Een pakket opnieuw afspelen met Packet Tracer Tool in FMC

Inhoud

Inleiding

Dit document beschrijft hoe u een pakket in uw FTD-apparaat kunt terugspelen met de FMC GUI Packet Tracer-tool.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van FirePOWER-technologie
- Kennis van pakketstroom door de firewall

Gebruikte componenten

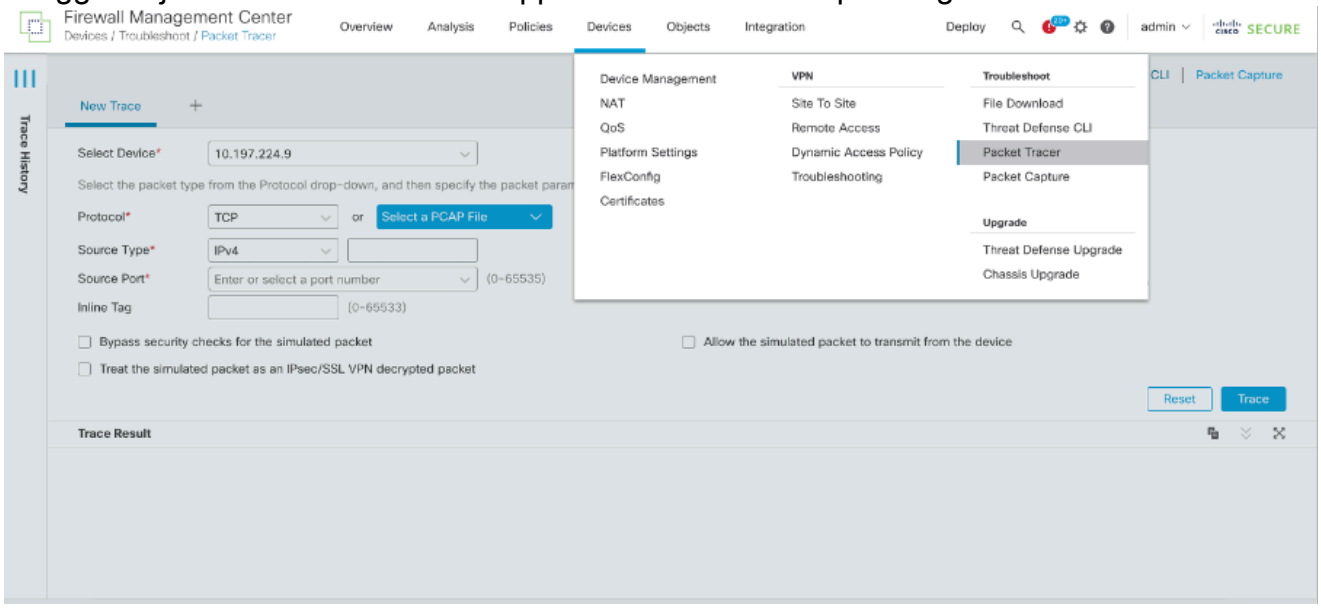
- Cisco Secure Firewall Management Center (FMC) en Cisco Firewall Threat Defence (FTD), versie 7.1 of hoger.
- Packet-opnamebestanden in pcap-formaat

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

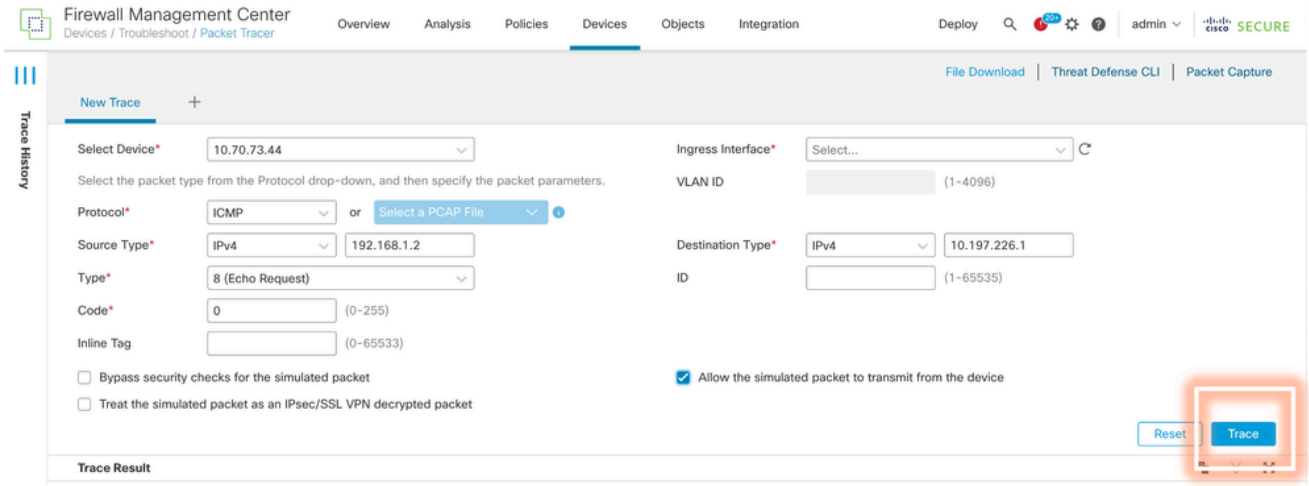
Het pakket opnieuw afspelen met behulp van het pakkettracer-

