Utiliser les captures Firepower Threat Defense et Packet Tracer

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
- Informations générales
  - Traitement des paquets FTD
- Configurer
  - Diagramme du réseau
  - Utiliser les captures du moteur Snort
    - Conditions préalables
    - Exigences
    - Solution
  - Utiliser les captures du moteur Snort
    - Exigences
    - Solution
    - Exemples De Filtres Tcpdump
  - Utiliser les captures du moteur FTD LINA
    - Exigences
    - Solution
  - Utiliser les captures du moteur LINA FTD - Exporter une capture via HTTP
    - Exigences
    - Solution
  - Utilisation des captures du moteur FTD LINA - Exportation d'une capture via FTP/TFTP/SCP
    - Exigences
    - Solution
  - Utilisation des captures du moteur FTD LINA - Suivi d'un paquet de trafic réel
    - Exigences
    - Solution
  - Outil de capture dans les versions du logiciel FMC post-6.2
    - Solution : utilisez l'interface de ligne de commande FTD
  - Suivre un paquet réel sur FMC post-6.2
  - Utilitaire Packet Tracer FTD
    - Exigences
    - Solution
  - Outil d'interface utilisateur Packet Tracer dans les versions du logiciel FMC postérieures à la version 6.2
- Informations connexes

Introduction

Ce document décrit comment utiliser les captures Firepower Threat Defense (FTD) et les utilitaires Packet Tracer.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions logicielles suivantes :

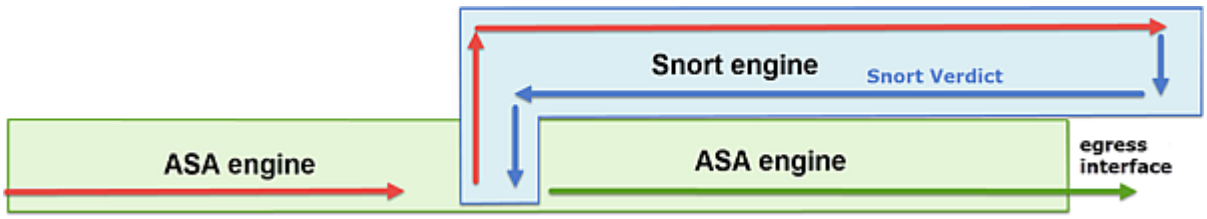
- ASA5515-X qui exécute le logiciel FTD 6.1.0
- FPR4110 qui exécute le logiciel FTD 6.2.2
- FS4000 qui exécute le logiciel Firepower Management Center (FMC) 6.2.2

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

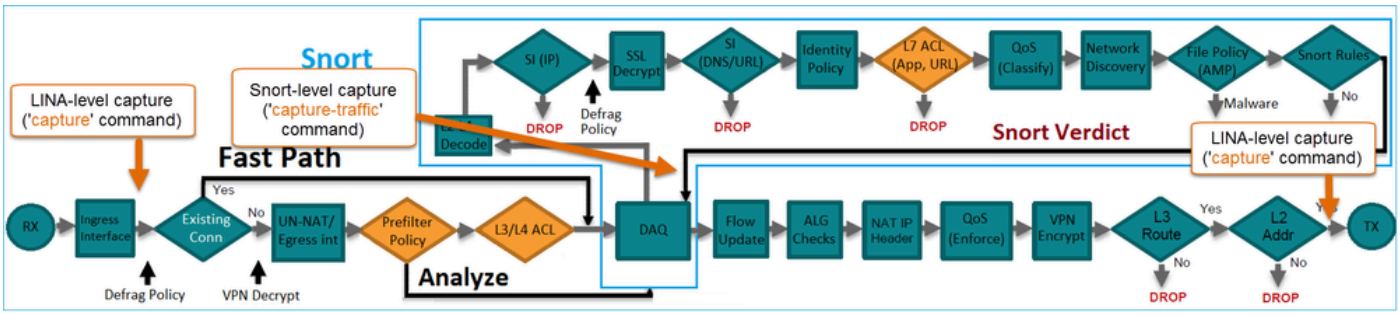
Traitement des paquets FTD

Le traitement des paquets FTD est visualisé comme suit :



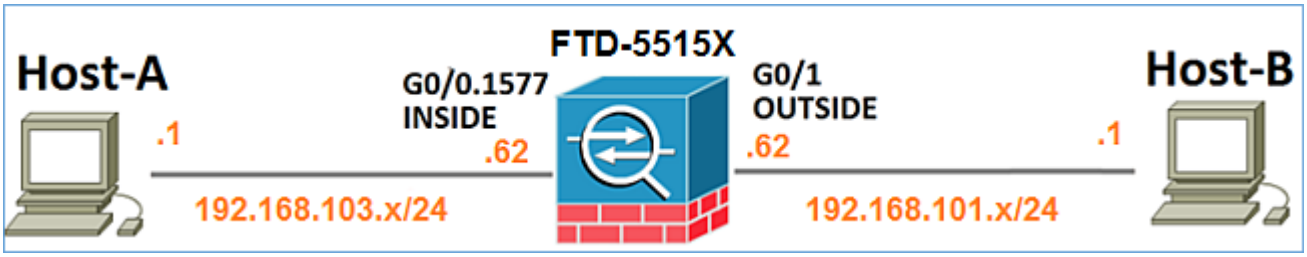
1. Un paquet entre dans l'interface d'entrée et est géré par le moteur LINA.
2. Si la politique exige que le paquet soit inspecté par le moteur Snort.
3. Le moteur Snort renvoie un verdict pour le paquet.
4. Le moteur LINA abandonne ou transfère le paquet en fonction du verdict du renifleur.

