

Configuración de interfaces de FDM en modo de par en línea

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Directrices y limitaciones](#)

[Antes de comenzar](#)

[Detalles del modo en línea](#)

[Diagrama de red de conjunto lineal](#)

[Configurar conjunto en línea](#)

[Modificación o eliminación de un conjunto en línea](#)

Introducción

Este documento describe los conjuntos en línea para FDM agregados en Cisco Secure Firewall 7.4.1.

Prerequisites

Requirements

Cisco recomienda tener conocimientos de estos temas:

- Conceptos y configuración de FDM
- Se aplica a FTD en las plataformas de las series 1000, 2100 y 3100 administradas por FDM

Componentes Utilizados

La información de este documento se basa en FDM 7.4.2.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Un conjunto en línea proporciona una interfaz de sólo IPS. Puede implementar interfaces sólo IPS si dispone de un firewall independiente que las proteja y no desea la sobrecarga de las funciones de firewall.

Un conjunto en línea actúa como una protuberancia en el cable, enlazando dos interfaces para acoplarse en una ranura en una red existente. Esta función permite instalar el dispositivo en cualquier entorno de red sin la configuración de dispositivos de red adyacentes. Las interfaces en línea reciben todo el tráfico incondicionalmente, pero todo el tráfico recibido en estas interfaces se retransmite fuera de un conjunto en línea a menos que se descarte explícitamente.

Directrices y limitaciones

- Solo puede configurar conjuntos en línea en estos modelos de dispositivos: Firepower serie 1000, Firepower serie 2100, Secure Firewall 3100.
- Tipos de interfaz permitidos en un conjunto en línea: físico, EtherChannel.
- No puede incluir la interfaz de administración en un conjunto en línea.
- No puede cambiar los atributos de las interfaces utilizadas en un conjunto en línea: nombre, modo, ID de interfaz, MTU, dirección IP.
- Si activa el modo de toque, la opción Snort Fail Open (Fallo al abrir) estará desactivada.
- Los paquetes de eco de detección de reenvío bidireccional (BFD) no se permiten a través del dispositivo cuando se utilizan conjuntos en línea. Si hay dos vecinos en cada lado del dispositivo que ejecuta BFD, el dispositivo descarta paquetes de eco BFD porque tienen la misma dirección IP de origen y de destino y parecen ser parte de un ataque LAND.
- Para conjuntos en línea e interfaces pasivas, el dispositivo admite hasta dos encabezados 802.1Q en un paquete (también conocido como compatibilidad Q-in-Q).



Nota: Las interfaces de tipo firewall no admiten Q-in-Q y solo admiten un encabezado 802.1Q.

- Las interfaces de un conjunto en línea no admiten routing, NAT, DHCP (servidor, cliente o relé), VPN, interceptación TCP, inspección de aplicaciones o Netflow.

Antes de comenzar

- Se recomienda configurar STP PortFast para los switches habilitados para STP que se conectan a las interfaces de par en línea de defensa contra amenazas.
- Configure las interfaces físicas o EtherChannel que pueden ser miembros del conjunto en línea. Solo puede configurar estos valores: Nombre, dúplex, velocidad y modo enrutado (no seleccione pasivo). No configure ningún tipo de direccionamiento, es decir, direcciones IP manuales, DHCP o PoE.

Detalles del modo en línea

- Esta función permite utilizar conjuntos en línea. Esto permite la inspección del tráfico sin asignación de IP.
- El modo en línea está disponible para interfaces físicas, EtherChannels y zonas de seguridad.
- El modo en línea se establece automáticamente para las interfaces y los EtherChannels cuando se utilizan en un par en línea.
- El modo en línea evita que se realicen cambios en las interfaces y los EtherChannels involucrados hasta que se eliminen del par en línea.
- Las interfaces que están en modo en línea se pueden asociar a las zonas de seguridad establecidas en modo en línea.

Diagrama de red de conjunto lineal

El tráfico fluye desde el Router1 al Router2 a través de las interfaces A y B utilizando solamente una conexión física.

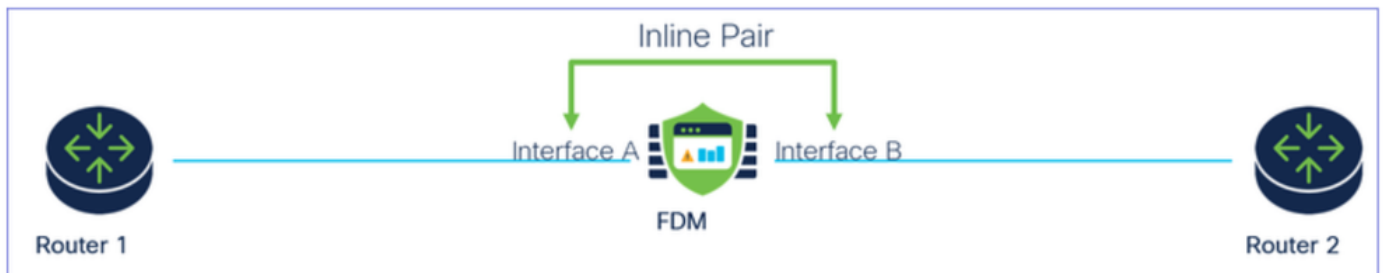


Diagrama de la red

Configurar conjunto en línea

- Desde el panel de FDM, navegue hasta la tarjeta Interfaces.

