

인라인 쌍 모드에서 FDM 인터페이스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[지침 및 제한 사항](#)

[시작하기 전에](#)

[인라인 모드 세부 정보](#)

[인라인 집합 네트워크 다이어그램](#)

[인라인 집합 구성](#)

[인라인 집합 수정 또는 삭제](#)

소개

이 문서에서는 Cisco Secure Firewall 7.4.1에 추가된 FDM용 인라인 집합에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- FDM 개념 및 구성
- FDM에서 관리되는 1000, 2100 및 3100 Series 플랫폼의 FTD에 적용됩니다.

사용되는 구성 요소

이 문서의 정보는 FDM 7.4.2를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

인라인 집합은 IPS 전용 인터페이스를 제공합니다. 이러한 인터페이스를 보호하는 별도의 방화벽이 있고 방화벽 기능의 오버헤드가 필요하지 않은 경우 IPS 전용 인터페이스를 구현할 수 있습니다.

인라인 집합은 와이어에서 범프(bump)처럼 작동하여 두 인터페이스를 기존 네트워크에 대한 슬롯

에 바인딩합니다. 이 기능을 사용하면 인접 네트워크 디바이스의 컨피그레이션 없이 디바이스를 모든 네트워크 환경에 설치할 수 있습니다. 인라인 인터페이스는 모든 트래픽을 조건 없이 수신하지만, 이러한 인터페이스에서 수신된 모든 트래픽은 명시적으로 삭제되지 않는 한 인라인 집합에서 다시 전송됩니다.

지침 및 제한 사항

- 다음 디바이스 모델에서만 인라인 집합을 구성할 수 있습니다. Firepower 1000 시리즈, Firepower 2100, 보안 방화벽 3100.
- 인라인 집합에서 허용되는 인터페이스 유형: 물리적, EtherChannel.
- 인라인 집합에 관리 인터페이스를 포함할 수 없습니다.
- 인라인 집합에서 사용되는 인터페이스의 특성은 변경할 수 없습니다. 이름, 모드, 인터페이스 ID, MTU, IP 주소
- Tap Mode(탭 모드)를 활성화하면 Snort Fail Open(Snort 실패 열기)이 비활성화됩니다.
- 인라인 집합을 사용하는 경우 디바이스를 통해 BFD(Bidirectional Forwarding Detection) 에코 패킷이 허용되지 않습니다. 디바이스의 양쪽에 BFD를 실행 중인 네이버가 두 개 있는 경우, 디바이스는 동일한 소스 및 목적지 IP 주소를 가지고 있으며 LAND 공격의 일부로 보이기 때문에 BFD 에코 패킷을 삭제합니다.
- 인라인 집합 및 패시브 인터페이스의 경우 디바이스는 패킷에서 최대 2개의 802.1Q 헤더를 지원합니다(Q-in-Q 지원이라고도 함).



참고: 방화벽 유형 인터페이스는 Q-in-Q를 지원하지 않으며 802.1Q 헤더를 하나만 지원합니다.

- 인라인 집합의 인터페이스는 라우팅, NAT, DHCP(서버, 클라이언트 또는 릴레이), VPN, TCP 가로채기, 애플리케이션 검사 또는 Netflow를 지원하지 않습니다.

시작하기 전에

- 위협 방어 인라인 쌍 인터페이스에 연결하는 STP 지원 스위치에 대해 STP PortFast를 설정하는 것이 좋습니다.
- 인라인 집합의 구성원이 될 수 있는 물리적 또는 EtherChannel 인터페이스를 구성합니다. 다음 값만 구성할 수 있습니다. 이름, 이중, 속도 및 라우팅 모드(패시브 선택 안 함) 주소 지정 유형, 즉 수동 IP 주소, DHCP 또는 PPOE를 구성하지 마십시오.

인라인 모드 세부 정보

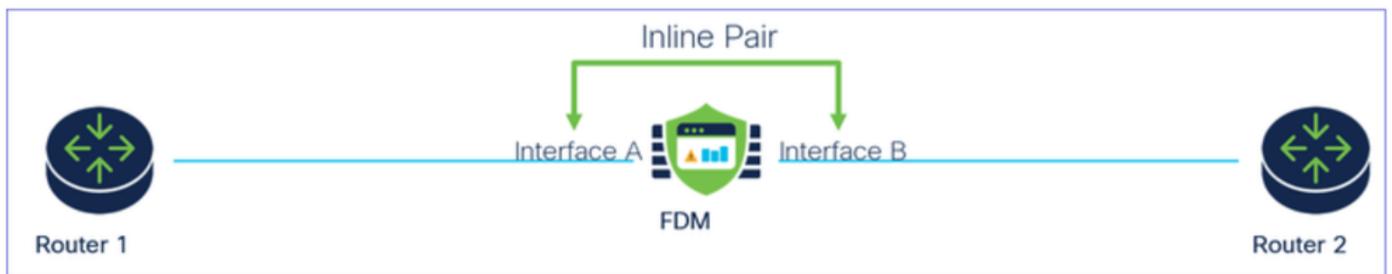
- 이 기능을 사용하면 인라인 집합을 사용할 수 있습니다. 이를 통해 IP 할당 없이 트래픽 검사

가 가능합니다.

