

# Configuration des interfaces Firepower Threat Defense en mode routé

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Produits connexes](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurer une interface routée et une sous-interface](#)

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

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

[Fonctionnement de l'interface routée FTD](#)

[Présentation de l'interface routée FTD](#)

[Vérifier](#)

[Suivre un paquet sur l'interface routée FTD](#)

[Informations connexes](#)

---

## Introduction

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

## Conditions préalables

### Exigences

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 :

- ASA5512-X - code FTD 6.1.0.x
- Firepower Management Center (FMC) - code 6.1.0.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.

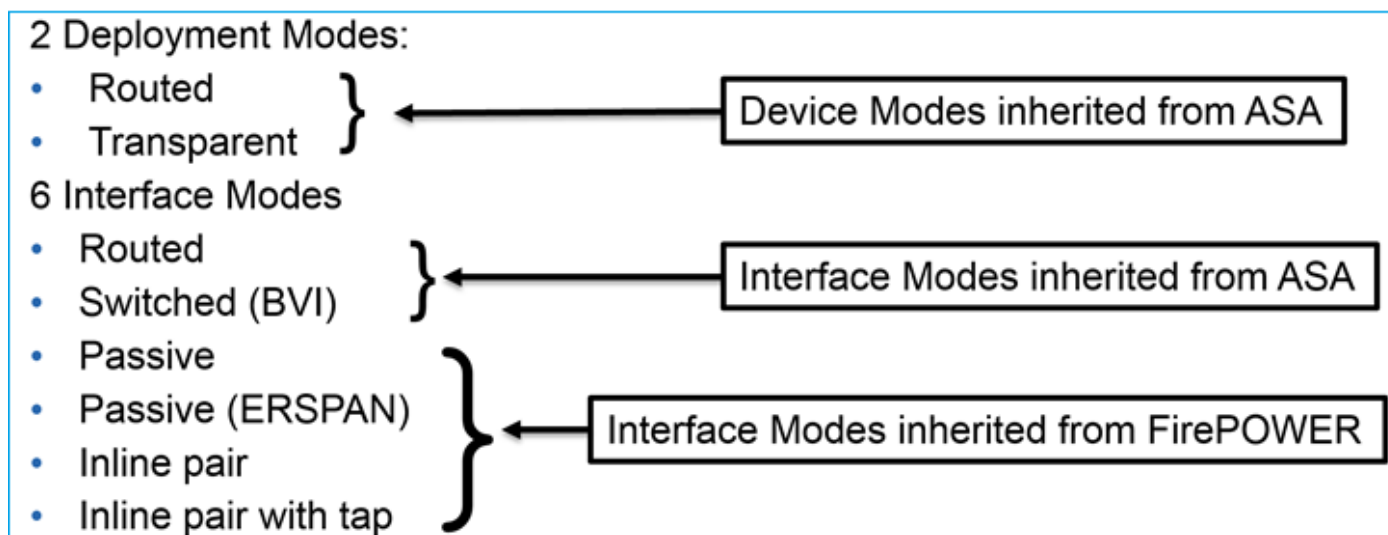
## Produits connexes


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

Le pare-feu Firepower Threat Defense (FTD) propose deux modes de déploiement et six modes d'interface, comme illustré dans cette image :



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

Présentation générale des différents modes de déploiement et d'interface FTD :

interface FTD mode	Mode de déploiement	Description	Le trafic peut être abandonné

	FTD		
Routés	Routés	Vérifications complètes du moteur LINA et du moteur Snort	Oui
Commuté	Transparent	Vérifications complètes du moteur LINA et du moteur Snort	Oui
Paire en ligne	Routé ou transparent	Moteur LINA partiel et contrôles Snort complets	Oui
Paire en ligne avec robinet	Routé ou transparent	Moteur LINA partiel et contrôles Snort complets	Non
Passif	Routé ou transparent	Moteur LINA partiel et contrôles Snort complets	Non
Passif (ERSPAN)	Routés	Moteur LINA partiel et contrôles Snort complets	Non

## Configurer

### Diagramme du réseau



### Configurer une interface routée et une sous-interface

Configurez la sous-interface G0/0.201 et l'interface G0/1 conformément à ces exigences :

Interface	G0/0,201	G0/1
-----------	----------	------

Nom	INTÉRIEUR	EXTÉRIEUR
Zone de sécurité	ZONE_INTERNE	ZONE_EXTERNE
Description	INTÉRIEUR	EXTERNE
ID de sous-interface	201	-
ID de VLAN	201	-
IPv4	Commutateurs 192.168.201.1/24	Commutateurs 192.168.202.1/24
Duplex/Vitesse	« Auto »	« Auto »

## Solution

### Étape 1. Configuration de l'interface logique

Accédez à Périphériques > Gestion des périphériques, sélectionnez le périphérique approprié et cliquez sur l'icône Modifier :

The screenshot shows the 'Devices' management page. The table below is a representation of the data shown:

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

Sélectionnez Add Interfaces > Sub Interface :

The screenshot shows the configuration page for the device 'FTD5512'. The 'Interfaces' tab is selected, and the 'Add Interfaces' dropdown menu is open, showing the following options:

- Sub Interface
- Redundant Interface
- Ether Channel Interface

The 'Sub Interface' option is highlighted with an orange box.

