Configuration des interfaces FTD en mode Inline-Pair

Table des matières

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

Il n'y a pas de conditions spécifiques pour ce document.

Composants utilisés

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

- Firepower 4150 FTD (codes 6.1.0.x et 6.3.x)
- Firepower Management Center (FMC) (codes 6.1.0.x et 6.3.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 connexes

Ce document peut également être utilisé avec les versions de matériel et de logiciel suivantes :

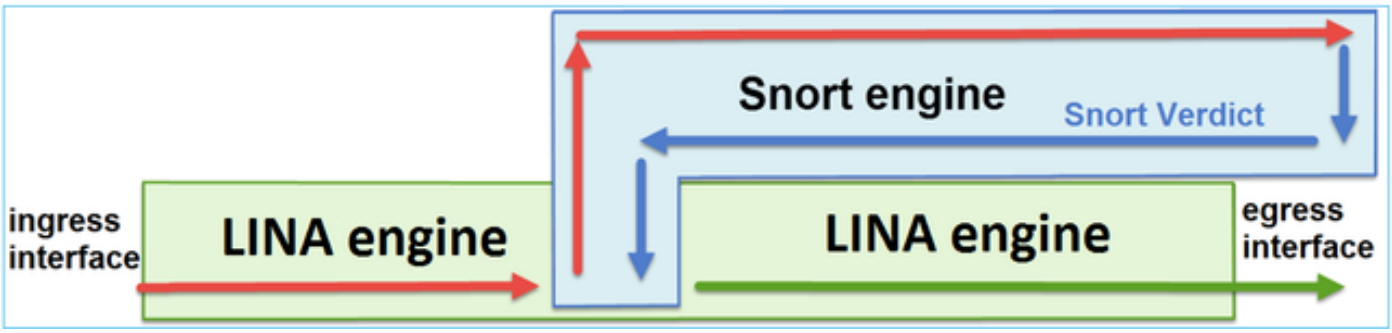
- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100, FPR4100, FPR9300
- VMware (ESXi), Amazon Web Services (AWS), machine virtuelle à base de noyau (KVM)
- Code logiciel FTD 6.2.x et versions ultérieures

Informations générales

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

- Moteur LINA
- Moteur du renifleur

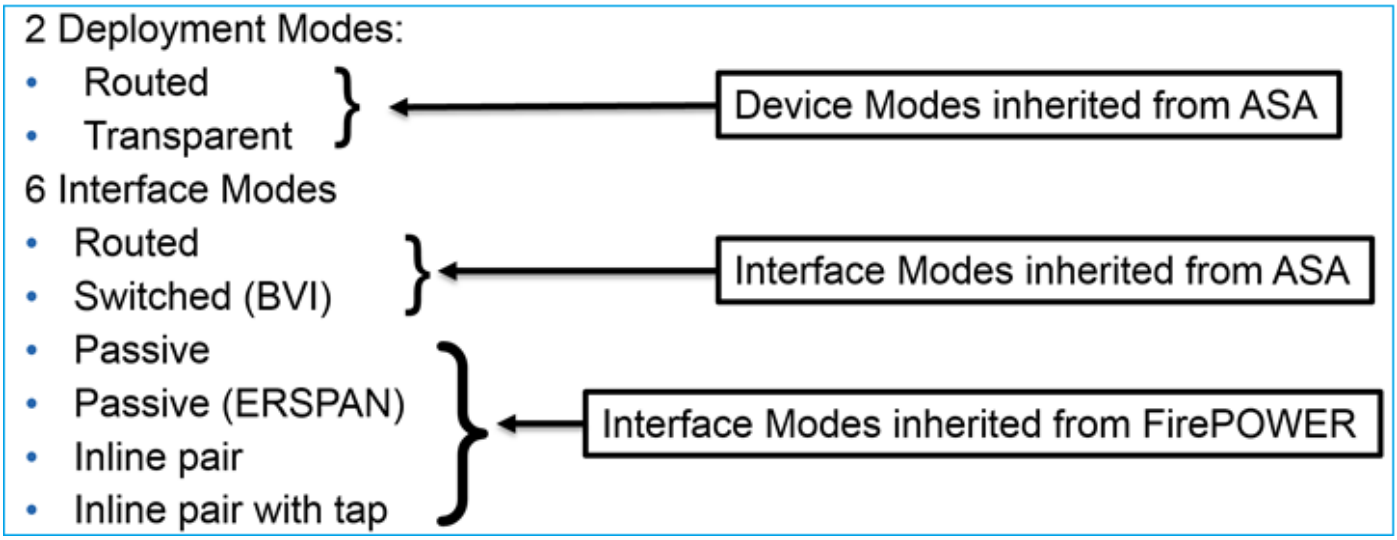
Cette figure montre comment les deux moteurs interagissent :



- Un paquet entre dans l'interface d'entrée et est géré par le moteur LINA
- Si cela est requis par la politique FTD, le paquet est inspecté par le moteur du renifleur
- 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.

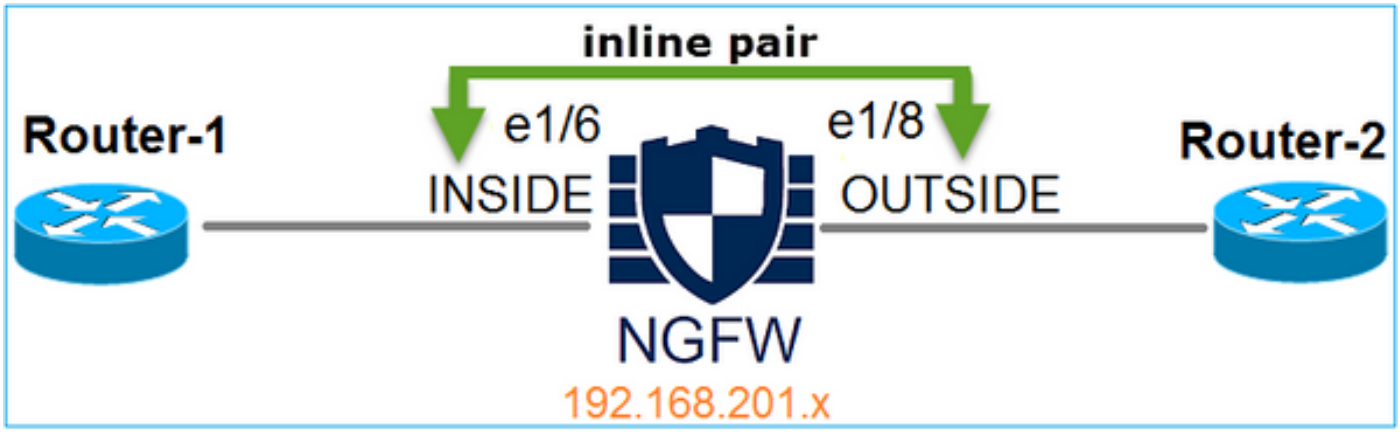
Voici une présentation générale des différents modes de déploiement et d'interface FTD :

mode d'interface FTD	Mode de déploiement FTD	Description	Le trafic peut être abandonné
Routés	Routés	Contrôles LINA complets et Snort-engine	Oui
Commuté	Transparent	Contrôles LINA complets et Snort-engine	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	Vérification partielle du moteur	Non

	transparent	LINA et vérification complète du moteur Snort	
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