- 인라인 모드는 물리적 인터페이스, EtherChannel 및 보안 영역에 사용할 수 있습니다.
- 인라인 모드에서 인터페이스 및 EtherChannel을 인라인 쌍에서 사용할 경우 인라인 모드가 자동으로 설정됩니다.
- 인라인 모드에서는 관련 인터페이스 및 EtherChannel을 인라인 쌍에서 제거할 때까지 해당 인터페이스에서 변경할 수 없습니다.
- 인라인 모드에 있는 인터페이스는 인라인 모드로 설정된 보안 영역과 연결할 수 있습니다.

인라인 집합 네트워크 다이어그램

트래픽은 물리적 연결만 사용하여 Router1에서 인터페이스 A 및 B를 통해 Router2로 흐릅니다.



네트워크 다이어그램

인라인 집합 구성

- FDM 대시보드에서 Interfaces(인터페이스) 카드로 이동합니다.

The screenshot shows the Cisco Firewall Device Manager (FDM) dashboard. The 'Interfaces' card is highlighted with a red box. The dashboard includes sections for 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The 'Interfaces' card shows 'Management: Merged' and 'Enabled 3 of 17'. Other cards include 'Routing', 'Updates', and 'System Settings'. The 'Interfaces' card has a 'View All Interfaces' link with a right arrow.

Interfaces 탭

- 인터페이스를 활성화하려면 인터페이스의 Status 아이콘을 클릭합니다.

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

상태 아이콘

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

인터페이스 활성화

- 인터페이스를 수정하려면 인터페이스에 대한 Edit(연필) 아이콘을 클릭합니다.

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

인터페이스 편집

- Interface Name(인터페이스 이름)을 입력하고 모드를 Routed(라우팅됨)로 선택합니다. IP 주소를 구성하지 마십시오.

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: /

인터페이스 편집

- 인라인 집합을 생성하려면 Inline Sets(인라인 집합) 탭으로 이동합니다.

Device Summary
Interfaces



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	

인라인 집합 생성

인라인 집합을 추가하려면 추가(+ 아이콘)를 클릭합니다.

Device Summary
Interfaces



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				

인라인 집합 추가

- 인라인 집합의 이름을 설정합니다.
- 원하는 MTU를 설정합니다(선택 사항). 기본값은 지원되는 최소 MTU인 1500입니다.
- Interface Pairs 섹션에서 인터페이스를 선택합니다. 추가 쌍이 필요한 경우 다른 쌍 추가 링크를 클릭합니다.

Create New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

 inline (Ethernet1/3) ▼



 inside (Ethernet1/2) ▼



[Add another pair](#)

CANCEL

OK

인터페이스 쌍

- 인라인 집합에 대한 고급 설정을 구성하려면 고급 탭으로 이동합니다.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Interface Pairs

inline (Ethernet1/3)



inside (Ethernet1/2)



[Add another pair](#)

CANCEL

OK

고급 설정

- Mode(모드)를 Inline(인라인)으로 선택합니다. Tap Mode(탭 모드)가 활성화된 경우 Snort Fail Open(Snort 실패 열기)이 비활성화됩니다.

Edit New Inline Set



Name

inline

MTU

1500

General

Advanced

Mode 



Tap



Inline

인라인 모드

- Snort Fail Open을 사용하면 Snort 프로세스가 사용 중이거나 중단된 경우 검사 없이 신규 및 기존 트래픽을 통과(활성화)하거나 삭제(비활성화)할 수 있습니다.
- 원하는 Snort Fail Open 설정을 선택합니다.
- Busy(사용 중) 및 Down(중단) 옵션 중 하나 또는 둘 다 설정할 수 없습니다.

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 실패 열기

- Propagate Link State 옵션은 인터페이스 중 하나가 다운될 때 인라인 쌍에서 두 번째 인터페이스를 자동으로 다운합니다. 다운된 인터페이스가 복구되면 두 번째 인터페이스도 자동으로 복구됩니다.
- 모든 것이 설정되면 확인을 클릭하여 컨피그레이션을 저장합니다.

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

링크 상태 전파

- 이 인라인 집합을 보안 영역에 추가하려면 Objects(개체) > Security Zones(보안 영역)로 이동합니다.
- 새 보안 영역을 생성하려면 Add(추가)를 클릭합니다.

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		

보안 영역 추가

- Name을 설정하고, 모드를 Inline으로 선택하고 Inline Set의 인터페이스를 추가합니다. 그런 다음 OK(확인)를 클릭하여 저장합니다.

Add Security Zone

Name
inline

Description

Mode
 Routed Passive Inline

Interfaces
+

inline (Ethernet1/3)

inside (Ethernet1/2)

CANCEL OK

인터페이스 추가

- Deployment(구축) 탭으로 이동하여 변경 사항을 구축합니다.

인라인 집합 수정 또는 삭제

Edit(수정) 및 Delete(삭제) 작업은 인라인 집합에 사용할 수 있습니다.

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	 

인라인 집합의 작업

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.