

Reproducción de un paquete mediante la herramienta Packet Tracer en FMC

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Reproducción del paquete mediante la herramienta de seguimiento de paquetes disponible en FMC](#)

[Reproduzca los paquetes mediante el archivo PCAP](#)

[Limitaciones del uso de esta opción](#)

[Documentos Relacionados](#)

Introducción

Este documento describe cómo puede reproducir un paquete en su dispositivo FTD utilizando la herramienta FMC GUI Packet Tracer.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de la tecnología Firepower
- Conocimiento del flujo de paquetes a través del firewall

Componentes Utilizados

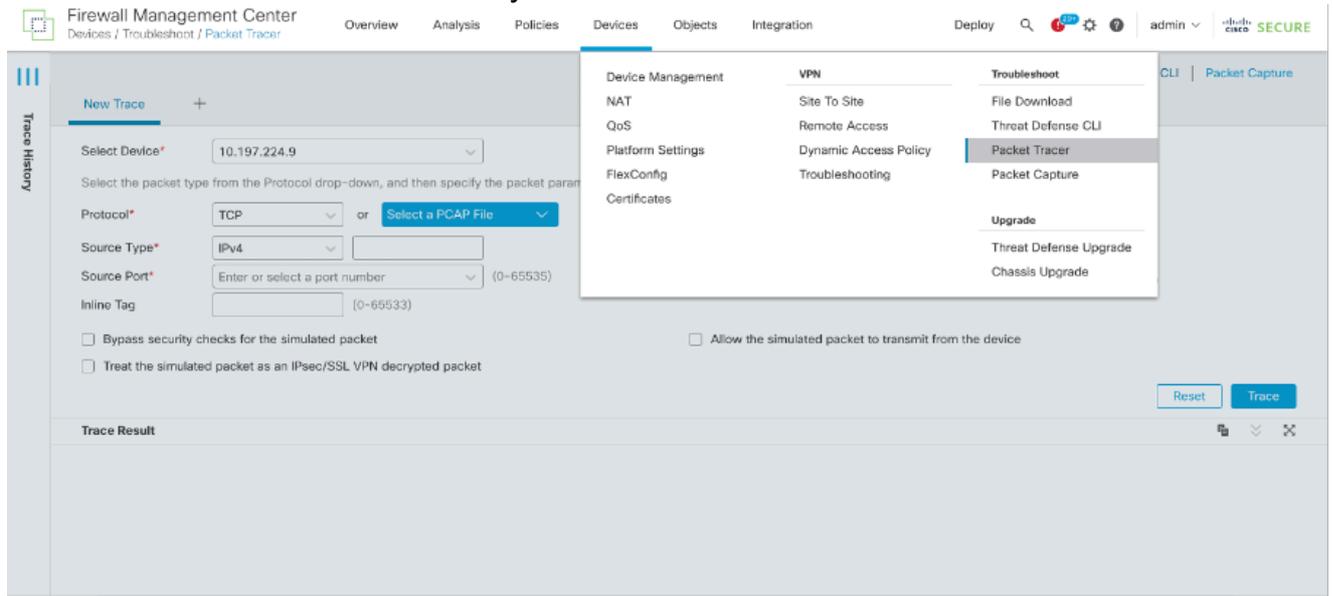
- Cisco Secure Firewall Management Center (FMC) y Cisco Firewall Threat Defence (FTD) versión 7.1 o posterior.
- Archivos de captura de paquetes en formato pcap

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

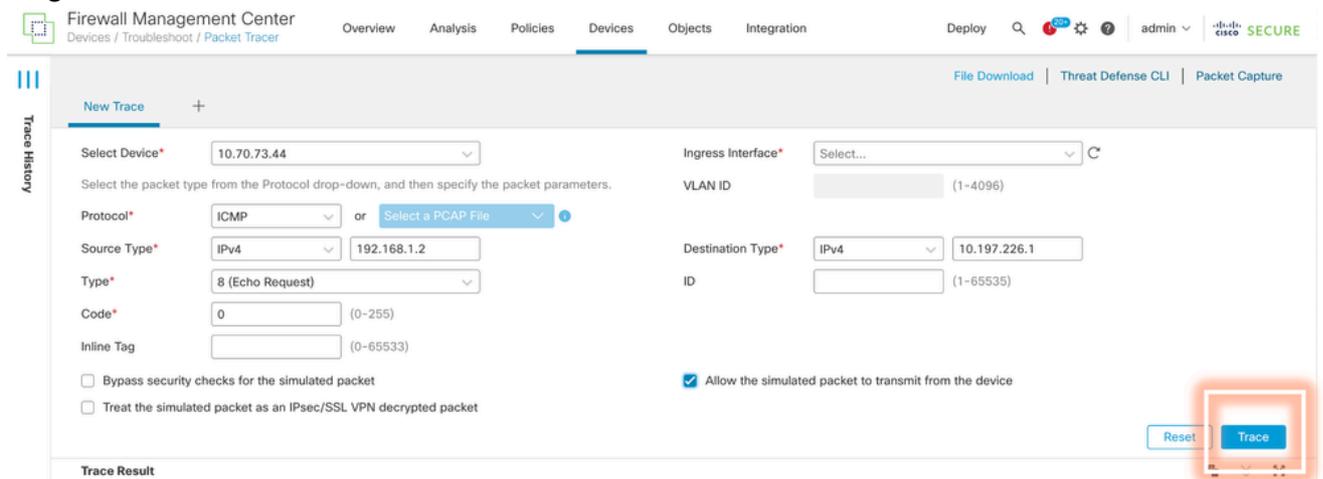
Reproducción del paquete mediante la herramienta de

seguimiento de paquetes disponible en FMC

1. Inicie sesión en la GUI de FMC. Vaya a Devices > Troubleshoot > Packet Tracer.



2. Proporcione los detalles de la interfaz de origen, destino, protocolo e ingreso. Haga clic en Seguimiento.



3. Utilice la opción Permitir que el paquete simulado transmita desde el dispositivo para reproducir este paquete desde el dispositivo.