En fonction de l'architecture, les captures FTD peuvent être effectuées dans les emplacements suivants :



Configurer

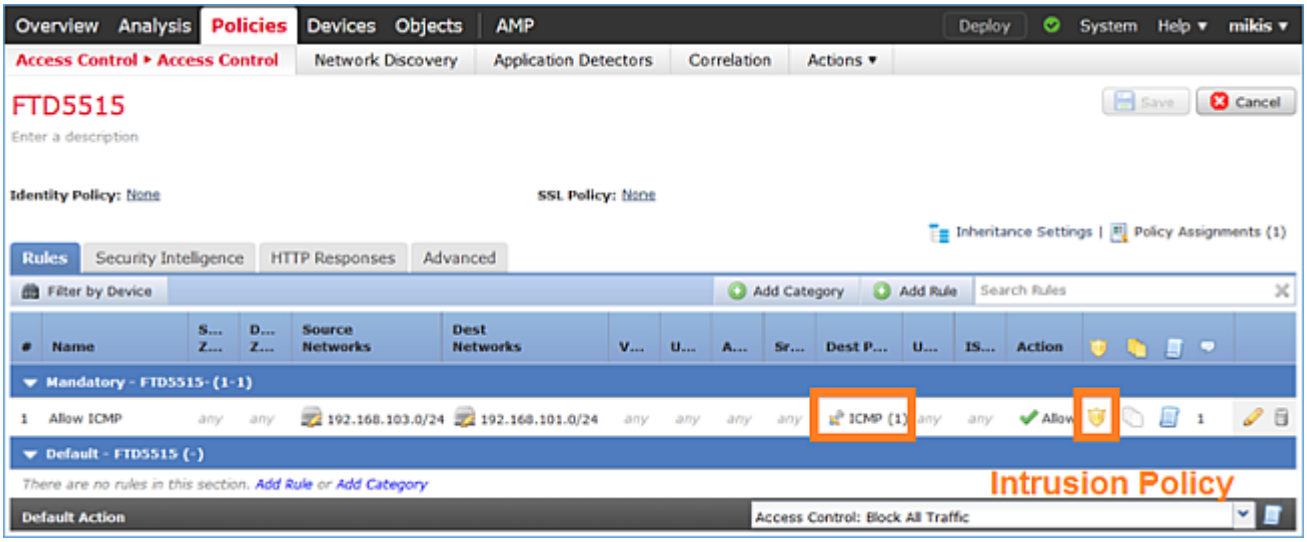
Diagramme du réseau



Utiliser les captures du moteur Snort

Conditions préalables

Une politique de contrôle d'accès (ACP) est appliquée sur le FTD qui permet au trafic ICMP (Internet Control Message Protocol) de passer. Une stratégie d'intrusion est également appliquée à la stratégie :



Exigences

1. Activez la capture en mode FTD CLISH sans filtre.

2. Envoyez une requête ping au FTD et vérifiez la sortie capturée.

Solution

Étape 1. Connectez-vous à la console FTD ou SSH à l'interface br1 et activez la capture en mode FTD CLISH sans filtre.

```
<#root>

>

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:
```

Sur FTD 6.0.x, la commande est :

```
<#root>

>

system support

capture-traffic
```

Étape 2. Envoyez une requête ping à FTD et vérifiez le résultat capturé.

```
<#root>

>

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, le
12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 1, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 2, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 2, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 3, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 3, leng
12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 4, le
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 4, leng
^C    <- to exit press CTRL + C
```

Utiliser les captures du moteur Snort

Exigences

1. Activez la capture en mode FTD CLISH à l'aide d'un filtre pour IP 192.168.101.1.
2. Envoyez une requête ping à FTD et vérifiez la sortie capturée.

Solution

Étape 1 : activation de la capture en mode FTD CLISH à l'aide d'un filtre pour IP 192.168.101.1

<#root>

>

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

Étape 2. Envoyez une requête ping au FTD et vérifiez le résultat capturé :

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

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

Vous pouvez utiliser l'option -n pour afficher les hôtes et les numéros de port au format numérique. Par exemple, la capture précédente s'affiche comme suit :

```
<#root>

>

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
```

Exemples De Filtres Tcpdump

Exemple 1 :

Afin de capturer Src IP ou Dst IP = 192.168.101.1 et Src port ou Dst port = TCP/UDP 23, entrez cette commande :

```
<#root>

Options:

-n host 192.168.101.1 and port 23
```

Exemple 2 :

Afin de capturer Src IP = 192.168.101.1 et Src port = TCP/UDP 23, entrez cette commande :

<#root>

Options:

-n src 192.168.101.1 and src port 23

Exemple 3 :

Afin de capturer Src IP = 192.168.101.1 et Src port = TCP 23, entrez cette commande :

<#root>

Options:

-n src 192.168.101.1 and tcp and src port 23

Exemple 4 :

Afin de capturer Src IP = 192.168.101.1 et voir l'adresse MAC des paquets, ajoutez l'option e, et entrez cette commande :

<#root>

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

Exemple 5 :

Afin de quitter après avoir capturé 10 paquets, entrez cette commande :

<#root>

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
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
```

Exemple 6 :

Afin d'écrire une capture dans un fichier avec le nom capture.pcap et de le copier via FTP vers un serveur distant, entrez cette commande :

```
<#root>

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.