gereedschap dat beschikbaar is op FMC

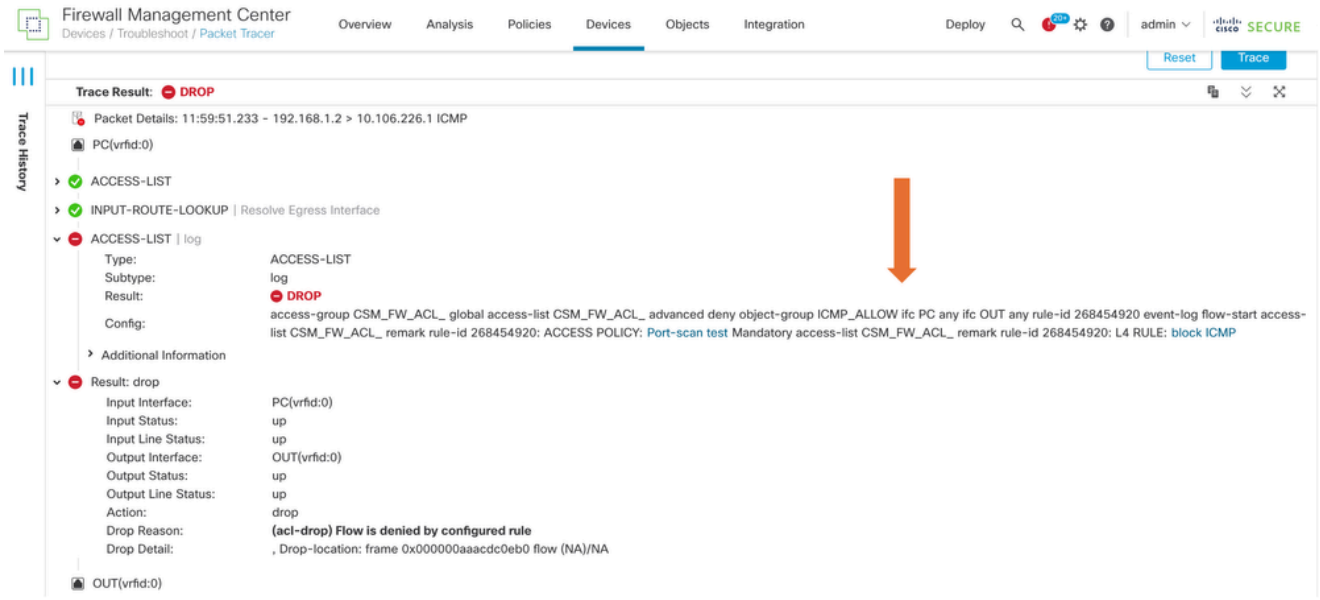
1. Inloggen bij de FMC GUI. Ga naar Apparaten > Probleemoplossing > Packet Tracer.



