

Configuration des interfaces FDM en mode Paire en ligne

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Directives et restrictions](#)

[Avant de commencer](#)

[Détails du mode en ligne](#)

[Diagramme de réseau à définition en ligne](#)

[Configurer le jeu en ligne](#)

[Modifier ou supprimer un jeu en ligne](#)

Introduction

Ce document décrit les jeux en ligne pour FDM ajoutés dans Cisco Secure Firewall 7.4.1.

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur ces sujets :

- Concepts et configuration de FDM
- S'applique aux FTD sur les plates-formes des gammes 1000, 2100 et 3100 gérées par FDM

Composants utilisés

Les informations de ce document sont basées sur FDM 7.4.2.

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.

Informations générales

Un ensemble en ligne fournit une interface IPS uniquement. Vous pouvez mettre en oeuvre des interfaces IPS uniquement si vous disposez d'un pare-feu distinct protégeant ces interfaces et que

vous ne souhaitez pas la surcharge des fonctions de pare-feu.

Un ensemble en ligne agit comme une bosse sur le fil, en reliant deux interfaces pour les insérer dans un réseau existant. Cette fonction permet d'installer le périphérique dans n'importe quel environnement réseau sans avoir à configurer des périphériques réseau adjacents. Les interfaces en ligne reçoivent tout le trafic de manière inconditionnelle, mais tout le trafic reçu sur ces interfaces est retransmis à partir d'un ensemble en ligne sauf s'il est explicitement abandonné.

Directives et restrictions

- Vous pouvez configurer des jeux en ligne sur ces modèles de périphériques uniquement : Gamme Firepower 1000, Firepower 2100, Pare-feu sécurisé 3100.
- Types d'interface autorisés dans un ensemble en ligne : physique, EtherChannel.
- Vous ne pouvez pas inclure l'interface de gestion dans un jeu en ligne.
- Vous ne pouvez pas modifier les attributs des interfaces utilisées dans un jeu en ligne : nom, mode, ID d'interface, MTU, adresse IP.
- Si vous activez le mode Tap, l'option Snort Fail Open est désactivée.
- Les paquets d'écho BFD (Bidirectional Forwarding Detection) ne sont pas autorisés à traverser le périphérique lors de l'utilisation d'ensembles en ligne. S'il y a deux voisins de part et d'autre du périphérique exécutant BFD, le périphérique abandonne les paquets d'écho BFD car ils ont les mêmes adresses IP source et de destination et semblent faire partie d'une attaque LAND.
- Pour les ensembles en ligne et les interfaces passives, le périphérique prend en charge jusqu'à deux en-têtes 802.1Q dans un paquet (également appelé prise en charge Q-in-Q).



Remarque : Les interfaces de type pare-feu ne prennent pas en charge Q-in-Q et ne prennent en charge qu'un en-tête 802.1Q.

- Les interfaces d'un ensemble en ligne ne prennent pas en charge le routage, la NAT, le protocole DHCP (serveur, client ou relais), le VPN, l'interception TCP, l'inspection d'application ou Netflow.

Avant de commencer

- Il est recommandé de configurer STP PortFast pour les commutateurs compatibles STP qui se connectent aux interfaces de paire en ligne de défense contre les menaces.
- Configurez les interfaces physiques ou EtherChannel qui peuvent être membres de l'ensemble en ligne. Vous ne pouvez configurer que ces valeurs : Nom, duplex, vitesse et mode routé (ne sélectionnez pas passif). Ne configurez aucun type d'adressage, c'est-à-dire des adresses IP manuelles, DHCP ou PPPoE.

Détails du mode en ligne

- Cette fonction vous permet d'utiliser des jeux en ligne. Cela permet l'inspection du trafic sans allocation IP.
- Le mode en ligne est disponible pour les interfaces physiques, les EtherChannels et les zones de sécurité.
- Le mode en ligne est automatiquement défini pour les interfaces et les EtherChannels lorsqu'ils sont utilisés dans une paire en ligne.
- Le mode en ligne empêche les modifications apportées aux interfaces et aux EtherChannels concernés jusqu'à ce qu'ils soient supprimés de la paire en ligne.
- Les interfaces qui sont en mode Inline peuvent être associées à des zones de sécurité définies en mode Inline.

