Configuration et mise en oeuvre des stratégies FTD Prefilter

Contenu

Introduction

Ce document décrit la configuration et la mise en oeuvre des stratégies de Pré-filtre de la défense contre des menaces de FirePOWER (FTD).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- ASA5506X qui exécute le code 6.1.0-195 FTD
- Centre de Gestion de FireSIGHT (FMC) ces passages 6.1.0-195
- Deux 3925 Routeurs de Cisco IOS® qui exécute 15.2 images

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Informations générales

Une stratégie de Prefilter est une fonctionnalité introduite dans la version 6.1 et atteint trois objectifs principaux :

1. Appariez le trafic basé sur les en-têtes intérieures et externes
2. Fournissez le contrôle d'accès tôt qui permet à un écoulement pour sauter renifle l'engine complètement
3. Fonctionnez comme texte d'attente pour les entrées de contrôle d'accès (as) qui sont migrées de l'outil de transfert de l'appliance de sécurité adaptable (ASA).

Temps de fin de laboratoire : 30 minutes.

Configurez

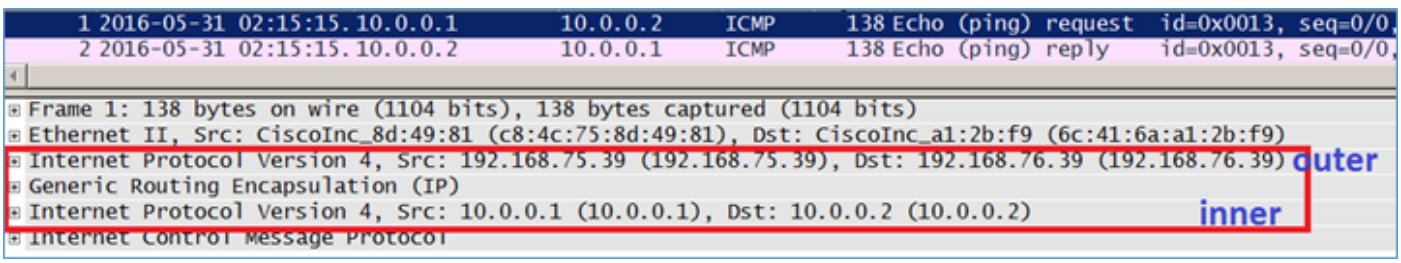
cas d'utilisation 1 de stratégie de Pré-filtre

Une stratégie de Pré-filtre peut utiliser un **type de règle de tunnel** qui permet à FTD pour filtrer basé sur chacun des deux intérieurs et/ou le trafic percé un tunnel par en-tête IP extérieure. Lorsque cet article a été écrit, le trafic percé un tunnel se rapporte :

- Encapsulation de routage générique (GRE)
- IP-in-IP
- IPv6-in-IP
- Port 3544 de Teredo

Considérez un tunnel GRE suivant les indications de l'image ici.

Quand vous cinglez de R1 à R2 avec l'utilisation d'un tunnel GRE, le trafic passe par les aspects de Pare-feu suivant les indications de l'image.



Si le Pare-feu est un **périphérique ASA,** il vérifie l'**en-tête IP externe** suivant les indications de l'image.


```
ASA# show conn
GRE OUTSIDE 192.168.76.39:0 INSIDE  192.168.75.39:0, idle 0:00:17, bytes 520, flags
```

Si le Pare-feu est un **périphérique de FirePOWER,** il vérifie l'**en-tête IP intérieure** suivant les indications de l'image.

Avec la stratégie de pré-filtre, un périphérique FTD peut apparier le trafic basé sur les en-têtes intérieures et externes.

Question principale :

Périphérique	Contrôles
ASA	IP externe
Reniflez	IP intérieur
FTD	Externe (Prefilter) + IP intérieur (contrôle d'accès Policy(ACP))

cas d'utilisation 2 de stratégie de Pré-filtre

Une stratégie de Pré-filtre peut utiliser un **type de règle de Prefilter** qui peut fournir le contrôle d'accès tôt et permettre à un écoulement pour sauter reniflez l'engine complètement suivant les indications de l'image.

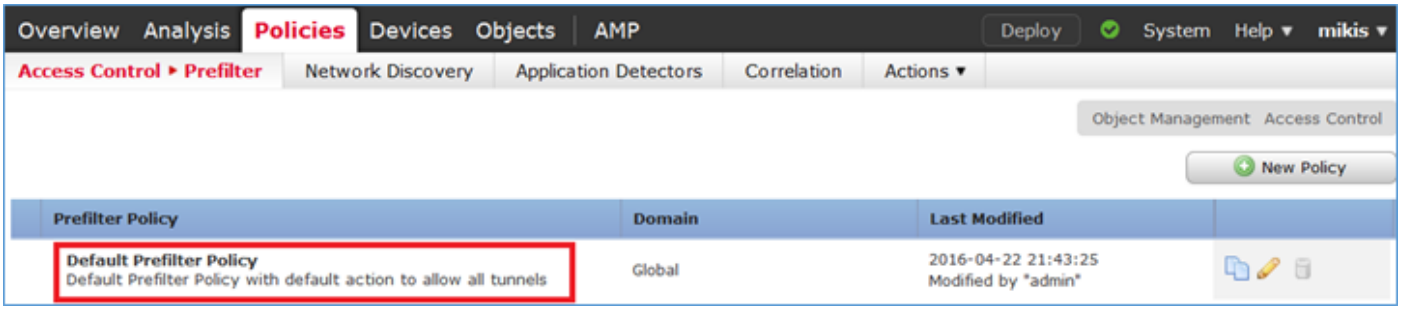
La tâche 1. vérifient la stratégie par défaut de Pré-filtre

Condition requise de tâche :

