

Configurer des interfaces de défense contre des menaces de FirePOWER en mode conduit

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurez](#)

[Diagramme du réseau](#)

[Configurez une interface conduite et une sous-interface](#)

[Étape 1. Configurez l'interface logique](#)

[Étape 2. Configurez l'interface physique](#)

[Exécution d'interface conduite par FTD](#)

[Aperçu d'interface conduit par FTD](#)

[Vérifiez](#)

[Tracez un paquet sur l'interface conduite par FTD](#)

[Informations connexes](#)

Introduction

Ce document décrit la configuration, vérification et le traitement de fond d'une paire intégrée reliant sur une appliance de la défense contre des menaces de FirePOWER (FTD).

Conditions préalables

Conditions requises

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

[Composants utilisés](#)

- ASA5512-X exécutant le code 6.1.0.x FTD
- Centre de Gestion de FirePOWER (FMC) exécutant 6.1.0.x

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

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

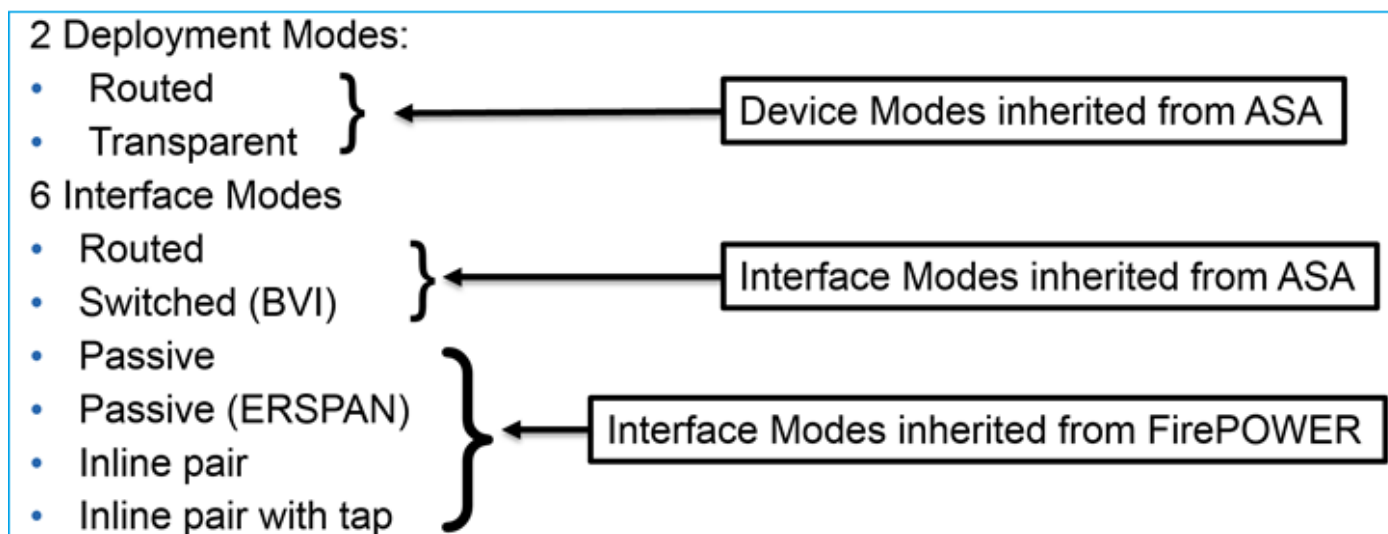
Produits connexes

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), services Web d'Amazon (AWS), clavier/vidéo/souris (KVM)
- Code logiciel 6.2.x FTD et plus tard.

Informations générales

FTD fournit deux modes de déploiement et six modes interface suivant les indications de l'image suivante :



Note: Vous pouvez mélanger des modes interface sur une appliance simple FTD.

