Verwenden von FirePOWER Threat Defense-Erfassungen und Packet Tracer

Inhalt

Einleitung

In diesem Dokument wird die Verwendung von FirePOWER Threat Defense (FTD)-Erfassungen und Packet Tracer-Dienstprogrammen beschrieben.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

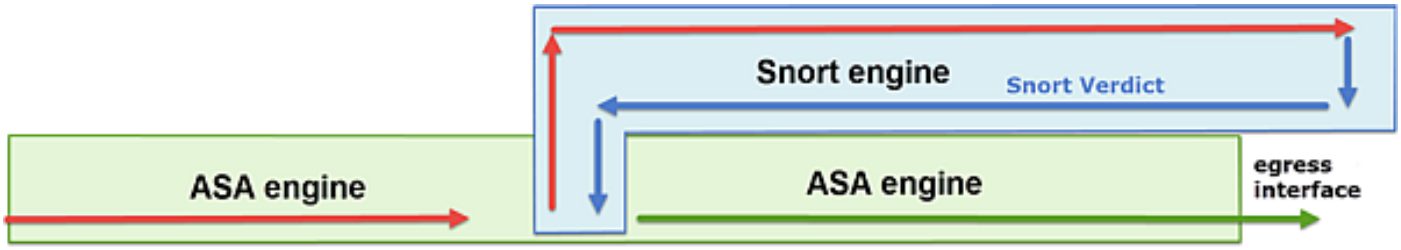
- ASA5515-X mit FTD Software 6.1.0
- FPR4110 mit FTD-Software 6.2.2
- FS4000 mit FirePOWER Management Center (FMC) Software 6.2.2

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 verstehen.

Hintergrundinformationen

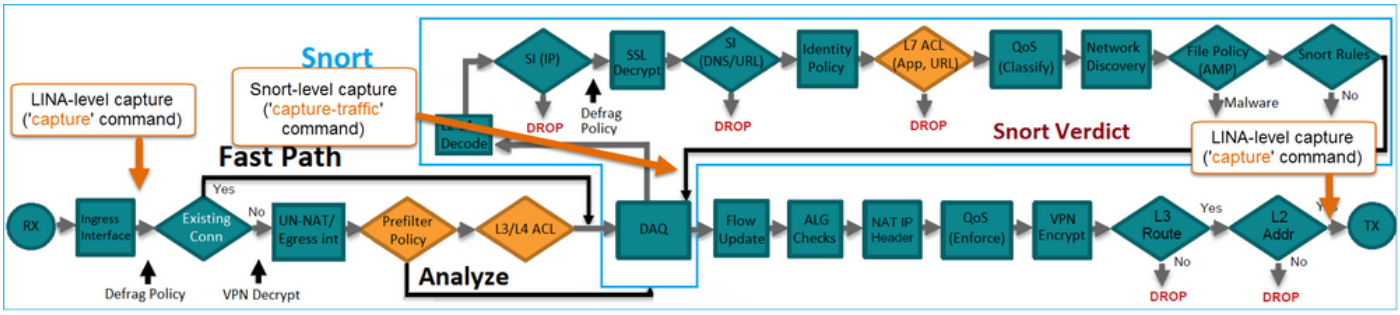
FTD-Paketverarbeitung

Die FTD-Paketverarbeitung wird wie folgt visualisiert:



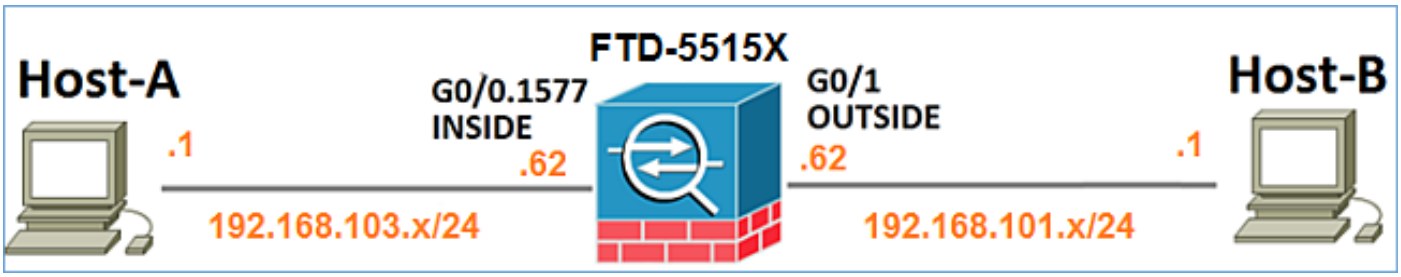
1. Ein Paket gelangt an die Eingangsschnittstelle, und es wird von der LINA-Engine verarbeitet.
2. Wenn die Richtlinie erfordert, dass das Paket von der Snort-Engine geprüft wird.
3. Die Snort-Engine gibt ein Urteil für das Paket zurück.
4. Die LINA-Engine verwirft oder leitet das Paket basierend auf dem Urteil von Snort weiter.

Basierend auf der Architektur können die FTD-Aufnahmen an folgenden Stellen durchgeführt werden:



Konfigurieren

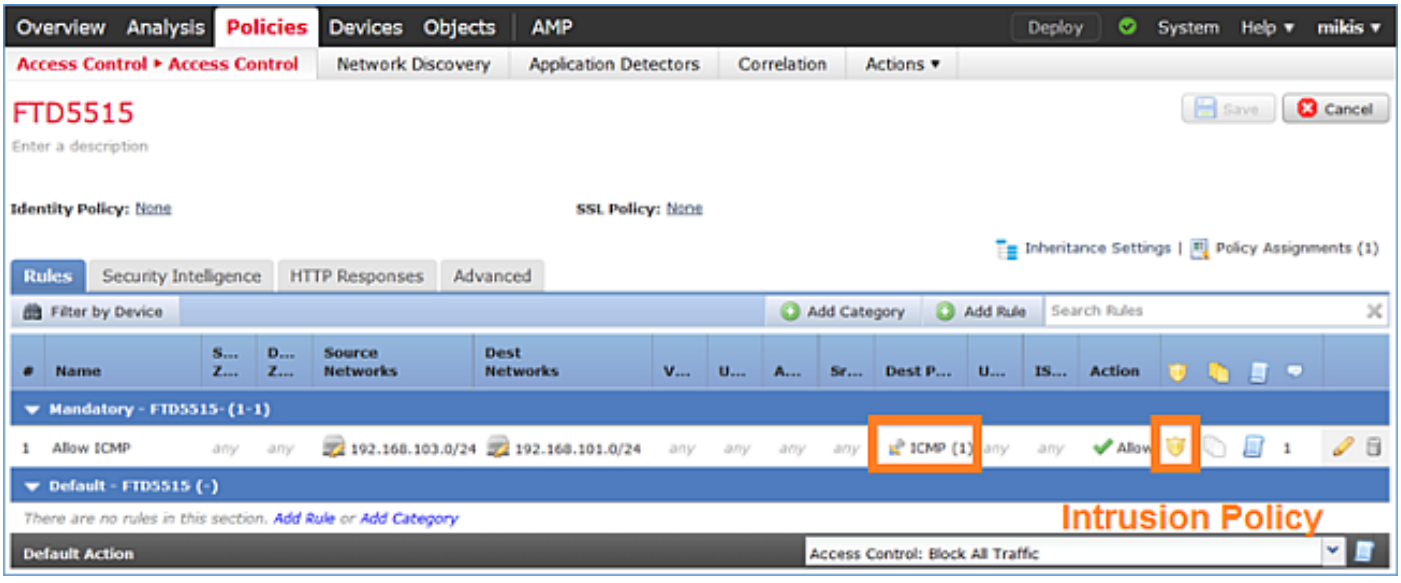
Netzwerkdiagramm



Arbeiten mit Snort Engine Captions

Voraussetzungen

Es gibt eine Zugriffskontrollrichtlinie (Access Control Policy, ACP), die auf FTD angewendet wird und den Durchfluss von Internet Control Message Protocol (ICMP)-Datenverkehr ermöglicht. Auf die Richtlinie wird außerdem eine Intrusion Policy angewendet:



Anforderungen

1. Aktivieren Sie die Erfassung im FTD-CLISH-Modus ohne Filter.
2. Senden Sie einen Ping durch die FTD, und überprüfen Sie die erfasste Ausgabe.

Lösung

Schritt 1: Melden Sie sich bei der FTD-Konsole oder SSH an der br1-Schnittstelle an, und aktivieren Sie die Erfassung im FTD CLISH-Modus ohne 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:
```

Auf FTD 6.0.x lautet der Befehl:

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

Schritt 2: Pingen Sie durch FTD und überprüfen Sie die erfasste Ausgabe.

```
> 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
```

Arbeiten mit Snort Engine Captions

Anforderungen

1. Aktivieren Sie die Erfassung im FTD-CLISH-Modus, indem Sie einen Filter für IP 192.168.101.1 verwenden.
2. Senden Sie einen Ping-Befehl über FTD, und überprüfen Sie die erfasste Ausgabe.

Lösung

Schritt 1: Aktivieren Sie die Erfassung im FTD CLISH-Modus, indem Sie einen Filter für IP 192.168.101.1 verwenden.

```
> 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
```

Schritt 2: Pingen Sie die FTD durch, und überprüfen Sie die erfasste Ausgabe:

```
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
```

Mit der Option **-n** können Sie die Hosts und Portnummern im numerischen Format anzeigen. Die frühere Erfassung wird beispielsweise angezeigt 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
```

Beispiele für TCP-Dump-Filter

Beispiel 1:

Geben Sie den folgenden Befehl ein, um Src IP oder Dst IP = 192.168.101.1 und Src port oder Dst port = TCP/UDP 23 zu erfassen:

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

Beispiel 2:

Geben Sie den folgenden Befehl ein, um Src IP = 192.168.101.1 und Src port = TCP/UDP 23 zu erfassen:

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

Beispiel 3:

Geben Sie den folgenden Befehl ein, um Src IP = 192.168.101.1 und Src port = TCP 23 zu erfassen:

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

Beispiel 4:

Um Src IP = 192.168.101.1 zu erfassen und die MAC-Adresse der Pakete anzuzeigen, fügen Sie die Option "e" hinzu, und geben Sie den folgenden Befehl ein:

```
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
```

Beispiel 5:

Geben Sie den folgenden Befehl ein, um das Programm zu beenden, nachdem Sie 10 Pakete erfasst haben:

```
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
```

Beispiel 6:

Um eine Aufzeichnung in eine Datei mit dem Namen **capture.pcap** zu schreiben und sie über FTP auf einen Remote-Server zu kopieren, geben Sie den folgenden Befehl ein:

```
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.

>
```

Arbeiten mit FTD LINA Engine erfasst

Anforderungen

1. Aktivieren Sie zwei Aufnahmen auf FTD mithilfe der folgenden Filter:

Quell-IP	192.168.103.1
Ziel-IP	192.168.101.1
Protokolle	ICMP
Schnittstelle	INNEN
Quell-IP	192.168.103.1
Ziel-IP	192.168.101.1
Protokolle	ICMP
Schnittstelle	AUSSEN

2. Pingen Sie von Host-A (192.168.103.1) an Host-B (192.168.101.1), und überprüfen Sie die Aufzeichnungen.

Lösung

Schritt 1: Aktivieren Sie die Aufzeichnungen:

```
> 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
```

Schritt 2: Überprüfen Sie die Aufzeichnungen in der CLI.

Ping von Host-A an Host-B:


```
> 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
```

Die beiden Aufnahmen haben aufgrund des Dot1Q-Headers auf der INSIDE-Schnittstelle unterschiedliche Größen, wie in diesem Ausgabebeispiel gezeigt:

```
> 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
```

Arbeiten mit FTD LINA Engine Captures - Exportieren einer Erfassung über HTTP

Anforderungen

Exportieren Sie die im vorherigen Szenario erstellten Aufnahmen mit einem Browser.

