Dépannage du chemin de données Firepower Phase 2 : Couche DAQ

Contenu

Introduction

Cet article fait partie d'une série d'articles qui expliquent comment dépanner systématiquement le chemin de données sur les systèmes Firepower pour déterminer si les composants de Firepower peuvent affecter le trafic. Reportez-vous à l'article Présentation pour obtenir des informations sur l'architecture des plates-formes Firepower et des liens vers les autres articles de dépannage du chemin de données.

Dans cet article, nous allons examiner la deuxième étape du dépannage du chemin de données Firepower : la couche DAQ (Data Aquisition).

Guide de la plate-forme

Le tableau suivant décrit les plates-formes couvertes par cet article.

Nom du code de la plate-forme	Description	Applicable Matériel Plates-formes	Notes
SFR	ASA avec module Firepower Services	Gamme ASA-5500-X	S/O

	(SFR) installé.		
FTD (tous)	S'applique à toutes les plates-formes Firepower Threat Defense (FTD)	Gamme ASA-5500-X, plates-formes de pare-feu de nouvelle génération virtuelles, FPR-2100, FPR-9300, FPR-4100	S/O
FTD (non SSP et FPR-2100)	Image FTD installée sur un ASA ou une plate-forme virtuelle	Gamme ASA-5500-X, plates-formes de pare-feu de nouvelle génération virtuelles, FPR-2100	S/O
FTD (SSP)	FTD installé en tant que périphérique logique sur un châssis basé sur Firepower eXtensible Operative System (FXOS)	FPR-9300, FPR-4100	La gamme 2100 n'utilise pas le gestionnaire de châssis FXOS

Dépannage de la phase DAQ Firepower

La couche DAQ (Data Aquisition) est un composant de Firepower qui traduit les paquets en une forme que snort peut comprendre. Il gère initialement le paquet lorsqu'il est envoyé au snort. Par conséquent, si les paquets sont en train d'entrer, mais pas de sortir, le dispositif Firepower ou le dépannage d'entrée de paquets n'a pas donné de résultats utiles, le dépannage DAQ peut être utile.

Capture du trafic au niveau de la couche DAQ

Pour obtenir l'invite à partir de laquelle exécuter la capture, vous devez d'abord vous connecter à l'adresse IP SFR ou FTD à l'aide de SSH.

> **Note**: Sur les périphériques FPR-9300 et 4100, entrez **connect ftd** en premier, pour finir à la deuxième **>** invite. Vous pouvez également utiliser SSH dans l'adresse IP du gestionnaire de châssis FXOS, puis entrer **connect module 1 console**, suivi de **connect ftd**.

Cet article explique comment collecter des captures de paquets au niveau DAQ Firepower.

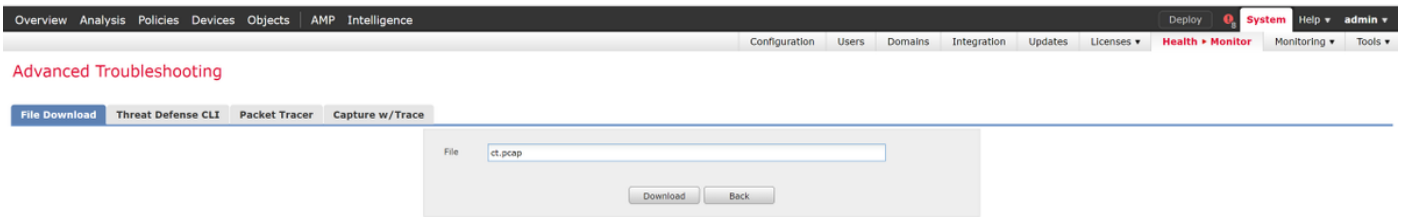
Notez que la syntaxe n'est pas la même que celle de la commande **capture** utilisée sur ASA ainsi que le côté LINA de la plate-forme FTD. Voici un exemple de capture de paquets DAQ exécutée à partir d'un périphérique FTD :

```
> system support capture-traffic

Please choose domain to capture traffic from:
  0 - br1
  1 - Router
  2 - my-inline inline set


Selection? 2


Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
Options: -s 1518 -w ct.pcap

> expert
admin@ciscoasa:~$ ls /ngfw/var/common/
ct.pcap
```

