Configuration des interfaces FTD en mode Inline-Pair

Table des matières

- Introduction
- Conditions préalables
  - Exigences
  - Composants utilisés
  - Produits associés
- Informations générales
- Configurer l'interface de paire en ligne sur FTD
  - Diagramme du réseau
- Vérifier
- Vérifier le fonctionnement de l'interface FTD Inline Pair
  - Théorie De Base
  - Vérification 1. Utilisation de Packet-Tracer
  - Vérification 2. Envoi de paquets TCP SYN/ACK par paire en ligne
  - Vérification 3. Débogage Du Moteur De Pare-Feu Pour Le Trafic Autorisé
  - Vérification 4. Vérification de la propagation à état de liens
  - Vérification 5. Configuration de la NAT statique
  - Étude de cas - Trafic asymétrique à travers les ensembles en ligne
- Block Packet on Inline Pair Interface Mode
- Configurer Le Mode Paire En Ligne Avec Touche
- Vérification de la paire FTD Inline avec fonctionnement de l'interface Tap
- Paire en ligne et Etherchannel
  - Etherchannel terminé sur FTD
  - Etherchannel via le FTD
- Dépannage
- Comparaison : Paire en ligne ou paire en ligne avec robinet
- Résumé
- Informations connexes

Introduction

Ce document décrit la configuration, la vérification et le fonctionnement d'une interface par paire en ligne sur un appareil Firepower Threat Defense (FTD).

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- Firepower 4112 FTD (code 7.x)
- Centre de gestion Firepower (FMC) (code 7.x)

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 également être utilisé avec les versions matérielles et logicielles suivantes :

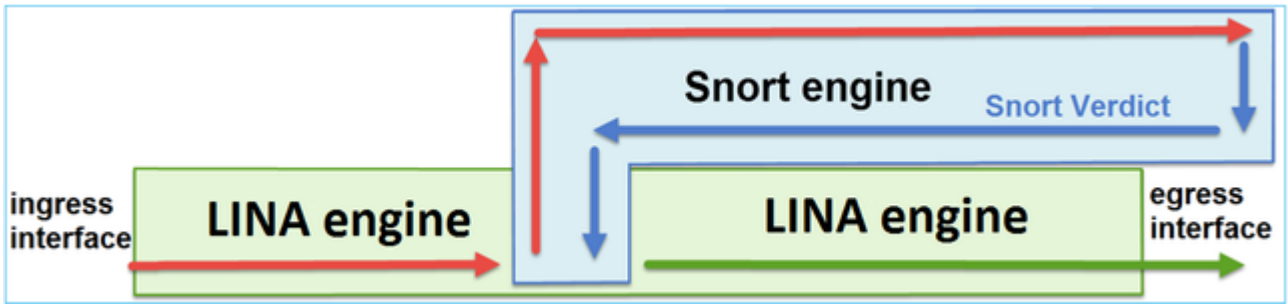
- FPR1000, FPR2100, FPR4100, FPR9300
- Pare-feu sécurisé séries 3100 et 4200
- vFTD
- Code logiciel FTD 6.2.x et versions ultérieures

Informations générales

Cisco Firepower Threat Defense (FTD) est une image logicielle unifiée qui comprend deux moteurs principaux :

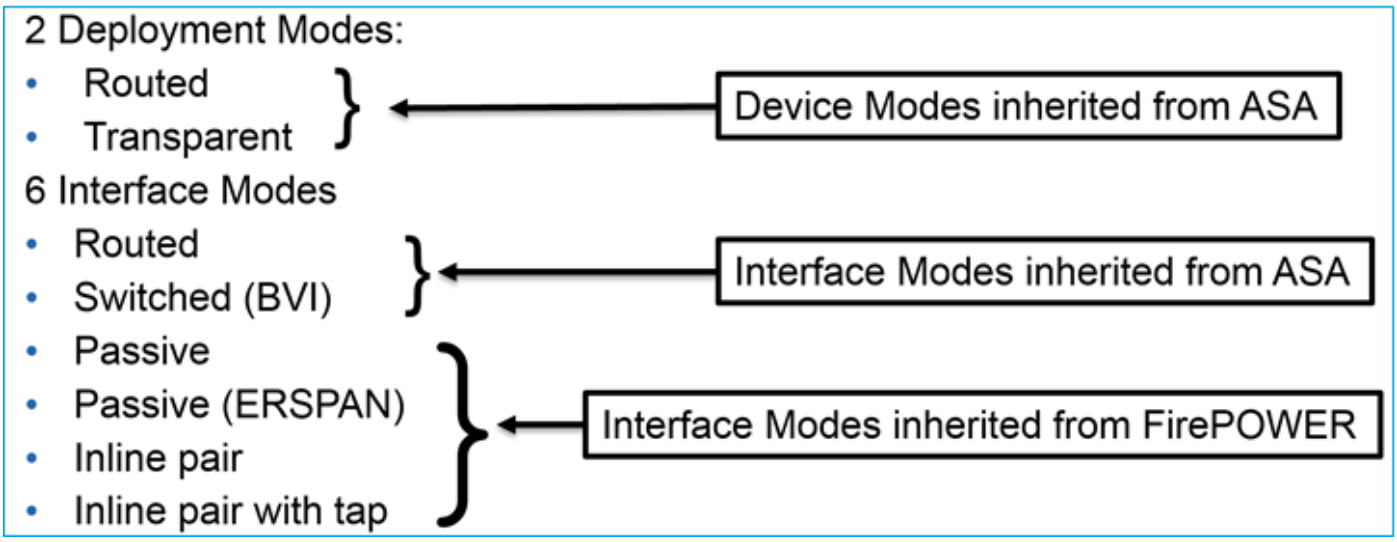
1. Moteur LINA
2. Moteur du renifleur

Cette figure montre comment les deux moteurs interagissent :



- 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 pour le paquet.
- Le moteur LINA abandonne ou transfère le paquet en fonction du verdict du renifleur.

FTD propose deux modes de déploiement et six modes d'interface, comme illustré dans l'image :



Remarque : Vous pouvez combiner les modes d'interface sur un seul appareil FTD.

Voici une présentation générale des différents modes de déploiement et d'interface FTD :

Mode interface FTD	Mode de déploiement FTD	Description	Le trafic peut être abandonné
Routés	Routés	Vérifications complètes du moteur LINA et du moteur Snort.	Oui

Commuté	Transparent	Vérifications complètes du moteur LINA et du moteur Snort.	Oui
Paire en ligne	Routé ou transparent	Vérification partielle du moteur LINA et vérification complète du moteur Snort.	Oui
Paire en ligne avec robinet	Routé ou transparent	Vérification partielle du moteur LINA et vérification complète du moteur Snort.	Non
Passif	Routé ou transparent	Vérification partielle du moteur LINA et vérification complète du moteur Snort.	Non
Passif (ERSPAN)	Routés	Vérification partielle du moteur LINA et vérification complète du moteur Snort.	Non

Configurer l'interface de paire en ligne sur FTD

Diagramme du réseau



Exigence

Configurez les interfaces physiques e1/3 et e1/4 en mode Inline Pair, conformément aux exigences suivantes :

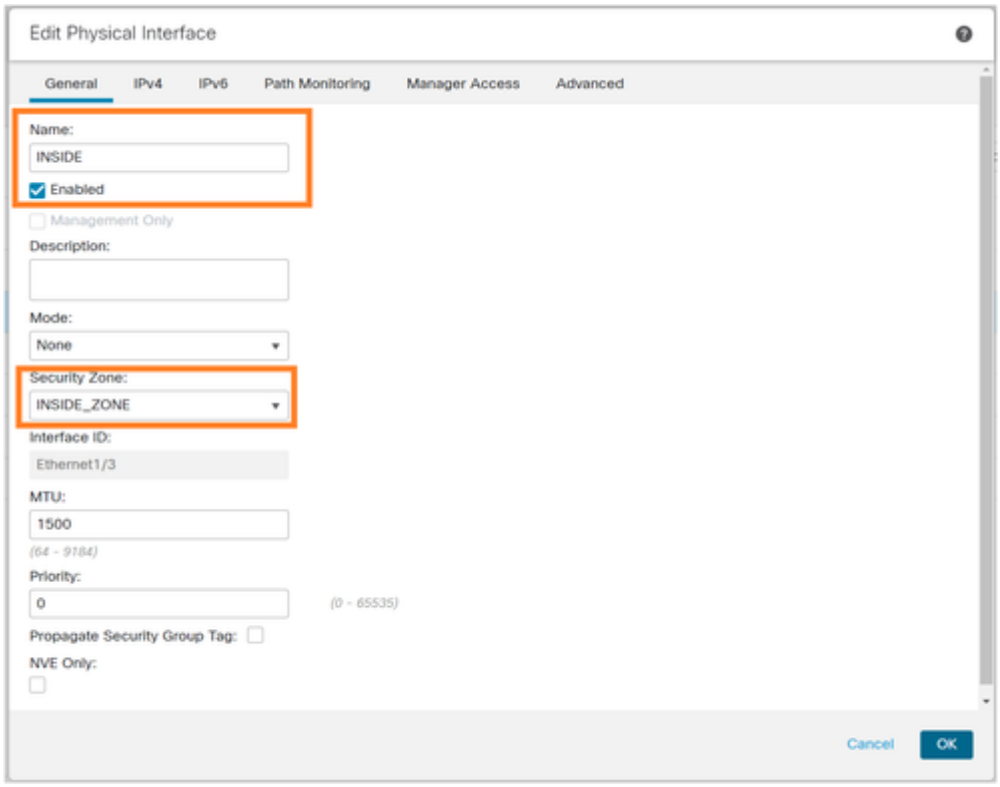
Interface	e1/3	e1/4
Nom	INTÉRIEUR	EXTÉRIEUR
Zone de sécurité	ZONE_INTERNE	ZONE_EXTERNE