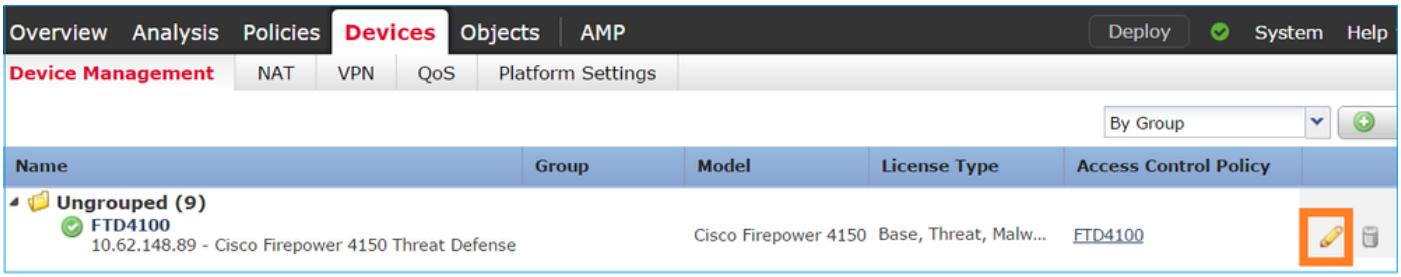
Exigence

Configurez les interfaces physiques e1/6 et e1/8 en mode Inline Pair, conformément aux exigences suivantes :

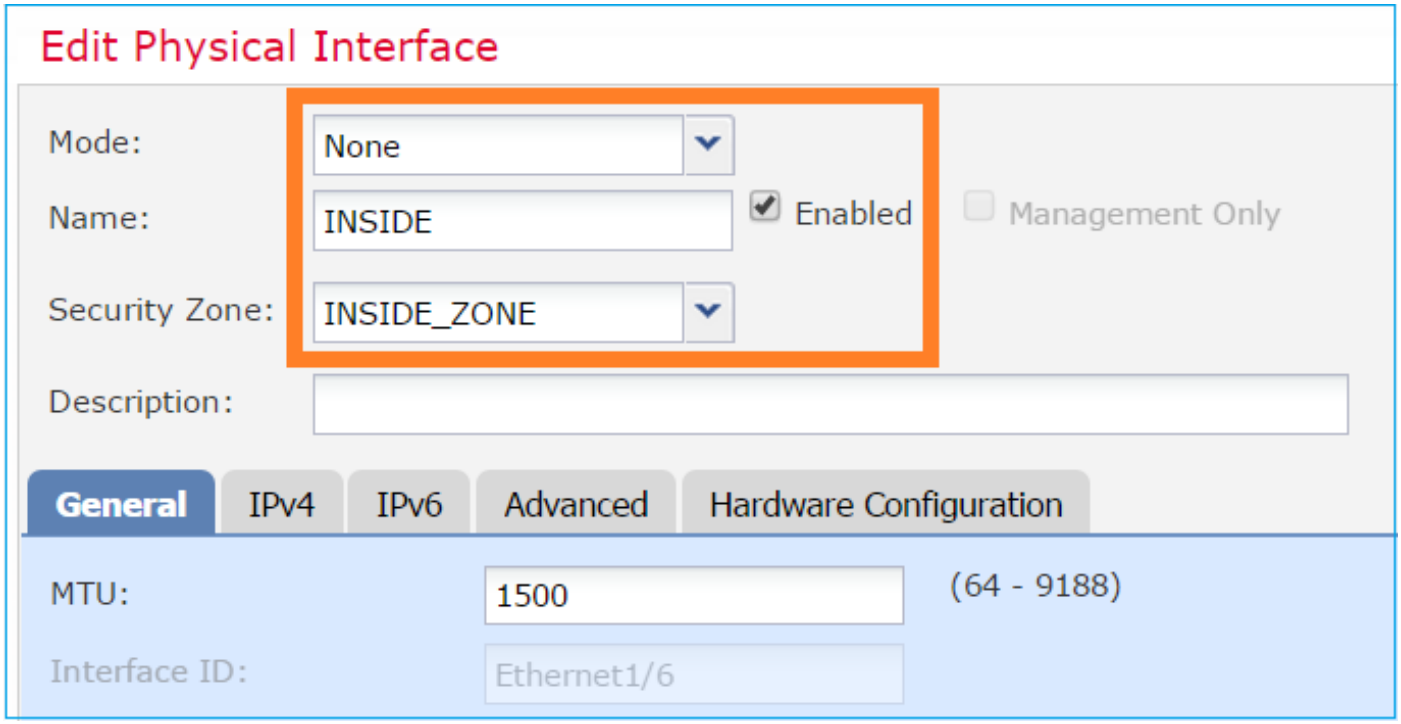
Interface	e1/6	e1/8
Nom	INTÉRIEUR	EXTÉRIEUR
Zone de sécurité	ZONE_INTERNE	ZONE_EXTERNE
Nom du jeu en ligne	Inline-Pair-1	
MTU du jeu en ligne	1500	
FailSafe	Activée	
Propager l'état des liaisons	Activée	

Solution

Étape 1. Afin de configurer les interfaces individuelles, accédez à Périphériques > Gestion des périphériques, sélectionnez le périphérique approprié et sélectionnez Modifier comme indiqué dans l'image.

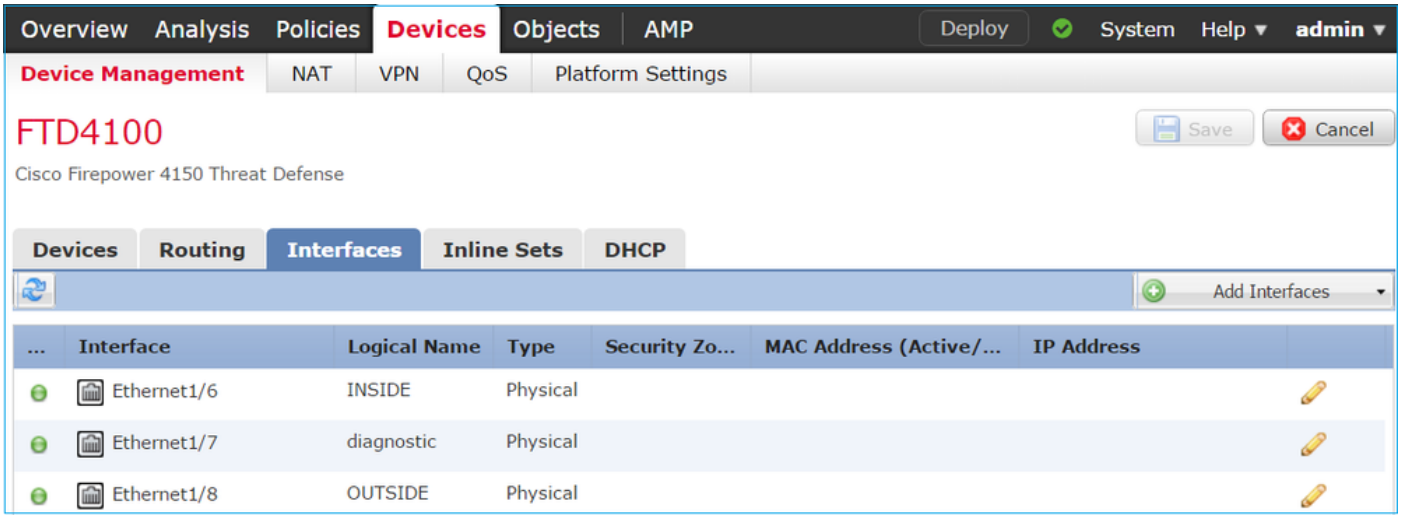


Ensuite, spécifiez Name et Tick Enabled pour l'interface comme indiqué dans l'image.