Comme le montre la capture d'écran ci-dessus, une capture au format PCAP appelé ct.pcap a été écrite dans le répertoire **/ngfw/var/common** (**/var/common** sur la plate-forme SFR). Ces fichiers de capture peuvent être copiés hors du périphérique Firepower à partir de l'invite > en utilisant les instructions de l'article mentionné ci-dessus.

Sinon, dans Firepower Management Center (FMC) version 6.2.0 et ultérieure, accédez à **Périphériques > Gestion des périphériques**. Cliquez ensuite sur le bouton en regard du périphérique en question, puis **Dépannage avancé > Téléchargement de fichier**.

Vous pouvez ensuite entrer le nom du fichier de capture et cliquer sur Télécharger.



Comment contourner Firepower

Si Firepower voit le trafic, mais qu'il a été déterminé que les paquets ne quittent pas le périphérique ou qu'il y a un autre problème avec le trafic, l'étape suivante consisterait à contourner la phase d'inspection Firepower pour confirmer que l'un des composants Firepower abandonne le trafic. Ci-dessous se trouve une ventilation de la façon la plus rapide d'avoir le contournement du trafic Firepower sur les différentes plates-formes.

SFR - Placez le module Firepower en mode surveillance uniquement

Sur l'ASA qui héberge le SFR, vous pouvez placer le module SFR en mode moniteur uniquement via l'interface de ligne de commande (CLI) ASA ou Cisco Adaptive Security Device Manager (ASDM). Cela entraîne l'envoi d'une copie des paquets actifs uniquement au module SFR.

Pour placer le module SFR en mode moniteur uniquement via l'interface de ligne de commande ASA, la carte de classe et la carte de stratégie utilisées pour la redirection SFR doivent d'abord être déterminées en exécutant la commande **show service-policy sfr**.

```
# show service-policy sfr

Global policy:
 Service-policy: global_policy
   Class-map: sfr
     SFR: card status Up, mode fail-open
       packet input 10000, packet output 9900, drop 100, reset-drop 0
```

Le résultat montre que la carte de stratégie global_policy applique l'action fail-open sfr sur la carte de classe « sfr ».

> **Note**: « fail-close » est également un mode dans lequel le SFR peut fonctionner, mais il n'est pas aussi couramment utilisé car il bloque tout le trafic si le module SFR est arrêté ou ne répond pas.

Afin de placer le module SFR en mode moniteur uniquement, vous pouvez émettre ces commandes pour annuler la configuration SFR actuelle et entrer la configuration moniteur uniquement :

```
# configure terminal
(config)# policy-map global_policy
(config-pmap)# class sfr
(config-pmap-c)# no sfr fail-open
(config-pmap-c)# sfr fail-open monitor-only

INFO: The monitor-only mode prevents SFR from denying or altering traffic.

(config-pmap-c)# write memory
Building configuration...
```

Une fois le module placé en mode moniteur uniquement, il peut être vérifié dans la sortie **show service-policy sfr**.

```
# sh service-policy sfr

Global policy:
 Service-policy: global_policy
   Class-map: sfr
     SFR: card status Up, mode fail-open monitor-only
       packet input 0, packet output 100, drop 0, reset-drop 0
```

> **Note**: Pour remettre le module SFR en mode en ligne, exécutez la commande **no sfr fail-open monitor-only** à partir de l'invite **(config-pmap-c)#** ci-dessus, suivie de **sfr {fail-open | fail-close}** qui était à l'origine là.

