

Configurer des interfaces de défense contre des menaces de puissance de feu en mode d'En ligne-paires

Contenu

[Introduction](#)

[Le but](#)

[Composants utilisés](#)

[Configurer une interface intégrée de paires sur FTD](#)

[Vérifier la configuration d'interface intégrée de paires](#)

[Vérifier l'exécution intégrée d'interface de paires FTD](#)

[Vérification 1 ? Utilisant le traceur de paquets](#)

[Vérification 2 ? Envoi des paquets du TCP SYN/ACK par les paires intégrées](#)

[Vérification 3 ? L'engine de Pare-feu mettent au point pour le trafic Allowed](#)

[Vérification 4 ? Vérifier la propagation d'État de lien](#)

[Vérification 5 ? Configurer NAT statique](#)

[Blocage d'un paquet sur le mode interface intégré de paires](#)

[Configurer le mode intégré de paires avec la prise](#)

[En vérifiant les paires intégrées FTD avec la prise reliez l'exécution](#)

[Comparaison : Paires intégrées contre des paires intégrées avec la prise](#)

[Résumé](#)

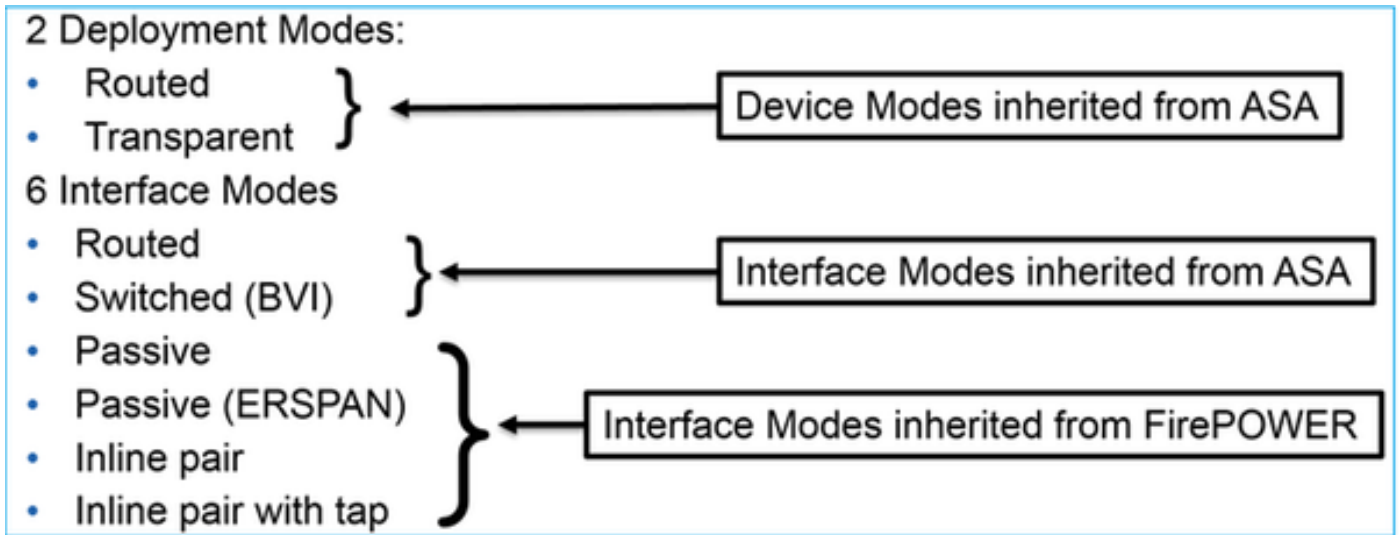
[Documents connexes](#)

Introduction

La défense contre des menaces de puissance de feu (FTD) est une image logicielle unifiée qui peut être installée sur les Plateformes suivantes :

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware (ESXi)
- Services Web d'Amazone (AWS)
- KVM
- Module de routeur ISR

FTD fournit 2 modes de déploiement et 6 modes interface



Remarque: Vous pouvez mélanger des modes interface sur une appliance du sigle FTD

Voici une vue d'ensemble à niveau élevé du divers déploiement et des modes interface FTD :

Mode interface FTD	Mode de déploiement FTD	Description	Le trafic peut être abandonné
Conduit	Conduit	Pleins ASA-engine et contrôles de Renifler-engine	Oui
Commuté	Transparent	Pleins ASA-engine et contrôles de Renifler-engine	Oui
Paires intégrées	Conduit ou transparent	ASA-engine partielle et pleins contrôles de Renifler-engine	Oui
Paires intégrées avec la prise	Conduit ou transparent	ASA-engine partielle et pleins contrôles de Renifler-engine	Non
Passif	Conduit ou transparent	ASA-engine partielle et pleins contrôles de Renifler-engine	Non
Passif (ERSPAN)	Conduit	ASA-engine partielle et pleins contrôles de Renifler-engine	Non

Le but

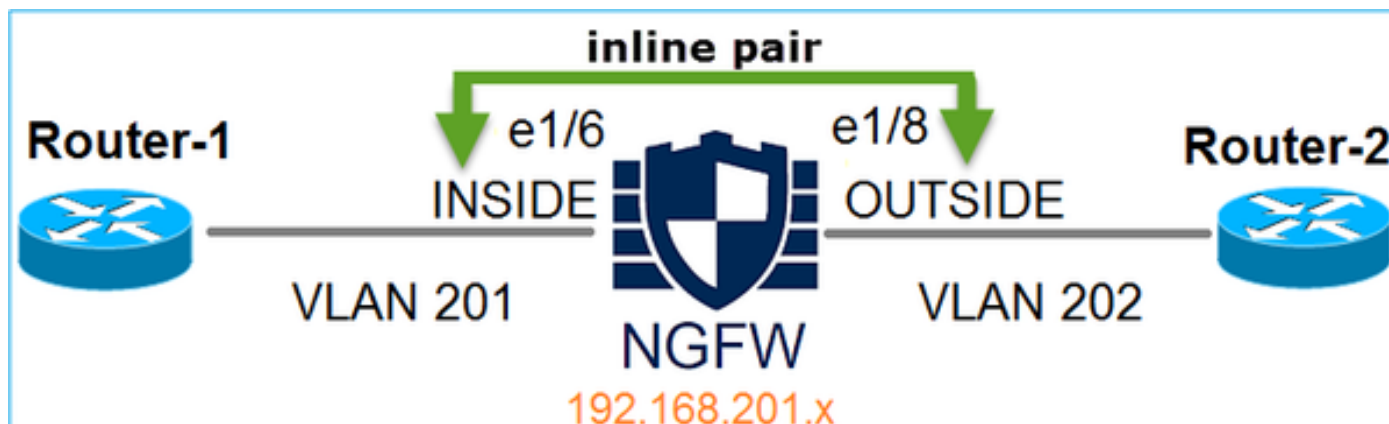
Le but de ce document est à :

