Fonctionner avec les captures et le traceur de paquets de la défense contre des menaces de FirePOWER (FTD)

Contenu

Introduction

Ce document décrit comment fonctionner avec des captures de la défense contre des menaces de FirePOWER (FTD) et des utilitaires de Packet Tracer.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

- ASA5515X exécutant le code 6.1.0 (construction 330) FTD
- FPR4110 exécutant le code 6.2.2 (construction 81) FTD
- Centre de Gestion de FirePOWER (FMC) exécutant 6.1.0 (construction 330)
- Centre de Gestion de FirePOWER (FMC) exécutant 6.2.2 (construction 81)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

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 les baisses d'ASP)

Configurez

Conditions préalables

Conditions requises

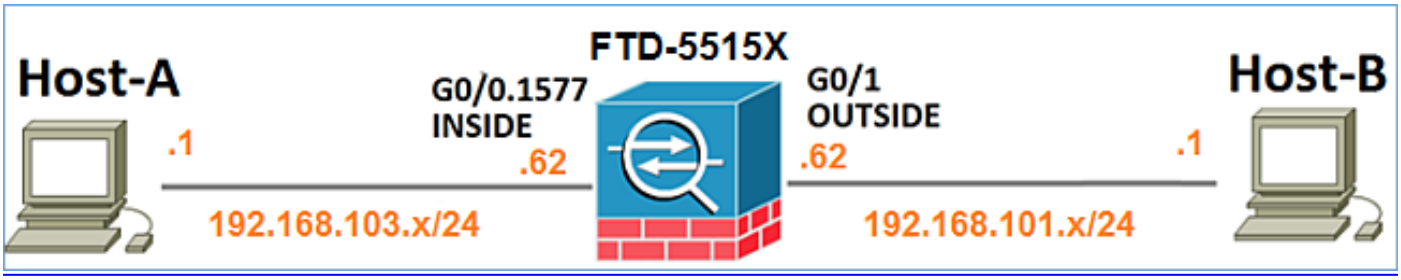
Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

- ASA5515-X exécutant le logiciel 6.1.0 FTD
- FPR4110 exécutant le logiciel 6.2.2 FTD
- FS4000 exécutant le logiciel 6.2.2 FMC

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

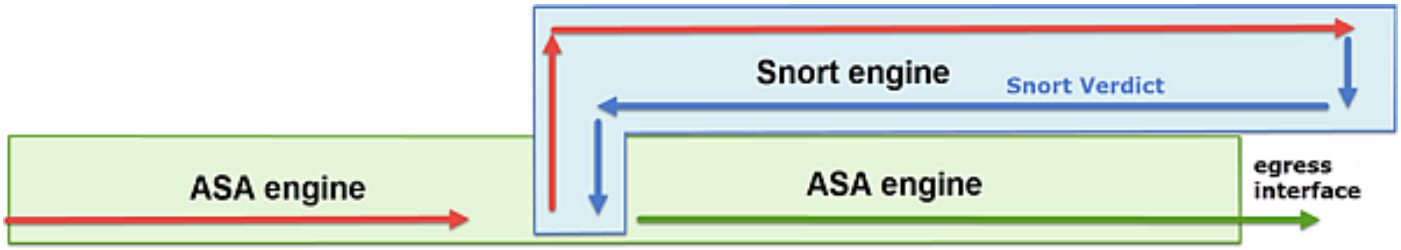
Diagramme du réseau



Informations générales

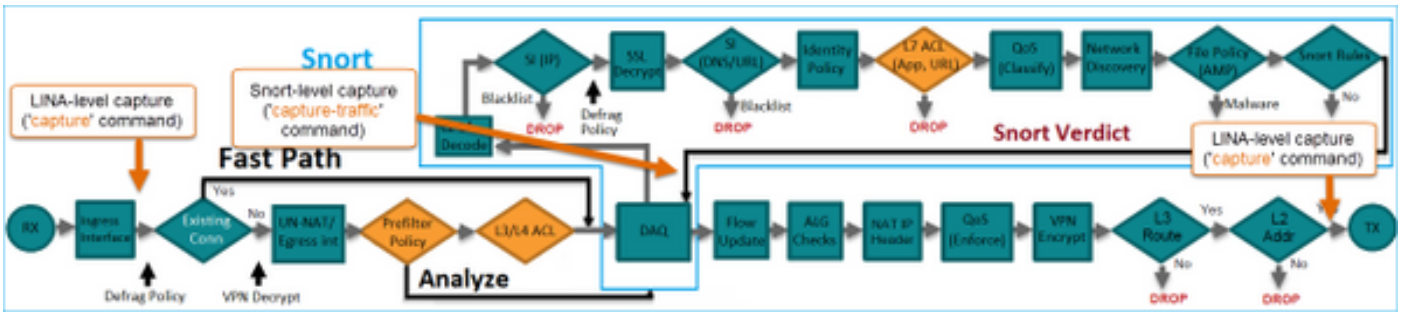
Traitement de paquets FTD

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 de LINA.
2. Si la stratégie exige 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 de LINA ou en avant le paquet basé sur le verdict du Snort.

