

# Gebruik Firepower Threat Defence Capture en Packet Tracer

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[FTD-pakketverwerking](#)

[Configureren](#)

[Netwerkdiagram](#)

[Werken met Snort Engine Captures](#)

[Voorwaarden](#)

[Vereisten](#)

[Oplossing](#)

[Werken met Snort Engine Captures](#)

[Vereisten](#)

[Oplossing](#)

[Voorbeelden van TCPdump-filter](#)

[Werken met FTD LINA Engine Captures](#)

[Vereisten](#)

[Oplossing](#)

[Werken met FTD LINA Engine Captures - Exporteer een Capture via HTTP](#)

[Vereisten](#)

[Oplossing](#)

[Werken met FTD LINA Engine Captures - Exporteer een Capture via FTP/TFTP/SCP](#)

[Vereisten](#)

[Oplossing](#)

[Werken met FTD LINA Engine Captures - Trace a Real Traffic Packet](#)

[Vereisten](#)

[Oplossing](#)

[Capture Tool in Post-6.2 FMC-softwareversies](#)

[Workaround - Gebruik de FTD CLI](#)

[Traceer een echt pakket op post-6.2 FMC](#)

[FTD-programma voor pakkettracing](#)

[Vereisten](#)

[Oplossing](#)

[Packet Tracer UI Tool in Post-6.2 FMC-softwareversies](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft hoe u de hulpprogramma's van Firepower Threat Defence (FTD) kunt gebruiken voor het detecteren en traceren van pakketten.

## Voorwaarden

### Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

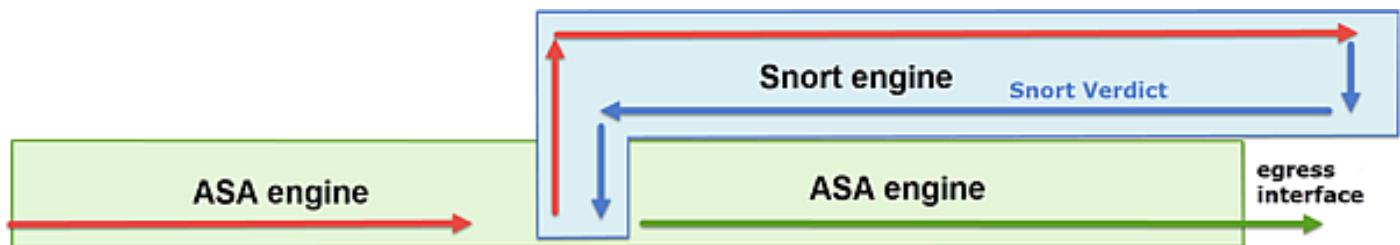
- ASA 5515-X waarin FTD-software 6.1.0 wordt uitgevoerd
- FPR4110 die FTD-software 6.2.2 uitvoert
- FS4000 die Firepower Management Center (FMC)-software draait 6.2.2

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.

## Achtergrondinformatie

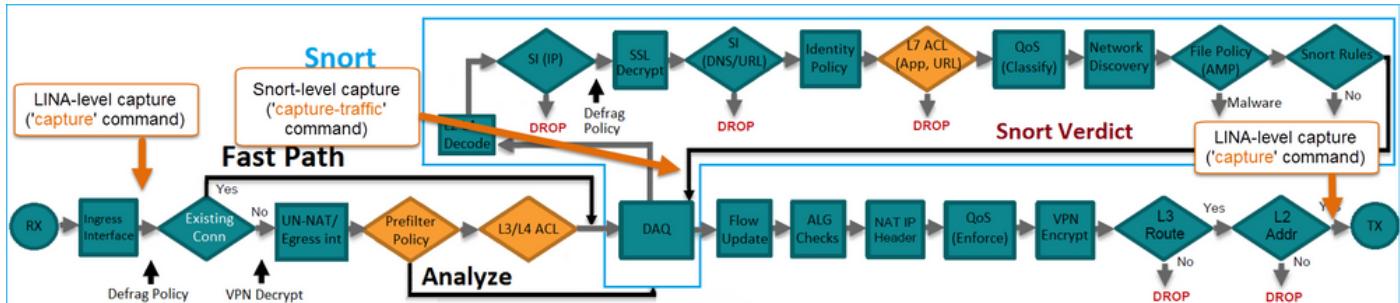
### FTD-pakketverwerking

De FTD-pakketverwerking wordt als volgt gevisualiseerd:



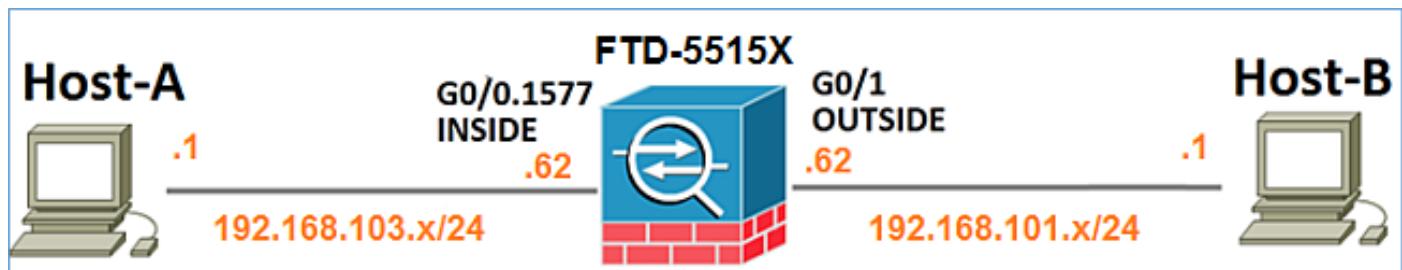
1. Een pakket gaat de toegangsinterface in, en het wordt behandeld door de motor van LINA.
2. Als het beleid vereist dat het pakket wordt geïnspecteerd door de Snort-engine.
3. De snort engine geeft een oordeel voor het pakket terug.
4. De LINA-engine wijst het pakket af of stuurt het door op basis van het Snort-oordeel.

Op basis van de architectuur kunnen de FTD-opnamen op deze plaatsen worden gemaakt:



# Configureren

## Netwerkdiagram



## Werken met Snort Engine Captures

### Voorwaarden

Er is een Access Control Policy (ACS) van toepassing op FTD die ICMP-verkeer (Internet Control Message Protocol) mogelijk maakt. Het beleid heeft ook een toegepast Inbraakbeleid:

Screenshot van de FTD5515 Access Control Policy interface:

- Policies** tab is geselecteerd.
- Identity Policy: None** en **SSL Policy: None** zijn ingesteld.
- Inheritance Settings** en **Policy Assignments (1)** zijn weergegeven.
- Rules** tab is geselecteerd.
- Mandatory - FTD5515-(1-1)** sectie:
  - Regel 1: Allow ICMP van **any** naar **any** (192.168.103.0/24 en 192.168.101.0/24) met actie **Allow**.
- Default - FTD5515 (-)** sectie:
  - Geen regels.
- Intrusion Policy** is weergegeven.
- Default Action**: Access Control: Block All Traffic.

### Vereisten

1. Schakel opname in op FTD CLISH-modus zonder filter.
2. Ping door de FTD en controleer de opgenomen uitvoer.

### Oplossing

Stap 1. Log in op de FTD-console of SSH op de br1-interface en schakel de opname in in de FTD CLISH-modus zonder filter.

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - Router

```
Selection? 1
```

```
Please specify tcpdump options desired.  
(or enter '?' for a list of supported options)  
Options:
```

Op FTD 6.0.x is de opdracht:

```
> system support capture-traffic
```

Stap 2. Ping door FTD en controleer de opgenomen uitvoer.

```
> capture-traffic
```

```
Please choose domain to capture traffic from:
```

- 0 - br1
- 1 - Router

```
Selection? 1
```

```
Please specify tcpdump options desired.  
(or enter '?' for a list of supported options)
```

```
Options:
```

```
12:52:34.749945 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,  
seq 1, length 80  
12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq  
1, length 80  
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,  
seq 2, length 80  
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq  
2, length 80  
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,  
seq 3, length 80  
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq  
3, length 80  
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,  
seq 4, length 80  
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq  
4, length 80  
^C<- to exit press CTRL + C
```

## Werken met Snort Engine Captures

### Vereisten

1. Opname op FTD CLISH-modus inschakelen met gebruik van een filter voor IP 192.168.101.1.
2. Ping door FTD en controleer de opgenomen uitvoer.

### Oplossing

**Stap 1. Schakel opname in op FTD CLISH-modus met behulp van een filter voor IP 192.168.101.1.**

```
> capture-traffic

Please choose domain to capture traffic from:
 0 - br1
 1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: host 192.168.101.1
```

**Stap 2. Ping door de FTD en controleer de opgenomen uitvoer:**

```
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 0, length 80
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 1, length 80
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 2, length 80
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, length 80
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 4, length 80
```

U kunt de **-n** optie gebruiken om de hosts en poortnummers in numerieke indeling te zien. De eerdere opname wordt bijvoorbeeld weergegeven als:

```
> capture-traffic

Please choose domain to capture traffic from:
 0 - br1
 1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -n host 192.168.101.1

13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 0, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 1, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 2, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length 80
13:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 4, length 80
```

