

# Wiedergabe eines Pakets mit dem Packet Tracer-Tool in FMC

## Inhalt

---

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Wiedergabe des Pakets mit dem auf FMC verfügbaren Tool zur Paketverfolgung](#)

[Wiedergabe der Pakete mit der PCAP-Datei](#)

[Einschränkungen bei der Verwendung dieser Option](#)

[Verwandte Dokumente](#)

---

## Einleitung

In diesem Dokument wird beschrieben, wie Sie ein Paket mithilfe des GUI Packet Tracer-Tools von FMC auf Ihrem FTD-Gerät wiedergeben können.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Kenntnisse der FirePOWER-Technologie
- Kenntnis des Paketflusses durch die Firewall

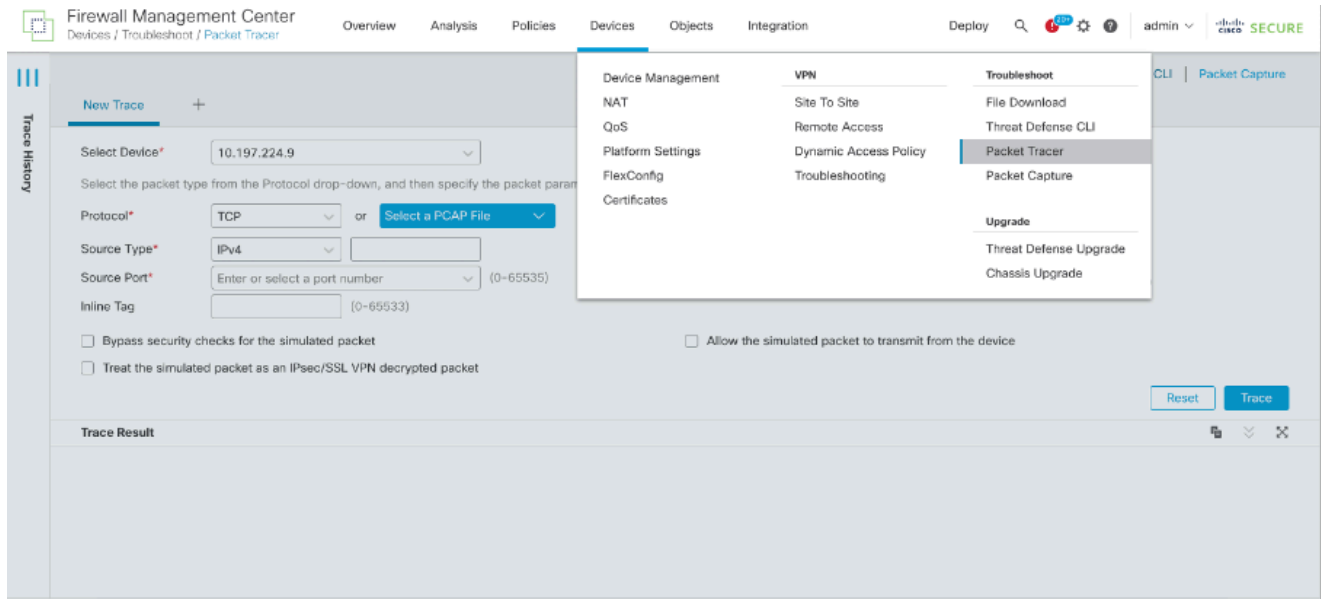
### Verwendete Komponenten

- Cisco Secure Firewall Management Center (FMC) und Cisco Firewall Threat Defense (FTD) Version 7.1 oder höher
- Paketerfassungsdateien im pcap-Format