- Expliquez la configuration et l'exécution des En ligne-paires FTD reliant

Composants utilisés

- Code s'exécutant 6.1.0.x de la puissance de feu 4150 FTD
- Centre de Gestion de puissance de feu (FMC) exécutant 6.1.0.x

Topologie



Configurer une interface intégrée de paires sur FTD

Condition requise

Configurez les interfaces physiques e1/6 et e1/8 en mode intégré de paires par conditions requises suivantes :

Interface	e1/6	e1/8
Nom	À L'INTÉRIEUR	DEHORS
Zone de Sécurité	INSIDE_ZONE	OUTSIDE_ZONE
Nom réglé intégré	Inline-Pair-1	
MTU réglé d'en ligne	1500	
De sécurité	Activé	
État de lien de propagation	Activé	

Solution

Étape 1 ? Configurer les interfaces individuelles

Naviguez vers les **périphériques** > la **Gestion de périphériques**, sélectionnez le périphérique approprié et cliquez sur en fonction l'icône **Edit** :

Name	Group	Model	License Type	Access Control Policy
Ungrouped (9) FTD4100 10.62.148.89 - Cisco Firepower 4150 Threat Defense		Cisco Firepower 4150	Base, Threat, Malw...	FTD4100

Spécifiez le nom et activez l'interface :

Edit Physical Interface

Mode: Enabled Management Only

Name:

Security Zone:

Description:

General | IPv4 | IPv6 | Advanced | Hardware Configuration

MTU: (64 - 9188)

Interface ID:

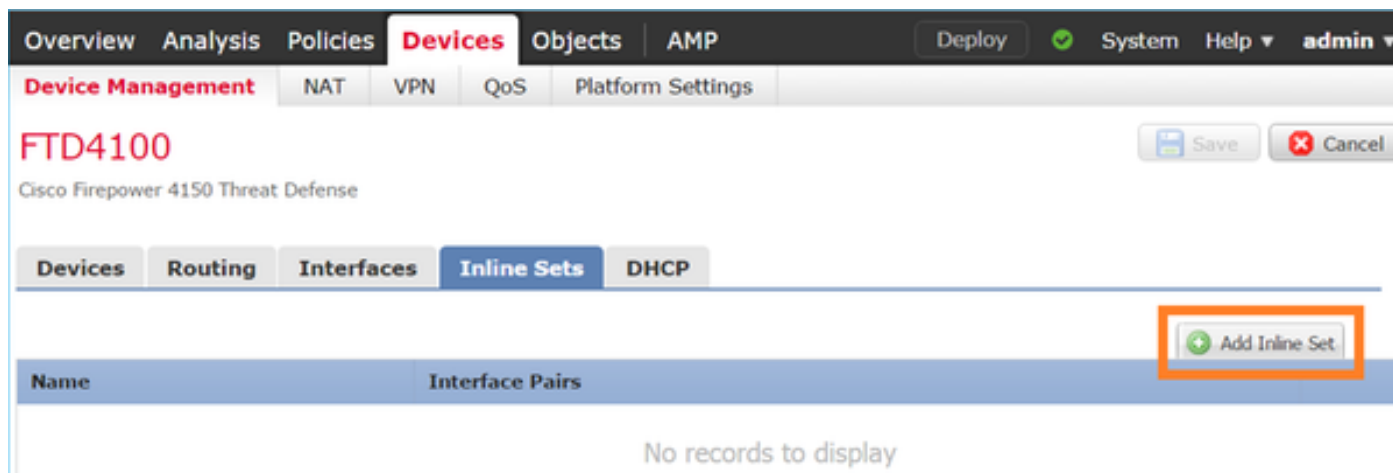
Le nom sera le nameif de l'interface

De même pour l'interface Ethernet1/8. Le résultat final :

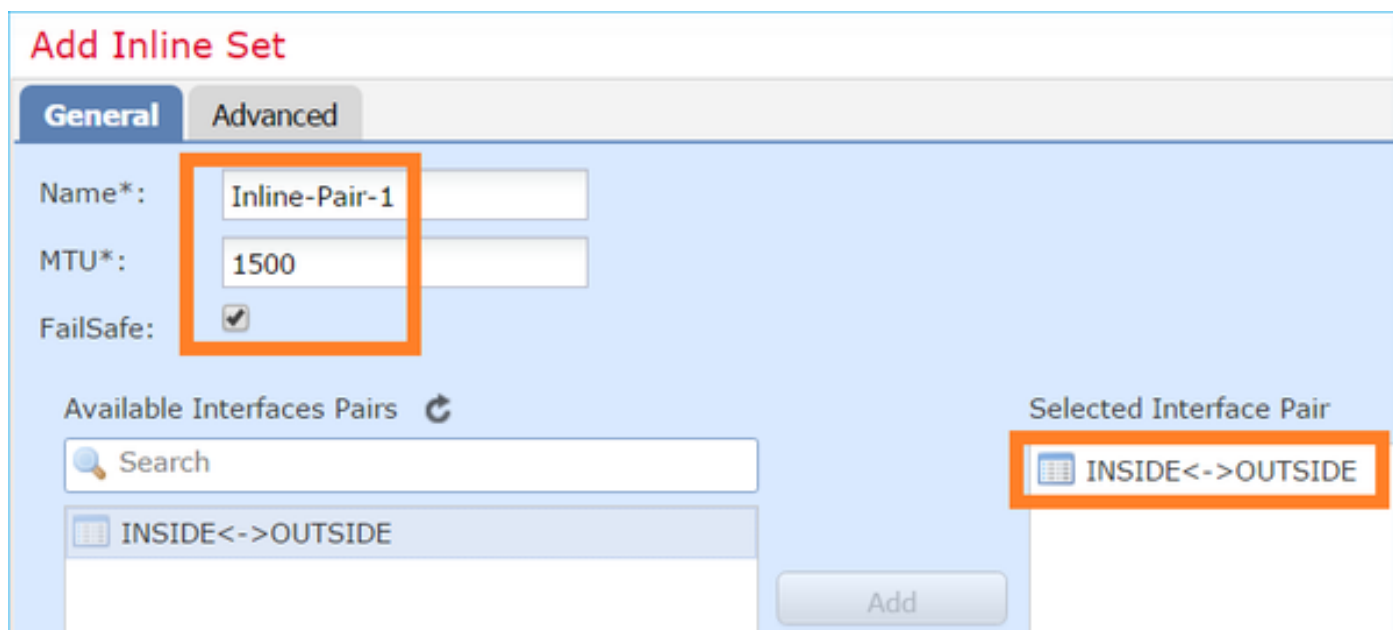
Interface	Logical Name	Type	Security Zo...	MAC Address (Active/...	IP Address
Ethernet1/6	INSIDE	Physical			
Ethernet1/7	diagnostic	Physical			
Ethernet1/8	OUTSIDE	Physical			