## Voorbeelden van TCPdump-filter

Voorbeeld 1:

Typ deze opdracht om Src IP of Dst IP = 192.168.101.1 en Src-poort of Dst-poort = TCP/UDP 23 op te nemen:

```
Options: -n host 192.168.101.1 and port 23
```

Voorbeeld 2:

Om Src IP = 192.168.101.1 en Src poort = TCP/UDP 23 op te nemen, voert u deze opdracht in:

```
Options: -n src 192.168.101.1 and src port 23
```

Voorbeeld 3:

Om Src IP = 192.168.101.1 en Src poort = TCP 23 op te nemen, voert u deze opdracht in:

```
Options: -n src 192.168.101.1 and tcp and src port 23
```

Voorbeeld 4:

Om Src IP = 192.168.101.1 op te nemen en te zien het MAC-adres van de pakketten de 'e' optie toevoegen en deze opdracht invoeren:

```
Options: -ne src 192.168.101.1
```

```
17:57:48.709954 6c:41:6a:a1:2b:f6 > a8:9d:21:93:22:90, ethertype IPv4 (0x0800), length 58:  
192.168.101.1.23 > 192.168.103.1.25420:  
Flags [S.], seq 3694888749, ack 1562083610, win 8192, options [mss 1380], length 0
```

Voorbeeld 5:

Om weg te gaan nadat u 10 pakketten hebt opgenomen, voert u deze opdracht in:

```
Options: -n -c 10 src 192.168.101.1
```

```
18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3758037348, win 32768,  
length 0  
18:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length  
2  
18:03:12.949932 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 1, win 32768, length  
10  
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 0  
18:03:13.249971 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 3, win 32768, length  
2  
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 0  
18:03:13.279969 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 5, win 32768, length  
10  
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 0  
18:03:13.309966 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 7, win 32768, length  
12  
18:03:13.349972 IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 9, win 32768, length 0
```

Voorbeeld 6:

Om een opname naar een bestand te schrijven met de naam **capture.pcap** en het via FTP naar een externe server te kopiëren, voert u deze opdracht in:

```
Options: -w capture.pcap host 192.168.101.1
```

```
CTRL + C <- to stop the capture
```

```
> file copy 10.229.22.136 ftp / capture.pcap
```

```
Enter password for ftp@10.229.22.136:
```

```
Copying capture.pcap
copy successful.
```

>

## Werken met FTD LINA Engine Captures

### Vereisten

1. Schakel twee opnamen in met het gebruik van deze filters:

Bron-IP	192.168.103.
	1
Bestemmings-IP	192.168.101.
Protocol	ICMP
Interface	BINNENKAN
	T
Bron-IP	192.168.103.
	1
Bestemmings-IP	192.168.101.
Protocol	ICMP
Interface	BUITEN

2. Pingen van host-A (192.168.103.1) naar host-B (192.168.101.1) en controle van de opnamen.

### Oplossing

- Stap 1. Schakel de opnamen in:

```
> capture CAPI interface INSIDE match icmp host 192.168.103.1 host 192.168.101.1
> capture CAPO interface OUTSIDE match icmp host 192.168.101.1 host 192.168.103.1
```

- Stap 2. Controleer de opnamen in de CLI.

Ping van host-A naar host-B:

```
C:\Users\cisco>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Reply from 192.168.101.1: bytes=32 time=4ms TTL=255
Reply from 192.168.101.1: bytes=32 time=5ms TTL=255
Reply from 192.168.101.1: bytes=32 time=1ms TTL=255
Reply from 192.168.101.1: bytes=32 time=1ms TTL=255
```

```
> show capture

capture CAPI type raw-data interface INSIDE [Capturing - 752 bytes]
  match icmp host 192.168.103.1 host 192.168.101.1
capture CAPO type raw-data interface OUTSIDE [Capturing - 720 bytes]
  match icmp host 192.168.101.1 host 192.168.103.1
```

De twee opnamen hebben verschillende afmetingen als gevolg van de Dot1Q-header op de

