Utilice capturas de Firepower Threat Defence y Packet Tracer

Contenido

Introducción

Este documento describe cómo utilizar capturas de Firepower Threat Defence (FTD) y utilidades de Packet Tracer.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

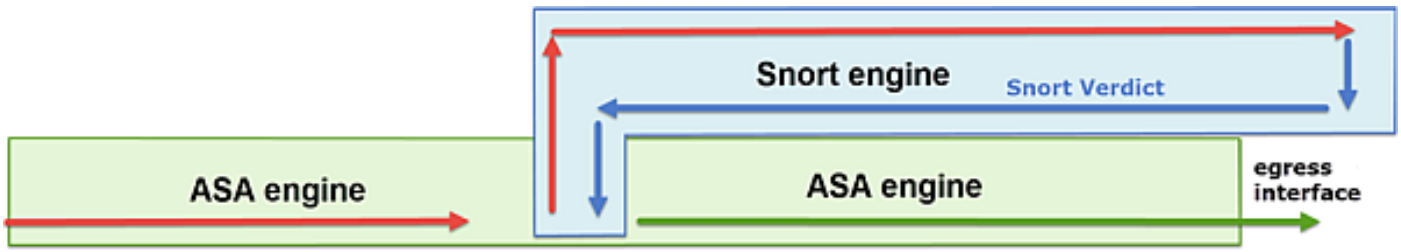
- ASA5515-X que ejecuta el software FTD 6.1.0
- FPR4110 que ejecuta el software FTD 6.2.2
- FS4000 que ejecuta el software Firepower Management Center (FMC) 6.2.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

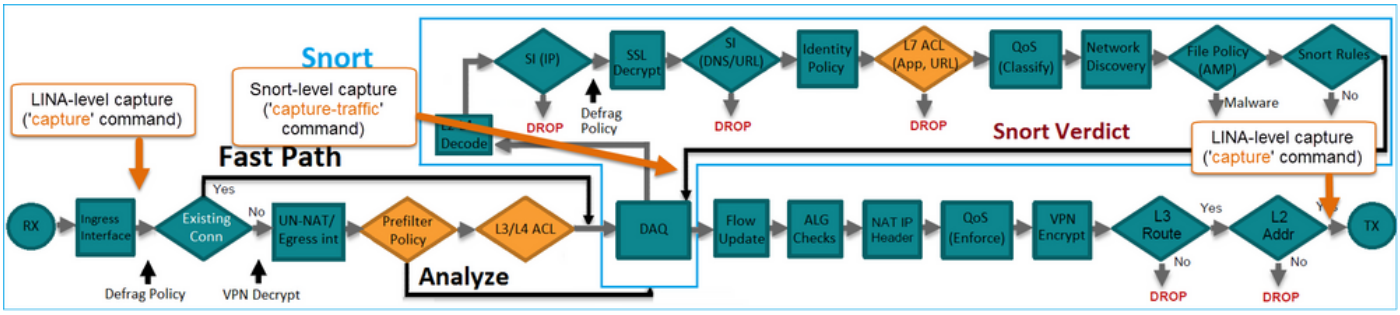
Procesamiento de paquetes FTD

El procesamiento de paquetes FTD se visualiza de la siguiente manera:



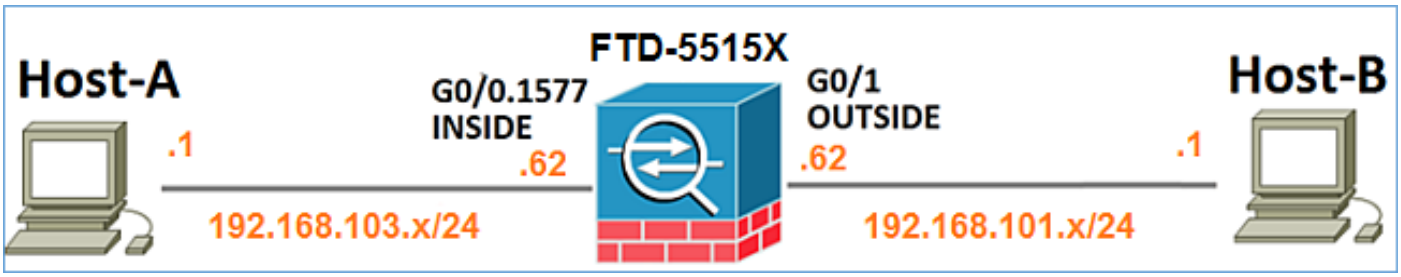
1. Un paquete ingresa a la interfaz de ingreso y es manejado por el motor LINA.
2. Si la política requiere que el motor Snort inspeccione el paquete.
3. El motor Snort devuelve un veredicto para el paquete.
4. El motor LINA descarta o reenvía el paquete en función del veredicto de Snort.

Según la arquitectura, las capturas de FTD se pueden realizar en los siguientes lugares:



Configurar

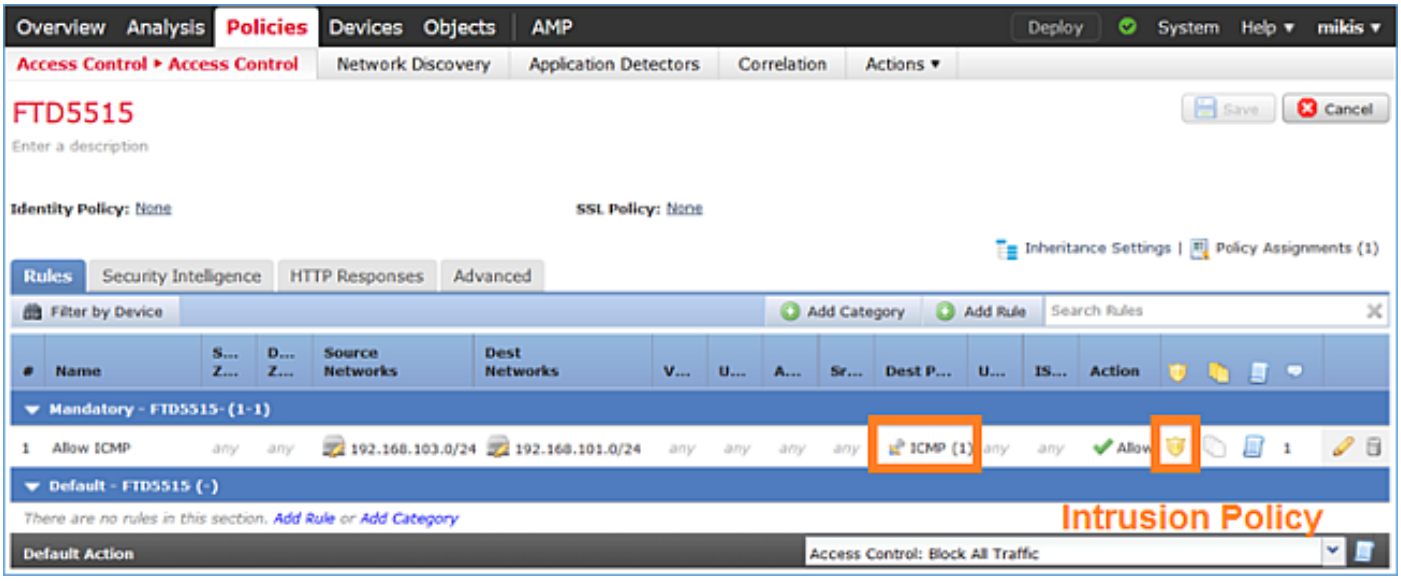
Diagrama de la red



Trabajo con capturas de motores Snort

Prerequisites

Existe una política de control de acceso (ACP) aplicada en FTD que permite el paso del tráfico ICMP (Internet Control Message Protocol). La política también tiene una política de intrusión aplicada:



Requirements

1. Activar la captura en el modo FTD CLISH sin un filtro.
2. Realice un ping del FTD y compruebe el resultado capturado.

Solución

Paso 1. Inicie sesión en la consola FTD o SSH en la interfaz br1 y habilite la captura en el modo FTD CLISH sin un filtro.

```
> 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:
```

En FTD 6.0.x, el comando es:

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

Paso 2. Haga ping a través de FTD y compruebe la salida capturada.

```
> 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-v1603-gw.cisco.com > olab-v1647-gw.cisco.com: ICMP echo request, id 0,
seq 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-v1603-gw.cisco.com > olab-v1647-gw.cisco.com: ICMP echo request, id 0,
seq 2, length 80
12:52:34.759955 IP olab-v1647-gw.cisco.com > olab-v1603-gw.cisco.com: ICMP echo reply, id 0, seq
2, length 80
12:52:34.759955 IP olab-v1603-gw.cisco.com > olab-v1647-gw.cisco.com: ICMP echo request, id 0,
seq 3, length 80
12:52:34.759955 IP olab-v1647-gw.cisco.com > olab-v1603-gw.cisco.com: ICMP echo reply, id 0, seq
3, length 80
12:52:34.759955 IP olab-v1603-gw.cisco.com > olab-v1647-gw.cisco.com: ICMP echo request, id 0,
seq 4, length 80
12:52:34.759955 IP olab-v1647-gw.cisco.com > olab-v1603-gw.cisco.com: ICMP echo reply, id 0, seq
4, length 80
^C<- to exit press CTRL + C
```

Trabajo con capturas de motores Snort

Requirements

1. Habilite la captura en el modo FTD CLISH con el uso de un filtro para IP 192.168.101.1.
2. Haga ping a través de FTD y compruebe la salida capturada.

Solución

Paso 1. Habilite la captura en el modo FTD CLISH con el uso de un filtro para 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
```

Paso 2. Realice un ping a través del FTD y compruebe la salida capturada:

```
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
```

Puede utilizar la opción **-n** para ver los hosts y los números de puerto en formato numérico. Por ejemplo, la captura anterior se muestra como:

```
> 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
```

Ejemplos Del Filtro Tcpdump

Ejemplo 1:

Para capturar IP de origen o IP de destino = 192.168.101.1 y puerto de origen o puerto de destino = TCP/UDP 23, ingrese este comando:

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

Ejemplo 2:

Para capturar Src IP = 192.168.101.1 y Src port = TCP/UDP 23, ingrese este comando:

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

Ejemplo 3:

Para capturar Src IP = 192.168.101.1 y Src port = TCP 23, ingrese este comando:

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

Ejemplo 4:

Para capturar Src IP = 192.168.101.1 y ver la dirección MAC de los paquetes, agregue la opción 'e' e ingrese este comando:

```
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
```

Ejemplo 5:

Para salir después de capturar 10 paquetes, ingrese este comando:

```
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
```

Ejemplo 6:

Para escribir una captura en un archivo con el nombre capture.pcap y copiarlo vía FTP a un servidor remoto, ingrese este comando:

```
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.

>
```

Trabajo con capturas del motor LINA FTD

Requirements

1. Habilitar dos capturas en FTD con el uso de estos filtros:

IP de origen	192.168.103.1
IP de destino	192.168.101.1
Protocolo	ICMP
Interfaz	DENTRO
IP de origen	192.168.103.1
IP de destino	192.168.101.1
Protocolo	ICMP
Interfaz	FUERA

2. Haga ping desde el Host-A (192.168.103.1) al Host-B (192.168.101.1) y compruebe las capturas.

Solución

Paso 1. Habilitar las capturas:

```
> 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
```

Paso 2. Verifique las capturas en la CLI.

Ping del Host A al 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
```

Las dos capturas tienen tamaños diferentes debido al encabezado Dot1Q en la interfaz INSIDE, como se muestra en este ejemplo de salida:

```
> 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
```

Trabajar con capturas del motor LINA de FTD - Exportar una captura a través de HTTP

Requirements

Exporte las capturas realizadas en la situación anterior con un explorador.