Configurez les paramètres de la sous-interface conformément aux exigences :

## 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 de l'interface :

## Add Sub Interface

Name:   Enabled  Management Only

Security Zone:  ▼

Description:

General

**IPv4**

IPv6

Advanced

IP Type:  ▼

IP Address:  eg. 1.1.1.1/255.255.255.228

Sous l'interface physique (GigabitEthernet0/0), spécifiez les paramètres Duplex et Speed (Vitesse) :

General IPv4 IPv6 Advanced **Hardware Configuration**

Duplex: auto

Speed: auto

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

### Edit Physical Interface

Mode: None

Name:  Enabled  Management Only

Security Zone:

Description:

General IPv4 IPv6 Advanced Hardware Configuration

MTU: 1500 (64 - 9198)

Interface ID: GigabitEthernet0/0

Étape 2. Configuration de l'interface physique

Modifiez l'interface physique GigabitEthernet0/1 conformément aux spécifications :

## 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 routée, le mode est : None
- Le nom est équivalent au nom de l'interface ASA si
- Sur FTD, toutes les interfaces ont un niveau de sécurité = 0
- same-security-traffic n'est pas applicable sur FTD. Le trafic entre les interfaces FTD (inter) et (intra) est autorisé par défaut

Sélectionnez Enregistrer et déployer.

## Vérification

Dans l'interface utilisateur 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)

À partir de la CLI FTD :

<#root>

>

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-Control0/0	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

<#root>

>

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 entre interface utilisateur graphique FMC et CLI FTD :

The image shows a correlation between the FMC GUI and the CLI. On the left, the 'Edit Sub Interface' GUI for 'INSIDE' is shown with the 'IPv4' tab selected. The 'Name' field is 'INSIDE', 'Security Zone' is 'INSIDE\_ZONE', and 'Description' is 'INTERNAL'. The 'IP Type' is 'Use Static IP' and the 'IP Address' is '192.168.201.1/24'. On the right, the CLI output for 'show running-config interface g0/0.201' is shown, with arrows pointing from the GUI fields to the corresponding CLI lines: 'INSIDE' points to 'nameif INSIDE', 'INSIDE\_ZONE' points to 'description INTERNAL', and '192.168.201.1/24' points to 'ip address 192.168.201.1 255.255.255.0'.

