

トランスペアレントモードで配備された Firepowerのイベントについて

内容

[はじめに](#)

[目的](#)

[トポロジ](#)

[使用するコンポーネント](#)

[基本シナリオ](#)

[設定の概要](#)

[L3スイッチ](#)

[FMCv](#)

[確認された動作](#)

[シナリオ1](#)

[シナリオ2](#)

はじめに

このドキュメントでは、さまざまなタイプのインラインセットを使用してFTDをトランスペアレントモードで展開する場合に、イベントがどのように表示されるかについて説明します。

目的

インラインセット設定を使用してFTDをトランスペアレントモードで展開した場合の、FMCでの接続イベントの動作を明確にする。

トポロジ

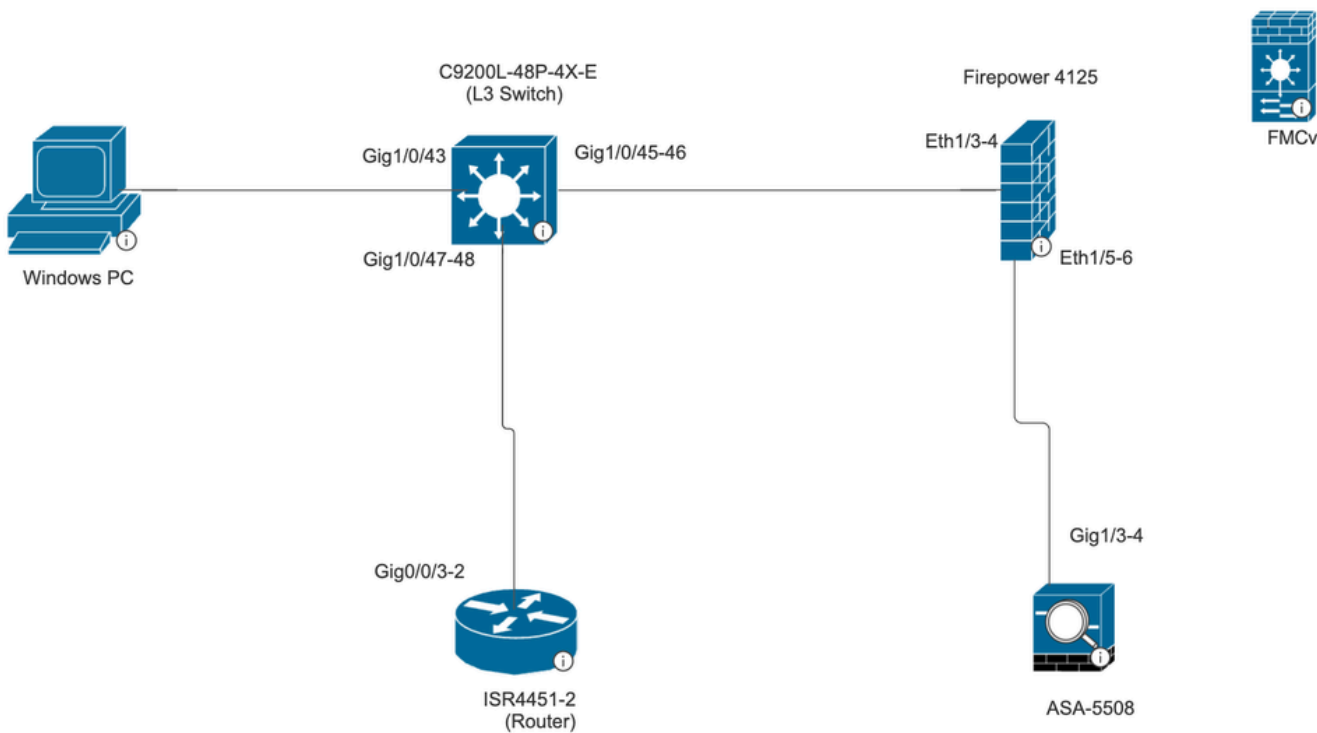


Figure 1. Topology

使用するコンポーネント

- PC仮想マシン
- C9200L-48P-4X-E (L3スイッチ)
- Firepower 4125 | 7.6
- FMCv | 7.6
- ASA 5508
- ISR4451-2 (ルータ)

基本シナリオ

Firepower 4125の1つのインラインセット設定に、選択された2つのインターフェイスペアが含まれている場合

- イーサネット1/3 (内部-1)
- イーサネット1/5 (外部1)
- イーサネット1/4 (内部-2)
- イーサネット1/6 (外部2)

