Reproduza um pacote usando a ferramenta Packet Tracer no FMC

Contents

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

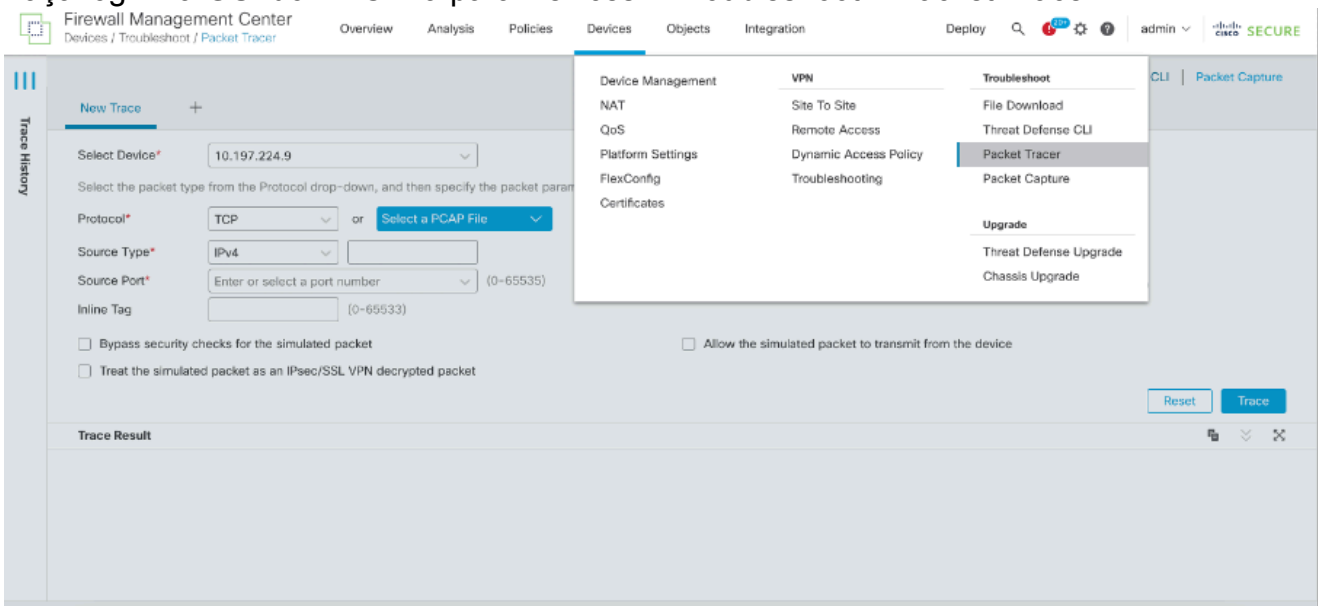
Componentes Utilizados

- 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

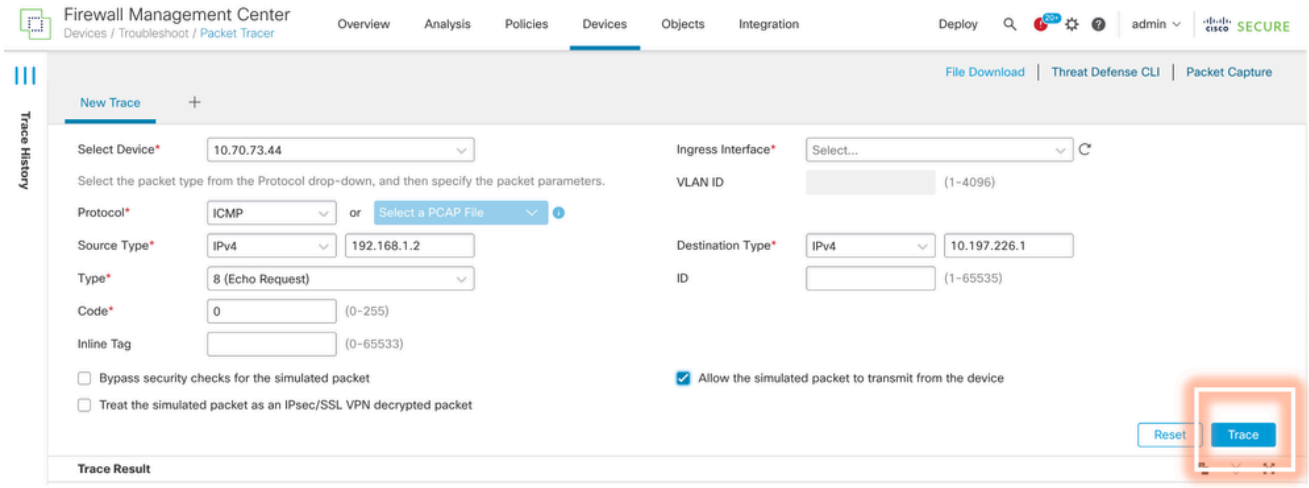
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer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