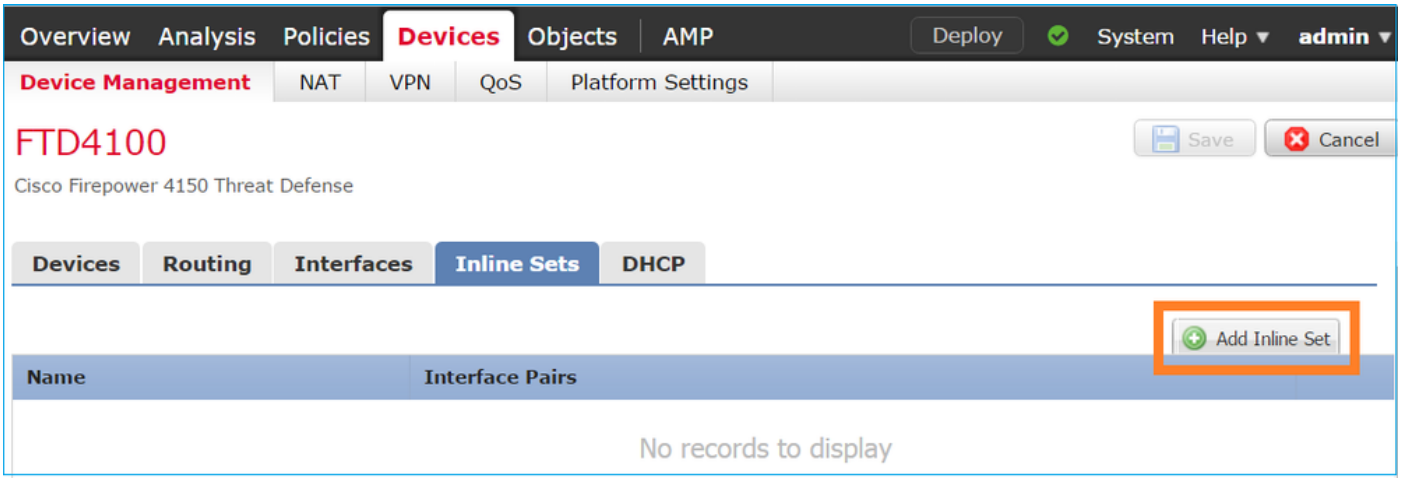
Remarque : le nom est le nom de l'interface.

De même pour l'interface Ethernet1/8. Le résultat final est tel qu'illustré sur l'image.

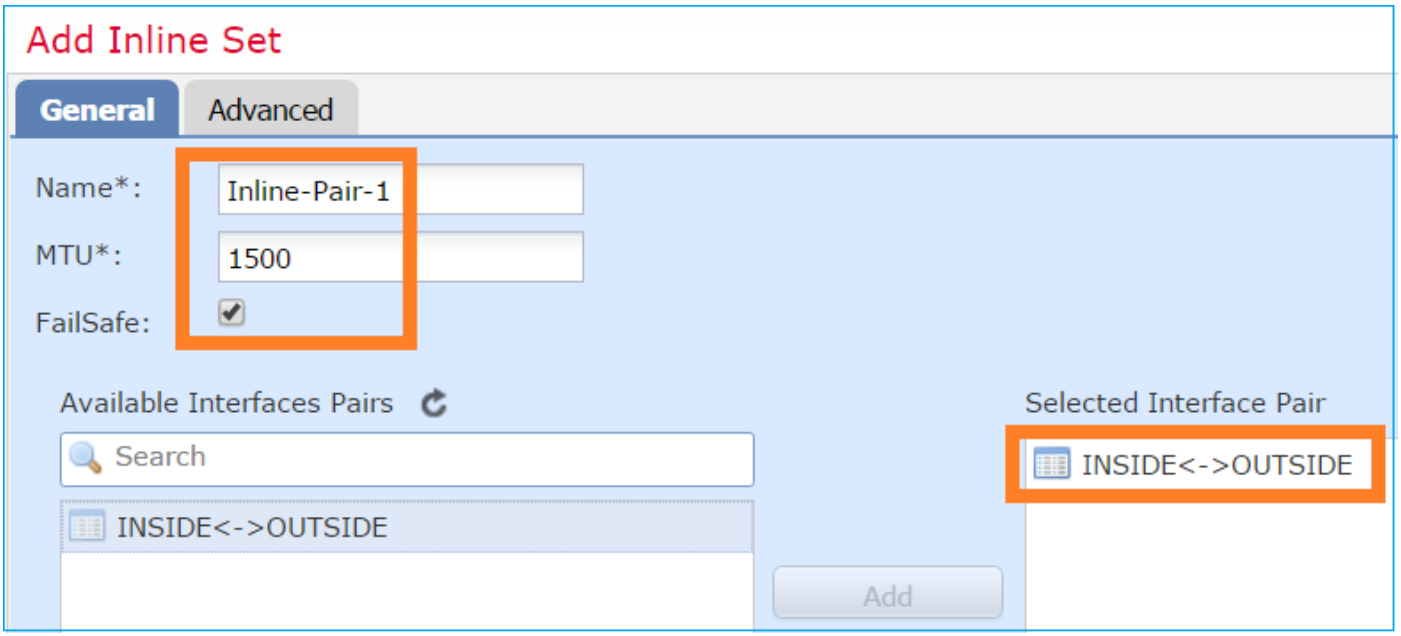


Étape 2. Configurer la paire en ligne.

