

Reproduza um pacote usando a ferramenta Packet Tracer no FMC

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Reproduzir o pacote usando a ferramenta packet tracer disponível no FMC](#)

[Repetir os pacotes usando o arquivo PCAP](#)

[Limitações de usar esta opção](#)

[Documentos relacionados](#)

Introdução

Este documento descreve como você pode reproduzir um pacote em seu dispositivo FTD usando a ferramenta Packet Tracer da GUI do FMC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento da tecnologia Firepower
- Conhecimento do fluxo de pacotes através do firewall

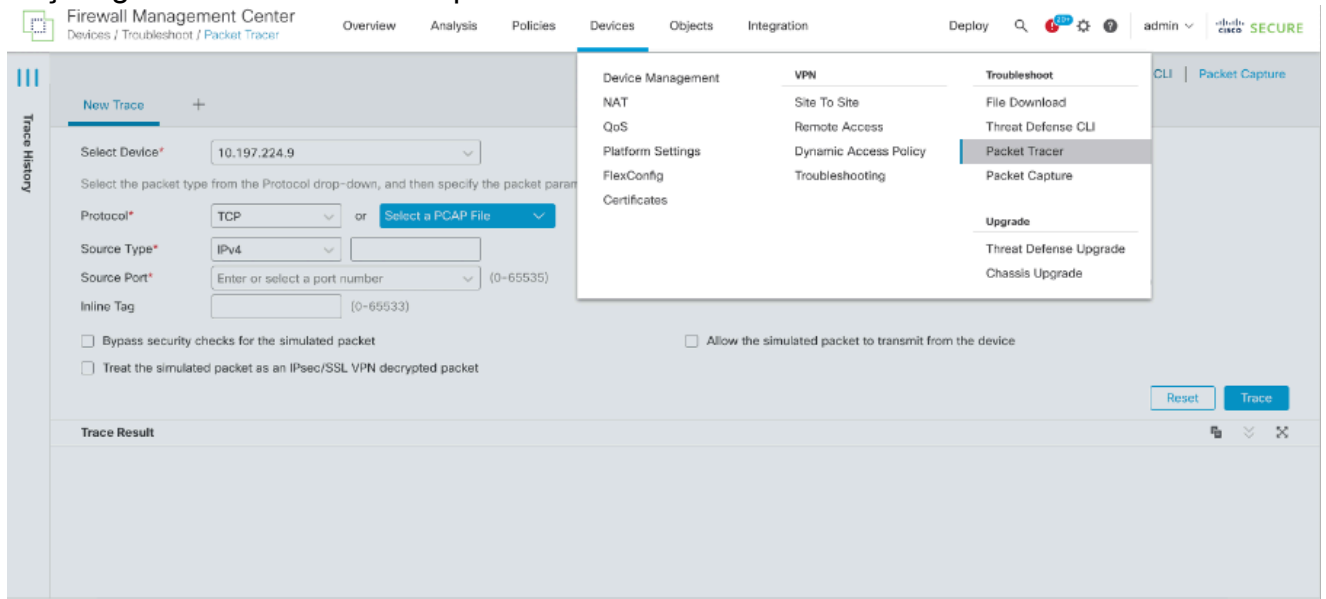
Componentes Utilizados

- Cisco Secure Firewall Management Center (FMC) e Cisco Firewall Threat Defense (FTD) versão 7.1 ou posterior.
- Arquivos de captura de pacote no formato pcap

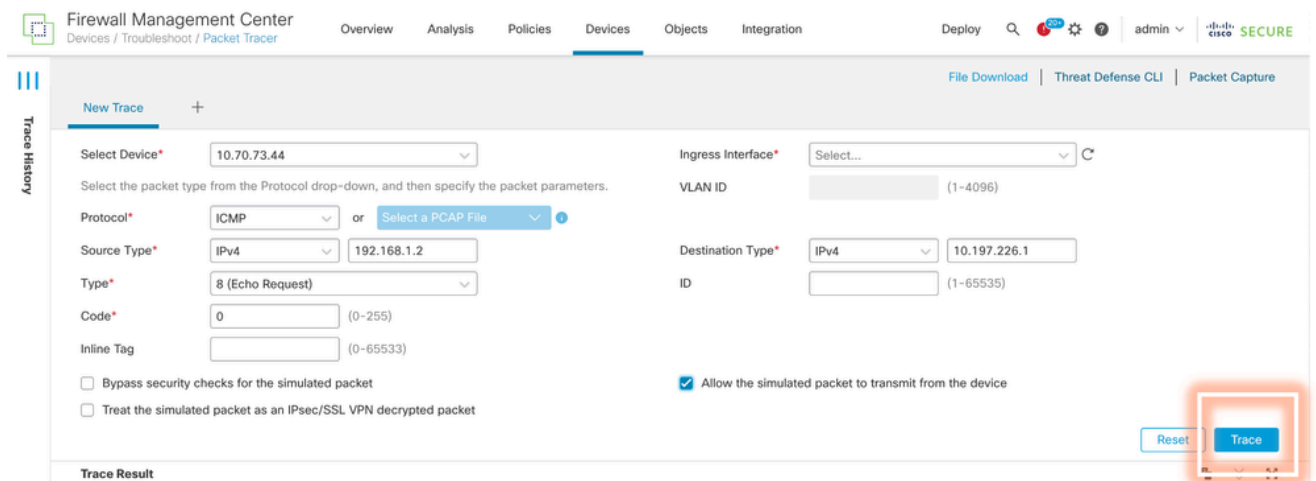
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Reproduzir o pacote usando a ferramenta packet tracer disponível no FMC

