Fonctionner avec les captures et le traceur de paquets FTD

Contenu

[Introduction](#)
[Composants utilisés](#)
[Topologie](#)
[Traitement de paquets FTD](#)
[Fonctionner avec des captures de Renifler-engine](#)
[Fonctionner avec des captures de Renifler-engine (avec des filtres de tcpdump)](#)
[Exemples de filtre de Tcpdump](#)
[Fonctionner avec des captures d'engine FTD ASA](#)
[Fonctionner avec des captures d'engine FTD ASA ? Exporter une capture utilisant le HTTP](#)
[Fonctionner avec des captures d'engine FTD ASA ? Exporter une capture utilisant FTP/TFTP/SCP](#)
[Fonctionner avec des captures d'engine FTD ASA ? Découverte d'un paquet](#)
[Utilisant l'utilitaire de traceur de paquets FTD](#)
[Documents connexes](#)

Introduction

Ce document décrit comment fonctionner avec des captures de la défense contre des menaces de puissance de feu (FTD) et des utilitaires de traceur de paquets.

Les captures de paquet est l'un des outils de dépannage les plus utilisés généralement. Les cas d'utilisation de captures de paquet sont :

- Pour montrer qu'un paquet arrive sur le périphérique
- Pour montrer qu'un paquet laisse le périphérique
- Pour montrer qu'un paquet est lâché par un périphérique (par exemple l'ASP ASA relâche)

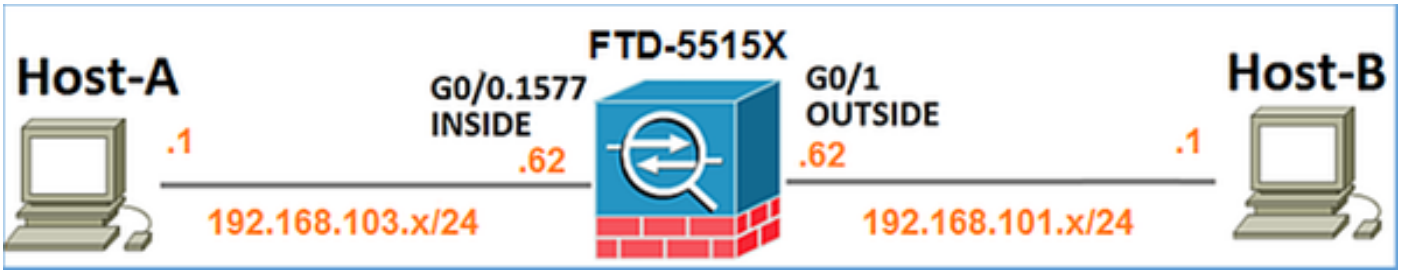
Sur FTD des paquets peuvent être capturés par deux engines :

1. Engine ASA
2. Reniflez l'engine

Composants utilisés

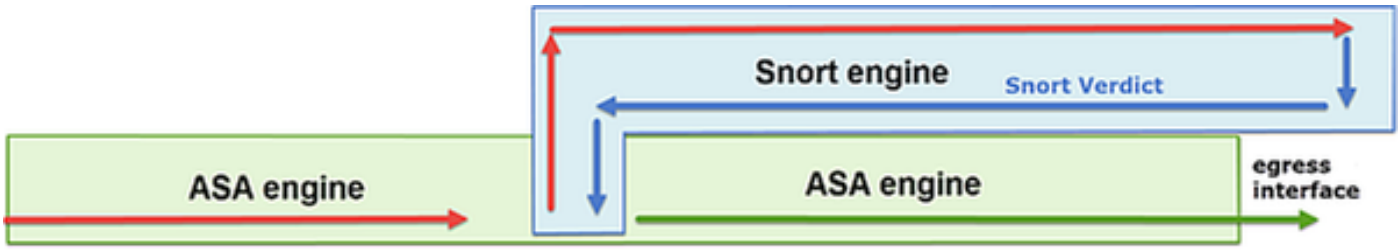
- ASA5515X exécutant le code 6.1.0 (construction 330) FTD
- Centre de Gestion de puissance de feu (FMC) exécutant 6.1.0 (construction 330)