Vous pouvez également placer le module en mode surveillance uniquement via l'ASDM en accédant à **Configuration > Firewall > Service Policy Rules.** Cliquez ensuite sur la règle en question. Ensuite, accédez à la page **Actions de règle** et cliquez sur l'onglet **Inspection FirePOWER ASA**. Une fois sur place, le **moniteur uniquement** peut être sélectionné.

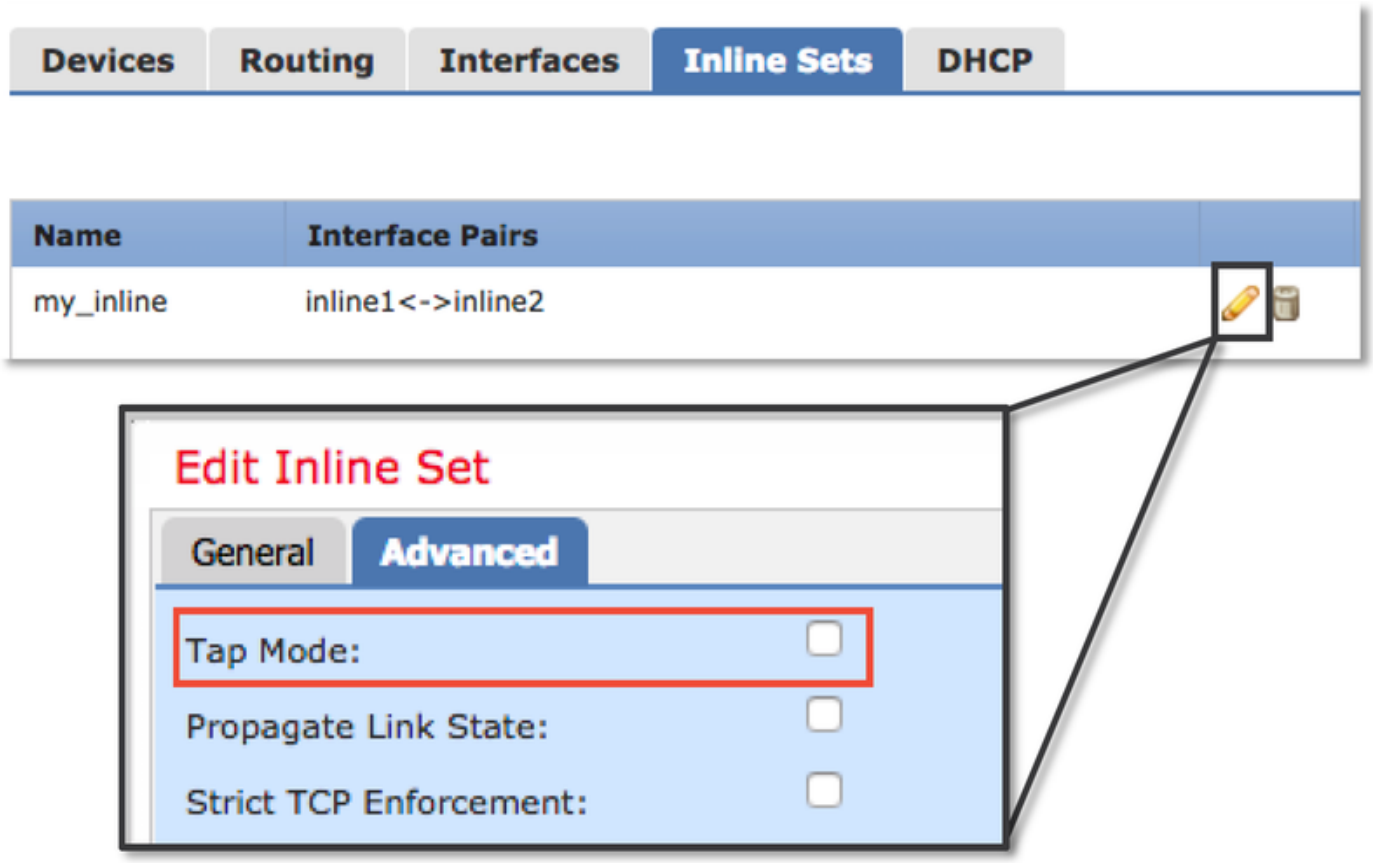
Si le problème de trafic persiste même après que le module SFR a été confirmé en mode moniteur uniquement, le module Firepower n'est pas à l'origine du problème. Packet Tracer peut ensuite être exécuté pour diagnostiquer davantage les problèmes au niveau de l'ASA.