Reproduzir o pacote usando a ferramenta packet tracer disponível no FMC

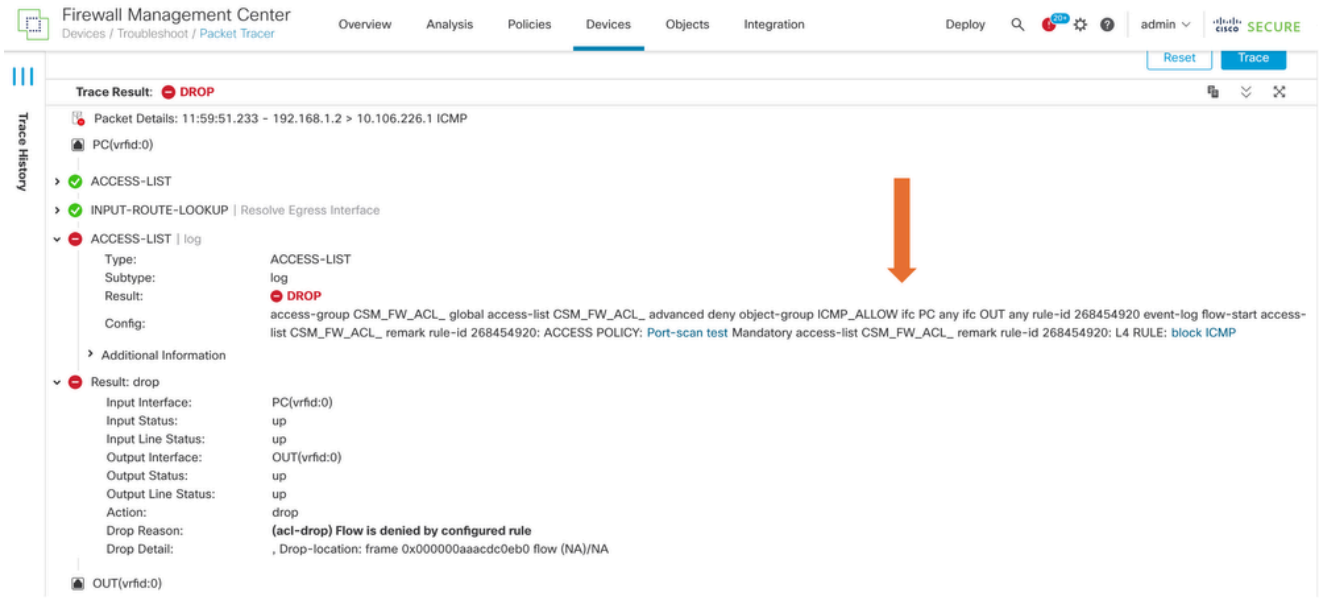
1. Faça login na GUI do FMC. Vá para Devices > Troubleshoot > Packet Tracer.