Étape 2 ? Configurer les paires intégrées

Naviguez vers l'onglet **intégré de positionnements** et cliquez sur en fonction l'en ligne **Add réglé** :

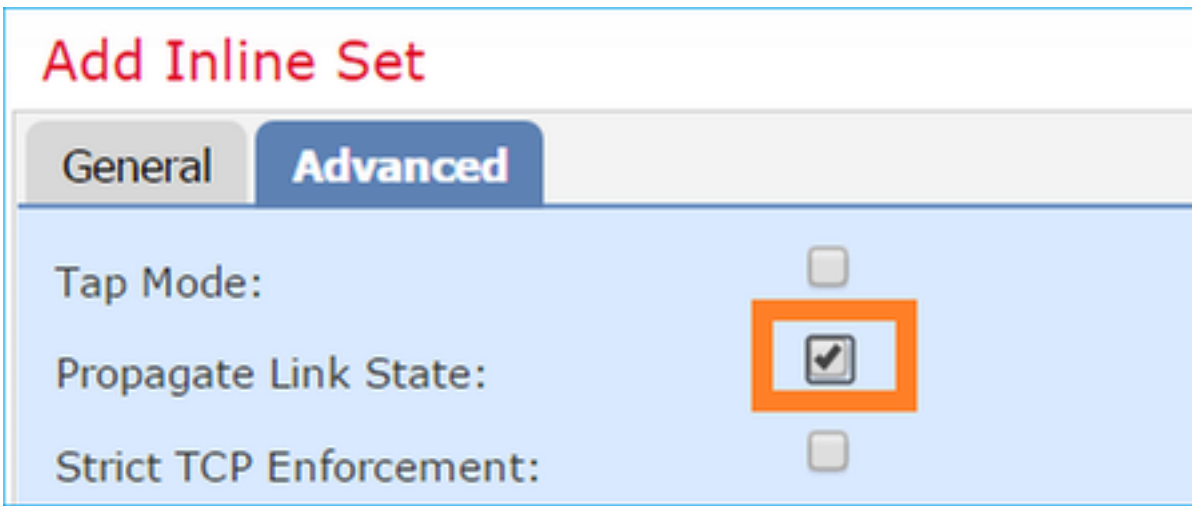


Configurez les configurations par conditions requises :



De sécurité permet au trafic pour traverser les paires intégrées non examinées au cas où les mémoires tampons d'interface seraient pleines (typiquement vu quand le périphérique est surchargé ou l'engine de renifler est surchargée). La taille de mémoire tampon d'interface est dynamiquement allouée.

Enable ? **État de lien de propagation** ? option :



La propagation d'état de lien réduit automatiquement la deuxième interface dans les paires intégrées d'interface quand une des interfaces dans le positionnement d'en ligne descend.

Sauvegardez les modifications et déployez-vous

Vérifier la configuration d'interface intégrée de paires

Vérifiez la configuration intégrée de paires du FTD CLI

Solution

Ouvrez une session à FTD CLI et vérifiez la configuration intégrée de paires :

```
> 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'identification groupe de passerelle est une valeur différente que 0. Si le mode de prise est sur puis il est 0

Interface et informations de nom :

```
> show nameif
Interface          Name          Security
Ethernet1/6       INSIDE        0
Ethernet1/7       diagnostic    0
Ethernet1/8       OUTSIDE       0
>
```

Vérifier l'état d'interface :

```
> 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
```

Vérifier les informations d'interface physique :

```
> 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 l'exécution intégrée d'interface de paires FTD

