Trabajo con las capturas y el Paquete-trazalíneas FTD

Contenido

[Introducción](#)
[Componentes usados](#)
[Topología](#)
[Proceso del paquete FTD](#)
[Trabajo con las capturas del Snort-motor](#)
[El trabajo con el Snort-motor captura (con los filtros del tcpdump)](#)
[Ejemplos del filtro del tcpdump](#)
[Trabajo con las capturas del motor FTD ASA](#)
[¿Trabajo con las capturas del motor FTD ASA? Exportación de una captura usando el HTTP](#)
[¿Trabajo con las capturas del motor FTD ASA? Exportación de una captura usando FTP/TFTP/SCP](#)
[¿Trabajo con las capturas del motor FTD ASA? Localizar un paquete](#)
[Usando la utilidad del paquete-trazalíneas FTD](#)
[Documentos Relacionados](#)

Introducción

Este documento describe cómo trabajar con las capturas de la defensa de la amenaza de la potencia de fuego (FTD) y las utilidades del paquete-trazalíneas.

Las capturas de paquetes son una de las herramientas de Troubleshooting más de uso general. Los casos del uso de las capturas de paquetes son:

- Para probar que un paquete llega en el dispositivo
- Para probar que un paquete sale del dispositivo
- Para probar que un paquete es caído por un dispositivo (e.g. ASA EL ASP cae)

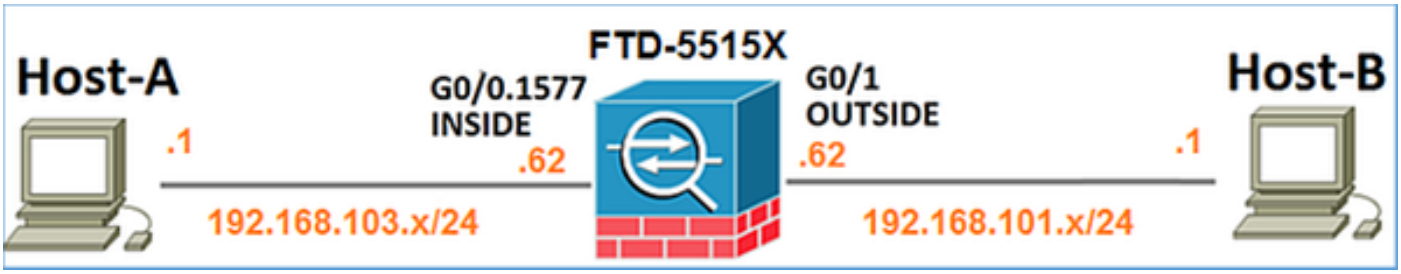
En FTD los paquetes se pueden capturar por dos motores:

1. Motor ASA
2. Motor del Snort

Componentes usados

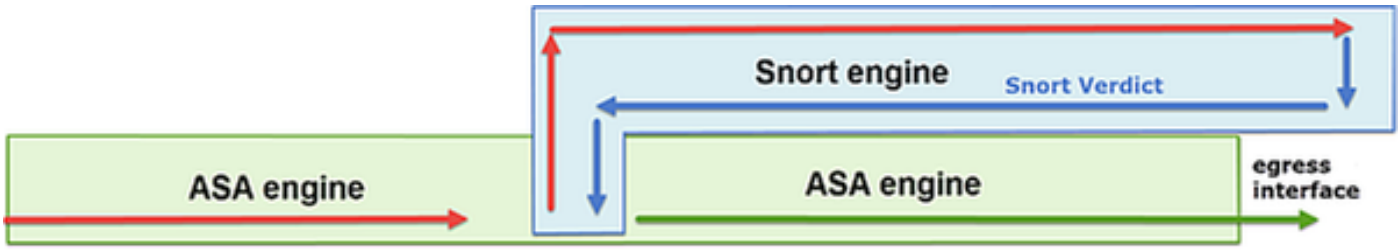
- ASA5515X que funciona con el código 6.1.0 (estructura 330) FTD
- Centro de administración de la potencia de fuego (FMC) que ejecuta 6.1.0 (estructura 330)