Topologie



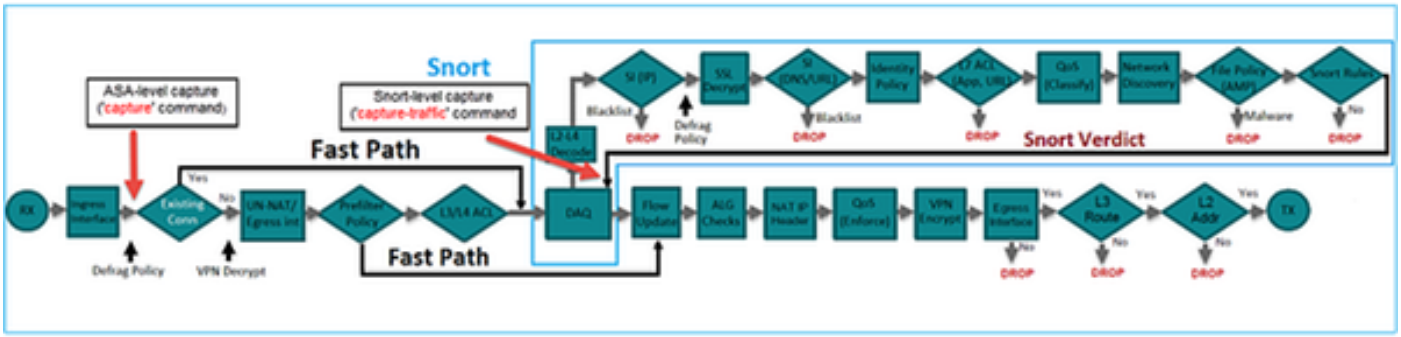
Traitement de paquets FTD

Le traitement de paquets FTD peut être visualisé comme suit :



1. Un paquet écrit l'interface d'entrée et il est manipulé par l'engine ASA
2. Si la stratégie dicte le paquet est examiné par l'engine de renifler
3. Reniflez l'engine renvoie un verdict (par exemple whitelist, liste noire) pour le paquet
4. Les baisses d'engine ASA ou en avant le paquet basé sur Snort ? verdict s

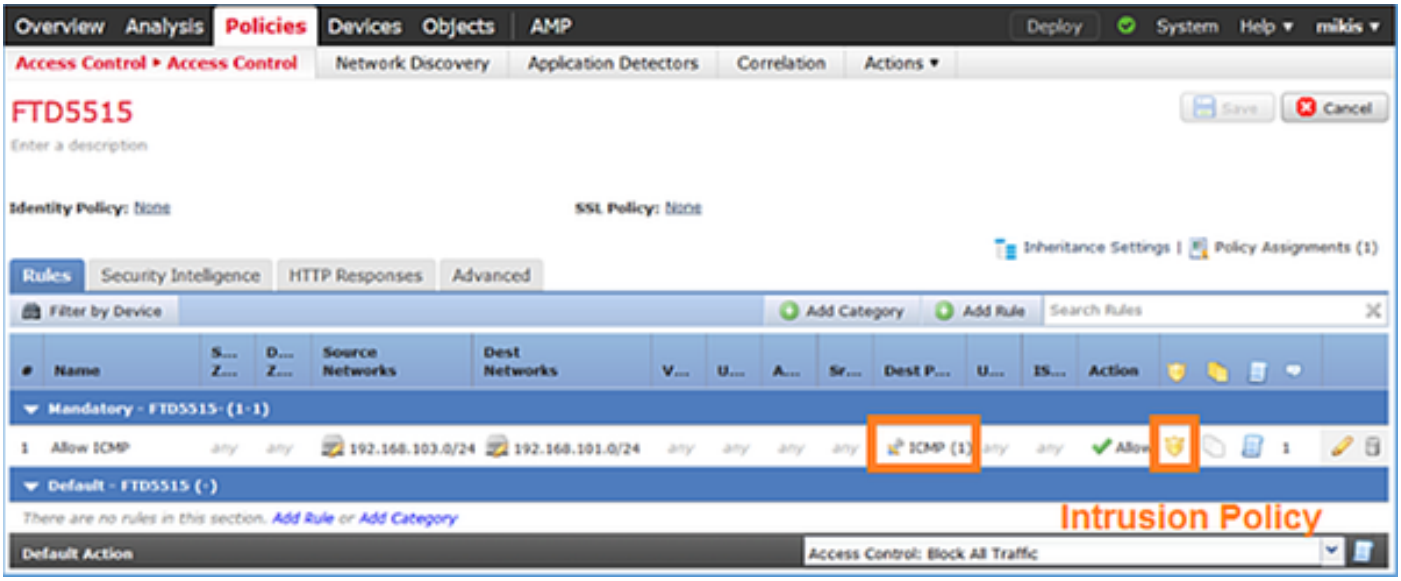
Basé sur l'architecture ci-dessus les captures FTD peuvent être prises sur 2 endroits différents :