Si le problème ne se pose plus, l'étape suivante consisterait à dépanner les composants du logiciel Firepower.

FTD (all) - Placer les jeux en ligne en mode TAP

Si le trafic passe par des paires d'interfaces configurées dans des jeux en ligne, le jeu en ligne peut être placé en mode TAP. Cela entraîne essentiellement que Firepower n'agit pas sur le paquet en direct. Il ne s'applique pas au routeur ou au mode transparent sans jeux en ligne, car le périphérique doit modifier les paquets avant de les envoyer au prochain saut et ne peut pas être placé en mode de contournement sans abandonner le trafic. Pour le mode routé et transparent sans jeux en ligne, passez à l'étape packet tracer.

Pour configurer le mode TAP à partir de l'interface utilisateur FMC, accédez à **Devices > Device Management**, puis modifiez le périphérique en question. Sous l'onglet **Ensembles en ligne**, cochez l'option **Mode TAP**.



Si le mode TAP résout le problème, l'étape suivante consiste à dépanner les composants du logiciel Firepower.

Si le mode TAP ne résout pas le problème, le problème se situe en dehors du logiciel Firepower.

Packet Tracer peut ensuite être utilisé pour diagnostiquer le problème.

Utilisation de Packet Tracer pour dépanner le trafic simulé

Packet Tracer est un utilitaire permettant d'identifier l'emplacement d'une perte de paquets. C'est un simulateur, donc il effectue une trace d'un paquet artificiel.

SFR - Exécuter Packet Tracer sur l'interface de ligne de commande ASA

Voici un exemple d'exécution de packet-tracer sur l'interface de ligne de commande ASA pour le trafic SSH. Pour plus d'informations sur la syntaxe de la commande packet tracer, reportez-vous à cette section du guide de référence des commandes de la gamme ASA.

Dans l'exemple ci-dessus, nous voyons à la fois le module ASA et le module SFR permettant les paquets ainsi que des informations utiles sur la façon dont l'ASA gérerait le flux de paquets.

FTD (all) - Exécuter Packet Tracer sur la CLI FTD

Sur toutes les plates-formes FTD, la commande packet tracer peut être exécutée à partir de l'interface de ligne de commande FTD.

```
> packet-tracer input inside tcp 192.168.62.60 10000 10.10.10.10 ssh

Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list

Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.100.1 using egress ifc  outside
```

```
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268434433
access-list CSM_FW_ACL_ remark rule-id 268434433: ACCESS POLICY:
My_AC_Policy - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268434433: L7 RULE: Block urls
Additional Information:
 This packet will be sent to snort for additional processing where a verdict will
be reached

Phase: 4
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
 match any
policy-map global_policy
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:
```

```
Phase: 5
Type: NAT
Subtype:
Result: ALLOW
Config:
object network 62_network
 nat (inside,outside) dynamic interface
Additional Information:
Dynamic translate 192.168.62.60/10000 to 192.168.100.51/10000

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 8
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 9
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 612016, packet dispatched to next module
```

```
Phase: 11
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 12
Type: SNORT
Subtype:
Result: DROP
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 1821549761
Reputation: packet blacklisted, drop
Snort: processed decoder alerts or actions queue, drop
IPS Event: gid 136, sid 1, drop
Snort detect_drop: gid 136, sid 1, drop
NAP id 1, IPS id 0, Verdict BLACKLIST, Blocked by Reputation
Snort Verdict: (black-list) black list this flow
```

Dans cet exemple, Packet Tracer montre bien la raison de la perte. Dans ce cas, il s'agit de la liste noire IP de la fonction Security Intelligence dans Firepower qui bloque le paquet. L'étape suivante consisterait à dépanner le composant logiciel Firepower qui cause la perte.