Nom du jeu en ligne	Inline-Pair-1	
MTU du jeu en ligne	1500	
Propager l'état des liaisons	Activée	

Solution

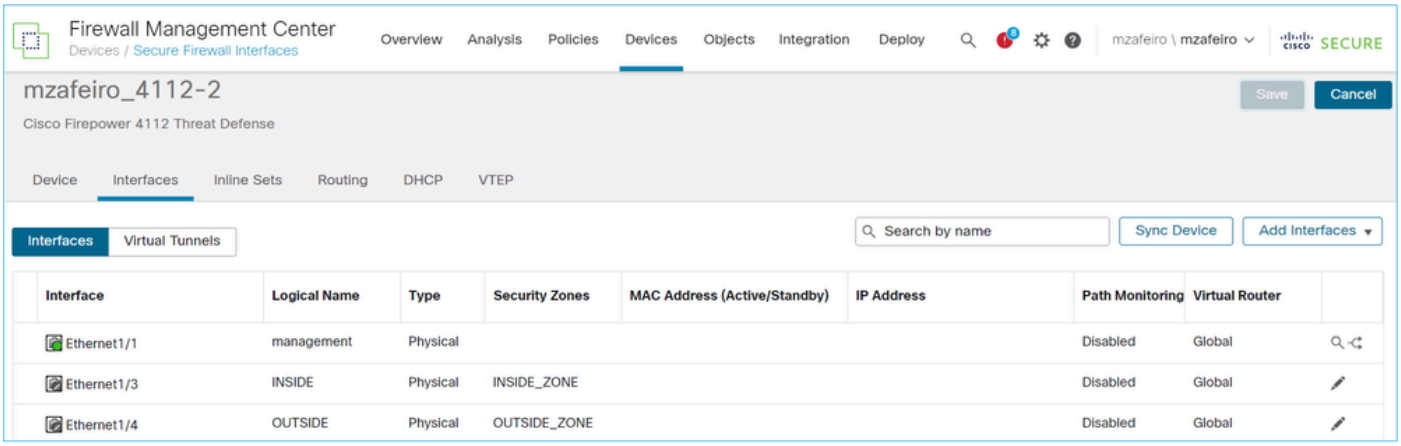
Étape 1. Afin de configurer vers les interfaces individuelles, accédez à Périphériques > Gestion des périphériques, sélectionnez le périphérique approprié et sélectionnez Modifier :

Ensuite, spécifiez Name et cochez Enabled pour l'interface comme indiqué dans l'image.



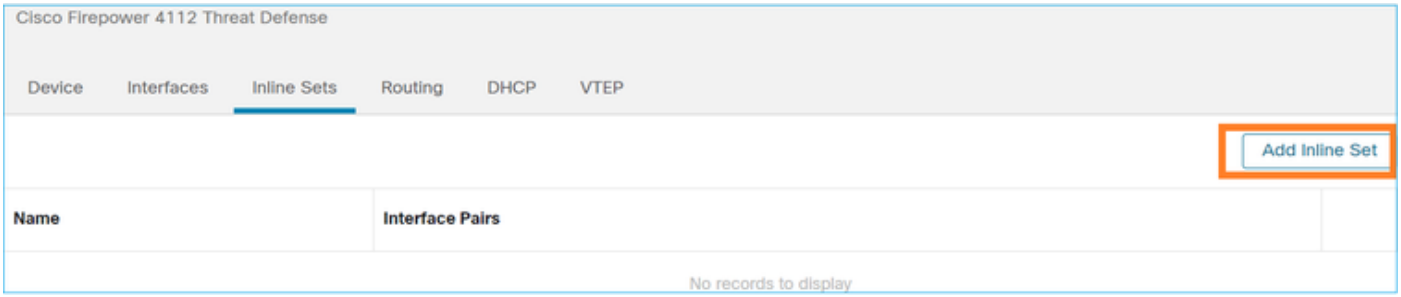
Remarque : Le nom est le nom de l'interface.

De même, pour l'interface Ethernet1/4. Le résultat final est le suivant :

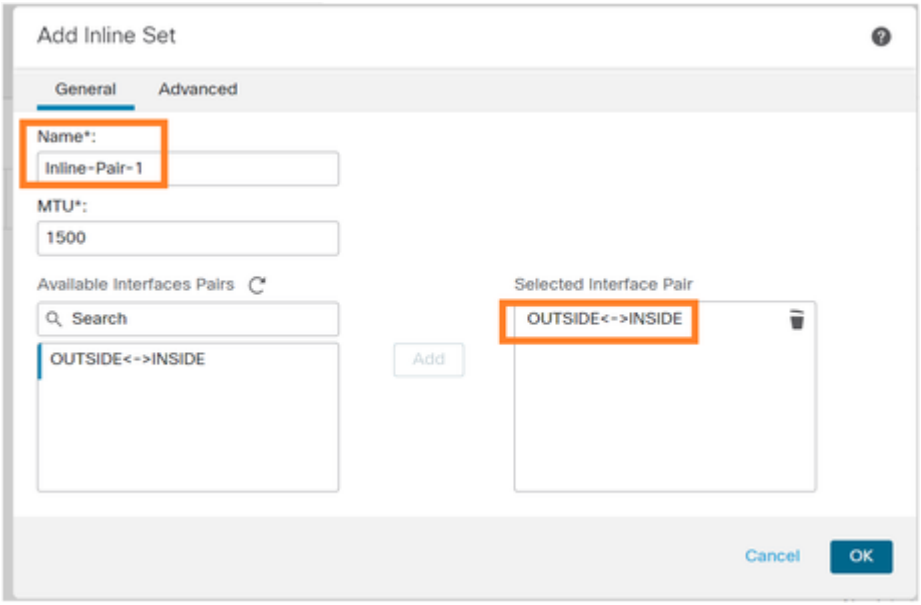


Étape 2 : configuration de la paire en ligne

Naviguez jusqu'à Inline Sets > Add Inline Set comme indiqué dans l'image.



Étape 3. Configurez les paramètres généraux conformément aux exigences indiquées dans l'image.



Étape 4. Activez l'option Propagate Link State dans les Advanced Settings comme indiqué dans l'image.



La propagation de l'état de la liaison désactive automatiquement la deuxième interface de la paire d'interfaces en ligne lorsque l'une des interfaces de l'ensemble en ligne est désactivée.

Étape 5 : enregistrement des modifications et déploiement.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vérifiez la configuration de la paire en ligne à partir de l'ILC FTD.

Solution

Connectez-vous à FTD CLI et vérifiez la configuration de la paire en ligne :

<#root>

```
firepower#
```

show inline-set

```
Inline-set Inline-Pair-1
```

```
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
      Current-Status: UP
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP
    Bridge Group ID: 507
```

Remarque : L'ID du groupe de ponts est une valeur différente de 0. Si le mode d'effleurement est activé, il est alors 0.