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

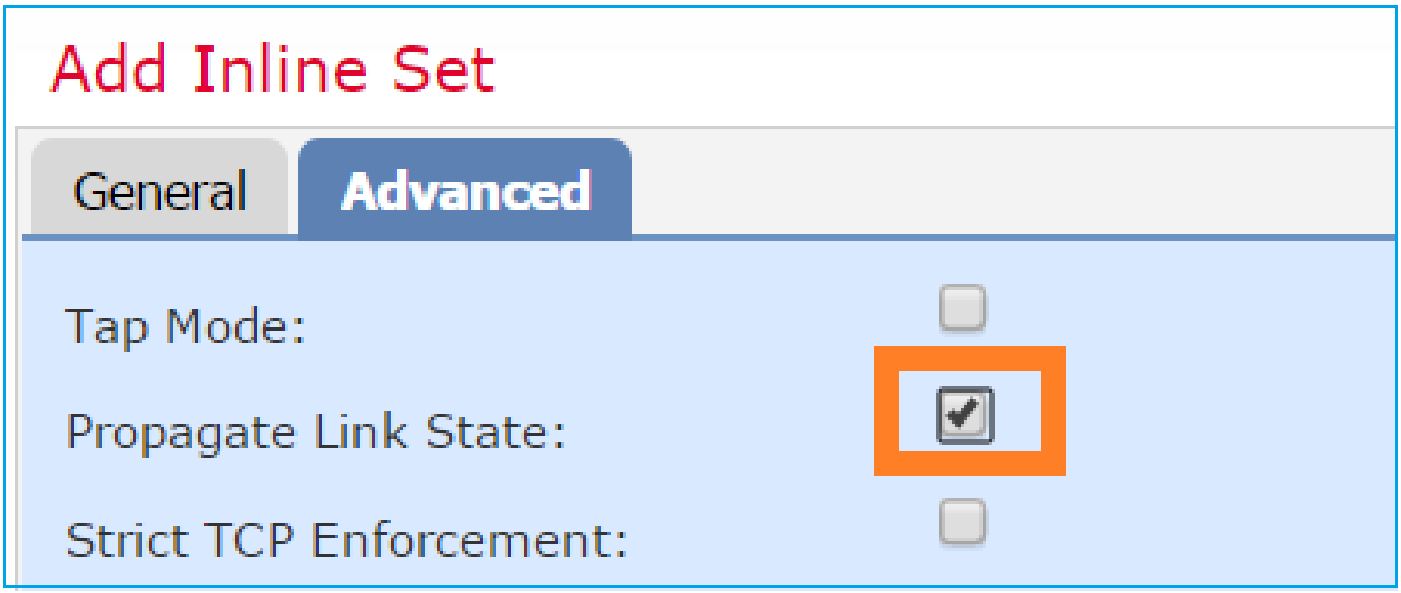


Étape 3. Configurez les paramètres généraux conformément aux exigences indiquées dans l'image.



Remarque : Failsafe permet au trafic de traverser la paire en ligne sans inspection au cas où les tampons d'interface seraient pleins (généralement vu quand le périphérique est surchargé ou le moteur Snort est surchargé). La taille de la mémoire tampon de l'interface est allouée dynamiquement.

Étape 4. Activez l'option Propagate Link State dans les paramètres avancés 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. Enregistrez les modifications et déployez.

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 :

```
> show inline-set

Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
  Tap mode is off
  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/8 "OUTSIDE"
      Current-Status: UP
    Bridge Group ID: 509
>
```

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

Interface et informations de nom :

```
<#root>

>

show nameif

Interface                Name                    Security
Ethernet1/6              INSIDE                    0

Ethernet1/7              diagnostic                0
Ethernet1/8              OUTSIDE                   0

>
```

Vérifiez l'état de l'interface :

```
<#root>

> show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
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

Ethernet1/6                unassigned      YES unset  up                    up
Ethernet1/7                unassigned      YES unset  up                    up
Ethernet1/8                unassigned      YES unset  up                    up
```

Vérifiez les informations d'interface physique :

```
<#root>

>

show interface e1/6
```

```
Interface Ethernet1/6 "INSIDE", is up, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.770e, MTU 1500


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


        IP address unassigned
  Traffic Statistics for "INSIDE":
        468 packets input, 47627 bytes
        12 packets output, 4750 bytes
        1 packets dropped
      1 minute input rate 0 pkts/sec,  200 bytes/sec
      1 minute output rate 0 pkts/sec,  7 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  96 bytes/sec
      5 minute output rate 0 pkts/sec,  8 bytes/sec
      5 minute drop rate, 0 pkts/sec
>

show interface e1/8


Interface Ethernet1/8 "OUTSIDE", is up, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.774d, MTU 1500


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


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        12 packets input, 4486 bytes
        470 packets output, 54089 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  7 bytes/sec
      1 minute output rate 0 pkts/sec,  212 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  7 bytes/sec
      5 minute output rate 0 pkts/sec,  106 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

Vérifier le fonctionnement de l'interface FTD Inline Pair

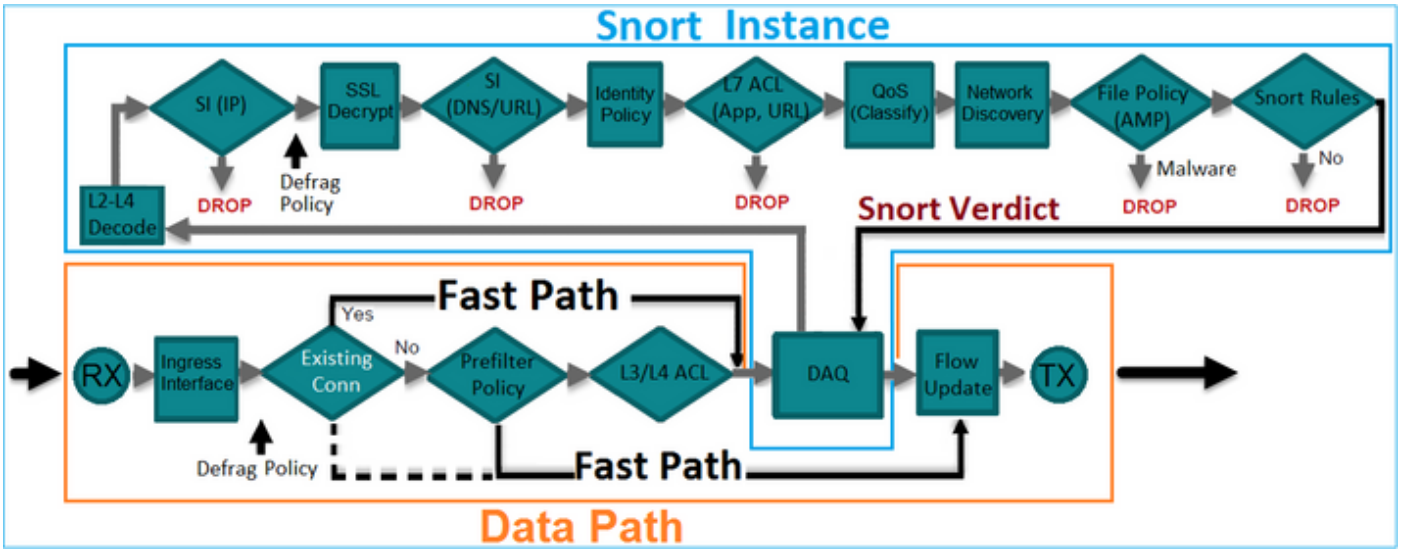
Cette section couvre ces contrôles de vérification afin de vérifier le fonctionnement de la paire en ligne :

- 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 à état de liens
- Vérification 5. Configurer la traduction d'adresses réseau (NAT) statique

Solution

Présentation architecturale

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

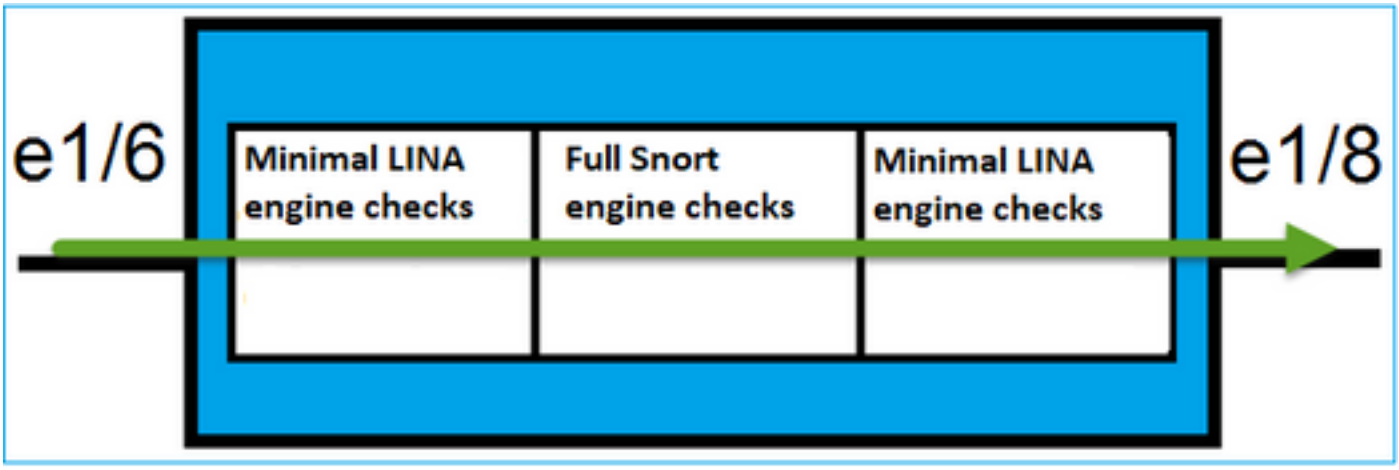


Remarque : seules les interfaces physiques peuvent être membres d'un ensemble de paires en ligne

Théorie de base

- Lorsque vous configurez une paire en ligne 2, les interfaces physiques 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. Avec l'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>

>

packet-tracer input INSIDE tcp 192.168.201.50 1111 192.168.202.50 80

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

Phase: 2

Type: NGIPS-MODE

Subtype: ngips-mode
Result: ALLOW
Config:
Additional Information:

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

Phase: 3

Type: ACCESS-LIST

Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE

Additional Information:

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

Phase: 4

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: 5

Type: FLOW-CREATION

Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 106, packet dispatched to next module

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

>

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>

>

capture CAPI interface INSIDE trace match ip host 192.168.201.60 any


>

capture CAPO interface OUTSIDE match ip host 192.168.201.60 any


>
```