Fonctionner avec des captures de Renifler-engine

Conditions préalables

Il y a une stratégie de contrôle d'accès (ACP) appliquée sur FTD qui permet au trafic d'ICMP pour intervenir. La stratégie a également une stratégie d'intrusion appliquée :



Conditions requises

1. Activez la capture sur le mode FTD CLISH utilisant aucun filtre
2. Cinglez par le FTD et vérifiez la sortie de capture

Solution

Étape 1 : Ouvrez une session à la console ou au SSH FTD à l'interface br1 et activez la capture sur le mode FTD CLISH utilisant aucun filtre

```
> 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:
```

Sur FTD 6.0.x la commande est :

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

Étape 2 : Cinglez par le FTD et vérifiez la sortie de capture

```
> 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
```

Fonctionner avec des captures de Renifler-engine (avec des filtres de tcpdump)

Conditions requises

1. Activez la capture sur le mode FTD CLISH utilisant un filtre pour IP 192.168.101.1
2. Cinglez par le FTD et vérifiez la sortie de capture

Solution

Étape 1 : Activez la capture sur le mode FTD CLISH utilisant un filtre pour 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
```

Étape 2 : Cinglez par le FTD et vérifiez la capture sortie :

```
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
```

Vous pouvez utiliser ? - n ? option de voir les hôtes et les numéros de port dans le format numérique. Par exemple la capture ci-dessus sera affichée en tant que :

```
> 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
```

Exemples de filtre de Tcpdump

Exemple 1

Pour capturer l'IP de Src ou le Dst IP = 192.168.101.1 et port de Src ou port de Dst = TCP/UDP 23 :

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

Exemple 2

Pour capturer Src IP = 192.168.101.1 et port de Src = TCP/UDP 23 :

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

Exemple 3

Pour capturer Src IP = 192.168.101.1 et port de Src = TCP 23 :

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

Exemple 4

Pour capturer Src IP = 192.168.101.1 et voir l'adresse MAC des paquets ajouter l'option « 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
```

Exemple 5

Pour quitter après avoir capturé 10 paquets :

```
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
```

Exemple 6

Pour écrire une capture à un fichier avec le nom capture.pcap et la copier par l'intermédiaire du FTP sur le serveur distant :

```
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.>
```

Fonctionner avec des captures d'engine FTD ASA

Conditions requises

1. Enable 2 captures sur FTD utilisant les filtres suivants :

Source ip	192.168.103.1
IP de destination	192.168.101.1
Protocol	ICMP
Interface	À L'INTÉRIEUR
Source ip	192.168.103.1
IP de	192.168.101.

destination	1
Protocol	ICMP
Interface	DEHORS

2. Cinglez du l'hôte-Un (192.168.103.1) l'hôte B (192.168.101.1) et vérifiez les captures.

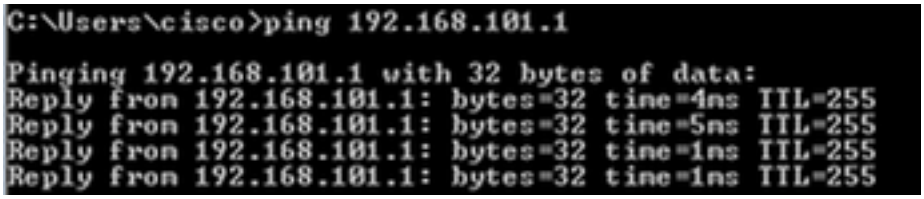
Solution

Étape 1 : Activation des captures :

```
> 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
```

Étape 2 : Vérifier les captures utilisant le CLI

Ping d'hôte-Un à l'hôte 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
```

Les 2 captures ont différentes tailles dues à l'en-tête Dot1Q sur l'interface interne. Ceci peut être affiché dans la sortie suivante :