>
```

Utiliser les captures du moteur FTD LINA

Exigences

1. Activez deux captures sur FTD à l'aide des filtres suivants :

Adresse IP source	192.168.103.1
Adresse IP de destination	192.168.101.1
Protocol	ICMP
Interface	INTÉRIEUR

Adresse IP source	192.168.103.1
Adresse IP de destination	192.168.101.1
Protocol	ICMP
Interface	EXTÉRIEUR

2. Envoyez une requête ping de l'hôte A (192.168.103.1) à l'hôte B (192.168.101.1) et vérifiez les captures.

Solution

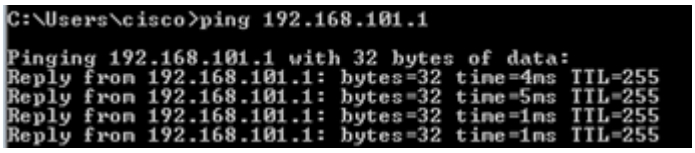
Étape 1 : activation des captures

<#root>

```
> 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 : vérification des captures dans l'interface de ligne de commande

Envoyez une requête ping de l'hôte A vers l'hôte B :



<#root>

```
> 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
```

Les deux captures ont des tailles différentes en raison de l'en-tête Dot1Q sur l'interface INSIDE, comme indiqué dans cet exemple de sortie :

```
<#root>

> 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
```

```
<#root>

> 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
```

Utiliser les captures du moteur LINA FTD - Exporter une capture via HTTP

Exigences

Exportez les captures effectuées dans le scénario précédent avec un navigateur.

Solution

Pour exporter les captures à l'aide d'un navigateur, vous devez :

1. Activez le serveur HTTPS.
2. Autoriser l'accès HTTPS.

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

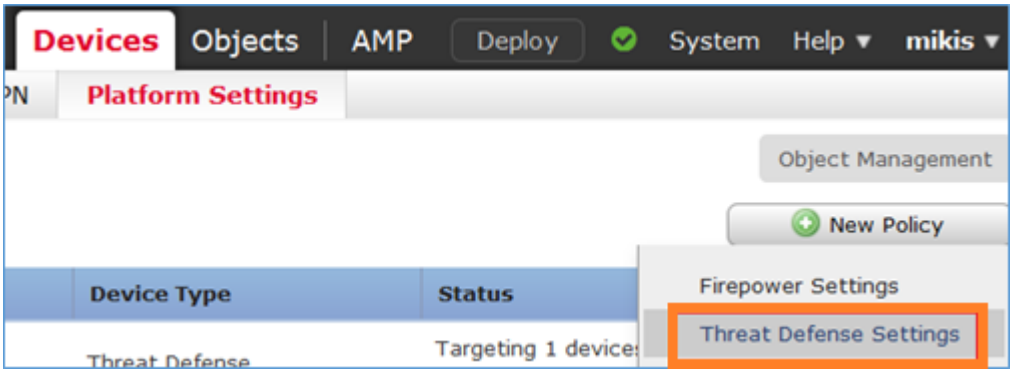
<#root>

>

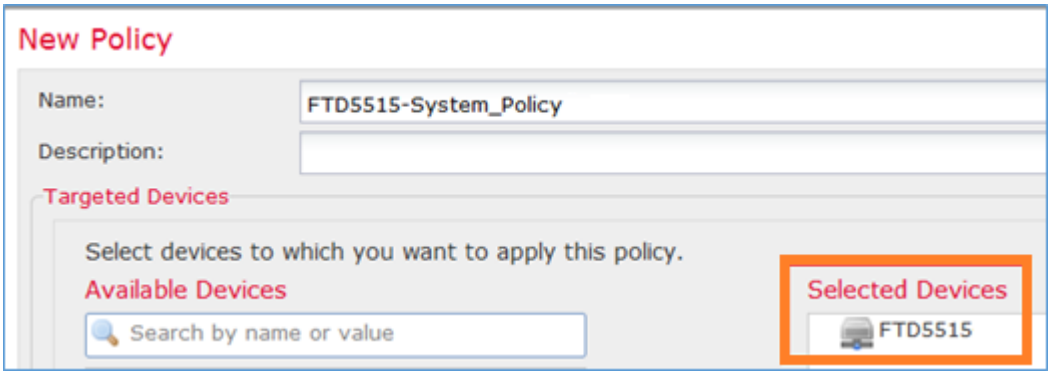
show running-config http

>

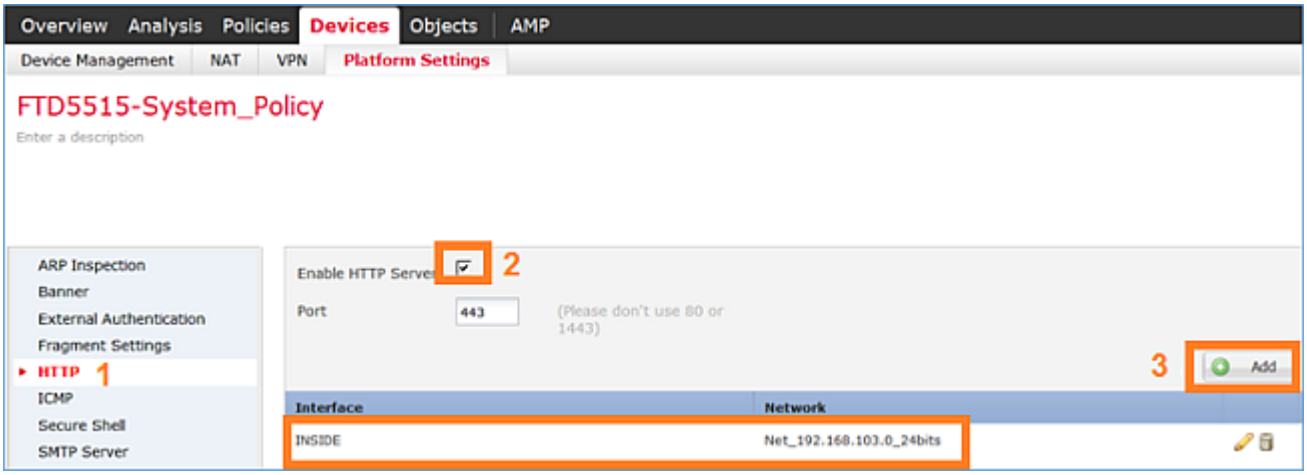
Étape 1. Accédez à Devices > Platform Settings, cliquez sur New Policy, et choisissez Threat Defense Settings :



