Clarifier les actions de règle de contrôle d'accès FTD

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Produits associés
- Informations générales
  - Mode de déploiement de la politique de contrôle d'accès
- Configurer
  - Actions disponibles pour la politique de contrôle d'accès
  - Interactions entre les politiques de contrôle d'accès et de préfiltre
  - Action Block (blocage) de la politique de contrôle d'accès
    - Scénario 1. Abandon LINA précoce
    - Scénario 2. Abandon en raison du verdict Snort
  - Action Block (blocage) de la politique de contrôle d'accès avec réinitialisation
  - Action Allow (autorisation) de la politique de contrôle d'accès
    - Scénario 1. Action Autoriser ACP (conditions L3/L4)
    - Scénario 2. Action Autoriser ACP (conditions L3-7)
    - Scénario 3. Renifler le verdict Fast-Forward avec Allow
  - Action Trust (confiance) de la politique de contrôle d'accès
    - Scénario 1. Action de confiance ACP
    - Scénario 2. Action d'approbation ACP (sans SI, QoS et politique d'identité)
  - Action Prefilter Policy Block (blocage de la politique de préfiltre)
  - Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre)
    - Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre) (ensemble en ligne)
    - Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre) (ensemble en ligne avec dérivateur)
  - Action Prefilter Policy Analyze (analyse de la politique de préfiltre)
    - Scénario 1. Préfiltrer l'analyse avec la règle de blocage ACP
    - Scénario 2. Préfiltrer l'analyse avec la règle d'autorisation ACP
    - Scénario 3. Préfiltrer l'analyse avec la règle d'approbation ACP
    - Scénario 4. Préfiltrer l'analyse avec la règle d'approbation ACP
  - Action Monitor (surveillance) de la politique de contrôle d'accès
  - Action Interactive Block (blocage interactif) de la politique de contrôle d'accès
  - Action Interactive Block (blocage interactif) de la politique de contrôle d'accès avec réinitialisation
  - Connexions secondaires et sténopés de Cisco Firepower Threat Defense (FTD)
  - Règles de Cisco Firepower Threat Defense (FTD)
- Résumé
- Informations connexes

Introduction

Ce document décrit les différentes actions disponibles sur la politique de contrôle d'accès et la politique de préfiltre de Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Décharge de flux
- Captures de paquets sur les appliances Firepower Threat Defense
- Packet Tracer et capture avec options de trace sur les appareils FTD

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firepower 4110 Threat Defense version 6.4.0 (build 113) et 6.6.0 (build 90)
- Centre de gestion Firepower Management Center (FMC) version 6.4.0 (build 113) et 6.6.0 (build 90)

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.

Produits associés

Ce document peut être utilisé avec les versions matérielles et logicielles suivantes :

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X

- FPR1000, FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), machine virtuelle à base de noyau (KVM)
- Module de routeur à services intégrés (ISR)
- Logiciel Firepower Threat Defense (FTD) versions 6.1.x et ultérieures

---

Remarque : Le flux de déchargement est pris en charge uniquement sur les instances natives des applications Cisco Adaptative Security Appliance (ASA) et Cisco Firepower Threat Defense (FTD) et sur les plateformes FPR4100 et FPR9300. Les instances de conteneur FTD ne prennent pas en charge le déchargement de flux.

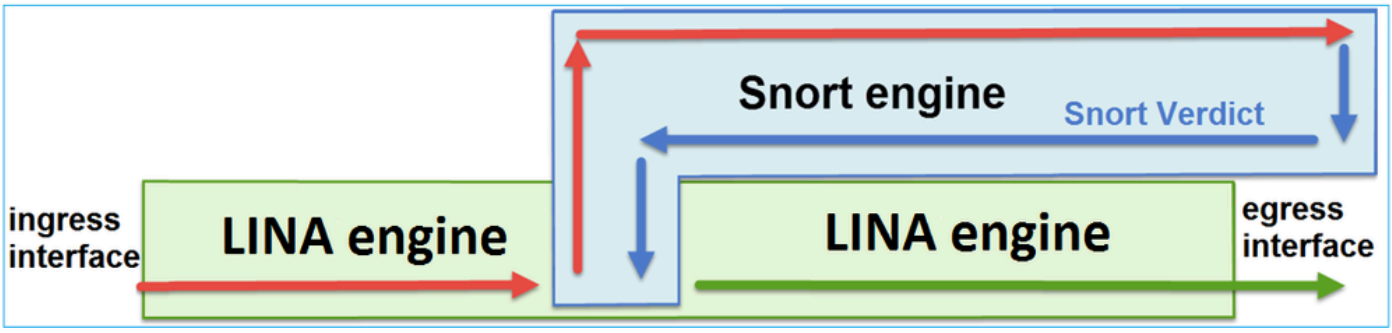
Informations générales

Le fonctionnement en arrière-plan de chaque action est examiné, ainsi que ses interactions avec d'autres fonctionnalités telles que le déchargement de flux et les protocoles qui ouvrent des connexions secondaires.

FTD est une image logicielle unifiée composée de deux moteurs principaux :

- Moteur LINA
- Moteur du renifleur

Cette figure illustre l'interaction entre les deux moteurs :



- Un paquet entre dans l’interface d’entrée et est géré par le moteur LINA.
- Si elle est requise par la politique FTD, le paquet est inspecté par le moteur Snort.
- Le moteur Snort renvoie un verdict (liste d'autorisation ou liste de blocage) pour le paquet.
- Le moteur LINA abandonne ou transfère le paquet en fonction du verdict du renifleur.

Mode de déploiement de la politique de contrôle d’accès

La stratégie FTD est configurée sur le FMC lorsque la gestion off-box (à distance) est utilisée ou lorsque le gestionnaire local Firepower Device Manager (FDM) est utilisé. Dans les deux cas, la politique de contrôle d'accès est déployée comme :

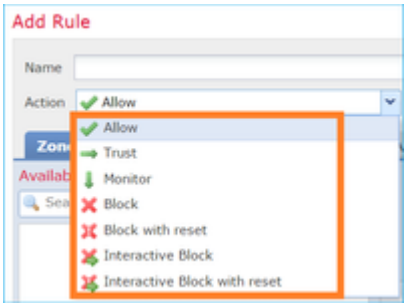
- Une liste de contrôle d'accès (ACL) globale nommée CSM_FW_ACL_ au moteur FTD LINA.
- Des règles de contrôle d'accès dans le fichier /ngfw/var/sf/detection_engines/<UUID>/ngfw.rules du moteur FTD du renifleur.

Configurer

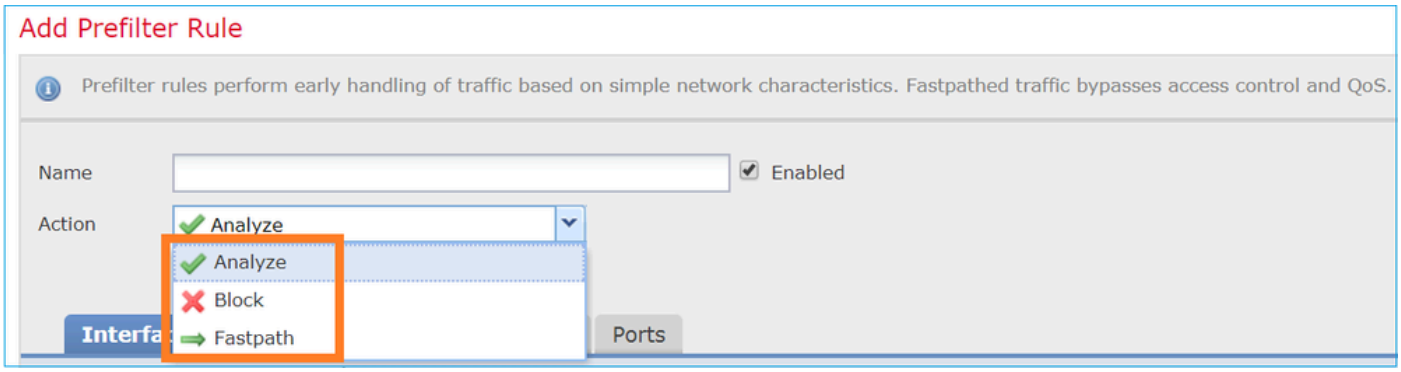
Actions disponibles pour la politique de contrôle d'accès

L'ACP FTD contient une ou plusieurs règles et chaque règle peut avoir l'une de ces actions :

- Allow
- Trust
- Monitor
- Block
- Block with reset
- Interactive Block
- Interactive Block with reset



De même, une stratégie de préfiltrage peut contenir une ou plusieurs règles et les actions possibles :



Interactions entre les politiques de contrôle d'accès et de préfiltre

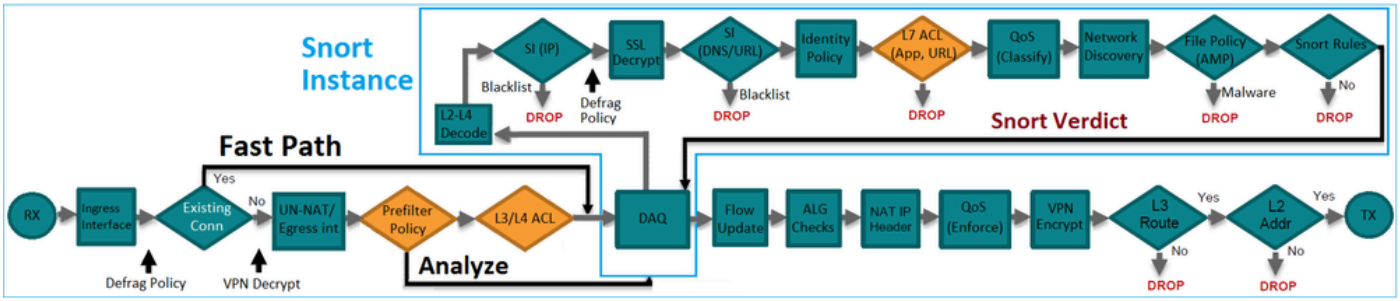
La stratégie de préfiltrage a été introduite dans la version 6.1 et a deux objectifs principaux :

Elle permet l'inspection du trafic en tunnel où le moteur FTD LINA vérifie l'en-tête IP externe tandis que le moteur du renifleur vérifie l'en-tête IP interne. Plus précisément, dans le cas du trafic tunnelisé (par exemple GRE), les règles de la politique de préfiltrage agissent toujours sur les en-têtes externes. Tandis que les règles de l'ACP sont toujours applicables aux sessions internes (en-têtes internes).

Le trafic en tunnel se reporte à ces protocoles :

- GRE
- IP-en-IP
- IPv6-en-IP
- Port Teredo 3544

Le contrôle d'accès anticipé (EAC) permet au flux de contourner complètement le moteur Snort :



Les règles de préfiltrage sont déployées sur FTD en tant qu'éléments de contrôle d'accès (ACE) de couche 3/4 et précèdent les ACE configurées de couche 3/4 :

```
firepower# show access-list
access-list CSM_FW_ACL_ line 1 remark rule-id 268434457: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 268434457: RULE: Fastpath_Rule1
access-list CSM_FW_ACL_ line 3 advanced trust ip host 192.168.75.16 any rule-id 268434457 event-log both (hitcnt=0)
access-list CSM_FW_ACL_ line 4 remark rule-id 268434456: PREFILTER POLICY: FTD_Prefilter_Policy
access-list CSM_FW_ACL_ line 5 remark rule-id 268434456: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 6 advanced permit ipinip any any rule-id 268434456 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 7 advanced permit 41 any any rule-id 268434456 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 8 advanced permit gre any any rule-id 268434456 (hitcnt=2) 0x52c7a066
access-list CSM_FW_ACL_ line 9 advanced permit udp any any eq 3544 rule-id 268434456 (hitcnt=0) 0xcf6309bc
access-list CSM_FW_ACL_ line 10 remark rule-id 268434445: ACCESS POLICY: FTD5506-1 - Mandatory/1
access-list CSM_FW_ACL_ line 12 advanced deny ip host 10.1.1.1 any rule-id 268434445 event-log flow-start (hitcnt=0) 0x8bf72c63
access-list CSM_FW_ACL_ line 14 remark rule-id 268434434: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 15 advanced permit ip any any rule-id 268434434 (hitcnt=410) 0xa1d3780e
```

Prefilter Rules

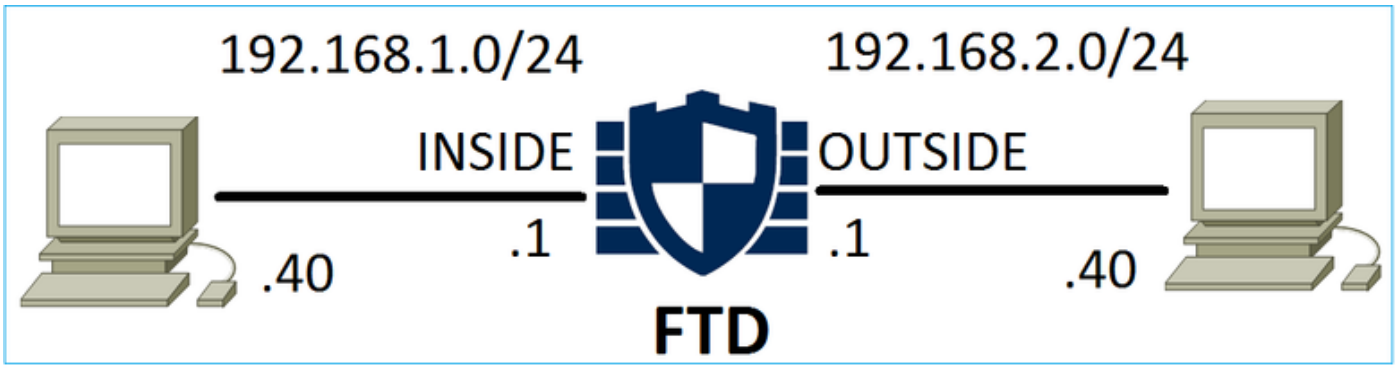
Tunnel Prefilter Rules

L3/L4 ACEs

Remarque : Règles de préfiltrage v/s ACP = première correspondance appliquée.

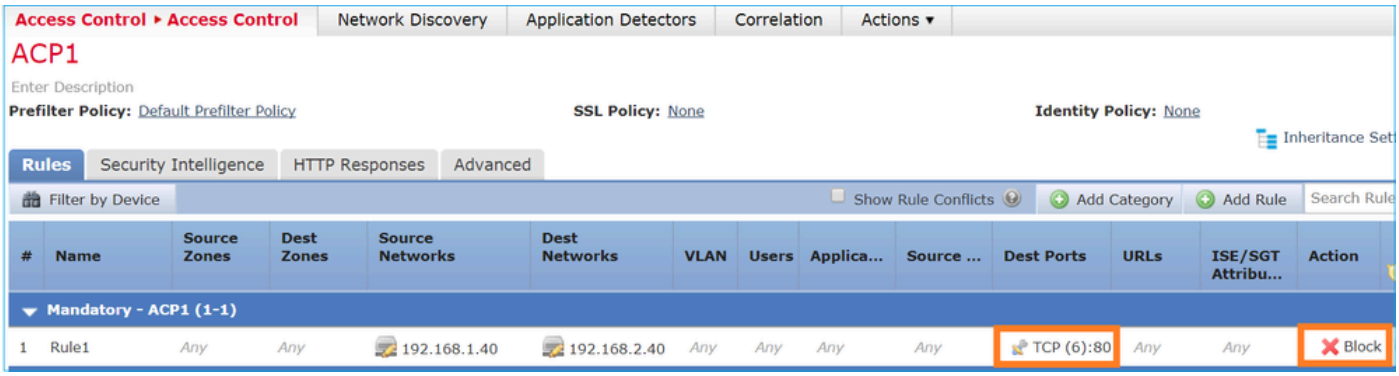
Action Block (blocage) de la politique de contrôle d'accès

Examinez la topologie :



Scénario 1. Abandon LINA précoce

L'ACP contient une règle de blocage qui utilise une condition L4 (Port de destination TCP 80) :



La politique déployée dans le renifleur :

<#root>

```
268435461

deny

 any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

La politique déployée dans LINA. Notez que la règle est poussée comme une action deny :

<#root>

```
firepower#

show access-list

…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced

deny

 tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268435461 event-log flow-start (hitcnt=0) 0x614
```

Vérifiez le comportement :

Lorsque l'hôte A (192.168.1.40) tente d'ouvrir une session HTTP vers l'hôte B (192.168.2.40), les paquets de synchronisation TCP (SYN) sont abandonnés par le moteur FTD LINA et n'atteignent pas le moteur Snort ou la destination :

<#root>

```
firepower#

show capture

capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface

INSIDE

 [Capturing -

430 bytes

]
  match ip host 192.168.1.40 any
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface
```

OUTSIDE

[Capturing -

0 bytes

]
match ip host 192.168.1.40 any

<#root>

firepower#

show capture CAPI

```
   1: 11:08:09.672801  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1
   2: 11:08:12.672435  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1
   3: 11:08:18.672847  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1
   4: 11:08:30.673610  192.168.1.40.32789 > 192.168.2.40.80: S 3249160620:3249160620(0) win 2920 <mss 1
```

<#root>

firepower#

show capture CAPI packet-number 1 trace

```
   1: 11:08:09.672801  192.168.1.40.32789 > 192.168.2.40.80:
```

S

```
 3249160620:3249160620(0) win 2920 <mss 1460,sackOK,timestamp 4060517 0>
...