Solución

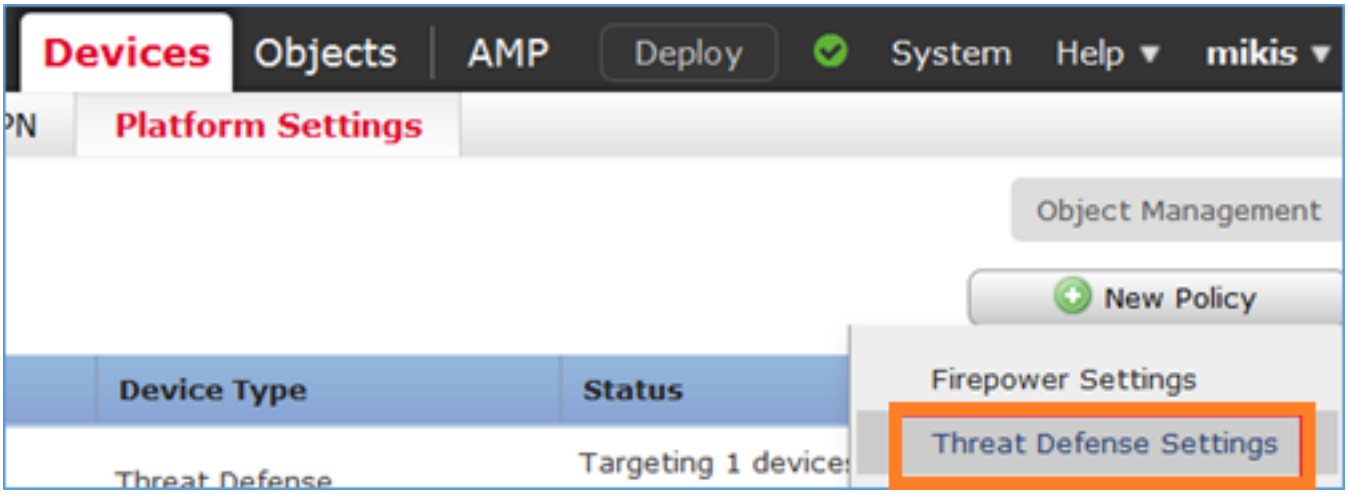
Para exportar las capturas con un navegador, necesita:

1. Activar el servidor HTTPS
2. Permitir acceso HTTPS

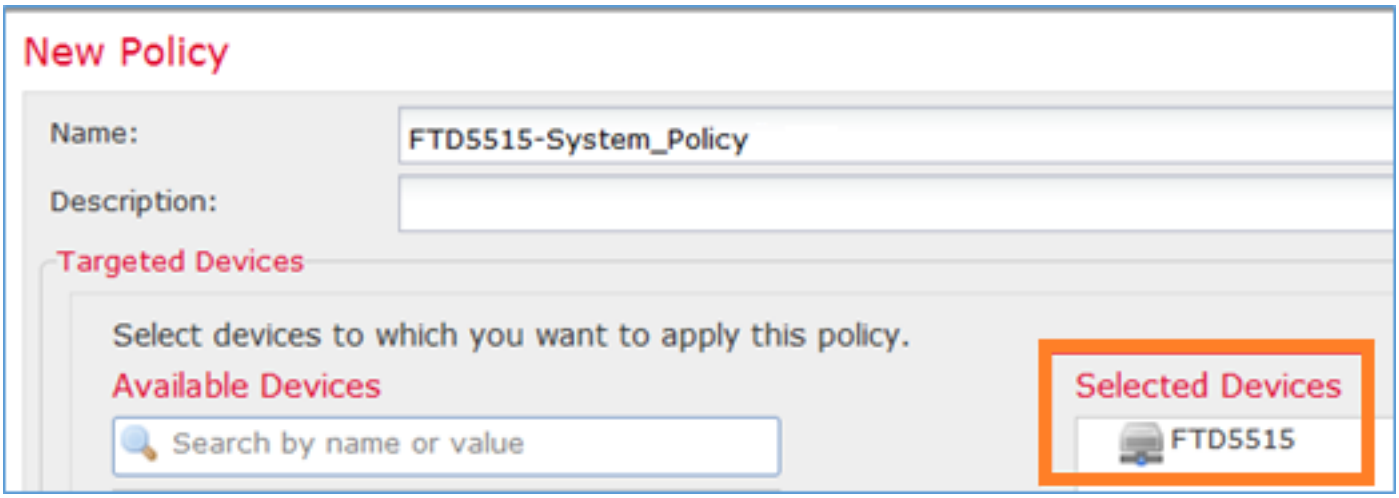
De forma predeterminada, el servidor HTTPS está deshabilitado y no se permite el acceso:

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

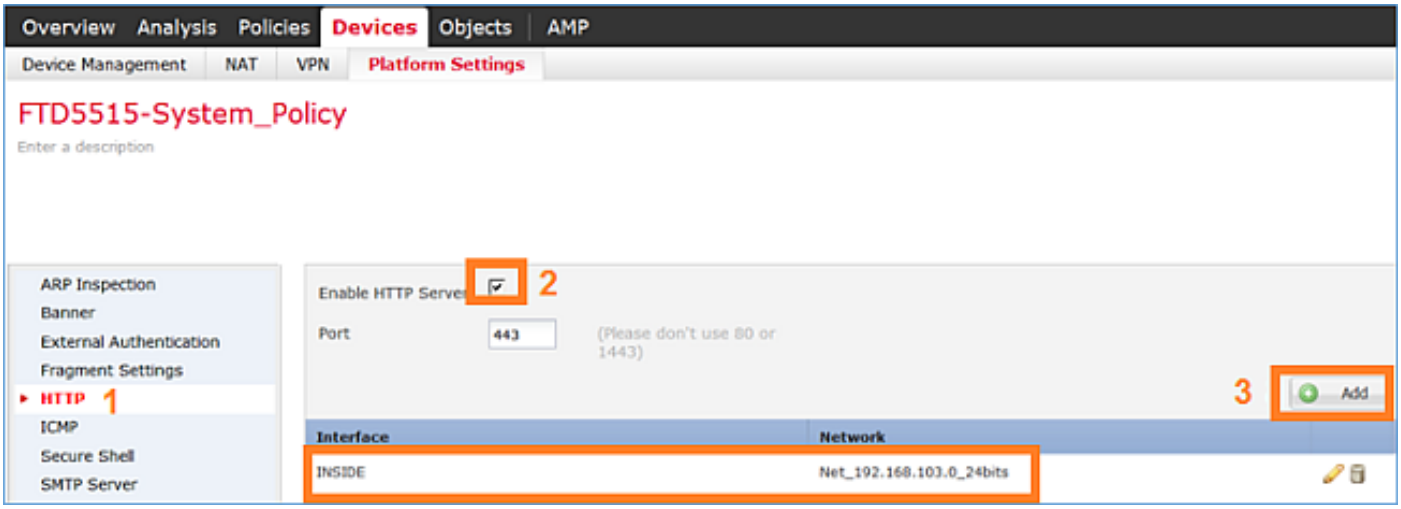
Paso 1. Navegue hasta **Dispositivos > Configuración de la plataforma**, haga clic en **Nueva política** y elija **Configuración de Threat Defence**:



Especifique el nombre de la política y el destino del dispositivo:



Paso 2. Habilite el servidor HTTPS y agregue la red a la que desea que se le permita acceder al dispositivo FTD a través de HTTPS:



Guardar e **implementar**.

En el momento de la implementación de la política, puede habilitar **debug http** para ver el inicio del servicio HTTP:

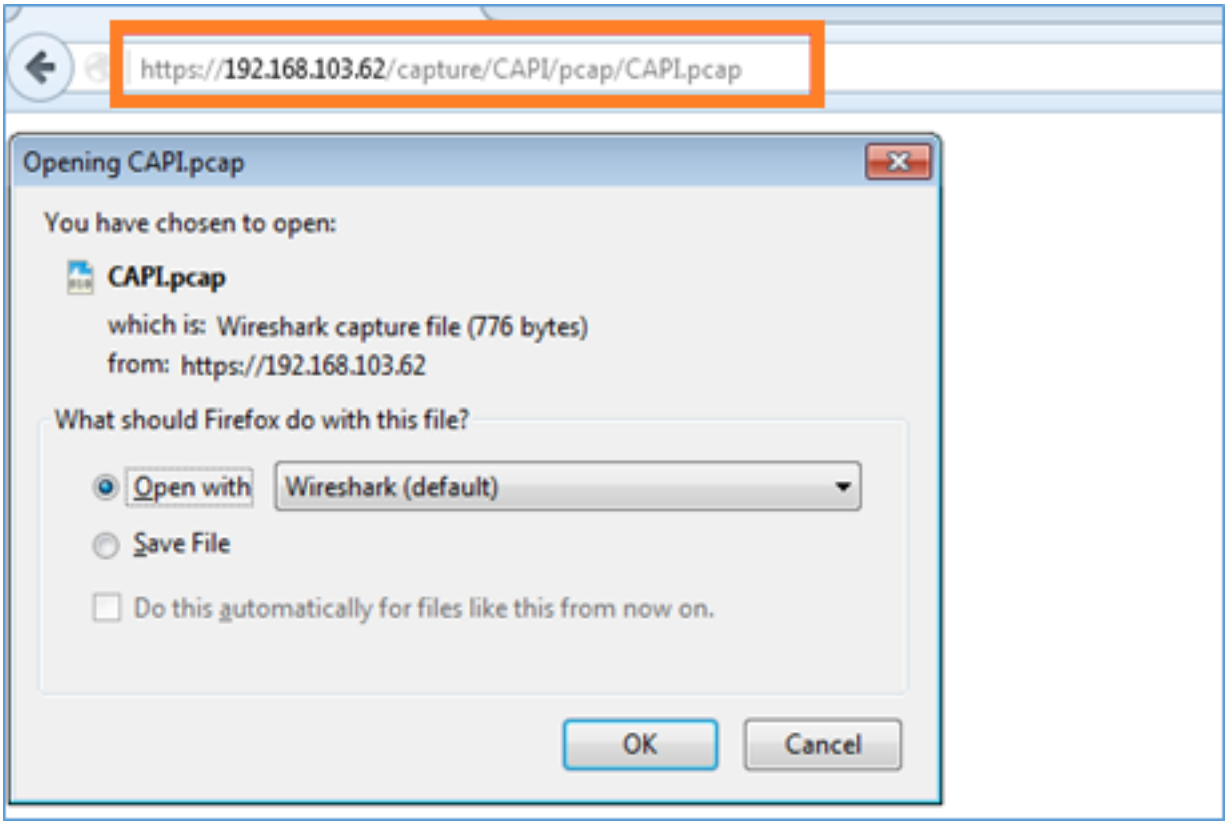
```
> debug http 255
```

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

El resultado en la CLI de FTD es:

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

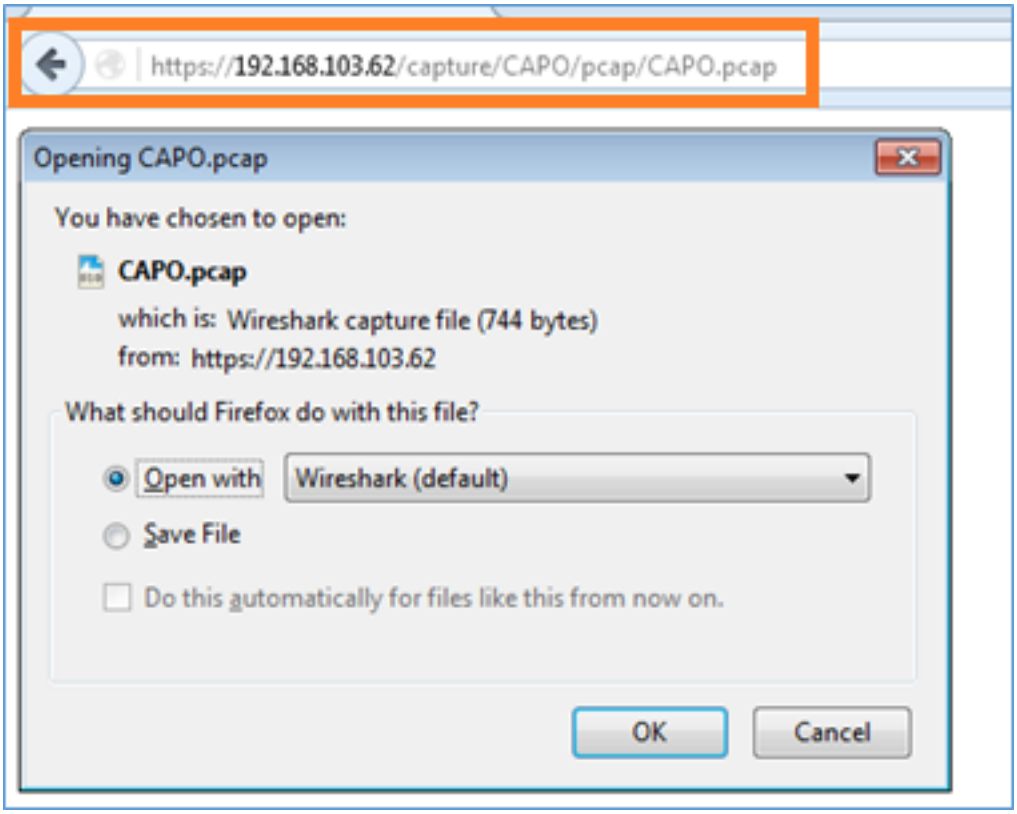
Abra un navegador en Host-A (192.168.103.1) y utilice esta URL para descargar la primera captura: https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap.