INSIDE-interface, zoals in dit uitvoervoorbeeld:

```
> show capture CAPI
8 packets captured
 1: 17:24:09.122338 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
 2: 17:24:09.123071 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
 3: 17:24:10.121392 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
 4: 17:24:10.122018 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
 5: 17:24:11.119714 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
 6: 17:24:11.120324 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
 7: 17:24:12.133660 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
 8: 17:24:12.134239 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown

> show capture CAPO
8 packets captured
 1: 17:24:09.122765 192.168.103.1 > 192.168.101.1: icmp: echo request
 2: 17:24:09.122994 192.168.101.1 > 192.168.103.1: icmp: echo reply
 3: 17:24:10.121728 192.168.103.1 > 192.168.101.1: icmp: echo request
 4: 17:24:10.121957 192.168.101.1 > 192.168.103.1: icmp: echo reply
 5: 17:24:11.120034 192.168.103.1 > 192.168.101.1: icmp: echo request
 6: 17:24:11.120263 192.168.101.1 > 192.168.103.1: icmp: echo reply
 7: 17:24:12.133980 192.168.103.1 > 192.168.101.1: icmp: echo request
 8: 17:24:12.134194 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

## Werken met FTD LINA Engine Captures - Exporteer een Capture via HTTP

### Vereisten

Exporteer de opnamen die in het eerder scenario met een browser zijn gemaakt.

### Oplossing

Om de opnamen met een browser te exporteren, moet u:

1. De HTTPS-server inschakelen
2. HTTPS-toegang toestaan

Standaard is de HTTPS-server uitgeschakeld en is geen toegang toegestaan:

```
> show running-config http
>
```

Stap 1. Navigeer naar **Apparaten > Platform-instellingen**, klik op **Nieuw beleid** en kies **Threat Defense-instellingen**:

The screenshot shows the Firepower Management Platform interface. At the top, there are tabs for Devices, Objects, AMP, Deploy, System, Help, and a user account (mikis). Below the tabs, a navigation bar includes PN, Platform Settings, Object Management, and a New Policy button. A dropdown menu is open over the Threat Defense Settings tab, which is highlighted with an orange border. The main content area shows a table with columns for Device Type and Status, and a message targeting one device. The Threat Defense tab is currently active.

Specificeer de beleidsnaam en het apparaatdoel:

The screenshot shows the 'New Policy' configuration screen. The policy name is set to 'FTD5515-System\_Policy'. Under 'Targeted Devices', it says 'Select devices to which you want to apply this policy.' The 'Available Devices' section contains a search bar with the placeholder 'Search by name or value'. The 'Selected Devices' section shows a single device, 'FTD5515', which is highlighted with an orange border.

Stap 2. Schakel de HTTPS-server in en voeg het netwerk toe waartoe u toegang wilt krijgen tot het FTD-apparaat via HTTPS:

The screenshot shows the configuration for the 'FTD5515-System\_Policy'. On the left, a sidebar lists various protocols: ARP Inspection, Banner, External Authentication, Fragment Settings, **HTTP** (selected), ICMP, Secure Shell, and SMTP Server. The main panel shows the 'Enable HTTP Server' checkbox checked (highlighted with a red box labeled 2) and the port set to 443. Below this, the 'Interface' table has 'INSIDE' listed under 'Network' (highlighted with a red box labeled 3). An 'Add' button is visible at the bottom right of the table.

**Opslaan en implementeren.**

Op het tijdstip van de beleidsplanning, kunt u **debug http** inschakelen om het begin van de HTTP-service te zien:

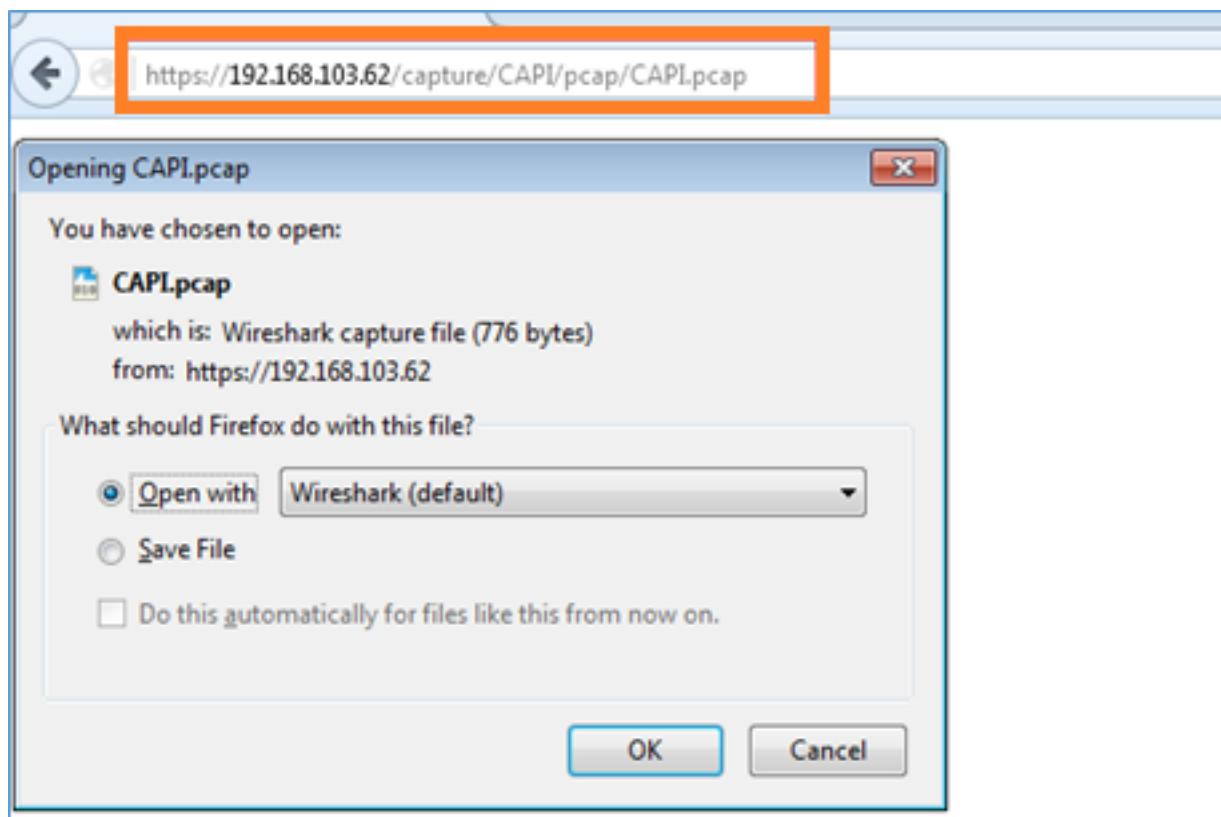
```
> debug http 255
```