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
```

access-list CSM_FW_ACL_ advanced deny tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268435461 e

```
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L4 RULE: Rule1
```

Additional Information:

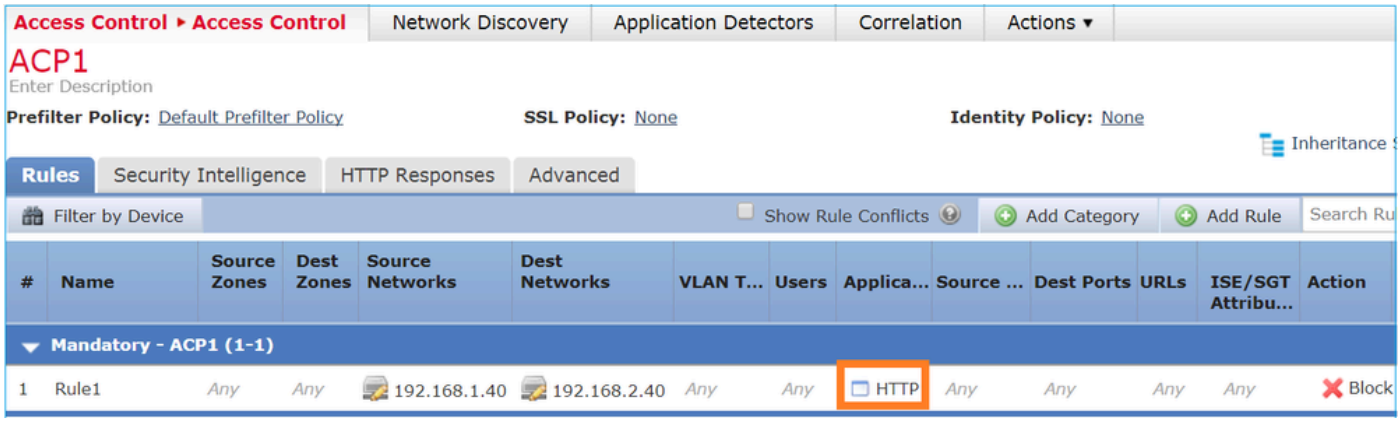
<- No Additional Information = No Snort Inspection

```
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
```

Drop-reason: (acl-drop) Flow is denied by configured rule

Scénario 2. Abandon en raison du verdict Snort

L'ACP contient une règle de blocage qui utilise une condition L7 (Application HTTP) :



La politique déployée dans le renifleur :

<#root>

```
268435461
```

deny

```
 any 192.168.1.40 32 any any 192.168.2.40 32 any any any
```

(appid 676:1)

Appid 676:1 = HTTP

La politique déployée dans LINA:

> Remarque : La règle est poussée en tant qu'action d'autorisation parce que le moteur LINA ne peut pas déterminer que la session utilise HTTP. Sur FTD, le mécanisme de détection d'application est dans le moteur Snort.

<#root>

```
firepower#

show access-list

…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced

permit

 ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461 (hitcnt=0) 0xb788b786
```

Pour une règle de blocage qui utilise Application comme condition, la trace d'un paquet réel montre que la session est abandonnée par le moteur LINA en raison du verdict du moteur Snort.

> Remarque : Pour que le moteur Snort puisse déterminer l'application, il doit inspecter quelques paquets (généralement 3 à 10, ce qui dépend du décodeur d'application). Ainsi, quelques paquets sont autorisés à passer par le FTD et sont transmis à sa destination. Les paquets autorisés sont toujours soumis à la vérification de la stratégie d'intrusion basée sur l'option Stratégie d'accès > Avancé > Stratégie d'intrusion utilisée avant que la règle de contrôle d'accès soit déterminée.

Vérifiez le comportement :

Lorsque l'hôte A (192.168.1.40) tente d'établir une session HTTP avec l'hôte B (192.168.2.40), la capture d'entrée LINA affiche :

<#root>

```
firepower#

show capture CAPI
```

```
8 packets captured

   1: 11:31:19.825564  192.168.1.40.32790 > 192.168.2.40.80:

S

 357753151:357753151(0) win 2920 <mss 1460,sackOK,timestamp 5450579 0>
   2: 11:31:19.826403  192.168.2.40.80 > 192.168.1.40.32790:

S

 1283931030:1283931030(0)

ack

 357753152 win 2896 <mss 1380,sackOK,timestamp 5449236 5450579>
   3: 11:31:19.826556  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199)

ack

 1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>
   4: 11:31:20.026899  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack 1283931031 w
   5: 11:31:20.428887  192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199) ack 1283931031 w
 ...
```

La saisie de sortie :

<#root>

```
firepower#

show capture CAPO

5 packets captured

   1: 11:31:19.825869  192.168.1.40.32790 > 192.168.2.40.80: S 1163713179:1163713179(0) win 2920 <mss 1
   2: 11:31:19.826312  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 wi
   3: 11:31:23.426049  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 wi
   4: 11:31:29.426430  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 wi
   5: 11:31:41.427208  192.168.2.40.80 > 192.168.1.40.32790: S 354801457:354801457(0) ack 1163713180 wi
```

La trace indique que le premier paquet (TCP SYN) est autorisé par le moteur Snort car le verdict de détection d'application n'a pas encore été atteint :

<#root>

firepower#

show capture CAPI packet-number 1 trace

   1: 11:31:19.825564 192.168.1.40.32790 > 192.168.2.40.80:

S

 357753151:357753151(0) win 2920 <mss 1460,sackOK,timestamp 5450579 0>
...

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461
access-list CSM_FW_ACL_ remark rule-id 268435461: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268435461: L7 RULE: Rule1

Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

...
Phase: 10
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:

New flow created with id 23194

, packet dispatched to next module
…
Phase: 12
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, seq 357753151
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType
Firewall:

pending rule-matching, id 268435461, pending AppID

NAP id 1, IPS id 0,

Verdict PASS

Snort Verdict: (pass-packet) allow this packet

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

Action: allow

Il en va de même pour le paquet TCP SYN/ACK :

<#root>

firepower#

show capture CAPO packet-number 2 trace

2: 11:31:19.826312 192.168.2.40.80 > 192.168.1.40.32790:

S

354801457:354801457(0)

ack

1163713180 win 2896 <mss 1460,sackOK,timestamp 5449236 5450579>
…

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:

Found flow with id 23194, using existing flow

…

Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, SYN, ACK, seq 1283931030, ack 357753152
AppID: service unknown (0), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType

Firewall: pending rule-matching, id 268435461, pending AppID

NAP id 1, 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: INSIDE
output-status: up
output-line-status: up

Action: allow

Snort retourne un verdict DROP une fois qu'une inspection du troisième paquet est terminée :

<#root>

firepower#

show capture CAPI packet-number 3 trace

   3: 11:31:19.826556 192.168.1.40.32790 > 192.168.2.40.80: P 357753152:357753351(199)

ack

 1283931031 win 2920 <nop,nop,timestamp 5450580 5449236>

Phase: 3
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Config:
Additional Information:

Found flow with id 23194, using existing flow

Phase: 5
Type: SNORT
Subtype:

Result: DROP

Config:

```
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 357753152, ack 1283931031

AppID: service HTTP (676)

, application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0, vlan 0, sgt 65535, user 9999997, url ht

Firewall: block rule, id 268435461, drop

Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0,

Verdict BLOCKLIST, Blocked by Firewall


Snort Verdict: (block-list) block list this flow


Result:
input-interface: INSIDE
input-status: up
input-line-status: up
Action: drop

Drop-reason: (firewall) Blocked by the firewall preprocessor
```

Vous pouvez également exécuter la commande system support trace à partir du mode FTD CLISH. Cet outil offre deux fonctions :

- Il affiche le verdict Snort pour chaque paquet lorsqu'il est envoyé à la bibliothèque d'acquisition de données (DAQ) et vu dans LINA. La bibliothèque est un composant situé entre le moteur FTD LINA et le moteur de renifleur.
- Il vous permet d'exécuter system support firewall-engine-debug en même temps pour voir ce qui se passe dans le moteur Snort lui-même.

⚠ Mise en garde : Vous devez utiliser les commandes de support du système sous la direction du support de Cisco, à l'exception des commandes documentées dans le guide des commandes de support du système ssl-client-hello- , qui est pour une utilisation générale.

En outre, utilisez toujours les filtres appropriés et ne laissez pas la commande s'exécuter indéfiniment, car cela peut affecter les performances du périphérique.

Voici un exemple de résultat :

<#root>

>

system support trace

Please specify an IP protocol:

tcp

Please specify a client IP address:

192.168.1.40

Please specify a client port:
Please specify a server IP address:

192.168.2.40

Please specify a server port:
Enable firewall-engine-debug too? [n]:

y

Monitoring packet tracer debug messages

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32791 6 Packet:

TCP, SYN

, seq 2620409313
192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 New session
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone first wit
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vla
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall:

pending rule-matching, 'Rule1', pending AppID

192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0,

Verdict PASS

Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32791 6 Packet:

TCP, SYN, ACK

, seq 3700371680, ack 2620409314

192.168.2.40-80 - 192.168.1.40-32791 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone first wit
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vla
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 pending rule order 2, 'Rule1', AppID
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall:

pending rule-matching, 'Rule1', pending AppID

192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0,

Verdict PASS

Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32791 6 Packet:

TCP, ACK

, seq 2620409314, ack 3700371681
192.168.2.40-80 - 192.168.1.40-32791 6 AppID:

service HTTP (676)

, application unknown (0)
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Starting with minimum 2, 'Rule1', and SrcZone first wit
192.168.1.40-32791 > 192.168.2.40-80 6 Firewall: starting rule matching, zone -1 -> -1, geo 0(0) -> 0,

url http://192.168.2.40/128k.html

192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0

match rule order 2, 'Rule1', action Block

192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 deny action
192.168.1.40-32791 > 192.168.2.40-80 6

Firewall: block rule, 'Rule1', drop

192.168.1.40-32791 > 192.168.2.40-80 6 Snort: processed decoder alerts or actions queue, drop
192.168.1.40-32791 > 192.168.2.40-80 6 AS 1 I 0 Deleting session
192.168.1.40-32791 > 192.168.2.40-80 6 NAP id 1, IPS id 0,

Verdict BLOCKLIST

192.168.1.40-32791 > 192.168.2.40-80 6 ===>

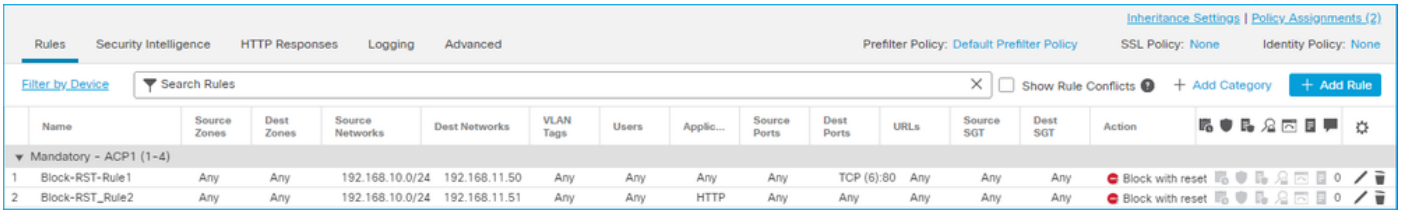
Blocked by Firewall

Résumé:

- L'action de blocage ACP est déployée en tant que règle d'autorisation ou de refus dans le moteur LINA, selon les conditions de la règle.
- Si les conditions sont L3/L4, le moteur LINA bloque le paquet. Dans le cas du protocole TCP, le premier paquet (TCP SYN) est bloqué.
- Si les conditions sont L7, le paquet est transmis au moteur Snort pour une inspection plus approfondie. Dans le cas d'un protocole TCP, quelques paquets sont autorisés par l'intermédiaire de Cisco FTD jusqu'à ce que le renifleur atteigne un verdict. Les paquets autorisés sont toujours soumis à la vérification de la stratégie d'intrusion basée sur l'option Access Policy > Advanced > Intrusion Policy utilisée avant que la règle de contrôle d'accès ne soit déterminée.

Action Block (blocage) de la politique de contrôle d'accès avec réinitialisation

Une règle Block (blocage) avec repos configurée sur l'interface utilisateur de Cisco Firepower Management Center (FMC) :



Le bloc avec la règle de réinitialisation est déployé sur le moteur FTD LINA en tant qu'autorisation et sur le moteur Snort en tant que règle de réinitialisation :

<#root>

```
firepower#
```

show access-list

```
…
access-list CSM_FW_ACL_ line 10 advanced
```

permit

```
 tcp 192.168.10.0 255.255.255.0 host 192.168.11.50 eq www rule-id 268438864 (hitcnt=0) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Block-RST_Rule2
access-list CSM_FW_ACL_ line 13 advanced
```

permit

```
 ip 192.168.10.0 255.255.255.0 host 192.168.11.51 rule-id 268438865 (hitcnt=0) 0x622350d0
```

Moteur du renifleur :

<#root>

```
admin@firepower:~$

cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules

…
# Start of AC rule.
268438864

reset

 any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865

reset

 any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1) (ip_protos 6, 17)
# End rule 268438865
```

Lorsqu'un paquet correspond à un bloc avec une règle de réinitialisation, FTD envoie un paquet de réinitialisation TCP ou un message ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) :

<#root>

```
root@kali:~/tests#

wget 192.168.11.50/file1.zip

--2020-06-20 22:48:10--  http://192.168.11.50/file1.zip
Connecting to 192.168.11.50:80... failed:

Connection refused.
```

Reportez-vous à la capture effectuée sur l'interface d'entrée FTD :

```
firepower# show capture CAPI
2 packets captured
1: 21:01:00.977259 802.1Q vlan#202 P0 192.168.10.50.41986 > 192.168.11.50.80: S 3120295488:3120295488(0
2: 21:01:00.978114 802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.41986: R 0:0(0) ack 3120295489 w
```

Le résultat de la trace du support système, dans ce cas, montre que le paquet est abandonné en raison du verdict Snort :

```
<#root>

>

system support trace


Enable firewall-engine-debug too? [n]:

y

Please specify an IP protocol: tcp
Please specify a client IP address:

192.168.10.50

Please specify a client port:
Please specify a server IP address:

192.168.11.50

Please specify a server port:
Monitoring packet tracer and firewall debug messages


192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3387496622
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0

Session: new snort session

192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9

new firewall session

192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 using HW or preset rule order 2, 'Block-RST-Rule1',
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 HitCount data sent for rule id: 268438864,
192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9

reset action

192.168.10.50-41984 > 192.168.11.50-80 6 AS 1-1 I 9 deleting firewall session flags = 0x0, fwFlags = 0x
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0

Firewall: block w/ reset rule, 'Block-RST-Rule1', drop

192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions queue,
192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 9, NAP id 1, IPS id 0,
```