Spécifiez le nom de la stratégie et la cible du périphérique :



Étape 2. Activez le serveur HTTPS et ajoutez le réseau que vous souhaitez autoriser à accéder au périphérique FTD via HTTPS :



Enregistrer et déployer.

Au moment du déploiement de la stratégie, vous pouvez activer debug http afin de voir le début du service HTTP :

```
<#root>

> debug http 255

debug http enabled at level 255.

http_enable: Enabling HTTP server
HTTP server starting.
```

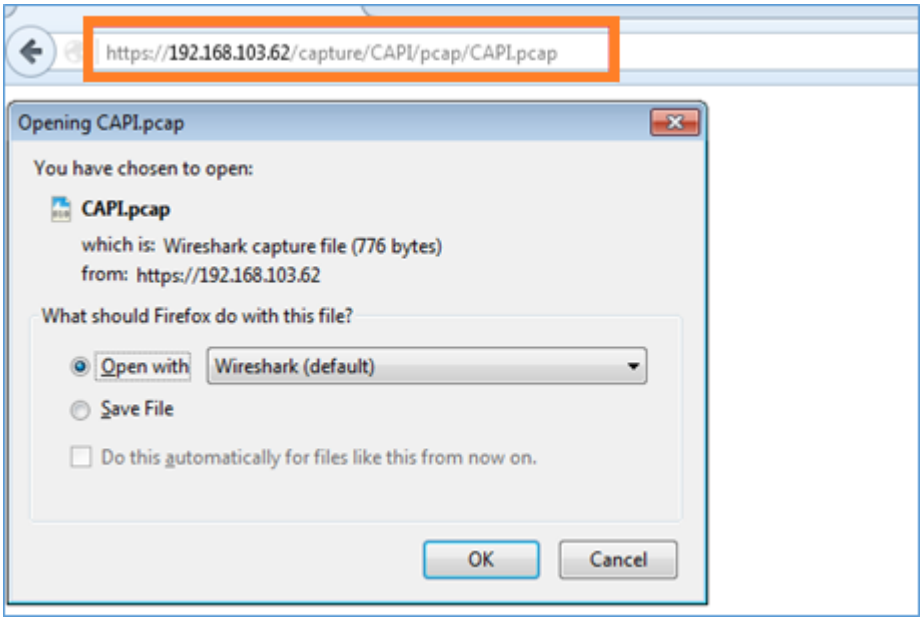
Le résultat sur l'interface CLI FTD est :

```
<#root>

> unebug all

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

Ouvrez un navigateur sur l'hôte A (192.168.103.1) et utilisez cette URL afin de télécharger la première capture : CAPI.pcap.

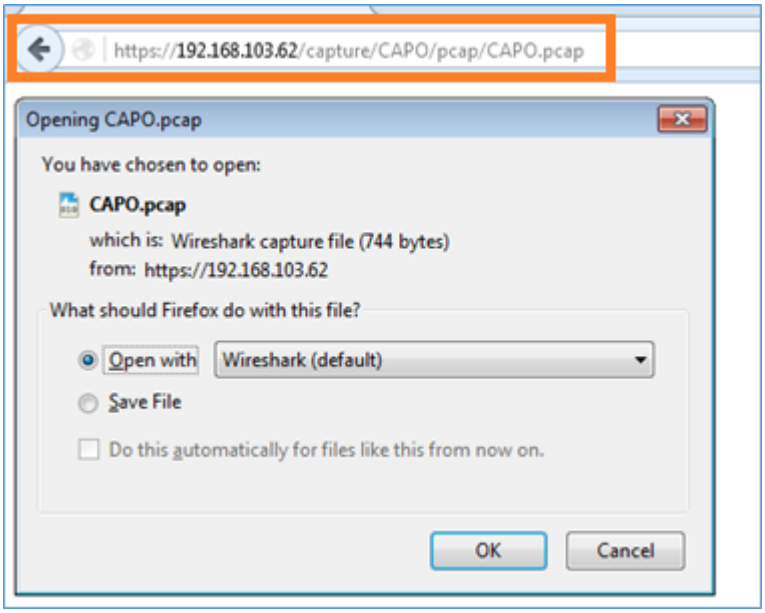


Pour référence :

Capturer CAPI.pcap	IP de l'interface de données FTD où le serveur HTTP est activé.

Capturer CAPI.pcap	Nom de la capture FTD.
Capturer CAPI.pcap	Nom du fichier qui est téléchargé.

Pour la deuxième capture, utilisez Capture CAPI.pcap.



Utilisation des captures du moteur FTD LINA - Exportation d'une capture via FTP/TFTP/SCP

Exigences

Exportez les captures effectuées dans les scénarios précédents avec les protocoles Cisco IOS®.

Solution

Exporter une capture vers un serveur FTP :

<#root>

```
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#
```

Exporter une capture vers un serveur TFTP :

<#root>

```
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#
```

Exporter une capture vers un serveur SCP :

<#root>

