

Konfigurieren von FDM-Schnittstellen im Inline-Pair-Modus

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Richtlinien und Einschränkungen](#)

[Vorbereitungen](#)

[Details zum Inline-Modus](#)

[Inline-Set-Netzwerkdiagramm](#)

[Inline-Set konfigurieren](#)

[Ändern oder Löschen eines Inline-Sets](#)

Einleitung

In diesem Dokument werden die Inline-Sets für FDM beschrieben, die in Cisco Secure Firewall 7.4.1 hinzugefügt wurden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- FDM Konzepte und Konfiguration
- Gilt für FTDs auf den von FDM verwalteten Plattformen der Serien 1000, 2100 und 3100

Verwendete Komponenten

Die in diesem Dokument enthaltenen Informationen basieren auf FDM 7.4.2.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Ein Inline-Set stellt eine Schnittstelle zur Verfügung, die nur IPS unterstützt. Sie können nur IPS-Schnittstellen implementieren, wenn Sie über eine separate Firewall verfügen, die diese Schnittstellen schützt, und den zusätzlichen Aufwand durch die Firewall-Funktionen vermeiden möchten.

Ein Inline-Set wirkt wie eine Beule am Kabel und verbindet zwei Schnittstellen miteinander, um einen Steckplatz in einem vorhandenen Netzwerk einzurichten. Mit dieser Funktion kann das Gerät in einer beliebigen Netzwerkumgebung installiert werden, ohne dass benachbarte Netzwerkgeräte konfiguriert werden müssen. Inline-Schnittstellen empfangen den gesamten Datenverkehr ohne Einschränkungen, aber der gesamte Datenverkehr, der auf diesen Schnittstellen empfangen wird, wird aus einem Inline-Set erneut übertragen, sofern er nicht explizit fallen gelassen wird.

Richtlinien und Einschränkungen

- Sie können Inline-Sets nur auf diesen Gerätemodellen konfigurieren: Firepower der Serie 1000, Firepower 2100, Secure Firewall 3100.
- In einem Inline-Set zulässige Schnittstellentypen: physisch, EtherChannel.
- Sie können die Management-Schnittstelle nicht in ein Inline-Set integrieren.
- Sie können die Attribute der in einem Inline-Set verwendeten Schnittstellen nicht ändern: Name, Modus, Schnittstellen-ID, MTU, IP-Adresse.
- Wenn Sie den Tap-Modus aktivieren, ist Snort Fail Open deaktiviert.
- BFD-Echo-Pakete (Bidirectional Forwarding Detection) sind bei Verwendung von Inline-Sätzen nicht zulässig. Wenn auf beiden Seiten des Geräts zwei Nachbarn BFD ausführen, verwirft das Gerät BFD-Echo-Pakete, da diese die gleiche Quell- und Ziel-IP-Adresse aufweisen und Teil eines LAN-Angriffs zu sein scheinen.
- Für Inline-Sets und passive Schnittstellen unterstützt das Gerät bis zu zwei 802.1Q-Header in einem Paket (auch als Q-in-Q-Unterstützung bezeichnet).



Anmerkung: Firewall-Schnittstellen unterstützen Q-in-Q nicht und nur einen 802.1Q-Header.

- Schnittstellen in einem Inline-Set unterstützen kein Routing, NAT, DHCP (Server, Client oder Relay), VPN, TCP Intercept, keine Anwendungsinspektion oder keinen NetFlow.

Vorbereitungen

- Es wird empfohlen, STP PortFast für STP-fähige Switches festzulegen, die mit den Inline-Pair-Schnittstellen zur Bedrohungsabwehr verbunden sind.
- Konfigurieren Sie die physischen oder EtherChannel-Schnittstellen, die Mitglieder des Inline-

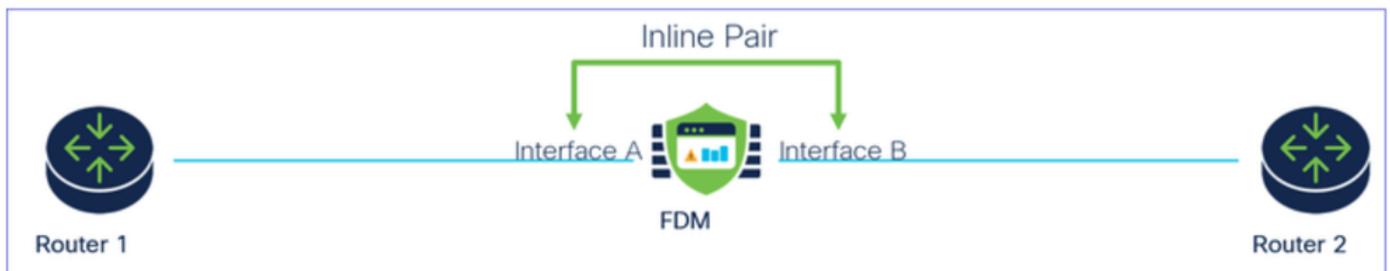
Sets sein können. Sie können nur diese Werte konfigurieren: Name, Duplex, Geschwindigkeit und Routed-Modus (wählen Sie nicht "passiv" aus). Konfigurieren Sie keine Adressierungsarten, d. h. manuelle IP-Adressen, DHCP oder PoE.