```
> 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
```

Fonctionner avec des captures d'engine FTD ASA ? Exporter une capture utilisant le HTTP

Conditions requises

Exportez les captures rentrées le scénario précédent utilisant un navigateur

Solution

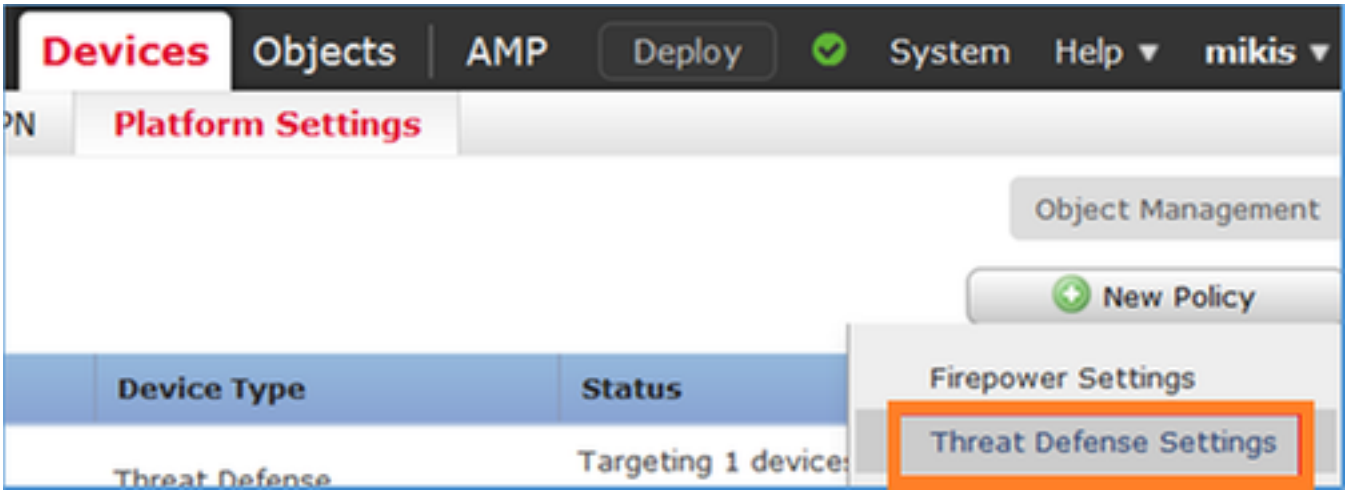
Afin d'exporter les captures utilisant le navigateur là est le besoin :

1. Serveur de l'enable HTTPS
2. Permettez l'accès HTTPS

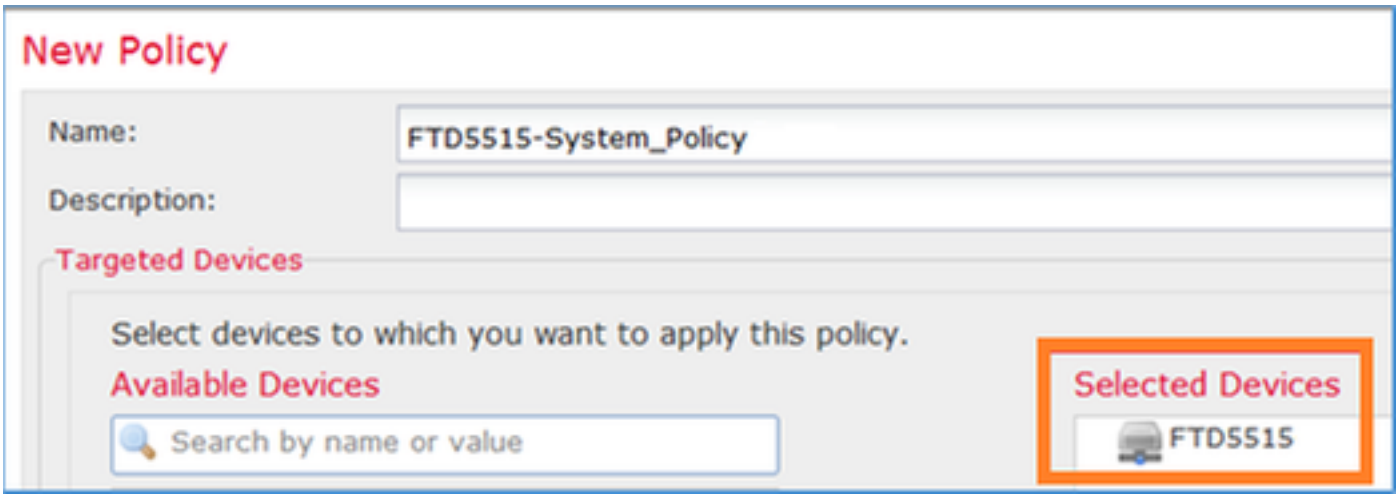
Par défaut le serveur HTTPS est désactivé et aucun accès n'est permis :

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

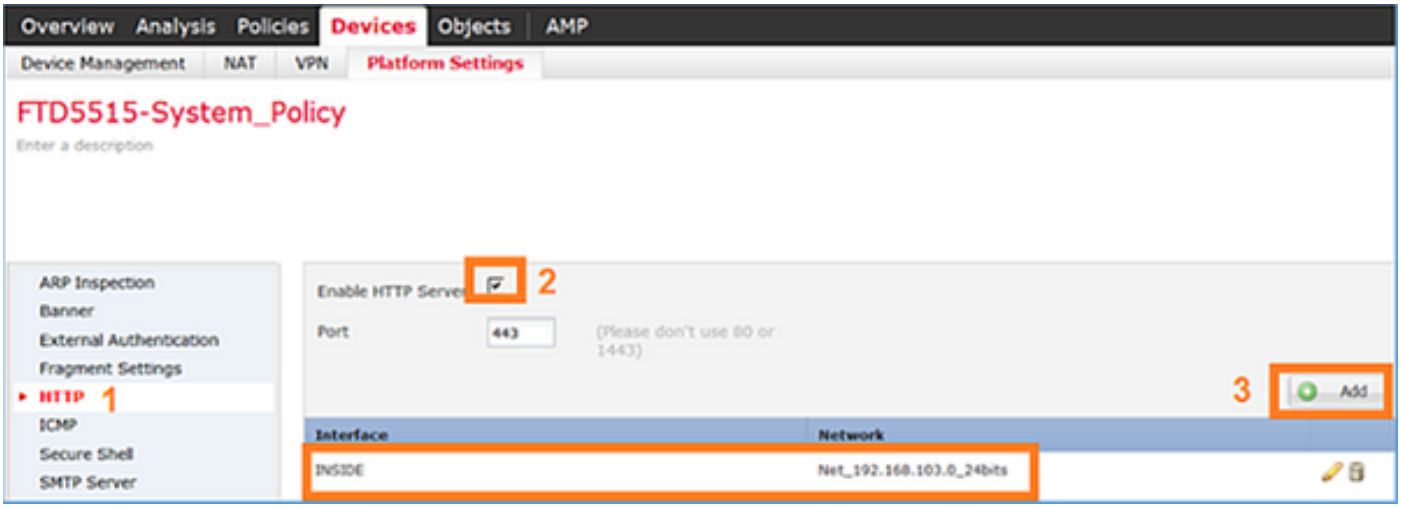
Étape 1 : Naviguez vers des **périphériques > des configurations de plate-forme,** cliquez sur en fonction la **nouvelle stratégie** et sélectionnez les **configurations de défense contre des menaces :**



