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 pakkettracering 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:

Overview Analysis Pol	icies Device	s Objects	AMP						Deploy	/ 0	System	Help 🔻	mikis v
Access Control > Access Co	ntrol Netwo	k Discovery	Application Det	ectors	Correla	tion	Actions •						
FTD5515												lave	Cancel
Enter a description													
Identity Policy: None			SSL Policy	r: None									
								Te i	Inherita	nce Settin	gs I 📑 P	olicy Assig	poments (1)
Rules Security Intelligence	HTTP Respon	ses Advanc	ed										
# Filter by Device					0	Add Cat	egory 🔾	Add Rule	Sea	rch Rules			х
# Name S	D Source Z Networks	Des	st works	v	U A	. sr	Dest P	u	IS	Action			,
▼ Mandatory - FTD5515- (1-)	ı)												
1 Allow ICMP any	any 🛛 👮 192.14	8.103.0/24 👳	192.168.101.0/24	any	any an	y any	and ICMP (1) any	any	🗸 Allow	V	1	J 🛙
▼ Default - FTD5515 (-)													
There are no rules in this section	n. Add Rule or Add	Category							l	ntrus	ion I	Polic	:y
Default Action						Access	Control: Block	k All Traff	le .				× 🗾

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.

```
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 - brl
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,
seg 1, length 80
12:52:34.749945 IP olab-v1647-gw.cisco.com > olab-v1603-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</pre>
```

Werken met Snort Engine Captures

Vereisten

- 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

Please choose domain to capture traffic from:

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:

```
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:

> capture-traffic

0 - br1 1 - Router

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
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: >

Werken met FTD LINA Engine Captures

Vereisten

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

192.168.103. Bron-IP 1 Bestemmings 192.168.101. -IP 1 Protocol ICMP **BINNENKAN** Interface Т 192.168.103. Bron-IP 1 Bestemmings 192.168.101. -IP 1 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 192.168.1	01.1: bytes=32 time=4ms TTL=255
Reply from 192.168.1	01.1: bytes=32 time=5ms TTL=255
Reply from 192.168.1	01.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1	01.1: 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

```
> show capture CAPI
8 packets captured
1: 17:24:09.122338 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
2: 17:24:09.123071 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
3: 17:24:10.121392 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
4: 17:24:10.122018 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo reply
5: 17:24:11.119714 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
6: 17:24:11.120324 802.10 vlan#1577 P0 192.168.101.1 > 192.168.101.1: icmp: echo reply
7: 17:24:12.133660 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request
8: 17:24:12.134239 802.10 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 packate charm

```
8 packets shown
```

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

Vereisten

Exporteer de opnamen die in het eerdere 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**:

Devices	O bjects	AMP	Deploy) 📀	System	Help 🔻	mikis 🔻
PN Platf	orm Settings						
						Object Ma	nagement
						🔘 New F	Policy
Devic	Device Type		Status		Firepov	ver Setting	s
Threa	Defense		Targeting 1 d	levice	Threat	Defense S	ettings

Specificeer de beleidsnaam en het apparaatdoel:

New Policy		
Name:	FTD5515-System_Policy	
Description:		
Targeted Devices		
Select devices to v	which you want to apply this policy.	
Available Devices		Selected Devices
Search by name	e or value	FTD5515

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

Overview Analysis Policie	Bevices Objects AMP		
Device Management NAT	VPN Platform Settings		
FTD5515-System_Po	blicy		
ARP Inspection	Enable HTTP Server 2		
Banner	Port (Please don't use 80 or		
External Authentication	1443)		
HTTP 1			3 🗿 Add
ICMP	Interface	Network	
Secure Shell SMTP Server	INSIDE	Net_192.168.103.0_24bits	/ 8

Opslaan en implementeren.

Op het tijdstip van de beleidsplanning, kunt u **debug http** inschakelen om het begin van de HTTPservice te zien: 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: <u>https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap</u>.

Opening CAPI.pcap	
 You have chosen to open: CAPLpcap which is: Wireshark capture file (776 bytes) from: https://192.168.103.62 What should Firefox do with this file? Open with Wireshark (default) Save File Do this automatically for files like this from now on. 	
OK Cancel	

Ter referentie:

https://192.168.103.62/capture/CAPI/pcap/C	IP van de FTD-gegevensinterface
API.pcap	waar HTTP-server is ingeschakeld
https://192.168.103.62/capture/CAPI/pcap/C API.pcap	De naam van de FTD-opname
https://192.168.103.62/capture/CAPI/pcap/C	De naam van het bestand dat is
<u>API.pcap</u>	gedownload

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

(192.)	168.103.62/capture/CAPO/pcap/CAPO.pcap	
Opening CAPO.pcap		—
You have chosen to	open:	
CAPO.pcap		
which is: Wire	shark capture file (744 bytes)	
from: https://	192.168.103.62	
What should Firefo	x do with this file?	
Open with	Wireshark (default)	-
© Crue File	The fact (delivery)	
Save File		
Do this <u>a</u> uto	matically for files like this from now on.	
	ОК Са	ancel

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]?

