Relire un paquet à l’aide de l’outil Packet Tracer dans FMC

Table des matières

Introduction

Ce document décrit comment vous pouvez relire un paquet dans votre périphérique FTD à l'aide de l'outil Packet Tracer de l'interface graphique FMC.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de la technologie Firepower
- Connaissance du flux de paquets dans le pare-feu

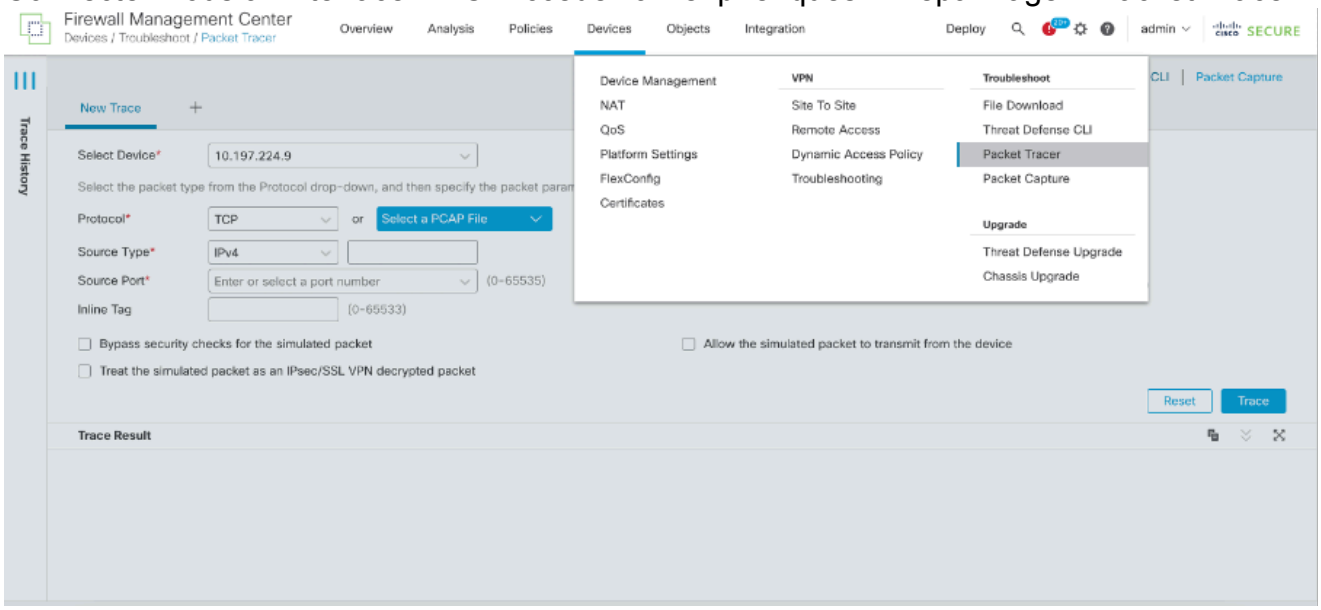
Composants utilisés

- Cisco Secure Firewall Management Center (FMC) et Cisco Firewall Threat Defense (FTD) version 7.1 ou ultérieure.
- Fichiers de capture de paquets au format pcap

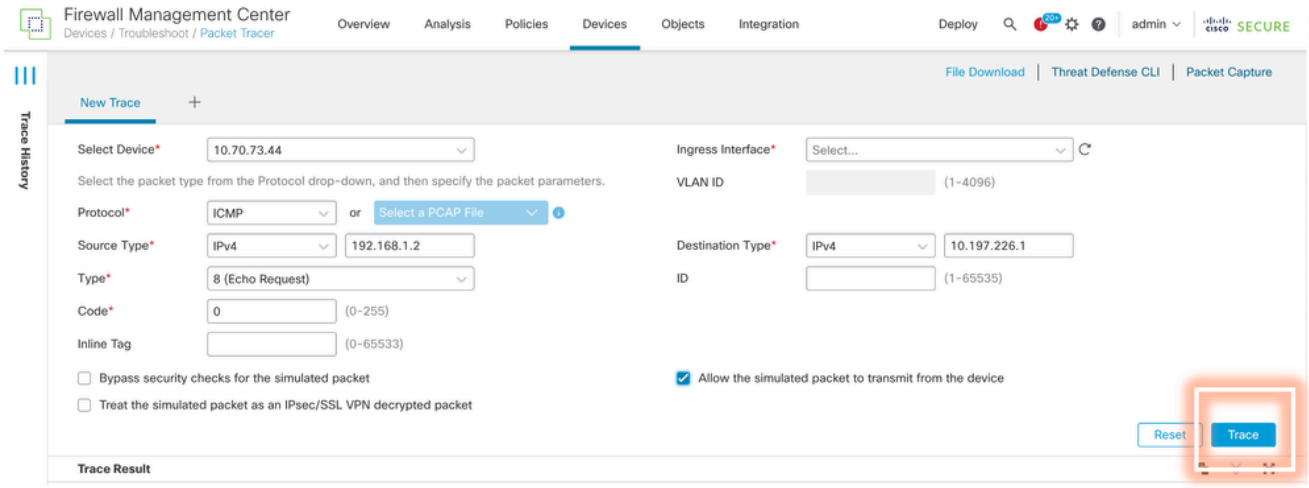
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Relire le paquet à l’aide de l’outil Packet Tracer disponible sur FMC