```
debug http enabled at level 255.  
http_enable: Enabling HTTP server  
HTTP server starting.
```

Het resultaat op FTD CLI is:

```
> unebug all  
> show run http  
http server enable  
http 192.168.103.0 255.255.255.0 INSIDE
```

Open een browser op Host-A (192.168.103.1) en gebruik deze URL om de eerste opname te downloaden: <https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap>.



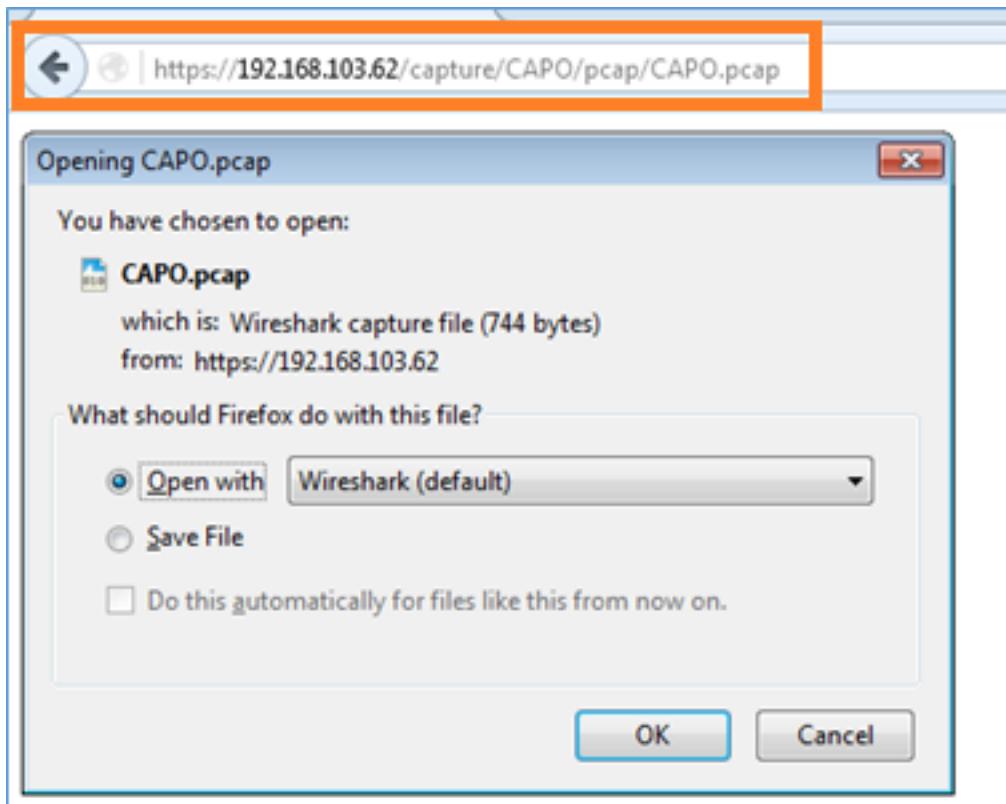
Ter referentie:

<https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap> IP van de FTD-gegevensinterface waar HTTP-server is ingeschakeld

<https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap> De naam van de FTD-opname

<https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap> De naam van het bestand dat is gedownload

Voor de tweede opname, gebruik <https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap>.



## Werken met FTD LINA Engine Captures - Exporteer een Capture via FTP/TFTP/SCP

### Vereisten

Exporteer de opnamen die zijn gemaakt in de eerdere scenario's met FTP/TFTP/SCP-protocollen.

### Oplossing

Exporteer een opname naar een FTP-server:

```
firepower# copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcap
Source capture name [CAPI]?