Interface et informations de nom :

<#root>

```
firepower#
```

show nameif

```
Interface       Name             Security
Ethernet1/1     management        0
Ethernet1/3     INSIDE            0
Ethernet1/4     OUTSIDE           0
```

Vérifiez l'état de l'interface :

<#root>

```
firepower#
```

show interface ip brief

```
Interface             IP-Address    OK? Method Status Protocol
Internal-Control0/0   unassigned    YES unset  up     up
Internal-Data0/0      unassigned    YES unset  up     up
Internal-Data0/1      unassigned    YES unset  up     up
Internal-Data0/2      169.254.1.1   YES unset  up     up
Internal-Data0/3      unassigned    YES unset  up     up
Internal-Data0/4      unassigned    YES unset  down   up
Ethernet1/1           203.0.113.130 YES unset  up     up
```

Ethernet1/3   unassigned   YES unset up   up

```
Ethernet1/4           unassigned    YES unset  up     up
```

Vérifiez les informations d'interface physique :

<#root>

```
firepower#

show interface e1/3
```

```
Interface Ethernet1/3 "INSIDE", is up, line protocol is up

  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
           MAC address ac4a.670e.641e, MTU 1500

IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1

           IP address unassigned
  Traffic Statistics for "INSIDE":
           170 packets input, 12241 bytes
            41 packets output, 7881 bytes
             9 packets dropped
      1 minute input rate 0 pkts/sec, 37 bytes/sec
      1 minute output rate 0 pkts/sec, 19 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec, 34 bytes/sec
      5 minute output rate 0 pkts/sec, 23 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

Vérifier le fonctionnement de l'interface FTD Inline Pair

Cette section couvre ces contrôles de vérification afin de vérifier le fonctionnement de la paire en ligne :

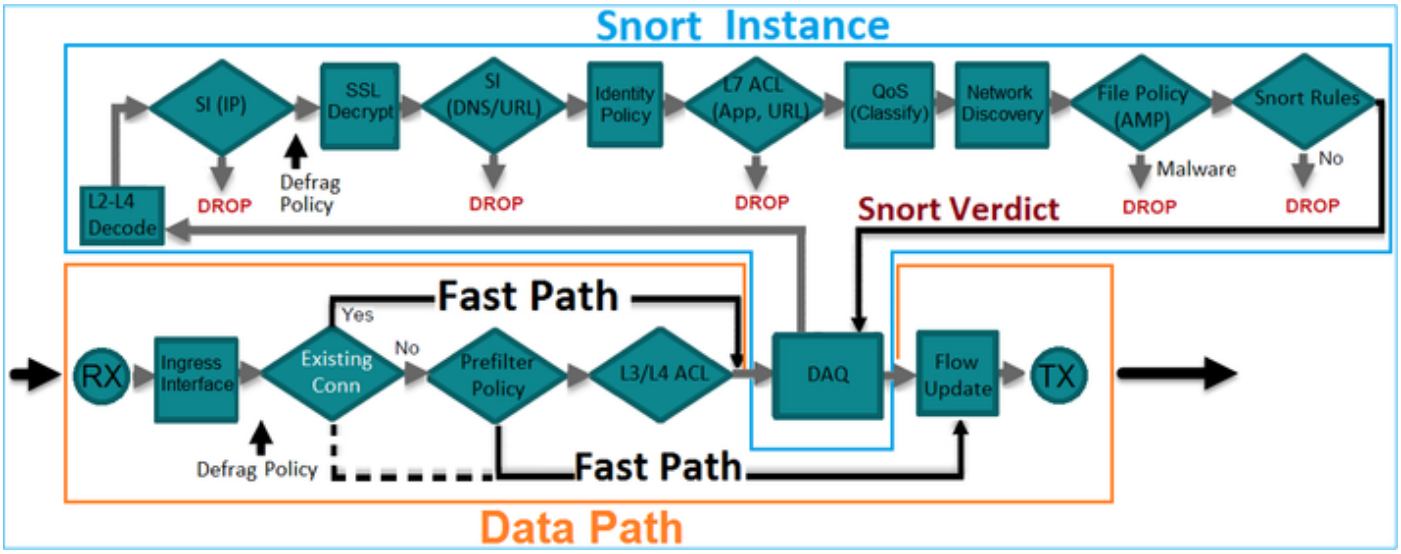
- Vérification 1. Avec l’utilisation de packet-tracer.
- Vérification 2. Activez la capture avec trace et envoyez un paquet de synchronisation/accusé de réception TCP (SYN/ACK) via la paire en ligne.

- Vérification 3. Surveiller le trafic FTD à l'aide du débogage du moteur de pare-feu
- Vérification 4. Vérification de la fonctionnalité de propagation d'état des liaisons
- Vérification 5. Configuration de la traduction d'adresses réseau (NAT) statique

Solution

Présentation architecturale

Lorsque 2 interfaces FTD fonctionnent en mode Inline-pair, un paquet est traité, comme illustré dans l'image.

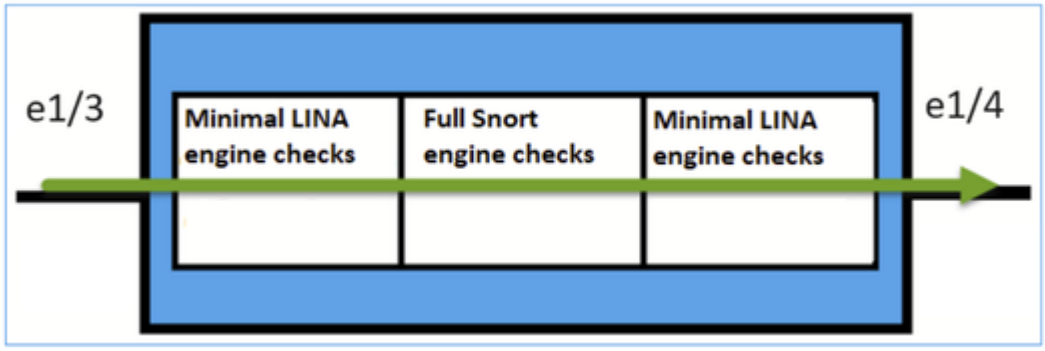


Remarque : Seules les interfaces physiques peuvent être membres d'un ensemble de paires en ligne.

Théorie De Base

- Lorsque vous configurez une liaison physique en ligne de paire 2, les interfaces sont pontées en interne.
- Très similaire au système de prévention des intrusions (IPS) en ligne classique.
- Disponible en modes de déploiement routé ou transparent.
- La plupart des fonctions du moteur LINA (NAT, routage, etc.) ne sont pas disponibles pour les flux qui passent par une paire en ligne.
- Le trafic de transit peut être abandonné.
- Quelques vérifications du moteur LINA sont appliquées ainsi que des vérifications complètes du moteur Snort.

Le dernier point peut être visualisé comme le montre l'image :



Vérification 1. Utilisation de Packet-Tracer

La sortie de packet-tracer qui émule un paquet qui traverse la paire en ligne avec les points importants mis en surbrillance :

<#root>

```
firepower#

packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80



Phase: 1



Type: NGIPS-MODE



Subtype: ngips-mode



Result: ALLOW



Elapsed time: 11834 ns
```

Config:

Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 11834 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.201.50 host 192.168.202.50 rule-id 268451044
access-list CSM_FW_ACL_ remark rule-id 268451044: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451044: L7 RULE: New-Rule-#1303-ALLOW
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: NGIPS-EGRESS-INTERFACE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Elapsed time: 2440 ns

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
Elapsed time: 68320 ns
Config:
Additional Information:
New flow created with id 1801, packet dispatched to next module

Phase: 5
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 18056 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 6
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 13668 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Phase: 7
Type: SNORT
Subtype: firewall
Result: ALLOW
Elapsed time: 67770 ns
Config:
Network 0, Inspection 0, Detection 0, Rule ID 268451044
Additional Information:
Starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt:
Matched rule ids 268451044 - Allow

Phase: 8
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 11002 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:

input-interface: INSIDE(vrfid:0)

input-status: up

input-line-status: up

output-interface: OUTSIDE(vrfid:0)

output-status: up

output-line-status: up

Action: allow

Time Taken: 204924 ns

Vérification 2. Envoi de paquets TCP SYN/ACK par paire en ligne

Vous pouvez générer des paquets TCP SYN/ACK à l'aide d'un paquet conçu par un utilitaire tel que Scapy. Cette syntaxe génère 3 paquets avec des indicateurs SYN/ACK activés :

<#root>

root@KALI:~#

scapy

INFO: Can't import python gnuplot wrapper . Won't be able to plot.
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.2.0)
>>>

conf.iface='eth0'

```
>>>

packet = IP(dst="192.168.201.60")/TCP(flags="SA",dport=80)

>>>

syn_ack=[]

>>>

for i in range(0,3): # Send 3 packets

...

syn_ack.extend(packet)

...
>>>

send(syn_ack)
```

Activez cette capture sur l'interface de ligne de commande FTD et envoyez quelques paquets TCP SYN/ACK :

<#root>

```
firepower#

capture CAPI interface INSIDE trace match ip host 192.168.201.60 any


firepower#

capture CAPO interface OUTSIDE match ip host 192.168.201.60 any
```

Les captures montrent que les 3 paquets SYN/ACK traversent le FTD :

<#root>