```
Verdict BLOCKLIST

192.168.10.50-41984 - 192.168.11.50-80 6 AS 1-1 CID 0 ===>

Blocked by Firewall


Verdict reason is sent to DAQ
```

Scénarios :

Comme l'action Block, cependant, elle met fin immédiatement à la connexion.

⚠ Mise en garde : Vous devez utiliser les commandes de support du système sous la direction du support de Cisco, à l'exception des commandes documentées dans le guide des commandes de support du système ssl-client-hello- , qui est pour une utilisation générale.

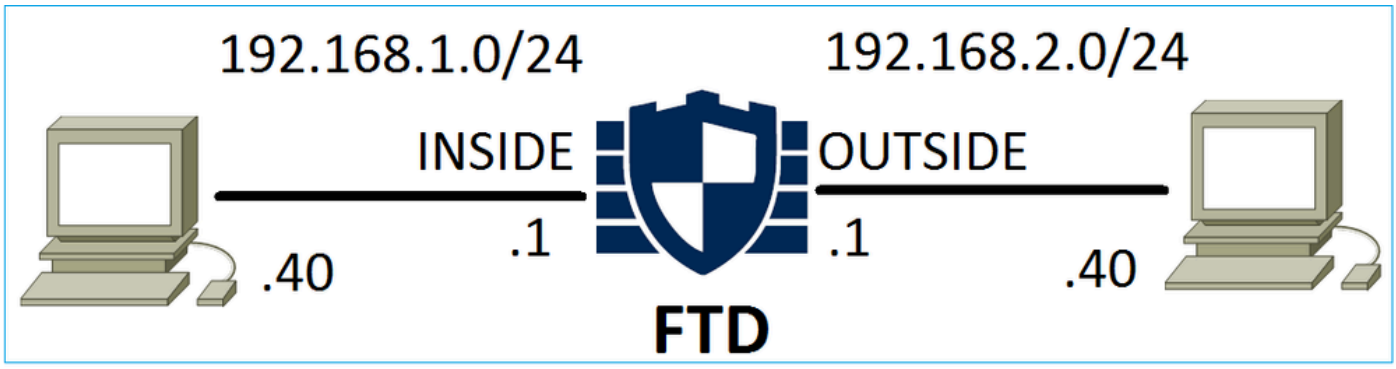
En outre, utilisez toujours les filtres appropriés et ne laissez pas la commande s'exécuter indéfiniment, car cela peut affecter les performances du périphérique.

Action Allow (autorisation) de la politique de contrôle d’accès

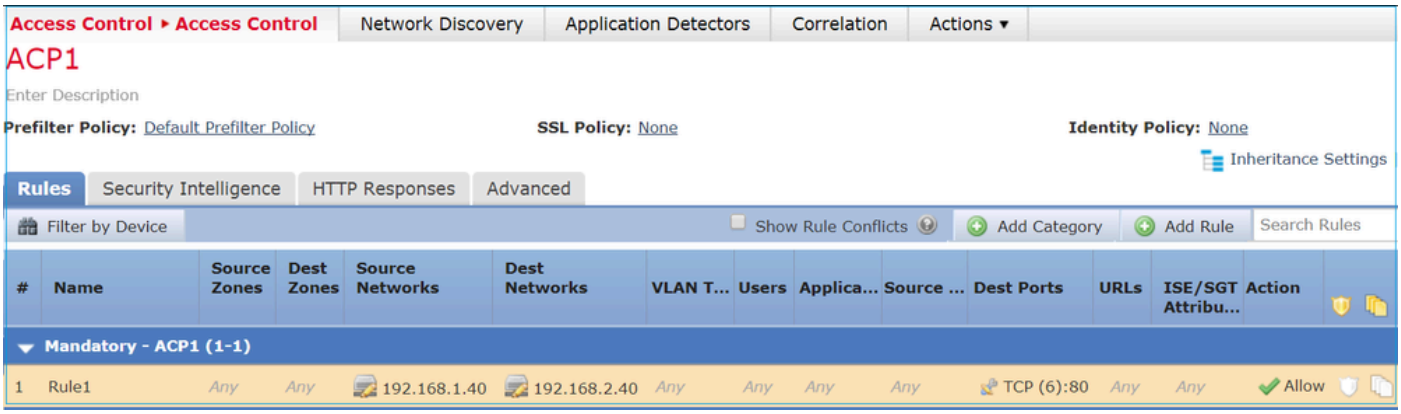
Scénario 1. Action Autoriser ACP (conditions L3/L4)

Normalement, vous configurez une règle Autoriser pour spécifier des inspections supplémentaires comme une politique d'intrusion et/ou une politique de fichier. Ce premier scénario illustre le fonctionnement d'une règle Allow lorsqu'une condition L3/L4 est appliquée.

Considérez cette topologie :



Cette stratégie est appliquée :



La politique déployée dans le renifleur. Notez que la règle est déployée en tant qu'action allow (autorisation) :

<#root>

```
# Start of AC rule.
268435461
```

allow

```
 any 192.168.1.40 32 any any 192.168.2.40 32 80 any 6
```

La stratégie du moteur LINA :

Remarque : La règle est déployée en tant qu'action d'autorisation, ce qui signifie qu'il s'agit d'une redirection vers Snort pour une inspection ultérieure.

<#root>

```
firepower#
```

show access-list

```
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L7 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced
```

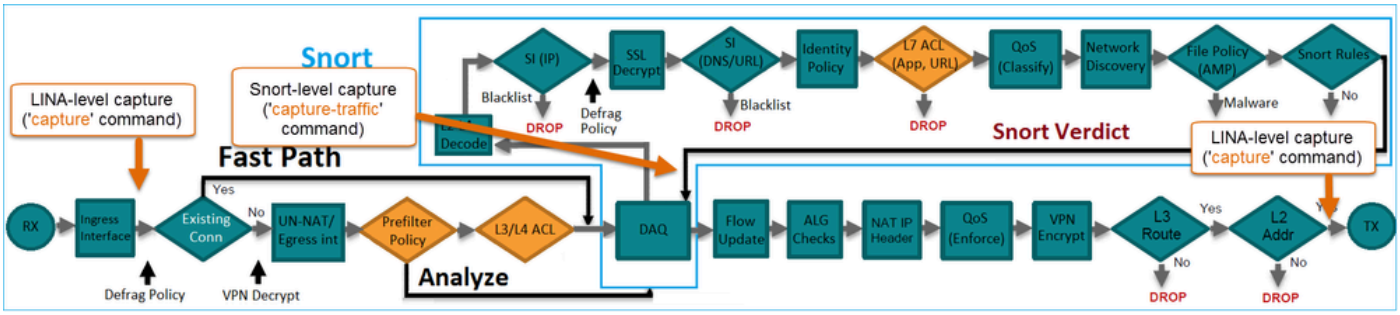
permit

```
 tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268435461 (hitcnt=1) 0x641a20c3
```

Pour voir comment FTD gère un flux qui correspond à une règle Allow, il existe plusieurs méthodes :

- Vérifier les statistiques du renifleur
- Utiliser l'outil CLISH de suivi du support système
- Avec l'option capture et trace du moteur LINA, vous pouvez éventuellement utiliser le trafic de capture du moteur Snort

Capture LINA c. trafic du renifleur :



Vérifiez le comportement

Effacez les statistiques de Snort et activez la trace de prise en charge du système à partir de CLISH, et lancez le flux HTTP de l'hôte-A (192.168.1.40) vers l'hôte-B (192.168.2.40). Tous les paquets sont transférés au moteur Snort et reçoivent un verdict PASS du moteur Snort :

<#root>

```
firepower#
```

clear snort statistics

⚠ Mise en garde : Vous devez utiliser les commandes de support du système sous la direction du support de Cisco, à l'exception des commandes documentées dans le guide des commandes de support du système ssl-client-hello- , qui est pour une utilisation générale.

En outre, utilisez toujours les filtres appropriés et ne laissez pas la commande s'exécuter indéfiniment, car cela peut affecter les performances du périphérique.

<#root>

```
>
```

system support trace

```
Please specify an IP protocol:
Please specify a client IP address:
```

192.168.1.40

```
Please specify a client port:
Please specify a server IP address:
```

192.168.2.40

```
Please specify a server port:
Enable firewall-engine-debug too? [n]:
Monitoring packet tracer debug messages

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, seq 361134402
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0,
```

Verdict PASS

```
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, SYN, ACK, seq 1591434735, ack 361134403
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service unknown (0), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0,
```

Verdict PASS

```
Trace buffer and verdict reason are sent to DAQ's PDTS

Tracing enabled by Lina
192.168.2.40-80 - 192.168.1.40-32797 6 Packet: TCP, ACK, seq 361134403, ack 1591434736
192.168.2.40-80 - 192.168.1.40-32797 6 AppID: service HTTP (676), application unknown (0)
192.168.1.40-32797 > 192.168.2.40-80 6 Firewall: allow rule, 'Rule1', allow
192.168.1.40-32797 > 192.168.2.40-80 6 NAP id 1, IPS id 0,
```

Verdict PASS

Les compteurs de paquets Pass augmentent :

<#root>

>

show snort statistics

```
Packet Counters:

  Passed Packets                                   54

  Blocked Packets                                   0
  Injected Packets                                  0
  Packets bypassed (Snort Down)                     0
  Packets bypassed (Snort Busy)                     0

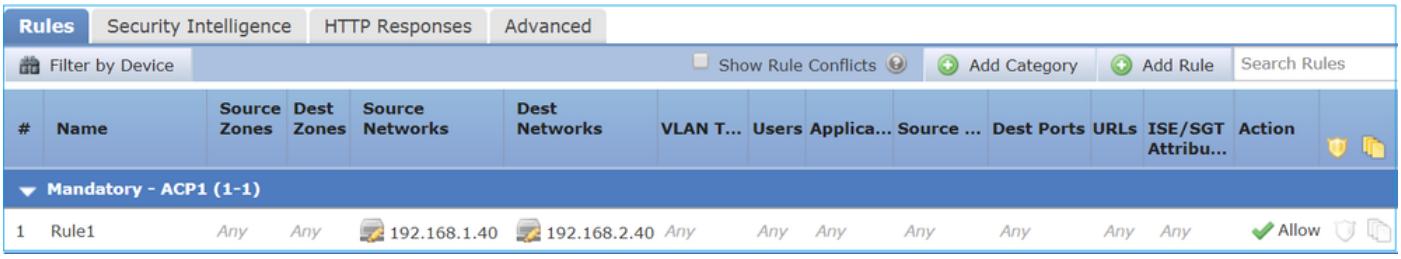
Flow Counters:
  Fast-Forwarded Flows                              0
  Blocklisted Flows                                 0
...
```

Paquets réussis = inspectés par le moteur de renifleur

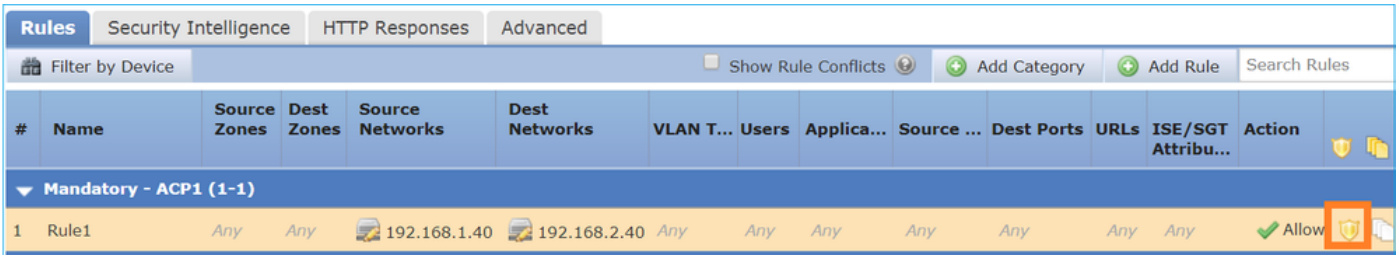
Scénario 2. Action Autoriser ACP (conditions L3-7)

Un comportement similaire est observé lorsque la règle Autoriser est déployée.

Seule une condition L3/L4 :



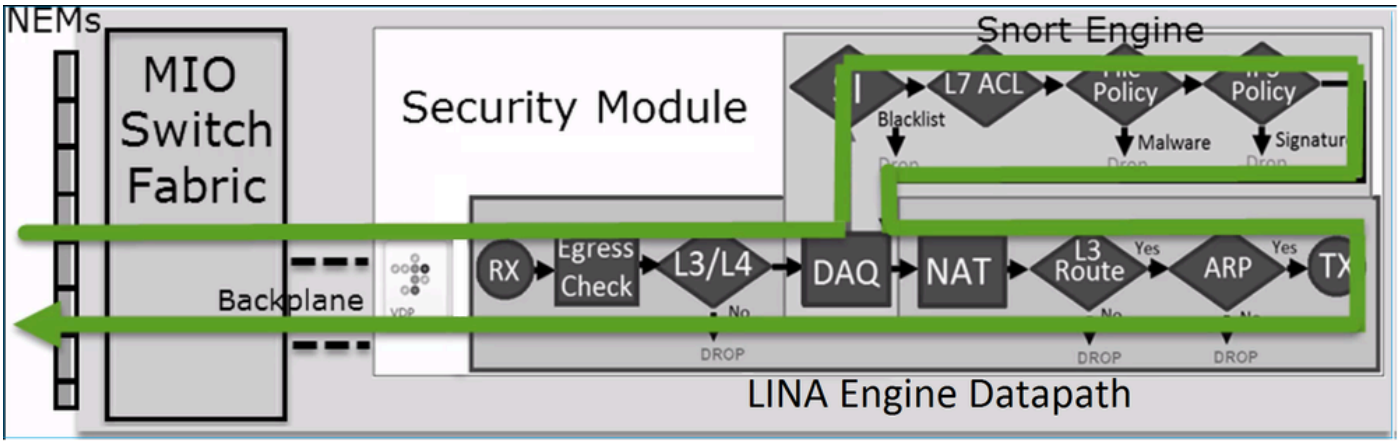
Une condition de couche 7 (par exemple, une politique d'intrusion, une politique de fichiers, une application) :



Résumé

En résumé, voici comment un flux est géré par un FTD déployé sur un FP4100/9300 lorsqu'une

règle Allow est mise en correspondance :



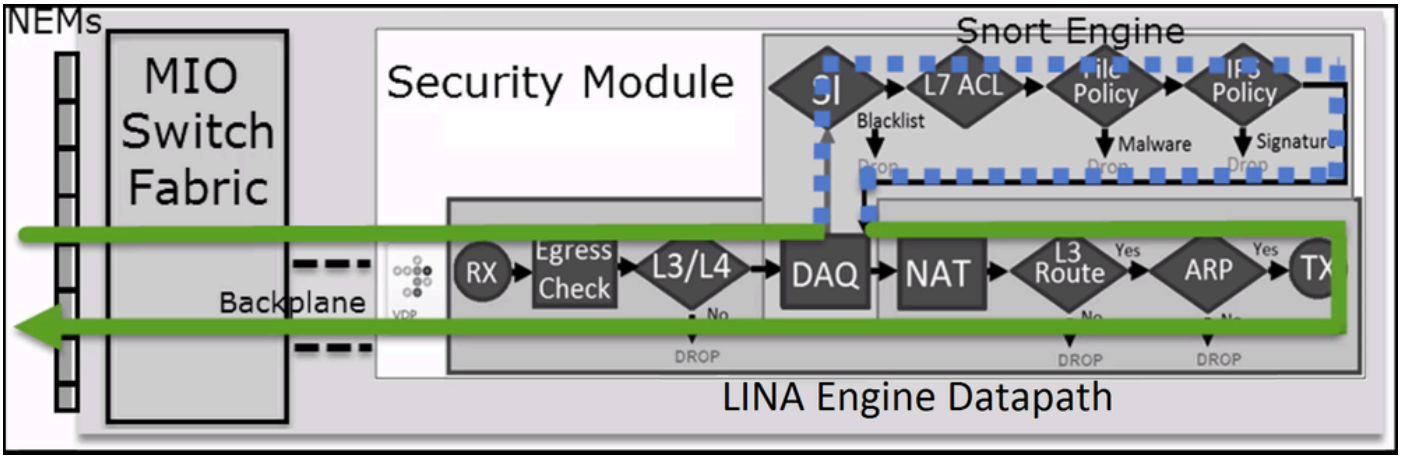
Remarque : Management Input Output (MIO) est le moteur de supervision du châssis Firepower.

Scénario 3. Renifler le verdict Fast-Forward avec Allow

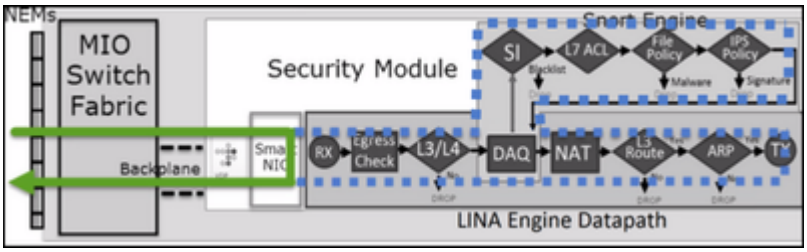
Dans certains cas, le moteur FTD Snort fournit un verdict PERMITLIST (avance rapide) et le flux restant est déchargé vers le moteur LINA (dans certains cas, il est déchargé vers l'accélérateur matériel - SmartNIC). Ces scénarios sont les suivants :

- Trafic SSL sans politique SSL configurée
- Contournement intelligent des applications

Reportez-vous à la représentation visuelle du chemin du paquet :



Ou dans certains cas :



Points principaux

- La règle Allow est déployée en tant que allow dans Snort et permit dans le moteur LINA.
- Dans la plupart des cas, tous les paquets d'une session sont transférés au moteur Snort pour une inspection supplémentaire.

Scénarios :

Vous ne configurez une règle Allow que lorsque vous avez besoin d'une inspection L7 par le moteur Snort tel que :

- Politique d’intrusion
- Politique de fichiers

Action Trust (confiance) de la politique de contrôle d’accès

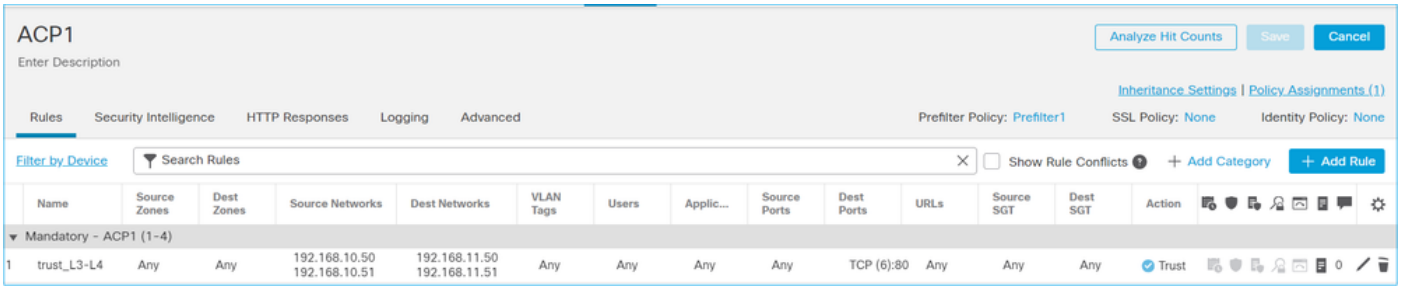
Scénario 1. Action de confiance ACP

Si vous ne souhaitez pas appliquer une inspection avancée de couche 7 au niveau Snort (par exemple, Stratégie d'intrusion, Stratégie de fichiers, Découverte réseau), mais que vous souhaitez utiliser des fonctionnalités telles que Security Intelligence (SI), Stratégie d'identité, QoS, il est recommandé d'utiliser l'Action d'approbation dans votre règle.

Topologie:



La politique configurée :



Référez-vous à la règle d'approbation telle qu'elle est déployée dans le moteur FTD Snort :

<#root>