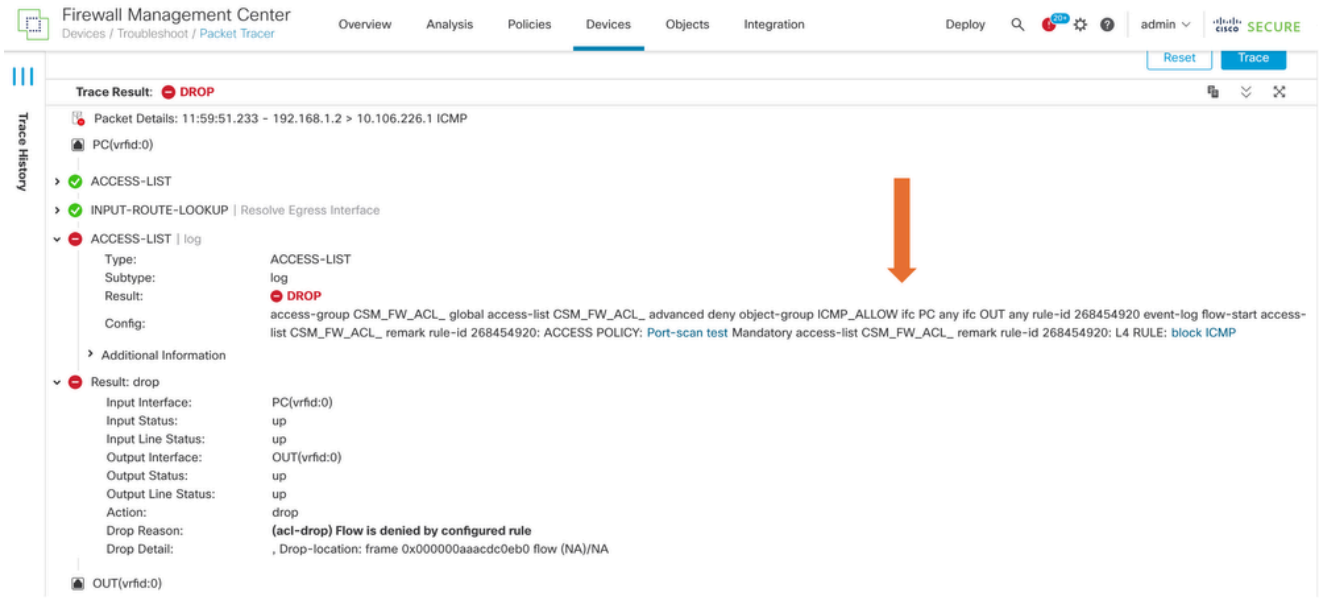
1. Connectez-vous à l'interface FMC. Accédez à Périphériques > Dépannage > Packet Tracer.