```
firepower#

show capture CAPI


3 packets captured
```

```
1: 09:20:18.206440 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
2: 09:20:18.208180 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3: 09:20:18.210026 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
firepower#
```

show capture CAPO

```
3 packets captured

1: 09:20:18.206684 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
2: 09:20:18.208210 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3: 09:20:18.210056 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
3 packets shown
```

La trace du premier paquet de capture révèle des informations supplémentaires comme le verdict du moteur Snort :

<#root>

```
firepower#
```

show capture CAPI packet-number 1 trace

```
3 packets captured

1: 09:20:18.206440 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 5978 ns
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Elapsed time: 5978 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip host 192.168.201.50 object-group FMC_INLINE_dst_rule_2684510
access-list CSM_FW_ACL_ remark rule-id 268451044: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451044: L7 RULE: New-Rule-#1303-ALLOW
object-group network FMC_INLINE_dst_rule_268451044
network-object 192.168.202.50 255.255.255.255
network-object 192.168.201.60 255.255.255.255
Additional Information:
This packet will be sent to snort for additional processing where a verdict will be reached
```

Phase: 3
Type: NGIPS-EGRESS-INTERFACE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Elapsed time: 1952 ns
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
Elapsed time: 45872 ns
Config:
Additional Information:
New flow created with id 1953, packet dispatched to next module

Phase: 5
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 18544 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 6
Type: SNORT
Subtype: identity
Result: ALLOW
Elapsed time: 25182 ns
Config:
Additional Information:
user id: no auth, realm id: 0, device type: 0, auth type: invalid, auth proto: basic, username: none, A
src sgt: 0, src sgt type: unknown, dst sgt: 0, dst sgt type: unknown, abp src: none, abp dst: none, loc

Phase: 7

Type: SNORT

Subtype: firewall

Result: ALLOW

Elapsed time: 50924 ns

Config:

Network 0, Inspection 0, Detection 0, Rule ID 268451044

Additional Information:

Starting rule matching, zone -1 -> -1, geo 0 -> 0, vlan 0, src sgt: 0, src sgt type: unknown, dst sgt: 0

Matched rule ids 268451044 - Allow

```
Phase: 8
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 17722 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE(vrfid:0)
output-status: up
output-line-status: up
Action: allow
Time Taken: 172152 ns


1 packet shown
```

La trace du deuxième paquet capturé indique que le paquet correspond à une connexion en cours, de sorte qu'il contourne la vérification de la liste de contrôle d'accès, mais est toujours inspecté par le moteur Snort :

<#root>

```
firepower#
```

show capture CAPI packet-number 2 trace

```
3 packets captured

2: 09:20:18.208180 192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) ack 0 win 8192
Phase: 1
Type: FLOW-LOOKUP
Subtype:
Result: ALLOW
Elapsed time: 1952 ns
Config:
Additional Information:
```

Found flow with id 1953, using existing flow

```
Phase: 2
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Elapsed time: 7320 ns
Config:
Additional Information:
Application: 'SNORT Inspect'

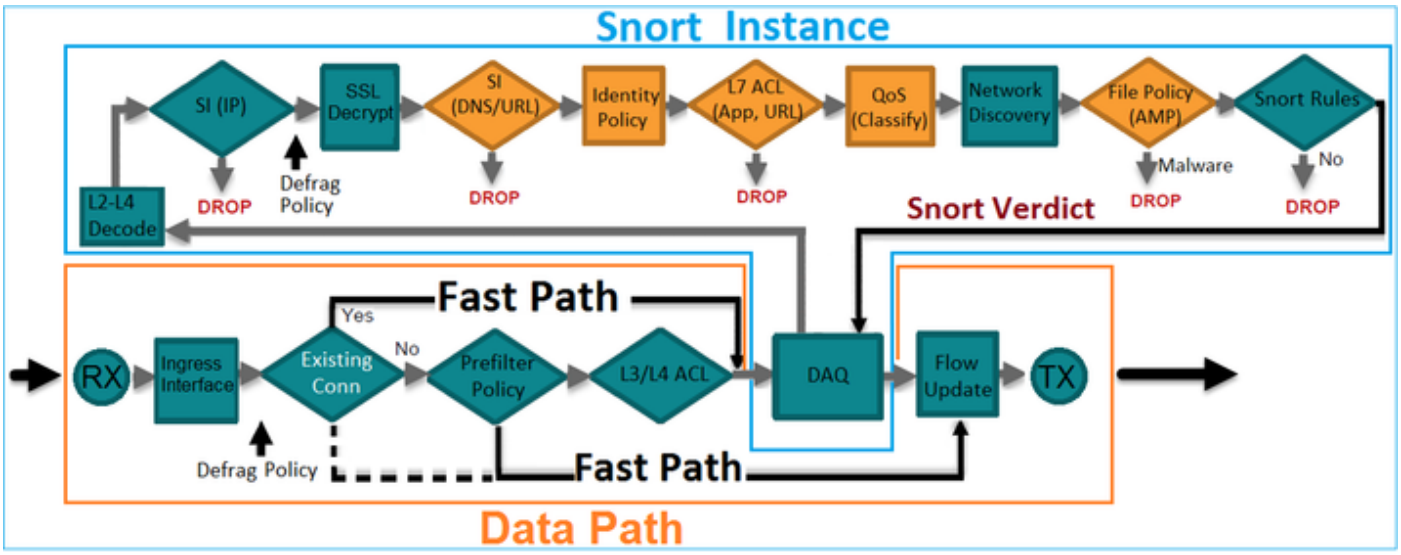
Phase: 3
Type: SNORT
Subtype: appid
Result: ALLOW
Elapsed time: 1860 ns
Config:
Additional Information:
service: (0), client: (0), payload: (0), misc: (0)

Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
Action: allow
Time Taken: 11132 ns


1 packet shown
```

Vérification 3. Débogage Du Moteur De Pare-Feu Pour Le Trafic Autorisé

Le débogage du moteur de pare-feu s'exécute sur des composants spécifiques du moteur FTD Snort Engine comme la politique de contrôle d'accès, comme illustré dans l'image :



Lorsque vous envoyez les paquets TCP SYN/ACK via Inline Pair, vous pouvez voir dans la sortie de débogage :

<#root>

>

system support firewall-engine-debug

Please specify an IP protocol:

tcp

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

192.168.201.60

Please specify a server port:

80

Monitoring firewall engine debug messages

192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 New session

```
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 using HW or preset rule order 3, id 268438528 action A
```

```
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 allow action
```

```
192.168.201.60-80 > 192.168.201.50-20 6 AS 4 I 12 Deleting session
```

Vérification 4. Vérification de la propagation à état de liens

Activez le journal de mémoire tampon sur FTD et arrêtez le port de commutation connecté à l'interface e1/4. Sur l'interface de ligne de commande FTD, vous devez voir que les deux interfaces sont tombées en panne :

<#root>

```
firepower#
```

```
show interface ip brief
```

```
Interface                IP-Address    OK? Method Status     Protocol
Internal-Control0/0      unassigned    YES unset  up         up
Internal-Data0/0         unassigned    YES unset  up         up
Internal-Data0/1         unassigned    YES unset  up         up
Internal-Data0/2         169.254.1.1   YES unset  up         up
Internal-Data0/3         unassigned    YES unset  up         up
Internal-Data0/4         unassigned    YES unset  down       up
Ethernet1/1              203.0.113.130 YES unset  up         up
```

```
Ethernet1/3              unassigned    YES unset  admin down down
```

```
Ethernet1/4              unassigned    YES unset  down       down
```

Les journaux FTD indiquent :

<#root>

```
firepower#

show log


...