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

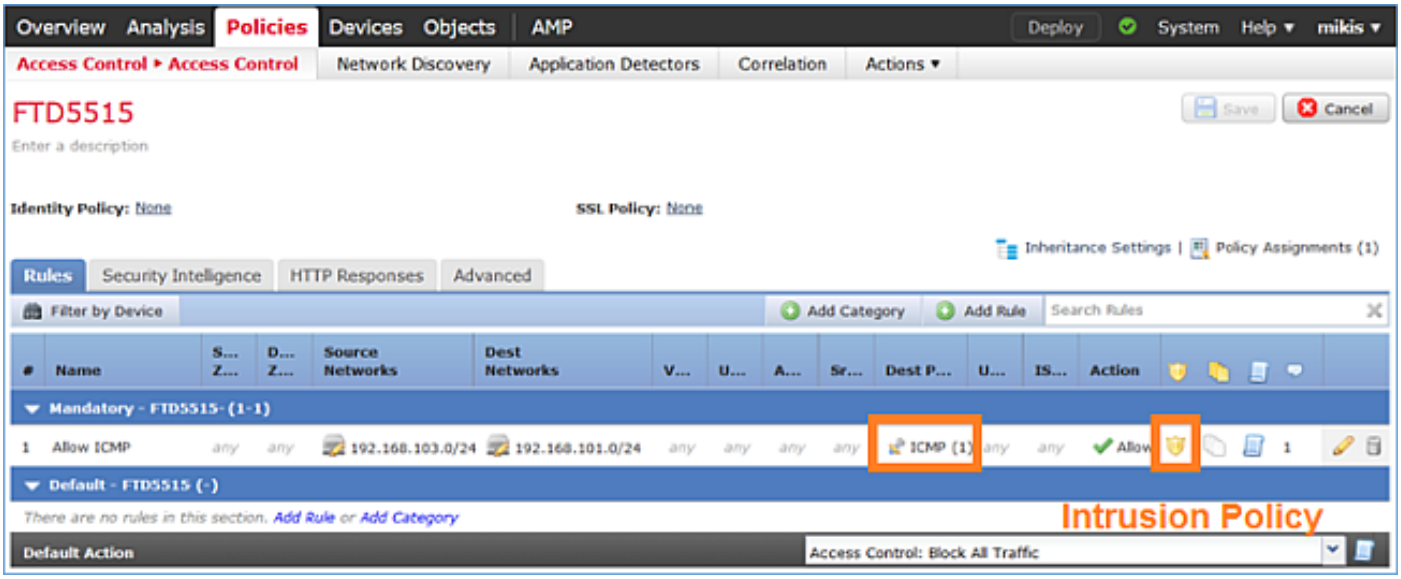


Configurez

Le travail avec reniflent des captures d'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-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 :

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

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

```
> capture-traffic

Please choose domain to capture traffic from:
```

```
  0 - br1
  1 - Router

Selection? 1

Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options:
12:52:34.749945 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0,
seq 1, length 80 12:52:34.749945 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo
reply, id 0, seq 1, length 80 12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-
gw.cisco.com: ICMP echo request, id 0, seq 2, length 80 12:52:34.759955 IP olab-vl647-
gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq 2, length 80 12:52:34.759955
IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo request, id 0, seq 3, length 80
12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-gw.cisco.com: ICMP echo reply, id 0, seq
3, length 80 12:52:34.759955 IP olab-vl603-gw.cisco.com > olab-vl647-gw.cisco.com: ICMP echo
request, id 0, seq 4, length 80 12:52:34.759955 IP olab-vl647-gw.cisco.com > olab-vl603-
gw.cisco.com: ICMP echo reply, id 0, seq 4, length 80
^C <- to exit press CTRL + C
```

Le travail avec reniflent des captures d'engine

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-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. Cinglez par le FTD et vérifiez la capture sortie :

```
> 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
```

Vous pouvez utiliser - l'option **n** 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-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 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 192.168.101.1
```

```
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

Pour quitter après avoir capturé 10 paquets :

```
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
```

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 192.168.101.1 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.

>
```

Travail avec des captures d'engine FTD LINA

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 destination	192.168.101.1
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 :

```
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
```

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 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
```

Travail avec des captures d'engine FTD LINA – Exportez une capture par l'intermédiaire du HTTP

Conditions requises

Exportez les captures rentrées le scénario précédent utilisant un navigateur.

Solution

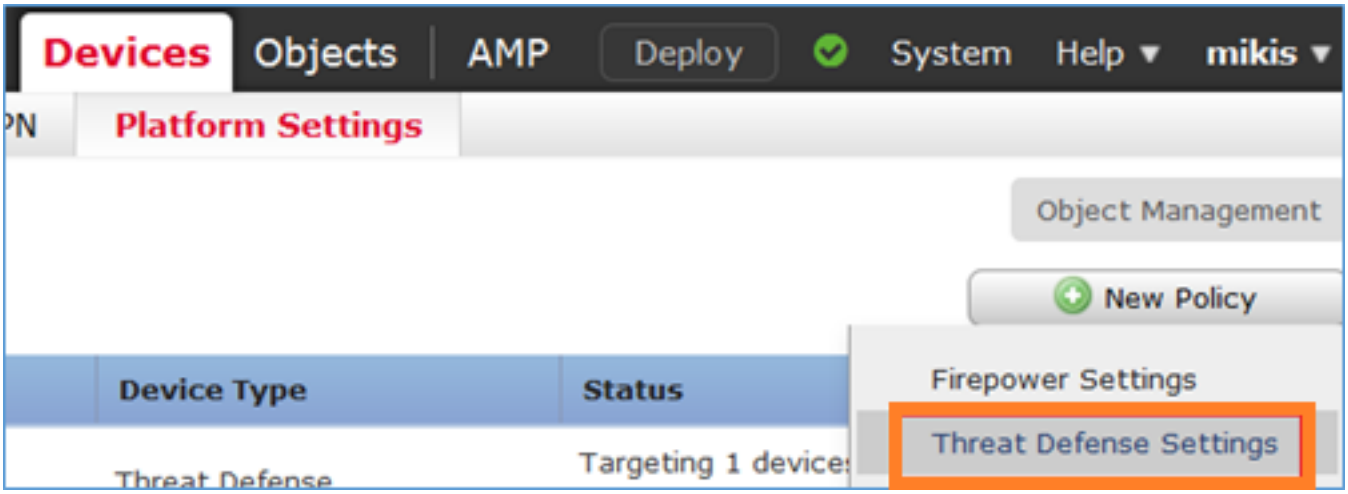
Afin d'exporter les captures utilisant le navigateur là est le besoin :