Address or name of remote host [192.168.78.73]?

Destination username [ftp_username]?

Destination password [ftp_password]?

Destination filename [CAPI.pcap]?
!!!!!
114 packets copied in 0.170 secs
firepower#
```

Exporteer een opname naar een TFTP-server:

```
firepower# copy /pcap capture:CAPI tftp://192.168.78.73
Source capture name [CAPI]? 
```

```
Address or name of remote host [192.168.78.73]?
```

```
Destination filename [CAPI]?
```

```
!!!!!!!!!!!!!!
```

```
346 packets copied in 0.90 secs
```

```
firepower#
```

Exporteer een opname naar een SCP server:

```
firepower# copy /pcap capture:CAPI scp://scp_username:scp_password@192.168.78.55
```

```
Source capture name [CAPI]?
```

```
Address or name of remote host [192.168.78.55]?
```

```
Destination username [scp_username]?
```

```
Destination filename [CAPI]?
```

```
The authenticity of host '192.168.78.55 (192.168.78.55)' can't be established.
```

```
RSA key fingerprint is
```

```
<cb:ca:9f:e9:3c:ef:e2:4f:20:f5:60:21:81:0a:85:f9:02:0d:0e:98:d0:9b:6c:dc:f9:af:49:9e:39:36:96:33  
>(SHA256).
```

```
Are you sure you want to continue connecting (yes/no)? yes
```

```
Warning: Permanently added '192.168.78.55' (SHA256) to the list of known hosts.
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
454 packets copied in 3.950 secs (151 packets/sec)
```

```
firepower#
```

Offload-opnamen van FTD. Momenteel, wanneer u opnamen van FTD moet offload, is de eenvoudigste methode om deze stappen uit te voeren:

1. Van Lina - kopiëren /pcap vastleggen:<cap\_name> disk0:
2. Van FPR root - mv /ngfw/mnt/disk0/<cap\_name> /ngfw/var/common/
3. Van FMC UI - **System > Health > Monitor > Device > Advanced Probleemoplossing** en voer het <cap\_name> in het veld en download in.

## Werken met FTD LINA Engine Captures - Trace a Real Traffic Packet

### Vereisten

Schakel een opname in op FTD met deze filters:

Bron-IP	192.168.103.
	1
Bestemmings-IP	192.168.101.
	1
Protocol	ICMP
Interface	BINNENKAN
	T
Packet-overtrekken	ja
Aantal overtrekkapketten	100

Pingel van host-A (192.168.103.1) de host-B (192.168.101.1) en controleer de opnamen.

## Oplossing

Een echt pakket overtrekken is erg handig om problemen met de connectiviteit op te lossen. Hiermee kunt u alle interne controles zien die een pakket doorloopt. Voeg de trefwoorden voor **overtrek toe** en specificeer het aantal pakketten dat u wilt overtrekken. Standaard overtrekt de FTD de eerste 50 ingangspakketten.

In dit geval, laat opname met spoordetail voor de eerste 100 pakketten toe die FTD op de INTERFACE VAN DE BINNENKANT ontvangt:

```
> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168.101.1
```

Ping van host-A naar host-B en controleer het resultaat:

```
C:\Users\cisco>ping 192.168.101.1

Pinging 192.168.101.1 with 32 bytes of data:
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=2ms TTL=255
Reply from 192.168.101.1: bytes=32 time=8ms TTL=255
```

De opgenomen pakketten zijn:

```
> show capture CAPI28 packets captured
 1: 18:08:04.232989 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
 2: 18:08:04.234622 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
 3: 18:08:05.223941 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
 4: 18:08:05.224872 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
 5: 18:08:06.222309 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
 6: 18:08:06.223148 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
 7: 18:08:07.220752 802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
 8: 18:08:07.221561 802.1Q vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
8 packets shown
```

Deze output toont een spoor van het eerste pakket. De delen die van belang zijn:

- Fase 12 is waar de 'voorwaartse stroom' te zien is. Dit is de LINA engine Dispatch Array (effectief de interne volgorde van de operaties).
- Fase 13 is de fase waarin FTD het pakket naar de gescande instantie stuurt.
- Fase 14 is waar het vonnis in kort geding te zien is.