Utilisation de Capture avec trace pour dépanner le trafic dynamique

Le trafic en direct peut également être suivi via la fonction de capture avec trace, disponible sur toutes les plates-formes via l'interface de ligne de commande. Voici un exemple d'exécution d'une capture avec trace sur le trafic SSH.

```
> capture ssh_traffic trace interface inside match tcp any any eq 22
> show capture ssh_traffic

7 packets captured

   1: 01:17:38.498906       192.168.62.70.48560 > 10.83.180.173.22: S 4250994241:4250994241(0) win 29200 <mss 1460,sackOK,timestamp 1045829951
0,nop,wscale 7>
   2: 01:17:38.510898       10.83.180.173.22 > 192.168.62.70.48560: S 903999422:903999422(0) ack 4250994242 win 17896 <mss 1380,sackOK,timestamp
513898266 1045829951,nop,wscale 7>
   3: 01:17:38.511402       192.168.62.70.48560 > 10.83.180.173.22: . ack 903999423 win 229 <nop,nop,timestamp 1045829956 513898266>
   4: 01:17:38.511982       192.168.62.70.48560 > 10.83.180.173.22: P 4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
   5: 01:17:38.513294       10.83.180.173.22 > 192.168.62.70.48560: . ack 4250994283 win 140 <nop,nop,timestamp 513898268 1045829957>
   6: 01:17:38.528125       10.83.180.173.22 > 192.168.62.70.48560: P 903999423:903999444(21) ack 4250994283 win 140 <nop,nop,timestamp 513898282
1045829957>
   7: 01:17:38.528613       192.168.62.70.48560 > 10.83.180.173.22: . ack 903999444 win 229 <nop,nop,timestamp 1045829961 513898282>
```

```
> show capture ssh_traffic packet-number 4 trace

7 packets captured

   4: 01:17:38.511982       192.168.62.70.48560 > 10.83.180.173.22: P
4250994242:4250994283(41) ack 903999423 win 229 <nop,nop,timestamp
1045829957 513898266>
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: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:
Found flow with id 626406, using existing flow

Phase: 4
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'
```

```
Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 4250994242, ack 903999423
AppID: service SSH (846), application unknown (0)
Firewall: starting rule matching, zone 1 -> 2, geo 0 -> 0, vlan 0, sgt 65535, user 2, icmpType 0, icmpCode 0
Firewall: trust/fastpath rule, id 268435458, allow
NAP id 1, IPS id 0, Verdict WHITELIST
Snort Verdict: (fast-forward) fast forward this flow

Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
```

Dans cet exemple, le quatrième paquet de la capture a été suivi, car il s'agit du premier paquet avec des données d'application définies. Comme indiqué, le paquet finit par être blanchi par le snort, ce qui signifie qu'aucune autre inspection du snort n'est nécessaire pour le flux, et autorisée globalement.

