

Configurar Interfaces do FDM no Modo de Par Embutido

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Diretrizes e limitações](#)

[Antes de Começar](#)

[Detalhes do Modo Embutido](#)

[Diagrama de rede de configuração in-line](#)

[Configurar Conjunto Embutido](#)

[Modificar ou excluir um conjunto embutido](#)

Introdução

Este documento descreve os Conjuntos Embutidos para FDM adicionados ao Cisco Secure Firewall 7.4.1.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- Conceitos e configuração do FDM
- Aplica-se a FTDs nas plataformas 1000, 2100 e 3100 Series gerenciadas pelo FDM

Componentes Utilizados

As informações neste documento são baseadas no FDM 7.4.2.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Um conjunto em linha fornece uma interface somente IPS. Você pode implementar interfaces somente IPS se tiver um firewall separado protegendo essas interfaces e não quiser a sobrecarga das funções de firewall.

Um conjunto em linha atua como um bump no fio, unindo duas interfaces para se encaixar em uma rede existente. Essa função permite que o dispositivo seja instalado em qualquer ambiente de rede sem a configuração de dispositivos de rede adjacentes. As interfaces em linha recebem todo o tráfego incondicionalmente, mas todo o tráfego recebido nessas interfaces é retransmitido para fora de um conjunto em linha, a menos que seja descartado explicitamente.

Diretrizes e limitações

- Você pode configurar conjuntos em linha apenas nestes modelos de dispositivo: Firepower 1000 Series, Firepower 2100, Secure Firewall 3100.
- Tipos de interface permitidos em um conjunto embutido: físico, EtherChannel.
- Não é possível incluir a interface de gerenciamento em um conjunto embutido.
- Você não pode alterar os atributos das interfaces usadas em um conjunto embutido: nome, modo, ID da interface, MTU, endereço IP.
- Se você habilitar o modo Tap, a opção Snort Fail Open será desabilitada.
- Pacotes de eco BFD (Detecção de Encaminhamento Bidirecional) não são permitidos através do dispositivo ao usar conjuntos em linha. Se houver dois vizinhos em ambos os lados do dispositivo executando o BFD, o dispositivo descartará os pacotes de eco BFD porque eles têm o mesmo endereço IP de origem e de destino e parecem fazer parte de um ataque LAND.
- Para conjuntos em linha e interfaces passivas, o dispositivo suporta até dois cabeçalhos 802.1Q em um pacote (também conhecido como suporte Q-in-Q).



Note: As interfaces do tipo firewall não suportam Q-in-Q e suportam apenas um cabeçalho 802.1Q.

- As interfaces em um conjunto em linha não suportam roteamento, NAT, DHCP (servidor, cliente ou relay), VPN, Interceptação de TCP, inspeção de aplicativos ou Netflow.

Antes de Começar

- É recomendável definir o PortFast de STP para switches ativados por STP que se conectam às interfaces de par em linha de defesa contra ameaças.
- Configure as interfaces física ou EtherChannel que podem ser membros do conjunto em linha. Você pode configurar apenas estes valores: Nome, duplex, velocidade e modo Roteado (não selecione passivo). Não configure nenhum tipo de endereçamento, isto é,

endereços IP manuais, DHCP ou PoE.

Detalhes do Modo Embutido

- Este recurso permite usar Conjuntos em linha. Isso permite a inspeção de tráfego sem alocação de IP.
- O Modo em linha está disponível para interfaces físicas, EtherChannels e Zonas de Segurança.
- O Modo em linha é automaticamente definido para Interfaces e EtherChannels quando eles são usados em um Par em linha.
- O modo em linha impede que sejam feitas alterações nas interfaces envolvidas e nos EtherChannels até que sejam removidas do par em linha.
- As interfaces que estão no modo in-line podem ser associadas a Zonas de segurança definidas para o modo in-line.

Diagrama de rede de configuração in-line

O tráfego flui do Roteador 1 para o Roteador 2 através das Interfaces A e B usando apenas uma conexão física.