Lösung

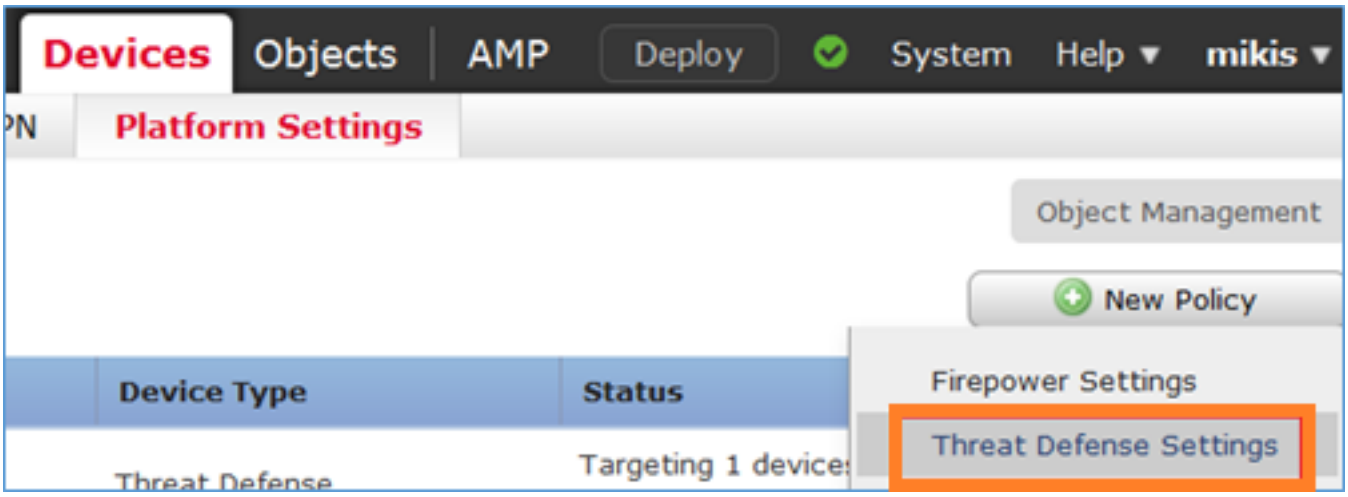
Um die Aufnahmen mit einem Browser zu exportieren, müssen Sie:

1. HTTPS-Server aktivieren
2. HTTPS-Zugriff zulassen

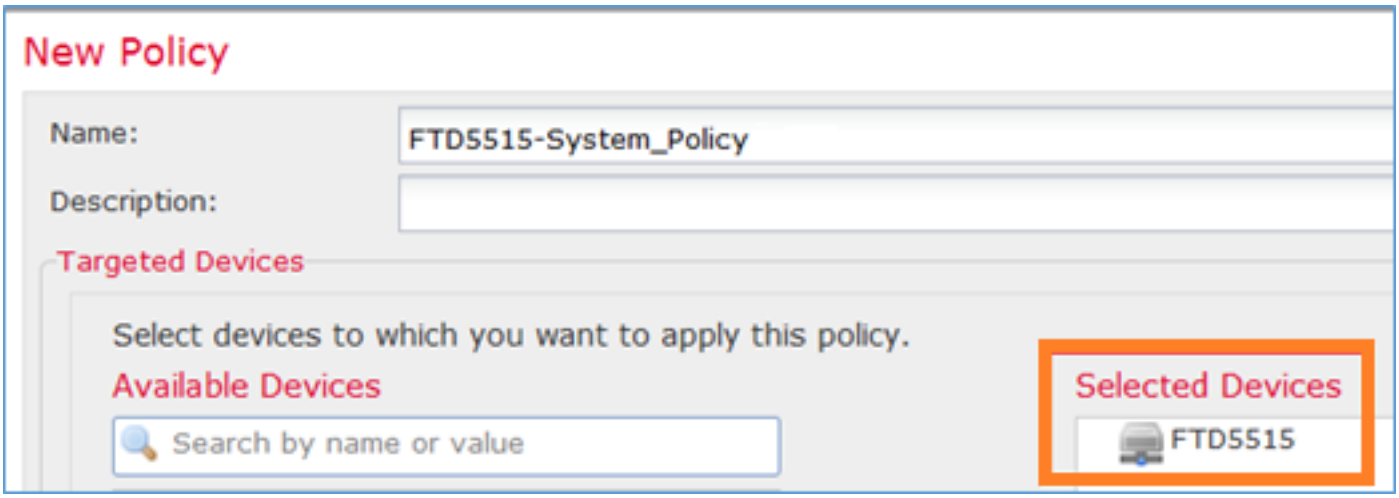
Standardmäßig ist der HTTPS-Server deaktiviert, und es ist kein Zugriff zulässig:

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

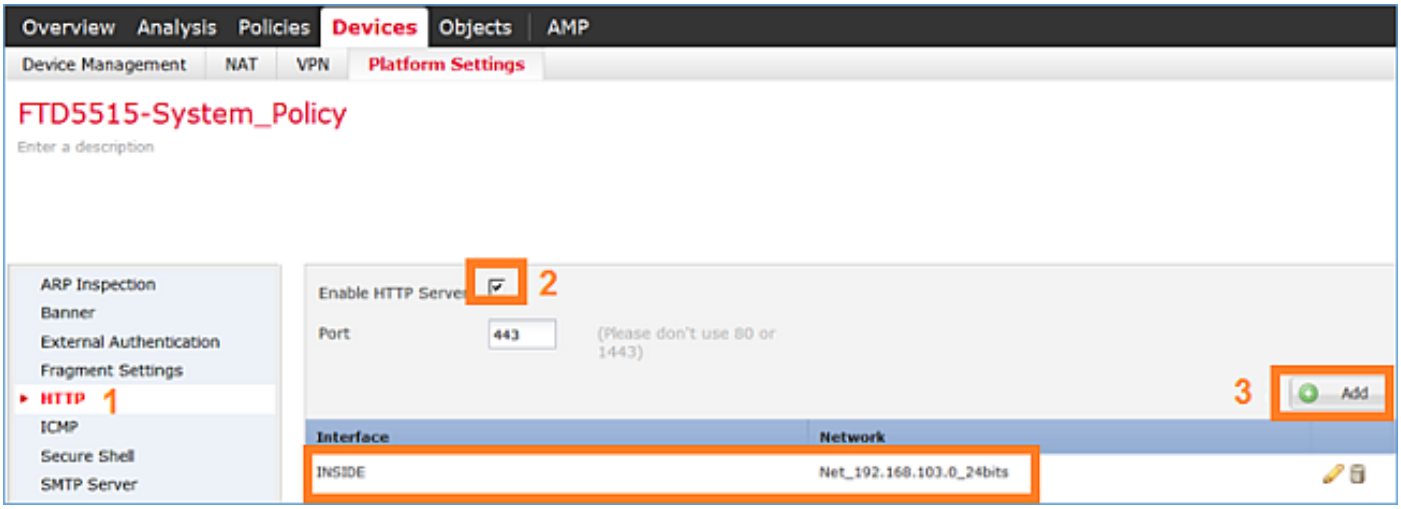
Schritt 1: Navigieren Sie zu **Geräte > Plattformeinstellungen,** klicken Sie auf **Neue Richtlinie**, und wählen Sie **Einstellungen zur Bedrohungsabwehr aus**:



Geben Sie den Richtliniennamen und das Geräteziel an:



Schritt 2: Aktivieren Sie den HTTPS-Server, und fügen Sie das Netzwerk hinzu, dem Sie den Zugriff auf das FTD-Gerät über HTTPS gestatten möchten:



Speichern und **Bereitstellen**.

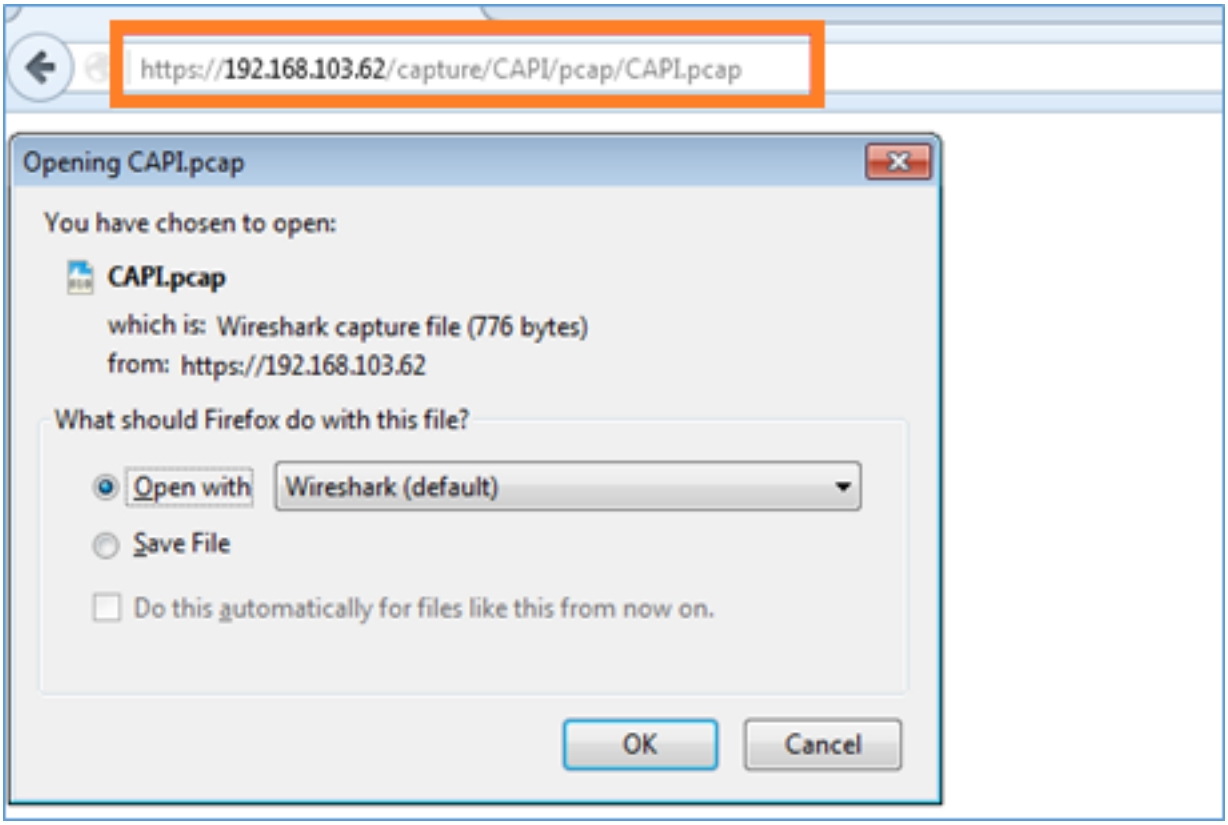
Zum Zeitpunkt der Richtlinienbereitstellung können Sie das **Debuggen von HTTP** aktivieren, um den Start des HTTP-Diensts anzuzeigen:

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

Die FTD-CLI bietet folgende Ergebnisse:

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

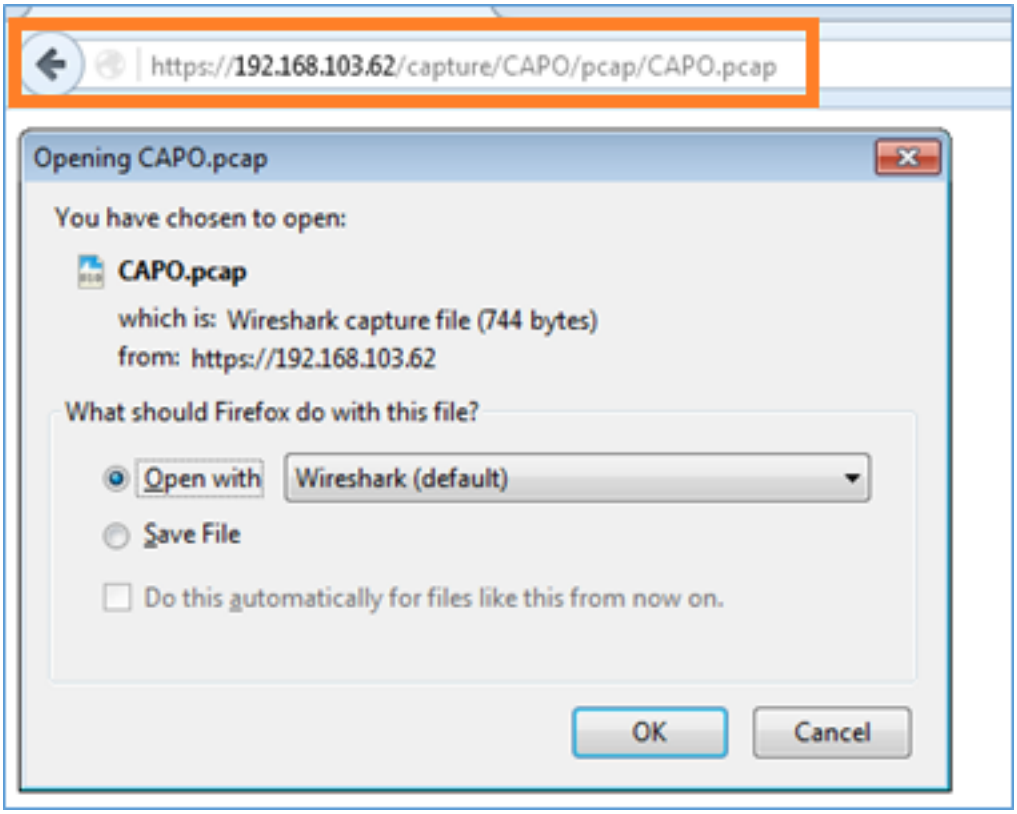
Öffnen Sie einen Browser auf Host-A (192.168.103.1), und verwenden Sie diese URL, um die erste Aufzeichnung herunterzuladen: https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap.