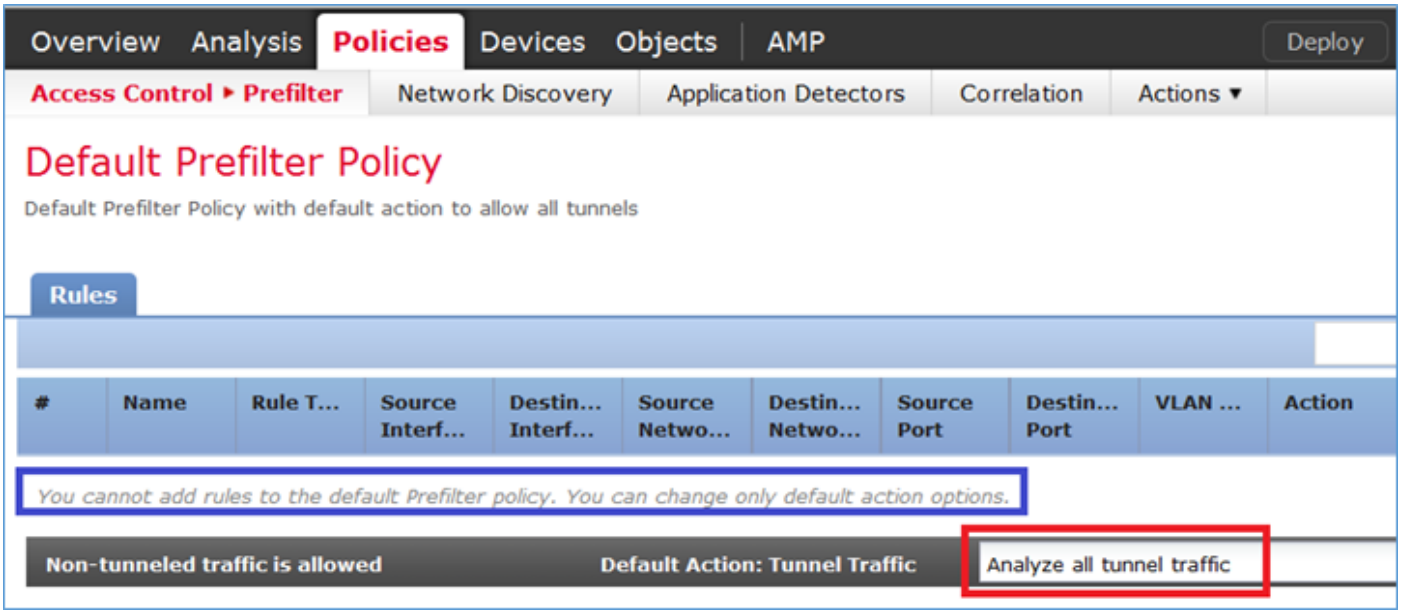
Vérifiez la stratégie par défaut de Prefilter

Solution :

Étape 1. Naviguez vers les **stratégies > le contrôle d'accès > le Prefilter**. Une stratégie par défaut de Prefilter existe déjà suivant les indications de l'image.



Étape 2. Choisi **éditez** pour voir les paramètres de la stratégie suivant les indications de l'image.



Étape 3. La stratégie de Pré-filtre est déjà reliée à la stratégie de contrôle d'accès suivant les indications de l'image.

Vérification CLI (LINA)

des règles de Pré-filtre sont ajoutées sur ACLs :

```
firepower# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list CSM_FW_ACL_; 5 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and
Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 5 advanced permit gre any any rule-id 9998 (hitcnt=5) 0x52c7a066
access-list CSM_FW_ACL_ line 6 advanced permit udp any any eq 3544 rule-id 9998 (hitcnt=0)
0xcf6309bc
```

Le trafic percé un tunnel par bloc de la tâche 2. avec la balise

Condition requise de tâche :

Le trafic d'ICMP de bloc qui est percé un tunnel à l'intérieur du tunnel GRE.

Solution :