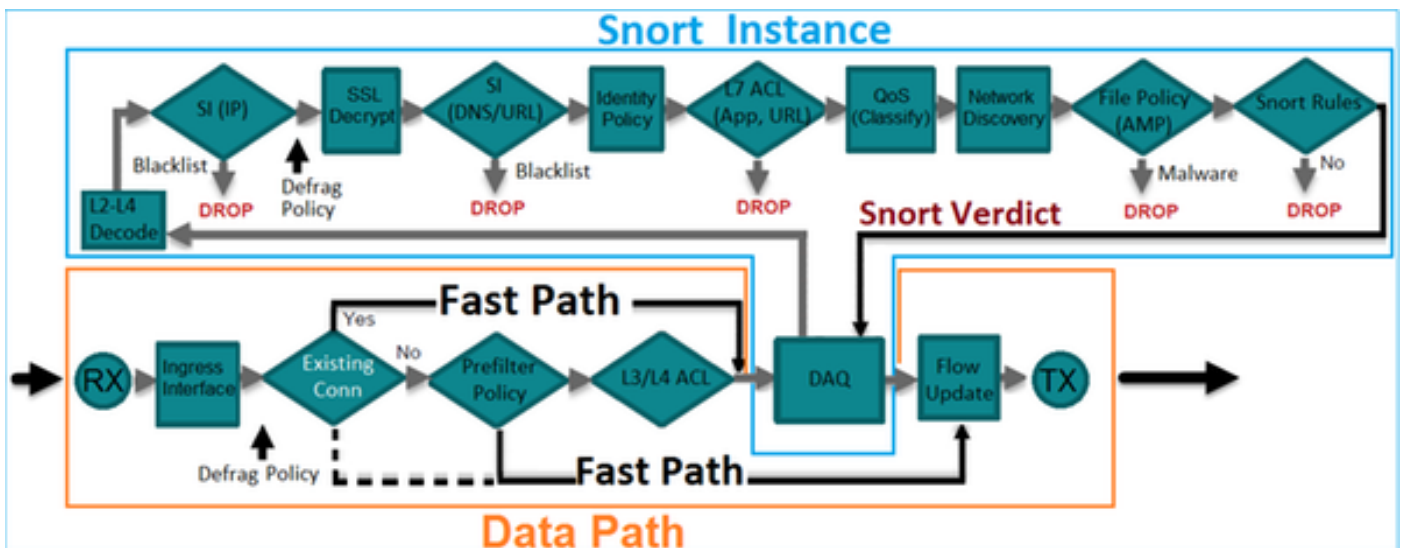
Cette section couvre les contrôles suivants de vérification afin de vérifier l'exécution intégrée de paires :

- Vérification 1 ? Utilisant le traceur de paquets
- Vérification 2 ? Activant la capture avec le suivi et envoyer un paquet du TCP SYN/ACK par les paires intégrées
- Vérification 3 ? En surveillant le trafic FTD utilisant l'engine de Pare-feu mettez au point
- Vérification 4 ? Vérifier la fonctionnalité de propagation d'État de lien
- Vérification 5 ? Configurer NAT statique

Solution

Aperçu architectural

Quand 2 interfaces FTD fonctionnent en mode d'En ligne-paires un paquet est manipulé comme suit :



Remarque: Seulement les interfaces physiques peuvent être des membres d'une paire intégrée réglée

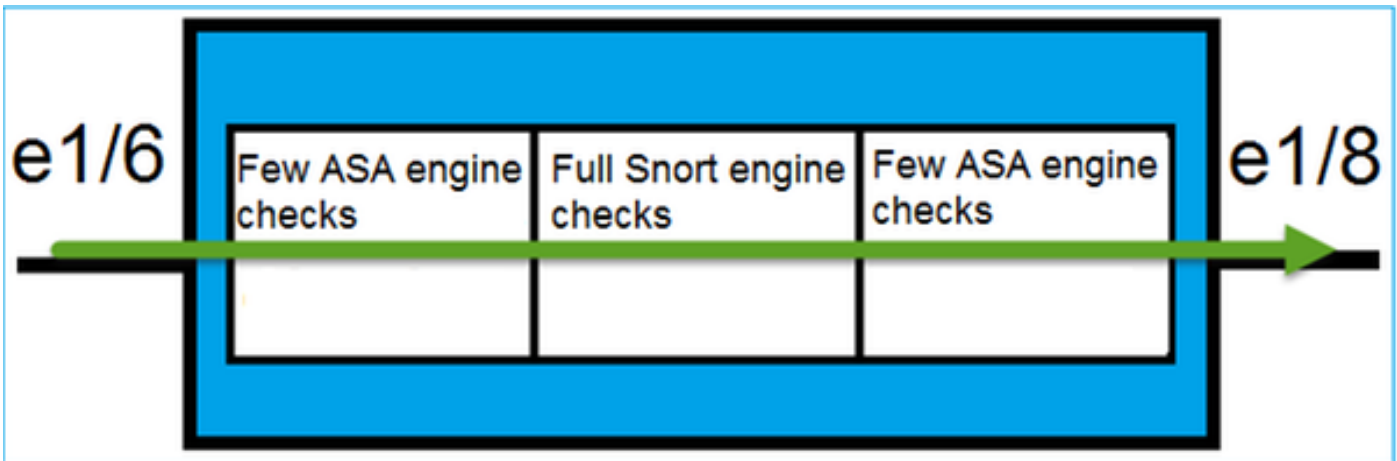
Théorie de base

- En configurant une paire intégrée 2 interfaces physiques sont intériorisées un pont

sur

- Très semblable à l'en ligne classique IPS
- Disponible dans des modes **conduits** ou **transparent de déploiement**
- La plupart des caractéristiques d'engine ASA (NAT, acheminement, L3/L4 ACL etc.) ne sont pas **disponibles** pour des écoulements allant par une paire intégrée
- Le trafic de transit **peut être abandonné**
- **Peu de** contrôles d'engine ASA sont appliqués avec **complètement reniflent des** contrôles d'engine

Le dernier point peut être visualisé comme suit :



Vérification 1 ? Utilisant le traceur de paquets

Voici le traceur de paquets sorti émulant un paquet traversant les paires intégrées avec les points intéressants mis en valeur :

```
> 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 will 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 will be sent to snort for additional processing where a verdict will be 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 des paquets du TCP SYN/ACK par les paires intégrées

Vous pouvez générer des paquets du TCP SYN/ACK utilisant un utilitaire de ouvrage de paquet comme Scapy. La syntaxe suivante générera 3 paquets avec des indicateurs SYN/ACK activés :

```
root@KALI:~# scapyINFO: 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 la capture suivante sur FTD CLI et envoyez peu de paquets du TCP SYN/ACK :

```
> 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 envoi les paquets par le FTD vous pouvez voir une connexion qui a été créée :

```
> 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
```

>

- **indicateur b** : Une ASA classique relâcherait un paquet non sollicité SYN/ACK à moins que l'état-contournement de TCP ait été activé. Une interface FTD en mode intégré de paires manipule une connexion TCP en mode et doesn d'état-contournement de TCP ? paquets TCP de baisse t qui mettent ? t appartiennent aux connexions existantes
- **Indicateur N** : Le paquet sera examiné par le FTD reniflent l'engine

Les captures prouvent ce qui précède puisque vous pouvez voir les 3 paquets traverser le FTD :

```
> 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 quittant le périphérique FTD :

```
> 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
```