Après avoir envoyé les paquets via le FTD, vous pouvez voir une connexion qui a été créée :

```
<#root>

>

show conn detail


1 in use, 34 most used
Flags: A - awaiting responder ACK to SYN, a - awaiting initiator ACK to SYN,


 b - TCP state-bypass or nailed,


       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - initiator FIN, f - responder FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - initiator data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, M - SMTP data, m - SIP media,

N - inspected by Snort

, n - GUP
       O - responder data, P - inside back connection,
       q - SQL*Net data, R - initiator acknowledged FIN,
       R - UDP SUNRPC, r - responder acknowledged FIN,
       T - SIP, t - SIP transient, U - up,
       V - VPN orphan, v - M3UA W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow


TCP Inline-Pair-1:OUTSIDE(OUTSIDE): 192.168.201.60/80 Inline-Pair-1:INSIDE(INSIDE): 192.168.201.50/20,



flags b N

, idle 13s, uptime 13s, timeout 1h0m, bytes 0

>
```

Remarque : b flag - Un ASA classique abandonnerait un paquet SYN/ACK non sollicité à moins que le contournement d'état TCP soit activé. Une interface FTD en mode Inline Pair gère une connexion TCP en mode de contournement d'état TCP et ne supprime pas les paquets TCP qui n'appartiennent pas aux connexions existantes.

Remarque : indicateur N - Le paquet est inspecté par le moteur FTD Snort.

Les captures le prouvent, puisque vous pouvez voir les 3 paquets qui traversent le FTD :

<#root>

>

show capture CAPI

3 packets captured

   1: 15:27:54.327146   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   2: 15:27:54.330000   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   3: 15:27:54.332517   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
3 packets shown
>

3 paquets quittent le périphérique FTD :

<#root>

>

show capture CAPO

3 packets captured

   1: 15:27:54.327299   192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

```
ack

 0 win 8192
   2: 15:27:54.330030       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
   3: 15:27:54.332548       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 0 win 8192
3 packets shown
>
```

Avec la trace du premier paquet de capture révèle quelques informations supplémentaires comme le verdict du moteur Snort :

<#root>

```
>

show capture CAPI packet-number 1 trace


3 packets captured

   1: 15:27:54.327146       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 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: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268438528
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION RULE

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

Phase: 5
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: 6
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 282, packet dispatched to next module

Phase: 7
Type: EXTERNAL-INSPECT

Subtype:
Result: ALLOW
Config:
Additional Information:

Application: 'SNORT Inspect'

Phase: 8
Type: SNORT

Subtype:

Result: ALLOW

Config:

```
Additional Information:
Snort Verdict: (pass-packet) allow this packet


Phase: 9
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
Action: allow


1 packet shown
>
```

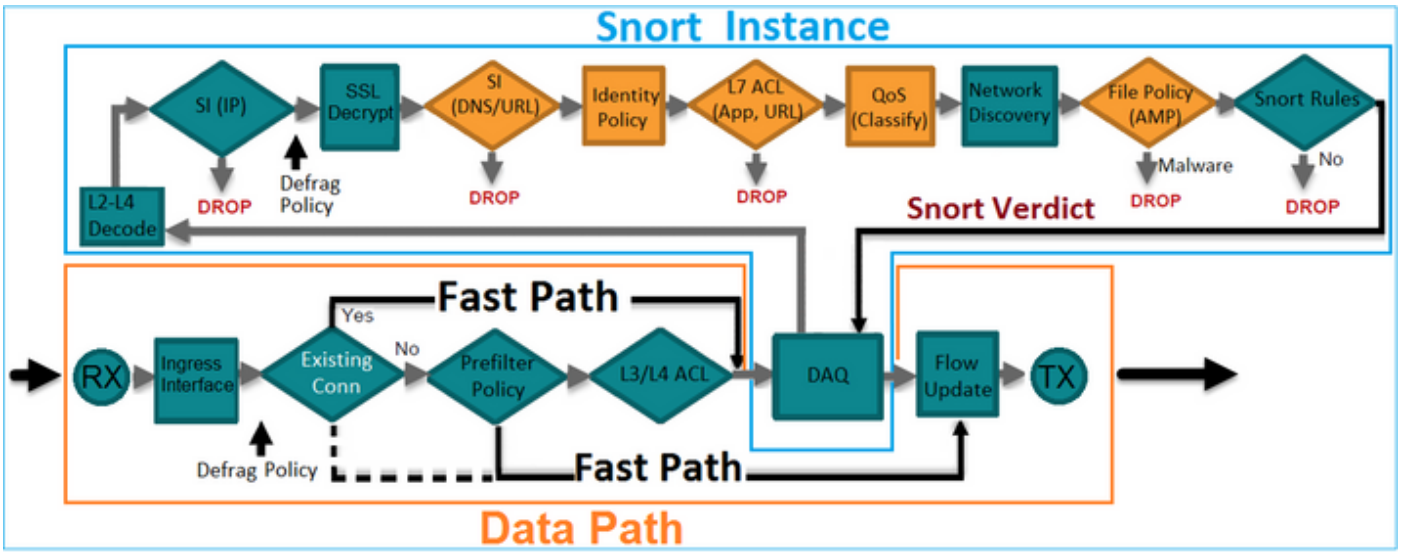
Avec le suivi du deuxième paquet capturé montre que le paquet correspond à une connexion courante de sorte qu'il contourne la vérification de l'ACL, mais est toujours inspecté par le moteur Snort :