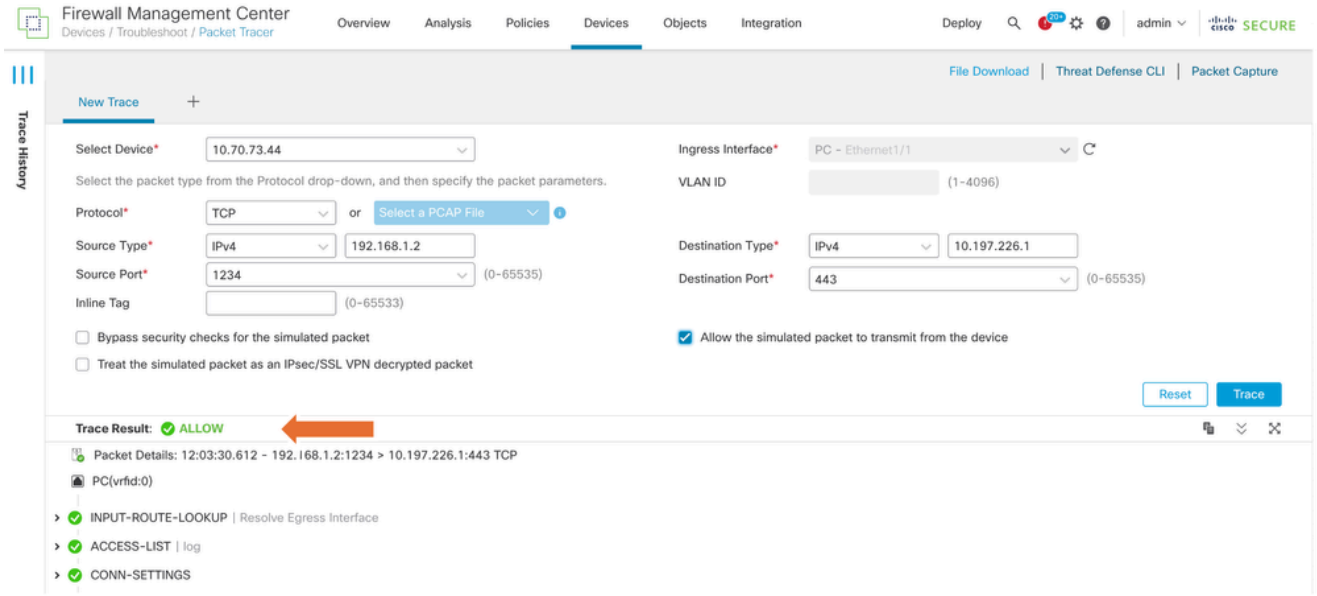
2. Verstrek de details van de bron, de bestemming, het protocol, de ingangsinterface. Klik op Overtrekken.



3. Gebruik de optie Het gesimuleerde pakket toestaan om van het apparaat over te brengen om dit pakket van het apparaat terug te spelen.
4. Merk op dat het pakket is gedropt omdat er een geconfigureerde regel in het toegangscontrolebeleid is om ICMP-pakketten te laten vallen.