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

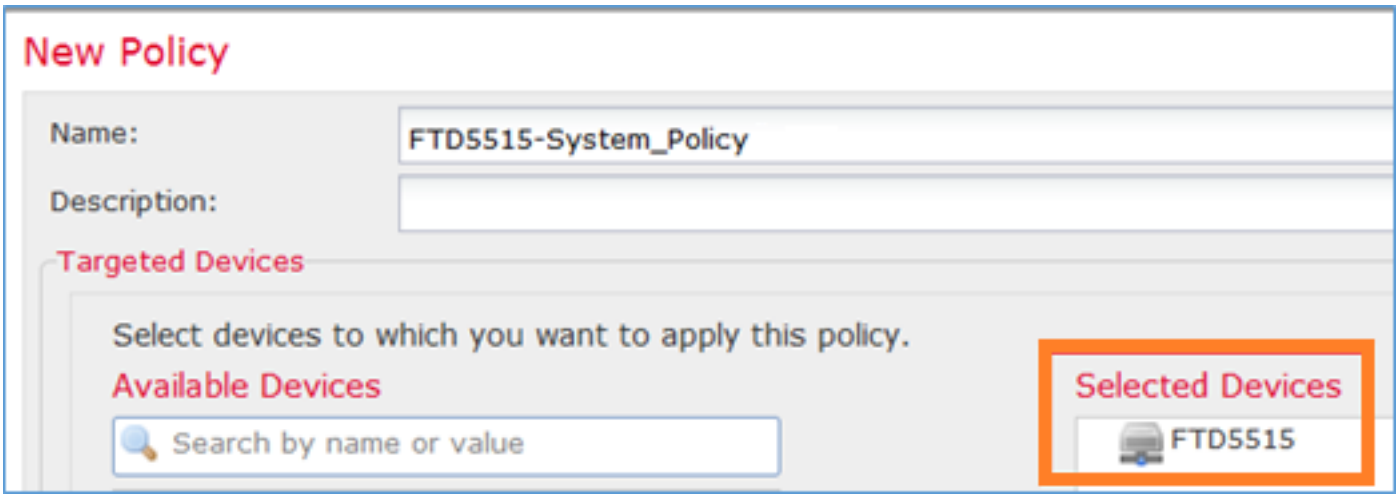
Par défaut le serveur HTTPS est désactivé et aucun accès n'est permis :

```
> show running-config http

>
```

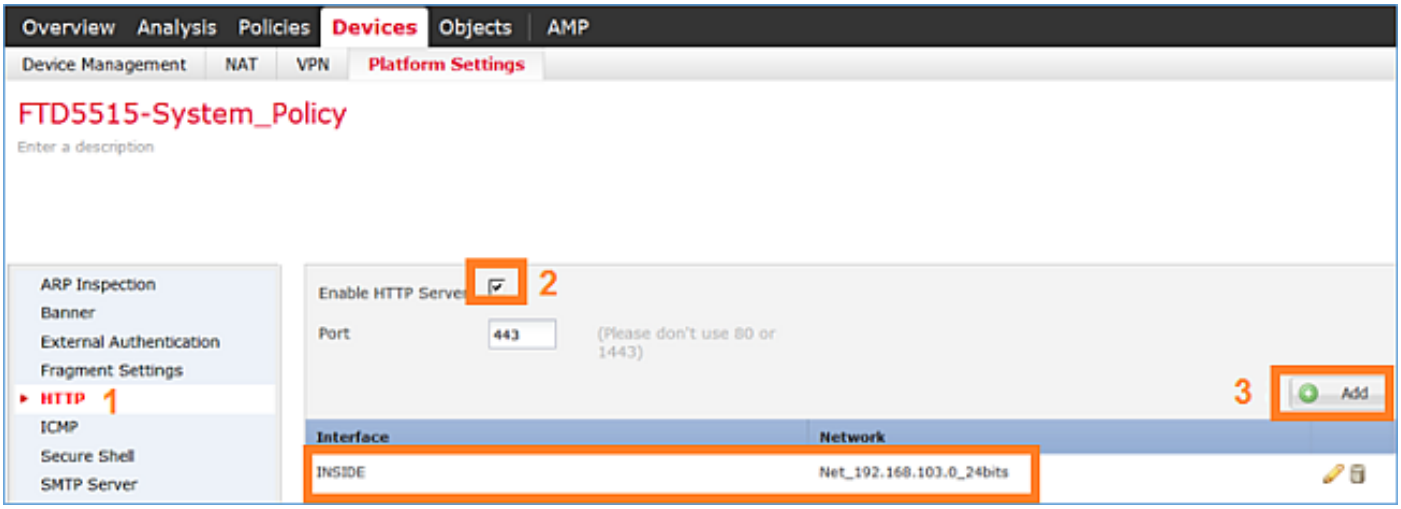
Étape 1. Naviguez vers des **périphériques > des configurations de plate-forme,** cliquez sur en fonction la **nouvelle stratégie** et sélectionnez les **configurations de défense contre des menaces :**