>

La découverte du premier paquet de capture indique certaines informations complémentaires

comme le verdict d'engine de renifler :

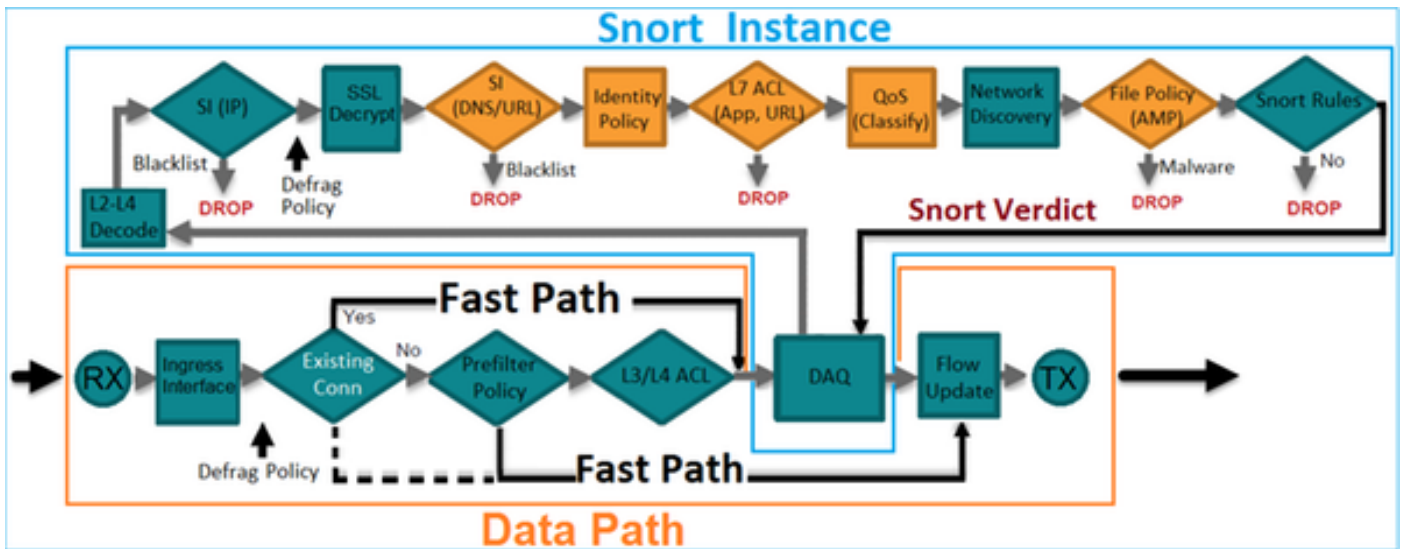
```
> show capture CAPI packet-number 1 trace3 packets captured 1: 15:27:54.327146 192.168.201.50.20
> 192.168.201.60.80: S 0:0(0) ack 0 win 8192Phase: 1Type: CAPTURESubtype:Result:
ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result:
ALLOWConfig:Implicit RuleAdditional Information:MAC Access listPhase: 3Type: NGIPS-MODESubtype:
ngips-modeResult: ALLOWConfig:Additional Information:The flow ingressed an interface configured
for NGIPS mode and NGIPS services will be appliedPhase: 4Type: ACCESS-LISTSubtype: logResult:
ALLOWConfig:access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip any any
rule-id 268438528access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: FTD4100 -
Default/laccess-list CSM_FW_ACL_ remark rule-id 268438528: L4 RULE: DEFAULT ACTION
RULEAdditional Information: This packet will be sent to snort for additional processing where a
verdict will be reachedPhase: 5Type: NGIPS-EGRESS-INTERFACE-LOOKUPSubtype: Resolve Egress
InterfaceResult: ALLOWConfig:Additional Information:Ingress interface INSIDE is in NGIPS inline
mode.Egress interface OUTSIDE is determined by inline-set configurationPhase: 6Type: FLOW-
CREATIONSubtype:Result: ALLOWConfig:Additional Information:New flow created with id 282, packet
dispatched to next modulePhase: 7Type: EXTERNAL-INSPECTSubtype:Result: ALLOWConfig:Additional
Information:Application: 'SNORT Inspect'Phase: 8Type: SNORTSubtype:Result:
ALLOWConfig:Additional Information:Snort Verdict: (pass-packet) allow this packetPhase: 9Type:
CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access listResult:input-interface:
OUTSIDEinput-status: upinput-line-status: upAction: allow1 packet shown>
```

La découverte du deuxième paquet capturé prouve que le paquet apparie une connexion existante ainsi il saute le contrôle d'ACL, mais est examinée toujours par l'engine de renifler :

```
> show capture CAPI packet-number 2 trace3 packets captured 2: 15:27:54.330000 192.168.201.50.20
> 192.168.201.60.80: S 0:0(0) ack 0 win 8192Phase: 1Type: CAPTURESubtype:Result:
ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result:
ALLOWConfig:Implicit RuleAdditional Information:MAC Access listPhase: 3Type: FLOW-
LOOKUPSubtype:Result: ALLOWConfig:Additional Information:Found flow with id 282, using existing
flowPhase: 4Type: EXTERNAL-INSPECTSubtype:Result: ALLOWConfig:Additional
Information:Application: 'SNORT Inspect'Phase: 5Type: SNORTSubtype:Result:
ALLOWConfig:Additional Information:Snort Verdict: (pass-packet) allow this packetPhase: 6Type:
CAPTURESubtype:Result: ALLOWConfig:Additional Information:MAC Access listResult:input-interface:
OUTSIDEinput-status: upinput-line-status: upAction: allow1 packet shown>
```

Vérification 3 ? L'engine de Pare-feu mettent au point pour le trafic Allowed

L'engine de Pare-feu mettent au point des passages contre les éléments spécifiques du FTD reniflent l'engine comme la stratégie de contrôle d'accès :



Quand l'envoi les paquets du TCP SYN/ACK par des paires intégrées de vous peut voir dans la sortie de débogage :

```
> 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 Allow and prefilter rule 0
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 ? Vérifier la propagation d'État de lien

Activez la mémoire tampon ouvrant une session FTD et arrête le switchport connecté à l'interface e1/6. Sur FTD CLI vous devriez voir que les deux interfaces sont descendues :