Spécifiez la cible de nom de stratégie et de périphérique :



Étape 2 : Activez le serveur HTTPS et ajoutez le réseau qui devrait être permis pour accéder au périphérique FTD au-dessus de HTTPS :



Sauvegardez et **déployez-vous**

Conseil

Tandis que vous déployez la stratégie vous pouvez activer **mettez au point le HTTP** afin de voir commencer de service HTTP :

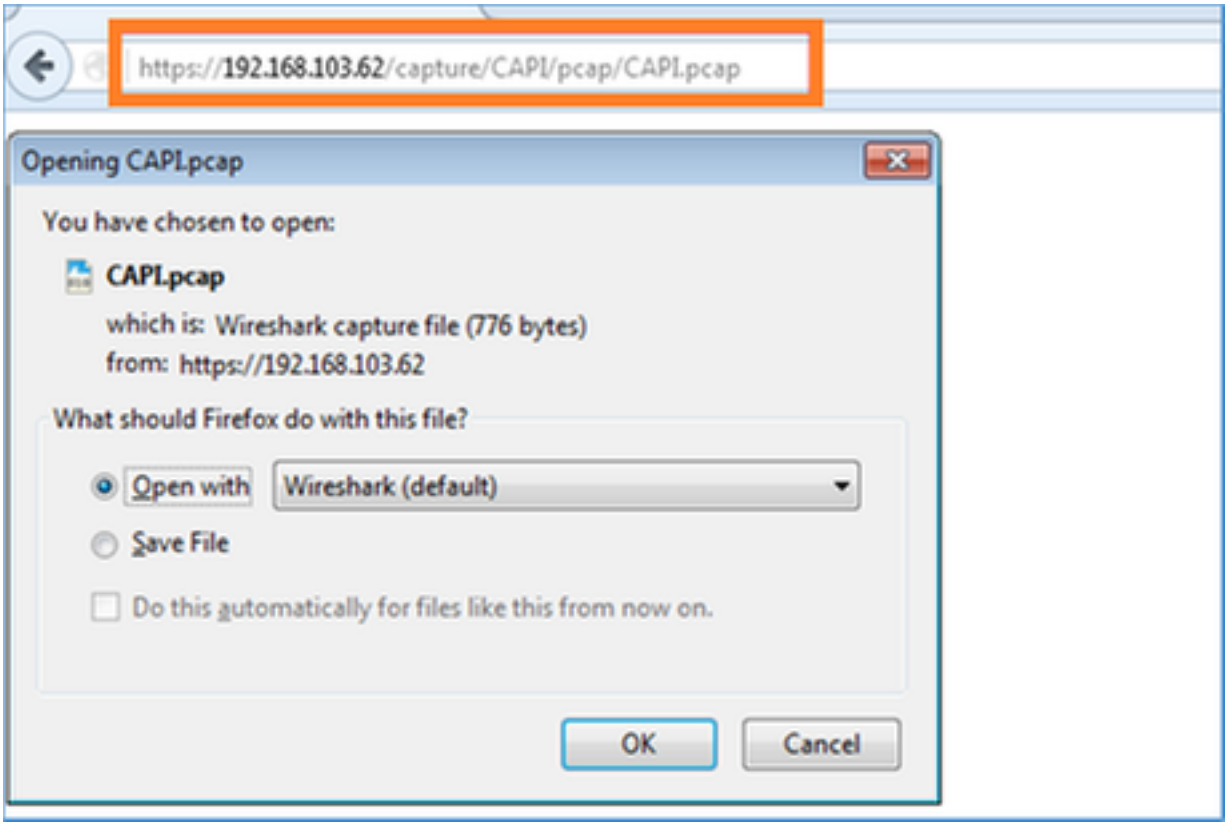
```
> debug http 255debug http enabled at level 255.http_enable: Enabling HTTP serverHTTP server starting.
```

Voici le résultat sur FTD CLI :

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

Ouvrez un navigateur sur l'hôte-Un (192.168.103.1) et employez l'URL suivant pour télécharger la première capture :