May 28 2024 07:35:10: %FTD-4-411002: Line protocol on Interface Ethernet1/4, changed state to down



May 28 2024 07:35:10: %FTD-4-411004: Interface INSIDE, changed state to administratively down



May 28 2024 07:35:10: %FTD-4-411004: Interface Ethernet1/3, changed state to administratively down



May 28 2024 07:35:10: %FTD-4-812005: Link-State-Propagation activated on inline-pair due to failure of i



May 28 2024 07:35:10: %FTD-4-411002: Line protocol on Interface Ethernet1/3, changed state to down
```

L'état de l'ensemble en ligne indique l'état des 2 membres d'interface :

```
<#root>
firepower#

show inline-set



Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off


Propagate-link-state option is on


  hardware-bypass mode is disabled
    Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
```

```
    Current-Status: Down(Propagate-Link-State-Activated)

    Interface: Ethernet1/3 "INSIDE"

Current-Status: Down(Administrative-Down-By-Propagate-Link-State)

Bridge Group ID: 507
```

Notez la différence d'état des 2 interfaces :

```
<#root>
firepower#
 show interface e1/3


Interface Ethernet1/3 "INSIDE", is admin down, line protocol is down

  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        MAC address ac4a.670e.641e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1

Administrative-Down-By-Propagate-Link-State

        IP address unassigned
  Traffic Statistics for "INSIDE":
        2400 packets input, 165873 bytes
        1822 packets output, 178850 bytes
        17 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  32 bytes/sec
      5 minute output rate 0 pkts/sec,  57 bytes/sec
      5 minute drop rate, 0 pkts/sec
firepower#

show interface e1/4


Interface Ethernet1/4 "OUTSIDE", is down, line protocol is down
```

```
  Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
        MAC address ac4a.670e.640e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1

        Propagate-Link-State-Activated


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        1893 packets input, 158046 bytes
        2386 packets output, 213997 bytes
        67 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  51 bytes/sec
      5 minute output rate 0 pkts/sec,  39 bytes/sec
      5 minute drop rate, 0 pkts/sec
```

Après avoir réactivé le port de commutation, les journaux FTD affichent :

<#root>

```
May 28 2024 07:38:04: %FTD-4-411001: Line protocol on Interface Ethernet1/4, changed state to up

May 28 2024 07:38:04: %FTD-4-411003: Interface Ethernet1/3, changed state to administratively up

May 28 2024 07:38:04: %FTD-4-411003: Interface INSIDE, changed state to administratively up

May 28 2024 07:38:04: %FTD-4-812006: Link-State-Propagation de-activated on inline-pair due to recovery

May 28 2024 07:38:05: %FTD-4-411002: Line protocol on Interface Ethernet1/4, changed state to down
```

Vérification 5. Configuration de la NAT statique

Solution

NAT n'est pas pris en charge pour les interfaces qui fonctionnent en mode inline, inline tap ou passive :

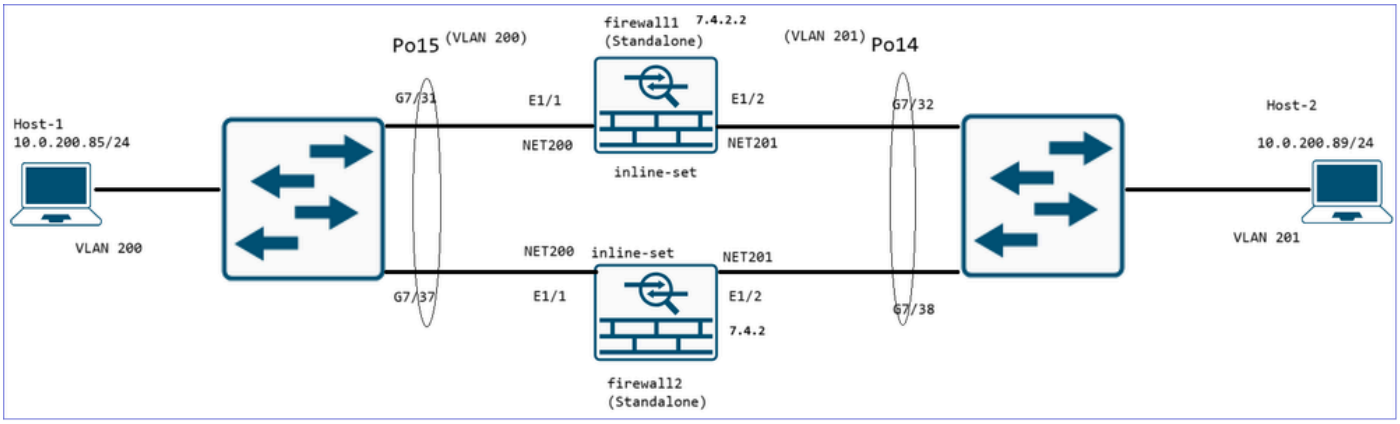
[Guide de configuration de Firepower Management Center, version 6.0.1]

Étude de cas - Trafic asymétrique à travers les ensembles en ligne

---

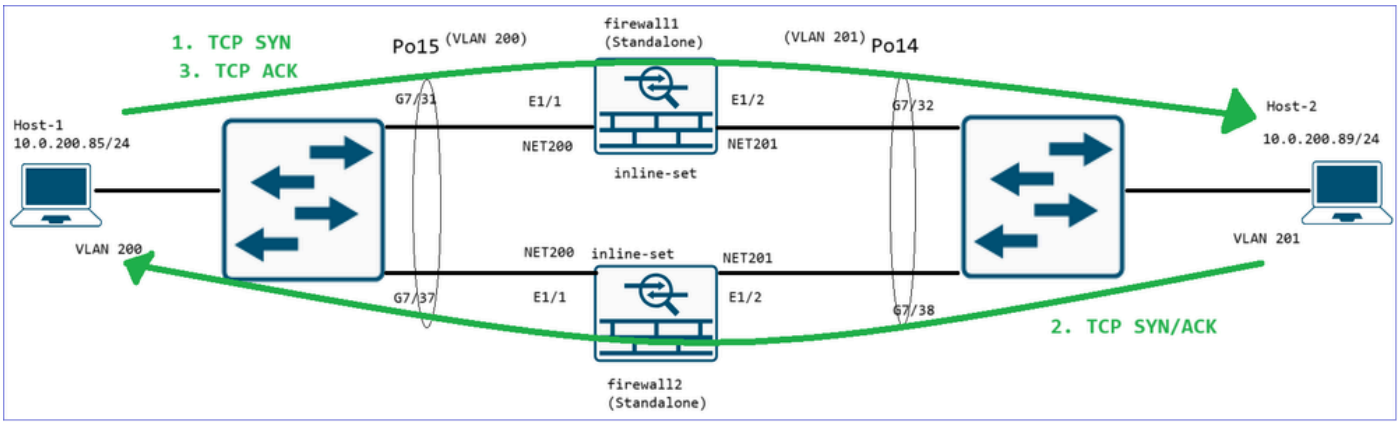
Avertissement : Sur les interfaces définies en ligne (mode IPS), le contournement d'état TCP est activé par défaut. Si le TSID ou une stratégie de déchiffrement TLS est configuré dans les paramètres avancés ACP, il remplace/désactive silencieusement ce comportement de contournement d'état TCP par défaut, de sorte que les vérifications d'état TCP sont appliquées au lieu d'être contournées.
Symptôme observable : Pour le trafic admissible au contournement d'état TCP traversant un ensemble en ligne (par exemple, les scénarios de trafic asymétrique où le trafic sort et entre dans différents ensembles en ligne), les paquets peuvent être abandonnés avec ASP drop tcp-not-syn (syslog 106015).

Considérez ce scénario :



Les deux pare-feu fonctionnent en mode autonome (ils exécutent même des versions logicielles différentes), mais gèrent le trafic provenant des mêmes interfaces port-channel.

Dans ce cas, vous pouvez avoir un trafic asymétrique dû à l'algorithme d'équilibrage de charge port-channel :



1. L'hôte 1 (10.0.200.85) envoie un SYN TCP vers l'hôte 2 (10.0.200.89). Ce paquet traverse firewall1.
2. L'hôte 2 (10.0.200.89) envoie un TCP SYN/ACK vers l'hôte 2 (10.0.200.85). Ce paquet traverse firewall2.
3. La connexion TCP en trois étapes est terminée lorsque l'hôte 1 envoie un accusé de réception TCP vers l'hôte 2. Ce paquet traverse le pare-feu 1.

Du point de vue de l'hôte 1, la connexion est établie avec succès :

<#root>

```
root@kali:/ #

wget -O - http://10.0.200.89/10K


--2025-05-06 08:20:28--  http://10.0.200.89/10K
Connecting to 10.0.200.89:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10240 (10K)
Saving to: 'STDOUT'
-                                                   100%[=======================================================
2025-05-06 08:20:28 (99.8 MB/s) - written to stdout [10240/10240]
```

La capture de paquets sur firewall1 affiche uniquement le trafic de Host1 vers Host2 :

<#root>

```
firepower#

show capture


capture CAPI type raw-data trace interface NET200 [Capturing - 875 bytes]
```

```
  match ip host 10.0.200.85 host 10.0.200.89
capture CAPO type raw-data trace interface NET201 [Capturing - 875 bytes]
  match ip host 10.0.200.85 host 10.0.200.89
```

Le contenu de la capture :

```
<#root>

firepower#

show capture CAPI



9 packets captured

   1: 12:21:14.161689       10.0.200.85.44806 > 10.0.200.89.80:

S

1877376557:1877376557(0) win 64240 <mss 1460,sackOK,timestamp 2133104674 0,nop,wscale 7>
   2: 12:21:14.162924       10.0.200.85.44806 > 10.0.200.89.80: .