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

Ficha Interfaces

- Para activar las interfaces, haga clic en el icono Status de la interfaz.

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 <small>Static</small>		Enabled	
> ○ Ethernet1/3		<input type="checkbox"/>	Routed			Enabled	
> ○ Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	

Icono de estado

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 <small>Static</small>		Enabled	
> ✓ Ethernet1/3		<input checked="" type="checkbox"/>	Routed			Enabled	

Activar interfaz

- Para Editar interfaces, haga clic en el icono Editar (lápiz) para la interfaz.

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	

Editar interfaz

- Introduzca el nombre de la interfaz y seleccione el modo como enrutado. No configure ninguna dirección IP.

Ethernet1/3

Edit Physical Interface



Interface Name

Mode

Status

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

Description

IPv4 Address IPv6 Address Advanced

Type

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

 /

Editar interfaz

- Para crear un conjunto en línea, desplácese a la pestaña Conjuntos en línea.

Device Summary

Interfaces

Cisco Firepower 2120 Threat Defense

Interfaces EtherChannels Virtual Tunnel Interfaces **Inline Sets**

17 Interfaces

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

Crear conjunto en línea

Para agregar un conjunto en línea, haga clic en Agregar (icono +).

The screenshot shows the configuration page for a Cisco Firepower 2120 Threat Defense device. At the top, there is a 'Device Summary' section with the title 'Interfaces'. Below this, a grid of interface icons is displayed, including MGMT, CONSOLE, and various numbered ports (1/1 through 1/16). The 'Inline Sets' tab is selected, showing a table with the following columns: NAME, MODE, MTU, INTERFACE PAIRS, and ACTIONS. The table is currently empty, with a message stating 'There are no Inline Sets yet. Start by creating the first Inline Set.' and a 'CREATE INLINE SET' button. A red box highlights a plus sign icon in the top right corner of the table area.

Agregar conjunto en línea

- Establezca un nombre para el conjunto en línea.
- Configure la MTU deseada (opcional) . El valor predeterminado es 1500, que es la MTU mínima admitida.
- En la sección Interface Pairs, seleccione las interfaces. Si se requieren más pares, haga clic en el enlace Agregar otro par.

Create New Inline Set



Name

inline

MTU

1500


General

Advanced

Interface Pairs

 inline (Ethernet1/3) ▼



 inside (Ethernet1/2) ▼



[Add another pair](#)

CANCEL

OK

Pares de interfaz

- Para configurar los parámetros avanzados del conjunto en línea, vaya a la ficha Advanced.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3)



inside (Ethernet1/2)



[Add another pair](#)

CANCEL

OK

Configuración avanzada

- Seleccione el Modo como En línea. Si está activado el modo de toque, la opción Snort Fail Open (Fallo al abrir) está desactivada.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

Modo en línea

- Snort Fail Open permite que el tráfico nuevo y existente pase sin inspección (activado) o se descarte (desactivado) cuando el proceso Snort está ocupado o inactivo.
- Seleccione la configuración deseada de Snort Fail Open.
- No se puede establecer ninguna de las opciones Busy y Down o ninguna de ellas.

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

Error al abrir Snort

- La opción Propagate Link State (Propagar estado de link) desactiva automáticamente la segunda interfaz en el par lineal cuando una de las interfaces deja de funcionar. Cuando la interfaz desactivada vuelve a activarse, la segunda interfaz también vuelve a activarse automáticamente.
- Una vez que todo esté configurado, haga clic en Aceptar para guardar la configuración.

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

Propagar estado de link

- Para agregar este conjunto en línea a una zona de seguridad, navegue hasta Objetos > Zonas de seguridad.
- Haga clic en Agregar para crear una nueva zona de seguridad.

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | cisco SECURE

Object Types

- Networks
- Ports
- Security Zones**
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies

Security Zones

2 objects

#	NAME	MODE	INTERFACES	ACTIONS
1	inside_zone	Routed		
2	outside_zone	Routed		

Agregar zona de seguridad

- Establezca un Nombre, seleccione el modo como Inline y agregue las interfaces del conjunto Inline. A continuación, haga clic en Aceptar para guardar.

Add Security Zone

Name

inline

Description

Mode

Routed Passive Inline

Interfaces

+ inline (Ethernet1/3)

inside (Ethernet1/2)

CANCEL OK

Agregar interfaces

- Vaya a la pestaña Implementación e Implemente los cambios.

Modificación o eliminación de un conjunto en línea

Las acciones Editar (Edit) y Borrar (Delete) están disponibles para los conjuntos en línea.

Device Summary
Interfaces

Cisco Firepower 2120 Threat Defense

MGMT	1/1	1/3	1/5	1/7	1/9	1/11
CONSOLE	1/2	1/4	1/6	1/8	1/10	1/12
SFP						

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

1 inline set

Filter +

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

Acciones del conjunto en línea

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).