```
> show capture CAPI2 packet-number 1 trace detail
8 packets captured
 1: 18:08:04.232989 000c.2998.3fec a89d.2193.2293 0x8100 Length: 78
     802.1Q vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request (ttl 128, id 3346)
Phase: 1
Type: CAPTURE
... output omitted ...

Phase: 12
Type: FLOW-CREATION
Subtype:
```

```

Result: ALLOW
Config:
Additional Information:
New flow created with id 195, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_snort
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_inspect_icmp
snp_fp_snort
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet

... output omitted ...

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

1 packet shown
>

```

## Capture Tool in Post-6.2 FMC-softwareversies

In FMC versie 6.2.x is een nieuwe wizard voor pakketopname geïntroduceerd. Navigeer naar **Apparaten > Apparaatbeheer** en klik op het pictogram **Probleemoplossing**. Kies vervolgens **Geavanceerde probleemoplossing** en neem uiteindelijk w/Trace op.

The screenshot shows the FMC UI with the 'Devices' tab selected. A device named 'FTD4110-2' is listed, showing its model as 'Cisco Firepower 4110 Base, Threat, Ma...', license type as 'ACP1', and access control policy as 'ACP1'. There are edit and delete icons for the device.

Kies Opname toevoegen om een FTD-opname te maken:

The screenshot shows the 'Advanced Troubleshooting' section for the device 'FTD4110-2'. The 'Capture w/Trace' tab is selected. An 'Add Capture' button is highlighted with an orange border. The interface includes fields for Auto Refresh Interval (set to 10 seconds) and Enable Auto Refresh.

The screenshot shows the 'Add Capture' dialog box. It includes fields for Name (CAPI), Interface (INSIDE), Protocol (IP), Source Host (192.168.0.10), Destination Host (192.168.2.10), SGT number (0), Buffer Size (524288 bytes), and Trace settings (Continuous Capture or Stop when full). Arrows point from the interface and protocol fields to boxes labeled 'Source interface' and 'IP Protocol'. An arrow points from the buffer size field to a box labeled 'Circular buffer'.

De huidige FMC UI-beperkingen zijn:

- Kan SRC- en DST-poorten niet specificeren
- Alleen standaard IP-protocollen kunnen worden aangepast
- Kan opname voor LINA engine ASP Drops niet inschakelen

### Workaround - Gebruik de FTD CLI

Zodra u een opname van de FMC UI toepast, loopt de opname:

Name	Interface	Type	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status
CAPI	INSIDE	raw-data	<input checked="" type="checkbox"/>	<input type="checkbox"/>	524288	1518	Capturing	IP	192.168.0.10	192.168.2.10	Running

Clear the capture Pause the capture Save the capture in pcap format

De opname op FTD CLI:

```
> show capture
capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

## Traceer een echt pakket op post-6.2 FMC

Op FMC 6.2.x kunt u met de wizard **Capture w/Trace** echte pakketten op FTD opnemen en overtrekken:

Add Capture

Name*: CAPI	Interface*: INSIDE
Match Criteria:	
Protocol*: IP	Source Network: 255.255.255.255
Source Host*: 192.168.16.111	Destination Network: 255.255.255.255
Destination Host*: 192.168.17.1	
<input type="checkbox"/> SGT number: 0 (0-65533)	
Buffer:	
Packet Size: 1518 14-1522 bytes	<input type="radio"/> Continuous Capture
Buffer Size: 524288 1534-33554432 bytes	<input checked="" type="radio"/> Stop when full
	Trace Count: 50

Trace ingress packets

U kunt het overgetrokken pakket controleren in de FMC UI:

## Advanced Troubleshooting

FTD4110-2

The screenshot shows the FTD4110-2 interface with the 'Capture w/Trace' tab selected. A table at the top displays packet details: CAPI, INSIDE, raw-data, Trace checked, Buffer Mode set to N, Buffer Size 524288, Packet Length 1518, Buffer Status Capturing, Protocol IP, Source 192.168.16.111, Destination 192.168.17.1, and Status Running. Below the table, a message indicates 'Packets Shown: 1 / Packets Captured: 1 / Traces: 1'. The main pane shows two sections of log output. The first section, labeled 'The packet is traced', contains logs for Phase 13 (EXTERNAL-INSPECT) and Phase 14 (SNORT). The second section, labeled 'The Snort verdict', contains logs for Snort Trace, Packet (ICMP), AppID (service ICMP (3501)), Firewall (allow rule, 'Default Action'), and NAP/NIPS verdict (PASS). Arrows point from the text labels to the corresponding log entries.

```
Packets Shown: 1 / Packets Captured: 1 / Traces: 1

config.
Additional Information:
New flow created with id 78, packet dispatched to next module

Phase: 13
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: allow rule, 'Default Action', allow
NAP id 1, IPS id 2, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
```