1. Faça login na GUI do FMC. Vá para Devices > Troubleshoot > Packet Tracer.



2. Forneça os detalhes da origem, do destino, do protocolo e da interface de entrada. Clique em Rastrear.



3. Use a opção Allow the simulated packet to transmit from the device (Permitir que o pacote simulado transmita do dispositivo) para reproduzir esse pacote a partir do dispositivo.
4. Observe que o pacote foi descartado porque há uma regra configurada na política de controle de acesso para descartar pacotes ICMP.

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 50% ⚙️ ? admin | cisco **SECURE**

Trace Result: **DROP**

Packet Details: 11:59:51.233 - 192.168.1.2 > 10.106.226.1 ICMP

PC(vrfid: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
- Additional Information
- Result: drop
 - Input Interface: PC(vrfid:0)
 - Input Status: up
 - Input Line Status: up
 - Output Interface: OUT(vrfid: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 0x00000aaacd0eb0 flow (NA)/NA

OUT(vrfid:0)

5. Esse packet tracer com pacotes TCP mostra o resultado final do rastreamento (como mostrado).

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 50% ⚙️ ? admin | cisco **SECURE**

File Download | Threat Defense CLI | Packet Capture

New Trace +

Select Device* 10.70.73.44

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 192.168.1.2

Source Port* 1234 (0-65535)

Inline Tag (0-65533)

Bypass security checks for the simulated packet

Treat the simulated packet as an IPsec/SSL VPN decrypted packet

Allow the simulated packet to transmit from the device

Reset Trace

Trace Result: **ALLOW**

Packet Details: 12:03:30.612 - 192.168.1.2:1234 > 10.197.226.1:443 TCP

PC(vrfid:0)

- INPUT-ROUTE-LOOKUP | Resolve Egress Interface
- ACCESS-LIST | log
- CONN-SETTINGS

Repetir os pacotes usando o arquivo PCAP

Você pode carregar o arquivo pcap usando o botão Selecionar um arquivo PCAP. Em seguida, selecione a interface Ingress e clique em Trace.

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin | **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)

Bypass security checks for the simulated packet

Treat the simulated packet as an IPsec/SSL VPN decrypted packet

Ingress Interface* outside - GigabitEthernet0/1

VLAN ID (1-4096)

Destination Type* IPv4

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

Allow the simulated packet to transmit from the device

Reset Trace

Trace Result

Limitações de usar esta opção

1. Só podemos simular pacotes TCP/UDP.
2. O número máximo de pacotes suportado em um arquivo PCAP é 100.
3. O tamanho do arquivo Pcap deve ser menor que 1 MB.
4. O nome do arquivo PCAP não deve exceder 64 caracteres (extensão incluída) e deve conter apenas caracteres alfanuméricos, caracteres especiais (".", "-", "_") ou ambos.
5. No momento, há suporte apenas para um único pacote de fluxo.

O Rastreamento 3 está mostrando o motivo da queda como cabeçalho IP inválido

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 ⚙️ ? admin | **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)

Bypass security checks for the simulated packet

Treat the simulated packet as an IPsec/SSL VPN decrypted packet

VLAN ID (1-4096)

Destination Type* IPv4 192.168.29.160

Destination Port* 161 (0-65535)

Allow the simulated packet to transmit from the device

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 0x000055f7c1b1b71b flow (NA)/NA

NP Identity Ifc

Documentos relacionados

Para obter mais informações sobre capturas de pacotes e rastreadores, consulte o [Cisco Live Document](#).

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.