Étape 1. Si vous appliquez ces l'ACP, vous pouvez voir que le trafic de Protocole ICMP (Internet Control Message Protocol) est bloqué, aucune matière si elle passe par le tunnel GRE ou pas, suivant les indications de l'image.


```
R1# ping 192.168.76.39
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
R1# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Dans ce cas, vous pouvez employer une stratégie de Pré-filtre pour répondre à l'exigence de tâche. La logique est comme suit :

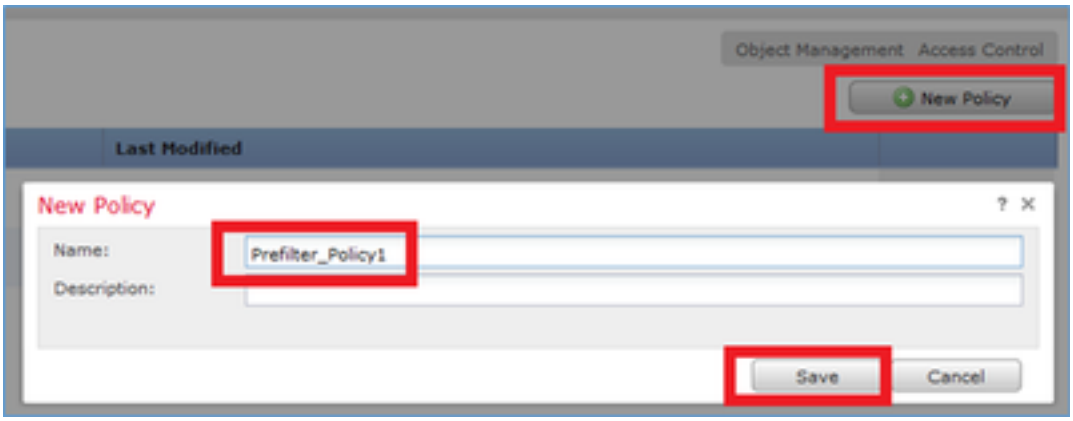
1. Vous étiquetez tous les paquets qui sont encapsulés à l'intérieur de GRE.
2. Vous créez une stratégie de contrôle d'accès qui apparie les paquets balisés et bloque l'ICMP.

Du point de vue d'architecture, les paquets sont vérifiés contre les règles de pré-filtre de LINA,

puis reniflent des règles de pré-filtre et l'ACP et reniflent finalement demande à LINA pour relâcher. Le premier paquet le fait par le périphérique FTD.

Étape 1. Définissez une balise pour le trafic percé un tunnel.

Naviguez vers les **stratégies > le contrôle d'accès > le Prefilter** et créez une nouvelle stratégie de Prefilter. Souvenez-vous que la stratégie par défaut de Prefilter ne peut pas être éditée suivant les indications de l'image.

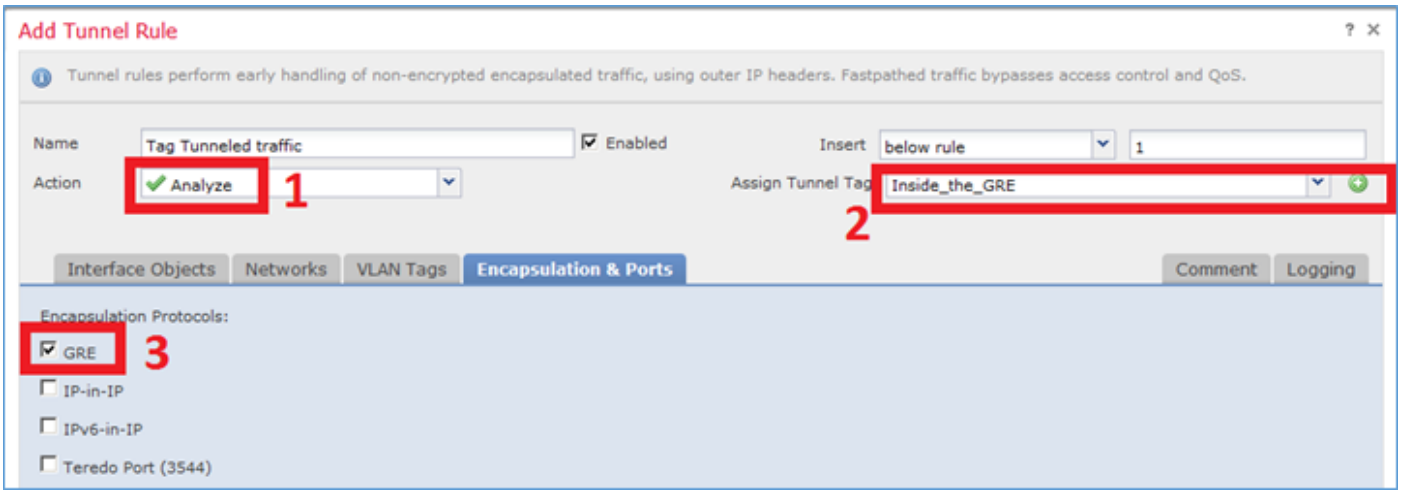


Àl'intérieur de la stratégie de Prefilter, vous pouvez définir deux types de règles :

- Règle de tunnel
- Règle de Prefilter

Vous pouvez penser à ces deux en tant que caractéristiques totalement différentes qui peuvent être configurées dans une stratégie de Prefilter.

Pour cette tâche, il est nécessaire de définir une règle de tunnel suivant les indications de l'image.

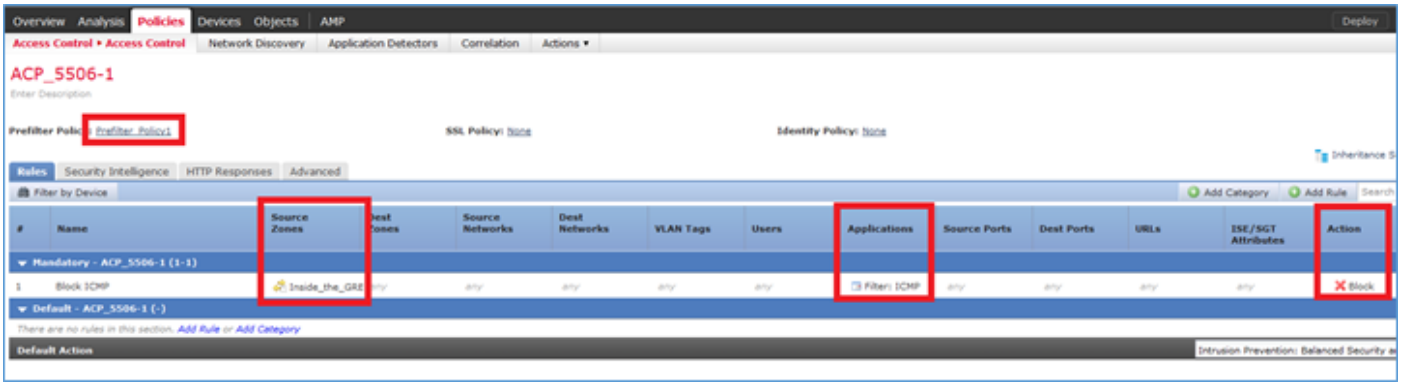


Quant aux actions :

Action	Description
Analysez	Après LINA, l'écoulement est vérifié par l'engine Snort. Sur option, une balise de tunnel être assignée au trafic percé un tunnel.
Bloc	L'écoulement est bloqué par LINA. L'en-tête externe doit être vérifiée.
Fastpath	L'écoulement est manipulé seulement par LINA sans nécessité d'engager l'engine de re

Étape 2. Définissez la stratégie de contrôle d'accès pour le trafic étiqueté.

Bien qu'il puisse ne pas être très intuitif au début, la balise de tunnel peut être utilisée par une règle de stratégie de contrôle d'accès comme **zone de source**. Naviguez vers les **stratégies > le contrôle d'accès** et créez une règle qui bloque l'ICMP pour le trafic étiqueté suivant les indications de l'image.



Note: La nouvelle stratégie de Prefilter est reliée à la stratégie de contrôle d'accès.

Vérification :

Capture d'enable sur LINA et sur CLISH :

```
firepower# show capture
capture CAPI type raw-data trace interface inside [Capturing - 152 bytes]
capture CAPO type raw-data trace interface outside [Capturing - 152 bytes]
```

```
> capture-traffic
Please choose domain to capture traffic from:
  0 - br1
  1 - Router

Selection? 1

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

De R1, essai pour cingler le périphérique du tunnel du distant GRE. Le ping échoue :

```
R1# ping 10.0.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

La capture CLISH prouve que la première requête d'écho est passée par FTD et la réponse a été bloquée :

```
Options: -n
18:21:07.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2:
ICMP echo request, id 65, seq 0, length 80
18:21:07.759939 IP 192.168.76.39 > 192.168.75.39: GREv0, length 104: IP 10.0.0.2 > 10.0.0.1:
```

```
ICMP echo reply, id 65, seq 0, length 80
18:21:09.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2:
ICMP echo request, id 65, seq 1, length 80
18:21:11.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2:
ICMP echo request, id 65, seq 2, length 80
18:21:13.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2:
ICMP echo request, id 65, seq 3, length 80
18:21:15.759939 IP 192.168.75.39 > 192.168.76.39: GREv0, length 104: IP 10.0.0.1 > 10.0.0.2:
ICMP echo request, id 65, seq 4, length 80
```

La capture de LINA confirme ceci :