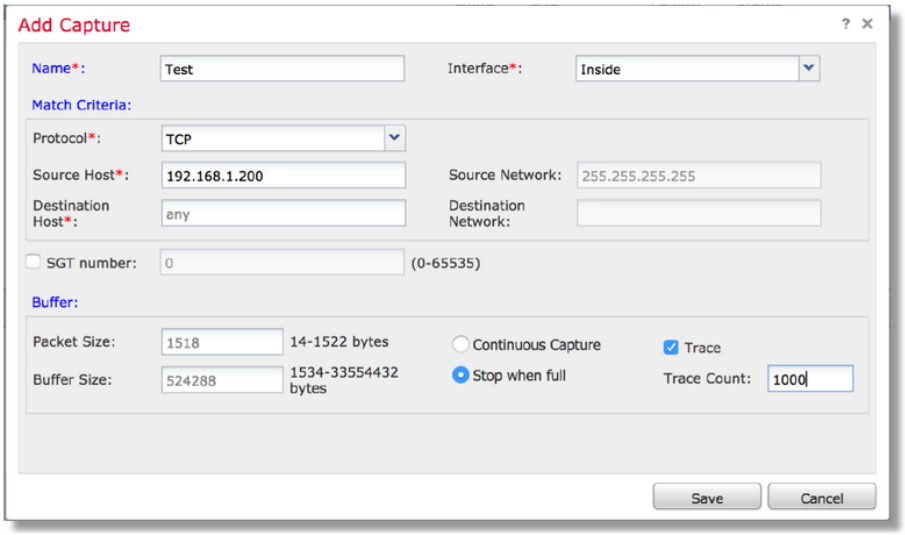
Pour plus d'informations sur la capture avec la syntaxe de trace, reportez-vous à cette section du guide de référence des commandes de la gamme ASA.

FTD (tous) - Exécution de la capture avec trace sur l'interface graphique de FMC

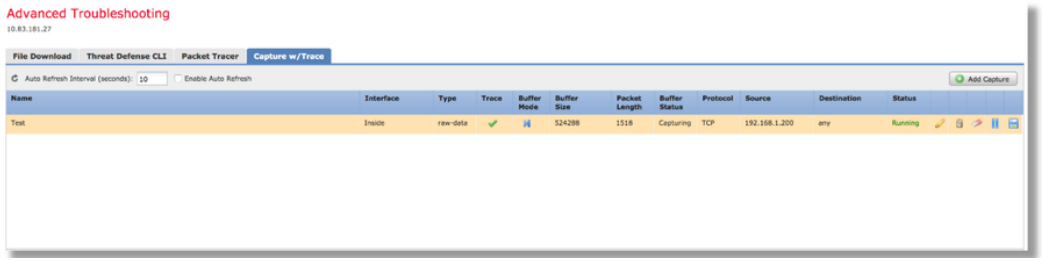
Sur les plates-formes FTD, la capture avec trace peut être exécutée sur l'interface FMC. Pour accéder à l'utilitaire, accédez à **Périphériques > Gestion des périphériques**.

Cliquez ensuite sur le bouton  en regard du périphérique en question, suivi de **Dépannage avancé > Capture avec suivi.**

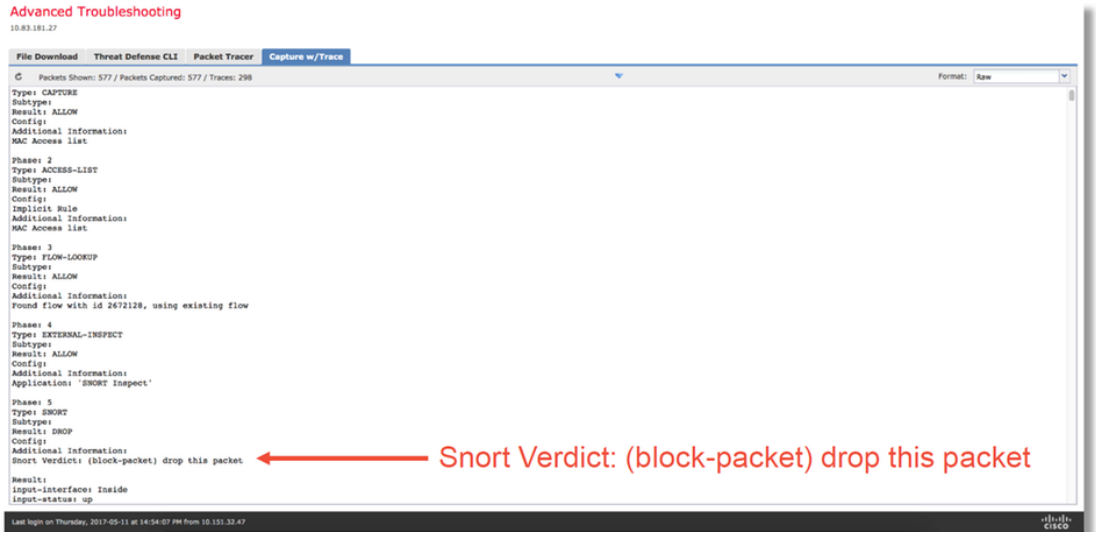
Vous trouverez ci-dessous un exemple d'exécution d'une capture avec trace via l'interface utilisateur graphique.