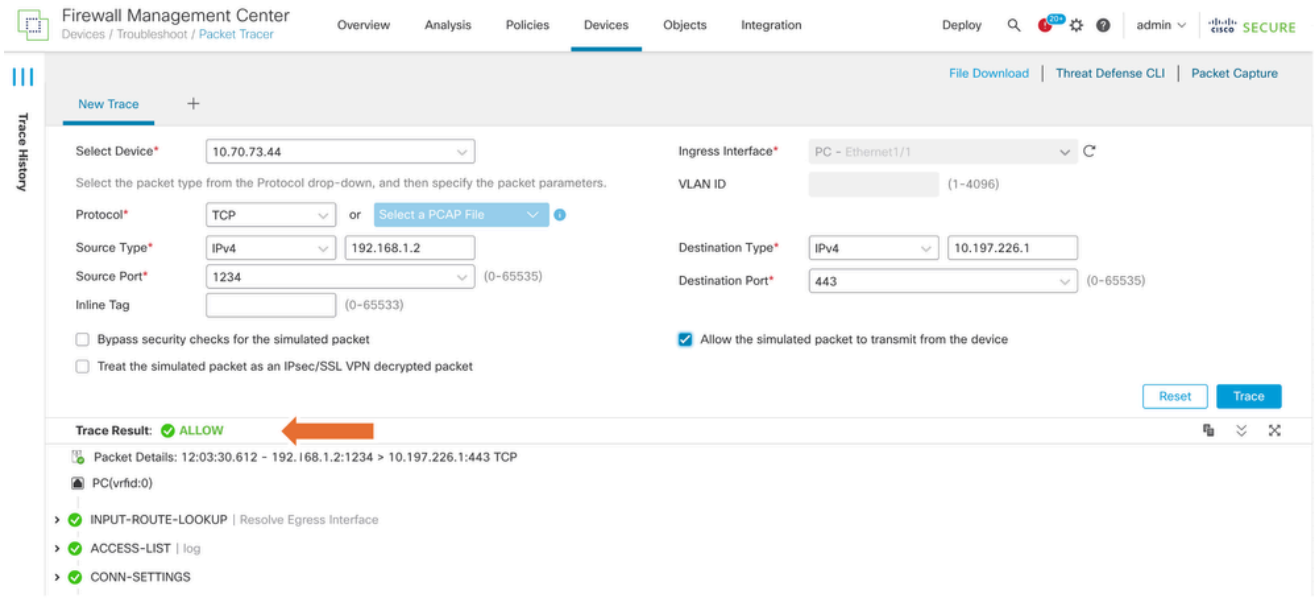
2. Fournissez les détails de la source, de la destination, du protocole et de l'interface d'entrée. Cliquez sur Trace.



3. Utilisez l'option Autoriser le paquet simulé à transmettre à partir du périphérique pour relire ce paquet à partir du périphérique.
4. Notez que le paquet a été abandonné car une règle configurée dans la stratégie de contrôle d'accès permet d'abandonner les paquets ICMP.