```
# Start of AC rule.
268438858
```

fastpath

```
 any 192.168.10.50 31 any any 192.168.11.50 31
```

80

```
 any
```

6

```
 (log dcforward flowend)
```

Remarque : Le numéro 6 est le protocole (TCP).

La règle dans FTD LINA :

<#root>

```
firepower#
```

show access-list | i 268438858

```
access-list CSM_FW_ACL_ line 17 remark rule-id 268438858: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 18 remark rule-id 268438858: L7 RULE: trust_L3-L4
access-list CSM_FW_ACL_ line 19 advanced permit tcp object-group FMC_INLINE_src_rule_268438858 object-g
  access-list CSM_FW_ACL_ line 19 advanced
```

permit

```
 tcp host 192.168.10.50 host 192.168.11.50 eq www rule-id 268438858 (hitcnt=19) 0x9d442895
  access-list CSM_FW_ACL_ line 19 advanced

permit

 tcp host 192.168.10.50 host 192.168.11.51 eq www rule-id 268438858 (hitcnt=0) 0xd026252b
  access-list CSM_FW_ACL_ line 19 advanced

permit

 tcp host 192.168.10.51 host 192.168.11.50 eq www rule-id 268438858 (hitcnt=0) 0x0d785cc4
  access-list CSM_FW_ACL_ line 19 advanced

permit

 tcp host 192.168.10.51 host 192.168.11.51 eq www rule-id 268438858 (hitcnt=0) 0x3b3234f1
```

Vérification :

Activez system support trace (trace de prise en charge du système) et lancez une session HTTP de l'hôte A (192.168.10.50) à l'hôte B (192.168.11.50).

⚠ Mise en garde : Vous devez utiliser les commandes de support du système sous la direction du support de Cisco, à l'exception des commandes documentées dans le guide des commandes de support du système ssl-client-hello- , qui est pour une utilisation générale.

En outre, utilisez toujours les filtres appropriés et ne laissez pas la commande s'exécuter indéfiniment, car cela peut affecter les performances du périphérique.

Trois paquets sont transférés au moteur Snort. Le moteur Snort envoie à LINA et le verdict PERMITLIST décharge le flux restant vers le moteur LINA :

```
<#root>

>

system support trace


Enable firewall-engine-debug too? [n]:

y
```

Please specify an IP protocol:

tcp
Please

specify a client IP address:

192.168.10.50

Please specify a client port:
Please specify a server IP address:

192.168.11.50

Please specify a server port:

80

Monitoring packet tracer and firewall debug messages

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet:

TCP, SYN

, seq 453426648
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 new firewall session
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 using HW or preset rule order 5, 'trust_L3-L4', act
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 HitCount data sent for rule id: 268438858,
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-L4', all
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0,

Verdict PASS

192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Packet:

TCP, SYN, ACK

, seq 2820426532, ack 453426649
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-L4', all
192.168.11.50-80 - 192.168.10.50-42126 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0,

Verdict PASS

192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet:

TCP, ACK

, seq 453426649, ack 2820426533

```
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: trust/fastpath rule, 'trust_L3-L4', all
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 2, NAP id 2, IPS id 0,
```

Verdict PERMITLIST

Une fois la connexion terminée, le moteur Snort reçoit les informations de métadonnées du moteur LINA et supprime la session :

<#root>

```
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2
```

Got end of flow event

```
 from hardware with flags 00010001. Rule Match Data: rule_id 0, rule_action 0 rev_id 0, rule_flags 3
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 Logging EOF for event from hardware with rule_id =
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 :
```

Received EOF, deleting the snort session.

```
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleting snort session, reason: timeout
192.168.10.50-42126 > 192.168.11.50-80 6 AS 1-1 I 2 deleting firewall session flags = 0x10003, fwFlags
192.168.10.50-42126 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: deleted snort session using 0 bytes; pro
```

La capture du moteur Snort affiche les trois paquets qui sont envoyés au moteur Snort :

<#root>

```
>
```

capture-traffic

```
Please choose domain to capture traffic from:
  0 - management0
  1 - management1
  2 - Global

Selection?
```

2

```
Please specify tcpdump options desired.
(or enter '?' for a list of supported options)
```

```
Options:

-n vlan and (host 192.168.10.50 and host 192.168.11.50)

10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [S], seq 3065553465, win 29200, option
10:26:16.525928 IP 192.168.11.50.80 > 192.168.10.50.42144: Flags [S.], seq 3581351172, ack 3065553466, w
10:26:16.525928 IP 192.168.10.50.42144 > 192.168.11.50.80: Flags [.], ack 1, win 229, options [nop,nop,T
```

La capture du moteur LINA montre le flux qui le traverse :

```
<#root>

firepower#

show capture CAPI


437 packets captured

   1: 09:51:19.431007  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: S 2459891187:24598911
   2: 09:51:19.431648  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: S 2860907367:28609073
   3: 09:51:19.431847  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: . ack 2860907368 win
   4: 09:51:19.431953  802.1Q vlan#202 P0 192.168.10.50.42118 > 192.168.11.50.80: P 2459891188:24598913
   5: 09:51:19.444816  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: . 2860907368:28609087
   6: 09:51:19.444831  802.1Q vlan#202 P0 192.168.11.50.80 > 192.168.10.50.42118: . 2860908736:28609101

…
```

La trace des paquets à partir de LINA est une autre façon d'afficher les verdicts Snort. Le premier paquet a reçu le verdict PASS :

```
<#root>

firepower#

 show capture CAPI packet-number 1 trace | i Type|Verdict

Type: CAPTURE
Type: ACCESS-LIST
Type: ROUTE-LOOKUP
Type: ACCESS-LIST
Type: CONN-SETTINGS
Type: NAT
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: CAPTURE
Type: NAT
Type: CAPTURE
Type: NAT
Type: IP-OPTIONS
```

```
Type: CAPTURE
Type: FLOW-CREATION
Type: EXTERNAL-INSPECT

Type: SNORT


Snort id 22, NAP id 2, IPS id 0, Verdict PASS


Snort Verdict: (pass-packet) allow this packet

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

Trace du paquet TCP SYN/ACK sur l'interface OUTSIDE :

<#root>

```
firepower#

show capture CAPO packet-number 2 trace | i Type|Verdict


Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT

Snort id 22, NAP id 2, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet

Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

L’ACK TCP reçoit le verdict PERMITLIST :

<#root>

```
firepower#

show capture CAPI packet-number 3 trace | i Type|Verdict


Type: CAPTURE
Type: ACCESS-LIST
Type: FLOW-LOOKUP
Type: EXTERNAL-INSPECT
Type: SNORT
```

```
Snort id 22, NAP id 2, IPS id 0, Verdict PERMITLIST

Snort Verdict: (fast-forward) fast forward this flow
Type: CAPTURE
```

Reportez-vous au résultat complet du verdict Snort (paquet #3) :

<#root>

```
firepower#

show capture CAPI packet-number 3 trace | b Type: SNORT


Type: SNORT

Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 687485179, ack 1029625865
AppID: service unknown (0), application unknown (0)
Firewall: trust/fastpath rule, id 268438858, allow
Snort id 31, NAP id 2, IPS id 0,

Verdict PERMITLIST

Snort Verdict: (fast-forward) fast forward this flow
```

Le quatrième paquet n'est pas transmis au moteur Snort car le verdict est mis en cache par le moteur LINA :

<#root>

```
firepower#

show capture CAPI packet-number 4 trace


441 packets captured

   4: 10:34:02.741523       802.1Q vlan#202 P0 192.168.10.50.42158 > 192.168.11.50.80: P 164375589:1643
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 1254, using existing flow



Phase: 4
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (fast-forward) fast forward this flow



Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow


1 packet shown
```

Les statistiques de Snort le confirment :

<#root>

```
firepower#

show snort statistics


Packet Counters:


Passed Packets                                               2

  Blocked Packets                                            0
  Injected Packets                                           0
```

```
  Packets bypassed (Snort Down)                                  0
  Packets bypassed (Snort Busy)                                  0

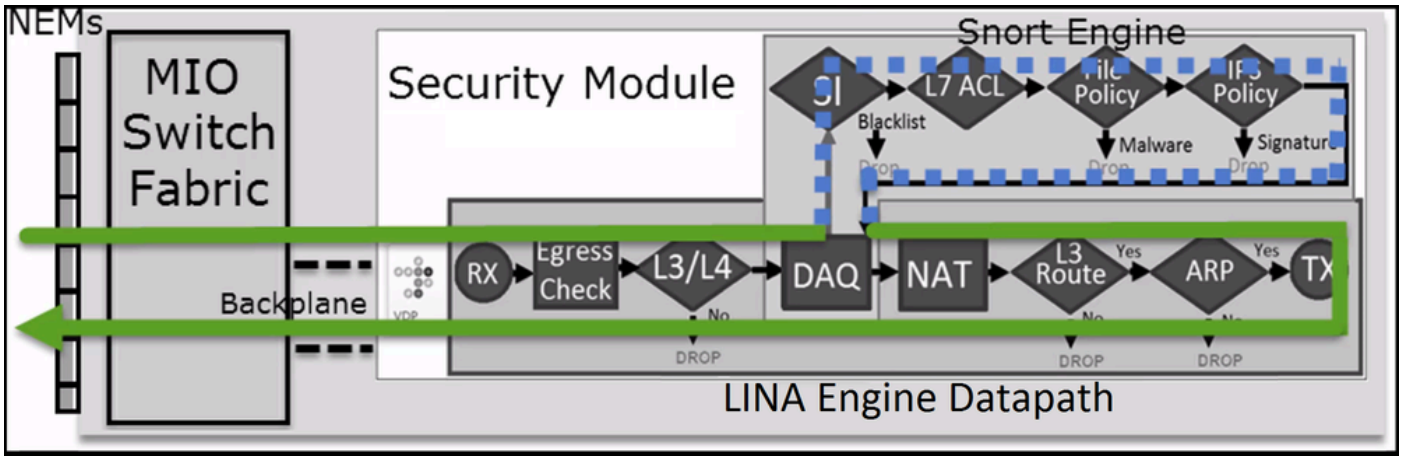
Flow Counters:


Fast-Forwarded Flows                                             1


  Blacklisted Flows                                              0

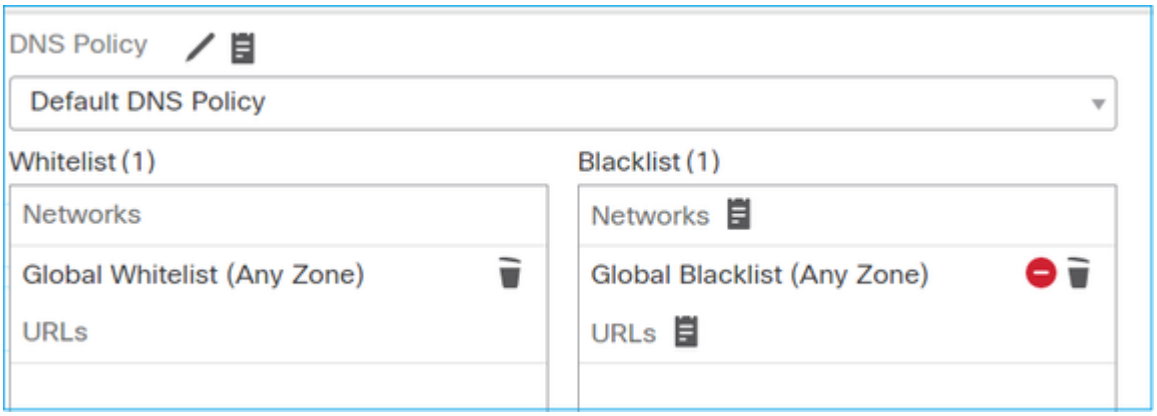
Miscellaneous Counters:
  Start-of-Flow events                                           0
  End-of-Flow events                                             1
  Denied flow events                                             0
  Frames forwarded to Snort before drop                          0
  Inject packets dropped                                         0
```

Reportez-vous au flux de paquets avec la règle Trust. Quelques paquets sont inspectés par le moteur Snort et les autres sont inspectés par LINA :



Scénario 2. Action d'approbation ACP (sans SI, QoS et politique d'identité)

Si vous souhaitez que FTD applique des contrôles de sécurité adaptative (SI) à tous les flux, SI est déjà activé au niveau ACP et vous pouvez spécifier les sources SI (TALOS, flux, listes). D'autre part, si vous souhaitez le désactiver, vous pouvez désactiver SI pour les réseaux globalement par ACP, SI pour les URL et SI pour DNS. L'ID des réseaux et l'URL sont désactivés :



Dans ce cas, la règle Trust (confiance) est déployée dans LINA en tant que trust :

<#root>

>

show access-list
...