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

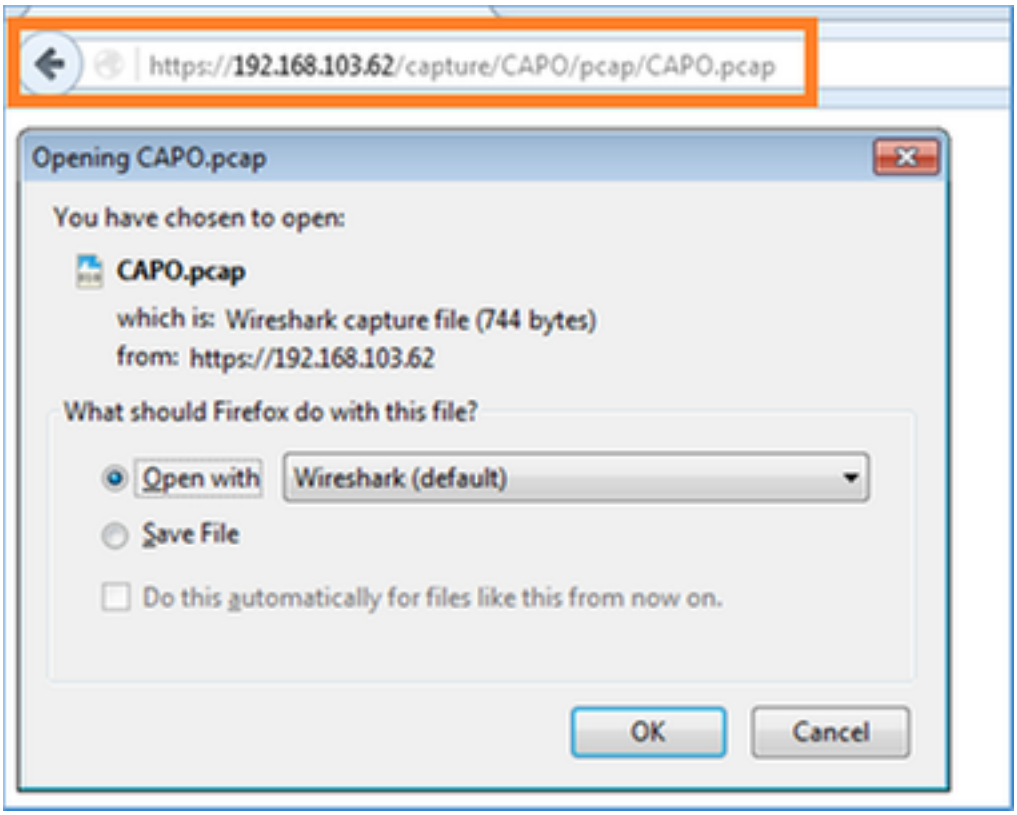


Pour la référence

https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	L'IP des données FTD relient où le serveur HTTP est activé
https://192.168.103.62/capture/CAPI/pcap/CAPI.pcap	Le nom de la capture FTD
https://192.168.103.62/capture/CAPI/pcap/ CAPI.pcap	Le nom du fichier qui sera téléchargé

Pour la deuxième capture :

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



Fonctionner avec des captures d'engine FTD ASA ? Exporter une capture utilisant FTP/TFTP/SCP

Conditions requises

Exportez les captures rentrées les scénarios précédents utilisant des protocoles FTP/TFTP/SCP

Solution

Exporter une capture à un ftp server :

