

# Descripción de los eventos de Firepower implementados en modo transparente

## Contenido

---

[Introducción](#)

[Objetivo](#)

[Topología](#)

[Componentes Utilizados](#)

[Escenario base](#)

[Información general sobre configuración](#)

[Switch L3](#)

[FMCv](#)

[Comportamiento observado](#)

[Escenario 1](#)

[Escenario 2](#)

---

## Introducción

Este documento describe cómo se muestran los eventos al implementar FTD en modo transparente con diferentes tipos de conjuntos en línea.

## Objetivo

Aclarar el comportamiento de los eventos de conexión en el FMC cuando el FTD se implementa en modo transparente con una configuración en línea establecida.

## Topología

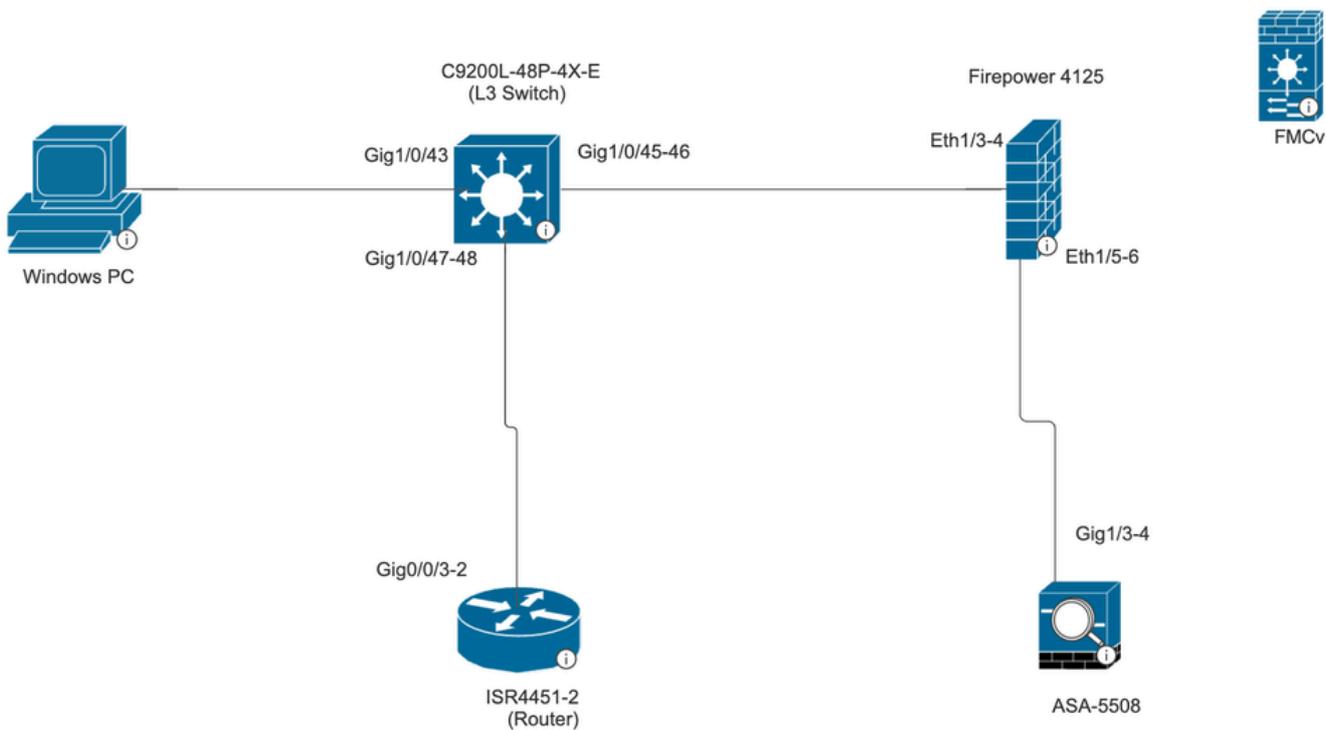


Figure 1. Topology

## Componentes Utilizados

- PC-Máquina virtual
- C9200L-48P-4X-E (switch L3)
- Firepower 4125 | 7,6
- FMCv | 7,6
- ASA 5508
- ISR4451-2 (router)

## Escenario base

Cuando una configuración de conjunto en línea en Firepower 4125 contiene dos pares de interfaz seleccionados