```
access-list CSM_FW_ACL_ line 9 remark rule-id 268435461: L4 RULE: Rule1
access-list CSM_FW_ACL_ line 10 advanced trust ip host 192.168.1.40 host 192.168.2.40 rule-id 268435461
```

Remarque : À partir de la section 6.2.2, FTD prend en charge TID. TID fonctionne comme SI, mais si SI est désactivé, il ne « force » pas les paquets à rediriger vers le moteur Snort pour l'inspection TID.

Vérifiez le comportement

Lancez une session HTTP de l'hôte-A (192.168.1.40) à l'hôte-B (192.168.2.40). Étant donné qu'il s'agit d'un FP4100 et qu'il prend en charge le déchargement de flux dans le matériel, gardez à l'esprit les événements suivants :

- Certains paquets sont transférés via le moteur FTD LINA et le flux restant est déchargé vers SmartNIC (accélérateur matériel).
- Aucun paquet n'est transféré au moteur Snort.

La table de connexion FTD LINA affiche l'indicateur"o", qui signifie que le flux a été déchargé vers le matériel. Notez également l'absence du drapeau "N". Cela signifie « no Snort redirection » :

<#root>

```
firepower#
```

```
show conn

1 in use, 15 most used

TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:32809, idle 0:00:00, bytes 949584, flags UIO

o
```

Les statistiques Snort affichent uniquement les événements de journalisation au début et à la fin de la session :

<#root>

```
firepower#

show snort statistics


Packet Counters:
  Passed Packets                                   0
  Blocked Packets                                  0
  Injected Packets                                 0
  Packets bypassed (Snort Down)                    0
  Packets bypassed (Snort Busy)                    0

Flow Counters:
  Fast-Forwarded Flows                             0
  Blacklisted Flows                                0

Miscellaneous Counters:


  Start-of-Flow events                             1
  End-of-Flow events                               1
```

Les journaux FTD LINA montrent que pour chaque session, deux flux (un par direction) ont été déchargés vers le matériel :

<#root>

```
Sep 27 2017 20:16:05: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Sep 27 2017 20:16:05: %ASA-6-302013: Built inbound TCP connection 25384 for INSIDE:192.168.1.40/32809 (
Sep 27 2017 20:16:05: %ASA-6-805001:

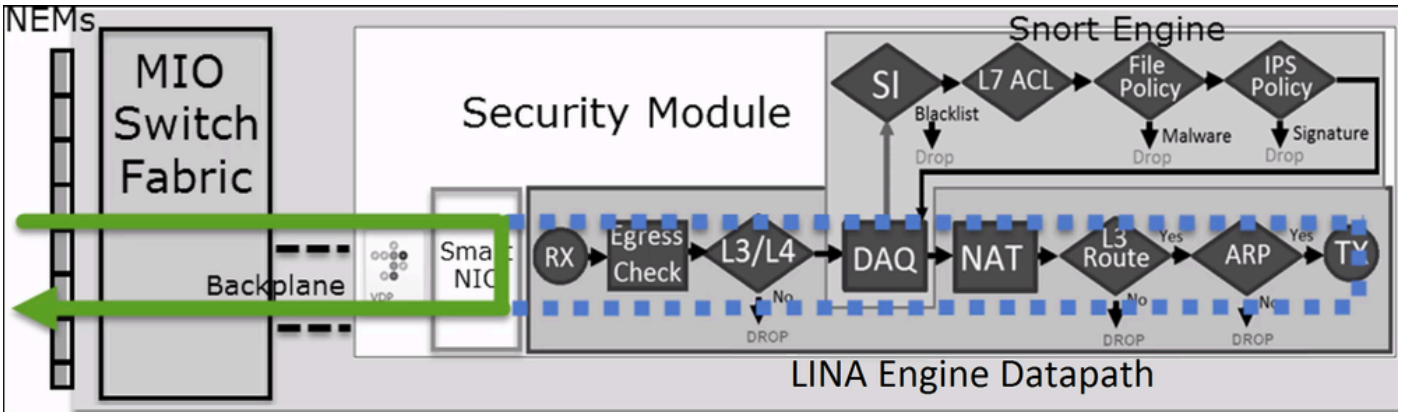
Offloaded TCP Flow for connection 25384 from INSIDE


:192.168.1.40/32809 (192.168.1.40/32809) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Sep 27 2017 20:16:05: %ASA-6-805001:

Offloaded TCP Flow for connection 25384 from OUTSIDE
```

```
:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32809 (192.168.1.40/32809)
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from OUTSIDE:
Sep 27 2017 20:16:05: %ASA-6-805002: TCP Flow is no longer offloaded for connection 25384 from INSIDE:1
Sep 27 2017 20:16:05: %ASA-6-302014: Teardown TCP connection 25384 for INSIDE:192.168.1.40/32809 to OUT
Sep 27 2017 20:16:05: %ASA-7-609002: Teardown local-host INSIDE:192.168.1.40 duration 0:00:00
```

Flux de paquets avec la règle Trust déployée comme action trust dans LINA. Quelques paquets sont inspectés par LINA, le reste est déchargé sur SmartNIC (FP4100/FP9300) :

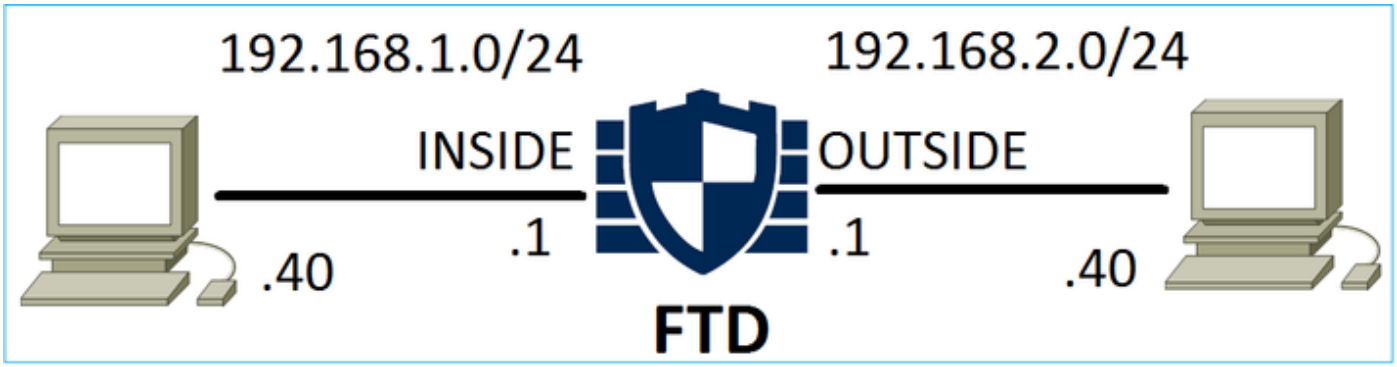


Scénarios :

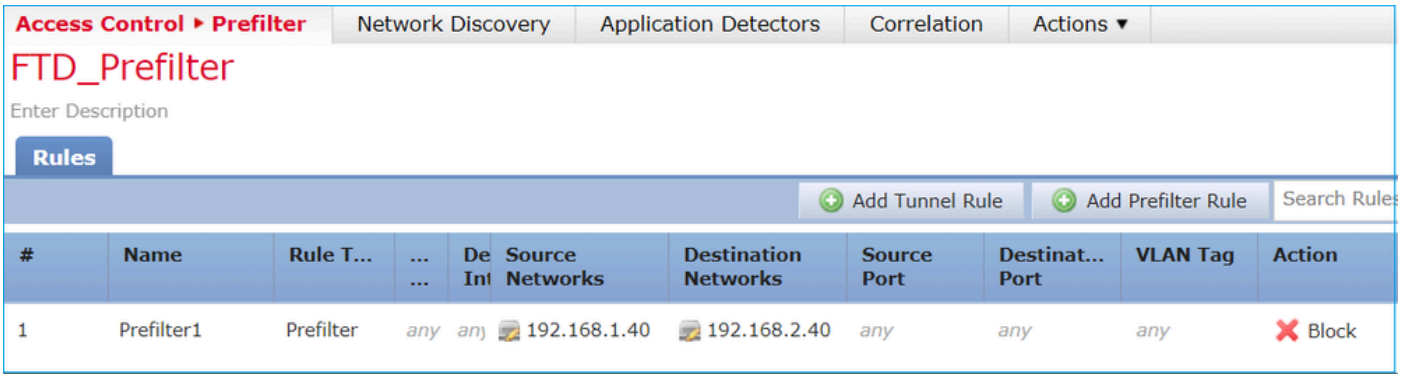
- Vous devez utiliser l'action Trust quand vous voulez seulement quelques paquets vérifiés par le moteur Snort (par exemple, Détection d'application, Vérification SI) et le flux restant est déchargé vers le moteur LINA.
- Si vous utilisez FTD sur FP4100/9300 et que vous voulez que le flux contourne complètement l'inspection Snort. examinez ensuite la règle de préfiltrage avec l'action FastPath (reportez-vous à la section associée dans ce document).

Action Prefilter Policy Block (blocage de la politique de préfiltre)

Examinez la topologie :



Reportez-vous à la politique de préfiltrage FTD :



La stratégie déployée dans le moteur FTD Snort (fichier ngfw.rules) :

<#root>

```
# Start of tunnel and priority rules.
#
```

These rules are evaluated by LINA

```
. Only tunnel tags are used from the matched rule id.
268437506
```

deny

```
 any 192.168.1.40 32 any any 192.168.2.40 32 any any any  (tunnel -1
```

Dans LINA :

<#root>

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506: PREFILTER POLICY: FTD_Prefilter
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced
```

deny

```
 ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506 event-log flow-start (hitcnt=0) 0x76476240
```

Lorsque vous tracez un paquet virtuel, il indique que le paquet est abandonné par LINA et n'est jamais transféré à Snort :

<#root>

```
firepower# packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40
…
Phase: 4

Type: ACCESS-LIST

Subtype: log

Result: DROP

Config:
access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced deny ip host 192.168.1.40 host 192.168.2.40 rule-id 268437506 event-log

access-list CSM_FW_ACL_ remark rule-id 268437506:

PREFILTER POLICY: FTD_Prefilter

access-list CSM_FW_ACL_ remark rule-id 268437506: RULE: Prefilter1
Additional Information:

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule
```

Les statistiques du renifleur montrent :

<#root>

```
firepower#

show snort statistics


Packet Counters:
  Passed Packets                                   0
  Blocked Packets                                  0
  Injected Packets                                 0
  Packets bypassed (Snort Down)                    0
  Packets bypassed (Snort Busy)                    0

Flow Counters:
  Fast-Forwarded Flows                             0
```

```
  Blacklisted Flows                                        0

Miscellaneous Counters:
  Start-of-Flow events                                     0
  End-of-Flow events                                       0


 Denied flow events                                       1
```

La politique de contrôle d'accès de LINA affiche :

```
<#root>

firepower#

show asp drop


Frame drop:


Flow is denied by configured rule (acl-drop)



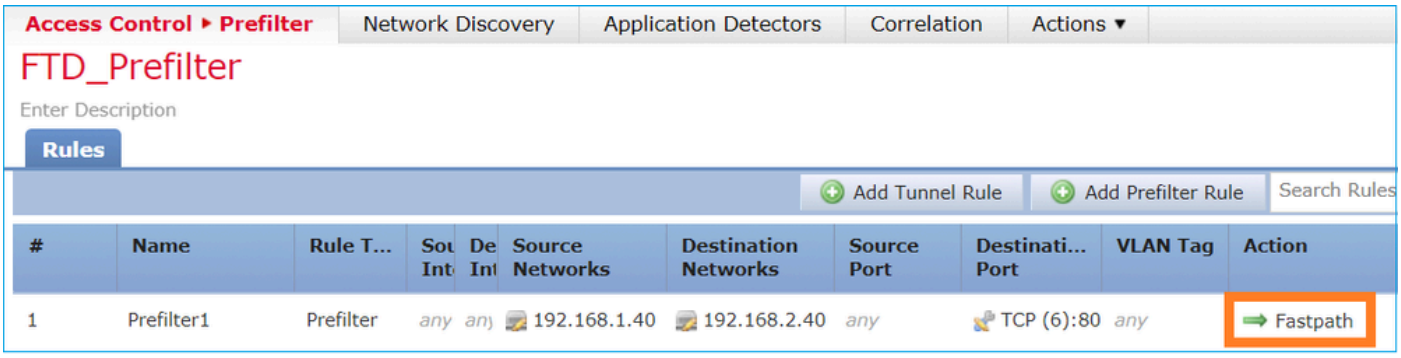

1
```

Scénarios :

Vous pouvez utiliser une règle de blocage du préfiltre lorsque vous souhaitez bloquer le trafic en fonction des conditions L3/L4 et sans inspection supplémentaire de votre trafic par Snort.

Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre)

Considérez la règle de stratégie de préfiltrage :



La stratégie déployée dans le moteur FTD Snort :

<#root>

268437506

fastpath

 any any any any any any any any (log dcforward flowend) (tunnel -1)

Dans FTD LINA :

<#root>

```
access-list CSM_FW_ACL_ line 1 remark rule-id 268437506:
```

PREFILTER POLICY: FTD_Prefilter

```
access-list CSM_FW_ACL_ line 2 remark rule-id 268437506: RULE: Prefilter1
access-list CSM_FW_ACL_ line 3 advanced
```

trust

 tcp host 192.168.1.40 host 192.168.2.40 eq www rule-id 268437506 event-log flow-end (hitcnt=0) 0xf3410

Vérifiez le comportement

Lorsque l'hôte A (192.168.1.40) tente d'ouvrir une session HTTP vers l'hôte B (192.168.2.40), certains paquets passent par LINA et les autres sont déchargés vers SmartNIC. Dans ce cas, la trace de support système avec firewall-engine-debug activé montre :

<#root>

```
>

system support trace

Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.1.40
Please specify a client port:
Please specify a server IP address: 192.168.2.40
Please specify a server port:
Enable firewall-engine-debug too? [n]: y
Monitoring packet tracer debug messages


192.168.1.40-32840 > 192.168.2.40-80 6 AS 1 I 8 Got end of flow event from hardware

 with flags 04000000
```

⚠ Mise en garde : Vous devez utiliser les commandes de support du système sous la direction du support de Cisco, à l'exception des commandes documentées dans le guide des commandes de support du système ssl-client-hello- , qui sont pour une utilisation générale.

En outre, utilisez toujours les filtres appropriés et ne laissez pas la commande s'exécuter indéfiniment, car cela peut affecter les performances du périphérique.

Les journaux LINA affichent le flux déchargé :

<#root>

```
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host INSIDE:192.168.1.40
Oct 01 2017 14:36:51: %ASA-7-609001: Built local-host OUTSIDE:192.168.2.40
Oct 01 2017 14:36:51: %ASA-6-302013: Built inbound TCP connection 966 for INSIDE:192.168.1.40/32840 (19
Oct 01 2017 14:36:51: %ASA-6-805001:

Offloaded TCP Flow for connection 966 from INSIDE

:192.168.1.40/32840 (192.168.1.40/32840) to OUTSIDE:192.168.2.40/80 (192.168.2.40/80)
Oct 01 2017 14:36:51: %ASA-6-805001:

Offloaded TCP Flow for connection 966 from OUTSIDE

:192.168.2.40/80 (192.168.2.40/80) to INSIDE:192.168.1.40/32840 (192.168.1.40/32840)
```

Les captures LINA montrent huit paquets traités par :

<#root>

```
firepower# show capture
capture CAPI type raw-data buffer 33554432 trace trace-count 100 interface INSIDE [Capturing -

3908 bytes]

  match ip host 192.168.1.40 host 192.168.2.40
capture CAPO type raw-data buffer 33554432 trace trace-count 100 interface OUTSIDE [Capturing -

3908 bytes]

  match ip host 192.168.1.40 host 192.168.2.40
```

<#root>

```
firepower#

show capture CAPI



8 packets captured


   1: 14:45:32.700021  192.168.1.40.32842 > 192.168.2.40.80: S 3195173118:3195173118(0) win 2920 <mss 1
   2: 14:45:32.700372  192.168.2.40.80 > 192.168.1.40.32842: S 184794124:184794124(0) ack 3195173119 wi
   3: 14:45:32.700540  192.168.1.40.32842 > 192.168.2.40.80: P 3195173119:3195173317(198) ack 184794125
   4: 14:45:32.700876  192.168.2.40.80 > 192.168.1.40.32842: . 184794125:184795493(1368) ack 3195173317
   5: 14:45:32.700922  192.168.2.40.80 > 192.168.1.40.32842: P 184795493:184796861(1368) ack 3195173317
   6: 14:45:32.701425  192.168.2.40.80 > 192.168.1.40.32842: FP 184810541:184810851(310) ack 3195173317
   7: 14:45:32.701532  192.168.1.40.32842 > 192.168.2.40.80: F 3195173317:3195173317(0) ack 184810852 w
   8: 14:45:32.701639  192.168.2.40.80 > 192.168.1.40.32842: . ack 3195173318 win 2697 <nop,nop,timesta
```

Les statistiques de flux de déchargement de Cisco FTD indiquent 22 paquets déchargés sur le matériel :

<#root>

```
firepower#

show flow-offload statistics

 Packet stats of port : 0

     Tx Packet count                 :              22
```

```
 Rx Packet count                :              22

        Dropped Packet count            :               0
        VNIC transmitted packet         :              22
        VNIC transmitted bytes          :           15308
        VNIC Dropped packets            :               0
        VNIC erroneous received         :               0
        VNIC CRC errors                 :               0
        VNIC transmit failed            :               0
        VNIC multicast received         :               0
```

Vous pouvez utiliser la commande show flow-offload flow pour afficher des informations supplémentaires liées aux flux déchargés.