```
<#root>

>

show capture CAPI packet-number 2 trace


3 packets captured

   2: 15:27:54.330000       192.168.201.50.20 > 192.168.201.60.80:

S

 0:0(0)

ack

 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: FLOW-LOOKUP
Subtype:ing
Result: ALLOW
Config:
Additional Information:
Found flow with id 282, using current flow



Phase: 4
Type: EXTERNAL-INSPECT

Subtype:
Result: ALLOW
Config:

Additional Information:
Application: 'SNORT Inspect'



Phase: 5
Type: SNORT

Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Verdict: (pass-packet) allow this packet


Phase: 6
Type: CAPTURE
Subtype:
Result: ALLOW
Config:
Additional Information:
MAC Access list

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
Action: allow


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 la paire en ligne, vous pouvez voir dans le résultat du 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 e1/6. Sur l'interface de ligne de commande FTD, vous devez voir que les deux interfaces sont désactivées :

```
<#root>

>

show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
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
Ethernet1/6                unassigned      YES unset  down                  down
Ethernet1/7                unassigned      YES unset  up                    up
Ethernet1/8                unassigned      YES unset  administratively down up

>
```

Les journaux FTD indiquent :

```
<#root>

>

show log

Jan 03 2017 15:53:19: %ASA-4-411002:
Line protocol on Interface Ethernet1/6, changed state to down

Jan 03 2017 15:53:19: %ASA-4-411004:
Interface OUTSIDE, changed state to administratively down

Jan 03 2017 15:53:19: %ASA-4-411004:
Interface Ethernet1/8, changed state to administratively down
```

```
Jan 03 2017 15:53:19: %ASA-4-812005:
Link-State-Propagation activated on inline-pair due to failure of interface Ethernet1/6(INSIDE) bringing
>
```

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

```
<#root>
>
show inline-set


Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off
  Tap mode is off
 Propagate-link-state option is on

  hardware-bypass mode is disabled

Interface-Pair[1]:

    Interface: Ethernet1/6 "INSIDE"

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

    Interface: Ethernet1/8 "OUTSIDE"

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

    Bridge Group ID: 509
>
```

Notez la différence d'état des 2 interfaces :

```
<#root>
>
show interface e1/6
```

```
Interface Ethernet1/6 "INSIDE", is down, line protocol is down


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.770e, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


  Propagate-Link-State-Activated


        IP address unassigned
  Traffic Statistics for "INSIDE":
        3393 packets input, 234923 bytes
        120 packets output, 49174 bytes
        1 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,  6 bytes/sec
      5 minute output rate 0 pkts/sec,  3 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

Et pour l'interface Ethernet1/8 :

```
<#root>

>

show interface e1/8


Interface Ethernet1/8 "OUTSIDE", is administratively down, line protocol is up


  Hardware is EtherSVI, BW 1000 Mbps, DLY 1000 usec
        MAC address 5897.bdb9.774d, MTU 1500
        IPS Interface-Mode: inline, Inline-Set: Inline-Pair-1


Down-By-Propagate-Link-State


        IP address unassigned
  Traffic Statistics for "OUTSIDE":
        120 packets input, 46664 bytes
        3391 packets output, 298455 bytes
        0 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,  3 bytes/sec
      5 minute output rate 0 pkts/sec,  8 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

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

```
<#root>

>

show log

...
Jan 03 2017 15:59:35: %ASA-4-411001:

Line protocol on Interface Ethernet1/6, changed state to up

Jan 03 2017 15:59:35: %ASA-4-411003:

Interface Ethernet1/8, changed state to administratively up

Jan 03 2017 15:59:35: %ASA-4-411003:

Interface OUTSIDE, changed state to administratively up

Jan 03 2017 15:59:35: %ASA-4-812006:

Link-State-Propagation de-activated on inline-pair due to recovery of interface Ethernet1/6(INSIDE) brir

>
```

Vérification 5. Configuration de la NAT statique

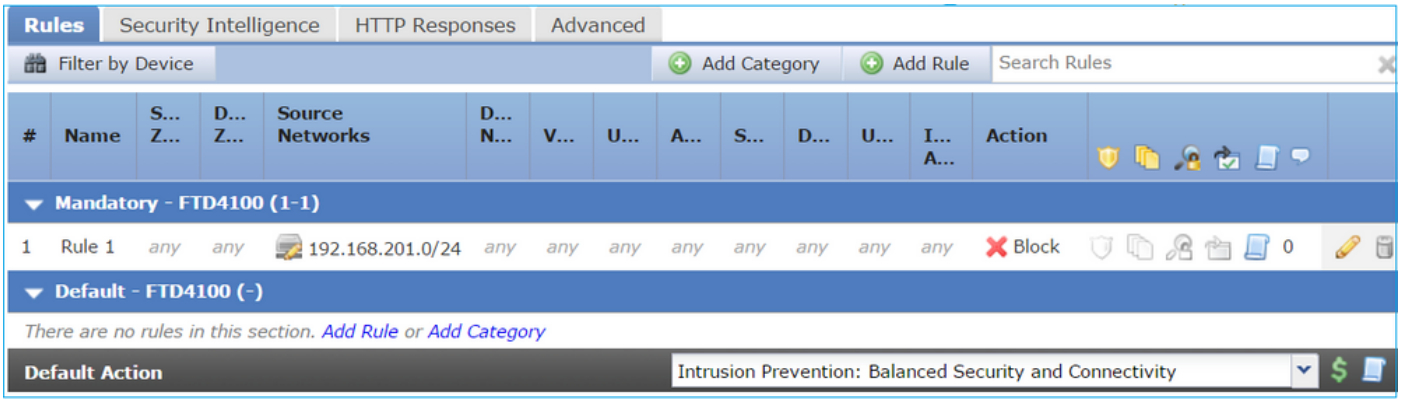
Solution

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

https://www.cisco.com/c/en/us/td/docs/security/firepower/601/configuration/guide/fpmc-config-guide-v601/Network_Address_Translation__NAT__for_Threat_Defense.html