4. Observe que se descartó el paquete porque hay una regla configurada en la política de control de acceso para descartar paquetes ICMP.

The screenshot shows the Firewall Management Center interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Devices' tab is active. The main content area displays a 'Trace Result: DROP' for a packet from 11:59:51.233 - 192.168.1.2 to 10.106.226.1 using ICMP. The trace path includes:

- PC(vrfd:0)
- ACCESS-LIST
- INPUT-ROUTE-LOOKUP | Resolve Egress Interface
- ACCESS-LIST | log
 - Type: ACCESS-LIST
 - Subtype: log
 - Result: DROP
 - Config: access-group CSM_FW_ACL_global access-list CSM_FW_ACL_advanced deny object-group ICMP_ALLOW ifc PC any ifc OUT any rule-id 268454920 event-log flow-start access-list CSM_FW_ACL_remark rule-id 268454920: ACCESS POLICY; Port-scan test Mandatory access-list CSM_FW_ACL_remark rule-id 268454920: L4 RULE: block ICMP
- Result: drop
 - Input Interface: PC(vrfd:0)
 - Input Status: up
 - Input Line Status: up
 - Output Interface: OUT(vrfd:0)
 - Output Status: up
 - Output Line Status: up
 - Action: drop
 - Drop Reason: (acl-drop) Flow is denied by configured rule
 - Drop Detail: , Drop-location: frame 0x000000aaacdc0eb0 flow (NA)/NA
- OUT(vrfd:0)

 An orange arrow points to the 'DROP' result in the 'ACCESS-LIST | log' section.

5. Este rastreador de paquetes con paquetes TCP es el resultado final del seguimiento (como se muestra).

The screenshot shows the Firewall Management Center interface for configuring a new trace. The 'New Trace' section includes:

- Select Device: 10.70.73.44
- Ingress Interface: PC - Ethernet1/1
- VLAN ID: (1-4096)
- Protocol: TCP (with a 'Select a PCAP File' button)
- Source Type: IPv4, Source: 192.168.1.2
- Source Port: 1234 (0-65535)
- Destination Type: IPv4, Destination: 10.197.226.1
- Destination Port: 443 (0-65535)
- Options: 'Allow the simulated packet to transmit from the device' is checked.

 The 'Trace Result' section shows 'Trace Result: ALLOW' with an orange arrow pointing to it. The packet details are: 12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP. The trace path includes:

- PC(vrfd:0)
- INPUT-ROUTE-LOOKUP | Resolve Egress Interface
- ACCESS-LIST | log
- CONN-SETTINGS

Reproduzca los paquetes mediante el archivo PCAP

Puede cargar el archivo PCAP mediante el botón Select a PCAP File (Seleccionar un archivo PCAP). A continuación, seleccione la interfaz de entrada y haga clic en Trace (Seguimiento).

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 2024 ⚙️ ? admin | cisco SECURE

File Download Threat Defense CLI Packet Capture

New Trace 3 +

Select Device* 10.197.224.9

Select the packet type from the Protocol drop-down, and then specify the packet parameters.

Protocol* TCP or **Select a PCAP File**

Source Type* IPv4

Source Port* Enter or select a port number (0-65535)

Inline Tag (0-65533)

Ingress Interface* outside - GigabitEthernet0/1

VLAN ID (1-4096)

Destination Type* IPv4

Destination Port* Enter or select a port number (0-65535)

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

Reset Trace

Trace Result

Limitaciones del uso de esta opción

1. Solo podemos simular paquetes TCP/UDP.
2. El número máximo de paquetes admitidos en un archivo PCAP es 100.
3. El tamaño del archivo Pcap debe ser inferior a 1 MB.
4. El nombre del archivo PCAP no debe superar los 64 caracteres (extensión incluida) y sólo debe contener caracteres alfanuméricos, caracteres especiales (".", "-", "_") o ambos.
5. Actualmente sólo se admite un paquete de flujo único.

El Trace 3 muestra la razón de descarte como encabezado IP no válido

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 2024 ⚙️ ? admin | cisco SECURE

Select the packet type from the Protocol drop-down, and then specify the packet parameters.

Protocol* UDP or single2.pcap

Source Type* IPv4 192.168.29.58

Source Port* 60376 (0-65535)

Inline Tag (0-65533)

VLAN ID (1-4096)

Destination Type* IPv4 192.168.29.160

Destination Port* 161 (0-65535)

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

Reset Trace

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

Documentos Relacionados

Para obtener más información sobre capturas y trazadores de paquetes, consulte [Cisco Live Document](#).

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).