Zur Referenz:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	IP der FTD-Datenschnittstelle, auf der der HTTP-Server aktiviert ist
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	Name der FTD-Erfassung
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	Der Name der heruntergeladenen Datei

Die zweite Aufnahme finden Sie unter https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap.



Arbeiten mit FTD LINA Engine Captures - Exportieren einer Erfassung über FTP/TFTP/SCP

Anforderungen

Exportieren Sie die in früheren Szenarien erstellten Aufnahmen mit FTP/TFTP/SCP-Protokollen.

Lösung

Exportieren einer Erfassung auf einen 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#
```

Exportieren einer Erfassung auf einen 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#
```

Exportieren einer Erfassung auf einen 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 Captures von FTD. Wenn Sie derzeit Captures von FTD entladen müssen, ist die einfachste Methode, folgende Schritte durchzuführen:

1. Aus Lina - kopieren Sie /pcap capture:<cap_name> disk0:

2. Von FPR-Root: mv /ngfw/mnt/disk0/<cap_name> /ngfw/var/common/

3. Von FMC UI - **System > Health > Monitor > Device > Advanced Troubleshooting** und geben Sie die **<cap_name>** in das Feld und download.

Arbeiten mit FTD LINA Engine erfasst - Verfolgen eines echten Datenverkehrspakets

Anforderungen

Aktivieren Sie die Erfassung auf FTD mit folgenden Filtern:

Quell-IP	192.168.103. 1
Ziel-IP	192.168.101. 1
Protokolle	ICMP
Schnittstelle	INNEN
Paketverfolgung	ja
Anzahl der Ablaufverfolgungsp	100

akete

Pingen Sie von Host-A (192.168.103.1) an Host-B (192.168.101.1) und überprüfen Sie die Aufnahmen.

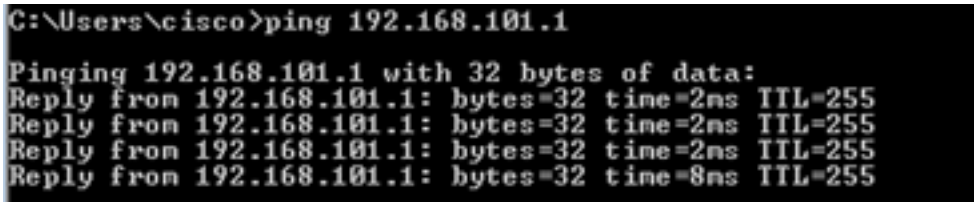
Lösung

Die Verfolgung eines echten Pakets ist sehr nützlich, um Verbindungsprobleme zu beheben. Es ermöglicht Ihnen, alle internen Prüfungen anzuzeigen, die ein Paket durchläuft. Fügen Sie die Schlüsselwörter für die **Ablaufverfolgungsdetails** hinzu, und geben Sie die Anzahl der Pakete an, die nachverfolgt werden sollen. Standardmäßig verfolgt das FTD die ersten 50 eingehenden Pakete.

Aktivieren Sie in diesem Fall die Erfassung mit Ablaufverfolgungsdetails für die ersten 100 Pakete, die FTD über die INSIDE-Schnittstelle empfängt:

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

Ping von Host-A an Host-B und Überprüfung des Ergebnisses:



Folgende Pakete wurden erfasst:

```
> 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
```

Diese Ausgabe zeigt eine Ablaufverfolgung des ersten Pakets an. Die interessanten Bereiche:

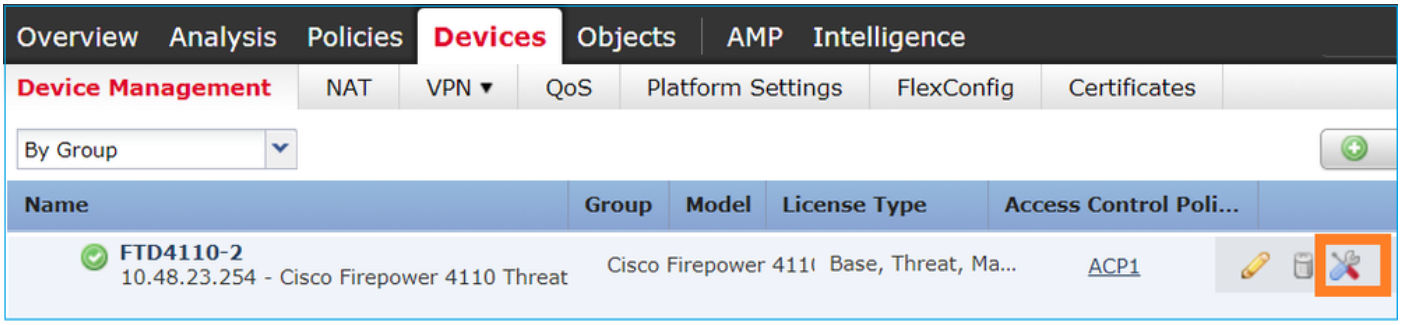
- In Phase 12 wird der "Vorwärtsfluss" angezeigt. Dies ist das LINA-Engine-Dispatch-Array (im Grunde die interne Reihenfolge der Vorgänge).
- Phase 13: FTD sendet das Paket an die Snort-Instanz.
- In Phase 14 wird das Snort-Urteil gefällt.

```
> 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
```