```
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:4
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#
```

Déchargement des captures de FTD. Actuellement, lorsque vous devez décharger des captures de FTD, la méthode la plus simple consiste à effectuer les étapes suivantes :

1. À partir de Lina - copy /pcap capture : <cap_name> disk0 :

2. À partir de la racine FPR - mv /ngfw/mnt/disk0/<nom_cap> /ngfw/var/common/

3. À partir de l'interface utilisateur FMC - System > Health > Monitor > Device > Advanced Troubleshooting et saisissez <cap_name> dans le champ et téléchargez.

Utilisation des captures du moteur FTD LINA - Suivi d'un paquet de trafic réel

Exigences

Activez une capture sur FTD avec les filtres suivants :

Adresse IP source	192.168.103.1
Adresse IP de destination	192.168.101.1
Protocol	ICMP
Interface	INTÉRIEUR
Suivi des paquets	oui
Nombre de paquets de suivi	100

Envoyez une requête ping à partir de l'hôte A (192.168.103.1) vers l'hôte B (192.168.101.1) et vérifiez les captures.

Solution

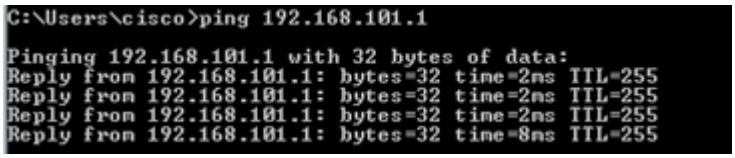
Suivre un paquet réel est très utile pour résoudre les problèmes de connectivité. Il vous permet de voir toutes les vérifications internes qu'un paquet passe. Ajoutez les mots clés trace detail et spécifiez le nombre de paquets que vous voulez tracer. Par défaut, le FTD effectue le suivi des 50 premiers paquets entrants.

Dans ce cas, activez la capture avec les détails de trace pour les 100 premiers paquets que FTD reçoit sur l'interface INSIDE :

<#root>

```
> capture CAPI2 interface INSIDE trace detail trace-count 100 match icmp host 192.168.103.1 host 192.168
```

Envoyez une requête ping de l'hôte A vers l'hôte B et vérifiez le résultat :



Les paquets capturés sont les suivants :

<#root>

```
> show capture CAPI2

8 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
```

Ce résultat montre une trace du premier paquet. Les parties qui présentent un intérêt :

- La phase 12 est l'endroit où l'écoulement direct est observé. Il s'agit du tableau d'envoi du moteur LINA (qui correspond en fait à l'ordre interne des opérations).
- La phase 13 est l'étape au cours de laquelle FTD envoie le paquet à l'instance Snort.
- La phase 14 est celle où le verdict Snort est vu.

<#root>

```
> 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

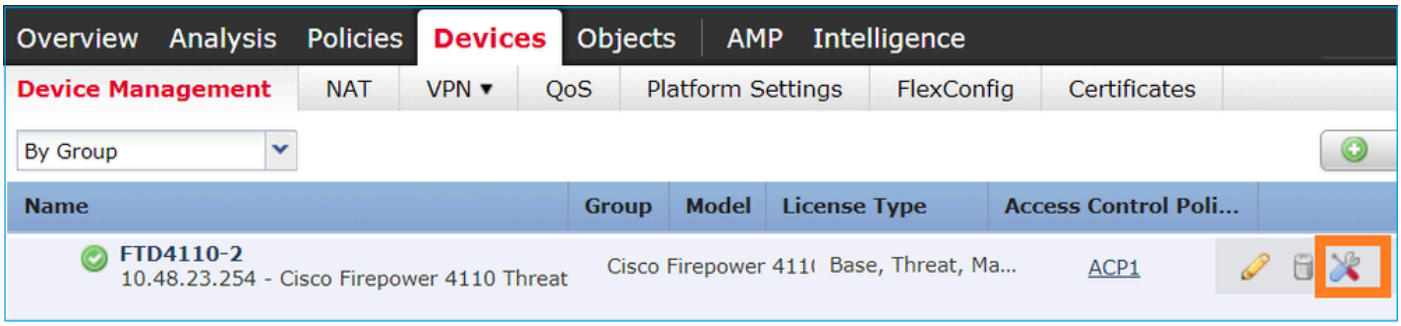

... output omitted ...