Block Packet on Inline Pair Interface Mode

Créez une règle de blocage, envoyez du trafic via la paire FTD Inline et observez le comportement 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>

>

show capture

capture CAPI type raw-data trace interface INSIDE

[Capturing - 210 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

Avec le suivi, un paquet révèle :

<#root>

>

show capture CAPI packet-number 1 trace

3 packets captured

   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: 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: DROP

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: drop

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


1 packet shown
```

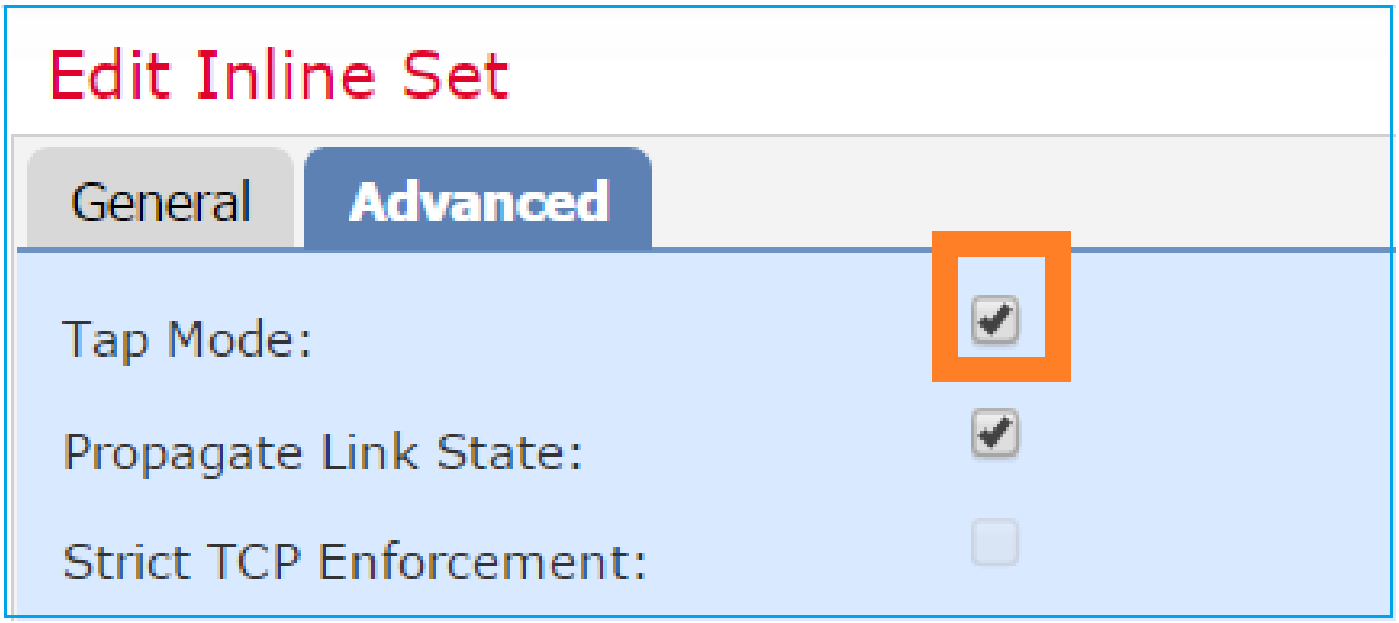
Dans cette trace, on peut voir que le paquet a été abandonné par le moteur FTD LINA et n'a pas été transféré au moteur FTD Snort.

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>

>

show inline-set
```

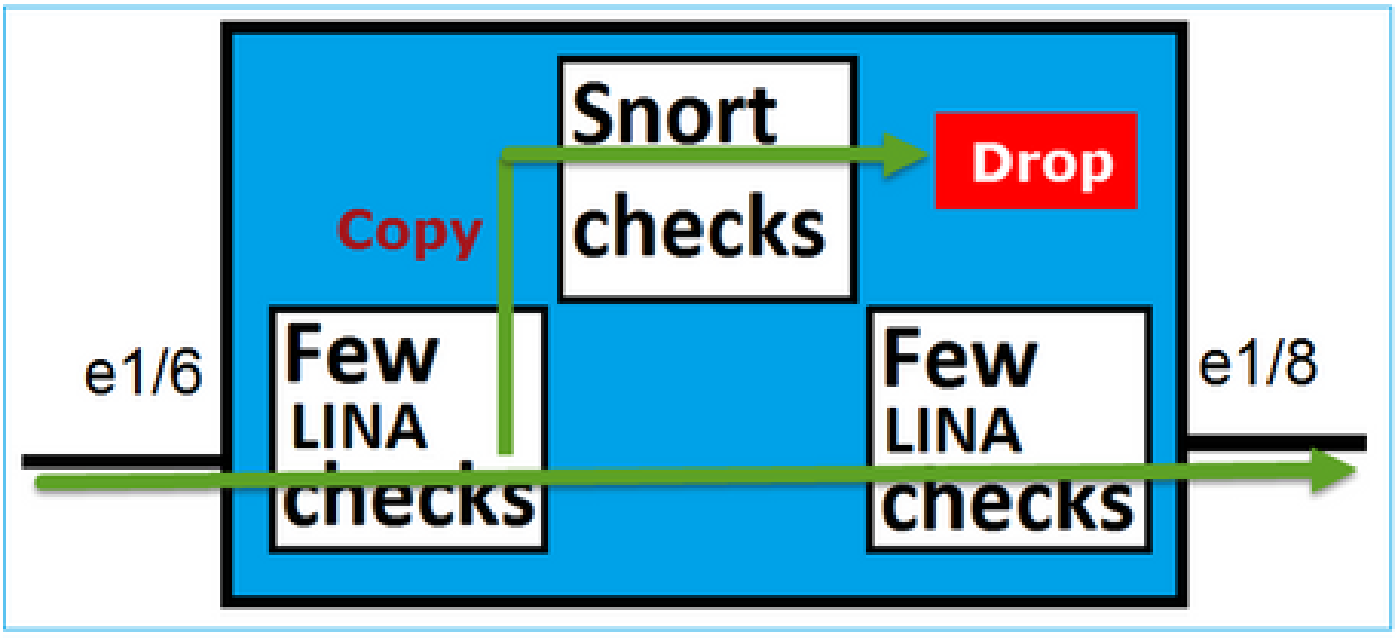
```
Inline-set Inline-Pair-1
  Mtu is 1500 bytes
  Failsafe mode is on/activated
  Failsecure mode is off

Tap mode is on

  Propagate-link-state option is on
  hardware-bypass mode is disabled
  Interface-Pair[1]:
    Interface: Ethernet1/6 "INSIDE"
      Current-Status: UP
    Interface: Ethernet1/8 "OUTSIDE"
      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 2, 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

Le dernier point est comme illustré sur l'image :



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

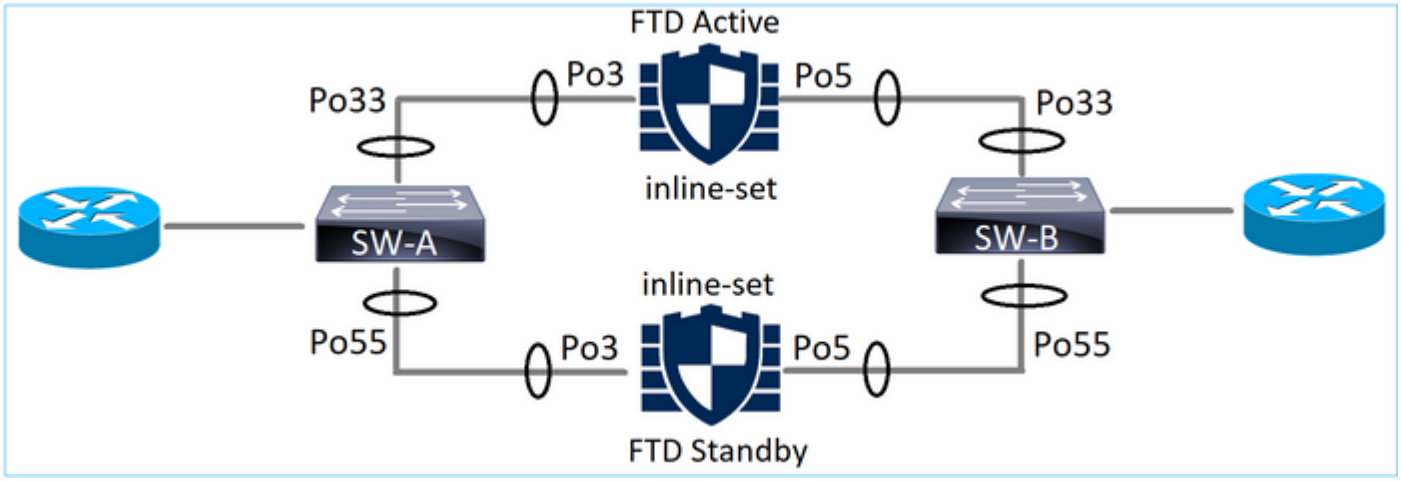
```
1 packet shown
>
```

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     Po35(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#
```