Topología



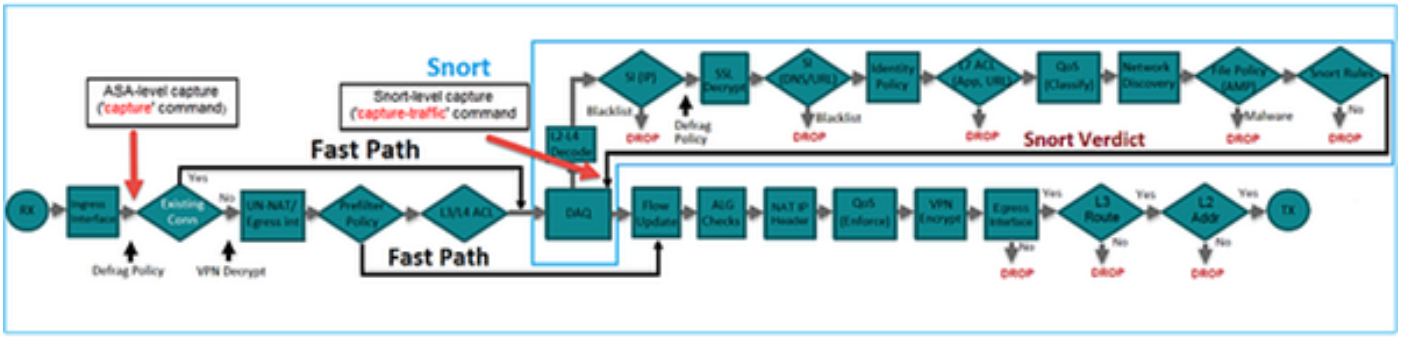
Proceso del paquete FTD

El proceso del paquete FTD puede ser visualizado como sigue:



1. Un paquete ingresa la interfaz de ingreso y es manejado por el motor ASA
2. Si la directiva dicta el paquete es examinado por el motor del Snort
3. El motor del Snort vuelve un veredicto (e.g lista blanca, lista negra) para el paquete
4. ¿Los descensos del motor ASA o adelante el paquete basados en el Snort? veredicto s

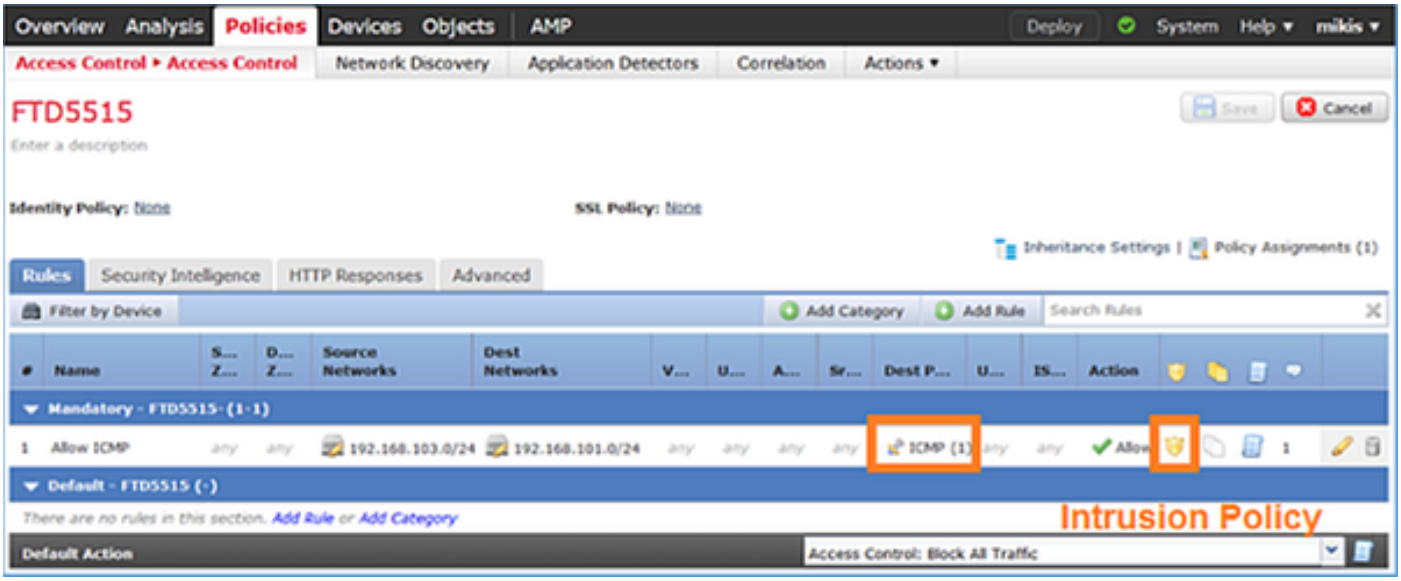
De acuerdo con la arquitectura antedicha las capturas FTD se pueden adquirir 2 diversos lugares:



Trabajo con las capturas del Snort-motor

Prerrequisitos

Hay una directiva del control de acceso (ACP) aplicada en FTD que permita que vaya el tráfico ICMP a través. La directiva tiene también una directiva de la intrusión aplicada:



Requisitos

1. Captura del permiso en el modo FTD CLISH usando ningún filtro
2. Haga ping con el FTD y marque la salida de la captura

Solución

Paso 1: Inicie sesión a la consola o a SSH FTD a la interfaz br1 y habilite la captura en el modo FTD CLISH usando ningún filtro

```
> capture-trafficPlease choose domain to capture traffic from: 0 - br1 1 - RouterSelection?
1Please 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 con el FTD y marque la salida de la captura

```
> capture-trafficPlease choose domain to capture traffic from: 0 - br1 1 - RouterSelection?
1Please 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 8012:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-
gw.cisco.com: ICMP echo reply, id 0, seq 1, length 8012:52:34.759955 IP olab-vl603-gw.cisco.com
> olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 2, length 8012:52:34.759955 IP olab-
vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 2, length
8012:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,
seq 3, length 8012:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo
reply, id 0, seq 3, length 8012:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-
gw.cisco.com: ICMP echo request, id 0, seq 4, length 8012:52:34.759955 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
```

El trabajo con el Snort-motor captura (con los filtros del tcpdump)

Requisitos

1. Habilite la captura en el modo FTD CLISH usando un filtro para IP 192.168.101.1
2. Haga ping con el FTD y marque la salida de la captura

Solución

Paso 1: Habilite la captura en el modo FTD CLISH usando un filtro para IP 192.168.101.1

```
> capture-trafficPlease choose domain to capture traffic from: 0 - br1 1 - RouterSelection?
1Please specify tcpdump options desired.(or enter '?' for a list of supported options)Options:
host 192.168.101.1
```

Paso 2: Haga ping con el FTD y marque la captura hecha salir:

```
13:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq
0, length 8013:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo
reply, id 3, seq 1, length 8013:28:36.079982 IP olab-vl647-gw.cisco.com > olab-vl603-
gw.cisco.com: ICMP echo reply, id 3, seq 2, length 8013:28:36.079982 IP olab-vl647-gw.cisco.com
> olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 3, length 8013:28:36.079982 IP olab-vl647-
gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 3, seq 4, length 80
```

¿Usted puede utilizar? ¿- n? opción para ver los host y los números del puerto en el formato numérico. Por ejemplo la captura antedicha será mostrada como:

```
> capture-trafficPlease choose domain to capture traffic from: 0 - br1 1 - RouterSelection?
1Please specify tcpdump options desired.(or enter '?' for a list of supported options)Options: -
n host 192.168.101.113:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq
0, length 8013:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 1,
length 8013:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 2, length
8013:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 3, length
8013:29:59.599959 IP 192.168.101.1 > 192.168.103.1: ICMP echo reply, id 5, seq 4, length 80
```

Ejemplos del filtro del tcpdump

Ejemplo 1

Para capturar el puerto IP o del dst IP= 192.168.101.1 y del src del src o el puerto del dst = TCP/UDP 23:

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

Ejemplo 2

Para capturar el puerto del src IP= 192.168.101.1 y del src = TCP/UDP 23:

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

Ejemplo 3

Para capturar el puerto del src IP= 192.168.101.1 y del src = TCP 23:

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

Ejemplo 4

Para capturar el src IP= 192.168.101.1 y ver la dirección MAC de los paquetes agregar la opción "e":

```
Options: -ne src 192.168.101.117:57:48.709954 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:

```
Options: -n -c 10 src 192.168.101.118:03:12.749945 IP 192.168.101.1.23 > 192.168.103.1.27287:
Flags [.], ack 3758037348, win 32768, length 018:03:12.749945 IP 192.168.101.1.23 >
192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 218:03:12.949932 IP 192.168.101.1.23 >
192.168.103.1.27287: Flags [P.], ack 1, win 32768, length 1018:03:13.249971 IP 192.168.101.1.23
> 192.168.103.1.27287: Flags [.], ack 3, win 32768, length 018:03:13.249971 IP 192.168.101.1.23
> 192.168.103.1.27287: Flags [P.], ack 3, win 32768, length 218:03:13.279969 IP 192.168.101.1.23
> 192.168.103.1.27287: Flags [.], ack 5, win 32768, length 018:03:13.279969 IP 192.168.101.1.23
> 192.168.103.1.27287: Flags [P.], ack 5, win 32768, length 1018:03:13.309966 IP
192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 7, win 32768, length 018:03:13.309966 IP
192.168.101.1.23 > 192.168.103.1.27287: Flags [P.], ack 7, win 32768, length 1218:03:13.349972
IP 192.168.101.1.23 > 192.168.103.1.27287: Flags [.], ack 9, win 32768, length 0
```