<#root>

>



```
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

>

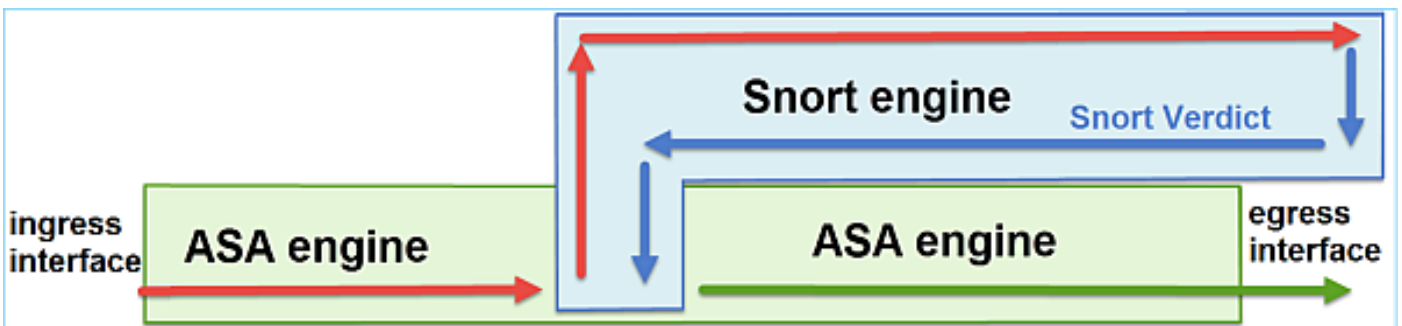
## Fonctionnement de l'interface routée FTD

Vérifiez le flux de paquets FTD lorsque des interfaces routées sont utilisées.

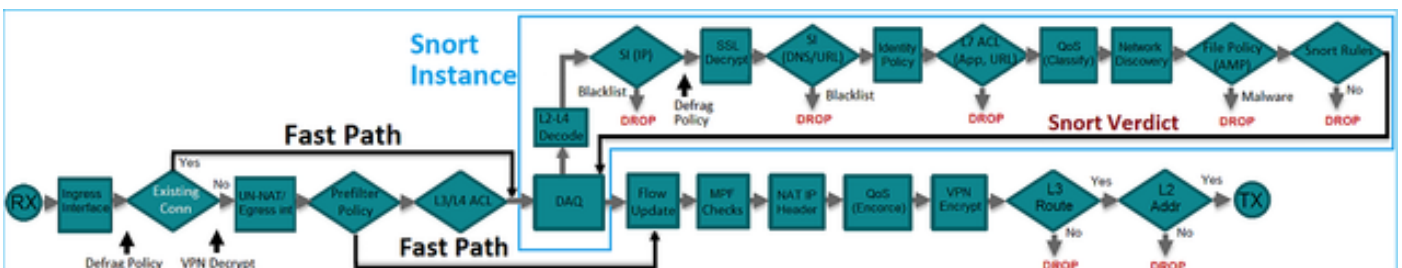
Solution

Présentation de FTD Architectural

Présentation générale du plan de données FTD :



Cette image montre quelques-unes des vérifications qui se produisent dans chaque moteur :



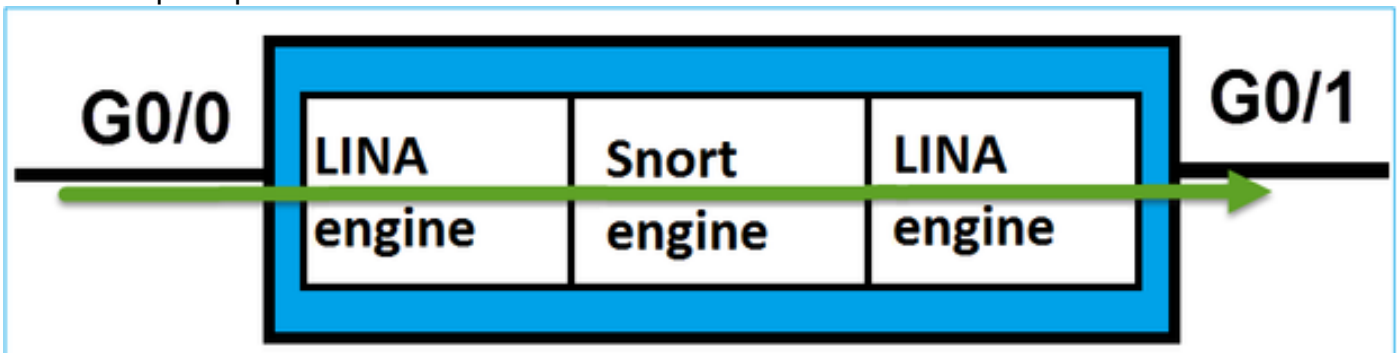
Points clés

- Les vérifications du bas correspondent au chemin de données du moteur FTD LINA
- Les vérifications dans la zone bleue correspondent à l'instance du moteur FTD Snort

## Présentation de l'interface routée FTD

- Disponible uniquement dans le déploiement routé
- Déploiement traditionnel de pare-feu C3
- Une ou plusieurs interfaces routables physiques ou logiques (VLAN)
- Permet de configurer des fonctionnalités telles que les protocoles NAT ou de routage dynamique
- Les paquets sont transférés en fonction de la recherche de route et le tronçon suivant est résolu en fonction de la recherche ARP
- Trafic réel peut être abandonné
- Les vérifications complètes du moteur LINA sont appliquées avec les vérifications complètes du moteur Snort

Le dernier point peut être visualisé comme suit :



## Vérifier

Suivre un paquet sur l'interface routée FTD

Diagramme du réseau



Utilisez packet-tracer avec les paramètres suivants pour voir les politiques appliquées :

Interface d'entrée	INTÉRIEUR
Protocole/Service	Port TCP 80
Adresse IP source	192.168.201.100
Adresse IP de destination	192.168.202.100

## Solution

Lorsqu'une interface routée est utilisée, le paquet est traité de la même manière qu'une interface routée ASA classique. Des vérifications telles que la recherche de route, MPF (Modular Policy Framework), NAT, la recherche ARP, etc., ont lieu dans le chemin de données du moteur LINA. De plus, si la politique de contrôle d'accès l'exige, le paquet est inspecté par le moteur Snort (l'une des instances Snort) où un verdict est généré et renvoyé au moteur LINA :

<#root>

```
>  
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 - Default/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 will 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

>



Remarque : au cours de la phase 4, le paquet est comparé à une carte TCP appelée UM\_STATIC\_TCP\_MAP. Il s'agit du mappage TCP par défaut sur FTD.

---

<#root>

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 Cisco Firepower Threat Defense pour Firepower Device Manager, version 6.1](#)
- [Installation et mise à niveau de Firepower Threat Defense sur les périphériques ASA 55xx-X](#)
- [Cisco Secure Firewall Threat Defense](#)
- [Assistance technique de Cisco et téléchargements](#)

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.