

FDM-interfaces in inline-paarmodus configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Richtlijnen en beperkingen](#)

[Voordat u begint](#)

[Details inline-modus](#)

[Inline set-netwerkdigram](#)

[Inline set configureren](#)

[Een inline set wijzigen of verwijderen](#)

Inleiding

Dit document beschrijft de Inline Sets voor FDM die is toegevoegd in Cisco Secure Firewall 7.4.1.

Voorwaarden

Vereisten

Cisco raadt u aan kennis van deze onderwerpen te hebben:

- FDM-concepten en -configuratie
- Is van toepassing op FTD's op de 1000, 2100 en 3100 Series platforms die worden beheerd door FDM

Gebruikte componenten

De informatie in dit document is gebaseerd op FDM 7.4.2.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Een inline set biedt een interface die alleen IPS bevat. U kunt IPS-only interfaces implementeren als u een afzonderlijke firewall hebt die deze interfaces beschermt en de overhead van

firewallfuncties niet wilt.

Een inline set werkt als een bult op de draad en bindt twee interfaces samen om in een bestaand netwerk te goten. Met deze functie kan het apparaat worden geïnstalleerd in een netwerkomgeving zonder configuratie van aangrenzende netwerkapparaten. Inline interfaces ontvangen al het verkeer onvoorwaardelijk, maar al het verkeer dat op deze interfaces wordt ontvangen, wordt opnieuw verzonden vanuit een inline set, tenzij dit expliciet wordt geannuleerd.

Richtlijnen en beperkingen

- U kunt alleen inline-sets op deze apparaatmodellen configureren: Firepower 1000 Series, Firepower 2100, Secure Firewall 3100.
- Interfacetypen toegestaan in een inline set: fysiek, EtherChannel.
- U kunt de beheerinterface niet in een inline-verzameling opnemen.
- U kunt de eigenschappen van de interfaces niet wijzigen die in een inline set worden gebruikt: naam, modus, interface-ID, MTU, IP-adres.
- Als u de tapmodus inschakelt, wordt de optie Openen bij mislukken gesynchroniseerd uitgeschakeld.
- BFD-echopakketten (Bidirectional Forwarding Detection) zijn niet toegestaan via het apparaat bij gebruik van inline sets. Als er twee burens aan beide kanten van het apparaat zijn die BFD in werking stellen, dan laat het apparaat BFD echopakketten vallen omdat zij de zelfde bron en bestemming IP adres hebben en schijnen om deel van een aanval van HET LAND te zijn.
- Voor inline sets en passieve interfaces ondersteunt het apparaat maximaal twee 802.1Q-headers in een pakket (ook bekend als Q-in-Q ondersteuning).



Opmerking: Firewall-type interfaces ondersteunen geen Q-in-Q, en ondersteunen slechts één 802.1Q header.

- Interfaces in een inline set ondersteunen geen routing, NAT, DHCP (server, client of relay), VPN, TCP-onderschepping, toepassingsinspectie of NetFlow.

Voordat u begint

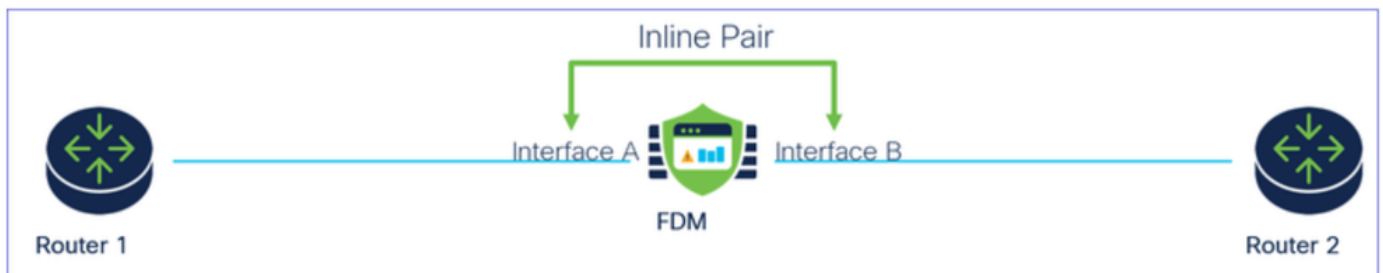
- Aanbevolen wordt om STP PortFast in te stellen voor STP-enabled switches die verbinding maken met de inline paarinterfaces van de bedreigingsverdediging.
- Configureer de fysieke of EtherChannel-interfaces die lid kunnen zijn van de inline set. U kunt deze waarden alleen configureren: Naam, duplex, snelheid en Routed mode (selecteer geen passieve modus). Configureer geen typen adressering, d.w.z. handmatige IP-adressen, DHCP of PoE.

