

Riprodurre un pacchetto utilizzando lo strumento Packet Tracer in FMC

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Riprodurre il pacchetto utilizzando lo strumento di traccia dei pacchetti disponibile in FMC](#)

[Riprodurre i pacchetti utilizzando il file PCAP](#)

[Limitazioni per l'utilizzo di questa opzione](#)

[Documenti correlati](#)

Introduzione

Questo documento descrive come è possibile riprodurre un pacchetto nel dispositivo FTD utilizzando lo strumento Packet Tracer dell'interfaccia utente di FMC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza della tecnologia Firepower
- Conoscenza del flusso di pacchetti attraverso il firewall

Componenti usati

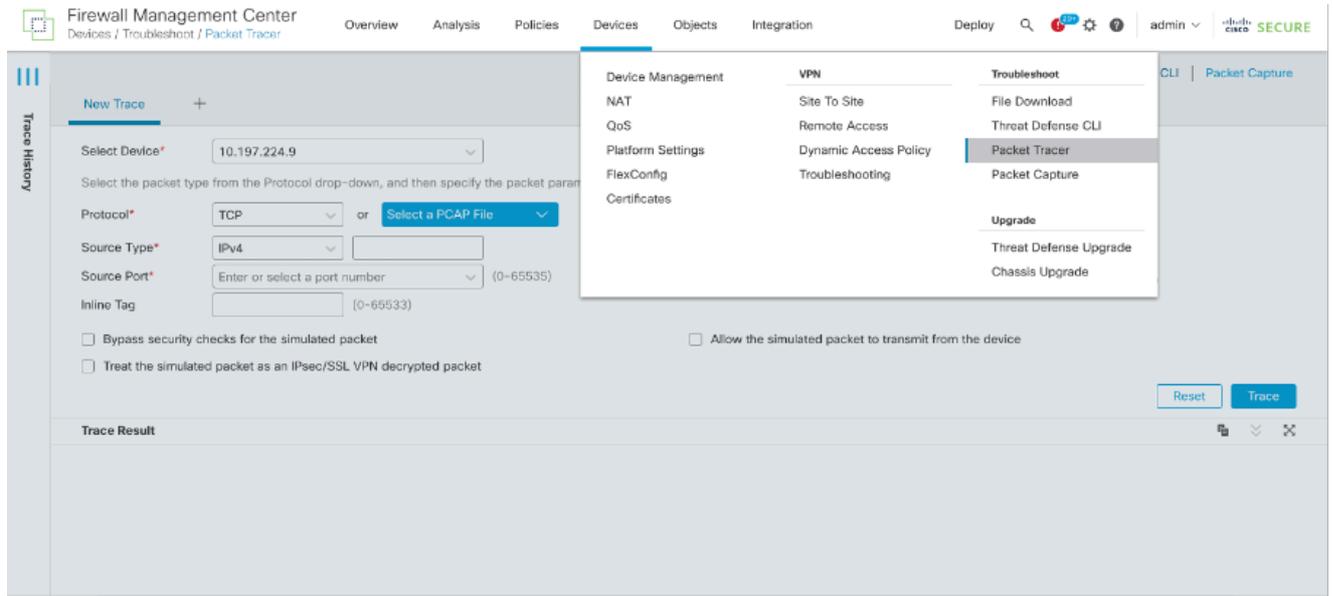
- Cisco Secure Firewall Management Center (FMC) e Cisco Firewall Threat Defense (FTD) versione 7.1 o successive.
- File di acquisizione pacchetti in formato pcap

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

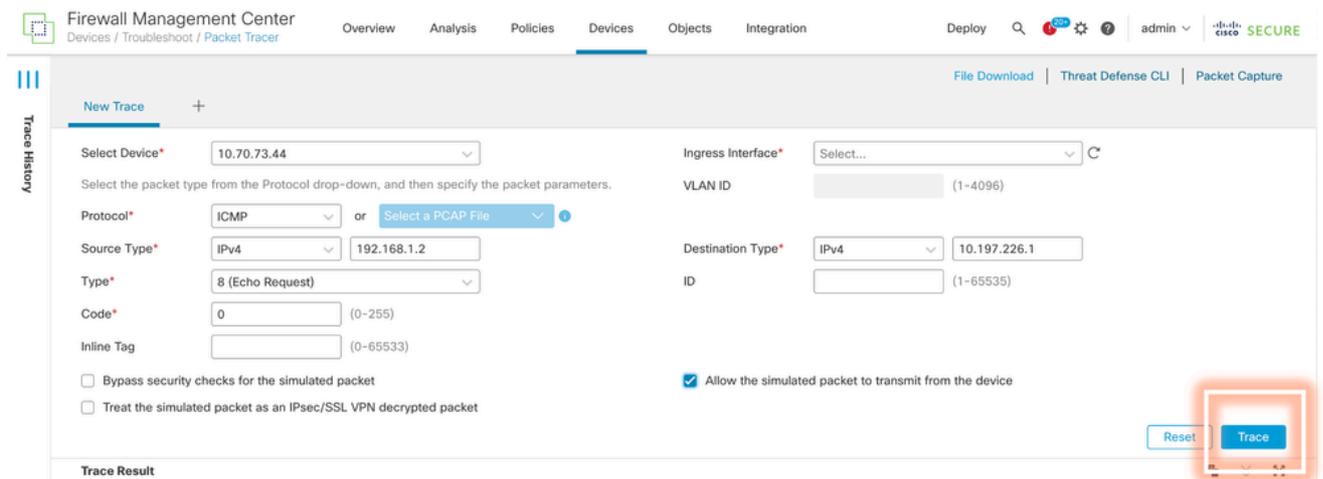
Riprodurre il pacchetto utilizzando lo strumento di traccia dei

pacchetti disponibile in FMC

1. Accedere alla GUI di FMC. Selezionare Devices > Troubleshoot > Packet Tracer.



2. Fornire i dettagli di origine, destinazione, protocollo e interfaccia in entrata. Fare clic su Traccia.



3. Usare l'opzione Consenti al pacchetto simulato di trasmettere dal dispositivo per riprodurre il pacchetto dal dispositivo.

4. Il pacchetto è stato eliminato perché nei criteri di controllo di accesso è presente una regola configurata per l'eliminazione dei pacchetti ICMP.

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 50% ⚙️ ? admin ▾ Cisco **SECURE**

Trace History

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. Questo packet tracer con i pacchetti TCP restituisce il risultato finale della traccia (come mostrato).

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

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

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

Riprodurre i pacchetti utilizzando il file PCAP

È possibile caricare il file pcap utilizzando il pulsante Seleziona file PCAP. Selezionare quindi l'interfaccia in ingresso e fare clic su Traccia.

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 2024 ⚙️ ? admin | cisco 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

Limitazioni per l'utilizzo di questa opzione

1. Possiamo solo simulare pacchetti TCP/UDP.
2. Il numero massimo di pacchetti supportati in un file PCAP è 100.
3. Le dimensioni del file Pcap devono essere inferiori a 1 MB.
4. Il nome del file PCAP non deve superare i 64 caratteri (estensione inclusa) e deve contenere solo caratteri alfanumerici, speciali (".", "-", "_") o entrambi.
5. Al momento sono supportati solo pacchetti a flusso singolo.

La traccia 3 mostra il motivo dell'eliminazione come intestazione IP non valida

Firewall Management Center
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 2024 ⚙️ ? admin | cisco 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(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

Documenti correlati

Per ulteriori informazioni sulle acquisizioni e i tracciatori dei pacchetti, fare riferimento a [Cisco Live Document](#).

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).