Para referencia:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	IP de la interfaz de datos de FTD donde está activado el servidor HTTP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	El nombre de la captura de FTD
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	El nombre del archivo que se descarga

Para la segunda captura, utilice https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap.



Trabajar con capturas del motor LINA FTD - Exportar una captura a través de FTP/TFTP/SCP

Requirements

Exporte las capturas tomadas en los escenarios anteriores con los protocolos FTP/TFTP/SCP.

Solución

Exportar una captura a un servidor FTP:

```
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#
```

Exportar una captura a un servidor TFTP:

```
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#
```

Exportar una captura a un servidor SCP:

```
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#
```

Descargar capturas de FTD. Actualmente, cuando necesita descargar capturas de FTD, el método más sencillo es realizar estos pasos:

1. De Lina - copy /pcap capture:<nombre_cap> disk0:

2. De FPR root - mv /ngfw/mnt/disk0/<nombre_cap> /ngfw/var/common/

3. Desde la interfaz de usuario de FMC - **System > Health > Monitor > Device > Advanced Troubleshooting** e ingrese el campo **<cap_name>** y descargue.

Trabajo con capturas del motor LINA de FTD - Seguimiento de un paquete de tráfico real

Requirements

Habilite una captura en FTD con estos filtros:

IP de origen	192.168.103.1
IP de destino	192.168.101.1
Protocolo	ICMP
Interfaz	DENTRO
Seguimiento de paquetes	sí
Número de	100

paquetes de
seguimiento

Haga ping desde el Host A (192.168.103.1) al Host B (192.168.101.1) y compruebe las capturas.

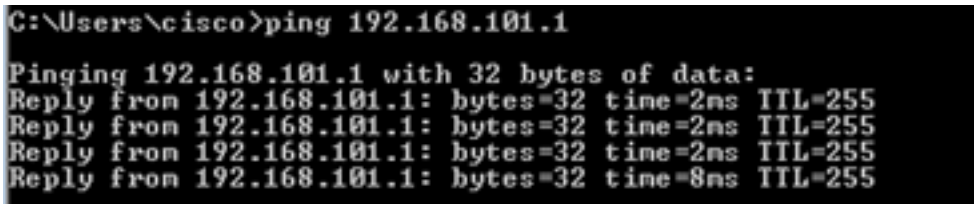
Solución

Rastrear un paquete real es muy útil para resolver problemas de conectividad. Le permite ver todas las comprobaciones internas por las que pasa un paquete. Agregue las palabras clave **trace detail** y especifique el número de paquetes de los que desea realizar un seguimiento. De forma predeterminada, el FTD rastrea los primeros 50 paquetes de ingreso.

En este caso, habilite la captura con detalles de seguimiento para los primeros 100 paquetes que FTD recibe en la interfaz INSIDE:

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

Haga ping desde el Host A al Host B y compruebe el resultado:



Los paquetes capturados son:

```
> 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
```

Este resultado muestra un seguimiento del primer paquete. Las partes que son de interés:

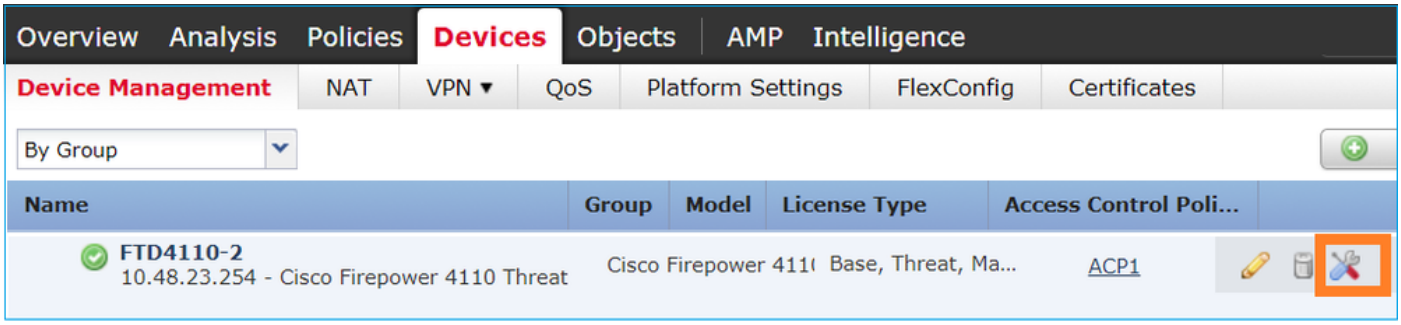
- La fase 12 es donde se ve el 'flujo de avance'. Se trata de la matriz de despacho del motor LINA (que, en la práctica, es el orden interno de las operaciones).
- En la fase 13, FTD envía el paquete a la instancia de Snort.
- En la fase 14 se ve el veredicto de Snort.

```
> 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 ...
```