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

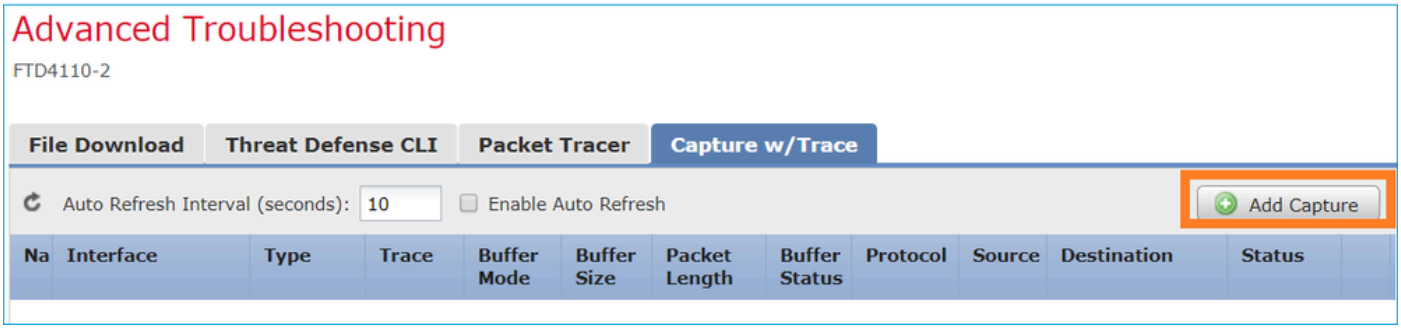
1 packet shown
>
```

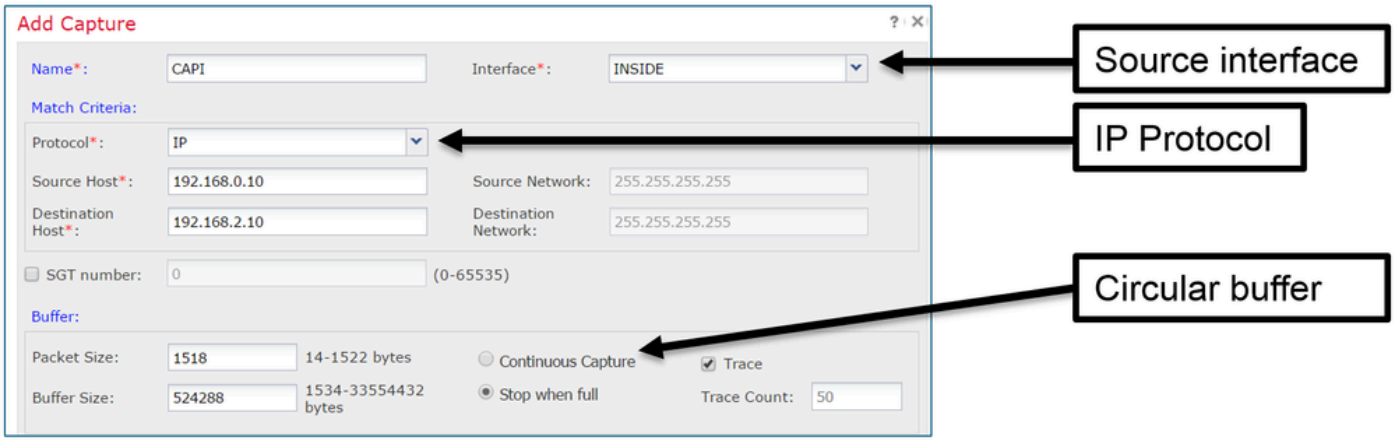
Outil de capture dans les versions du logiciel FMC post-6.2

Dans FMC Version 6.2.x, un nouvel assistant de capture de paquets a été introduit. Accédez à Périphériques > Gestion des périphériques et cliquez sur l'icône Dépannage. Choisissez ensuite Advanced Troubleshooting et enfin Capture w/Trace.



Choisissez Add Capture pour créer une capture FTD :



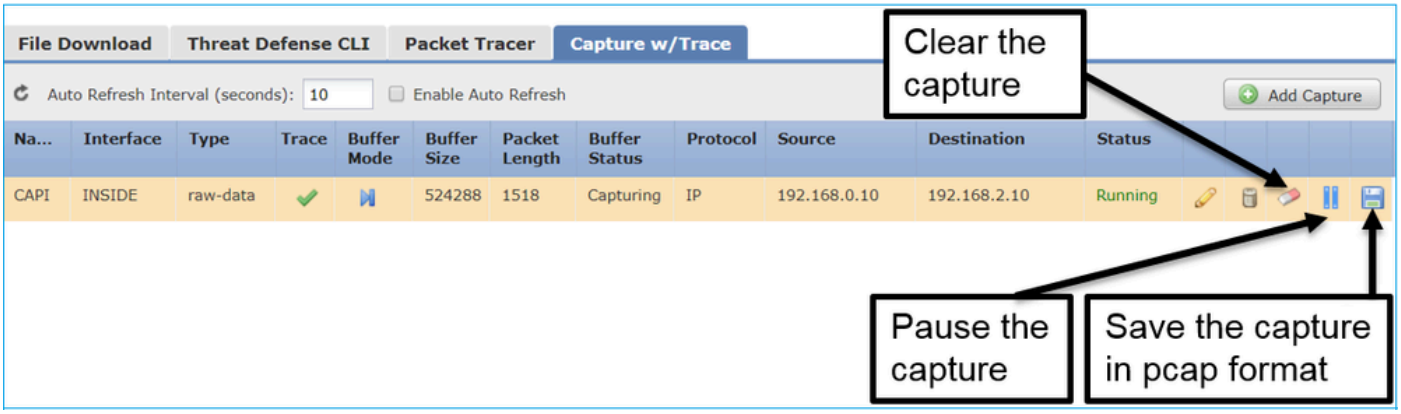


Les limitations actuelles de l'interface utilisateur FMC sont :

- Impossible de spécifier les ports Src et Dst
- Seuls les protocoles IP de base peuvent être associés
- Impossible d'activer la capture pour les abandons ASP du moteur LINA

Solution : utilisez l'interface de ligne de commande FTD

Dès que vous appliquez une capture à partir de l'interface utilisateur FMC, la capture s'exécute :



Capture sur l'interface CLI FTD :

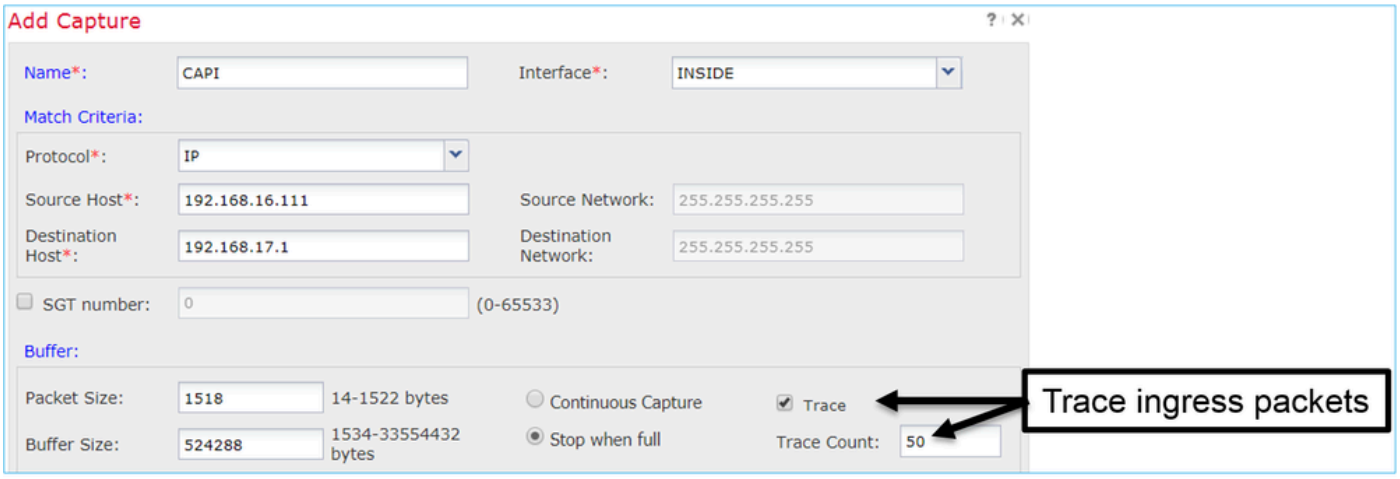
<#root>