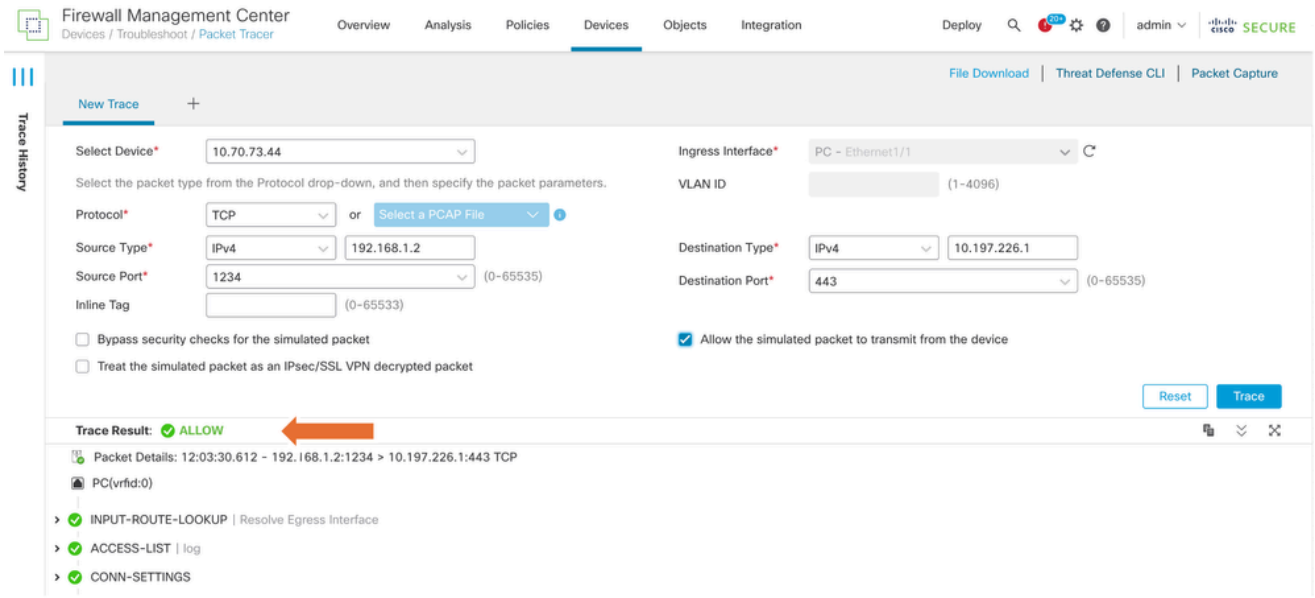
2. Forneça os detalhes da origem, do destino, do protocolo e da interface de entrada. Clique em Rastrear.



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.