Details inline-modus

- Deze eigenschap staat u toe om Inline reeksen te gebruiken. Dit maakt verkeersinspectie zonder IP-toewijzing mogelijk.
- De inline modus is beschikbaar voor fysieke interfaces, EtherChannel en security zones.
- De inline modus wordt automatisch ingesteld voor interfaces en EtherChannel wanneer deze in een inline paar worden gebruikt.
- De inline modus voorkomt dat er wijzigingen worden aangebracht op de betrokken interfaces en EtherChannel totdat deze worden verwijderd uit het inline paar.
- Interfaces die in de inline modus staan, kunnen worden gekoppeld aan security zones die zijn ingesteld op de inline modus.

Inline set-netwerkdigram

Verkeerstromen van Router1 naar Router2 door interfaces A en B die slechts een fysieke verbinding gebruiken.



Netwerkdigram

Inline set configureren

- Van het FDM dashboard, navigeer aan Interfaces kaart.

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

Tabblad Interfaces

- Klik op het pictogram Status van de interface om interfaces in te schakelen.

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	

Statuspictogram

Device Summary Interfaces

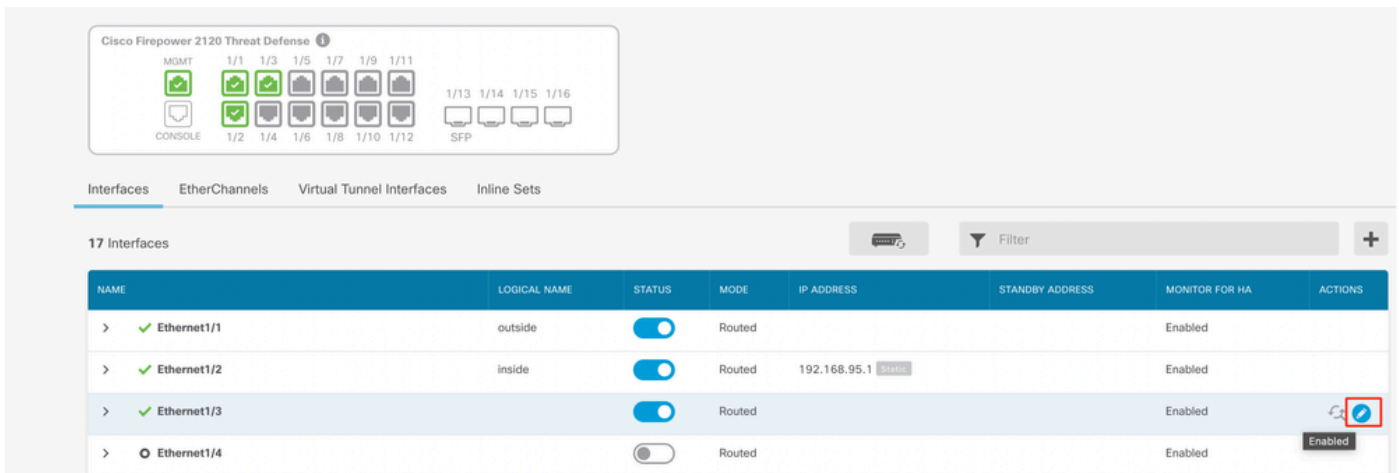
Interfaces EtherChannels Virtual Tunnel Interfaces Inline Sets

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	

Interface inschakelen

- Als u interfaces wilt bewerken, klikt u op het pictogram Bewerken (potlood) voor de 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	

Interface bewerken

- Voer de interfacenaam in en selecteer de modus zoals Routed. Configureer geen IP-adres.

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

 /

Interface bewerken

- Als u een inline set wilt maken, navigeer dan naar het tabblad Inline sets.