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 engine de LINA et contrôles de Renifler-engine	Oui
Commuté	Transparent	Pleins engine de LINA et contrôles de Renifler-engine	Oui
Paires intégrées	Conduit ou	Engine partielle de LINA et pleins	Oui

Paires intégrées avec la prise	transparent Conduit ou transparent	contrôles de Renifler-engine Engine partielle de LINA et pleins contrôles de Renifler-engine	Non
Passif	Conduit ou transparent	Engine partielle de LINA et pleins contrôles de Renifler-engine	Non
Passif (ERSPAN)	Conduit	Engine partielle de LINA et pleins contrôles de Renifler-engine	Non

Configurez

[Diagramme du réseau](#)



Configurez une interface conduite et une sous-interface

Configurez la sous-interface G0/0.201 et l'interface G0/1 selon des conditions requises suivantes :

Interface	G0/0.201	G0/1
Nom	À L'INTÉRIEUR	DEHORS
Zone de Sécurité	INSIDE_ZONE	OUTSIDE_ZONE
Description	INTERNE	EXTERNE
Sous ID d'interface	201	-
ID de VLAN	201	-
Ipv4	192.168.201.1/24	192.168.202.1/24
Duplex/vitesse	Automatique	Automatique

Solution

Étape 1. Configurez l'interface logique

Naviguez vers les **périphériques** > la **Gestion de périphériques**, sélectionnez le périphérique approprié et sélectionnez l'icône d'éditer :

Overview Analysis Policies Devices Objects AMP				
Device Management NAT VPN QoS Platform Settings				
Name	Group	Model	License Type	Access Control Policy
Ungrouped (8)				
FTD5512 10.62.148.10 - Cisco ASA5512-X Threat Defense		Cisco ASA5512-X Threat Defense	Base, Threat, Malware, URL Filtering	FTD5512

Choisi ajoutez les interfaces > l'interface de sous-titre :

Overview Analysis Policies Devices Objects AMP						
Device Management NAT VPN QoS Platform Settings						
FTD5512						
Cisco ASA5512-X Threat Defense						
Devices Routing Interfaces Inline Sets DHCP						
St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0		Physical			
	GigabitEthernet0/1		Physical			

Configurez les configurations de sous-interface selon des conditions requises :

Add Sub Interface

Name: Enabled Management Only

Security Zone: ▼

Description:

General IPv4 IPv6 Advanced

MTU: (64 - 9198)

Interface *: ▼ Enabled

Sub-Interface ID *: (1 - 4294967295)

VLAN ID: (1 - 4094)

Paramètres IP d'interface :

Add Sub Interface

Name:	<input type="text" value="INSIDE"/>	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Management Only
Security Zone:	<input type="text" value="INSIDE_ZONE"/>		
Description:	<input type="text" value="INTERNAL"/>		
General IPv4 IPv6 Advanced			
IP Type:	<input type="text" value="Use Static IP"/>		
IP Address:	<input type="text" value="192.168.201.1/24"/>	eg. 1.1.1.1/255.255.255.228	

Sous l'interface physique (GigabitEthernet0/0) spécifiez le duplex et les configurations de débit :

General IPv4 IPv6 Advanced Hardware Configuration			
Duplex:	<input type="text" value="auto"/>		
Speed:	<input type="text" value="auto"/>		

Activez l'interface physique (G0/0 dans ce cas) :

Edit Physical Interface				
Mode:	<input type="text" value="None"/>			
Name:	<input type="text"/>	<input checked="" type="checkbox"/> Enabled	<input type="checkbox"/> Management Only	
Security Zone:	<input type="text"/>			
Description:	<input type="text"/>			
General IPv4 IPv6 Advanced Hardware Configuration				
MTU:	<input type="text" value="1500"/>	(64 - 9198)		
Interface ID:	<input type="text" value="GigabitEthernet0/0"/>			

Étape 2. Configurez l'interface physique

Éditez l'interface physique GigabitEthernet0/1 selon des conditions requises :

Edit Physical Interface

Mode: ▼

Name: Enabled Management Only

Security Zone: ▼

Description:

General **IPv4** IPv6 Advanced Hardware Configuration

IP Type: ▼

IP Address: eg. 1.1.1.1/255.255.255.228

- Pour l'interface conduite le mode est : **Aucun**
- Le nom est équivalent au **nameif d'interface ASA**
- Sur FTD toutes les interfaces ont le niveau de Sécurité = 0
- **le même-Sécurité-traffic** s'applique pas applicable sur FTD. On permet le trafic entre les interfaces FTD (inter) et le hairpinning (intra) par défaut

Sélectionnez la **sauvegarde** et **déployez-vous**.