- Ethernet 1/3 (INSIDE-1)
- Ethernet 1/5 (EXTERNAL1)
- Ethernet 1/4 (INSIDE-2)
- Ethernet 1/6 (EXTERNA2)

Firewall Management Center  
Devices / Secure Firewall Interfaces

Search Deploy admin

### 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

Search Deploy admin

### 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

## Información general sobre configuración

Switch L3

Canal de puerto 2 (Gig 1/0/45-46)

ASA 5508

Canal de puerto 2 (Gig 1/3-4)

ASA se implementa en el modo de brazo único, lo que significa que el tráfico entra y sale del ASA a través del mismo canal de puerto que es el canal de puerto 2.

El canal de puerto se configura en el ASA y el switch para equilibrar la carga del tráfico entre los dos.

Firepower 4125 está registrado en FMCv.

## FMCv

### Configurar

Prefilter-policy:

Pre-filter rule internal-external con action Fastpath.

Objeto de interfaz de origen: INTERNAL\_1 Objeto de interfaz de destino: EXTERNO\_1.

The screenshot shows the configuration page for a pre-filter policy in FMCv. The policy name is 'Internal-External', which is enabled. The action is set to 'Fastpath'. The policy is inserted 'below rule' and is the first rule in the list. The time range is set to 'None'. The configuration is for 'Interface Objects'. The 'Available Interface Objects' list contains 'EXTERNAL\_1' and 'INTERNAL\_1'. The 'Source Interface Objects' list contains 'INTERNAL\_1'. The 'Destination Interface Objects' list contains 'EXTERNAL\_1'. There are 'Add to Source' and 'Add to Destination' buttons between the available and source/destination lists. The 'Interface Objects' tab is selected, with other tabs for 'Networks', 'VLAN Tags', and 'Ports'. There are also 'Comment' and 'Logging' options on the right side of the configuration area.

La política de control de acceso se configura con allow all any-any.

## Comportamiento observado

### Escenario 1

Tráfico ICMP generado desde VM-PC con destino a ISR4451-2 (router):

El tráfico ICMP toma el trayecto:

Switch L3 ----- VM-PC ----- FPR4125 ----- ASA 5508 -----FPR4125 ----- Switch L3 ---- Router  
ISR.

Solo se ve un evento de conexión en el evento de conexión FMC porque el tráfico ICMP entra y sale a través del mismo par de línea (INSIDE-2 >>EXTERNAL2) en el FPR 4125.

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

Para cumplir con nuestro requisito de inspeccionar el tráfico a través del FTD, necesitamos configurar PBR para redirigir el tráfico (tanto solicitudes como respuestas) a través del FTD. Por lo tanto, configuramos PBR en las interfaces del switch conectadas al PC y al router.

## Escenario 2

Tráfico ICMP generado desde VM-PC con destino a ISR4451-2 (router):

El tráfico ICMP toma el trayecto:

Switch L3 ----- VM-PC ----- FPR4125 ----- ASA 5508 -----FPR4125 ----- Switch L3 ---- Router ISR.

The screenshot shows the Cisco Firewall Management Center (FMC) interface for a Cisco Firepower 4125 Threat Defense device. The 'Inline Sets' tab is selected, showing a table with two entries:

| Name        | Interface Pairs      |   |
|-------------|----------------------|---|
| INLINE-SET1 | INSIDE-1<->EXTERNAL1 | <a href="#">edit</a> <a href="#">delete</a> |
| INLINE-SET2 | INSIDE-2<->EXTERNAL2 | <a href="#">edit</a> <a href="#">delete</a> |

The interface also includes a search bar, a 'Deploy' button, and a user profile 'admin'. The bottom of the page shows 'Displaying 1-2 of 2 rows' and 'Page 1 of 1'.

Cuando separamos la configuración de par en línea en dos conjuntos en línea diferentes, como se muestra en la figura anterior. El tráfico sale del FTD a través de INSIDE-1 y entra a través de EXTERNAL2. Por lo tanto, se utilizan dos conjuntos en línea .

Al observar los eventos de conexión en el FMC, observamos dos eventos de conexión , uno para el tráfico saliente y otro para el entrante.

La razón detrás de este comportamiento es que cuando el tráfico en FTD utiliza dos pares de línea diferentes para el mismo tráfico , siempre vemos dos eventos de conexión en el FMC.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).