```
> show capture CAPI | include ip-proto-47
 102: 18:21:07.767523  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 107: 18:21:09.763739  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 111: 18:21:11.763769  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 115: 18:21:13.763784  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
 120: 18:21:15.763830  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
>
> show capture CAPO | include ip-proto-47
  93: 18:21:07.768133  192.168.75.39 > 192.168.76.39:  ip-proto-47, length 104
  94: 18:21:07.768438  192.168.76.39 > 192.168.75.39:  ip-proto-47, length 104
```

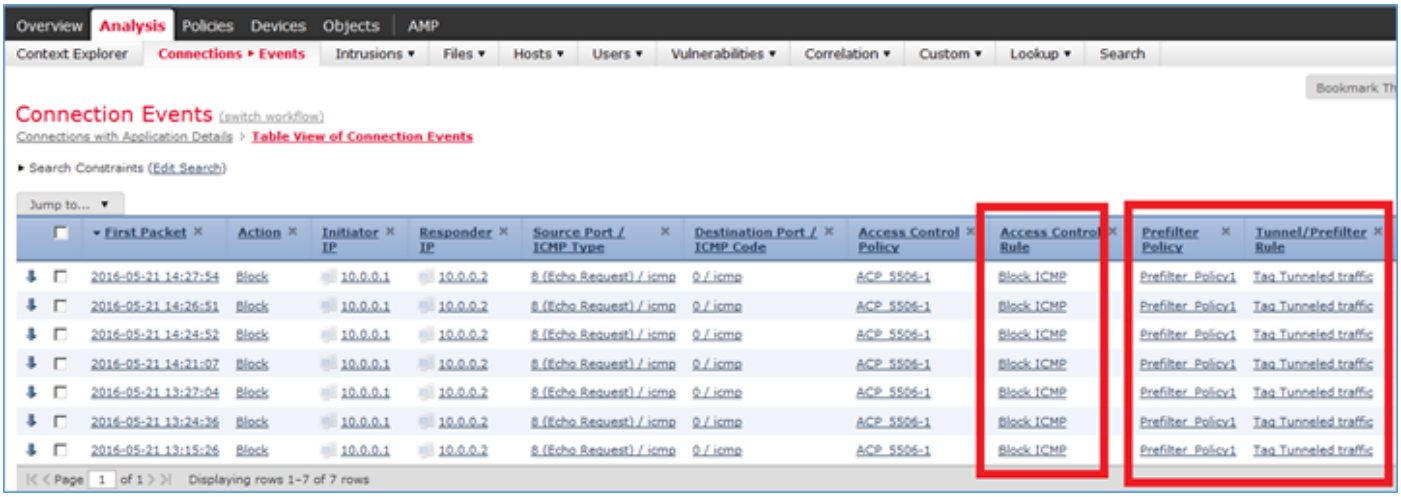
Activez le Pare-feu-engine-debug CLISH, les compteurs clairs de baisse d'ASP de LINA et faites le même test. Les CLISH mettent au point prouvent que pour la requête d'écho vous avez apparié la règle de prefilter et pour la réponse d'écho la règle ACP :

```
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 New session
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 using prefilter rule 268434441 with tunnel zone 1
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1
-> -1, geo 0 -> 0, vlan 0, sgt tag: 65535, svc 0, payload 0, client 0, misc 0, user 9999997,
icmpType 8, icmpCode 0
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 pending rule order 3, 'Block ICMP', AppId
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 using prefilter rule 268434441 with tunnel zone 1
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 Starting with minimum 0, id 0 and SrcZone first with zones 1
-> -1, geo 0 -> 0, vlan 0, sgt tag: 65535, svc 3501, payload 0, client 2000003501, misc 0, user
9999997, icmpType 0, icmpCode 0
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 match rule order 3, 'Block ICMP', action Block
10.0.0.1-8 > 10.0.0.2-0 1 AS 1 I 0 deny action
```

La baisse d'ASP prouve que Snort a relâché les paquets :

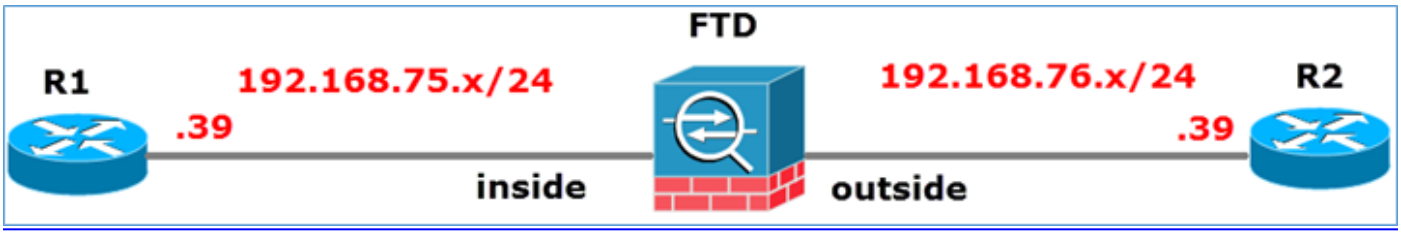
```
> show asp drop