Vérification

Du GUI FMC :

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
●	GigabitEthernet0/0		Physical			
●	GigabitEthernet0/1	OUTSIDE	Physical	OUTSIDE_ZONE		192.168.202.1/24(Static)
●	GigabitEthernet0/2		Physical			
●	GigabitEthernet0/3		Physical			
●	GigabitEthernet0/4		Physical			
●	GigabitEthernet0/5		Physical			
●	Diagnostic0/0		Physical			
●	GigabitEthernet0/0.201	INSIDE	SubInterf...	INSIDE_ZONE		192.168.201.1/24(Static)

Du FTD CLI :

> **show interface ip brief**

Interface	IP-Address	OK?	Method	Status	Protocol
GigabitEthernet0/0	unassigned	YES	unset	up	up
GigabitEthernet0/0.201	192.168.201.1	YES	manual	up	up
GigabitEthernet0/1	192.168.202.1	YES	manual	up	up
GigabitEthernet0/2	unassigned	YES	unset	administratively down	down
GigabitEthernet0/3	unassigned	YES	unset	administratively down	down
GigabitEthernet0/4	unassigned	YES	unset	administratively down	down
GigabitEthernet0/5	unassigned	YES	unset	administratively down	down
Internal-Contro0/0	127.0.1.1	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
Management0/0	unassigned	YES	unset	up	up

> **show ip**

System IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

Current IP Addresses:

Interface	Name	IP address	Subnet mask	Method
GigabitEthernet0/0.201	INSIDE	192.168.201.1	255.255.255.0	manual
GigabitEthernet0/1	OUTSIDE	192.168.202.1	255.255.255.0	manual

Corrélation GUI et FTD CLI FMC :

The screenshot shows the GUI configuration for the sub-interface GigabitEthernet0/0.201. The 'Name' field is 'INSIDE', 'Security Zone' is 'INSIDE_ZONE', and 'Description' is 'INTERNAL'. Under the 'IPv4' tab, 'IP Type' is 'Use Static IP' and 'IP Address' is '192.168.201.1/24'. The terminal window on the right shows the CLI configuration for the same interface, with arrows pointing from the GUI fields to the corresponding CLI lines.

```

> show running-config interface g0/0.201
!
interface GigabitEthernet0/0.201
description INTERNAL
vlan 201
nameif INSIDE
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.201.1 255.255.255.0

```

> **show interface g0/0.201**

Interface GigabitEthernet0/0.201 "INSIDE", is up, line protocol is up

Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

VLAN identifier 201

Description: INTERNAL

MAC address a89d.21ce.fdea, MTU 1500

IP address 192.168.201.1, subnet mask 255.255.255.0

Traffic Statistics for "INSIDE":

1 packets input, 28 bytes

1 packets output, 28 bytes

0 packets dropped

> **show interface g0/1**

Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up

Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)

Input flow control is unsupported, output flow control is off

Description: EXTERNAL

MAC address a89d.21ce.fde7, MTU 1500

IP address 192.168.202.1, subnet mask 255.255.255.0

0 packets input, 0 bytes, 0 no buffer

Received 0 broadcasts, 0 runts, 0 giants

0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort

0 pause input, 0 resume input

0 L2 decode drops

1 packets output, 64 bytes, 0 underruns

0 pause output, 0 resume output

0 output errors, 0 collisions, 12 interface resets

0 late collisions, 0 deferred

0 input reset drops, 0 output reset drops

input queue (blocks free curr/low): hardware (511/511)

output queue (blocks free curr/low): hardware (511/511)

Traffic Statistics for "OUTSIDE":

0 packets input, 0 bytes

0 packets output, 0 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, 0 bytes/sec