```
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#
```

Exporter une capture à un serveur 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#
```

Exporter une capture à un serveur 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#
```

Fonctionner avec des captures d'engine FTD ASA ? Découverte d'un paquet

Conditions requises

Activez une capture sur FTD utilisant les filtres suivants :

Source ip	192.168.103.1
IP de destination	192.168.101.1
Protocol	ICMP
Interface	À L'INTÉRIEUR
Suivi de paquet	oui
Nombre de paquets de suivi	100

Cinglez du l'hôte-Un (192.168.103.1) l'hôte B (192.168.101.1) et vérifiez les captures.

Solution

La découverte d'un vrai paquet peut être très utile pour dépanner des problèmes de connectivité. Il laisse voir tous les contrôles internes par lesquels un paquet va. Ajoutez ? **détail de suivi** ? les mots clé et spécifient la quantité de paquets qui seront tracés. Par défaut le FTD trace les 50 premiers paquets d'entrée.

Activez dans ce cas la capture avec le détail de suivi pour les 100 premiers paquets que FTD reçoit sur l'interface interne :

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

Cinglez du l'hôte-Un à l'hôte B et vérifiez le résultat :

```
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
```

Voici les paquets capturés :

```
> 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
```

Voici un suivi du premier paquet. Les pièces intéressantes sont :

- Phase 12 où peut être vu « l'écoulement en avant ». C'est la baie de répartition d'engine ASA (efficacement la commande interne des exécutions)
- Phase 13 où FTD envoie le paquet pour renifler l'exemple
- Phase 14 où le verdict de renifler est vu

```
> 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>
```

Utilisant l'utilitaire de traceur de paquets FTD

Conditions requises

Utilitaire de traceur de paquets d'utilisation pour l'écoulement et le contrôle suivants comment le paquet sera manipulé intérieurement :

Interface d'entrée	À L'INTÉRIEUR
Protocol	Requête d'écho d'ICMP
Source ip	192.168.103.1
IP de destination	192.168.101.1

Solution

Le traceur de paquets génèrera un **paquet virtuel.** Pendant qu'il peut voir au-dessous du paquet est un sujet pour renifler l'inspection, mais la capture sur l'engine Snort prouve que le paquet virtuel n'est pas envoyé réellement par lui :

```
> 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 >
```

Documents connexes

Guide de référence des commandes de défense contre des menaces de puissance de feu

Notes en version système de puissance de feu, version 6.1.0

Guide de configuration de défense contre des menaces de puissance de feu de Cisco pour le gestionnaire de périphérique de puissance de feu, version 6.1