ack

 3274105192 win 502 <nop,nop,timestamp 2133104676 1658009126>
   3: 12:21:14.163077       10.0.200.85.44806 > 10.0.200.89.80: P 1877376558:1877376687(129) ack 327410
   4: 12:21:14.164801       10.0.200.85.44806 > 10.0.200.89.80: . ack 3274106640 win 501 <nop,nop,times
   5: 12:21:14.164908       10.0.200.85.44806 > 10.0.200.89.80: . ack 3274108088 win 494
...
```

La capture de paquets sur le pare-feu2 affiche uniquement le trafic de l'hôte 2 vers l'hôte 1 :

```
<#root>

FTD1010-12#

show capture CAPI



11 packets captured

   1: 12:21:14.198949       10.0.200.89.80 > 10.0.200.85.44806:

S
```

```
 3274105191:3274105191(0)

ack

 1877376558 win 65160 <mss 1460,sackOK,timestamp 1658009126 2133104674,nop,wscale 7>
   2: 12:21:14.200001       10.0.200.89.80 > 10.0.200.85.44806: . ack 1877376687 win 509 <nop,nop,times
   3: 12:21:14.200825       10.0.200.89.80 > 10.0.200.85.44806: . 3274105192:3274106640(1448) ack 18773
   4: 12:21:14.200947       10.0.200.89.80 > 10.0.200.85.44806: . 3274106640:3274108088(1448) ack 18773
   5: 12:21:14.200963       10.0.200.89.80 > 10.0.200.85.44806: . 3274108088:3274109536(1448) ack 18773
   6: 12:21:14.200978       10.0.200.89.80 > 10.0.200.85.44806: . 3274109536:3274110984(1448) ack 18773
   7: 12:21:14.200993       10.0.200.89.80 > 10.0.200.85.44806: P 3274110984:3274112432(1448) ack
...
```

Les journaux système du pare-feu1 indiquent que le paquet TCP SYN a créé une connexion de contournement d'état TCP :

<#root>

```
firepower#

show logging


...
May 06 2025 12:21:14: %FTD-6-302303:

Built TCP state-bypass connection

 106977 from NET200:10.0.200.85/44806 (10.0.200.85/44806) to NET201:10.0.200.89/80 (10.0.200.89/80)
```

Sur firewall2, le paquet TCP SYN/ACK a également créé une connexion de contournement d'état TCP :

<#root>

```
FTD1010-12#

show logging


...
May 06 2025 12:21:14: %FTD-6-302303:
```

```
Built TCP state-bypass
```

```
connection
```

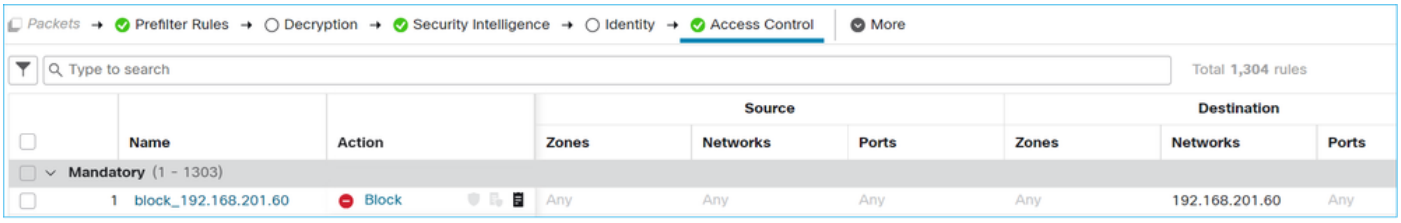
```
 325 from NET201:10.0.200.89/80 (10.0.200.89/80) to NET200:10.0.200.85/44806 (10.0.200.85/44806)
```

Points principaux

- Le trafic asymétrique fonctionne via un ensemble en ligne de différents périphériques pare-feu puisque les deux périphériques gèrent la connexion TCP en mode de contournement d'état TCP.
- Notez que le contournement d'état TCP n'est pas configuré manuellement sur les pare-feu, mais il est le résultat de l'opération d'interface en ligne.

Block Packet on Inline Pair Interface Mode

Créez une règle de blocage, envoyez du trafic via la paire FTD Inline et observez le comportement, comme illustré dans l'image.



Solution

Activez la capture avec trace et envoyez les paquets SYN/ACK via la paire en ligne FTD. Le trafic est bloqué :

<#root>

```
firepower#
```

```
show capture
```

```
capture CAPI type raw-data trace interface INSIDE
```

```
[Capturing - 270 bytes]


  match ip host 192.168.201.60 any
capture CAPO type raw-data interface OUTSIDE

[Capturing - 0 bytes]


  match ip host 192.168.201.60 any
```

Dans la trace, il est possible de voir que le paquet a été abandonné par le moteur LINA FTD et n'a pas été transféré au moteur Snort FTD.

<#root>

```
firepower#

show capture CAPI packet-number 1 trace



4 packets captured

   1: 09:41:54.562547       192.168.201.50.59144 > 192.168.201.60.80: S 3817586151:3817586151(0) win 64
Phase: 1
Type: NGIPS-MODE
Subtype: ngips-mode
Result: ALLOW
Elapsed time: 10126 ns
Config:
Additional Information:
The flow ingressed an interface configured for NGIPS mode and NGIPS services will be applied

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Elapsed time: 10126 ns
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip any host 192.168.201.60 rule-id 268451045 event-log flow-start
access-list CSM_FW_ACL_ remark rule-id 268451045: ACCESS POLICY: mzafeiro_2m - Mandatory
access-list CSM_FW_ACL_ remark rule-id 268451045: L4 RULE: block_192.168.201.60
Additional Information:

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

Time Taken: 20252 ns
```

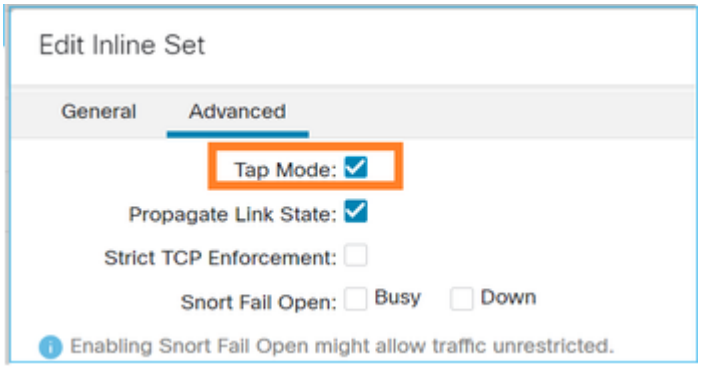
```
1 packet shown
```

Configurer Le Mode Paire En Ligne Avec Touche

Activez le mode Tap sur la paire en ligne.

Solution

Accédez à Périphériques > Gestion des périphériques > Jeux en ligne > Modifier le jeu en ligne > Avancé et activez Toucher le mode, comme indiqué dans l'image.



Vérification

<#root>

```
firepower#

 show inline-set



Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Fail-open for snort down is off
  Fail-open for snort busy is off


Tap mode is on
```

```
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/4 "OUTSIDE"
      Current-Status: UP
    Interface: Ethernet1/3 "INSIDE"
      Current-Status: UP
```

Bridge Group ID: 0

Vérification de la paire FTD Inline avec fonctionnement de l'interface Tap

Théorie De Base

- Lorsque vous configurez une paire en ligne avec Tap, les interfaces physiques sont pontées en interne.
- Il est disponible en mode de déploiement routé ou transparent.
- La plupart des fonctions du moteur LINA (NAT, routage, etc.) ne sont pas disponibles pour les flux qui passent par la paire en ligne.
- Le trafic réel ne peut pas être abandonné.
- Quelques vérifications de moteur LINA sont appliquées avec des vérifications de moteur Snort complètes à une copie du trafic réel.

La paire en ligne avec le mode Tap ne supprime pas le trafic de transit. Avec la trace d'un paquet, il confirme ceci :

<#root>

>

show capture CAPI packet-number 2 trace

```
3 packets captured

   2: 13:34:30.685084       192.168.201.50.20 > 192.168.201.60.80: S 0:0(0) win 8192
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: NGIPS-MODE
Subtype: ngips-mode

Result: ALLOW
Config:
Additional Information:

The flow ingressed an interface configured for NGIPS mode and NGIPS services is applied



Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: WOULD HAVE DROPPED

Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log fl
access-list CSM_FW_ACL_ remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/1
access-list CSM_FW_ACL_ remark rule-id 268441600: L4 RULE: Rule 1
Additional Information:

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

Action: Access-list would have dropped, but packet forwarded due to inline-tap

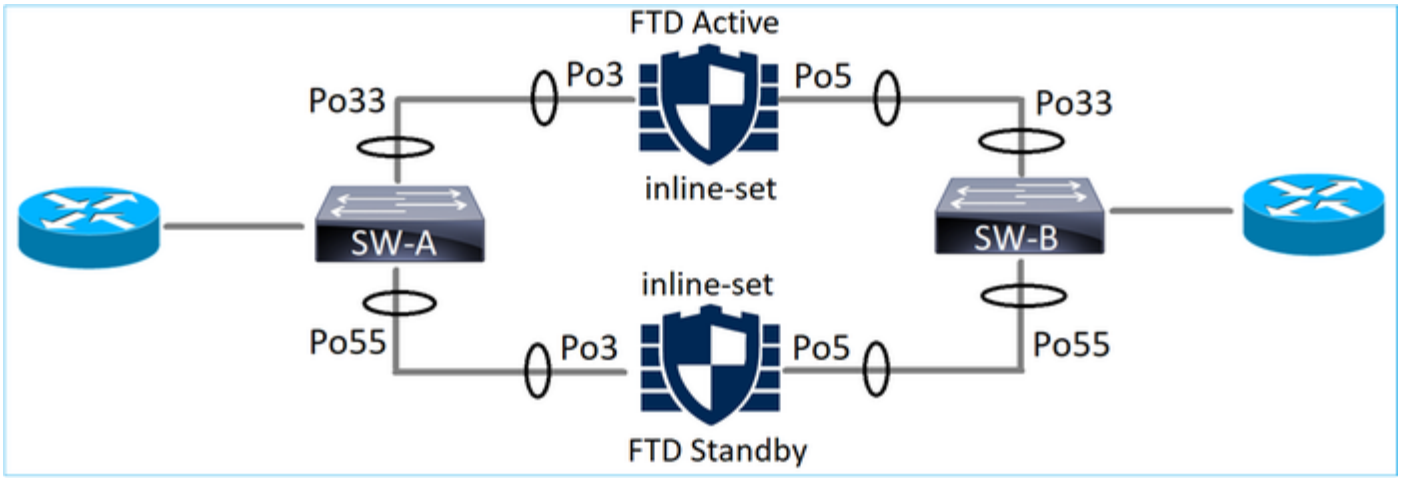

1 packet shown
>
```

Paire en ligne et Etherchannel

Vous pouvez configurer la paire en ligne avec etherchannel de deux manières :

1. Etherchannel terminé sur FTD.
2. Etherchannel passe par le FTD (nécessite le code FXOS 2.3.1.3 et versions ultérieures).

Etherchannel terminé sur FTD



Etherchannels sur SW-A :

<#root>

SW-A#

show etherchannel summary | i Po33|Po55

```
33     Po33(SU)         LACP      Gi3/11(P)
35     Po55(SU)         LACP      Gi2/33(P)
```

Etherchannels sur SW-B :

<#root>

SW-B#

show etherchannel summary | i Po33|Po55

```
33     Po33(SU)         LACP        Gi1/0/3(P)
55     Po55(SU)         LACP        Gi1/0/4(P)
```

Le trafic est transféré via le FTD actif en fonction de l'apprentissage des adresses MAC :

<#root>

```
SW-B#

 show mac address-table address 0017.dfd6.ec00

          Mac Address Table
------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC

Po33

Total Mac Addresses for this criterion: 1
```

Le jeu en ligne sur FTD :

<#root>

```
FTD#

show inline-set

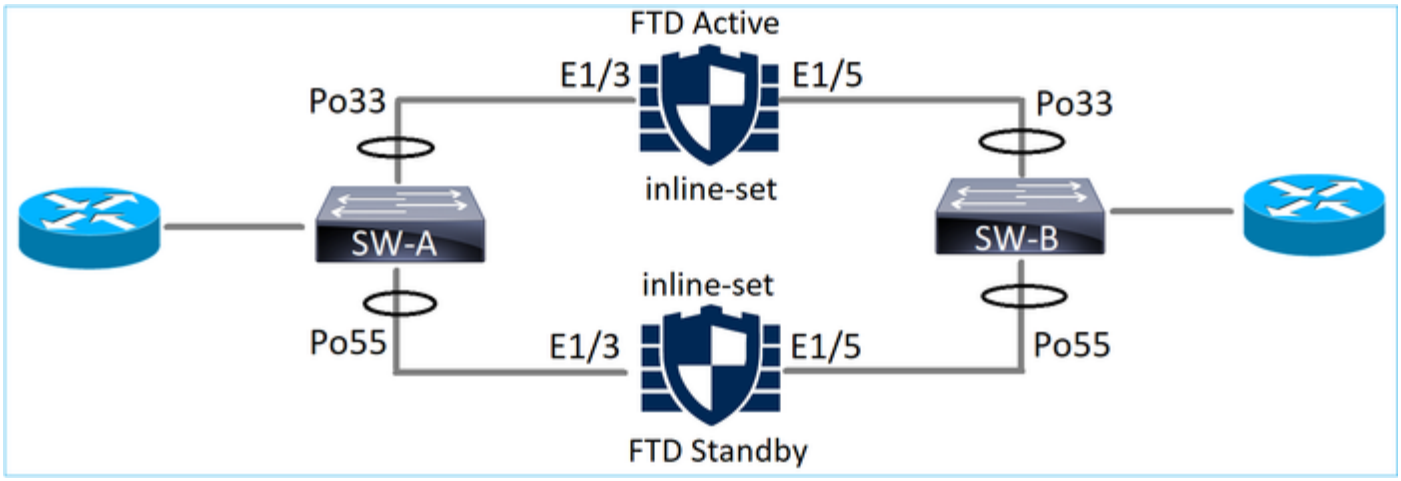

Inline-set SET1
  Mtu is 1500 bytes
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled


Interface-Pair[1]:
    Interface: Port-channel3 "INSIDE"
      Current-Status: UP
    Interface: Port-channel5 "OUTSIDE"
      Current-Status: UP

    Bridge Group ID: 775
```

Remarque : Dans le cas d'un événement de basculement FTD, la panne de trafic dépend principalement du temps que les commutateurs mettent à apprendre l'adresse MAC de l'homologue distant.

Etherchannel via le FTD



Etherchannels sur SW-A :

<#root>

SW-A#

show etherchannel summary | i Po33|Po55

33 Po33(SU) LACP Gi3/11(P)
55 Po55(SD) LACP Gi3/7

(I)

Les paquets LACP via le FTD de secours sont bloqués :

<#root>

FTD#

capture ASP type asp-drop fo-standby

FTD#

show capture ASP | i 0180.c200.0002

29: 15:28:32.658123 a0f8.4991.ba03 0180.c200.0002 0x8809 Length: 124
70: 15:28:47.248262 f0f7.556a.11e2 0180.c200.0002 0x8809 Length: 124

Etherchannels sur SW-B :

<#root>

```
SW-B#

show etherchannel summary | i Po33|Po55


33     Po33(SU)         LACP        Gi1/0/3(P)
55     Po55(SD)         LACP        Gi1/0/4

(s)
```

Le trafic est transféré via le FTD actif en fonction de l'apprentissage des adresses MAC :

<#root>

```
SW-B#

 show mac address-table address 0017.dfd6.ec00

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 201    0017.dfd6.ec00    DYNAMIC

Po33

Total Mac Addresses for this criterion: 1
```

Le jeu en ligne sur FTD :

<#root>

```
FTD#

show inline-set


Inline-set SET1
  Mtu is 1500 bytes
```

```
  Fail-open for snort down is on
  Fail-open for snort busy is off
  Tap mode is off
  Propagate-link-state option is off
  hardware-bypass mode is disabled


Interface-Pair[1]:


    Interface: Ethernet1/3 "INSIDE"


      Current-Status: UP


    Interface: Ethernet1/5 "OUTSIDE"