Frame drop:
  No route to host (no-route)                              366
  Reverse-path verify failed (rpf-violated)                  2
  Flow is denied by configured rule (acl-drop)               2
  Snort requested to drop the frame (snort-drop)             5
```

Dans les événements de connexion, vous pouvez voir la stratégie de Prefilter et ordonner que vous étiez assortie suivant les indications de l'image.



Le contournement de la tâche 3. reniflent l'engine avec des règles de Fastpath Prefilter

[Diagramme du réseau](#)

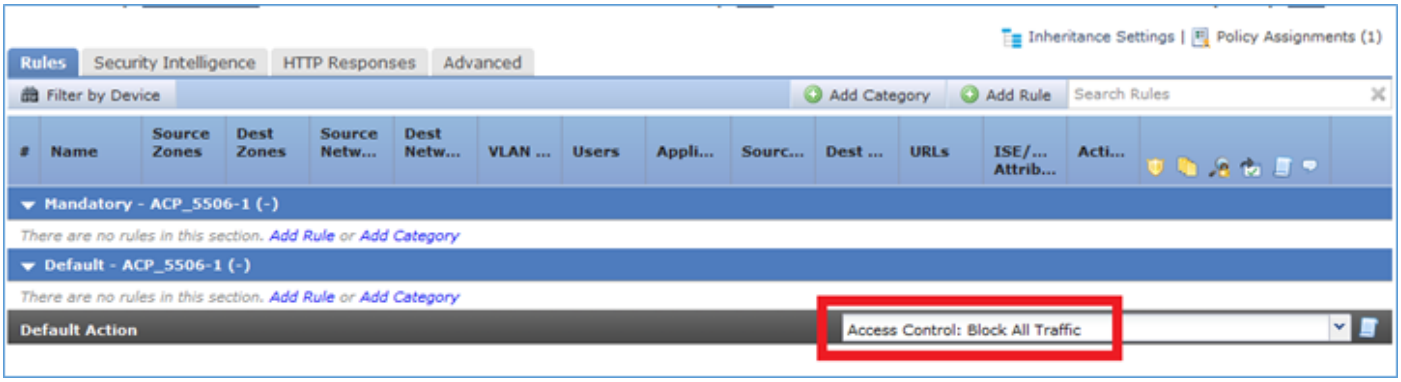


Condition requise de tâche :

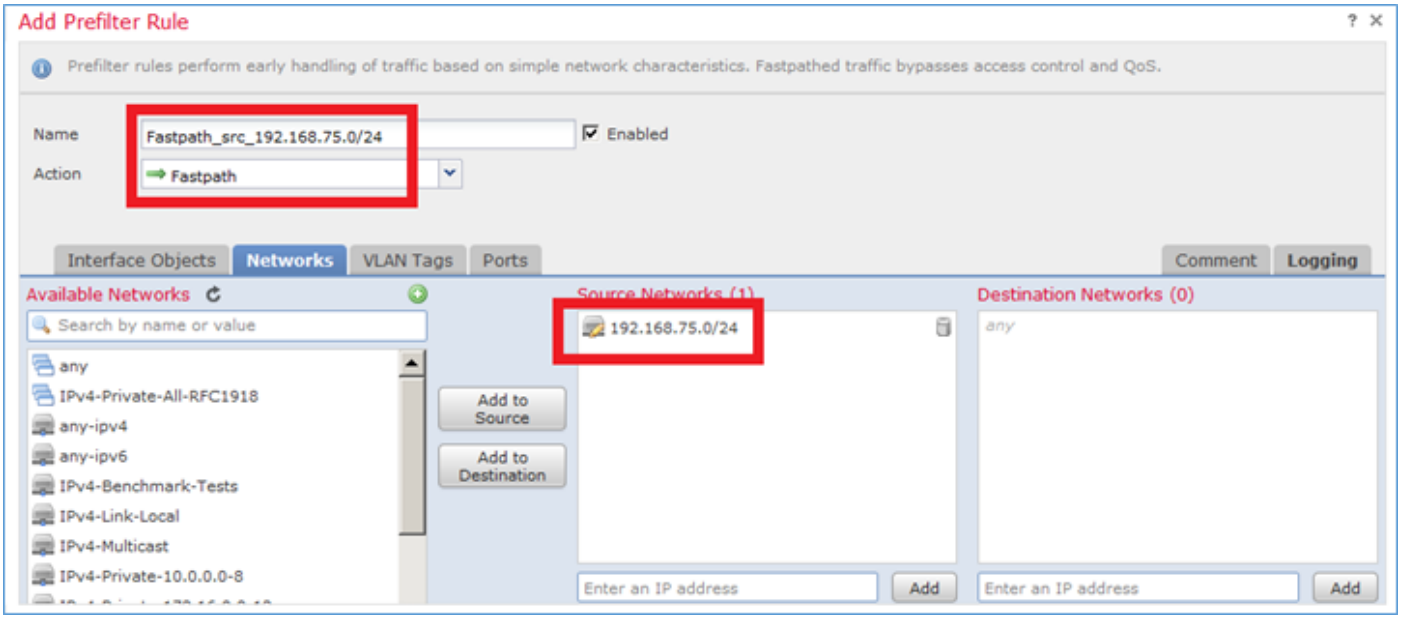
1. Retirez les règles existantes de stratégie de contrôle d'accès et ajoutez une règle de stratégie de contrôle d'accès qui bloque tout le trafic.
2. Configurez une règle de stratégie de Prefilter que saute l'engine de renifler pour le trafic originaire du réseau 192.168.75.0/24.

Solution :

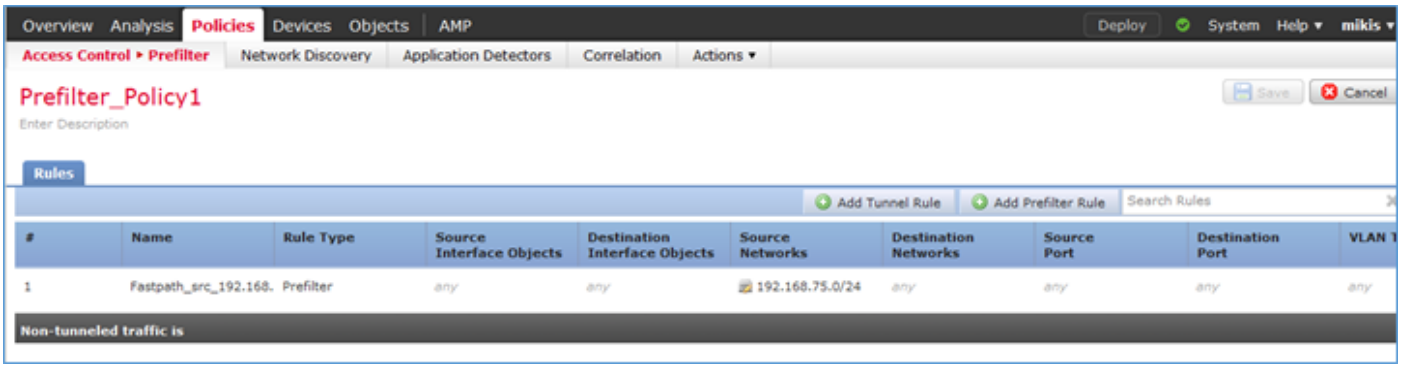
Étape 1. La stratégie de contrôle d'accès qui bloque tout le trafic est suivant les indications de l'image.



Étape 2. Ajoutez une règle de Prefilter avec **Fastpath** comme action pour le réseau 192.168.75.0/24 de source suivant les indications de l'image.



Étape 3. Le résultat est suivant les indications de l'image.



Étape 4. **Sauvegardez** et **déployez-vous**.

Activez la capture avec le suivi sur les deux interfaces FTD :

```
firepower# capture CAPI int inside trace match icmp any any
firepower# capture CAPO int outsid trace match icmp any any
```

Essayez de cingler de R1 (192.168.75.39) à R2 (192.168.76.39) par le FTD. Le ping échoue :

