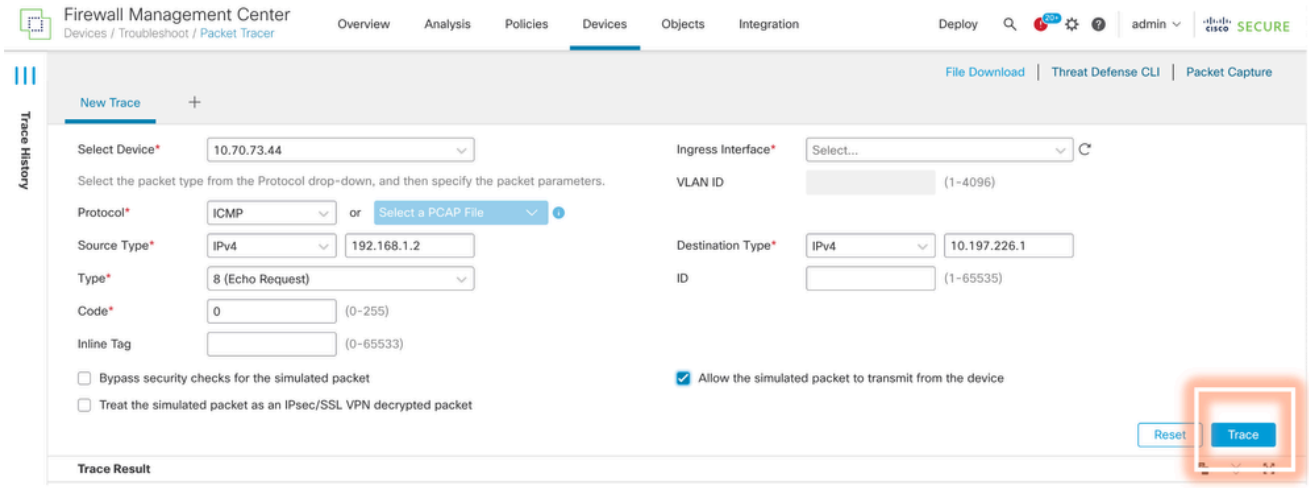
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Replay the packet using packet tracer tool available on FMC

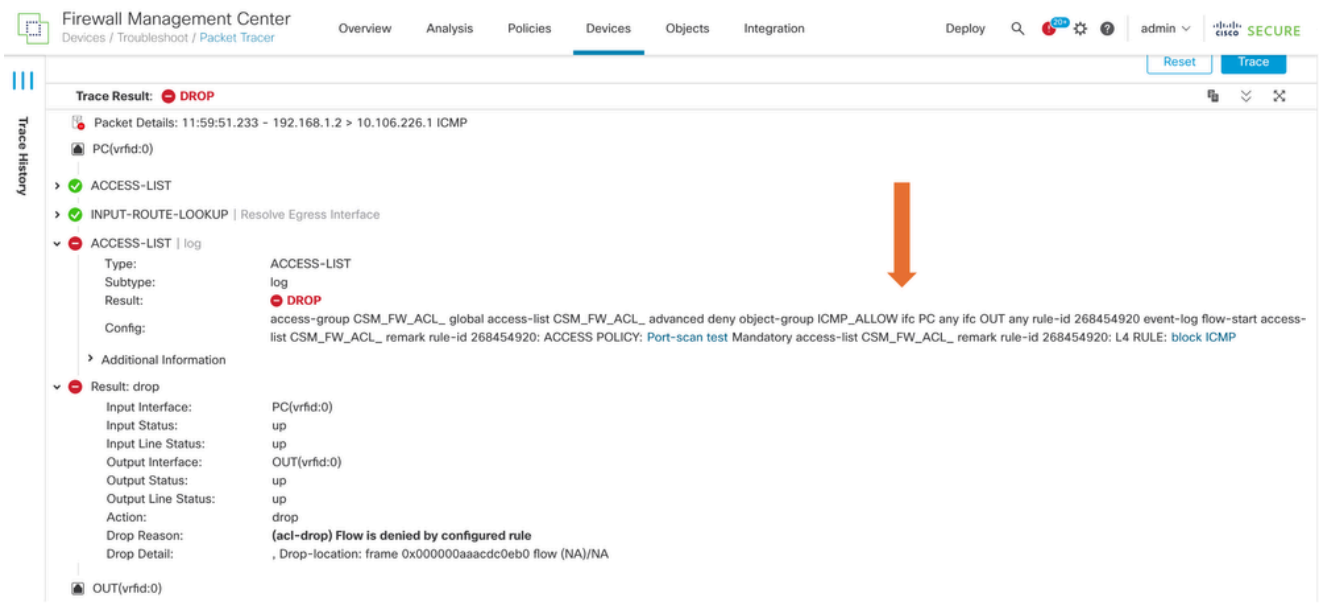
1. Login to FMC GUI. Go to Devices > Troubleshoot > Packet Tracer.