Device Summary

Interfaces

Cisco Firepower 2120 Threat Defense

Interfaces EtherChannels Virtual Tunnel Interfaces **Inline Sets**

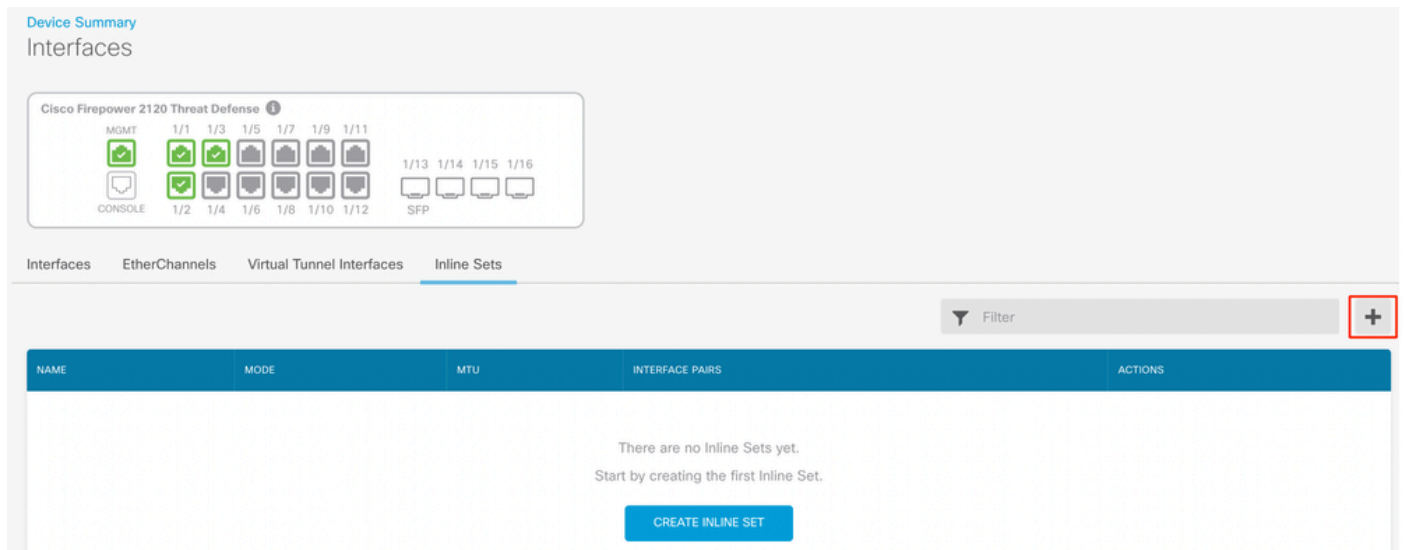
17 Interfaces

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	

Inline set maken

Als u een inline set wilt toevoegen, klikt u op Toevoegen (+ pictogram).



The screenshot shows the 'Device Summary' page for a Cisco Firepower 2120 Threat Defense device. The 'Interfaces' section is active, and the 'Inline Sets' tab is selected. A table with columns for NAME, MODE, MTU, INTERFACE PAIRS, and ACTIONS is present, but it is empty. A message states: 'There are no Inline Sets yet. Start by creating the first Inline Set.' Below this message is a 'CREATE INLINE SET' button. A red box highlights a plus sign icon in the top right corner of the interface.

Inline set toevoegen

- Stel een naam in voor de inline set.
- Stel gewenste MTU in (optioneel) . De standaard is 1500, wat het minimum ondersteunde MTU is.
- Selecteer in de sectie Interfaceparen de interfaces. Als er meer paren nodig zijn, klikt u op Een andere paarkoppeling toevoegen.

Create New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

 inline (Ethernet1/3) ▼



 inside (Ethernet1/2) ▼



[Add another pair](#)

CANCEL

OK

Interfaceparen

- Om de geavanceerde instellingen voor de Inline Set te configureren, navigeer je naar het tabblad Advanced.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3)



inside (Ethernet1/2)



[Add another pair](#)

CANCEL

OK

Geavanceerde instellingen

- Selecteer de modus als inline. Als de tapmodus is ingeschakeld, wordt Snort Fail Open uitgeschakeld.

Edit New Inline Set



Name


inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

Modus inline

- Snort Fail Open maakt het mogelijk dat nieuw en bestaand verkeer zonder inspectie (ingeschakeld) of neerzetten (uitgeschakeld) doorgaat wanneer het Snort-proces bezig of ingedrukt is.
- Selecteer de gewenste instellingen voor snurken bij openen faalt.
- Geen, één of beide van de opties Bezig en Omlaag kunnen worden ingesteld.

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

Snelfout bij openen

- De optie Propagate Link State brengt automatisch de tweede interface in het inline paar omlaag wanneer een van de interfaces omlaag gaat. Wanneer de neergehaalde interface weer omhoog komt, komt de tweede interface ook automatisch terug omhoog.
- Als alles is ingesteld, klikt u op OK om de configuratie op te slaan.

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

Verspreid linkstatus

- Als u deze inline set wilt toevoegen aan een beveiligingszone, navigeert u naar Objecten > Beveiligingszones.
- Klik op Add om een nieuwe security zone te maken.

Firewall Device Manager

Monitoring Policies **Objects** Device: firepower

admin Administrator

Object Types

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

Security Zones

2 objects Filter +

#	NAME	MODE	INTERFACES	ACTIONS
1	inside_zone	Routed		
2	outside_zone	Routed		

Security zone toevoegen

- Stel een naam in, selecteer de modus als Inline en voeg de interfaces van de Inline set toe. Klik vervolgens op OK om op te slaan.

Add Security Zone

Name
inline

Description

Mode
 Routed Passive Inline

Interfaces
+
inline (Ethernet1/3)
inside (Ethernet1/2)

CANCEL OK

Interfaces toevoegen

- Navigeer naar het tabblad Implementatie en implementeer de wijzigingen.

Een inline set wijzigen of verwijderen

Bewerk en verwijder acties zijn beschikbaar voor de inline sets.



Device Summary
Interfaces

Cisco Firepower 2120 Threat Defense

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

1 inline set

Filter +

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

Handelingen van Inline Set

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.