<#root>

```
firepower#

show flow-offload flow



Total offloaded flow stats: 2 in use, 4 most used, 20% offloaded, 0 collisions
TCP intfc 103 src 192.168.1.40:39301 dest 192.168.2.40:20, static, timestamp 616063741, packets 33240,
TCP intfc 104 src 192.168.2.40:20 dest 192.168.1.40:39301, static, timestamp 616063760, packets 249140,
firepower#

show conn



5 in use, 5 most used
Inspect Snort:
        preserve-connection: 1 enabled, 0 in effect, 4 most enabled, 0 most in effect

TCP OUTSIDE  192.168.2.40:21 INSIDE  192.168.1.40:40988, idle 0:00:00, bytes 723, flags UIO
TCP OUTSIDE  192.168.2.40:21 INSIDE  192.168.1.40:40980, idle 0:02:40, bytes 1086, flags UIO
TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:49442, idle 0:00:00, bytes 86348310, flags UIO N1
TCP OUTSIDE  192.168.2.40:20 INSIDE  192.168.1.40:39301, idle 0:00:00, bytes 485268628, flags U

o <- offloaded flow

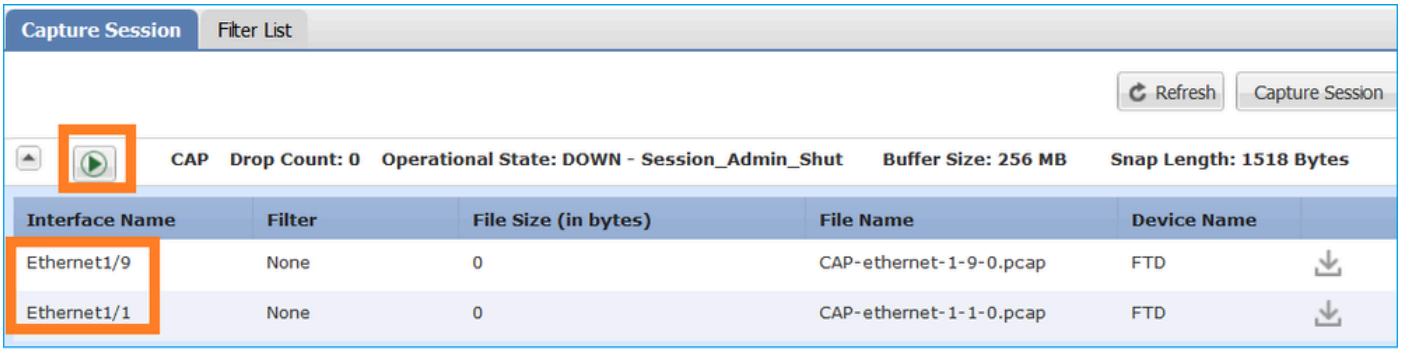


TCP OUTSIDE  192.168.2.40:20 INSIDE  192.168.1.40:34713, idle 0:02:40, bytes 821799360, flags UFRIO
```

- Le pourcentage est basé sur la sortie "show conn". Par exemple, si 5 cons au total sont traitées par le moteur FTD LINA et que l'une d'elles est déchargée, alors 20 % sont déclarés comme déchargés.
- La limite maximale de sessions déchargées dépend de la version du logiciel (par exemple, ASA 9.8.3 et FTD 6.2.3 prennent en charge 4 millions de flux déchargés bidirectionnels ou 8 millions de flux déchargés unidirectionnels).
- Si le nombre de flux déchargés atteint la limite (par exemple, 4 millions de flux

bidirectionnels), aucune nouvelle connexion n'est déchargée jusqu'à ce que les connexions en cours soient supprimées de la table déchargée.

Pour afficher tous les paquets sur FP4100/9300 qui sont traités via FTD (déchargé + LINA), vous devez activer la capture au niveau du châssis :



La capture du fond de panier du châssis indique les deux directions. En raison de l'architecture de capture FXOS (deux points de capture par direction), chaque paquet est affiché deux fois :

Statistiques sur les paquets :

- Total des paquets passant par Cisco FTD : 30
- Paquets passant par FTD LINA : 8
- Paquets déchargés vers l'accélérateur SmartNIC HW : 22

Si la plate-forme est différente de FP4100/FP9300 et que tous les paquets sont traités par le moteur LINA puisque le déchargement de flux n'est pas pris en charge (notez l'absence de l'indicateur o) :

<#root>

```
FP2100-6#

show conn addr 192.168.1.40

33 in use, 123 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 2 most enabled, 0 most in effect

TCP OUTSIDE  192.168.2.40:80 INSIDE  192.168.1.40:50890, idle 0:00:09, bytes 175, flags

UxIO
```

Les syslogs LINA affichent uniquement les événements de configuration et de fin de connexion :

<#root>

```
FP2100-6#

show log | i 192.168.2.40

Jun 21 2020 14:29:44: %FTD-6-302013:

Built inbound TCP

 connection 6914 for INSIDE:192.168.1.40/50900 (192.168.11.101/50900) to OUTSIDE:192.168.2.40/80 (192.1
Jun 21 2020 14:30:30: %FTD-6-302014:

Teardown TCP connection

 6914 for INSIDE:192.168.1.40/50900 to OUTSIDE:192.168.2.40/80 duration 0:00:46 bytes 565 TCP FINs from
```

Scénarios :

- Utilisez l'action Prefilter Fastpath quand vous voulez contourner complètement l'inspection Snort. Vous souhaitez généralement effectuer cette opération pour les flux de données volumineux en lesquels vous avez confiance, comme les sauvegardes ou les transferts de bases de données.
- Sur les appareils FP4100/9300, l'action Fastpath déclenche des débordements et seuls quelques paquets sont traités par le moteur FTD LINA. Les autres sont gérés par SmartNIC, ce qui réduit la latence

Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre) (ensemble en ligne)

Si une action FastPath de stratégie de préfiltrage est appliquée au trafic qui passe par un ensemble en ligne (interfaces NGIPS), ces points doivent être pris en considération :

- La règle est appliquée au moteur LINA en tant qu'action d'approbation.
- Le flux n’est pas contrôlé par le moteur du renifleur.
- Le délestage de flux (accélération matérielle) ne se produit pas, car il ne s'applique pas aux interfaces NGIPS.

Référez-vous à la trace de paquet dans le cas de l'action Prefilter Fastpath qui a été appliquée à un jeu en ligne :

```
firepower# packet-tracer input inside tcp 192.168.1.40 12345 192.168.1.50 80 detailed

Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied
Forward Flow based lookup yields rule:
in id=0x2ad7ac48b330, priority=501, domain=ips-mode, deny=false
hits=2, user_data=0x2ad80d54abd0, cs_id=0x0, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside, output_ifc=any

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced trust ip object 192.168.1.0 object 192.168.1.0 rule-id 268438531 event
access-list CSM_FW_ACL_ remark rule-id 268438531: PREFILTER POLICY: PF1
access-list CSM_FW_ACL_ remark rule-id 268438531: RULE: 1
Additional Information:
Forward Flow based lookup yields rule:
in id=0x2ad9f9f8a7f0, priority=12, domain=permit, trust
hits=1, user_data=0x2ad9b23c5d40, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any
dst ip/id=192.168.1.0, mask=255.255.255.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Ingress interface inside is in NGIPS inline mode.
Egress interface outside is determined by inline-set configuration

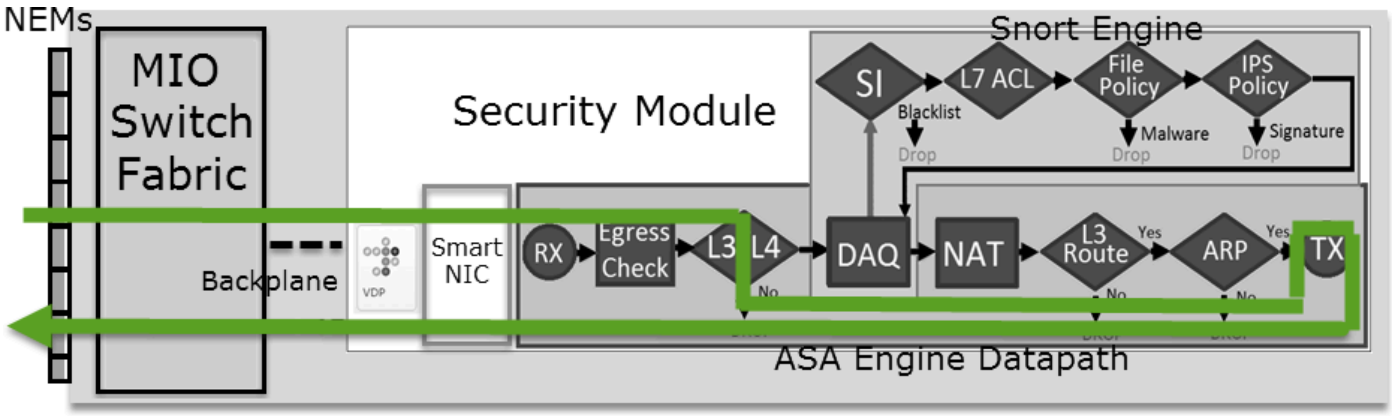
Phase: 4
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 7, packet dispatched to next module
Module information for forward flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_ips_tcp_state_track_lite
snp_fp_ips_mode_adj
snp_fp_tracer_drop
snp_ifc_stat

Result:
```

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

Image de la représentation visuelle du chemin du paquet :



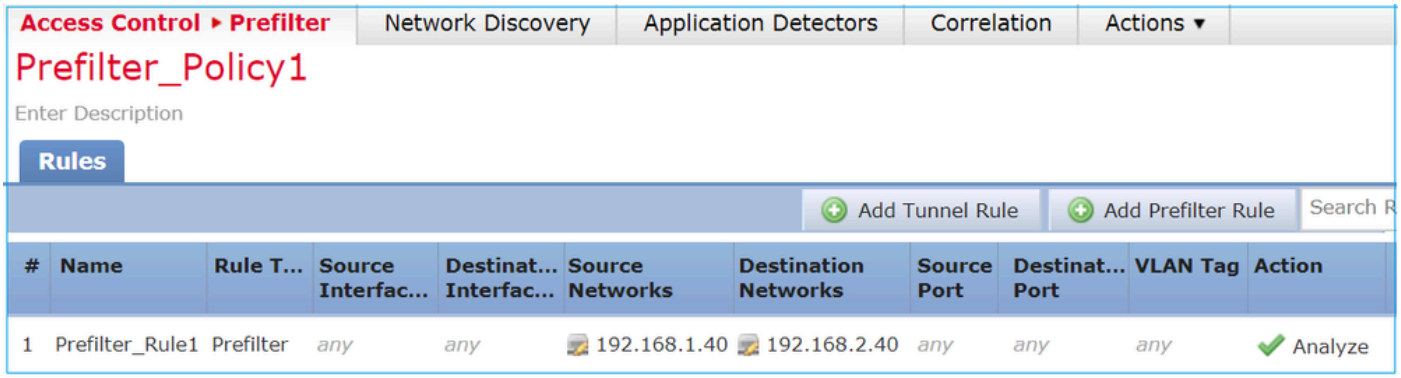
Action Prefilter Policy Fastpath (Fastpath pour la politique de préfiltre) (ensemble en ligne avec dérivateur)

Il s'agit du même cas que le cas Inline-Set.

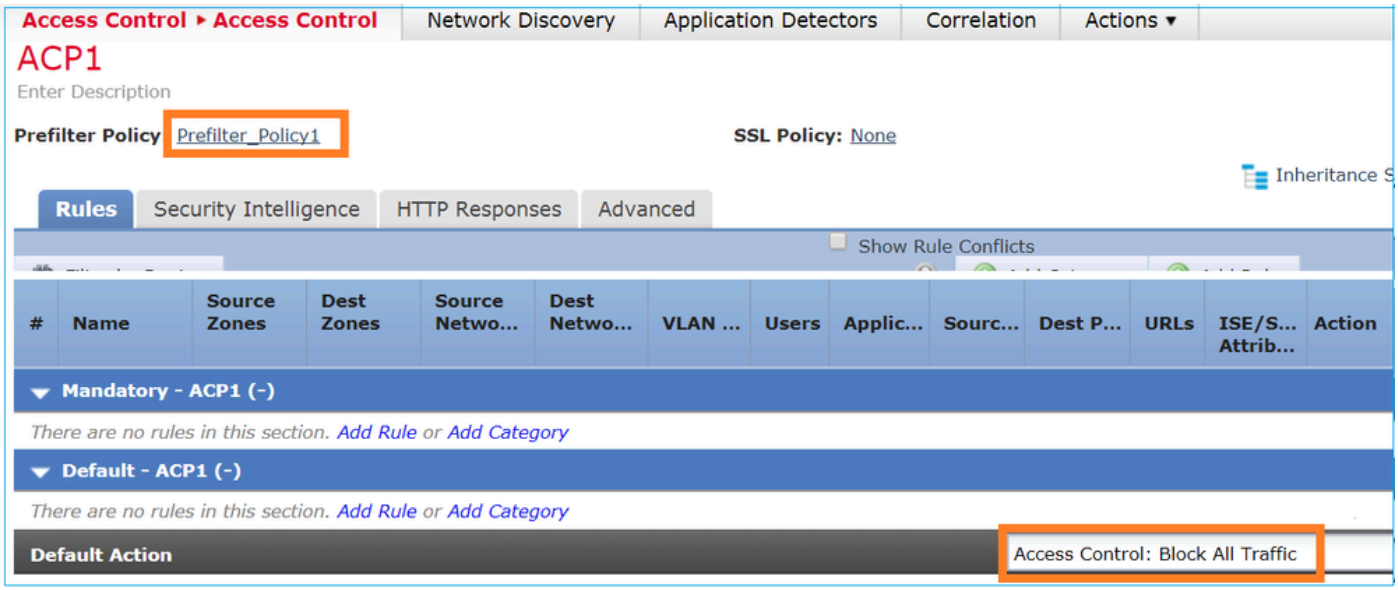
Action Prefilter Policy Analyze (analyse de la politique de préfiltre)

Scénario 1. Préfiltrer l'analyse avec la règle de blocage ACP

Vérifiez la stratégie de préfiltre qui contient la règle Analyze :



L'ACP contient uniquement la règle par défaut qui est définie sur Bloquer tout le trafic :



La stratégie déployée dans le moteur FTD Snort (fichier ngfw.rules) :

<#root>

```
# Start of tunnel and priority rules.

# These rules are evaluated by LINA. Only tunnel tags are used from the matched rule id.

268435460 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any  (tunnel -1)
268435459 allow any any  1025-65535 any any  3544 any 17  (tunnel -1)
268435459 allow any any  3544 any any  1025-65535 any 17  (tunnel -1)
268435459 allow any any  any any any  any any 47  (tunnel -1)
268435459 allow any any  any any any  any any 41  (tunnel -1)
268435459 allow any any  any any any  any any 4  (tunnel -1)
# End of tunnel and priority rules.

# Start of AC rule.

268435458 deny any any  any any any  any any any  (log dcforward flowstart)

# End of AC rule.
```

La stratégie déployée dans le moteur FTD LINA :

<#root>

```
access-list CSM_FW_ACL_ line 3 advanced

permit
```

```
 ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 (hitcnt=0) 0xb788b786
```

Vérifiez le comportement

Le traceur de paquets affiche le paquet est autorisé par LINA, il est transféré au moteur Snort (en raison de l'action permit) et le moteur Snort retourne un verdict de bloc comme l'action par défaut de l'AC est mise en correspondance.