Firewall Management Center
Devices / Secure Firewall Interfaces

Firepower threat defense

Cisco Firepower 4125 Threat Defense

Device **Interfaces** Inline Sets Routing DHCP VTEP

Interfaces Virtual Tunnels

Search by name Sync Device Add Interfaces

| Interface | Logical Name | Type | Security Zones | MAC Address (Active/Sta... | IP Address | Path Moni... | Virtual Router |
|-------------|--------------|----------|----------------|----------------------------|------------|--------------|----------------|
| Ethernet1/1 | | Physical | | | | Disabled | |
| Ethernet1/2 | | Physical | | | | Disabled | |
| Ethernet1/3 | INSIDE-1 | Physical | | | | Disabled | |
| Ethernet1/4 | INSIDE-2 | Physical | | | | Disabled | |
| Ethernet1/5 | EXTERNAL1 | Physical | | | | Disabled | |
| Ethernet1/6 | EXTERNAL2 | Physical | | | | Disabled | |
| Ethernet1/7 | | Physical | | | | Disabled | |
| Ethernet1/8 | diagnostic | Physical | | | | Disabled | Global |

Firewall Management Center
Devices / Secure Firewall InlineSets

Firepower threat defense

Cisco Firepower 4125 Threat Defense

Device Interfaces **Inline Sets** Routing DHCP VTEP

Add Inline Set

| Name | Interface Pairs |
|-------------|--|
| INLINE-SET1 | INSIDE-1↔EXTERNAL1, INSIDE-2↔EXTERNAL2 |

Displaying 1-1 of 1 rows | Page 1 of 1

設定の概要

L3スイッチ

ポートチャネル2(Gig 1/0/45-46)

ASA 5508

ポートチャンネル2(Gig 1/3-4)

ASAはワンアームモードで導入されます。つまり、トラフィックは同じポートチャンネル (ポートチャンネル2) を通ってASAに出入りします。

ASAとスイッチの間でトラフィックのロードバランシングを行うために、ポートチャンネルが設定されます。

Firepower 4125はFMCvに登録されています。

FMCv

設定

プレフィルタポリシー :

アクションFastpathを使用したフィルター前ルールの内部外部。

送信元インターフェイスオブジェクト : INTERNAL_1宛先インターフェイスオブジェクト :

EXTERNAL_1。

The screenshot shows the configuration page for a pre-filter policy in the ASA configuration tool. The policy name is "Internal-External" and it is enabled. The action is set to "Fastpath". The time range is set to "None". The source interface object is "INTERNAL_1" and the destination interface object is "EXTERNAL_1".

Name: Internal-External Enabled

Insert: below rule 1

Action: Fastpath

Time Range: None +

Interface Objects Networks VLAN Tags Ports Comment Logging

Available Interface Objects

EXTERNAL_1
INTERNAL_1

Add to Source
Add to Destination

Source Interface Objects (1): INTERNAL_1

Destination Interface Objects (1): EXTERNAL_1

アクセスコントロールポリシーは、allow all any-anyで設定されます。

確認された動作

シナリオ 1

VM-PCから生成されたISR4451-2 (ルータ) 宛てのICMPトラフィック :

ICMPトラフィックは次のパスを通ります。

VM-PC ----- L3Switch ----- FPR4125 ----- ASA 5508 -----FPR4125 ----- L3スイッチ---- ISRルータ

FPR 4125上の同じインラインペア(INSIDE-2 >>EXTERNAL2)を介してICMPトラフィックが入力および出力されるため、FMC接続イベントには接続イベントが1つだけ表示されます。

Policy-Based Routing (PBR) is configured on the switch interfaces connected to the firewall and router.

FTD経由のトラフィックを検査するという要件を満たすため、FTD経由でトラフィック (要求と応答の両方) をリダイレクトするようにPBRを設定する必要がありました。したがって、PCとルータに接続されているスイッチインターフェイスにPBRを設定しました。

シナリオ 2

VM-PCから生成されたISR4451-2 (ルータ) 宛てのICMPトラフィック :

ICMPトラフィックは次のパスを通ります。

VM-PC ----- L3Switch ----- FPR4125 ----- ASA 5508 -----FPR4125 ----- L3スイッチ---- ISRルータ

| Name | Interface Pairs | |
|-------------|----------------------|---|
| INLINE-SET1 | INSIDE-1<->EXTERNAL1 | edit delete |
| INLINE-SET2 | INSIDE-2<->EXTERNAL2 | edit delete |

上記の図に示すように、インラインペア設定を2つの異なるインラインセットに分割します。トラフィックはINSIDE-1からFTDを出て、EXTERNAL2から入ります。

したがって、2つのインラインセットが使用されます (DTEとDTEの両方)。

FMCで接続イベントを監視すると、発信トラフィック用と着信トラフィック用の2つの接続イベント (MACアドレスとMACアドレス) が確認できます。

この動作の背後にある理由は、FTD上のトラフィックが同じトラフィックに2つの異なるインラインペアを使用する場合 (FMC上で常に2つの接続イベントが見られる場合) に必ず発生します。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。