```
> 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
>
```

L'exposition de logs FTD :

> show logging

```
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-Propogation activated on inline-pair due to
failure of interface Ethernet1/6(INSIDE) bringing down pair interface Ethernet1/8(OUTSIDE)
>
```

L'état d'en ligne-positionnement affiche l'état des 2 membres d'interface :

> 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 dans le statut des 2 interfaces :

> 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 :

> 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 switchport les logs FTD affichent :

```
> show logging
```

```
...
```

```
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) bringing up pair interface Ethernet1/8(OUTSIDE)
```

>

Vérification 5 ? Configurer NAT statique

Solution

NAT n'est pas pris en charge pour des interfaces fonctionnant dans l'en ligne, la prise intégrée ou les modes passifs :

<http://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>

Blocage d'un paquet sur le mode interface intégré de paires

Créez une règle de bloc comme le suivant, envoyez le trafic par les paires intégrées FTD et observez le comportement :

Rules														
Security Intelligence														
HTTP Responses														
Advanced														
Filter by Device														
Add Category														
Add Rule														
Search Rules														
#	Name	S... Z...	D... Z...	Source Networks	D... N...	V...	U...	A...	S...	D...	U...	I... A...	Action	
Mandatory - FTD4100 (1-1)														
1	Rule 1	any	any	192.168.201.0/24	any	any	any	any	any	any	any	any	Block	
Default - FTD4100 (-)														
There are no rules in this section. Add Rule or Add Category														
Default Action														
Intrusion Prevention: Balanced Security and Connectivity														

Solution

Activez la capture avec le suivi et envoyez les paquets SYN/ACK par les paires d'en ligne FTD. Le trafic est bloqué :

```
> 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
```

La découverte d'un paquet indique :

```
> 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 will be 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 flow-start
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

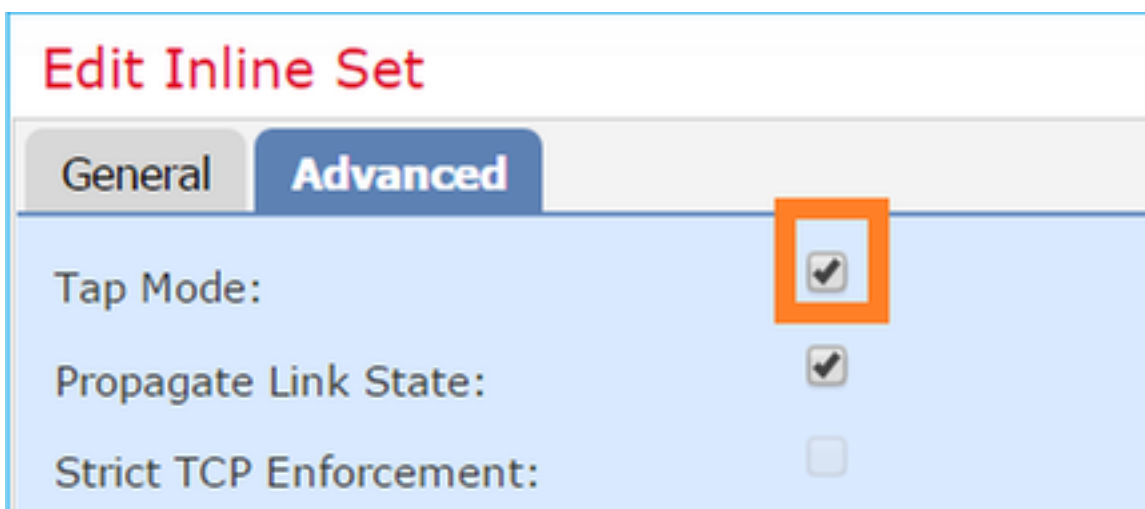
Dans le suivi ci-dessus il peut voir que le paquet a été lâché par l'engine FTD ASA et n'a pas été expédié au FTD reniflent l'engine.

Configurer le mode intégré de paires avec la prise

Mode de prise d'enable sur les paires intégrées

Solution

Naviguez vers les **périphériques > la Gestion de périphériques > les positionnements intégrés**, éditez les paires intégrées, cliquez sur en fonction l'**onglet Avancé** et activez le **mode de prise** :



Vérification

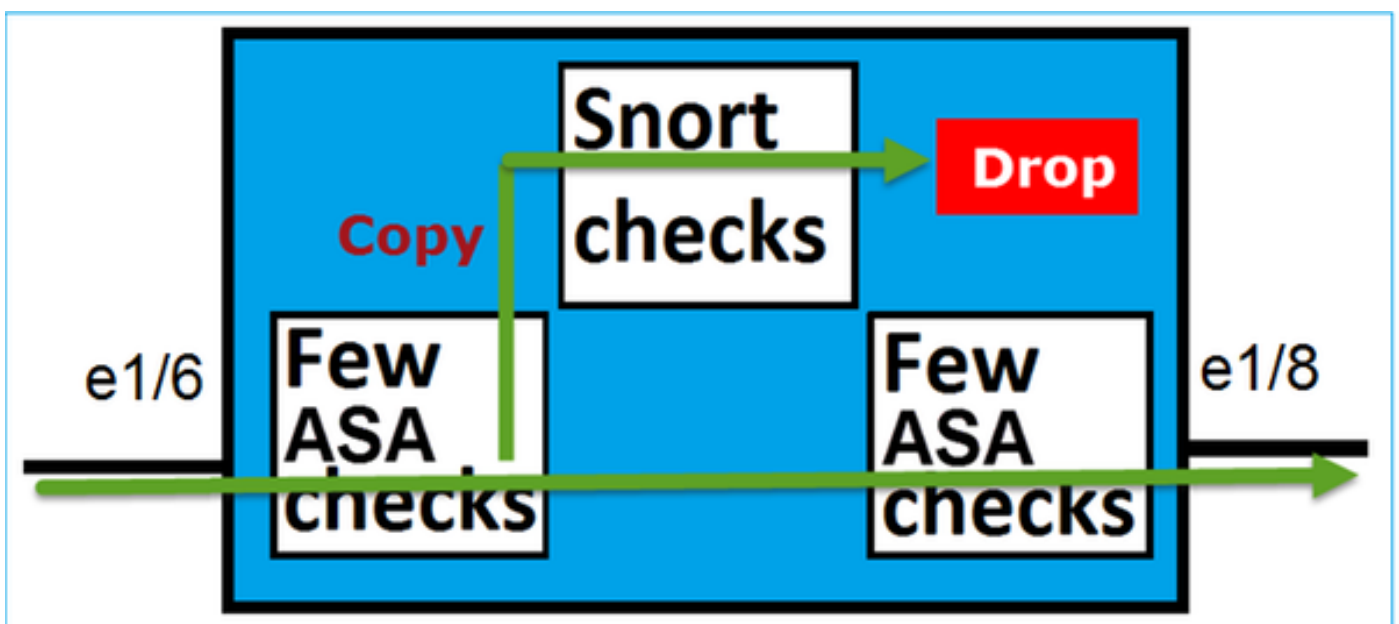
```
> show inline-set Inline-set Inline-Pair-1 Mtu is 1500 bytes Failsafe mode is on/activated
Failsecure mode is off Tap mode is on Propagate-link-state option is on hardware-bypass mode is
disabled Interface-Pair[1]: Interface: Ethernet1/6 "INSIDE" Current-Status: UP Interface:
Ethernet1/8 "OUTSIDE" Current-Status: UP Bridge Group ID: 0>
```