```
> show capture

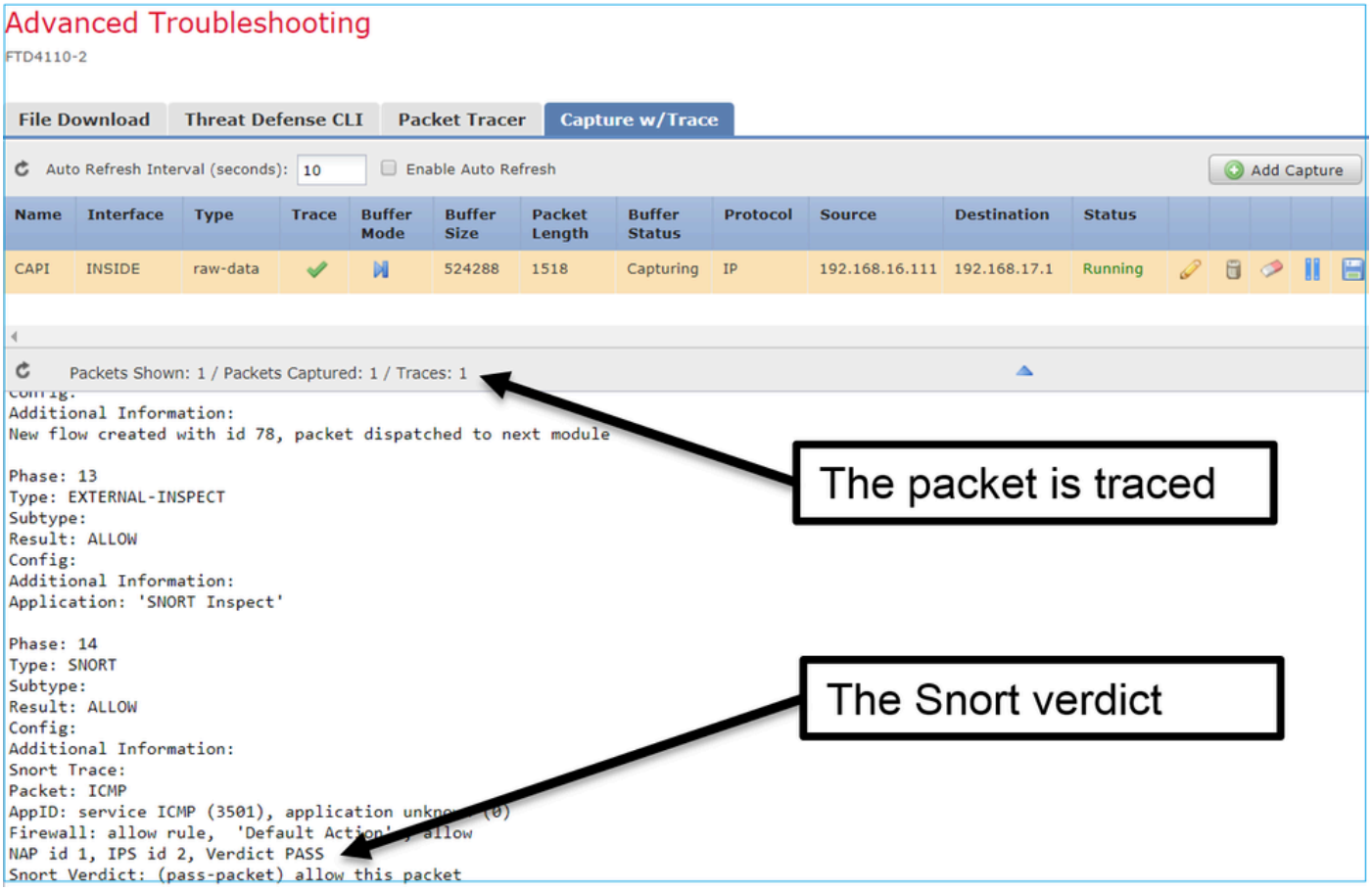
capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