Remarque : Le renifleur n'évalue pas le trafic en fonction des règles du tunnel.

Lorsque vous tracez un paquet, le résultat est le même :

<#root>

```
firepower#

packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40

...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460

access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:

 This packet will be sent to snort for additional processing where a verdict will be reached

…
Phase: 14

Type: SNORT

Subtype:

Result: DROP

Config:
Additional Information:
Snort Trace:
Packet: ICMP
```

```
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType
```

Firewall: block rule, id 268435458, drop

```
Snort: processed decoder alerts or actions queue, drop
NAP id 1, IPS id 0,
```

Verdict BLOCKLIST, Blocked by Firewall

```
Snort Verdict:
```

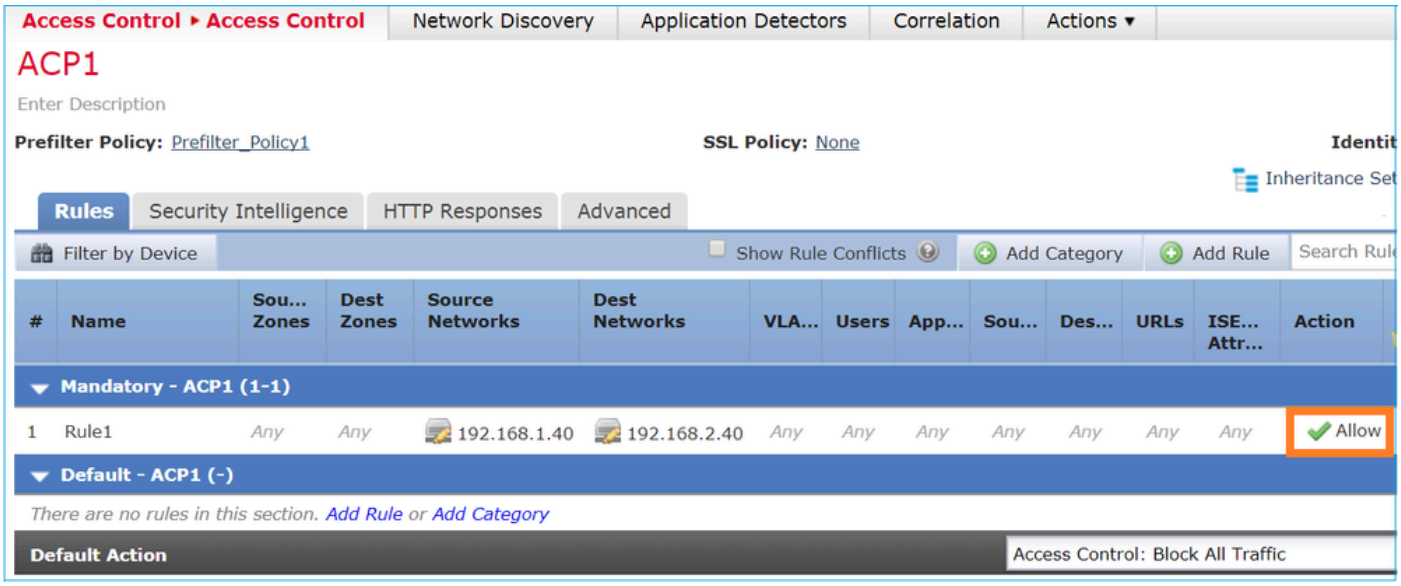
(block-list) block list this flow

```
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
```

Drop-reason: (firewall) Blocked by the firewall preprocessor

Scénario 2. Préfiltrer l'analyse avec la règle d'autorisation ACP

Si l'objectif est de permettre au paquet de traverser le FTD, vous devez ajouter une règle dans ACP. L'action peut être Autoriser ou Approuver, ce qui dépend de l'objectif (par exemple, si vous voulez appliquer une inspection L7, vous devez utiliser l'action Autoriser) :



La stratégie déployée dans le moteur FTD Snort :

<#root>

```
# Start of AC rule.

268435461 allow any 192.168.1.40 32 any any 192.168.2.40 32 any any any

268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

Dans le moteur LINA :

<#root>

```
access-list CSM_FW_ACL_ line 3 advanced

permit

 ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 (hitcnt=1) 0xb788b786
```

Vérifiez le comportement

Le traceur de paquets montre que le paquet correspond à la règle 268435460 dans LINA et 268435461 dans le moteur Snort :

<#root>

```
firepower#

packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40

...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced

permit

 ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:
```

This packet will be sent to snort for additional processing where a verdict will be reached

…
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType
Firewall:

allow rule, id 268435461, allow

NAP id 1, IPS id 0,

Verdict PASS

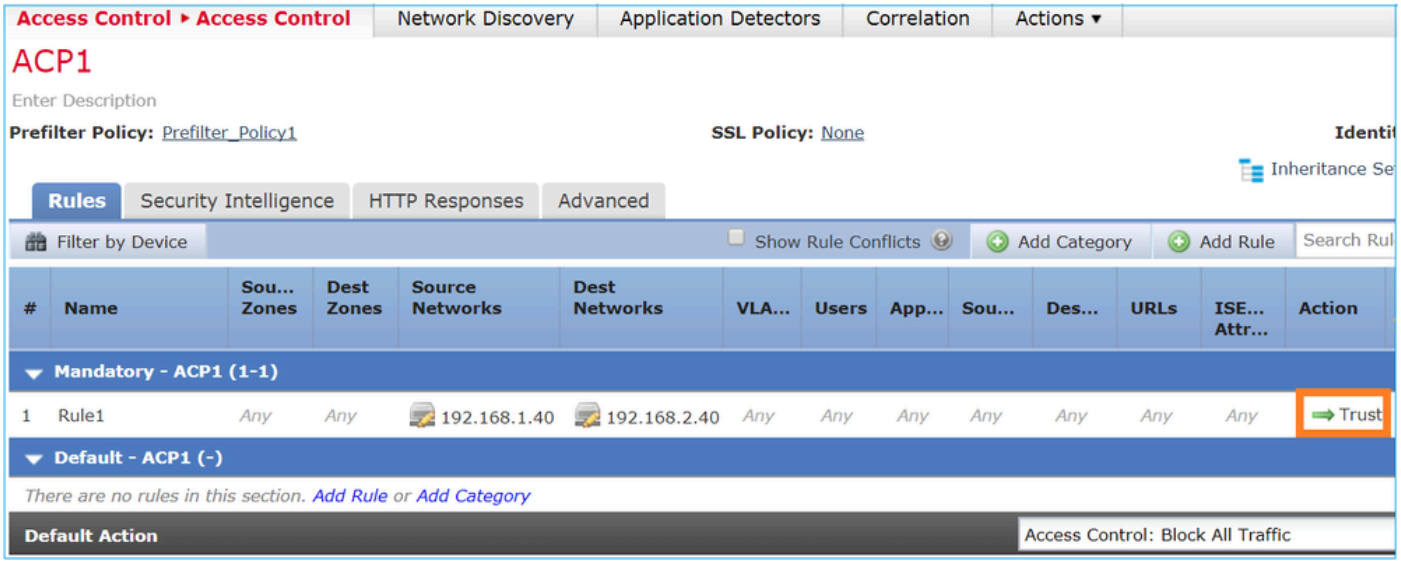
Snort Verdict: (pass-packet) allow this packet

…
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up

Action: allow

Scénario 3. Préfiltrer l'analyse avec la règle d'approbation ACP

Reportez-vous à l'image de stratégie de préfiltrage si l'ACP contient une règle d'approbation :



Renifleur :

<#root>

```
# Start of AC rule.
```

268435461 fastpath any 192.168.1.40 32 any any 192.168.2.40 32 any any any

```
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

LINA :

<#root>

```
access-list CSM_FW_ACL_ line 3 advanced
```

permit

```
 ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460 (hitcnt=2) 0xb788b786
```

N'oubliez pas que si est activé par défaut, la règle Trust est déployée en tant qu'action permit sur LINA ; ainsi, quelques paquets sont redirigés vers le moteur Snort pour inspection.

Vérifiez le comportement

Le traceur de paquets indique que le moteur Snort Permit répertorie le paquet et décharge le flux restant vers LINA :

<#root>

firepower#

packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40

...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global

access-list CSM_FW_ACL_ advanced permit ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460

access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

…
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType
Firewall:

trust/fastpath rule, id 268435461, allow

NAP id 1, IPS id 0,

Verdict PERMITLIST

Snort Verdict: (fast-forward) fast forward this flow

…
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up

Action: allow

Scénario 4. Préfiltrer l'analyse avec la règle d'approbation ACP

Dans ce scénario, Security Intelligence a été désactivée manuellement.

La règle est déployée dans Snort :

<#root>

```
# Start of AC rule.
268435461
```

fastpath

```
 any 192.168.1.40 32 any any 192.168.2.40 32 any any any
268435458 deny any any  any any any  any any any  (log dcforward flowstart)
# End of AC rule.
```

Dans LINA, la règle est déployée en tant qu'approbation. Un paquet correspond à la règle d'autorisation (vérifiez le nombre de succès ACE) qui est déployée en raison de la règle Analyze Prefilter et le paquet est inspecté par le moteur Snort :

<#root>

```
access-list CSM_FW_ACL_ line 3 advanced
```

permit ip host 192.168.1.40 host 192.168.2.40

```
 rule-id 268435460 (hitcnt=3) 0xb788b786
...
access-list CSM_FW_ACL_ line 13 advanced
```

trust ip host 192.168.1.40 host 192.168.2.40

```
 rule-id 268435461 event-log flow-end (hitcnt=0) 0x5c1346d6
...
access-list CSM_FW_ACL_ line 16 advanced
```

deny ip any any

```
 rule-id 268435458 event-log flow-start (hitcnt=0) 0x97aa021a
```

Vérifiez le comportement

<#root>

```
firepower#

packet-tracer input INSIDE icmp 192.168.1.40 8 0 192.168.2.40


...
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced

permit

 ip host 192.168.1.40 host 192.168.2.40 rule-id 268435460
access-list CSM_FW_ACL_ remark rule-id 268435460: PREFILTER POLICY: Prefilter_Policy1
access-list CSM_FW_ACL_ remark rule-id 268435460: RULE: Prefilter_Rule1
Additional Information:


This packet will be sent to snort for additional processing where a verdict will be reached


...
Phase: 14
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: ICMP
AppID: service ICMP (3501), application unknown (0)
Firewall: starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, sgt 65535, user 9999997, icmpType
Firewall:

trust/fastpath rule, id 268435461, allow

NAP id 1, IPS id 0,

Verdict PERMITLIST

Snort Verdict: (fast-forward) fast forward this flow
…
Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up

Action: allow
```

Points principaux

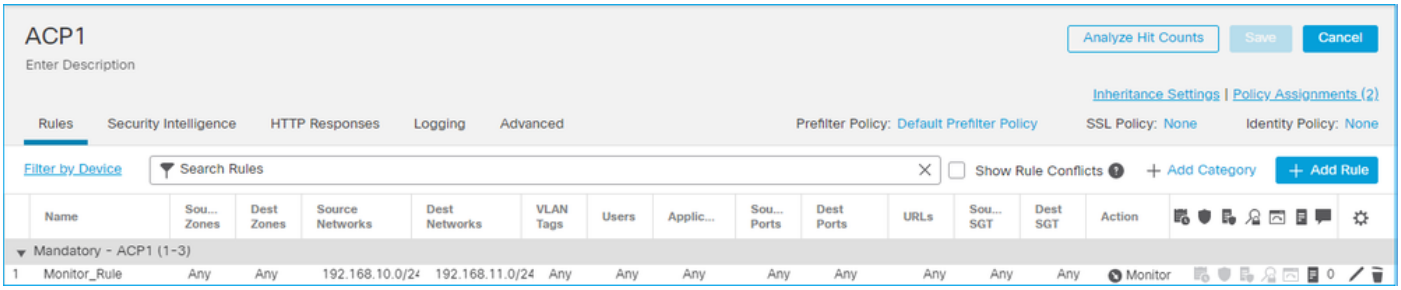
- L'action Analyze est déployée en tant que règle d'autorisation dans le moteur LINA. Cela a un effet sur le paquet à transmettre au moteur Snort pour inspection.
- L'action Analyze ne déploie aucune règle dans le moteur Snort. Vous devez vous assurer que vous configurez une règle dans ACP correspondant dans Snort.
- En fonction de la règle ACP déployée dans Snort (block vs allow vs fastpath), aucun paquet, tous les paquets ou quelques-uns sont autorisés par Snort.

Scénarios :

- Un exemple d'utilisation d'Analyze Action est quand vous avez une règle FastPath large dans la politique de préfiltrage et que vous voulez mettre quelques exceptions pour des flux spécifiques afin qu'ils soient inspectés par Snort.

Action Monitor (surveillance) de la politique de contrôle d’accès

Une règle Monitor (surveillance) configurée sur l’interface utilisateur de Cisco FMC :



La règle de surveillance est déployée sur le moteur FTD LINA en tant qu'action d'autorisation et sur le moteur Snort en tant qu'action d'audit :

<#root>

```
firepower#
```

show access-list

```
…
access-list CSM_FW_ACL_ line 10 advanced
```

permit

```
 ip 192.168.10.0 255.255.255.0 192.168.11.0 255.255.255.0 rule-id
```

```
268438863

 (hitcnt=0) 0x61bbaf0c
```

La règle du renifleur :

```
<#root>

admin@firepower:~$

cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules


…
# Start of AC

rule.
268438863 audit

 any 192.168.10.0 24 any any 192.168.11.0 24 any any any (log dcforward flowend)
# End rule 268438863
```

Points principaux

- La règle de surveillance ne supprime ni n'autorise le trafic, mais elle génère un événement de connexion. Le paquet est vérifié par rapport aux règles suivantes et est autorisé ou abandonné.
- Les événements de connexion FMC montrent que le paquet correspond à deux règles :



Le résultat de la commande System support trace montre que les paquets correspondent aux deux règles :

```
<#root>

>
```

```
system support trace


Enable firewall-engine-debug too? [n]:

y

Please specify an IP protocol: tcp
Please specify a client IP address:

192.168.10.50

Please specify a client port:
Please specify a server IP address:

192.168.11.50

Please specify a server port:
Monitoring packet tracer and firewall debug messages


192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 419031630
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.50-41922 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 new firewall session
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 Starting AC with minimum 2, 'Monitor_Rule', and IP
192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19

match rule order 2, 'Monitor_Rule', action Audit

192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19

match rule order 3, 'trust_L3-L4', action Trust

192.168.10.50-41922 > 192.168.11.50-80 6 AS 1-1 I 19 MidRecovery data sent for rule id: 268438858,rule_
```

⚠ Mise en garde : Vous devez utiliser les commandes de support du système sous la direction du support de Cisco, à l'exception des commandes documentées dans le guide des commandes de support du système ssl-client-hello- , qui sont pour une utilisation générale.

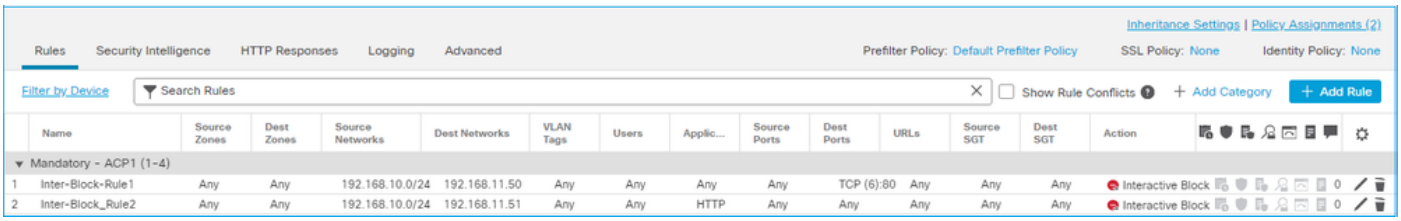
En outre, utilisez toujours les filtres appropriés et ne laissez pas la commande s'exécuter indéfiniment, car cela peut affecter les performances du périphérique.

Scénarios :

Utilisé pour surveiller l’activité du réseau et générer un événement de connexion.