Spécifiez la cible de nom de stratégie et de périphérique :



Étape 2. Activez le serveur HTTPS et ajoutez le réseau que vous voulez être permis pour accéder au périphérique FTD au-dessus de HTTPS :



Sauvegardez et **déployez-vous.**

Pendant le déploiement de stratégie vous pouvez activer **mettez au point le HTTP** afin de voir commencer de service HTTP :

```
> debug http 255
```

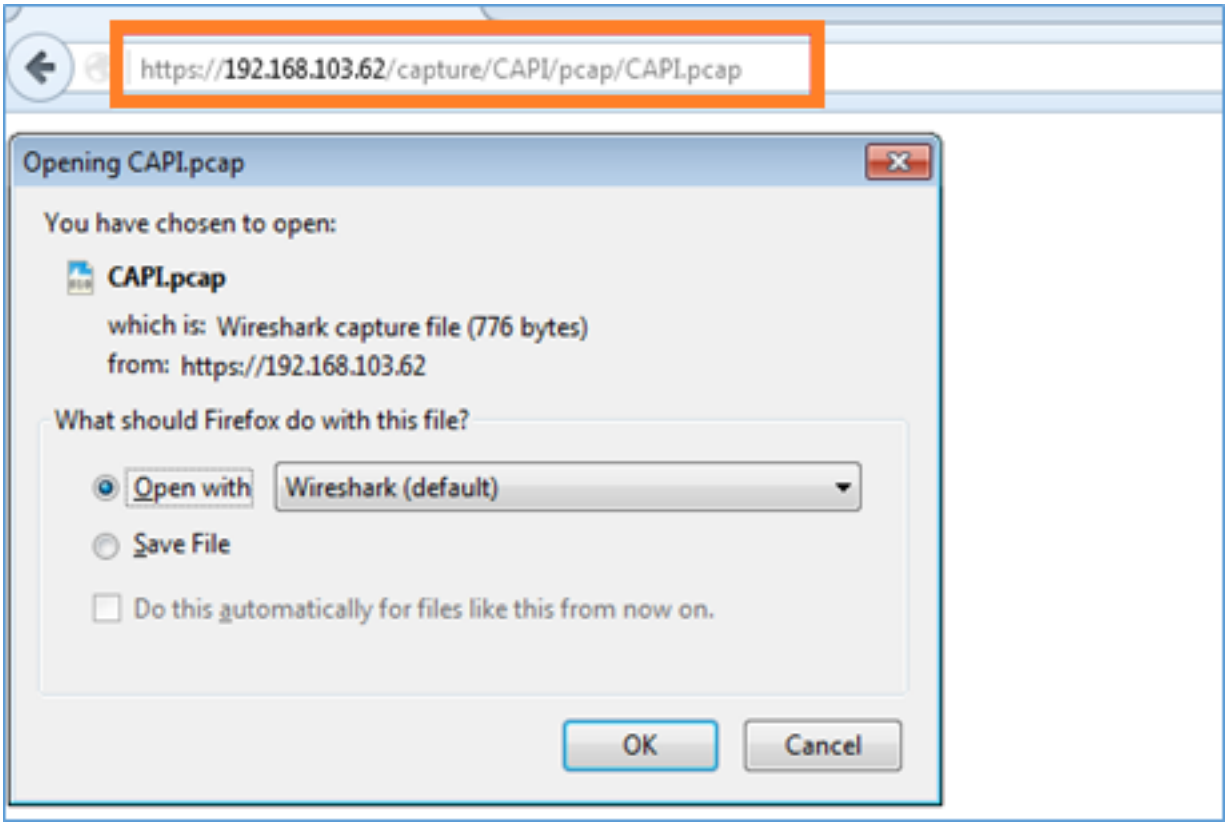
```
debug http enabled at level 255.
http_enable: Enabling HTTP server HTTP server starting.
```