5 minute output rate 0 pkts/sec, 0 bytes/sec

5 minute drop rate, 0 pkts/sec

>

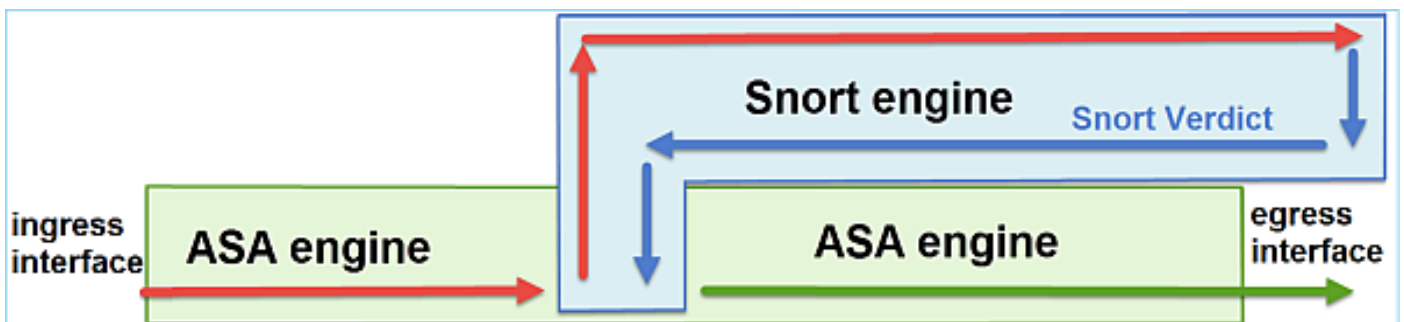
Exécution d'interface conduite par FTD

Vérifiez le traitement de paquets FTD quand les interfaces conduites sont en service.

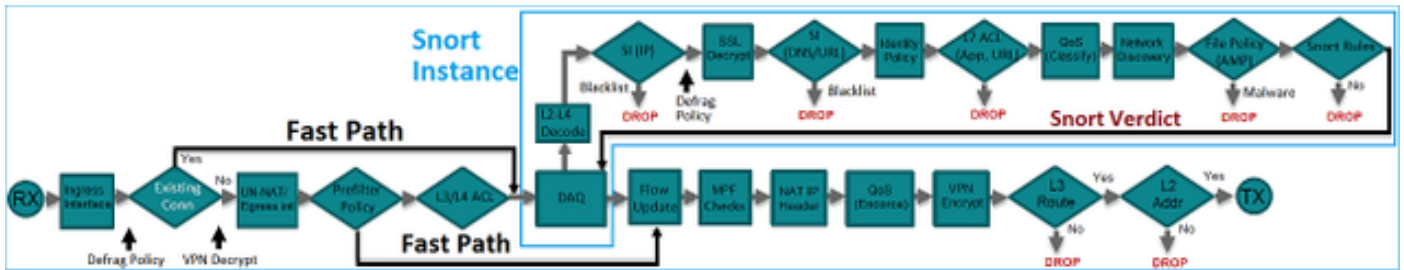
Solution

Aperçu architectural FTD

Une vue d'ensemble à niveau élevé du plan de données FTD :



L'image suivante affiche certains des contrôles qui se produisent dans chaque engine :



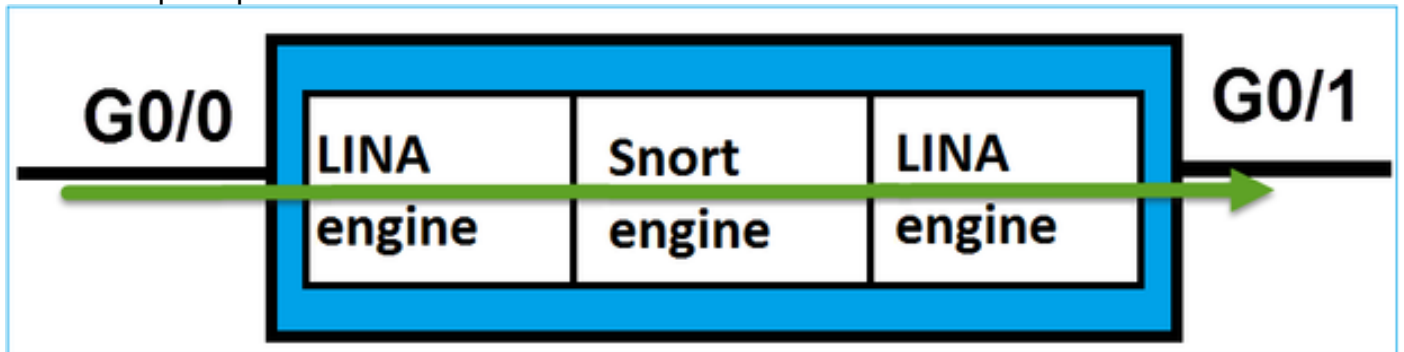
Points clé

- Les contrôles inférieurs correspondent au chemin de données d'engine FTD LINA
- Les contrôles à l'intérieur de la case bleue correspondent au FTD reniflent l'exemple d'engine