Details zum Inline-Modus

- Mit dieser Funktion können Sie Inline-Sets verwenden. Dadurch wird eine Überprüfung des Datenverkehrs ohne IP-Zuweisung ermöglicht.
- Der Inline-Modus ist für physische Schnittstellen, EtherChannels und Sicherheitszonen verfügbar.
- Der Inline-Modus wird automatisch für Schnittstellen und EtherChannels festgelegt, wenn sie in einem Inline-Paar verwendet werden.
- Der Inline-Modus verhindert, dass Änderungen an den betreffenden Schnittstellen und EtherChannels vorgenommen werden, bis diese aus dem Inline-Paar entfernt werden.
- Schnittstellen, die sich im Inline-Modus befinden, können Sicherheitszonen zugeordnet werden, die auf den Inline-Modus gesetzt sind.

Inline-Set-Netzwerkdiagramm

Der Datenverkehr fließt von Router1 zu Router2 über die Schnittstellen A und B und nutzt dabei nur eine physische Verbindung.



Netzwerkdiagramm

Inline-Set konfigurieren

- Navigieren Sie im FDM-Dashboard zu Schnittstellen-Karte.

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](#)

Registerkarte Schnittstellen

- Um Schnittstellen zu aktivieren, klicken Sie auf das Statussymbol der Schnittstelle.

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	

Statussymbol

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	

Schnittstelle aktivieren

- Um Schnittstellen zu bearbeiten, klicken Sie für die Schnittstelle auf das Bleistiftsymbol für Edit (Bearbeiten).

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	

Schnittstelle bearbeiten

- Geben Sie den Schnittstellennamen ein, und wählen Sie den Modus "Routed" aus. Konfigurieren Sie keine IP-Adressen.

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: /

Schnittstelle bearbeiten

- Um ein Inline-Set zu erstellen, navigieren Sie zur Registerkarte Inline-Sets.

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**

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

Inline-Set erstellen

Um ein Inline-Set hinzuzufügen, klicken Sie auf Hinzufügen (Symbol +).

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**

Filter +

NAME	MODE	MTU	INTERFACE PAIRS	ACTIONS
There are no Inline Sets yet. Start by creating the first Inline Set.				

CREATE INLINE SET

Inline-Satz hinzufügen

- Legen Sie einen Namen für den Inline-Satz fest.
- Stellen Sie die gewünschte MTU ein (optional). Der Standardwert ist 1500 (dies ist die mindestens unterstützte MTU).
- Wählen Sie im Abschnitt Schnittstellenpaare die Schnittstellen aus. Wenn mehr Paare erforderlich sind, klicken Sie auf Add another pair link.

Create New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

 inline (Ethernet1/3) ▼



 inside (Ethernet1/2) ▼



[Add another pair](#)

CANCEL

OK

Schnittstellenpaare

- Um die erweiterten Einstellungen für das Inline-Set zu konfigurieren, navigieren Sie zur Registerkarte Erweitert.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3)



inside (Ethernet1/2)



[Add another pair](#)

CANCEL

OK

Erweiterte Einstellungen

- Wählen Sie den Modus als Inline aus. Wenn der Tap-Modus aktiviert ist, ist Snort Fail Open deaktiviert.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

Modus Inline

- Snort Fail Open lässt zu, dass neuer und vorhandener Datenverkehr ohne Prüfung (aktiviert) oder Abwurf (deaktiviert) weitergeleitet wird, wenn der Snort-Prozess ausgelastet oder ausgefallen ist.
- Wählen Sie die gewünschten Snort Fail Open-Einstellungen aus.
- Es können keine, eine oder beide Optionen Besetzt und Abwärts eingestellt werden.

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

- Mit der Option Link-Zustand propagieren wird die zweite Schnittstelle im Inline-Paar automatisch deaktiviert, wenn eine der Schnittstellen ausfällt. Wenn die ausgefallene Schnittstelle wieder verfügbar ist, wird auch die zweite Schnittstelle automatisch wieder aktiviert.
- Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf OK, um die Konfiguration zu speichern.

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

Verknüpfungstatus propagieren

- Um diese Inline-Gruppe einer Sicherheitszone hinzuzufügen, navigieren Sie zu Objekte > Sicherheitszonen.
- Klicken Sie auf Hinzufügen, um eine neue Sicherheitszone zu erstellen.

The screenshot shows the Firewall Device Manager interface for a firepower device. The 'Objects' tab is selected, and the 'Security Zones' section is active. A table lists two security zones: 'inside_zone' and 'outside_zone', both in 'Routed' mode. A red box highlights the '+' button in the top right corner of the table, indicating the 'Add' action.

#	NAME	MODE	INTERFACES	ACTIONS
1	inside_zone	Routed		
2	outside_zone	Routed		

Sicherheitszone hinzufügen

- Legen Sie einen Namen fest, wählen Sie den Modus als Inline aus, und fügen Sie die Schnittstellen des Inline Sets hinzu. Klicken Sie dann auf OK, um zu speichern.

Add Security Zone

Name
inline

Description

Mode
 Routed Passive Inline

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

CANCEL OK

Schnittstellen hinzufügen

- Navigieren Sie zur Registerkarte "Bereitstellung", und stellen Sie die Änderungen bereit.

Ändern oder Löschen eines Inline-Sets

Für die Inline Sets sind Bearbeitungs- und Löschaktionen verfügbar.

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	

Aktionen des Inline-Sets

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.