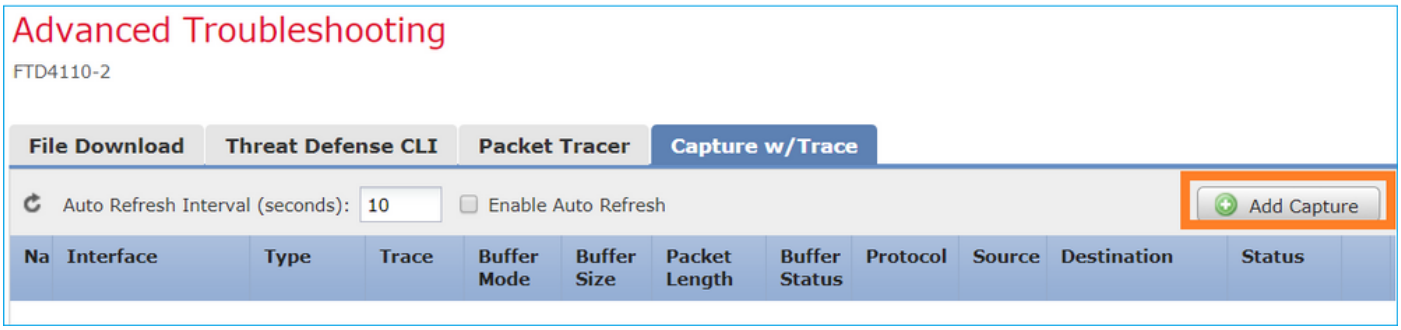
```
... output omitted ...

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
>
```

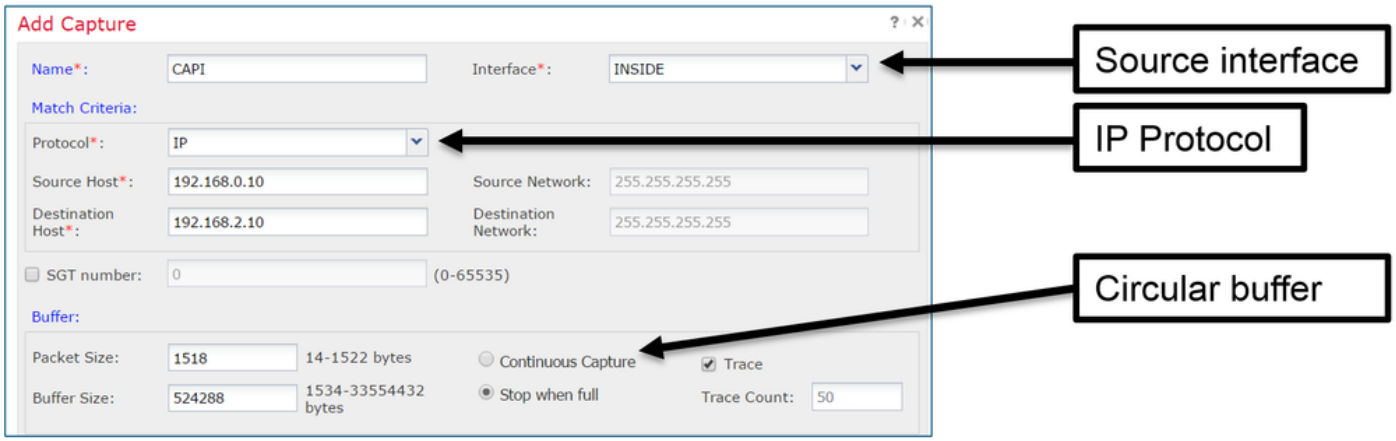
Erfassungstool in Post-6.2 FMC-Softwareversionen

In FMC Version 6.2.x wurde ein neuer Paketerfassungs-Assistent eingeführt. Navigieren Sie zu **Geräte > Geräteverwaltung,** und klicken Sie auf das Symbol **Fehlerbehebung**. Wählen Sie dann **Erweiterte Fehlerbehebung** und schließlich **Erfassung mit Trace**.



Wählen Sie **Erfassung hinzufügen**, um eine FTD-Erfassung zu erstellen:



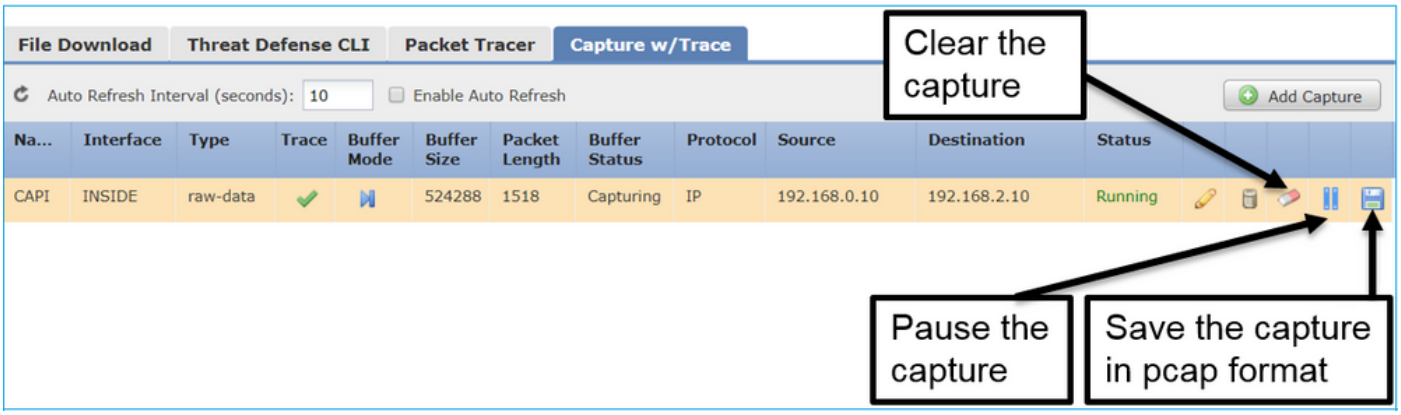


Die aktuellen Einschränkungen der FMC-Benutzeroberfläche sind:

- Src- und Dst-Ports können nicht angegeben werden
- Nur grundlegende IP-Protokolle können zugeordnet werden
- Erfassung für ASP-Drops des LINA-Moduls kann nicht aktiviert werden

Problemumgehung: Verwenden der FTD-CLI

Sobald Sie eine Erfassung von der FMC-Benutzeroberfläche aus anwenden, wird die Erfassung ausgeführt:

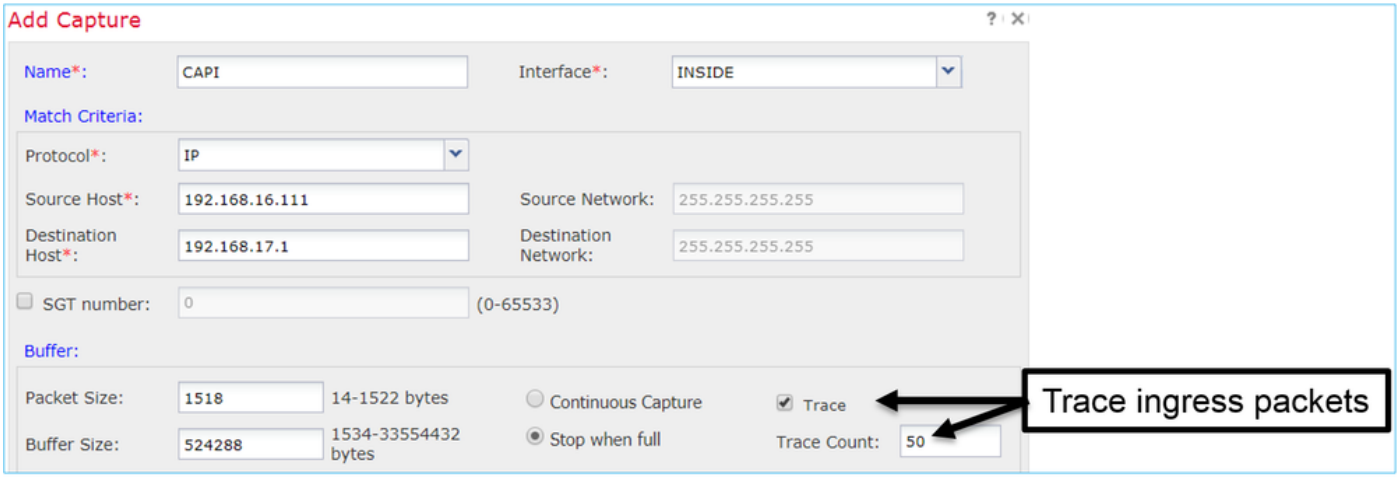


Erfassung auf FTD CLI:

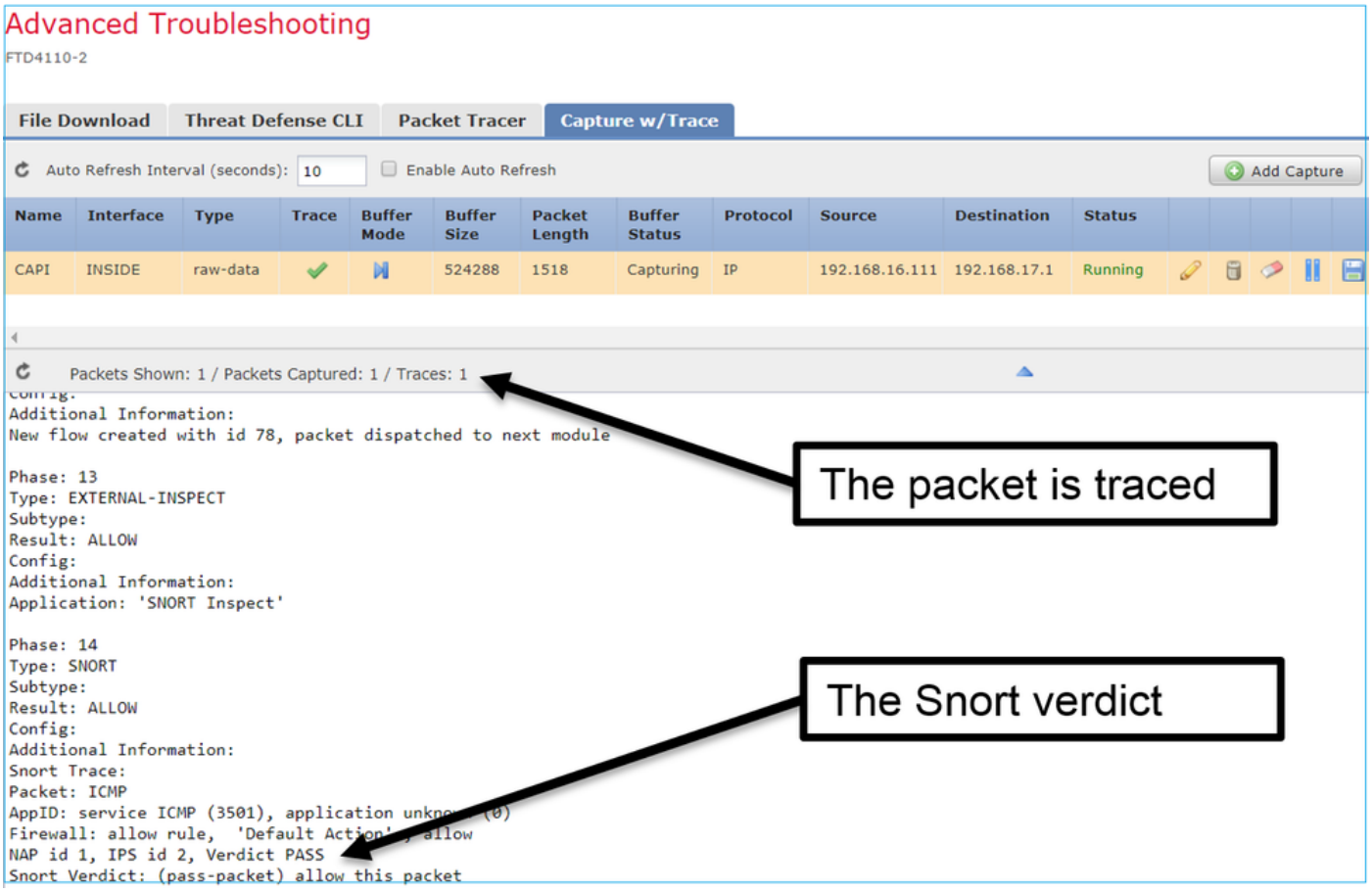
```
> show capture
capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

Verfolgen eines echten Pakets mit Post-6.2 FMC

Auf FMC 6.2.x ermöglicht der **Capture mit Trace**-Assistent das Erfassen und Verfolgen echter Pakete auf FTD:



Sie können das verfolgte Paket in der FMC-Benutzeroberfläche überprüfen:



FTD Packet Tracer-Dienstprogramm

Anforderungen

Verwenden Sie das Packet Tracer-Dienstprogramm für diesen Fluss, und überprüfen Sie, wie das Paket intern verarbeitet wird:

Eingangsschnittstelle	INNEN
Protokolle	ICMP-Echoanfrage
Quell-IP	192.168.103.1
Ziel-IP	192.168.101.1

Lösung

Packet Tracer generiert ein **virtuelles Paket**. Wie in diesem Beispiel gezeigt, wird das Paket einer Snort-Prüfung unterzogen. Eine Erfassung, die gleichzeitig auf Snort-Ebene durchgeführt wird (**Erfassungsverkehr)**, zeigt die ICMP-Echoanfrage an:

```
> 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 >
```

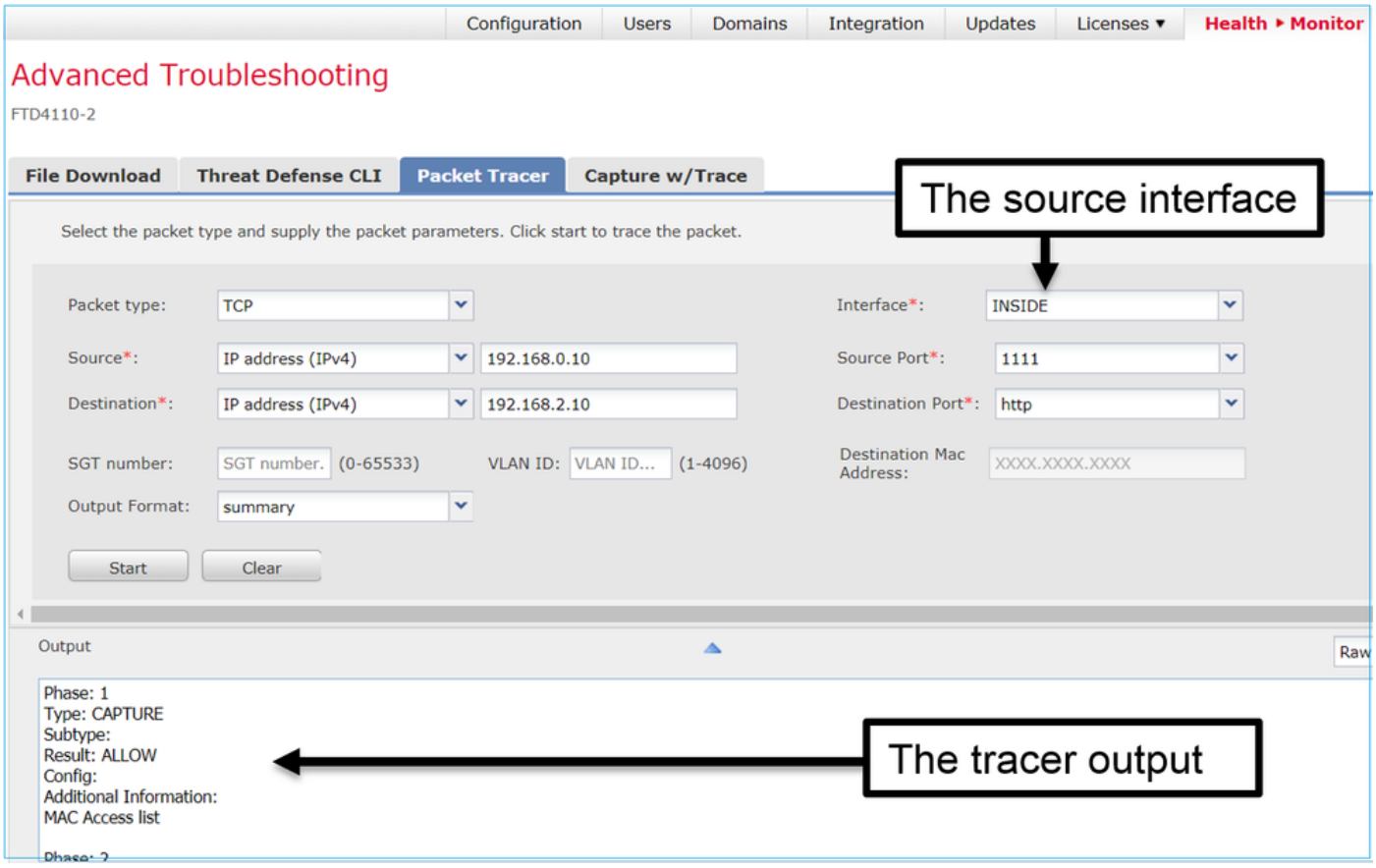
Die Snort-Level-Erfassung zum Zeitpunkt des Packet-Tracer-Tests zeigt das virtuelle Paket:

```
> 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
```

Benutzeroberfläche von Packet Tracer in Post-6.2 FMC-Softwareversionen

In FMC Version 6.2.x wurde das **Packet Tracer** UI Tool vorgestellt. Der Zugriff auf das Tool erfolgt auf die gleiche Weise wie auf das Erfassungstool, und Sie können Packet Tracer auf FTD über die FMC-Benutzeroberfläche ausführen:



Zugehörige Informationen

- Firepower Threat Defense - Referenzhandbuch
- Versionshinweise für FirePOWER-System, Version 6.1.0
- Cisco Firepower Threat Defense - Konfigurationsleitfaden für Firepower Device Manager, Version 6.1
- Technischer Support und Dokumentation für Cisco Systeme

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.