Action Interactive Block (blocage interactif) de la politique de contrôle d'accès

Une règle Interactive Block (blocage interactif) configurée sur l'interface utilisateur de Cisco FMC :



La règle de blocage interactif est déployée sur le moteur LINA FTD en tant qu'action d'autorisation et sur le moteur Snort en tant que règle de contournement :

<#root>

```
firepower#

show access-list

…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced

permit

 tcp 192.168.10.0 255.255.255.0 host 192.168.11.50 eq www rule-id 268438864 (hitcnt=3) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced

permit

 ip 192.168.10.0 255.255.255.0 host 192.168.11.51 rule-id 268438865 (hitcnt=0) 0x622350d0
```

Moteur du renifleur :

<#root>

```
admin@firepower:~$

cat /var/sf/detection_engines/9e080e5c-adc3-11ea-9d37-44884cf7e9ba/ngfw.rules

…
# Start of AC rule.
268438864
```

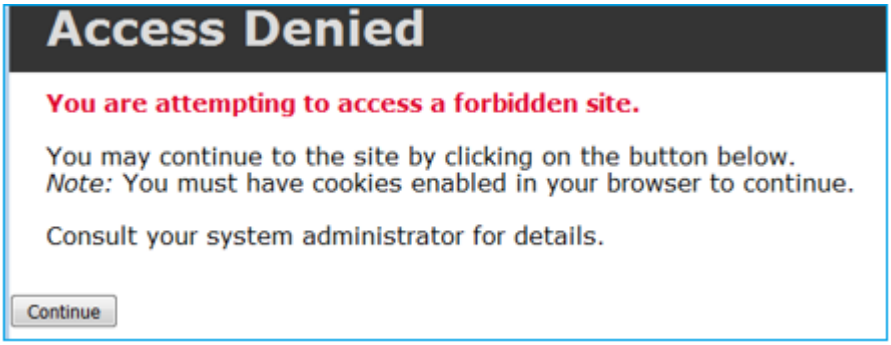
bypass

```
 any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865
```

bypass

```
 any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1) (ip_protos 6, 17)
# End rule 268438865
```

La règle Interactive Block (blocage interactif) invite l'utilisateur à interdire la destination:



Par défaut, le pare-feu vous permet de contourner le blocage pendant 600 secondes :



Dans la sortie de trace de support du système, vous pouvez voir que initialement le pare-feu bloque le trafic et affiche la page de blocage :

<#root>

>

system support trace

…

```
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 983273680, ack 2014879580
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 Starting AC with minimum 2, 'Inter-Block-Rule1', a
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 match rule order 2, 'Inter-Block-Rule1',

action Interactive

192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22

bypass action sending HTTP interactive response of 1093 bytes

192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-Block-Ru
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions queue,
192.168.10.52-58717 > 192.168.11.50-80 6 AS 1-1 I 22 deleting firewall session flags = 0x800, fwFlags =
192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 22, NAP id 1, IPS id 0,

Verdict BLACKLIST

192.168.10.52-58717 - 192.168.11.50-80 6 AS 1-1 CID 0 ===>

Blocked by Firewall

Verdict reason is sent to DAQ
```

Une fois que l'utilisateur a sélectionné Continue (ou actualise la page du navigateur), le débogage montre que les paquets sont autorisés par la même règle, qui imite une action Allow :

<#root>

```
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1357413630, ack 2607625293
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 Starting AC with minimum 2, 'Inter-Block-Rule1', an
192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8 match rule order 2, 'Inter-Block-Rule1',

action Interactive

192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8

bypass action interactive bypass

192.168.10.52-58718 > 192.168.11.50-80 6 AS 1-1 I 8

allow action

192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1', allow
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-Block-R
192.168.10.52-58718 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 8, NAP id 1, IPS id 0,

Verdict PASS
```

⚠ Mise en garde : Vous devez utiliser les commandes de support du système sous la direction du support de Cisco, à l'exception des commandes documentées dans le guide de commandes system support ssl-client-hello- , qui est pour une utilisation générale.

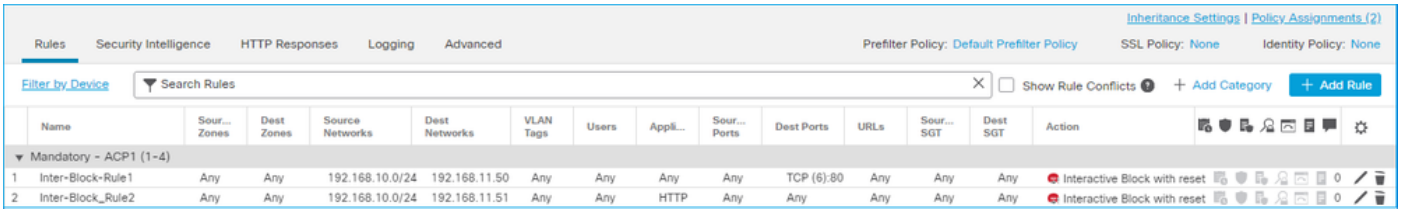
En outre, utilisez toujours les filtres appropriés et ne laissez pas la commande s'exécuter indéfiniment, car cela peut affecter les performances du périphérique.

Scénarios :

Afficher une page d'avertissement aux utilisateurs Web et leur proposer la possibilité de continuer.

Action Interactive Block (blocage interactif) de la politique de contrôle d’accès avec réinitialisation

Une règle Interactive Block (blocage interactif) avec réinitialisation configurée sur l’interface utilisateur de Cisco FMC :



Le bloc interactif avec une règle de réinitialisation est déployé sur le moteur LINA FTD en tant qu'action d'autorisation et sur le moteur Snort en tant que règle d'initialisation :

<#root>

```
firepower#
```

show access-list

```
…
access-list CSM_FW_ACL_ line 9 remark rule-id 268438864: L7 RULE: Inter-Block-Rule1
access-list CSM_FW_ACL_ line 10 advanced
```

permit

```
 tcp 192.168.10.0 255.255.255.0 host 192.168.11.50 eq www rule-id 268438864 (hitcnt=13) 0xba785fc0
access-list CSM_FW_ACL_ line 11 remark rule-id 268438865: ACCESS POLICY: ACP1 - Mandatory
access-list CSM_FW_ACL_ line 12 remark rule-id 268438865: L7 RULE: Inter-Block_Rule2
access-list CSM_FW_ACL_ line 13 advanced
```

```
permit

 ip 192.168.10.0 255.255.255.0 host 192.168.11.51 rule-id 268438865 (hitcnt=0) 0x622350d0
```

Moteur du renifleur :

<#root>

```
# Start of AC rule.
268438864

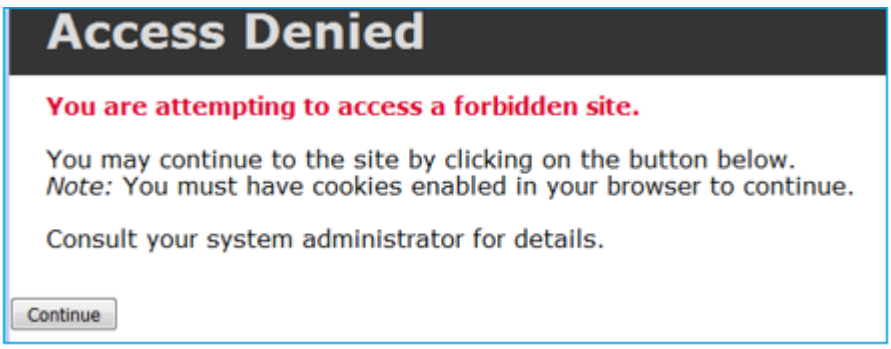
intreset

 any 192.168.10.0 24 any any 192.168.11.50 32 80 any 6
# End rule 268438864
268438865

intreset

 any 192.168.10.0 24 any any 192.168.11.51 32 any any any (appid 676:1) (ip_protos 6, 17)
# End rule 268438865
```

Comme avec le Block with Reset, l'utilisateur peut sélectionner l'option Continue :



Dans le débogage Snort, l'action indiquée dans Réinitialisation interactive.

⚠ Mise en garde : Vous devez utiliser les commandes de support du système sous la direction du support de Cisco, à l'exception des commandes documentées dans le guide des commandes de support du système ssl-client-hello- , qui est pour une utilisation générale.

En outre, utilisez toujours les filtres appropriés et ne laissez pas la commande s'exécuter indéfiniment, car cela peut affecter les performances du périphérique.

<#root>

>

system support trace

Enable firewall-engine-debug too? [n]:

y

Please specify an IP protocol: tcp
Please specify a client IP address:

192.168.10.52

Please specify a client port:
Please specify a server IP address:

192.168.11.50

Please specify a server port:
Monitoring packet tracer and firewall debug messages

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, SYN, seq 3232128039
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Session: new snort session
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 new firewall session
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-Rule1', a
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1', action In
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 MidRecovery data sent for rule id: 268438864,rule_
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 HitCount data sent for rule id: 268438864,
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict PASS

192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Packet: TCP, SYN, ACK, seq 2228213518, ack 323212
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
192.168.11.50-80 - 192.168.10.52-58958 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack 2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service unknown (0), application unknown (
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0, Verdict PASS

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3232128040, ack 2228213519
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 Starting AC with minimum 2, 'Inter-Block-Rule1', a
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 match rule order 2, 'Inter-Block-Rule1',

action Interactive Reset

192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24

bypass action sending HTTP interactive response of 1093 bytes

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive block rule, 'Inter-Block-Ru
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort: processed decoder alerts or actions queue,
192.168.10.52-58958 > 192.168.11.50-80 6 AS 1-1 I 24 deleting firewall session flags = 0x800, fwFlags =
192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 24, NAP id 1, IPS id 0,

```
Verdict BLACKLIST

192.168.10.52-58958 - 192.168.11.50-80 6 AS 1-1 CID 0 ===>

 Blocked by Firewall

Verdict reason is sent to DAQ
```

La page de blocage s'affiche pour l'utilisateur final. Si l'utilisateur sélectionne Continuer (ou actualise la page Web), la même règle correspond, ce qui autorise le trafic à travers :

<#root>

```
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 1593478294, ack 3135589307
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 Starting AC with minimum 2, 'Inter-Block-Rule1', a
192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 match rule order 2, 'Inter-Block-Rule1',

action Interactive Reset

192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14

bypass action interactive bypass

192.168.10.52-58962 > 192.168.11.50-80 6 AS 1-1 I 14 allow action
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1', allow
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-Block-R
192.168.10.52-58962 - 192.168.11.50-80 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0,

Verdict PASS


192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Packet: TCP, ACK, seq 3135589307, ack 1593478786
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 AppID: service HTTP (676), application unknown (0
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: allow rule, 'Inter-Block-Rule1', allow
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Firewall: interactive bypass rule, 'Inter-Block-R
192.168.11.50-80 - 192.168.10.52-58962 6 AS 1-1 CID 0 Snort id 14, NAP id 1, IPS id 0,

Verdict PASS
```

Interactive Block (blocage interactif) avec règle de réinitialisation envoie un message de réinitialisation du protocole TCP au trafic non Web :

<#root>

```
firepower#

show cap CAPI | i 11.50
```

```
   2: 22:13:33.112954       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: S 3109534920:310
   3: 22:13:33.113626       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: S 3422362500:342
   4: 22:13:33.113824       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack 3422362501
   5: 22:13:33.114953       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P 3422362501:342
   6: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P 3422362543:342
   7: 22:13:33.114984       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010: P 3422362549:342
   8: 22:13:33.115182       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack 3422362543
   9: 22:13:33.115411       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack 3422362549
  10: 22:13:33.115426       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: . ack 3422362570
  12: 22:13:34.803699       802.1Q vlan#202 P0 192.168.10.50.40010 > 192.168.11.50.21: P 3109534921:310
  13: 22:13:34.804523       802.1Q vlan#202 P0 192.168.11.50.21 > 192.168.10.50.40010:
```

R

```
 3422362570:3422362570(0) ack 3109534931 win 0
```

Connexions secondaires FTD et Trous D'Épingle

Dans les versions plus anciennes (par exemple 6.2.2, 6.2.3), le moteur Snort n'ouvre pas de trous d'épingle pour les connexions secondaires (par exemple, FTD Data) ou lors de l'utilisation de l'action Trust. Dans les versions récentes, ce comportement a changé et le moteur Snort ouvre des trous d'épingle même avec l'action Trust.

Règles de Cisco Firepower Threat Defense (FTD)

- Utilisez les règles de chemin rapide de la stratégie de préfiltrage pour les flux de graisse importants et pour réduire la latence dans la boîte.
- Utilisez les règles Prefilter Block (blocage du préfiltre) pour le trafic qui doit être bloqué en fonction des conditions L3/L4.
- Utilisez les règles d'approbation ACP pour contourner de nombreuses vérifications Snort, mais profitez tout de même de fonctionnalités telles que la stratégie d'identité, la qualité de service, l'analyse de l'environnement, la détection d'applications et les filtres d'URL.
- Placez les règles qui affectent les performances moindres du pare-feu en haut de la politique de contrôle d'accès à l'aide des directives suivantes :
    - Règles de blocage (couches 1 à 4) - Bloc de préfiltrage
    - Autoriser les règles (couches 1 à 4) - Préfiltre FastPath
    - Règles de blocage ACP (couches 1 à 4)
    - Règles d'approbation (couches 1 à 4)
    - Règles de blocage (couches 5 à 7 - Détection d'application, Filtrage d'URL)
    - Autoriser les règles (Couches 1 à 7 - Détection des applications, Filtrage des URL, Stratégie contre les intrusions/Stratégie de fichiers)
    - Règle Block (blocage) (règle par défaut)

- Éviter une consignation excessive (consigner au début ou à la fin ; et éviter les deux en

même temps)
- Soyez conscient de l’extension des règles, pour vérifier le nombre de règles dans LINA

<#root>

```
firepower#

show access-list | include elements

access-list CSM_FW_ACL_;

7 elements

; name hash: 0x4a69e3f3
```

Résumé

Actions du préfiltre

Rule Action (FMC UI)	LINA Action	Snort Action	Notes
Fastpath	Trust	Fastpath	Static Flow Offload to SmartNIC (4100/9300). **No packets** are sent to Snort engine.
Analyze	Permit	-	The ACP rules are checked. **Few** or **all packets** are sent to Snort engine for inspection. Traffic is allowed or dropped based on Snort engine verdict
Block (Prefilter)	Deny	-	Early drop by FTD LINA **No packets** are sent to Snort engine

Actions de la politique de contrôle d’accès

Rule Action (FMC UI)	Additional Conditions	LINA Action	Snort Action	Notes
Block	The rule matches L3/L4 conditions	Deny	Deny	
Block	The rule has L7 conditions	Permit	Deny	
Allow		Permit	Allow	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, or ID) enabled	Permit	Fastpath	6.3+ supports Dynamic Flow Offload (4100/9300)
Trust	(SI, QoS, and ID) disabled	Trust	Fastpath	Static Flow Offload (4100/9300)
Monitor		Permit	Audit	Monitor Rule doesn't drop or permit traffic, but it generates a Connection Event. The packet is checked against subsequent rules and it is either allowed or dropped
Block with reset		Permit	Reset	When a packet matches Block with reset rule FTD sends a TCP Reset packet or an ICMP Type 3 Code 13 Destination Unreachable (Administratively filtered) message
Interactive Block		Permit	Bypass	Interactive Block Rule prompts the user that the destination is forbidden If bypassed, by default, the firewall allows to bypass the block for 600 seconds
Interactive Block with reset		Permit	Intreset	Same as Interactive Block with the addition of a TCP RST in case of non-web traffic

Remarque : Avec le code logiciel FTD 6.3, le déchargement de flux dynamique peut décharger les connexions qui répondent à des critères supplémentaires ; par exemple, les paquets sécurisés qui nécessitent une inspection Snort. Consultez la section Décharger les connexions volumineuses (flux) du Guide de configuration de Firepower Management Center pour plus de détails.

Informations connexes

- Règles de contrôle d'accès de Cisco FTD
- Préfiltres et politiques de préfiltre de Cisco FTD
- Analysez les captures de pare-feu Firepower pour résoudre efficacement les problèmes de réseau
- Utilisation des captures Cisco Firepower Threat Defense (FTD) et du traceur de paquet
- Configurez la connexion sur Cisco FTD à l'aide de Cisco FMC
- Assistance et documentation techniques - Cisco Systems
- Déchargement de connexions importantes

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.