Ejemplo 6

Para escribir una captura a un archivo con el nombre capture.pcap y copiarla vía el FTP al servidor remoto:

```
Options: -w capture.pcap host 192.168.101.1CTRL + C <- to stop the capture> system file copy
10.229.22.136 ftp / capture.pcapEnter password for ftp@10.229.22.136:Copying capture.pcapCopy
successful.>
```

Trabajo con las capturas del motor FTD ASA

Requisitos

1. Permiso 2 capturas en FTD usando los filtros siguientes:

IP de la fuente	192.168.103.1
IP de destino	192.168.101.1
Protocolo	ICMP
Interfaz	DENTRO
IP de la fuente	192.168.103.1
IP de destino	192.168.101.1
Protocolo	ICMP

Interfaz FUERA

2. Haga ping del Host-a (192.168.103.1) el Host-b (192.168.101.1) y marque las capturas.

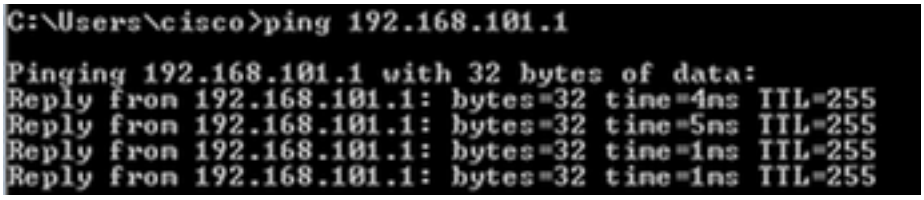
Solución

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: Marcar las capturas usando el CLI

Ping del Host-a al Host-b:




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

Las 2 capturas tienen diversos tamaños debido a la encabezado del dot1q en la interfaz interior. Esto se puede mostrar en el producto siguiente:

```
> show capture CAPI8 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 reply8 packets shown > show capture CAPO8 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 reply8 packets shown
```

¿Trabajo con las capturas del motor FTD ASA? Exportación de una captura usando el HTTP

Requisitos

Exporte las capturas admitidas el escenario previó usando un navegador

Solución

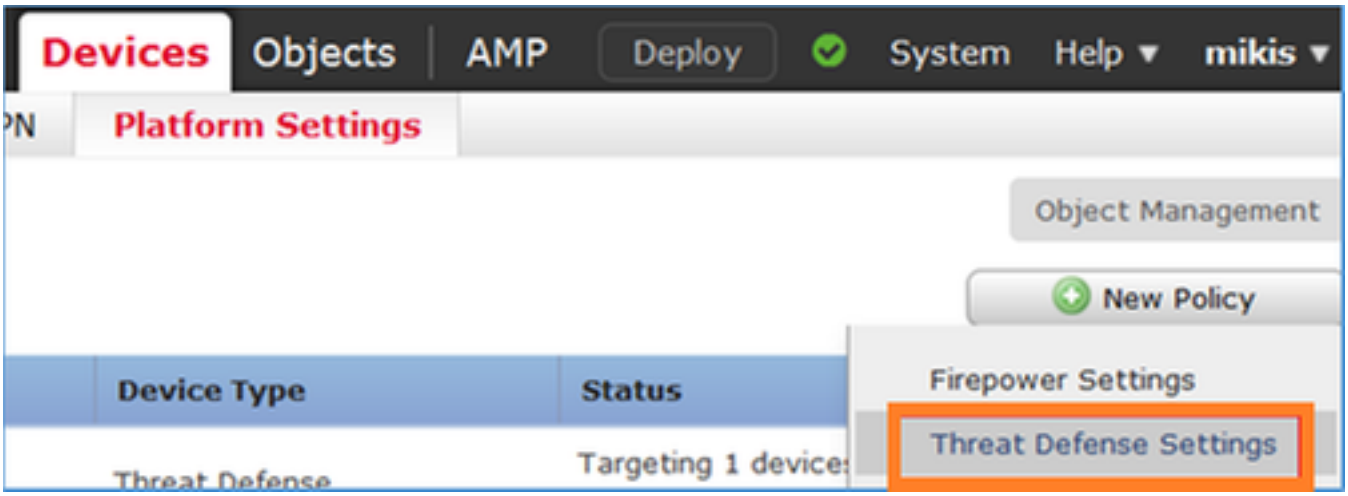
Para exportar las capturas usando el navegador allí es necesidad:

1. Servidor HTTPS del permiso
2. Permita el acceso HTTPS

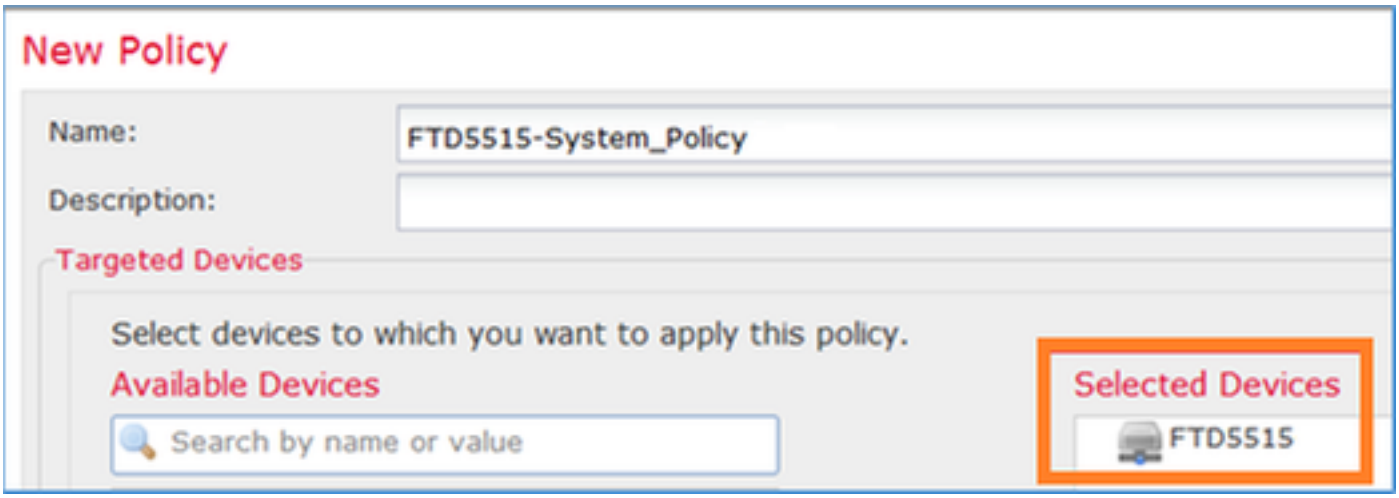
Por abandono inhabilitan al servidor HTTPS y no se permite ningún acceso:

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

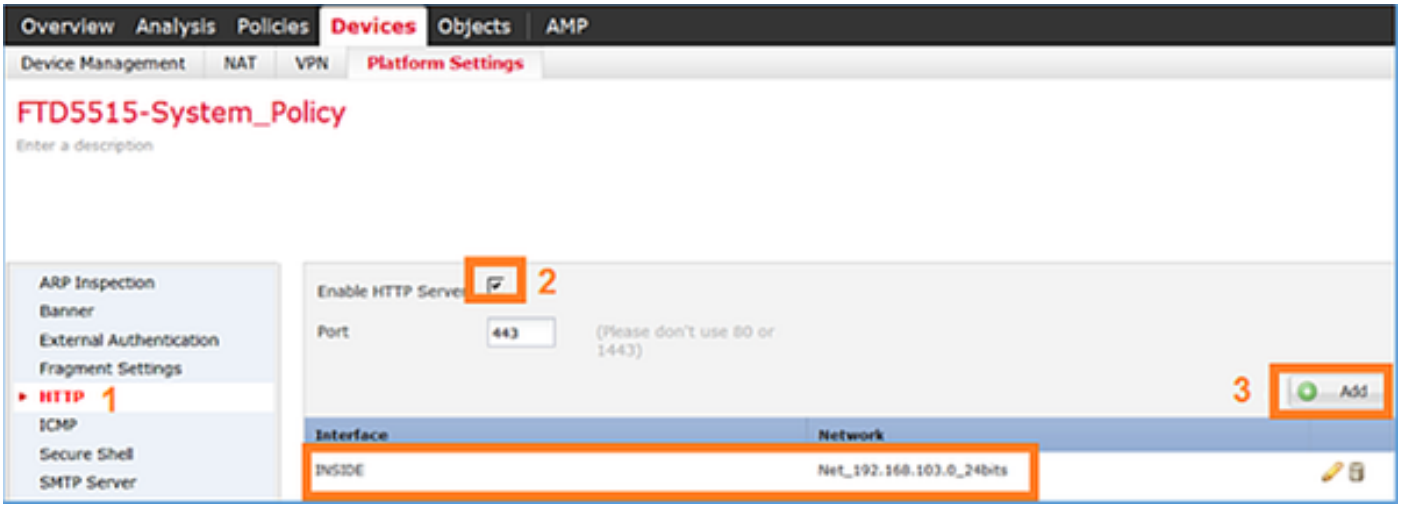
Paso 1: Navegue a los **dispositivos > a las configuraciones de la plataforma,** haga clic en la **nueva directiva** y seleccione las **configuraciones de la defensa de la amenaza:**