Le résultat sur FTD CLI :

```
> unebug all
> show run http
http server enable http 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

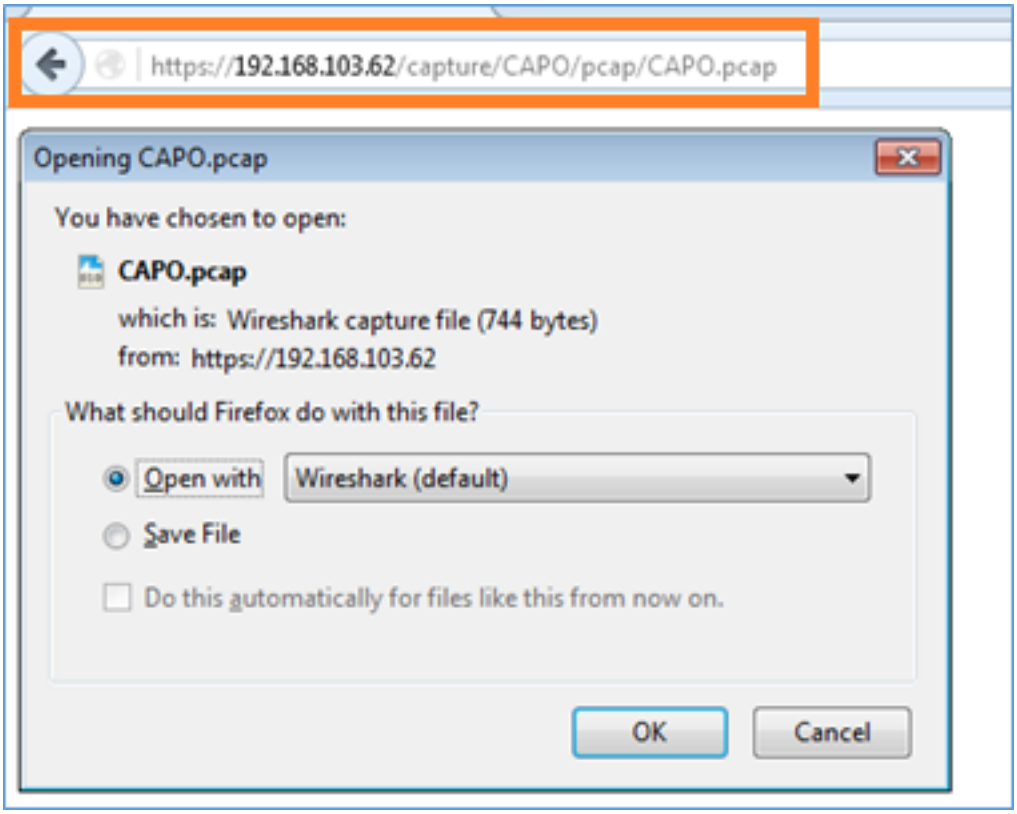


Pour la référence

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



Travail avec des captures d'engine FTD LINA – Exportez une capture par l'intermédiaire de 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.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 à un serveur 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#
```

Exporter une capture à un serveur 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#
```

Travail avec des captures d'engine FTD LINA – Tracez un vrai paquet du trafic

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 les mots clé « de **détail de suivi** » et spécifiez la quantité de paquets que vous voulez être tracé. 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
```

Les paquets capturés :

```
> 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
```

La sortie suivante affiche 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 de LINA (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

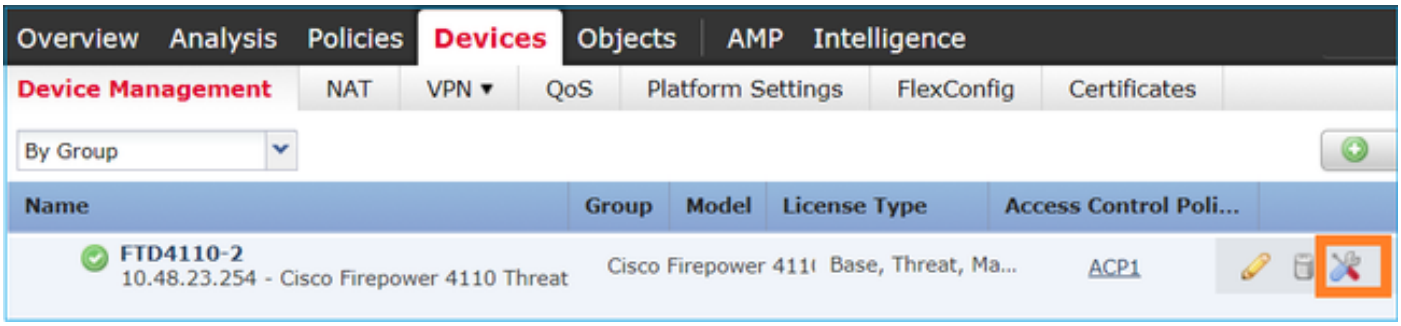
```
> show capture CAPI2 packet-number 1 trace detail
8 packets captured
```

```
   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
>
```

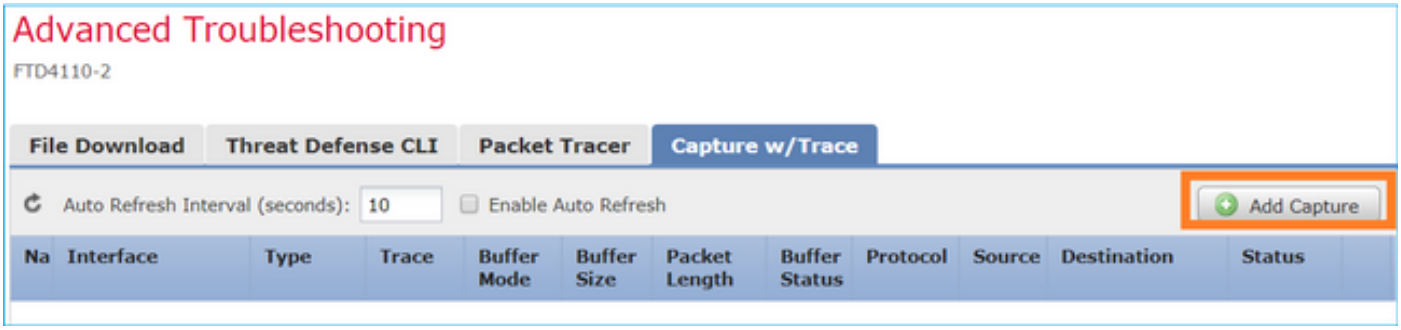
L'outil de capture dans des versions de logiciel Post-6.2 FMC