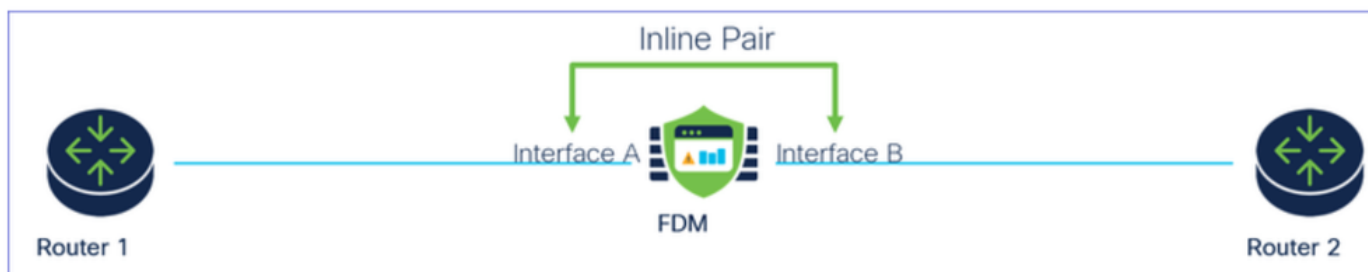


Diagrama de Rede

Configurar Conjunto Embutido

- No painel do FDM, navegue até o cartão 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

Guia Interfaces

- Para ativar interfaces, clique no ícone Status da 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 <small>Static</small>		Enabled	
> ○ Ethernet1/3		<input type="checkbox"/>	Routed			Enabled	
> ○ Ethernet1/4		<input type="checkbox"/>	Routed			Enabled	

Ícone de Status

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	

Ativar interface



- Para Editar interfaces, clique no ícone Editar (lápiz) da interface.

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 1/13 1/14 1/15 1/16

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

Editar interface

- Insira o Nome da interface e selecione o modo como Roteado. Não configure nenhum endereço 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

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

/

Editar interface

- Para criar um Conjunto Embutido, navegue até a guia Conjuntos Embutidos.

Device Summary

Interfaces

Cisco Firepower 2120 Threat Defense

MGMT

1/1

1/3

1/5

1/7

1/9

1/11

1/13

1/14

1/15

1/16

CONSOLE

1/2

1/4

1/6

1/8

1/10

1/12

SFP

Interfaces EtherChannels Virtual Tunnel Interfaces Inline Sets

17 Interfaces Filter

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	

Criar Conjunto Embutido

Para adicionar um Conjunto interno, clique em Adicionar (ícone +).

The screenshot displays the 'Device Summary' for a Cisco Firepower 2120 Threat Defense device. Under the 'Interfaces' tab, there is a grid of interface icons including MGMT, CONSOLE, and various numbered ports (1/1 through 1/16). A red box highlights a '+' icon in the top right corner of the interface configuration area. Below this, the 'Inline Sets' tab is selected, showing a table with columns for 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.

Adicionar Conjunto Embutido

- Defina um nome para o conjunto embutido.
- Defina a MTU desejada (opcional) . O padrão é 1500, que é o MTU mínimo suportado.
- Na seção Interface Pairs, selecione as interfaces. Se mais pares forem necessários, clique em Adicionar outro link 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 interface

- Para definir as configurações avançadas para o Conjunto em linha, navegue até a guia Avançado.

Edit New Inline Set



Name

inline

MTU

1500


General

Advanced

Interface Pairs

 inline (Ethernet1/3) ▼



 inside (Ethernet1/2) ▼



[Add another pair](#)

CANCEL

OK

Configurações avançadas

- Selecione Mode como Inline. Se o Modo de toque estiver ativado, a opção Falha ao abrir do Snort estará desativada.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

Modo Embutido

- Snort Fail Open permite que o tráfego novo e existente passe sem inspeção (habilitado) ou descarte (desabilitado) quando o processo Snort estiver ocupado ou inativo.
- Selecione as configurações desejadas de Snort Fail Open.
- É possível definir as opções Ocupado e Inativo ou nenhuma delas.

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 (Falha ao abrir)

- A opção Propagate Link State desativa automaticamente a segunda interface no par em linha quando uma das interfaces é desativada. Quando a interface inoperante volta a ficar ativa, a segunda interface também volta a ficar ativa automaticamente.
- Quando tudo estiver definido, clique em Ok para salvar a configuração.

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 do Link

- Para adicionar esse conjunto embutido a uma zona de segurança, navegue até Objetos > Zonas de segurança.
- Clique em Adicionar para criar uma nova zona de segurança.

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		

Adicionar Zona de Segurança

- Defina um Nome, selecione o modo como Inline e adicione as interfaces do Conjunto em linha. Em seguida, clique em OK para salvar.

Add Security Zone

Name

inline

Description

Mode

Routed Passive Inline

Interfaces

+ inline (Ethernet1/3)

inside (Ethernet1/2)

CANCEL OK

Adicionar interfaces

- Navegue até a guia Implantação e Implante as alterações.

Modificar ou excluir um conjunto embutido

As ações Editar e Excluir estão disponíveis para os Conjuntos Embutidos.

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: 1/13, 1/14, 1/15, 1/16

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

1 inline set Filter +

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

Ações do Conjunto Embutido

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.