## FTD-programma voor pakkettraceren

### Vereisten

Gebruik het hulpprogramma Packet Tracer voor deze stroom en controleer hoe het pakket intern wordt verwerkt:

Ingress-interface	BINNENKANT
Protocol	ICMP-echoverzoek
Bron-IP	192.168.103.1
Bestemmings-IP	192.168.101.1

### Oplossing

Packet Tracer genereert een **virtueel pakket**. Zoals in dit voorbeeld wordt getoond, wordt het pakket onderworpen aan Snelinspectie. Een opname die tegelijkertijd op Snelniveau (**opname-verkeer**) is genomen, toont het ICMP-echoverzoek:

```
> packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1
```

```
Phase: 1
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list
```

Phase: 2  
Type: ACCESS-LIST  
Subtype:  
Result: ALLOW  
Config:  
Implicit Rule  
Additional Information:  
MAC Access list

Phase: 3  
Type: ROUTE-LOOKUP  
Subtype: Resolve Egress Interface  
Result: ALLOW  
Config:  
Additional Information:  
found next-hop 192.168.101.1 using egress ifc OUTSIDE

Phase: 4  
Type: ACCESS-LIST  
Subtype: log  
Result: ALLOW  
Config:  
access-group CSM\_FW\_ACL\_ global  
access-list CSM\_FW\_ACL\_ advanced permit ip 192.168.103.0 255.255.255.0 192.168.101.0  
255.255.255.0 rule-id 268436482 event-log both  
access-list CSM\_FW\_ACL\_ remark rule-id 268436482: ACCESS POLICY: FTD5515 - Mandatory/1  
access-list CSM\_FW\_ACL\_ remark rule-id 268436482: L4 RULE: Allow ICMP  
**Additional Information:**  
**This packet is sent to snort for additional processing where a verdict is reached**

... output omitted ...

Phase: 12  
Type: FLOW-CREATION  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
New flow created with id 203, packet dispatched to next module

Phase: 13  
Type: SNORT  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
Snort Trace:  
Packet: ICMP  
AppID: service ICMP (3501), application unknown (0)  
Firewall: allow rule, id 268440225, allow  
NAP id 2, IPS id 0, Verdict PASS  
Snort Verdict: (pass-packet) allow this packet

Result: input-interface: INSIDE input-status: up input-line-status: up output-interface: OUTSIDE  
output-status: up output-line-status: up Action: allow >

**De opname op sorteerniveau ten tijde van de pakkettracerest toont het virtuele pakket:**

> **capture-traffic**

Please choose domain to capture traffic from:  
0 - management0  
1 - Router

```
Selection? 1
```

```
Please specify tcpdump options desired.  
(or enter '?' for a list of supported options)  
Options: -n  
13:27:11.939755 IP 192.168.103.1 > 192.168.101.1: ICMP echo request, id 0, seq 0, length 8
```

## Packet Tracer UI Tool in Post-6.2 FMC-softwareversies

In FMC Versie 6.2.x werd de **Packet Tracer** UI-tool geïntroduceerd. Het gereedschap is op dezelfde manier toegankelijk als het opnamegereedschap en u kunt Packet Tracer op FTD uitvoeren vanuit de FMC UI:

The screenshot shows the FMC interface with the following details:

- Header:** Configuration, Users, Domains, Integration, Updates, Licenses ▾, Health ▾ Monitor.
- Section:** Advanced Troubleshooting (FTD4110-2).
- Tab:** Packet Tracer (selected).
- Form Fields:**
  - Packet type: TCP
  - Source\*: IP address (IPv4) 192.168.0.10
  - Destination\*: IP address (IPv4) 192.168.2.10
  - SGT number: SGT number (0-65533)
  - VLAN ID: VLAN ID... (1-4096)
  - Output Format: summary
  - Interface\*: INSIDE
  - Source Port\*: 1111
  - Destination Port\*: http
  - Destination Mac Address: XXXX.XXXX.XXXX
- Buttons:** Start, Clear.
- Output Section:** Phase: 1, Type: CAPTURE, Subtype: ALLOW, Result: ALLOW, Config: Additional Information: MAC Access list.
- Annotations:**
  - A callout box labeled "The source interface" points to the "Interface" dropdown.
  - A callout box labeled "The tracer output" points to the "Output" section.
  - An arrow points from the "Output" section to the "The tracer output" callout box.

## Gerelateerde informatie

- [Naslaghandleiding voor FirePOWER Threat Defense](#)
- [Firepower System release opmerkingen, versie 6.1.0](#)
- [Cisco Firepower Threat Defense Configuration Guide voor Firepower Device Manager, versie 6.1](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)

## 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.