```
R1# ping 192.168.76.39
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.76.39, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Capture sur les expositions d'interface interne :

```
firepower# show capture CAPI

5 packets captured

   1: 23:35:07.281738   192.168.75.39 > 192.168.76.39: icmp: echo request
   2: 23:35:09.278641   192.168.75.39 > 192.168.76.39: icmp: echo request
```

```
   3: 23:35:11.279251   192.168.75.39 > 192.168.76.39: icmp: echo request
   4: 23:35:13.278778   192.168.75.39 > 192.168.76.39: icmp: echo request
   5: 23:35:15.279282   192.168.75.39 > 192.168.76.39: icmp: echo request
5 packets shown
```

Le suivi du premier paquet (requête d'écho) affiche (des points importants mis en valeur) :

Spoiler

suivi du paquet-nombre 1 du show capture CAPI de firepower#

5 paquets capturés

1 : 23:35:07.281738 192.168.75.39 > 192.168.76.39 : ICMP : requête d'écho

Phase : 1

Type : CAPTURE

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Liste d'accès de MAC

Phase : 2

Type : LISTE D'ACCÈS

Sous-type :

Résultat : LAISSEZ

Config :

Règle implicite

Les informations complémentaires :

Liste d'accès de MAC

Phase : 3

Type : RECHERCHE DE ROUTE

Sous-type : Interface de sortie de résolution

Résultat : LAISSEZ

Config :

Les informations complémentaires :

prochain-saut trouvé 192.168.76.39 utilisant l'ifc de sortie dehors

Phase : 4

Type : LISTE D'ACCÈS

Sous-type : log

Résultat : LAISSEZ

Config :

access-group CSM_FW_ACL_ global

la liste d'accès CSM_FW_ACL_ a avancé l'IP 192.168.75.0 255.255.255.0 de **confiance** n'importe quel event-log chacun des deux du règle-id 268434448

règle-id 268434448 de remarque de la liste d'accès CSM_FW_ACL_ : STRATÉGIE PREFILTER : Prefilter_Policy1

règle-id 268434448 de remarque de la liste d'accès CSM_FW_ACL_ : RÈGLE : Fastpath_src_192.168.75.0/24

Les informations complémentaires :

Phase : 5

Type : CONN-SETTINGS

Sous-type :

Résultat : LAISSEZ

Config :

classe-par défaut de class-map

match any

policy-map global_policy

classe-par défaut de classe

placez la connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Les informations complémentaires :

Phase : 6

Type : NAT

Sous-type : par-session

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 7

Type : IP-OPTIONS

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 8

Type : EXAMINEZ

Sous-type : NP-examinez

Résultat : LAISSEZ

Config :

class-map inspection_default

match default-inspection-traffic

policy-map global_policy

class inspection_default

examinez l'ICMP

service-policy global_policy global

Les informations complémentaires :

Phase : 9

Type : EXAMINEZ

Sous-type : NP-examinez

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 10

Type : NAT

Sous-type : par-session

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 11

Type : IP-OPTIONS

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 12

Type : FLOW-CREATION

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Le nouvel écoulement créé avec l'id 52, paquet a acheminé au prochain module

Phase : 13

Type : LISTE D'ACCÈS

Sous-type : log

Résultat : LAISSEZ

Config :

access-group CSM_FW_ACL_ global

la liste d'accès CSM_FW_ACL_ a avancé l'IP 192.168.75.0 255.255.255.0 de confiance n'importe quel event-log chacun des deux du règle-id 268434448

règle-id 268434448 de remarque de la liste d'accès CSM_FW_ACL_ : STRATÉGIE PREFILTER : Prefilter_Policy1

règle-id 268434448 de remarque de la liste d'accès CSM_FW_ACL_ : RÈGLE : Fastpath_src_192.168.75.0/24

Les informations complémentaires :

Phase : 14

Type : CONN-SETTINGS

Sous-type :

Résultat : LAISSEZ

Config :

classe-par défaut de class-map

match any

policy-map global_policy

classe-par défaut de classe

placez la connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Les informations complémentaires :

Phase : 15

Type : NAT

Sous-type : par-session

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 16

Type : IP-OPTIONS

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 17

Type : RECHERCHE DE ROUTE

Sous-type : Interface de sortie de résolution

Résultat : LAISSEZ

Config :

Les informations complémentaires :

prochain-saut trouvé 192.168.76.39 utilisant l'ifc de sortie dehors

Phase : 18

Type : ADJACENCY-LOOKUP

Sous-type : prochain-saut et contiguïté

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Active de contiguïté

le MAC address 0004.deab.681b de prochain-saut frappe 140372416161507

Phase : 19

Type : CAPTURE

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Liste d'accès de MAC

Résultat :