Suivre un paquet réel sur FMC post-6.2

Sur FMC 6.2.x, l'assistant Capture avec suivi vous permet de capturer et de suivre des paquets réels sur FTD :



Vous pouvez vérifier le paquet suivi dans l'interface utilisateur FMC :



Utilitaire Packet Tracer FTD

Exigences

Utilisez l'utilitaire Packet Tracer pour ce flux et vérifiez la manière dont le paquet est traité en interne :

Interface d'entrée	INTÉRIEUR
Protocol	Requête d'écho ICMP
Adresse IP source	192.168.103.1
Adresse IP de destination	192.168.101.1

Solution

Packet Tracer génère un paquet virtuel. Comme le montre cet exemple, le paquet est soumis à l'inspection Snort. Une capture effectuée en même temps au niveau du Snort (capture-traffic) montre la requête d'écho ICMP :

<#root>

> 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
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 capture de niveau Snort au moment du test Packet Tracer montre le paquet virtuel :

```
<#root>

>

capture-traffic


Please choose domain to capture traffic from:
  0 - management0
  1 - Router

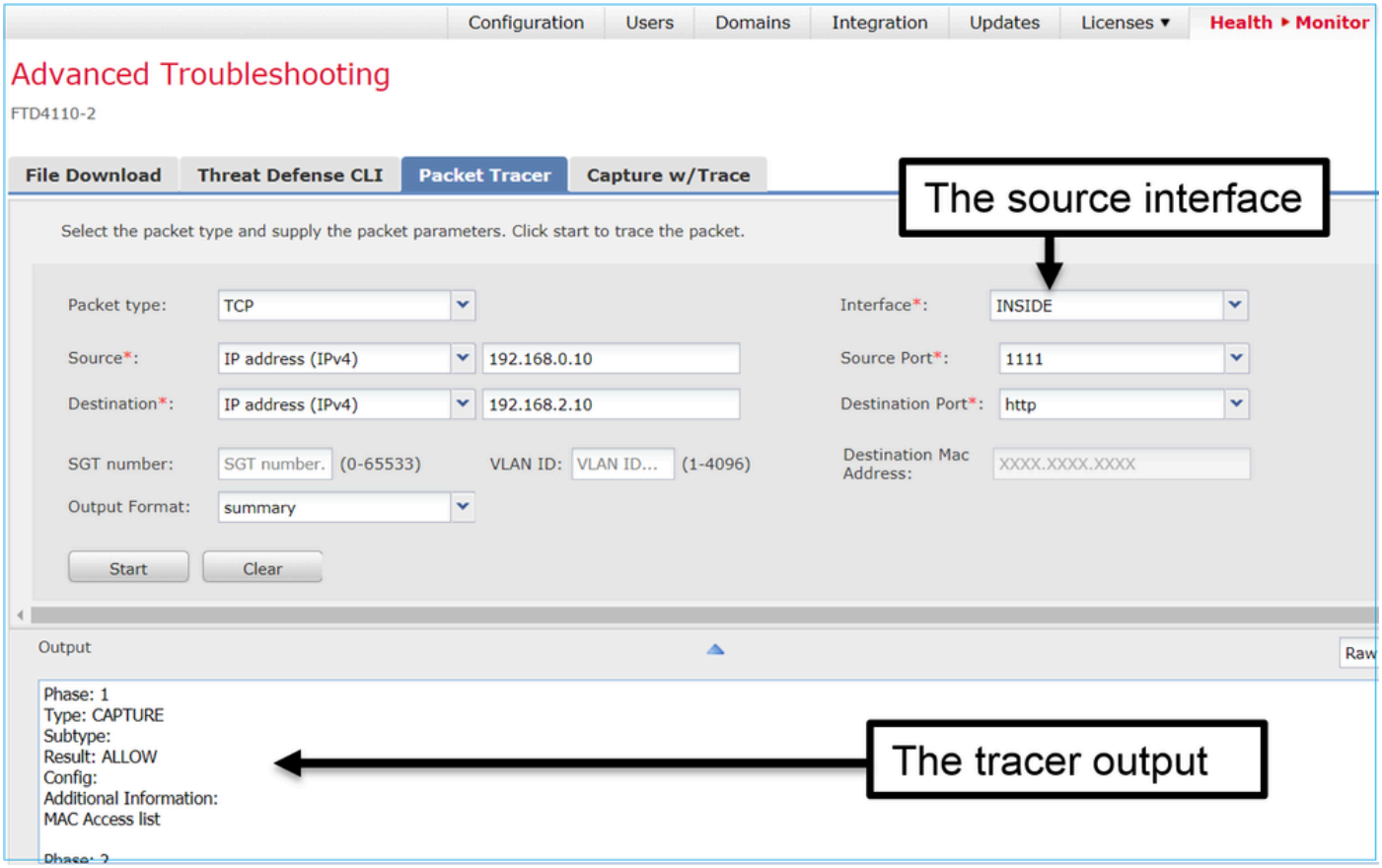
Selection? 1

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
```

Outil d'interface utilisateur Packet Tracer dans les versions du logiciel FMC postérieures à la version 6.2

Dans FMC version 6.2.x, l'outil d'interface utilisateur Packet Tracer a été introduit. L'outil est accessible de la même manière que l'outil de capture et vous permet d'exécuter Packet Tracer sur FTD à partir de l'interface utilisateur FMC :



Informations connexes

- Guide de référence des commandes Firepower Threat Defense
- Notes de version du système Firepower, version 6.1.0
- Guide de configuration de Cisco Firepower Threat Defense pour Firepower Device Manager, version 6.1
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.