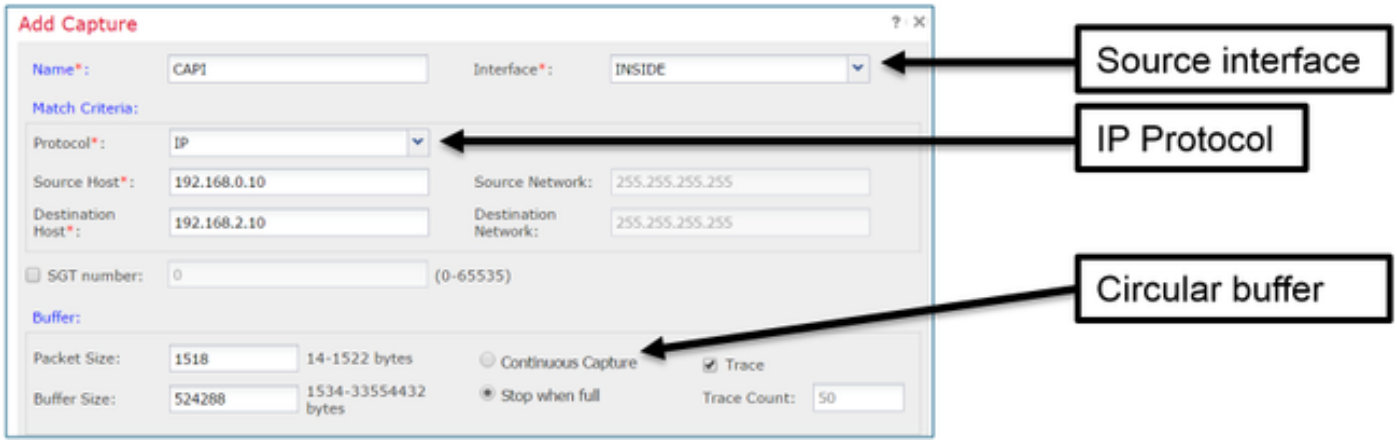
Dans la version FMC 6.2.x un nouvel assistant de capture de paquet a été présenté. Naviguez vers les **périphériques > la Gestion de périphériques** et sélectionnez l'icône de **dépannage**.

Sélectionnez alors le **dépannage** et finalement la **capture avancés w/Trace.**



Choisi **ajoutez la capture** pour créer une capture FTD :



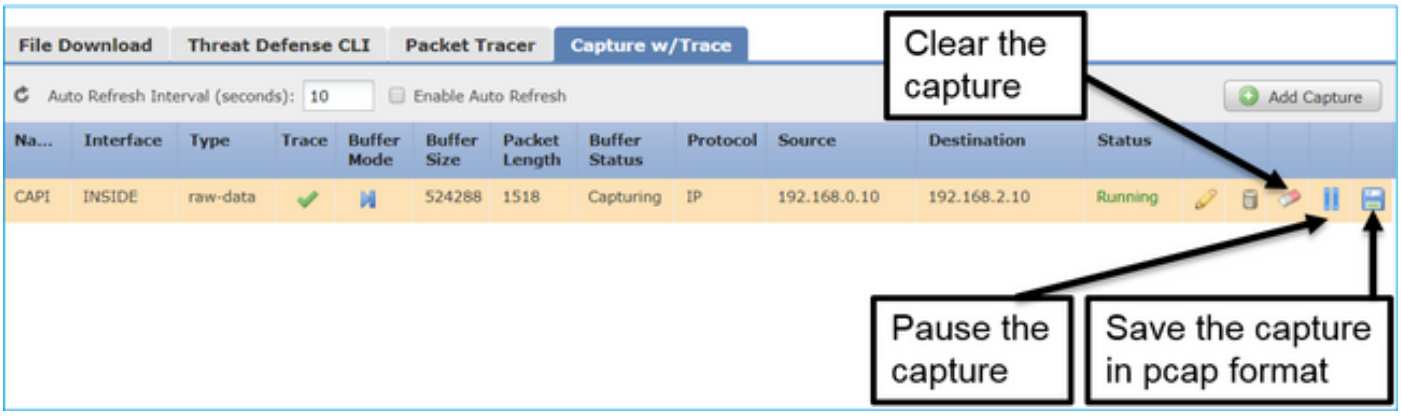


Limites du courant FMC UI

- Ne peut pas spécifier des ports de Src et de Dst
- Seulement des protocoles fondamentaux IP peuvent être appariés
- Ne peut pas activer la capture pour des baisses d'ASP d'engine de LINA

Contournement – Utilisez le FTD CLI.

Dès que vous appliquerez une capture à partir de FMC UI la capture s'exécute :