      Current-Status: UP


    Bridge Group ID: 519
```

⚠ Mise en garde : Dans ce scénario, en cas d'événement de basculement FTD, le temps de convergence dépend principalement de la négociation Etherchannel LACP, et du temps qu'il prend la panne, qui peut être beaucoup plus long. Si le mode Etherchannel est ON (pas de LACP), le temps de convergence dépend de l'apprentissage des adresses MAC.

Dépannage

Aucune information spécifique n'est actuellement disponible pour cette configuration.

Comparaison : Paire en ligne ou paire en ligne avec robinet

	Paire en ligne	Paire en ligne avec robinet
show inline-	> show inline-set	> show inline-set

set	Inline-set Inline-Pair-1
	  Mtu est de 1 500 octets
	  Le mode FailSafe est activé/activé
	  Le mode Failsecure est désactivé
	  Le mode Effleurement est désactivé
	  L'option Propagate-link-state est activée
	  le mode de contournement matériel est désactivé
	  Paire-Interface[1] :
	  Interface: Ethernet1/6 « INTERNE »
	  Current-Status : ASCENDANT
	  Interface: Ethernet1/8 "EXTÉRIEUR"
	  Current-Status : ASCENDANT
	  ID du groupe de ponts : 509
	>
		Inline-set Inline-Pair-1
		  Mtu est de 1 500 octets
		  Le mode FailSafe est activé/activé
		  Le mode Failsecure est désactivé
		  Le mode Effleurement est activé
		  L'option Propagate-link-state est activée
		  le mode de contournement matériel est désactivé
		  Paire-Interface[1] :
		  Interface: Ethernet1/6 « INTERNE »
		  Current-Status : ASCENDANT
		  Interface: Ethernet1/8 "EXTÉRIEUR"
		  Current-Status : ASCENDANT
		  ID du groupe de ponts : 0
		
		>

show interface	> show interface e1/6
	Interface Ethernet1/6 « INSIDE », activée, protocole de ligne activé
	  Le matériel est EtherSVI, BW 1000 Mbits/s, DLY 1000 usec
	  Adresse MAC 5897.bdb9.770e, MTU 1500
	  Mode d'interface IPS : Inline, Inline-Set : Inline-Pair-1
	  Adresse IP non attribuée
	  Statistiques de trafic pour "INSIDE" :
	  3 957 paquets en entrée, 264913 octets
	  144 paquets en sortie, 58664 octets
	  4 paquets abandonnés
	  Débit d'entrée de 1 minute 0 pkts/sec, 26 octets/sec
	  Débit de sortie de 1 minute 0 pqts/sec, 7 octets/sec
	  Taux d'abandon de 1 minute, 0 pqts/sec
	  Débit d'entrée de 5 minutes 0 pkts/sec, 28 octets/sec
	  Débit de sortie de 5 minutes 0 pkts/sec, 9 octets/sec
	  Taux d'abandon de 5 minutes, 0 pqt/s
	> show interface e1/8
		> show interface e1/6
		Interface Ethernet1/6 « INSIDE », activée, protocole de ligne activé
		  Le matériel est EtherSVI, BW 1000 Mbits/s, DLY 1000 usec
		  Adresse MAC 5897.bdb9.770e, MTU 1500
		  Mode d'interface IPS : inline-tap, Inline-Set : Inline-Pair-1
		  Adresse IP non attribuée
		  Statistiques de trafic pour "INSIDE" :
		  24 paquets en entrée, 1 378 octets
		  0 paquet en sortie, 0 octet
		  24 paquets abandonnés
		  Débit d'entrée de 1 minute 0 pqts/sec, 0 octets/sec
		  Débit de sortie de 1 minute 0 pqts/sec, 0 octets/sec
		  Taux d'abandon de 1 minute, 0 pqts/sec
		  Débit d'entrée de 5 minutes 0 pqts/sec, 0 octets/sec
		  Débit de sortie de 5 minutes 0 pkts/sec, 0 octets/sec
		  Taux d'abandon de 5 minutes, 0 pqt/s
		> show interface e1/8
		Interface Ethernet1/8 « OUTSIDE »,

	Interface Ethernet1/8 « OUTSIDE », activée, protocole de ligne activé
	  Le matériel est EtherSVI, BW 1000 Mbits/s, DLY 1000 usec
	  Adresse MAC 5897.bdb9.774d, MTU 1500
	  Mode d'interface IPS : Inline, Inline-Set : Inline-Pair-1
	  Adresse IP non attribuée
	  Statistiques de trafic pour "OUTSIDE" :
	  144 paquets en entrée, 55634 octets
	  3 954 paquets en sortie, 339987 octets
	  0 paquet abandonné
	  Débit d'entrée de 1 minute 0 pqts/sec, 7 octets/sec
	  Débit de sortie de 1 minute 0 pkts/sec, 37 octets/sec
	  Taux d'abandon de 1 minute, 0 pqts/sec
	  Débit d'entrée de 5 minutes 0 pqts/sec, 8 octets/sec
	  Débit de sortie de 5 minutes 0 pkts/sec, 39 octets/sec
	  Taux d'abandon de 5 minutes, 0 pqt/s
	>
		activée, protocole de ligne activé
		  Le matériel est EtherSVI, BW 1000 Mbits/s, DLY 1000 usec
		  Adresse MAC 5897.bdb9.774d, MTU 1500
		  Mode d'interface IPS : inline-tap, Inline-Set : Inline-Pair-1
		  Adresse IP non attribuée
		  Statistiques de trafic pour "OUTSIDE" :
		  1 paquet en entrée, 441 octets
		  0 paquet en sortie, 0 octet
		  1 paquets abandonnés
		  Débit d'entrée de 1 minute 0 pqts/sec, 0 octets/sec
		  Débit de sortie de 1 minute 0 pqts/sec, 0 octets/sec
		  Taux d'abandon de 1 minute, 0 pqts/sec
		  Débit d'entrée de 5 minutes 0 pqts/sec, 0 octets/sec
		  Débit de sortie de 5 minutes 0 pkts/sec, 0 octets/sec
		  Taux d'abandon de 5 minutes, 0 pqt/s
		>

Pour traiter un paquet avec une règle de blocage	> show capture CAPI packet-number 1 trace
	
	3 paquets capturés
	
	  1: 16:12:55.785085 192.168.201.50.20 > 192.168.201.60.80 : S 0:0(0) ack 0 win 8192
	Phase : 1
	type : SAISIR
	Sous-type :
	Résultat : ALLOW
	Config :
	Informations complémentaires :
	Liste d'accès MAC
	
	Phase : 2
	type : LISTE D'ACCÈS
		> show capture CAPI packet-number 1 trace
		
		3 paquets capturés
		
		  1: 16:56:02.631437 192.168.201.50.20 > 192.168.201.60.80 : S 0:0(0) win 8192
		Phase : 1
		type : SAISIR
		Sous-type :
		Résultat : ALLOW
		Config :
		Informations complémentaires :
		Liste d'accès MAC
		
		Phase : 2
		type : LISTE D'ACCÈS
		Sous-type :

	Sous-type : Résultat : ALLOW Config : Règle Implicite Informations complémentaires : Liste d'accès MAC Phase : 3 type : NGIPS-MODE Sous-type : ngips-mode Résultat : ALLOW Config : Informations complémentaires : Le flux a pénétré dans une interface configurée pour le mode NGIPS et les services NGIPS est appliqué Phase : 4 type : LISTE D'ACCÈS Sous-type : journal de bord Résultat : CHUTE Config : access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-start access-list CSM_FW_ACL_ remark rule-id 268441600 : POLITIQUE D'ACCÈS : FTD4100 - Obligatoire/1 access-list CSM_FW_ACL_ remark rule-id 268441600 : RÈGLE L4 : Règle 1 Informations complémentaires : Résultat : input-interface : INTÉRIEUR input-status : ascendant input-line-status : ascendant Action : laisser tomber Raison de l'abandon : (suppression de liste de contrôle d'accès) Le flux est refusé par la règle configurée 1 paquet affiché >	Résultat : ALLOW Config : Règle Implicite Informations complémentaires : Liste d'accès MAC Phase : 3 type : NGIPS-MODE Sous-type : ngips-mode Résultat : ALLOW Config : Informations complémentaires : Le flux a pénétré dans une interface configurée pour le mode NGIPS et les services NGIPS est appliqué Phase : 4 type : LISTE D'ACCÈS Sous-type : journal de bord Résultat : AURAIT CHUTÉ Config : access-group CSM_FW_ACL_ global access-list CSM_FW_ACL_ advanced deny ip 192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-start access-list CSM_FW_ACL_ remark rule-id 268441600 : POLITIQUE D'ACCÈS : FTD4100 - Obligatoire/1 access-list CSM_FW_ACL_ remark rule-id 268441600 : RÈGLE L4 : Règle 1 Informations complémentaires : Résultat : input-interface : INTÉRIEUR input-status : ascendant input-line-status : ascendant Action : La liste d'accès aurait été abandonnée, mais le paquet aurait été transféré en raison de la touche en ligne 1 paquet affiché >

Résumé

- Lorsque vous utilisez le mode Inline Pair, le paquet passe principalement par le moteur FTD Snort.
- Les connexions TCP sont traitées en mode de contournement d’état TCP.
- Du point de vue du moteur FTD LINA, une stratégie ACL est appliquée.
- Lorsque le mode Paire en ligne est utilisé, les paquets peuvent être bloqués puisqu'ils sont traités en ligne.
- Lorsque le mode Tap est activé, une copie du paquet est inspectée et abandonnée en interne pendant que le trafic réel passe par FTD sans modification.

Informations connexes

- Cisco Firepower NGFW
- Assistance et documentation techniques - Cisco Systems

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

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