Clicking **Add Capture** button will display this popup window



View of all current captures



Example output shows the packet was blocked by Snort

Si la capture avec trace indique la cause de la perte de paquets, l'étape suivante consiste à dépanner les composants logiciels individuels.

S'il n'indique pas clairement la cause du problème, l'étape suivante consisterait à accélérer le chemin du trafic.

Création d'une règle PreFilter Fastpath dans FTD

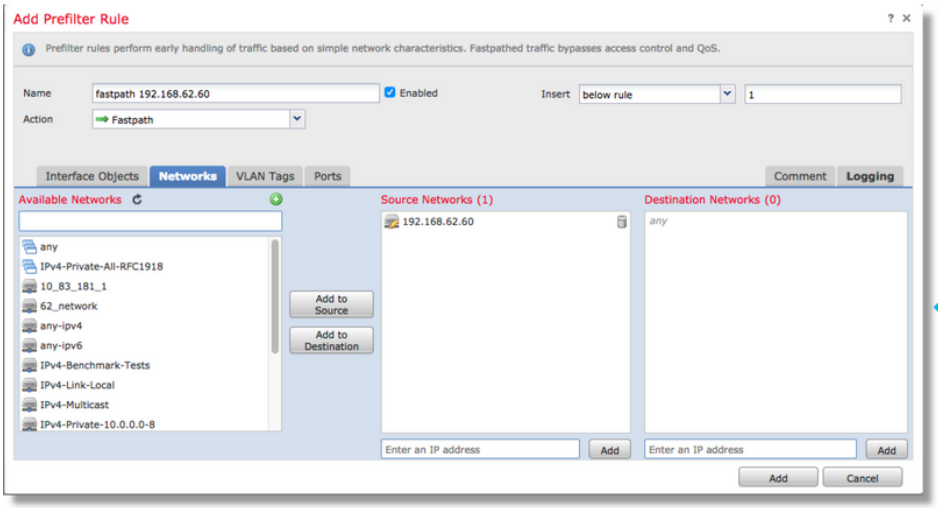
Sur toutes les plates-formes FTD, il existe une politique de pré-filtre, qui peut être utilisée pour détourner le trafic de l'inspection Firepower (snort).

Sur le FMC, cette option se trouve sous **Politiques > Contrôle d'accès > Préfiltre**. La stratégie de pré-filtre par défaut ne peut pas être modifiée. Une stratégie personnalisée doit donc être créée.

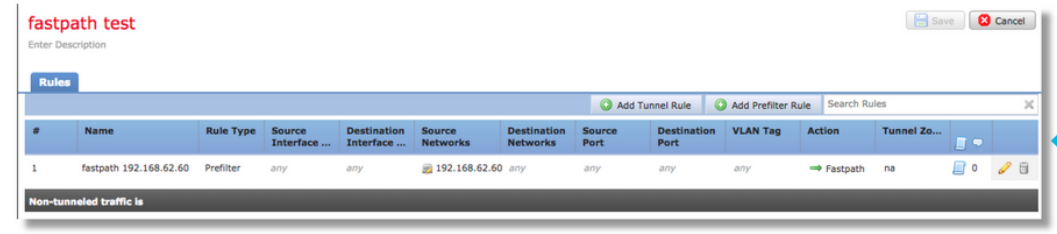
Par la suite, la nouvelle stratégie de préfiltre doit être associée à la stratégie de contrôle d'accès. Ceci est configuré dans l'onglet Avancé de la stratégie de contrôle d'accès dans la section

Paramètres de stratégie de préfiltre.