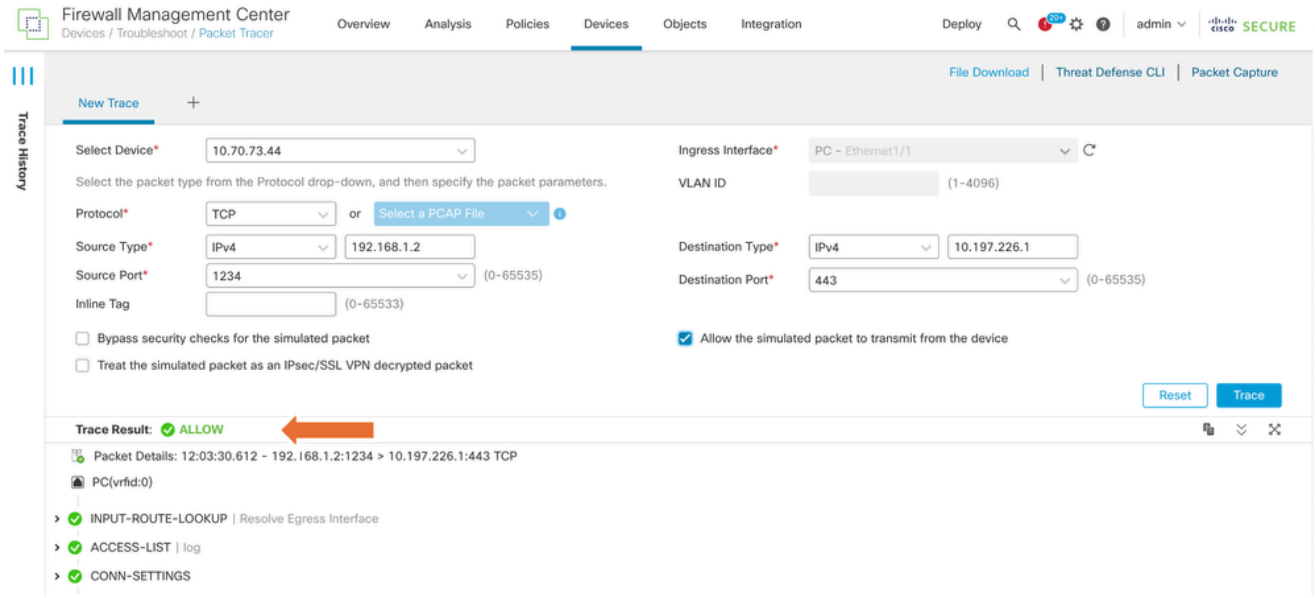
2. Provide the details of the source, destination, protocol, ingress interface. Click Trace.



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.