interface d'entrée : dehors

entrée-état : vers le haut de

entrée-ligne-état : vers le haut de

sortie-interface : dehors

sortie-état : vers le haut de

sortie-ligne-état : vers le haut de

Action : laissez

1paquet affiché

firepower#

les paquets du suivi 5 du paquet-nombre 1 du show capture CAPI de firepower# ont capturé 1 : 23:35:07.281738 192.168.75.39 > 192.168.76.39 : ICMP : phase de requête d'écho : 1 type : Sous-type de CAPTURE : Résultat : PERMETTEZ le config : Les informations complémentaires : Phase de liste d'accès de MAC : Type 2 : Sous-type de LISTE D'ACCÈS : Résultat : PERMETTEZ le config : Les informations complémentaires implicites de règle : Phase de liste d'accès de MAC : Type 3 : Sous-type de RECHERCHE DE ROUTE : Résultat d'interface de sortie de résolution : PERMETTEZ le config : Les informations complémentaires : prochain-saut trouvé 192.168.76.39 utilisant l'ifc de sortie en dehors de la phase : Type 4 : Sous-type de LISTE D'ACCÈS : résultat de log : PERMETTEZ le config : la liste d'accès globale CSM_FW_ACL_ de l'access-group CSM_FW_ACL_ a avancé l'IP 192.168.75.0 255.255.255.0 de confiance n'importe quel event-log du règle-id 268434448 les deux le règle-id 268434448 de remarque de la liste d'accès CSM_FW_ACL_ : STRATÉGIE PREFILTER : Prefilter_Policy1 règle-id 268434448 de remarque de la liste d'accès CSM_FW_ACL_ : RÈGLE : Les informations complémentaires Fastpath_src_192.168.75.0/24 : Phase : Type 5 : Sous-type CONN-SETTINGS : Résultat : PERMETTEZ le config : les informations complémentaires globales de la connection advanced-options UM_STATIC_TCP_MAP de classe-par défaut de classe de global_policy de policy-map de match any de classe-par défaut de class-map de global_policy réglé de service-stratégie : Phase : Type 6 : Sous-type NAT : résultat de par-session : PERMETTEZ le config : Les informations complémentaires : Phase : Type 7 : Sous-type IP-OPTIONS : Résultat : PERMETTEZ le config : Les informations complémentaires : Phase : Type 8 : EXAMINEZ le sous-type : NP-examinez le résultat : PERMETTEZ le config : l'inspection_default de classe de global_policy de policy-map du par défaut-inspection-trafic de correspondance d'inspection_default de class-map examinent les informations complémentaires globales de global_policy de service-stratégie d'ICMP : Phase : Type 9 : EXAMINEZ le sous-type : NP-examinez le résultat : PERMETTEZ le config : Les informations complémentaires : Phase : Type 10 : Sous-type NAT : résultat de par-session : PERMETTEZ le config : Les informations complémentaires : Phase : Type 11 : Sous-type IP-OPTIONS : Résultat : PERMETTEZ le config : Les informations complémentaires : Phase : Type 12 : Sous-type FLOW-CREATION : Résultat : PERMETTEZ le config : Les informations complémentaires : Le nouvel écoulement créé avec l'id 52, paquet a acheminé à la phase prochaine de module : Type 13 : Sous-type de LISTE D'ACCÈS : résultat de log : PERMETTEZ le config : la liste d'accès globale CSM_FW_ACL_ de l'access-group CSM_FW_ACL_ a avancé l'IP 192.168.75.0 255.255.255.0 de confiance n'importe quel event-log du règle-id 268434448 les deux le règle-id 268434448 de remarque de la liste d'accès CSM_FW_ACL_ : STRATÉGIE PREFILTER : Prefilter_Policy1 règle-id 268434448 de remarque de la liste d'accès CSM_FW_ACL_ : RÈGLE : Les informations complémentaires Fastpath_src_192.168.75.0/24 : Phase : Type 14 : Sous-type CONN-SETTINGS : Résultat : PERMETTEZ le config : les informations complémentaires globales de la connection advanced-options

UM_STATIC_TCP_MAP de classe-par défaut de classe de global_policy de policy-map de match any de classe-par défaut de class-map de global_policy réglé de service-stratégie : Phase : Type 15 : Sous-type NAT : résultat de par-session : PERMETTEZ le config : Les informations complémentaires : Phase : Type 16 : Sous-type IP-OPTIONS : Résultat : PERMETTEZ le config : Les informations complémentaires : Phase : Type 17 : Sous-type de RECHERCHE DE ROUTE : Résultat d'interface de sortie de résolution : PERMETTEZ le config : Les informations complémentaires : prochain-saut trouvé 192.168.76.39 utilisant l'ifc de sortie en dehors de la phase : Type 18 : Sous-type ADJACENCY-LOOKUP : prochain-saut et résultat de contiguïté : PERMETTEZ le config : Les informations complémentaires : le MAC address actif 0004.deab.681b de prochain-saut de contiguïté frappe la phase 140372416161507 : Type 19 : Sous-type de CAPTURE : Résultat : PERMETTEZ le config : Les informations complémentaires : Résultat de liste d'accès de MAC : interface d'entrée : entrée-état extérieur : vers le haut du l'entrée-ligne-état : vers le haut de la sortie-interface : sortie-état extérieur : vers le haut du sortie-ligne-état : vers le haut de l'action : permettez le firepower# affiché par 1paquet

Capture sur les expositions extérieures d'interface :

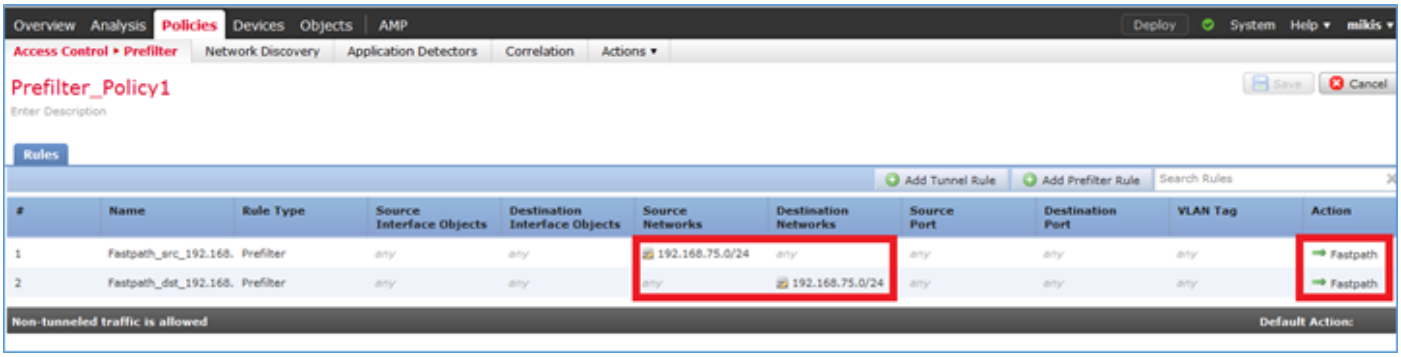
```
firepower# show capture CAPO

10 packets captured

   1: 23:35:07.282044   192.168.75.39 > 192.168.76.39: icmp: echo request
   2: 23:35:07.282227   192.168.76.39 > 192.168.75.39: icmp: echo reply
   3: 23:35:09.278717   192.168.75.39 > 192.168.76.39: icmp: echo request
   4: 23:35:09.278962   192.168.76.39 > 192.168.75.39: icmp: echo reply
   5: 23:35:11.279343   192.168.75.39 > 192.168.76.39: icmp: echo request
   6: 23:35:11.279541   192.168.76.39 > 192.168.75.39: icmp: echo reply
   7: 23:35:13.278870   192.168.75.39 > 192.168.76.39: icmp: echo request
   8: 23:35:13.279023   192.168.76.39 > 192.168.75.39: icmp: echo reply
   9: 23:35:15.279373   192.168.75.39 > 192.168.76.39: icmp: echo request
  10: 23:35:15.279541   192.168.76.39 > 192.168.75.39: icmp: echo reply
10 packets shown
```