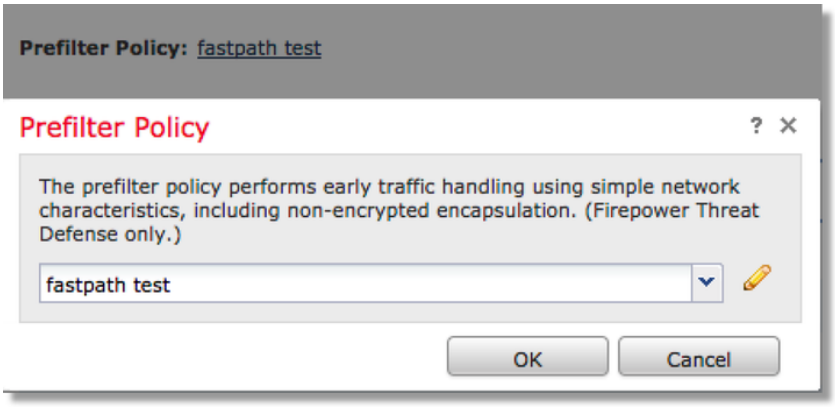
Voici un exemple de création d'une règle Fastpath dans une stratégie de préfiltre et de vérification du nombre de résultats.



Clicking **Add Prefilter Rule** button will display this popup window.



View of all rules in the **fastpath test** Prefilter policy



From AC policy make sure the Prefilter Policy is set to the custom Prefilter Policy

View of connection events matching prefilter rule

First Packet	Last Packet	Action	Reason	Initiator IP	Responder IP	Source Port / ICMP Type	Destination Port / ICMP Code	Prefilter Policy	Tunnel/Prefilter Rule
2017-05-15 16:05:14	2017-05-15 16:05:14	Fastpath		192.168.62.60	10.83.180.173	48480 / tcp	22 (ssh) / tcp	fastpath test	fastpath 192.168.62.60

[Cliquez ici](#) pour plus de détails sur l'opération et la configuration des stratégies de préfiltre.

Si l'ajout d'une stratégie de pré-filtre résout le problème de trafic, la règle peut être laissée en place si vous le souhaitez. Toutefois, aucune autre inspection n'est effectuée sur ce débit. Le dépannage ultérieur du logiciel Firepower devra être effectué.

Si l'ajout de la stratégie de préfiltre ne résout pas le problème, le paquet avec l'étape de suivi peut être exécuté à nouveau pour suivre le nouveau chemin du paquet.

Données à fournir au TAC

Données	Instructions
Sortie de commande	Reportez-vous à cet article pour obtenir des instructions.
Captures de paquets	Pour ASA/LINA : https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-ne configure-asa-00.html Pour Firepower : http://www.cisco.com/c/en/us/support/docs/security/sourcefire-firepower-80 sourcefire-00.html
Sortie ASA 'show tech'	Connectez-vous à l'interface de ligne de commande ASA et faites enregistrer la session de t commande show techcommand, puis fournissez le fichier de sortie de session de terminal a Ce fichier peut être enregistré sur disque ou sur un système de stockage externe à l'aide de show tech | redirection disk0:/show_tech.log
Dépannage du fichier à partir du périphérique Firepower inspectant le trafic	http://www.cisco.com/c/en/us/support/docs/security/sourcefire-defense-center/117663-techn

Étape suivante

S'il a été déterminé qu'un composant logiciel Firepower est la cause du problème, l'étape suivante consisterait à exclure systématiquement chaque composant, en commençant par Security Intelligence.

Cliquez ici pour passer au guide suivant.