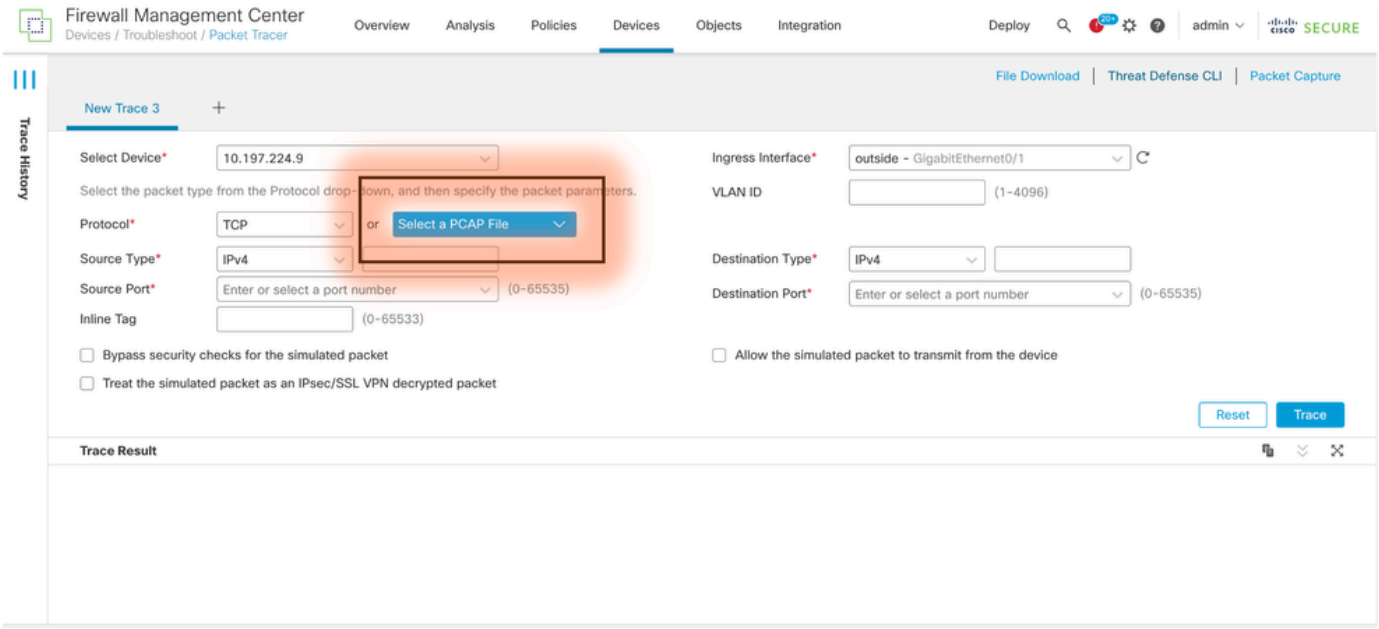


5. Esse packet tracer com pacotes TCP mostra o resultado final do rastreamento (como mostrado).



Repetir os pacotes usando o arquivo PCAP

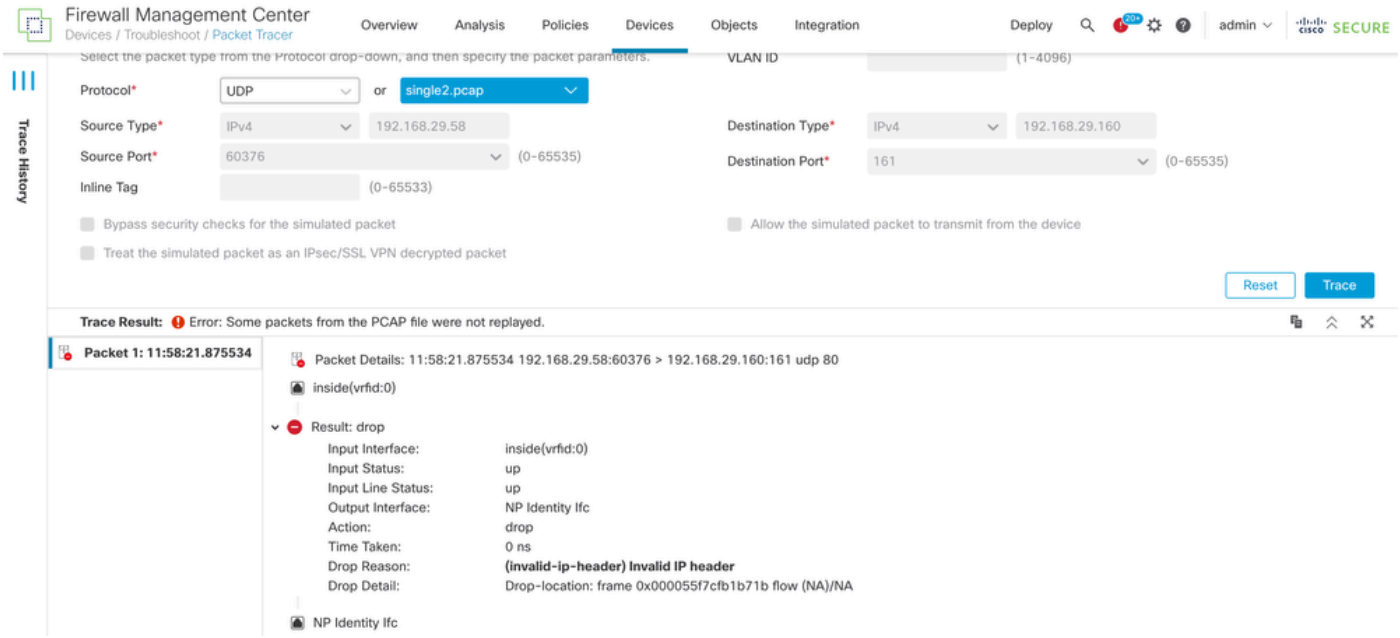
Você pode carregar o arquivo pcap usando o botão Selecionar um arquivo PCAP. Em seguida, selecione a interface Ingress e clique em Trace.



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



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.