111111

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

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#

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 overtrekpakketten	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:

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	ſ	C:\Use	ers\c	isco>pi	ng 192.1	68.101.1		
Reply from 192.168.101.1: bytes=32 time=2ms ITL=255 Reply from 192.168.101.1: bytes=32 time=2ms ITL=255 Reply from 192.168.101.1: bytes=32 time=2ms ITL=255 Reply from 192.168.101.1: bytes=32 time=8ms ITL=255	þ	Pingin	ng 19	2.168.10	1.1 wit	h 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=8ms TTL=255	ĺ	Reply	from	192.168	3.101.1:	bytes=32	time=2ms	TTL=255
Reply from 192.168.101.1: bytes=32 time=2ms IIL=255 Reply from 192.168.101.1: bytes=32 time=8ms IIL=255	į	Reply	from	192.168	3.101.1:	bytes=32	time=2ms	TTL=255
Reply from 192.168.101.1: bytes=32 time=8ms IIL=255	į	Reply	from	192.168	3.101.1:	bytes=32	time=2ms	TTL=255
	ĺ	Reply	from	192.168	3.101.1:	bytes=32	time=8ns	TTL=255

De opgenomen pakketten zijn:

```
> show capture CAPI28 packets captured

1: 18:08:04.232989 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

2: 18:08:04.234622 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo request

3: 18:08:05.223941 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

4: 18:08:05.224872 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo request

5: 18:08:06.222309 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

6: 18:08:06.223148 802.10 vlan#1577 P0 192.168.101.1 > 192.168.101.1: icmp: echo request

8: 18:08:07.220752 802.10 vlan#1577 P0 192.168.103.1 > 192.168.101.1: icmp: echo request

8: 18:08:07.221561 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo request

8: 18:08:07.221561 802.10 vlan#1577 P0 192.168.101.1 > 192.168.103.1: icmp: echo request

9: neglests above
```

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**.

Overview Analysis	Policies Devices	Objects	s AM	P Inte	lligence				
Device Management	NAT VPN V	os Pl	atform S	ettings	FlexCon	fig	Certificates		
By Group 🗸]								\bigcirc
Name		Group	Model	License	Туре	Acce	ss Control Poli.		
FTD4110-2 10.48.23.254 - C	isco Firepower 4110 Threat	Cisco	Firepower	411(Bas	e, Threat, M	a	ACP1	Ø	6 🔀

Kies Opname toevoegen om een FTD-opname te maken:

Advance FTD4110-2	d Troi	ublesho	oting]							
File Downlo	ad Ti	nreat Defe	nse CLI	Packet	Tracer	Capture	w/Trace				
C Auto Refre	sh Interva	l (seconds):	10	🔲 Enable A	uto Refre	sh					O Add Capture
Na Interface		Туре	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status
Add Capture								? · ×			
Name*:	CAPI			Interface*:	INSI	DE	•	-		Sourc	e interface
Match Criteria:											
Protocol*:	IP		~	←						IP Pro	otocol
Source Host*:	192.168.0	.10		Source Netv	vork: 255.	255.255.255					
Destination Host*:	192.168.2	.10		Destination Network:	255.	255.255.255					
SGT number:	0		((0-65535)						Circu	ar huffer
Buffer:										Oncu	
Packet Size:	1518	14-152	2 bytes	Continue	us Capture	Trace	e				
Buffer Size:	524288	1534-3 bytes	3554432	Stop who	en full	Trace Co	ount: 50				

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:

File Download Threat Defense CLI Packet Tracer		Capture w/Trace			Clear the											
C Auto Refresh Interval (seconds): 10 🛛 Enable Auto Refresh								capture	1		٢	Add C	Captu	re		
Na	Interface	Туре	Trace	Buffer Mode	Buffer Size	Packet Length	Buffer Status	Protocol	Source	Destination	Status					
CAPI	INSIDE	raw-data	~	М	524288	1518	Capturing	IP	192.168.0.10	192.168.2.10	Running	Ø	6	0	11	Ę
											_					Î
									[Pause the capture	Save in po	ə th cap	e c for	ap ma	tur at	e

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*:	Ib			
Source Host*:	192.168.16.111	Source Network:	255.255.255.255	
Destination Host*:	192.168.17.1	Destination Network:	255.255.255.255	
SGT number:	0	(0-65533)		
Buffer:				
Packet Size:	1518 14-1522 bytes	Continuous Cap	ture 🕑 Trace	Trace ingress packets
Buffer Size:	524288 1534-33554432 bytes	Stop when full	Trace Count: 50	

U kunt het overgetrokken pakket controleren in de FMC UI:



FTD-programma voor pakkettracering

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 (opnameverkeer) 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 pakkettracertest 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:

		Configuration	Users	Domains	Integration	Updates	Licenses v	Health > Monitor		
Advanced Tro	oubleshooting									
File Download	Threat Defense CLI	Packet Tracer Ca	apture w	/Trace		ne sou	urce int	erface		
Select the packet	type and supply the packet pa	arameters. Click start to	o trace the	packet.		1				
Packet type:	тср	•			Interface*:	INSIDE		•		
Source*:	IP address (IPv4)	▼ 192.168.0.10			Source Port*:	1111		~		
Destination*:	IP address (IPv4)	▼ 192.168.2.10			Destination Por	t*: http		~		
SGT number:	SGT number. (0-65533)	VLAN ID: VLA	N ID (1-4096)	Destination Ma Address:	cXXXXX.XX	000.0000			
Output Format:	summary	~								
Start	Clear									
< Output				•				Raw		
Phase: 1 Type: CAPTURE										
Subtype: Result: ALLOW	▲	The tracer output								
Additional Informatio MAC Access list	n:									
Dhase 7										

Gerelateerde informatie

- Naslaghandleiding voor FirePOWER Threat Defense
- Firepower System release opmerkingen, versie 6.1.0
- <u>Cisco Firepower Threat Defense Configuration Guide voor Firepower Device Manager, versie</u>
 <u>6.1</u>
- 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.