Aperçu d'interface conduit par FTD

- Disponible seulement dans le déploiement **conduit**
- **Déploiement** traditionnel du **Pare-feu L3**
- Un ou plusieurs (VLAN) interfaces routable physiques ou logiques
- Permet des caractéristiques comme NAT ou des protocoles de routage dynamique à configurer
- Des paquets sont expédiés basés sur la **recherche de route** et le prochain saut est résolu a basé sur la **consultation d'ARP**
- Le trafic réel **peut être abandonné**
- **Les pleins** contrôles d'engine de LINA sont appliqués avec **complètement reniflent des** contrôles d'engine

Le dernier point peut être visualisé comme suit :



Vérifiez

Tracez un paquet sur l'interface conduite par FTD

[Diagramme du réseau](#)



Utilisez le traceur de paquets avec les paramètres suivants pour voir les stratégies appliquées :

Interface d'entrée	À L'INTÉRIEU
Protocol/service	R
Source ip	Port TCP 80
IP de destination	192.168.201.100
	00
	192.168.202.100
	00

Solution

Quand une interface conduite est utilisée le paquet est traité d'une manière semblable à une interface conduite par ASA classique. Les contrôles comme la recherche de route, la consultation modulaire etc. du cadre de stratégie (MPF), NAT, de l'ARP ont lieu dans le chemin de données d'engine de LINA. Supplémentaire, si la stratégie de contrôle d'accès exige ainsi, le paquet est examiné par l'engine de renifler (un des exemples de renifler) où un verdict (liste noire, Whitelist) est généré et retourné de nouveau à l'engine de LINA :

```
> packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80
```

Phase: 1

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface

Result: ALLOW

Config:

Additional Information:

found next-hop 192.168.202.100 using egress ifc OUTSIDE

Phase: 2

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 268437505

access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 -

Defau

1t/1

access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE

Additional Information:

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

wil

l be reached

Phase: 3

Type: CONN-SETTINGS

Subtype:

Result: ALLOW

Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 6

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 7

Type: IP-OPTIONS

Subtype:

Result: ALLOW

Config:

Additional Information:

Phase: 8

Type: FLOW-CREATION

Subtype:

Result: ALLOW

Config:

Additional Information:

New flow created with id 11336, packet dispatched to next module

Result:

input-interface: INSIDE

input-status: up

input-line-status: up

output-interface: OUTSIDE

output-status: up

output-line-status: up

Action: allow

>

Note: Dans la phase 4 le paquet est vérifié contre une carte de TCP appelée l'UM_STATIC_TCP_MAP. C'est la carte par défaut de TCP sur FTD.

```
firepower# show run all tcp-map
!  
tcp-map UM_STATIC_TCP_MAP  
no check-retransmission  
no checksum-verification  
exceed-mss allow  
queue-limit 0 timeout 4  
reserved-bits allow  
syn-data allow  
synack-data drop  
invalid-ack drop  
seq-past-window drop  
tcp-options range 6 7 allow  
tcp-options range 9 18 allow  
tcp-options range 20 255 allow  
tcp-options selective-ack allow  
tcp-options timestamp allow  
tcp-options window-scale allow  
tcp-options mss allow  
tcp-options md5 clear  
ttl-evasion-protection  
urgent-flag allow  
window-variation allow-connection  
!  
>
```

Informations connexes

- [Guide de configuration de défense contre des menaces de Cisco FirePOWER pour le gestionnaire de périphérique de FirePOWER, version 6.1](#)
- [Installant et améliorant la défense contre des menaces de FirePOWER sur des périphériques ASA 55xx-X](#)
- [Fonctionner avec les captures et le traceur de paquets de la défense contre des menaces de FirePOWER \(FTD\)](#)
- [Support et documentation techniques - Cisco Systems](#)