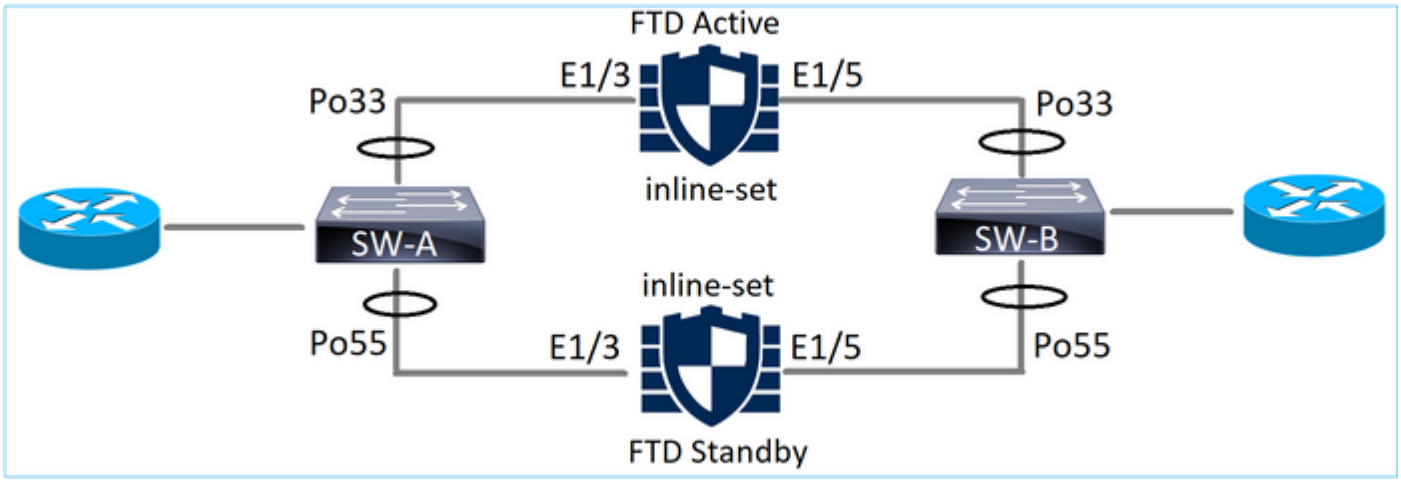
```
show inline-set
```

```
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 : en cas de basculement FTD, la panne du trafic dépend principalement du temps

nécessaire aux commutateurs pour 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
```

⚠ Attention : dans ce scénario, en cas d'événement de basculement FTD, le temps de convergence dépend principalement de la négociation Etherchannel LACP et le temps nécessaire à la panne peut être 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 vs Paire en ligne avec robinet

	Paire en ligne	Paire en ligne avec Tap
show inline-set	> show inline-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 « INSIDE » État actuel : UP Interface : Ethernet1/8 "EXTÉRIEUR" État actuel : UP ID du groupe de ponts : 509 >	> show inline-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 activé L'option Propagate-link-state est activée le mode de contournement matériel est désactivé Paire-Interface[1] : Interface : Ethernet1/6 « INSIDE » État actuel : UP Interface : Ethernet1/8 "EXTÉRIEUR" État actuel : UP 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 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	> 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 », 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

	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 >	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 : CAPTURE Sous-type : Résultat : ALLOW Config : Informations supplémentaires: Liste d'accès MAC Phase : 2 Type : ACCESS-LIST Sous-type : Résultat : ALLOW Config : Règle Implicite Informations supplémentaires: Liste d'accès MAC Phase : 3 Type : NGIPS-MODE Sous-type : ngips-mode Résultat : ALLOW Config : Informations supplémentaires: Le flux a pénétré dans une interface configurée pour le mode NGIPS et les	> 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 : CAPTURE Sous-type : Résultat : ALLOW Config : Informations supplémentaires: Liste d'accès MAC Phase : 2 Type : ACCESS-LIST Sous-type : Résultat : ALLOW Config : Règle Implicite Informations supplémentaires: Liste d'accès MAC Phase : 3 Type : NGIPS-MODE Sous-type : ngips-mode Résultat : ALLOW Config : Informations supplémentaires: Le flux a pénétré dans une interface configurée pour le mode NGIPS et les services NGIPS est appliqué

	services NGIPS est appliqué Phase : 4 Type : ACCESS-LIST Sous-type : log Résultat : DROP 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 : L4 RULE : Règle 1 Informations supplémentaires: Résultat : input-interface : INSIDE input-status : up input-line-status : up Action : abandonner Raison de l'abandon : (acl-drop) le flux est refusé par la règle configurée 1 paquet affiché >	Phase : 4 Type : ACCESS-LIST Sous-type : log Résultat : AURAIT ABANDONNÉ 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 : L4 RULE : Règle 1 Informations supplémentaires: Résultat : input-interface : INSIDE input-status : up input-line-status : up Action : la liste de contrôle 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.