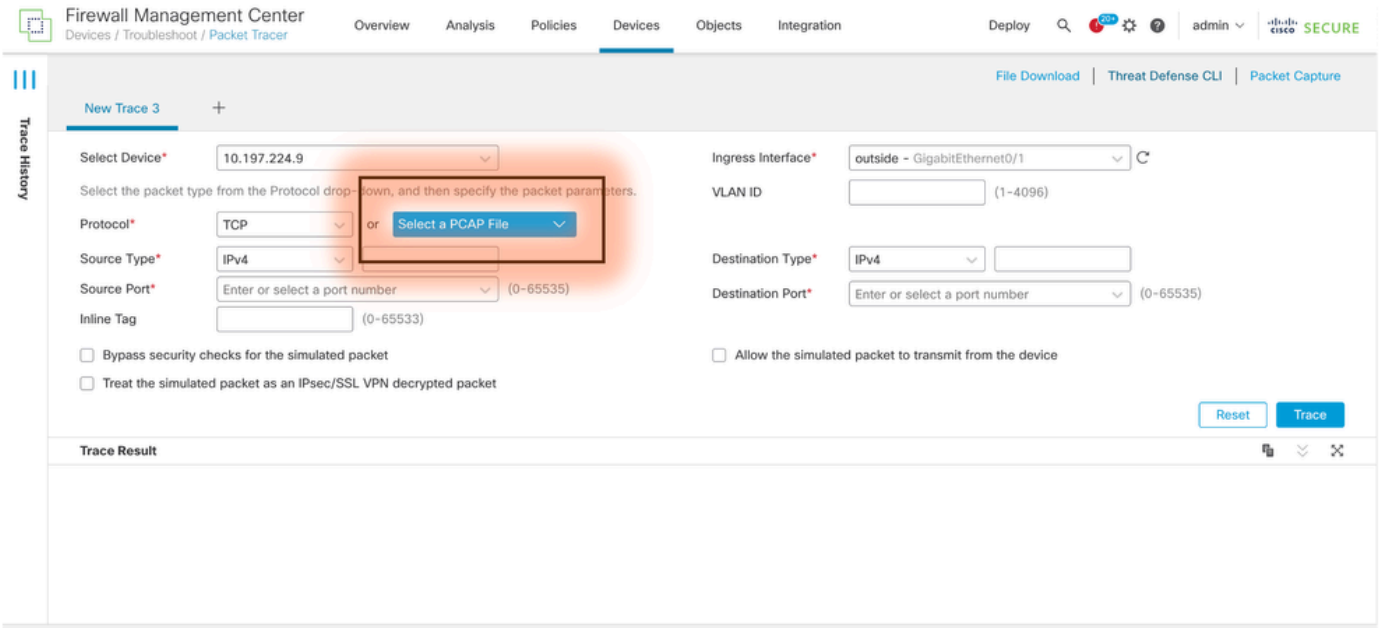


5. Dit pakkettracer met TCP pakt het eindresultaat van het overtrekken (zoals getoond).



Packets met PCAP-bestand terugspelen

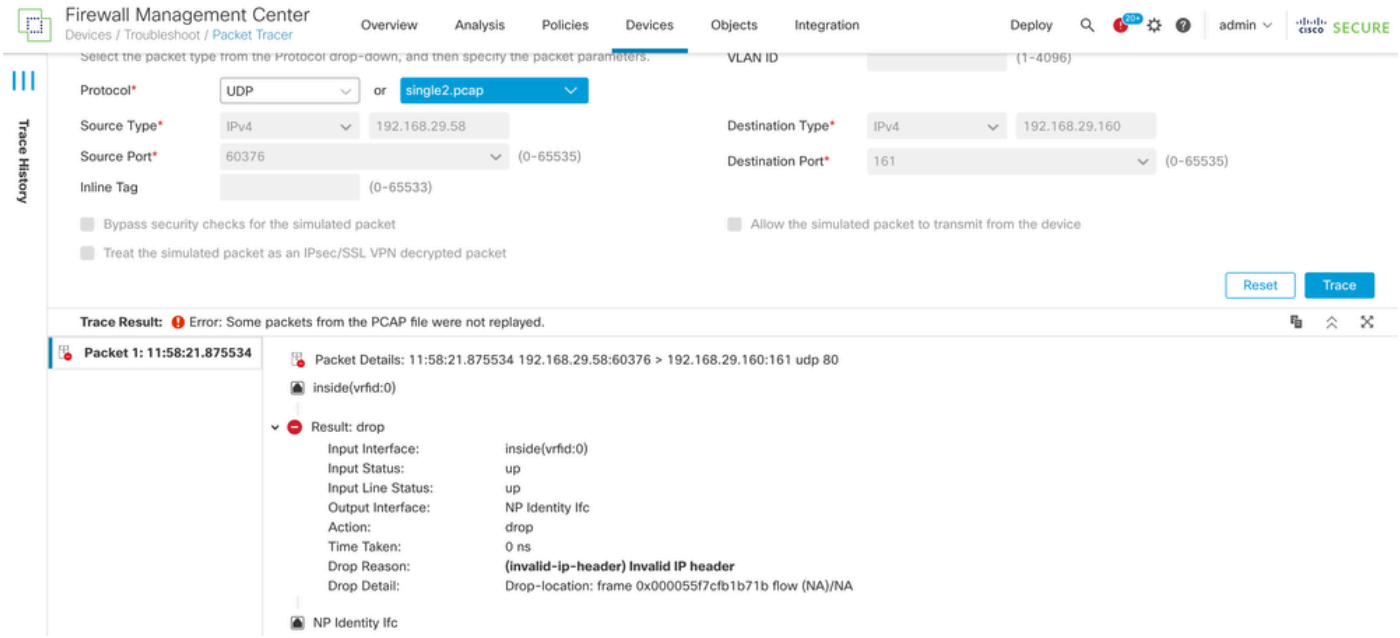
U kunt het PCAP-bestand uploaden met de knop Select a PCAP File. Selecteer vervolgens de interface Ingress en klik op Trace.



Beperkingen bij het gebruik van deze optie

1. We kunnen alleen TCP/UDP-pakketten simuleren.
2. Het maximale aantal pakketten dat in een PCAP-bestand wordt ondersteund, is 100.
3. De maximale bestandsgrootte moet minder dan 1 MB zijn.
4. De PCAP-bestandsnaam mag niet meer dan 64 tekens lang zijn (extensie meegeleverd) en mag alleen alfanumerieke, speciale tekens (".", "-", "_") of beide bevatten.
5. Momenteel worden slechts één stroompakketten ondersteund.

Trace 3 toont druppelreden als ongeldige ip header



Verwante documenten

Raadpleeg Cisco Live Document voor meer informatie over pakketopnamen en tracers.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.