Especifique el nombre y el dispositivo de destino de la directiva:



Paso 2: Habilite al servidor HTTPS y agregue la red que se debe permitir acceder el dispositivo FTD sobre el HTTPS:



Salve y despliegue

Recomendación

Mientras que usted está desplegando la directiva usted puede permitir al **HTTP del debug** para ver comenzar del servicio HTTP:

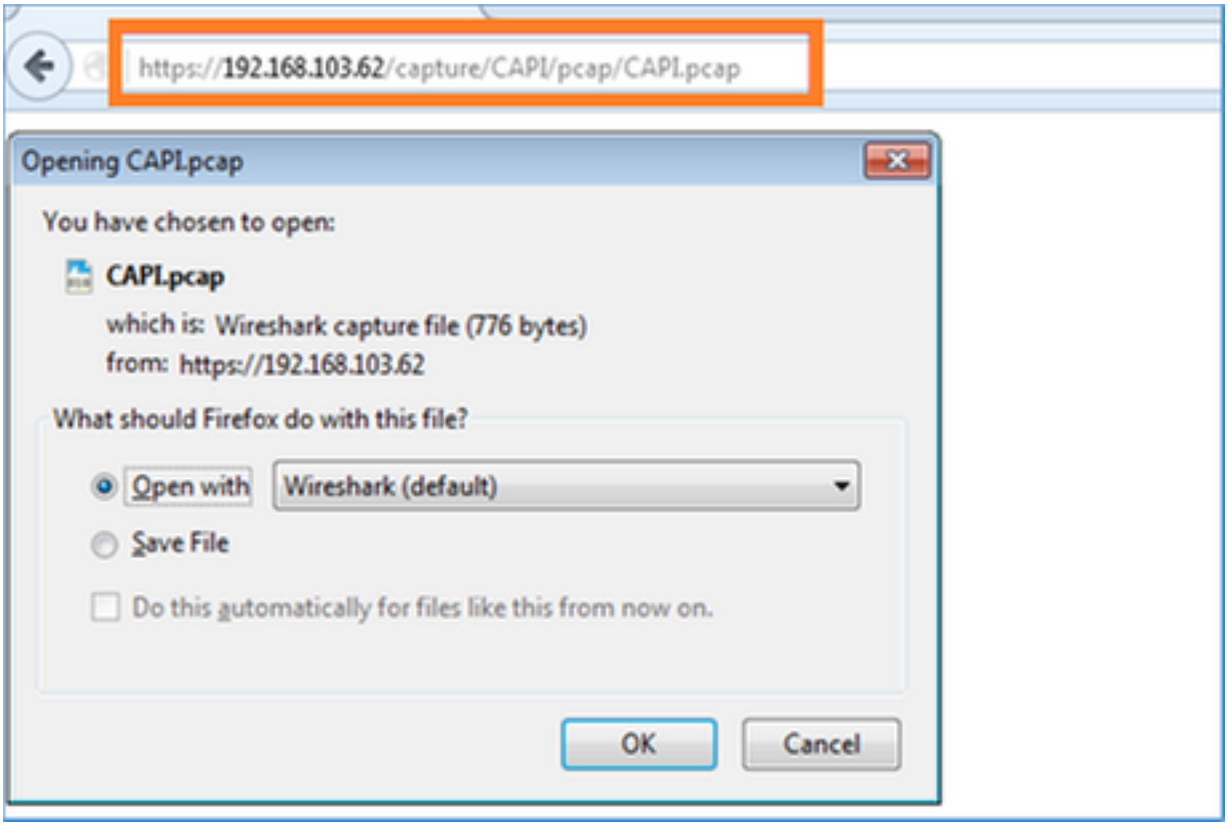
```
> debug http 255debug http enabled at level 255.http_enable: Enabling HTTP serverHTTP server starting.
```

Aquí está el resultado en FTD CLI:

```
> unebug all> show run httphttp server enablehttp 192.168.103.0 255.255.255.0 INSIDE
```