Le suivi du paquet de retour prouve qu'il apparie l'écoulement existant (52), mais il est bloqué par l'ACL :

```
firepower# show capture CAPO packet-number 2 trace

10 packets captured

   2: 23:35:07.282227       192.168.76.39 > 192.168.75.39: icmp: echo reply
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 52, using existing flow

Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: DROP
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any any rule-id 268434432 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268434432: ACCESS POLICY: ACP_5506-1 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268434432: L4 RULE: DEFAULT ACTION RULE
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

Étape 5. Ajoutez une plus de règle de prefilter pour le trafic de retour. Le résultat est suivant les indications de l'image.



Tracez maintenant le paquet de retour que vous voyez (des points importants mis en valeur) :

Spoiler

suivi du paquet-nombre 2 de CAPO de show capture de firepower#

10 paquets capturés

2 : 00:01:38.873123 192.168.76.39 > 192.168.75.39 : ICMP : réponse d'écho

Phase : 1

Type : CAPTURE

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Liste d'accès de MAC

Phase : 2

Type : LISTE D'ACCÈS

Sous-type :

Résultat : LAISSEZ

Config :

Règle implicite

Les informations complémentaires :

Liste d'accès de MAC

Phase : 3

Type : FLOW-LOOKUP

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Écoulement trouvé avec l'id 62, utilisant l'écoulement existant

Phase : 4

Type : LISTE D'ACCÈS

Sous-type : log

Résultat : LAISSEZ

Config :

access-group CSM_FW_ACL_ global

la liste d'accès CSM_FW_ACL_ a avancé l'IP de confiance n'importe quel event-log chacun des deux du règle-id 268434450 de 192.168.75.0 255.255.255.0

règle-id 268434450 de remarque de la liste d'accès CSM_FW_ACL_ : STRATÉGIE PREFILTER : Prefilter_Policy1

règle-id 268434450 de remarque de la liste d'accès CSM_FW_ACL_ : RÈGLE :

Fastpath_dst_192.168.75.0/24

Les informations complémentaires :

Phase : 5

Type : CONN-SETTINGS

Sous-type :

Résultat : LAISSEZ

Config :

classe-par défaut de class-map

 match any

policy-map global_policy

 classe-par défaut de classe

 placez la connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Les informations complémentaires :

Phase : 6

Type : NAT

Sous-type : par-session

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 7

Type : IP-OPTIONS

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Phase : 8

Type : RECHERCHE DE ROUTE

Sous-type : Interface de sortie de résolution

Résultat : LAISSEZ

Config :

Les informations complémentaires :

prochain-saut trouvé 192.168.75.39 utilisant l'ifc de sortie à l'intérieur

Phase : 9

Type : ADJACENCY-LOOKUP

Sous-type : prochain-saut et contiguïté

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Active de contiguïté

le MAC address c84c.758d.4981 de prochain-saut frappe 140376711128802

Phase : 10

Type : CAPTURE

Sous-type :

Résultat : LAISSEZ

Config :

Les informations complémentaires :

Liste d'accès de MAC

Résultat :

interface d'entrée : à l'intérieur

entrée-état : vers le haut de

entrée-ligne-état : vers le haut de

sortie-interface : à l'intérieur

sortie-état : vers le haut de

sortie-ligne-état : vers le haut de

Action : laissez

les paquets du suivi 10 du paquet-nombre 2 de CAPO de show capture de firepower# ont capturé 2 : 00:01:38.873123 192.168.76.39 > 192.168.75.39 : ICMP : phase de réponse d'écho : 1 type : Sous-type de CAPTURE : Résultat : PERMETTEZ le config : Les informations complémentaires : Phase de liste d'accès de MAC : Type 2 : Sous-type de LISTE D'ACCÈS : Résultat : PERMETTEZ le config : Les informations complémentaires implicites de règle : Phase de liste d'accès de MAC : Type 3 : Sous-type FLOW-LOOKUP : Résultat : PERMETTEZ le config : Les informations complémentaires : Écoulement trouvé avec l'id 62, utilisant la phase d'écoulement existante : Type 4 : Sous-type de LISTE D'ACCÈS : résultat de log : PERMETTEZ le config : la liste d'accès globale CSM_FW_ACL_ de l'access-group CSM_FW_ACL_ a avancé l'IP de confiance n'importe quel event-log du règle-id 268434450 de 192.168.75.0 255.255.255.0 les deux le règle-id 268434450 de remarque de la liste d'accès CSM_FW_ACL_ : STRATÉGIE PREFILTER : Prefilter_Policy1 règle-id 268434450 de remarque de la liste d'accès CSM_FW_ACL_ : RÈGLE : Les informations complémentaires Fastpath_dst_192.168.75.0/24 : Phase : Type 5 : Sous-type CONN-SETTINGS : Résultat : PERMETTEZ le config : les informations complémentaires globales de la connection advanced-options UM_STATIC_TCP_MAP de classe-par défaut de classe de global_policy de policy-map de match any de classe-par défaut de class-map de global_policy réglé de service-stratégie : Phase : Type 6 : Sous-type NAT : résultat de par-session : PERMETTEZ le config : Les informations complémentaires : Phase : Type 7 : Sous-type IP-OPTIONS : Résultat : PERMETTEZ le config : Les informations complémentaires : Phase : Type 8 : Sous-type de RECHERCHE DE ROUTE : Résultat d'interface de sortie de résolution : PERMETTEZ le config : Les informations complémentaires : prochain-saut trouvé 192.168.75.39 utilisant l'ifc de sortie à l'intérieur de la phase : Type 9 : Sous-type ADJACENCY-LOOKUP : prochain-saut et résultat de contiguïté : PERMETTEZ le config : Les informations complémentaires : le MAC address actif c84c.758d.4981 de prochain-saut de contiguïté frappe la phase 140376711128802 : Type 10 : Sous-type de CAPTURE : Résultat : PERMETTEZ le config : Les informations complémentaires : Résultat de liste d'accès de MAC : interface d'entrée : entrée-état intérieur : vers le haut du l'entrée-ligne-état : vers le haut de la sortie-interface : sortie-état intérieur : vers le haut du sortie-ligne-état : vers le haut de l'action : laissez

Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

La vérification a été expliquée dans les sections respectives de tâches.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Toutes les versions du guide de configuration de centre de Gestion de Cisco FirePOWER peuvent être trouvées ici :

https://www.cisco.com/c/en/us/td/docs/security/firepower/roadmap/firepower-roadmap.html#id_47280

- Le centre d'assistance technique global de Cisco (TAC) recommande vivement ce guide visuel pour la connaissance pratique en profondeur sur des technologies de sécurité de nouvelle génération de Cisco FirePOWER, y compris celles mentionnées en cet article : http://www.ciscopress.com/title/9781587144806

- Pour toute la configuration et dépanner TechNotes : https://www.cisco.com/c/en/us/support/security/defense-center/tsd-products-support-series-home.html

- Support et documentation techniques - Cisco Systems