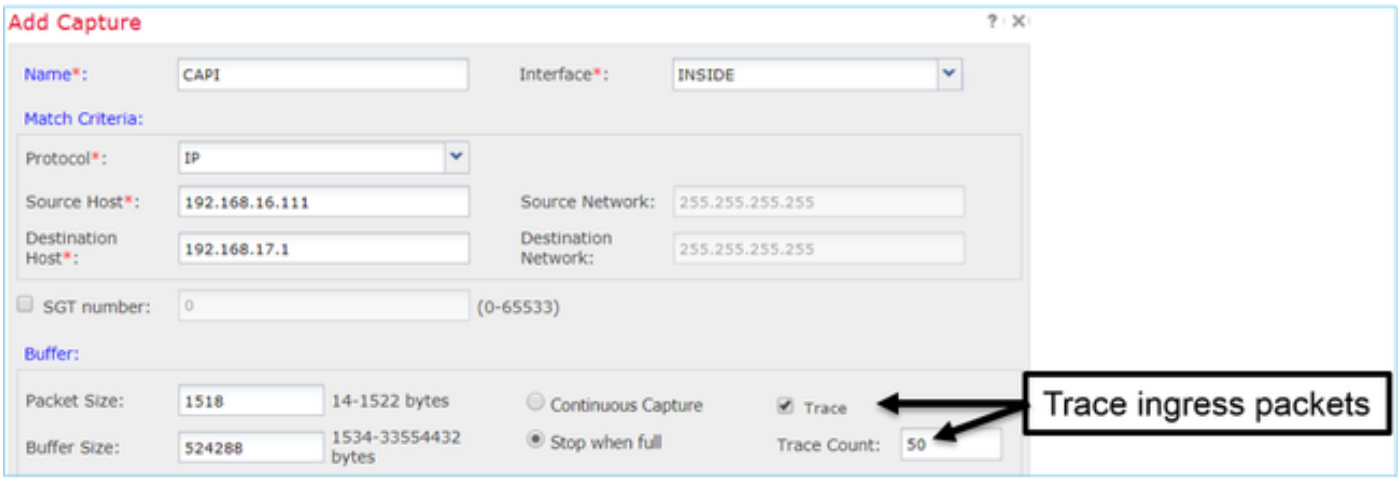


La capture sur FTD CLI :

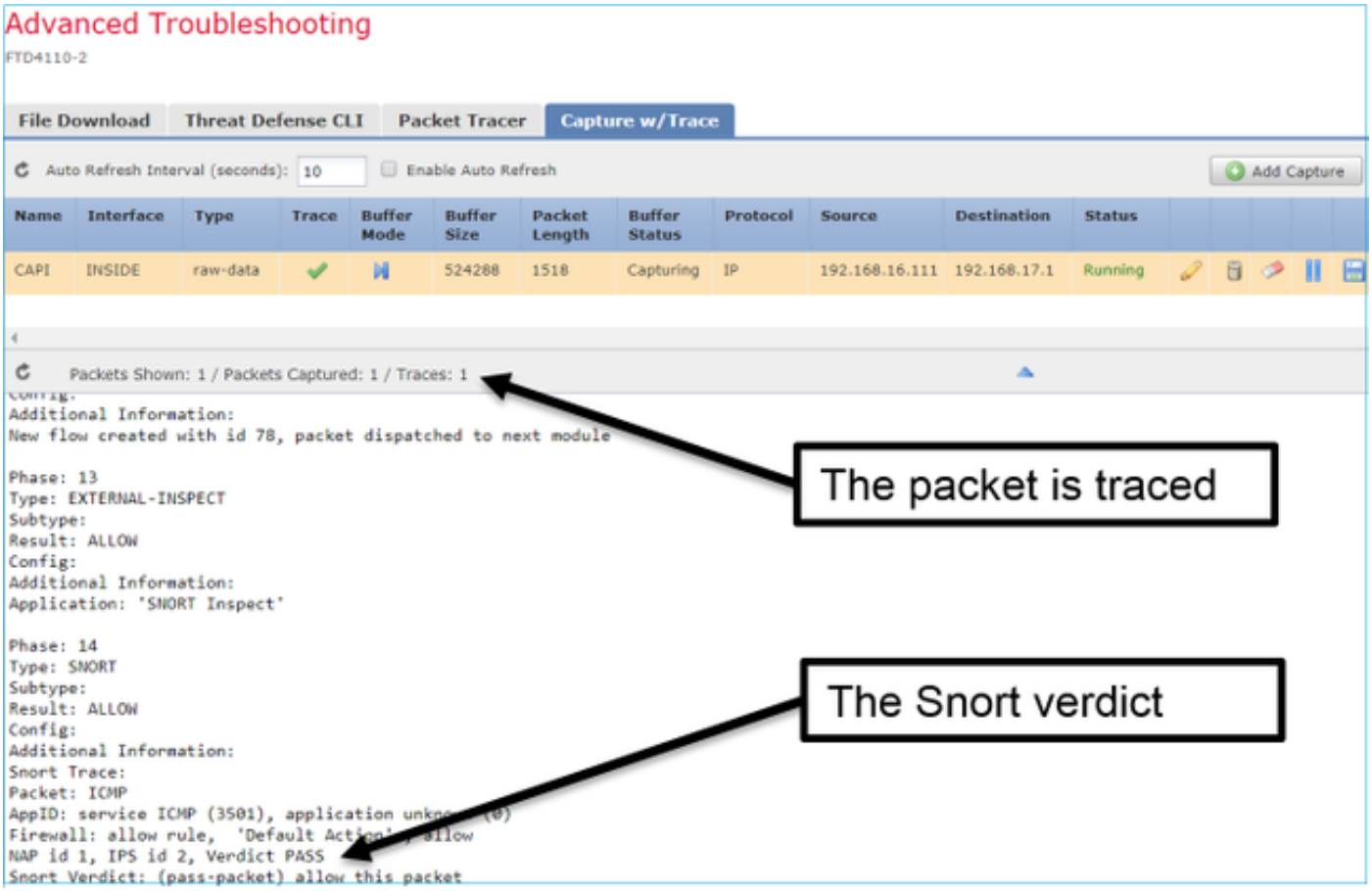
```
> show capture
capture CAPI%intf=INSIDE% type raw-data trace interface INSIDE [Capturing - 0 bytes]
  match ip host 192.168.0.10 host 192.168.2.10
>
```