Abra a un navegador en el Host-a (192.168.103.1) y utilice el URL siguiente para descargar la primera captura:

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap

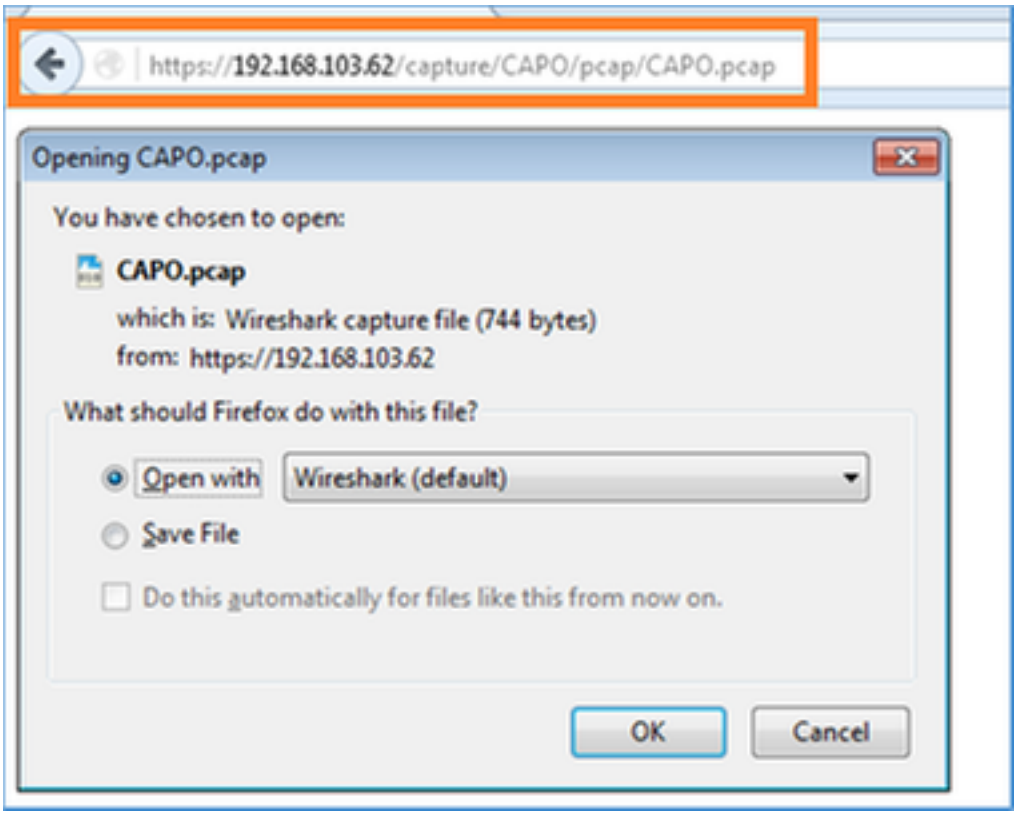


Para la referencia

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	IP de la Interfaz de datos FTD donde habilitan al servidor HTTP
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	El nombre de la captura FTD
https://192.168.103.62/capture/CAPI/pcap/ CAPI.pcap	El nombre del archivo que será descargado

Para la segunda captura:

https://192.168.103.62/capture/CAPO/pcap/CAPO.pcap



¿Trabajo con las capturas del motor FTD ASA? Exportación de una captura usando FTP/TFTP/SCP

Requisitos

Exporte las capturas admitidas los escenarios previos usando los protocolos FTP/TFTP/SCP

Solución

Exportación de una captura a un servidor FTP:

```
firepower# copy /pcap capture:CAPI ftp://ftp_username:ftp_password@192.168.78.73/CAPI.pcapSource
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#
```

Exportación de una captura a un servidor TFTP:

```
firepower# copy /pcap capture:CAPI tftp://192.168.78.73Source capture name [CAPI]?Address or
name of remote host [192.168.78.73]?Destination filename [CAPI]?!!!!!!!!!!!!!!!!346 packets
copied in 0.90 secs
firepower#
```

Exportación de una captura a un servidor de SCP:

```
firepower# copy /pcap capture:CAPI scp://scp_username:scp_password@192.168.78.55Source 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)? yesWarning: Permanently added
'192.168.78.55' (SHA256) to the list of known
hosts.!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!454
packets copied in 3.950 secs (151 packets/sec)
firepower#
```

¿Trabajo con las capturas del motor FTD ASA? Localizar un paquete

Requisitos

Habilite una captura en FTD usando los filtros siguientes:

IP de la fuente	192.168.103.1
IP de destino	192.168.101.1
Protocolo	ICMP
Interfaz	DENTRO
Seguimiento del paquete	sí
Número de paquetes del seguimiento	100

Haga ping del Host-a (192.168.103.1) el Host-b (192.168.101.1) y marque las capturas.