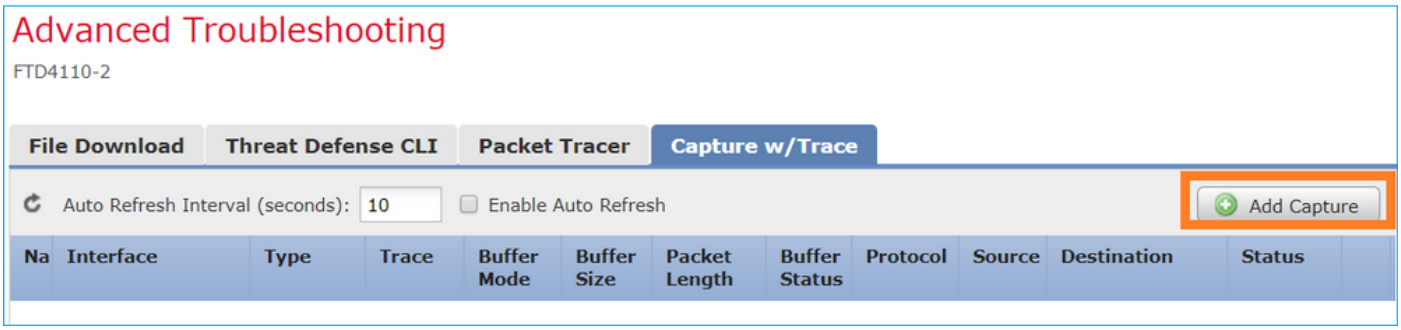
```
Phase: 12
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 195, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_snort
snp_fp_inspect_icmp
snp_fp_adjacency
snp_fp_fragment
snp_ifc_stat

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
>
```

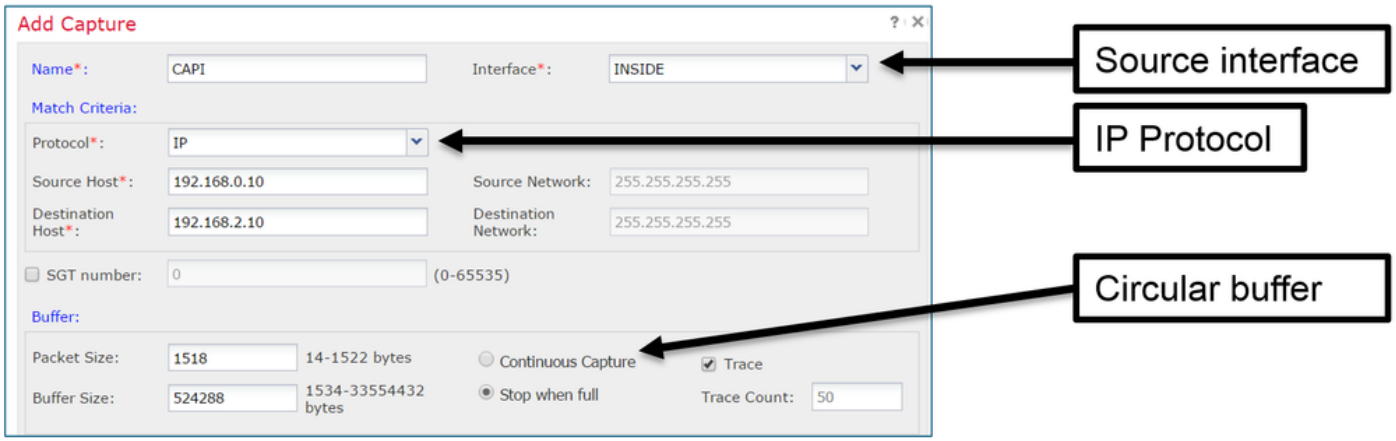
Herramienta de captura en versiones posteriores a la 6.2 de FMC Software

En la versión 6.2.x de FMC, se introdujo un nuevo asistente de captura de paquetes. Navegue hasta **Devices > Device Management** y haga clic en el icono **Troubleshoot**. Luego elija **Solución de problemas avanzada** y finalmente **Capture w/Trace**.



Elija **Agregar Captura** para crear una captura FTD:



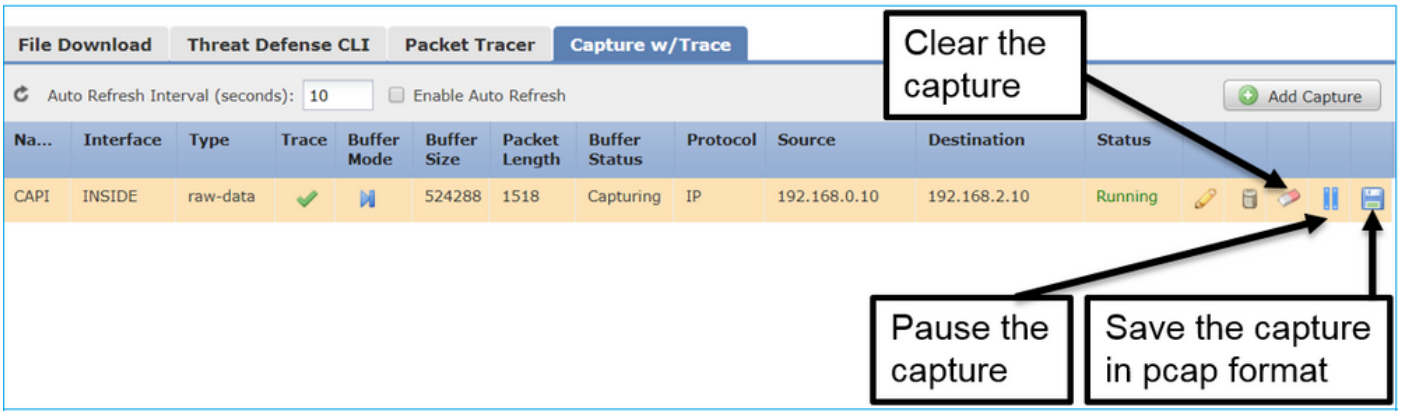


Las limitaciones actuales de la interfaz de usuario de FMC son:

- No se pueden especificar los puertos Src y Dst
- Sólo se pueden encontrar protocolos IP básicos
- No se puede habilitar la captura para ASP Drops del motor LINA

Solución: utilice la CLI de FTD

Tan pronto como aplique una captura desde la interfaz de usuario de FMC, la captura se ejecuta:

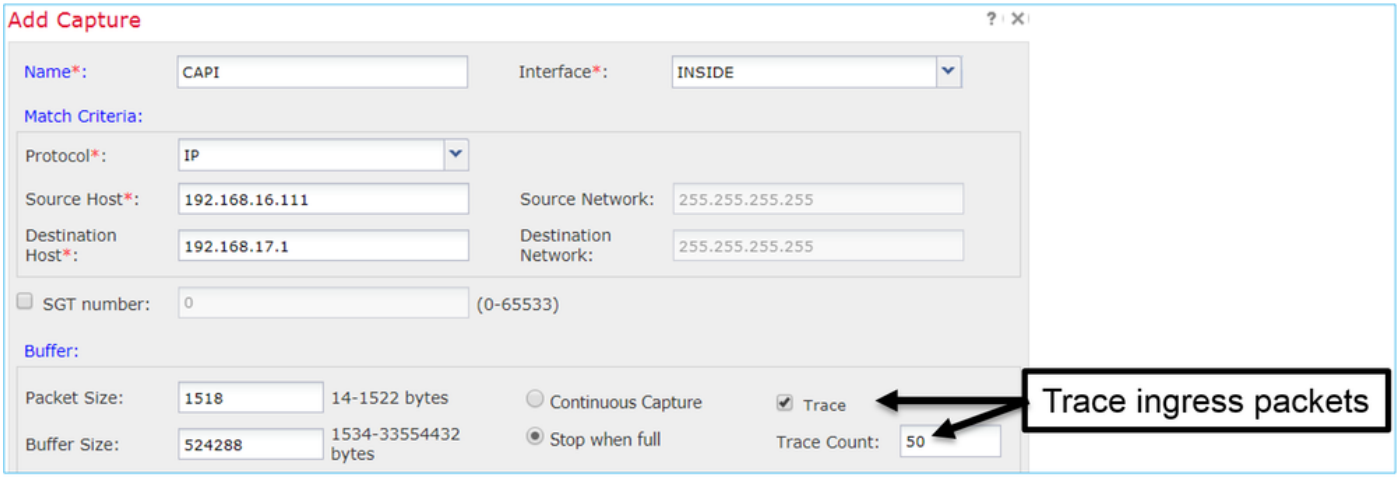


La captura en FTD CLI:

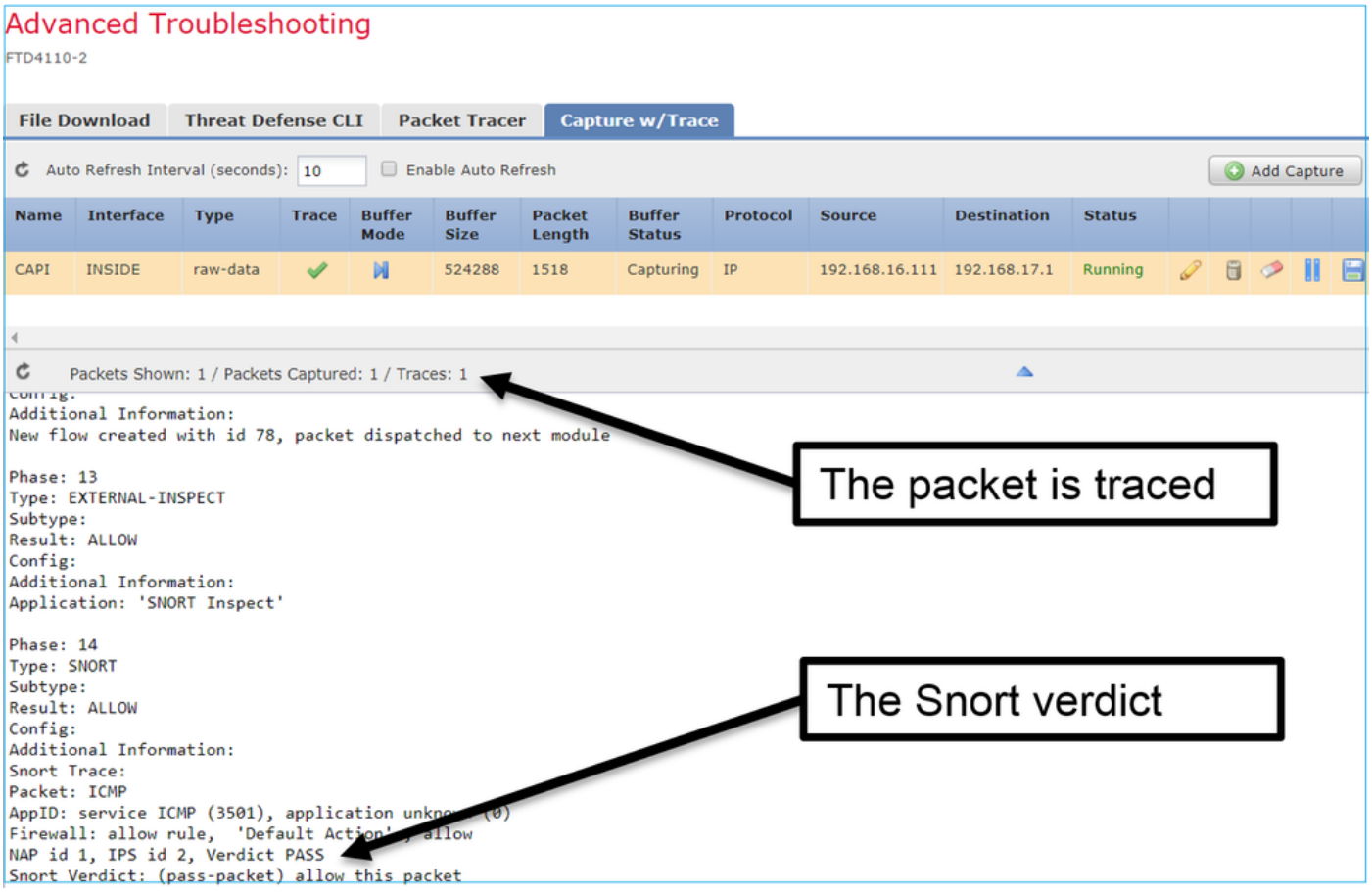
```
> show capture
capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

Seguimiento de un paquete real en FMC posterior a la versión 6.2

En FMC 6.2.x, el asistente **Capture w/Trace** le permite capturar y rastrear paquetes reales en FTD:



Puede verificar el paquete rastreado en la interfaz de usuario de FMC:



Utilidad FTD Packet Tracer

Requirements

Utilice la utilidad Packet Tracer para este flujo y verifique cómo se maneja el paquete internamente:

Interfaz de entrada	DENTRO
Protocolo	solicitud de eco ICMP
IP de origen	192.168.103.1
IP de destino	192.168.101.1

Solución

Packet Tracer genera un **paquete virtual**. Como se muestra en este ejemplo, el paquete está sujeto a la inspección de Snort. Una captura tomada al mismo tiempo en el nivel de Snort (**capture-traffic**) muestra la solicitud de eco ICMP:

```
> 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 >
```

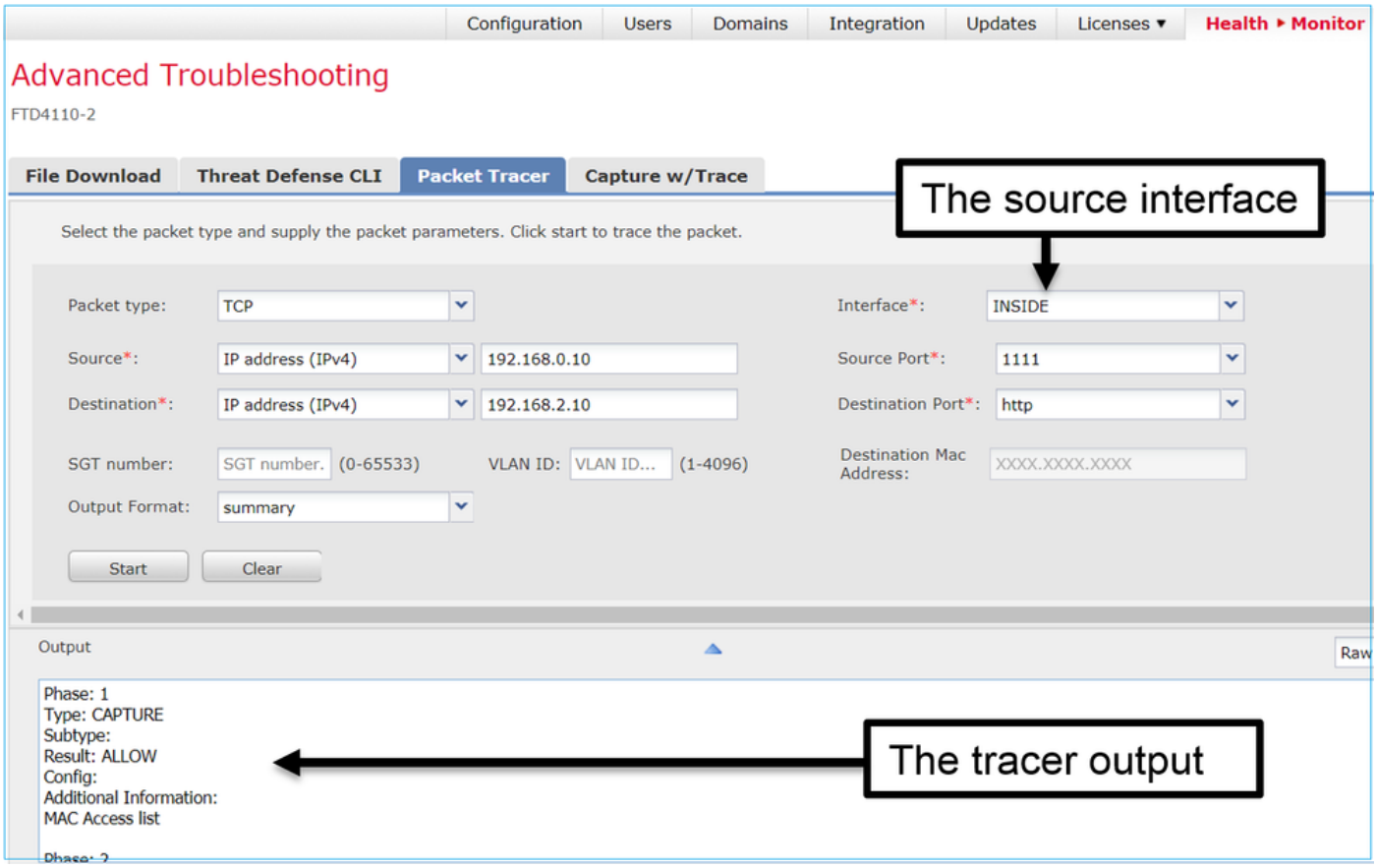
La captura de nivel Snort en el momento de la prueba del rastreador de paquetes muestra el paquete virtual:

```
> 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
```

Herramienta de interfaz de usuario Packet Tracer en versiones de software posteriores a la 6.2 FMC

En la versión 6.2.x de FMC se introdujo la herramienta de interfaz de usuario **Packet Tracer**. La herramienta es accesible de la misma manera que la herramienta de captura y le permite ejecutar Packet Tracer en FTD desde la interfaz de usuario de FMC:



Información Relacionada

- Guía De Referencia Del Comando Firepower Threat Defence
- Notas de la versión del sistema Firepower, versión 6.1.0
- Guía de configuración de Cisco Firepower Threat Defense para Firepower Device Manager, versión 6.1
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).