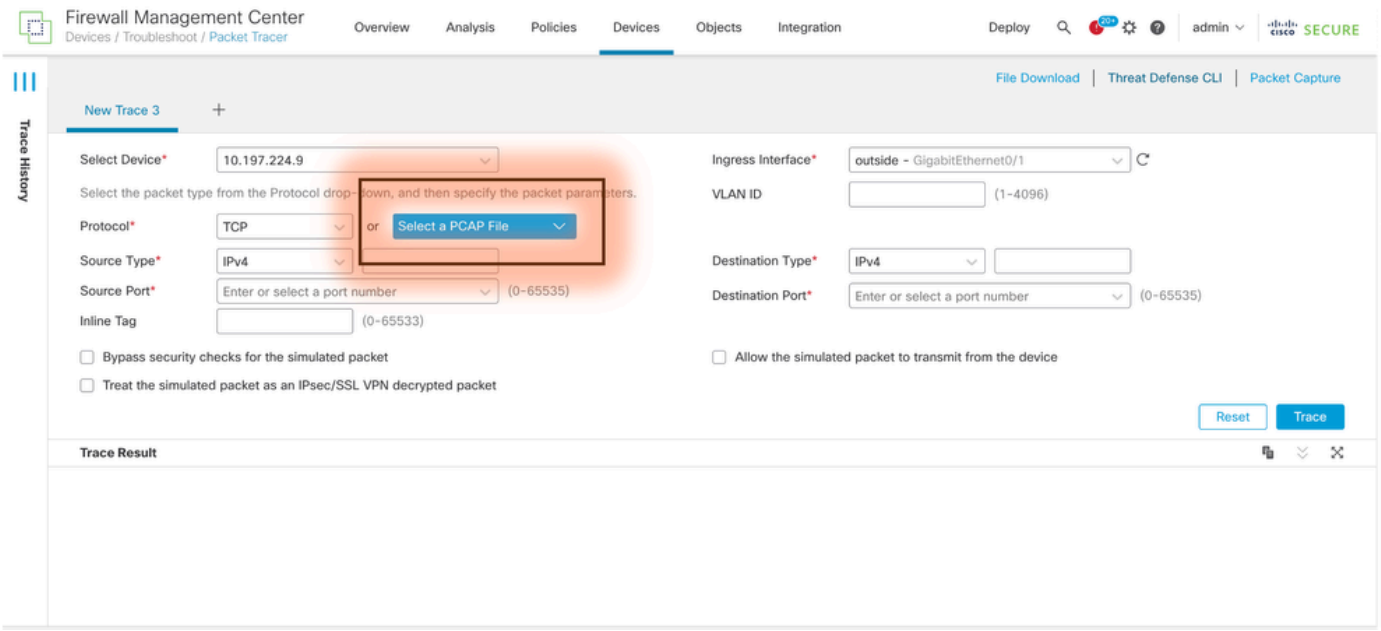


5. This packet tracer with TCP packets the final result of the trace (as shown).



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.

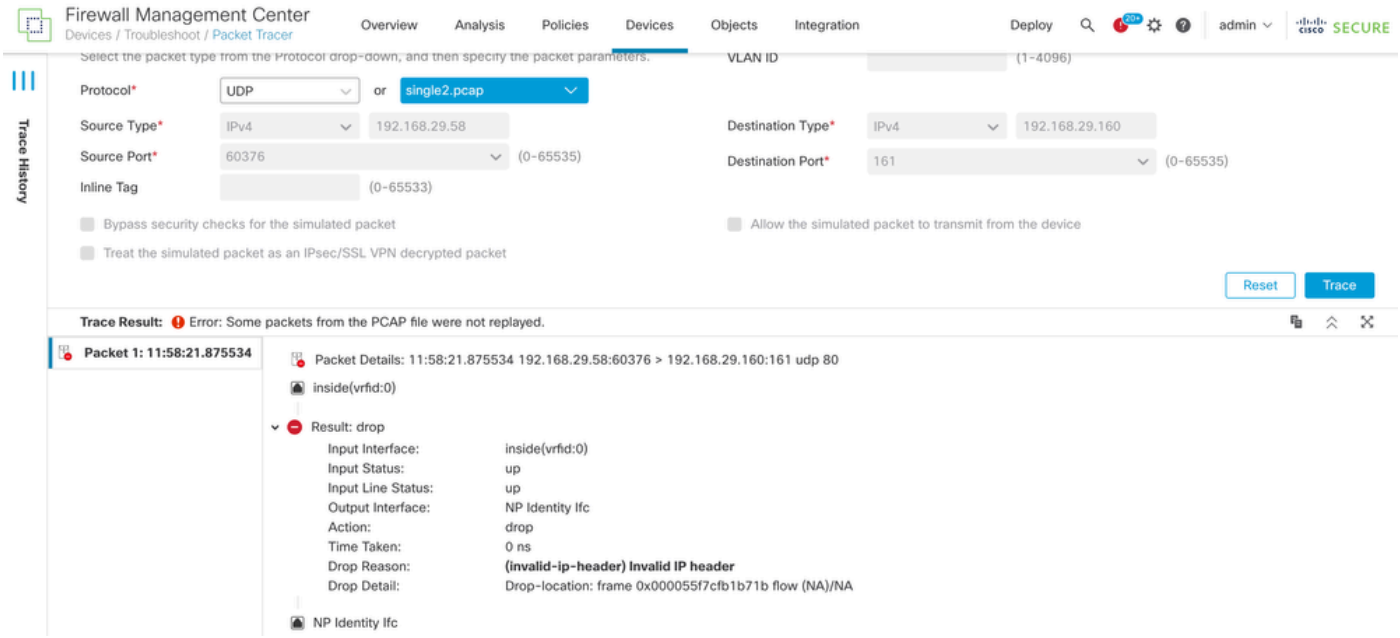


Limitations of using this option

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



Related Documents

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