Diagramme de réseau à définition en ligne

Le trafic circule de Router1 vers Router2 via les interfaces A et B en utilisant uniquement une connexion physique.



Diagramme du réseau

Configurer le jeu en ligne

- Dans le tableau de bord FDM, accédez à Interfaces card.

Firewall Device Manager

Monitoring Policies Objects **Device: firepower**

Model: Cisco Firepower 2120 Threat Defense | Software: 7.4.2-172 | VDB: 376.0 | Intrusion Rule Update: 20231011-1536 | Cloud Services: Not Registered | Register | High Availability: Not Configured

Interfaces
Management: Merged
Enabled 3 of 17
[View All Interfaces](#)

Routing
There are no static routes yet
[View Configuration](#)

Updates
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds
[View Configuration](#)

System Settings
[Management Access](#)
[Logging Settings](#)
[DHCP Server / Relay](#)
[DDNS Service](#)

Onglet Interface

- Pour activer les interfaces, cliquez sur l'icône Status de l'interface.

Device Summary

Interfaces

Interfaces | EtherChannels | Virtual Tunnel Interfaces | Inline Sets

17 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ Ethernet1/1	outside	<input checked="" type="checkbox"/>	Routed			Enabled	
> ✓ Ethernet1/2	inside	<input checked="" type="checkbox"/>	Routed	192.168.95.1		Enabled	
> ○ Ethernet1/3		<input type="checkbox"/>	Routed			Enabled	
> ○ Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	

icône d'état

Device Summary

Interfaces



Interfaces | EtherChannels | Virtual Tunnel Interfaces | Inline Sets

17 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ Ethernet1/1	outside	<input checked="" type="checkbox"/>	Routed			Enabled	
> ✓ Ethernet1/2	inside	<input checked="" type="checkbox"/>	Routed	192.168.95.1		Enabled	
> ✓ Ethernet1/3		<input checked="" type="checkbox"/>	Routed			Enabled	

Activer l'interface

- Pour modifier les interfaces, cliquez sur l'icône Edit (crayon) pour l'interface.

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ Ethernet1/1	outside	<input checked="" type="checkbox"/>	Routed			Enabled	
> ✓ Ethernet1/2	inside	<input checked="" type="checkbox"/>	Routed	192.168.95.1 <small>Static</small>		Enabled	
> ✓ Ethernet1/3		<input checked="" type="checkbox"/>	Routed			Enabled	
> ○ Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	

Modifier l'interface

- Saisissez le nom de l'interface et sélectionnez le mode Routed. Ne configurez aucune adresse IP.

Ethernet1/3

Edit Physical Interface



Interface Name

Inline

Mode

Routed

Status



Most features work with named interfaces only, although some require unnamed interfaces.

Description

IPv4 Address IPv6 Address Advanced

Type

Static

IP Address and Subnet Mask

 /

e.g. 192.168.5.15/17 or 192.168.5.15/255.255.128.0

Standby IP Address and Subnet Mask

 /

Modifier l'interface

- Pour créer un jeu en ligne, accédez à l'onglet Jeux en ligne.

Device Summary

Interfaces

Cisco Firepower 2120 Threat Defense

Interfaces EtherChannels Virtual Tunnel Interfaces **Inline Sets**

17 Interfaces

Filter

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ Ethernet1/1	outside	<input checked="" type="checkbox"/>	Routed			Enabled	
> ✓ Ethernet1/2	inside	<input checked="" type="checkbox"/>	Routed	192.168.95.1 <small>Static</small>		Enabled	
> ✓ Ethernet1/3	inline	<input checked="" type="checkbox"/>	Routed			Enabled	
> ○ Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	

Créer un jeu en ligne

Pour ajouter un jeu en ligne, cliquez sur Ajouter (icône +).