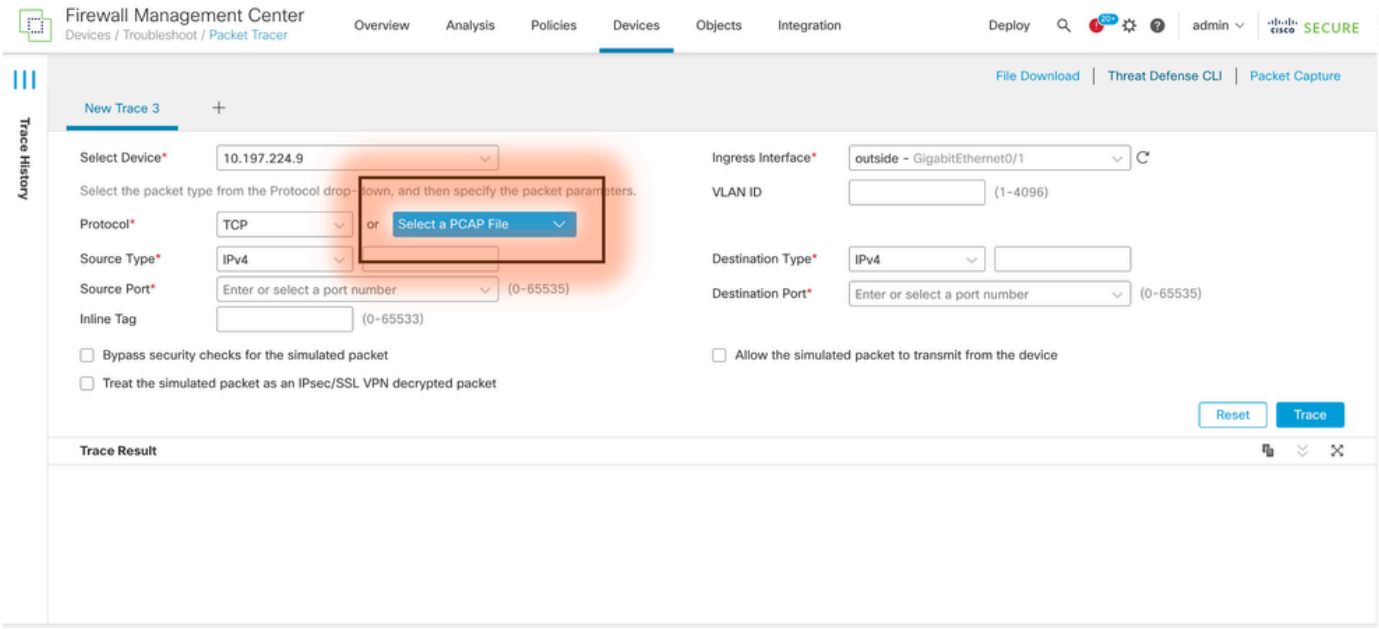


5. Ce traceur de paquets avec des paquets TCP génère le résultat final du suivi (comme illustré).



Rediffusion des paquets à l'aide du fichier PCAP

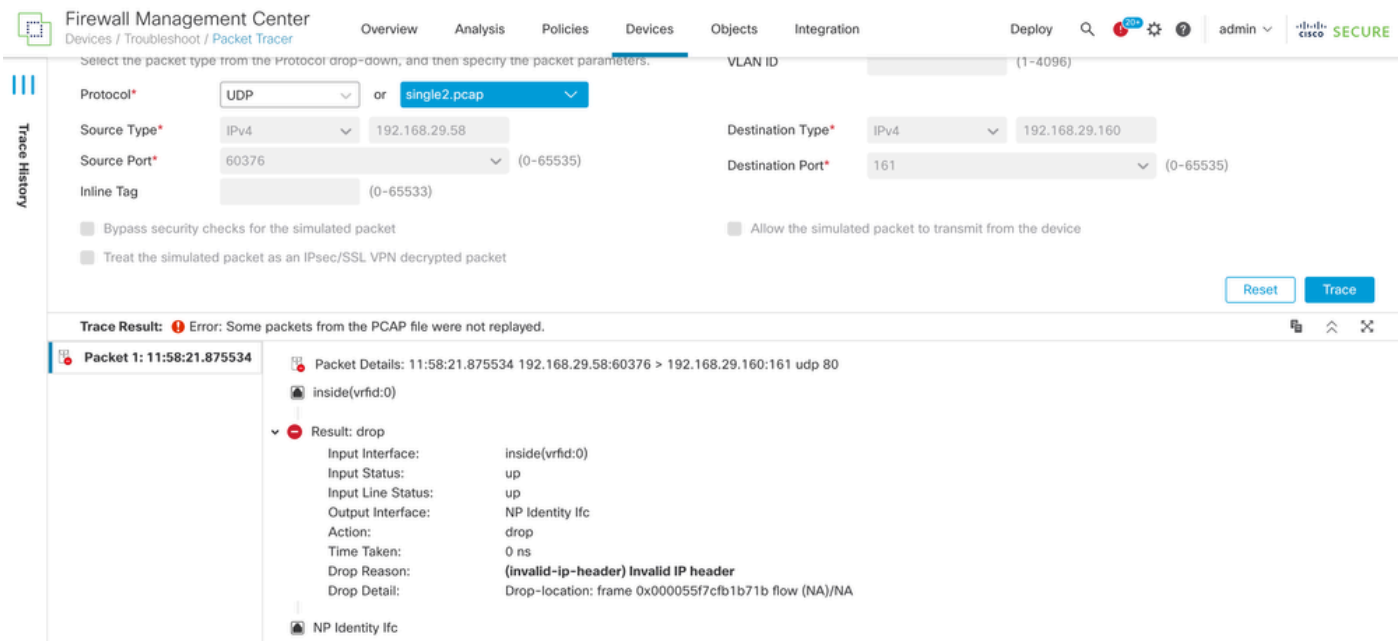
Vous pouvez télécharger le fichier PCAP à l'aide du bouton Sélectionner un fichier PCAP. Sélectionnez ensuite l'interface d'entrée et cliquez sur Trace.



Limites de l'utilisation de cette option

1. Nous ne pouvons simuler que des paquets TCP/UDP.
2. Le nombre maximal de paquets pris en charge dans un fichier PCAP est de 100.
3. La taille du fichier Pcap doit être inférieure à 1 Mo.
4. Le nom du fichier PCAP ne doit pas dépasser 64 caractères (extension incluse) et ne doit contenir que des caractères alphanumériques, des caractères spéciaux («.», «-», «_») ou les deux.
5. Actuellement, un seul flux de paquets est pris en charge.

Le Trace 3 affiche la raison de suppression comme en-tête IP non valide



Documents associés

Pour plus d'informations sur les captures de paquets et les traceurs, veuillez vous reporter au document Cisco Live Document.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.