En vérifiant les paires intégrées FTD avec la prise reliez l'exécution

Théorie de base

- En configurant une paire intégrée avec des interfaces physiques de la prise 2 sont intérieurement jetés un pont sur
- Disponible dans des modes conduits ou transparents de déploiement
- La plupart de caractéristiques d'engine ASA (NAT, acheminement, L3/L4 ACL etc.) ne sont pas disponibles pour des écoulements allant par les paires intégrées
- Le trafic réel ne peut pas être abandonné
- Peu de contrôles d'engine ASA sont appliqués avec complètement reniflent des contrôles d'engine à une copie du trafic réel

Le dernier point peut être visualisé comme suit :



La paire intégrée avec le mode de prise ne relâche pas le trafic de transit. Traçant un paquet confirme ceci :

```
> show capture CAPI packet-number 2 trace3 packets captured 2: 13:34:30.685084 192.168.201.50.20
> 192.168.201.60.80: S 0:0(0) win 8192Phase: 1Type: CAPTURESubtype:Result:
ALLOWConfig:Additional Information:MAC Access listPhase: 2Type: ACCESS-LISTSubtype:Result:
ALLOWConfig:Implicit RuleAdditional Information:MAC Access listPhase: 3Type: NGIPS-MODESubtype:
ngips-modeResult: ALLOWConfig:Additional Information:The flow ingressed an interface configured
for NGIPS mode and NGIPS services will be appliedPhase: 4Type: ACCESS-LISTSubtype: logResult:
WOULD HAVE DROPPEDConfig:access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced deny ip
192.168.201.0 255.255.255.0 any rule-id 268441600 event-log flow-startaccess-list CSM_FW_ACL_
remark rule-id 268441600: ACCESS POLICY: FTD4100 - Mandatory/laccess-list CSM_FW_ACL_ remark
rule-id 268441600: L4 RULE: Rule 1Additional Information:Result:input-interface: INSIDEinput-
status: upinput-line-status: upAction: Access-list would have dropped,but packet forwarded due
to inline-tap1 packet shown
>
```

Comparaison : Paires intégrées contre des paires intégrées avec la prise

	Paires intégrées	Paires intégrées avec la prise
	>affichez l'en ligne-positionnement	> affichez l'en ligne-positionnement
affichez l'en ligne-positionnement	En ligne-positionnement Inline-Pair-1 Le mtu est de 1500 octets Le mode de sécurité est on/activated Le mode de Failsecure est éteint Le mode de prise est éteint l'option de Propagation-lien-état est allumée le mode de matériel-contournement est désactivé Interface-Pair[1] : Interface : Ethernet1/6 « INTÉRIEUR » Courant-état : VERS LE HAUT DE Interface : Ethernet1/8 « EXTÉRIEUR » Courant-état : VERS LE HAUT DE Identification groupe de passerelle : 509	En ligne-positionnement Inline-Pair-1 Le mtu est de 1500 octets Le mode de sécurité est on/activated Le mode de Failsecure est éteint Le mode de prise est allumé l'option de Propagation-lien-état est allumée le mode de matériel-contournement est désactivé Interface-Pair[1] : Interface : Ethernet1/6 « INTÉRIEUR » Courant-état : VERS LE HAUT DE Interface : Ethernet1/8 « EXTÉRIEUR » Courant-état : VERS LE HAUT DE Identification groupe de passerelle : 0
	>	>
	>affichez l'interface e1/6	>affichez l'interface e1/6
show interface	Reliez Ethernet1/6 « INTÉRIEUR », êtes, ligne protocole est Le matériel est EtherSVI, BW 1000 Mbits/s, usec DLY 1000 Adresse MAC 5897.bdb9.770e, MTU 1500 Mode interface IPS : en ligne , En ligne-positionnement : Inline-Pair-1 Adresse IP non affectée Statistiques de trafic pour le « INTÉRIEUR » : entrée de 3957 paquets, 264913 octets sortie de 144 paquets, 58664 octets 4 paquets relâchés 1 paquets minute du débit en entrée	Reliez Ethernet1/6 « INTÉRIEUR », êtes, protocole est Le matériel est EtherSVI, BW 1000 Mbits usec DLY 1000 Adresse MAC 5897.bdb9.770e, MTU 1500 Mode interface IPS : en ligne-prise , En ligne-positionnement : Inline-Pair-1 Adresse IP non affectée Statistiques de trafic pour le « INTÉRIEUR » : 24 entrées de paquets, 1378 octets 0 sorties de paquets, octets 0 24 paquets relâchés 1 paquets minute du débit en entrée