Solución

Localizar un paquete real puede ser muy útil para resolver problemas los problemas de conectividad. Permite ver todos los controles internos a través de los cuales un paquete está pasando. ¿Agregue? ¿**localice el detalle**? las palabras claves y especifican la cantidad de paquetes que sean localizados. Por abandono el FTD localiza los primeros 50 paquetes de ingreso.

En este caso habilite la captura con el detalle de la traza para los primeros 100 paquetes que FTD recibe en la interfaz interior:

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

Haga ping del Host-a al Host-b y marque el resultado:

```
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
```

Aquí están los paquetes capturados:

```
> 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 reply8 packets shown
```

Aquí está una traza del primer paquete. Las piezas interesantes son:

- Fase 12 donde se puede considerar el “flujo delantero”. Éste es el arsenal del envío del motor ASA (con eficacia la orden de funcionamiento interna)
- Fase 13 donde FTD envía el paquete para resoplar caso
- Fase 14 donde se considera el veredicto del Snort

```
> show capture CAPI2 packet-number 1 trace detail8 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: 1Type: CAPTURE... output omitted
...Phase: 12Type: FLOW-CREATIONSubtype:Result: ALLOWConfig:Additional Information:New flow
created with id 195, packet dispatched to next moduleModule information for forward flow
...snp_fp_inspect_ip_optionssnp_fp_snortsnp_fp_inspect_icmpsnp_fp_adjacencysnp_fp_fragmentsnp_ifc_stat Module information for reverse flow
...snp_fp_inspect_ip_optionssnp_fp_inspect_icmpsnp_fp_snortsnp_fp_adjacencysnp_fp_fragmentsnp_ifc_stat Phase: 13Type: EXTERNAL-INSPECTSubtype:Result: ALLOWConfig:Additional Information:Application: 'SNORT Inspect' Phase: 14Type: SNORTSubtype:Result: ALLOWConfig:Additional Information:Snort Verdict: (pass-packet) allow this packet... output
omitted ...Result:input-interface: OUTSIDEinput-status: upinput-line-status: upoutput-interface:
OUTSIDEoutput-status: upoutput-line-status: upAction: allow 1 packet shown>
```

Usando la utilidad del paquete-trazalíneas FTD

Requisitos

Utilice la utilidad del paquete-trazalíneas para el flujo siguiente y marque cómo el paquete será manejado internamente:

Interfaz de ingreso	DENTRO
Protocolo	Pedido de eco ICMP
IP de la fuente	192.168.103.1
IP de destino	192.168.101.1

Solución

el Paquete-trazalíneas generará un **paquete virtual.** Mientras que puede ser visto debajo del paquete es un tema a resoplar examen, pero captura en el motor del Snort muestra que el paquete virtual no se está enviando realmente a través de él:

```
> packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1 Phase: 1Type:
CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access list Phase: 2Type: ACCESS-
LISTSubtype:Result: ALLOWConfig:Implicit RuleAdditional Information:MAC Access list Phase:
3Type: ROUTE-LOOKUPSubtype: Resolve Egress InterfaceResult: ALLOWConfig:Additional
Information:found next-hop 192.168.101.1 using egress ifc OUTSIDE Phase: 4Type: ACCESS-
LISTSubtype: logResult: ALLOWConfig:access-group CSM_FW_ACL_ globalaccess-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 bothaccess-list CSM_FW_ACL_ remark rule-id 268436482: ACCESS POLICY: FTD5515 -
Mandatory/1access-list CSM_FW_ACL_ remark rule-id 268436482: L4 RULE: Allow ICMPAdditional
Information: This packet will be sent to snort for additional processing where a verdict will be
reached ... output omitted ... Phase: 12Type: FLOW-CREATIONSubtype:Result:
ALLOWConfig:Additional Information:New flow created with id 203, packet dispatched to next
module Result:input-interface: INSIDEinput-status: upinput-line-status: upoutput-interface:
OUTSIDEoutput-status: upoutput-line-status: upAction: allow >
```

Documentos Relacionados

Guía de referencia de comandos de la defensa de la amenaza de la potencia de fuego

Notas del Sistema XX, versión de la potencia de fuego, versión 6.1.0

Guía de configuración de la defensa de la amenaza de la potencia de fuego de Cisco para el administrador de dispositivo de la potencia de fuego, versión 6.1