Tracez un vrai paquet sur Post-6.2 FMC

Sur FMC 6.2.x l'assistant de la **capture w/Trace** laisse capturer et tracer de vrais paquets sur FTD :



Vous pouvez vérifier le paquet tracé dans FMC UI :



L'utilitaire FTD Packet Tracer

Conditions requises

Utilisez l'utilitaire de Packet Tracer pour l'écoulement suivant et vérifiez 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

Packet Tracer génèrera un **paquet virtuel.** Comme il peut voir au-dessous du paquet est un sujet pour renifler l'inspection. Une capture prise en même temps à niveau reniflé (le capture-**trafic**) affiche la requête d'écho d'ICMP :

```
> packet-tracer input INSIDE icmp 192.168.103.1 8 0 192.168.101.1

Phase: 1
Type: CAPTURE
```

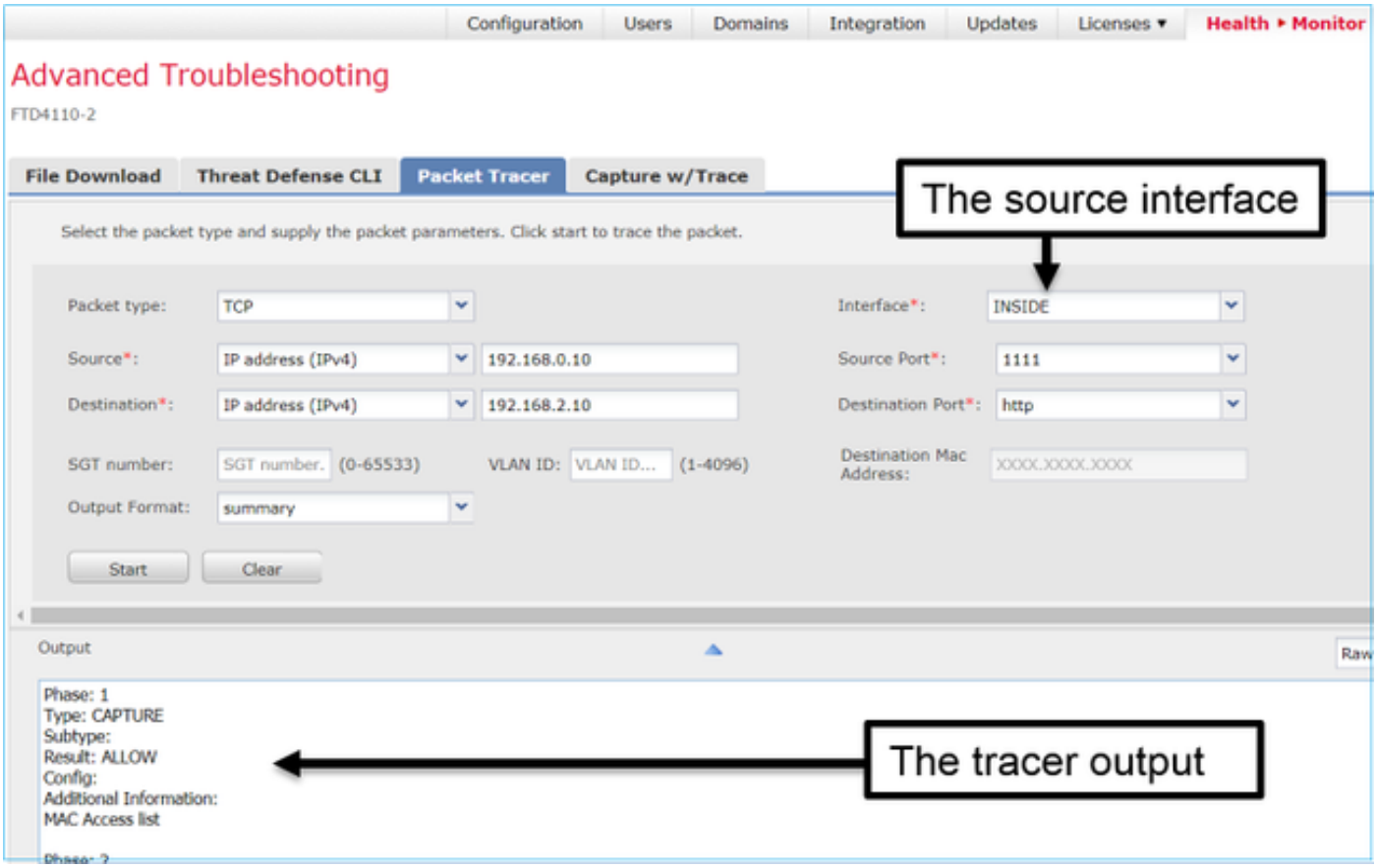
```
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

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 will be sent to snort for additional processing where a
verdict will be 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 niveau reniflé pendant le test de traceur de paquets affiche le paquet virtuel :

```
> 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
```

L'outil de Packet Tracer UI dans des versions de logiciel Post-6.2 FMC

Dans la version FMC 6.2.x l'outil de **Packet Tracer** UI a été introduit. L'outil est accessible de la même manière que l'outil de capture et te permet pour exécuter Packet Tracer sur FTD du FMC UI :



Informations connexes

- Guide de référence des commandes de défense contre des menaces de FirePOWER
- Notes en version système de FirePOWER, version 6.1.0
- Guide de configuration de défense contre des menaces de Cisco FirePOWER pour le gestionnaire de périphérique de FirePOWER, version 6.1
- **Support et documentation techniques - Cisco Systems**