

Een pakket opnieuw afspelen met Packet Tracer Tool in FMC

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Het pakket opnieuw afspelen met behulp van het pakkettracer-gereedschap dat beschikbaar is op FMC](#)

[Packets met PCAP-bestand terugspelen](#)

[Beperkingen bij het gebruik van deze optie](#)

[Verwante documenten](#)

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

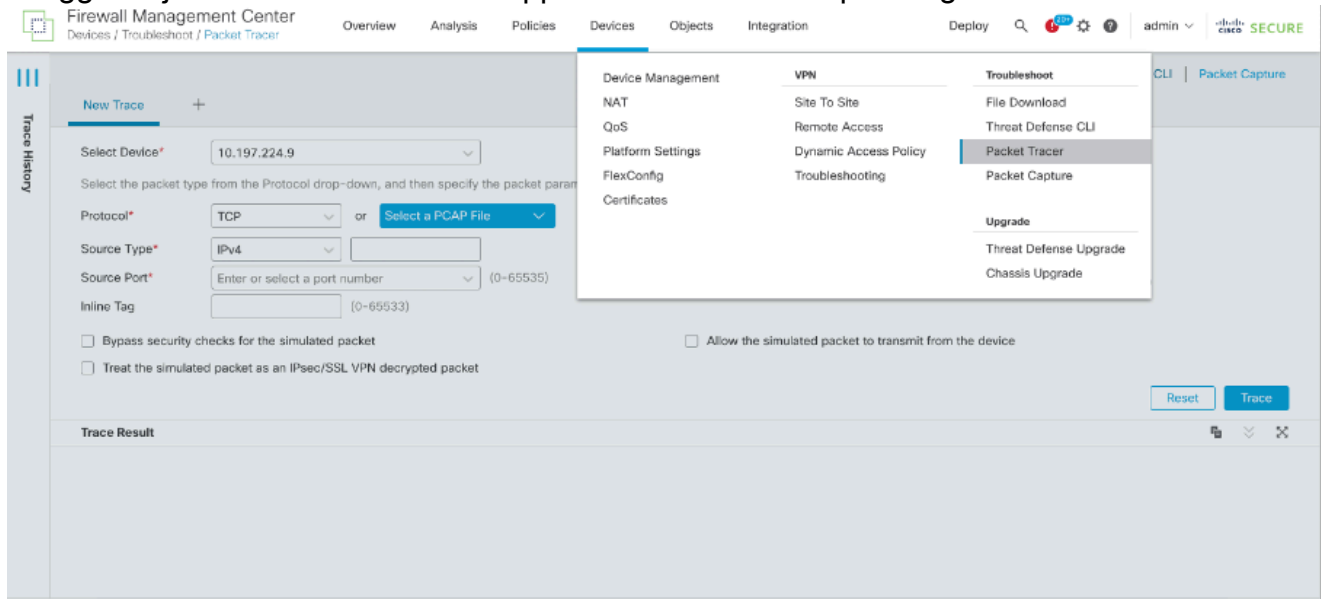
- Cisco Secure Firewall Management Center (FMC) en Cisco Firewall Threat Defence (FTD), versie 7.1 of hoger.
- Packet-opnamebestanden in pcap-formaat

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.

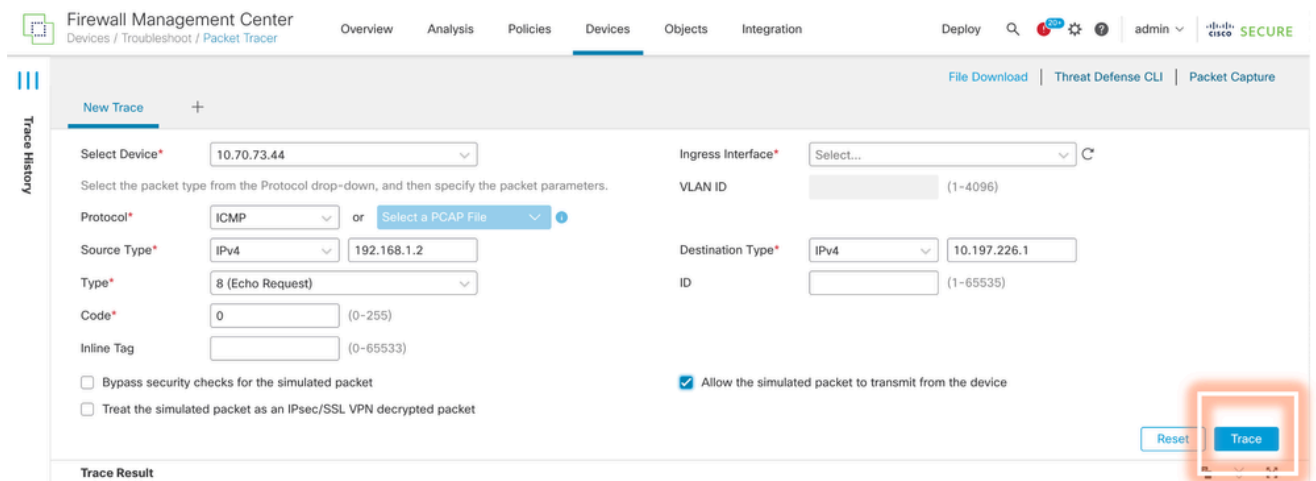
Het pakket opnieuw afspelen met behulp van het pakkettracer-

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.

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 500 ⚙️ ? admin ✓ CISCO SECURE

Trace History

Trace Result: **DROP**

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

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
 - Additional Information
- ✗ 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 0x000000aaacd0eb0 flow (NA)/NA

OUT(vrfd:0)

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

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration Deploy 🔍 500 ⚙️ ? admin ✓ CISCO SECURE

Trace History

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

Ingress Interface* PC - Ethernet1/1

VLAN ID (1-4096)

Destination Type* IPv4 10.197.226.1

Destination Port* 443 (0-65535)

Reset Trace

Trace Result: **ALLOW**

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

PC(vrfd:0)

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

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.

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)

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

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

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)

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(vrfd:0)

Result: drop

Input Interface: inside(vrfd: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

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.