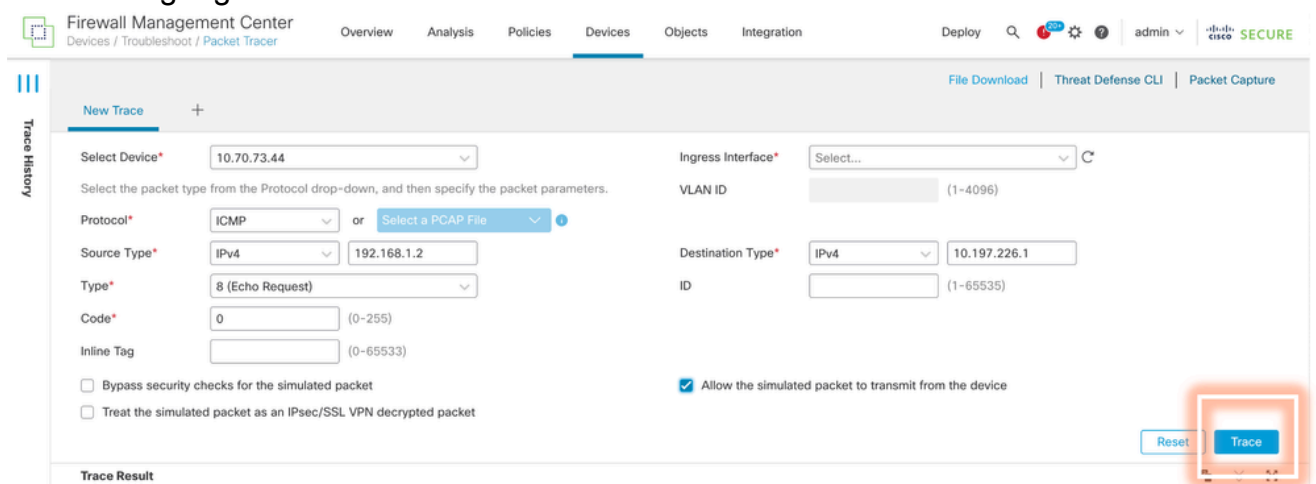
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Wiedergabe des Pakets mit dem auf FMC verfügbaren Tool zur Paketverfolgung

1. Melden Sie sich an der FMC-GUI an. Gehen Sie zu Devices > Troubleshoot > Packet Tracer.



2. Geben Sie die Details zu Quelle, Ziel, Protokoll und Eingangsschnittstelle an. Klicken Sie auf Nachverfolgung.



3. Verwenden Sie die Option Senden des simulierten Pakets vom Gerät zulassen, um dieses Paket vom Gerät wiederzugeben.

4. Beachten Sie, dass das Paket verworfen wurde, da in der Zugriffskontrollrichtlinie eine konfigurierte Regel zum Verwerfen von ICMP-Paketen vorhanden ist.

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 0x000000aaadc0eb0 flow (NA)/NA
- OUT(vrfid:0)

5. Dieser Paket-Tracer mit TCP-Paketen stellt das Endergebnis der Verfolgung dar (wie dargestellt).

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

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(vrfid:0)

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

## Wiedergabe der Pakete mit der PCAP-Datei

Sie können die PCAP-Datei über die Schaltfläche PCAP-Datei auswählen hochladen. Wählen Sie dann die Eingangsschnittstelle aus und klicken Sie auf Trace (Verfolgung).

Firewall Management Center  
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 2024 ⚙️ ? 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

## Einschränkungen bei der Verwendung dieser Option

1. Wir können nur TCP-/UDP-Pakete simulieren.
2. Eine PCAP-Datei unterstützt maximal 100 Pakete.
3. Die Größe der PCAP-Datei muss kleiner als 1 MB sein.
4. Der PCAP-Dateiname darf maximal 64 Zeichen lang sein (Erweiterung eingeschlossen) und nur alphanumerische Sonderzeichen (".", "-", "\_") oder beides enthalten.
5. Derzeit werden nur einzelne Datenflusspakete unterstützt.

In Trace 3 wird der Verwerfungsgrund als ungültiger IP-Header angezeigt.

Firewall Management Center  
Devices / Troubleshoot / Packet Tracer

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 2024 ⚙️ ? 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(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

## Verwandte Dokumente

Weitere Informationen zu Paketerfassungen und Tracern finden Sie im [Cisco Live-Dokument](#).

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.