The screenshot shows the 'Device Summary' for a Cisco Firepower 2120 Threat Defense. Under the 'Interfaces' section, there are tabs for 'Interfaces', 'EtherChannels', 'Virtual Tunnel Interfaces', and 'Inline Sets'. The 'Inline Sets' tab is active. A filter bar is visible with a '+' icon highlighted in a red box. Below the filter bar is a table with columns: NAME, MODE, MTU, INTERFACE PAIRS, and ACTIONS. The table is empty, and a message states: 'There are no Inline Sets yet. Start by creating the first Inline Set.' with a 'CREATE INLINE SET' button below it.

Ajouter un jeu en ligne

- Définissez un nom pour l'ensemble en ligne.
- Définissez le MTU souhaité (facultatif). La valeur par défaut est 1500, ce qui correspond au MTU minimum pris en charge.
- Dans la section Interface Pairs, sélectionnez les interfaces. Si d'autres paires sont nécessaires, cliquez sur le lien Ajouter une autre paire.

Create New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

 inline (Ethernet1/3) 



 inside (Ethernet1/2) 



[Add another pair](#)

CANCEL

OK

Paires d'interfaces

- Pour configurer les paramètres avancés de l'ensemble en ligne, accédez à l'onglet Avancé.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3)



inside (Ethernet1/2)



[Add another pair](#)

CANCEL

OK

Paramètres avancés

- Sélectionnez le mode comme Inline. Si le mode Tap est activé, l'option Échec du renversement ouvert est désactivée.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

Mode en ligne

- Snort Fail Open permet au trafic nouveau et existant de passer sans inspection (activé) ou abandon (désactivé) lorsque le processus Snort est occupé ou arrêté.
- Sélectionnez les paramètres Snort Fail Open souhaités.
- Aucune, une ou les deux options Occupé et Arrêté peuvent être définies.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode



Tap



Inline

Enabling " Snort Fail Open" might allow traffic unrestricted.

Snort Fail Open Busy Down

Propagate Link State

CANCEL

OK

Snort Fail Open

- L'option Propagate Link State désactive automatiquement la deuxième interface de la paire en ligne lorsque l'une des interfaces est désactivée. Lorsque l'interface désactivée redémarre, la deuxième interface redémarre également automatiquement.
- Une fois que tout est défini, cliquez sur Ok pour enregistrer la configuration.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode

Tap Inline

Enabling "Snort Fail Open" might allow traffic unrestricted.

Snort Fail Open Busy Down

Propagate Link State

CANCEL

OK

Propager l'état des liaisons

- Pour ajouter cet ensemble en ligne à une zone de sécurité, accédez à Objets > Zones de sécurité.
- Cliquez sur Add pour créer une nouvelle zone de sécurité.

The screenshot shows the Firewall Device Manager interface for a firepower device. The 'Objects' tab is selected in the top navigation bar. On the left sidebar, 'Security Zones' is highlighted. The main content area displays 'Security Zones' with a table listing 2 objects:

#	NAME	MODE	INTERFACES	ACTIONS
1	inside_zone	Routed		
2	outside_zone	Routed		

A red box highlights the '+' button in the top right corner of the table, indicating the 'Add' button for creating a new security zone.

Ajouter une zone de sécurité

- Définissez un nom, sélectionnez le mode Inline et ajoutez les interfaces de l'ensemble Inline. Cliquez ensuite sur OK pour enregistrer.

Add Security Zone

Name

inline

Description

Mode

Routed Passive Inline

Interfaces

+ inline (Ethernet1/3)

inside (Ethernet1/2)

CANCEL OK

Ajouter des interfaces

- Accédez à l'onglet Déploiement et Déployez les modifications.

Modifier ou supprimer un jeu en ligne

Les actions Modifier et Supprimer sont disponibles pour les jeux en ligne.

Device Summary
Interfaces


Cisco Firepower 2120 Threat Defense

MGMT, CONSOLE, 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9, 1/10, 1/11, 1/12, 1/13, 1/14, 1/15, 1/16 SFP

Interfaces | EtherChannels | Virtual Tunnel Interfaces | **Inline Sets**

1 inline set

Filter +

NAME	MODE	MTU	INTERFACE PAIRS	ACTIONS
inline	Inline	1500	inline ↔ inside	 

Actions du jeu en ligne

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.