0/sec, 26 octets/sec
 1 paquets minute du débit sortant 0/sec, 7 octets/sec
 1 débit minute de baisse, 0 paquets/sec
 5 paquets minute du débit en entrée
 0/sec, 28 octets/sec
 5 paquets minute du débit sortant 0/sec, 9 octets/sec
 5 débits minute de baisse, 0 paquets/sec
> affichez l'interface e1/8
 Reliez Ethernet1/8 « EXTÉRIEUR », êtes, ligne protocole est
 Le matériel est EtherSVI, BW 1000 Mbits/s, usec DLY 1000
 Adresse MAC 5897.bdb9.774d, MTU 1500
 Mode interface IPS : **en ligne**, En ligne-positionnement : Inline-Pair-1
 Adresse IP non affectée
 Statistiques de trafic pour le « EXTÉRIEUR » :
 entrée de 144 paquets, 55634 octets
 sortie de 3954 paquets, 339987 octets
 paquets 0 relâchés
 1 paquets minute du débit en entrée
 0/sec, 7 octets/sec
 1 paquets minute du débit sortant 0/sec, 37 octets/sec
 1 débit minute de baisse, 0 paquets/sec
 5 paquets minute du débit en entrée
 0/sec, 8 octets/sec
 5 paquets minute du débit sortant 0/sec, 39 octets/sec
 5 débits minute de baisse, 0 paquets/sec
>
>suivi du paquet-nombre 1 du show capture CAPI

3 paquets capturés

1 : 16:12:55.785085 192.168.201.50.20 >
 192.168.201.60.80 : Victoire 8192 S 0:0(0) ACK
 0
 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

0/sec, 0 octets/sec
 1 paquets minute du débit sortant 0/sec, 0 octets/sec
 1 débit minute de baisse, 0 paquets/sec
 5 paquets minute du débit en entrée
 0/sec, 0 octets/sec
 5 paquets minute du débit sortant 0/sec, 0 octets/sec
 5 débits minute de baisse, 0 paquets/sec
> affichez l'interface e1/8
 Reliez Ethernet1/8 « EXTÉRIEUR », êtes, ligne protocole est
 Le matériel est EtherSVI, BW 1000 Mbits/s, usec DLY 1000
 Adresse MAC 5897.bdb9.774d, MTU 1500
 Mode interface IPS : **en ligne-prise**, En ligne-positionnement : Inline-Pair-1
 Adresse IP non affectée
 Statistiques de trafic pour le « EXTÉRIEUR » :
 Entrée de 1paquet, 441 octets
 0 sorties de paquets, octets 0
 1paquet relâchés
 1 paquets minute du débit en entrée
 0/sec, 0 octets/sec
 1 paquets minute du débit sortant 0/sec, 0 octets/sec
 1 débit minute de baisse, 0 paquets/sec
 5 paquets minute du débit en entrée
 0/sec, 0 octets/sec
 5 paquets minute du débit sortant 0/sec, 0 octets/sec
 5 débits minute de baisse, 0 paquets/sec
>
> suivi du paquet-nombre 1 du show capture CAPI

3 paquets capturés

1 : 16:56:02.631437 192.168.201.50.20 >
 192.168.201.60.80 : Victoire 8192 S 0:0(0) ACK
 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 :

Traitement
 des paquets
 avec la règle
 de **bloc**

Config :
Règle implicite
Les informations complémentaires :
Liste d'accès de MAC

Phase : 3
Type : NGIPS-MODE
Sous-type : ngips-mode
Résultat : LAISSEZ
Config :
Les informations complémentaires :
L'écoulement ingressé une interface
configurée pour le mode NGIPS et les services
NGIPS seront appliqués

Phase : 4
Type : LISTE D'ACCÈS
Sous-type : log
Résultat : BAISSÉ
Config :
access-group CSM_FW_ACL_ global
la liste d'accès CSM_FW_ACL_ avancée
refusent à IP 192.168.201.0 255.255.255.0
n'importe quel écoulement-commencement
d'event-log du règle-id 268441600
règle-id 268441600 de remarque de la liste
d'accès CSM_FW_ACL_ : STRATÉGIE
D'ACCESS : FTD4100 - Mandatory/1
règle-id 268441600 de remarque de la liste
d'accès CSM_FW_ACL_ : RÈGLE L4 : Règle 1
Les informations complémentaires :

Résultat :
interface d'entrée : À L'INTÉRIEUR
entrée-état : vers le haut de
entrée-ligne-état : vers le haut de
Action : baisse
Baisse-raison : l'écoulement (d'acl-baisse) est
refusé par règle configurée

1paquet affiché
>

Règle implicite
Les informations complémentaires :
Liste d'accès de MAC

Phase : 3
Type : NGIPS-MODE
Sous-type : ngips-mode
Résultat : LAISSEZ
Config :
Les informations complémentaires :
L'écoulement ingressé une interface
configurée pour le mode NGIPS et les ser
NGIPS seront appliqués

Phase : 4
Type : LISTE D'ACCÈS
Sous-type : log
Résultat : AURAIT RELÂCHÉ
Config :
access-group CSM_FW_ACL_ global
la liste d'accès CSM_FW_ACL_ avancée
refusent à IP 192.168.201.0 255.255.255.0
n'importe quel écoulement-commencemen
d'event-log du règle-id 268441600
règle-id 268441600 de remarque de la list
d'accès CSM_FW_ACL_ : STRATÉGIE
D'ACCESS : FTD4100 - Mandatory/1
règle-id 268441600 de remarque de la list
d'accès CSM_FW_ACL_ : RÈGLE L4 : Rè
Les informations complémentaires :

Résultat :
interface d'entrée : À L'INTÉRIEUR
entrée-état : vers le haut de
entrée-ligne-état : vers le haut de
Action : La liste d'accès aurait chuté, mais
paquet a expédié l'en ligne-prise due

1paquet affiché
>

Résumé

- En utilisant le mode intégré de paires le paquet passe principalement par le FTD reniflent l'engine.
- Des connexions TCP sont manipulées en mode d'état-contournement de TCP
- D'un point de vue d'engine FTD ASA une stratégie d'ACL est appliquée
- Quand le mode intégré de paires est en service des paquets peuvent être bloqués puisqu'ils sont sur place traité
- Quand le mode de prise est activé une copie du paquet est examinée et abandonnée intérieurement tandis que le trafic réel passe par FTD non modifié

Documents connexes

[Puissance de feu NGFW de Cisco](#)