

# Informazioni sugli eventi in Firepower distribuiti in modalità trasparente

## Sommario

---

[Introduzione](#)

[Obiettivo](#)

[Topologia](#)

[Componenti usati](#)

[Scenario di base](#)

[Panoramica della configurazione](#)

[Switch L3](#)

[FMCv](#)

[Comportamento osservato](#)

[Scenario 1](#)

[Scenario 2](#)

---

## Introduzione

In questo documento viene descritta la modalità di visualizzazione degli eventi quando si distribuisce FTD in modalità trasparente con diversi tipi di set inline.

## Obiettivo

Per chiarire il comportamento degli eventi di connessione nel FMC quando il FTD viene distribuito in modalità trasparente con una configurazione inline-set.

## Topologia

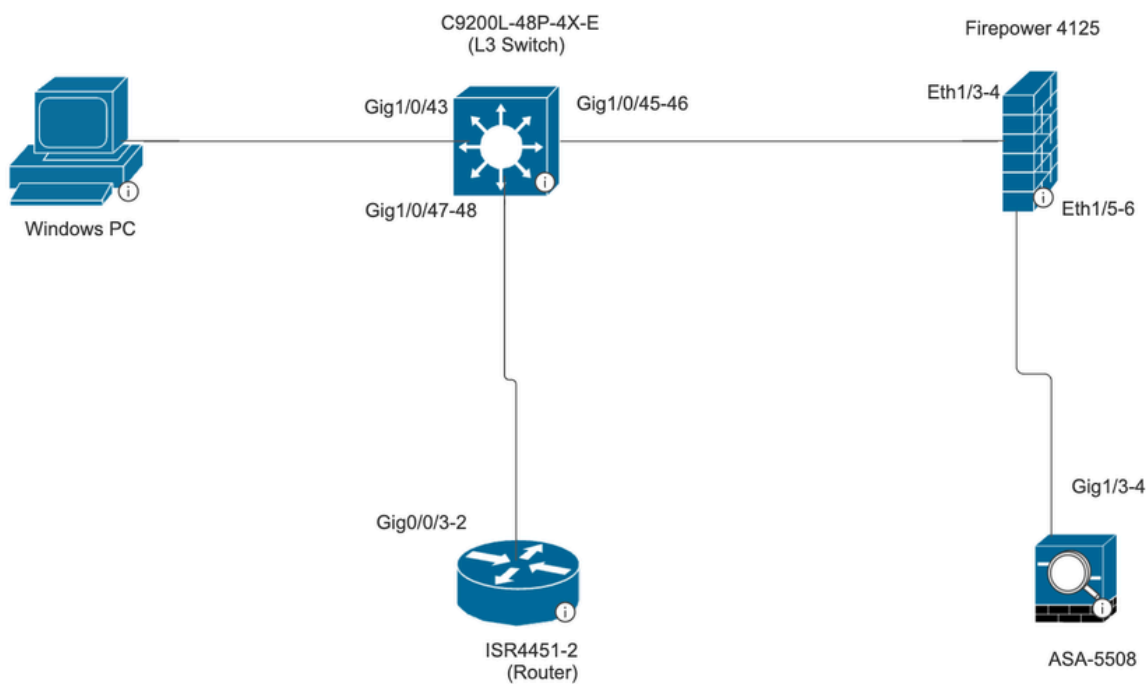


Figure 1. Topology

## Componenti usati

- PC-Macchina virtuale
- C9200L-48P-4X-E (switch L3)
- Firepower 4125 | 7,6
- FMCv | 7,6
- ASA 5508
- ISR 4451-2 (router)

## Scenario di base

Quando una configurazione Inline-set su Firepower 4125 contiene due coppie di interfacce selezionate  
Ethernet 1/3 (INTERNA-1)  
Ethernet 1/5 (ESTERNO1)  
Ethernet 1/4 (INTERNO-2)  
Ethernet 1/6 (ESTERNO2)

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

## Panoramica della configurazione

Switch L3

Port-channel 2 ( Gig 1/0/45-46)

ASA 5508

Canale porta 2 (Gig 1/3-4)

L'ASA viene distribuita in modalità One-arm, ossia il traffico entra ed esce dall'ASA attraverso lo stesso canale di porta, ossia il canale di porta 2.

Il canale della porta è configurato sull'appliance ASA e lo switch per bilanciare il carico del traffico tra le due porte.

Firepower 4125 è registrato su FMCv.

## FMCv

### Configurazione

Criterio-prefiltro:

Regola pre-filtro interna-esterna con azione Fastpath.

Oggetto interfaccia di origine: INTERNAL\_1 Oggetto interfaccia di destinazione: ESTERNO\_1.

The screenshot shows the configuration page for an access rule in FMCv. The rule name is 'Internal-External', it is enabled, and the action is 'Fastpath'. The source interface object is 'INTERNAL\_1' and the destination is 'EXTERNAL\_1'. The rule is inserted 'below rule' and has a priority of '1'. The time range is set to 'None'. The interface objects are listed as 'INTERNAL\_1' and 'EXTERNAL\_1'.

I criteri di controllo di accesso sono configurati con l'opzione consenti tutti gli elementi.

## Comportamento osservato

### Scenario 1

Traffico ICMP generato da VM-PC destinato a ISR4451-2(router) :

Il traffico ICMP ha il seguente percorso:

VM-PC — L3Switch — FPR4125 — ASA 5508 — FPR4125 — L3 Switch — Router ISR.

Nell'evento di connessione FMC viene visualizzato un solo evento di connessione, in quanto il

traffico ICMP entra ed esce attraverso la stessa coppia in linea (INSIDE-2 >>EXTERNAL2) sull'FPR 4125.

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

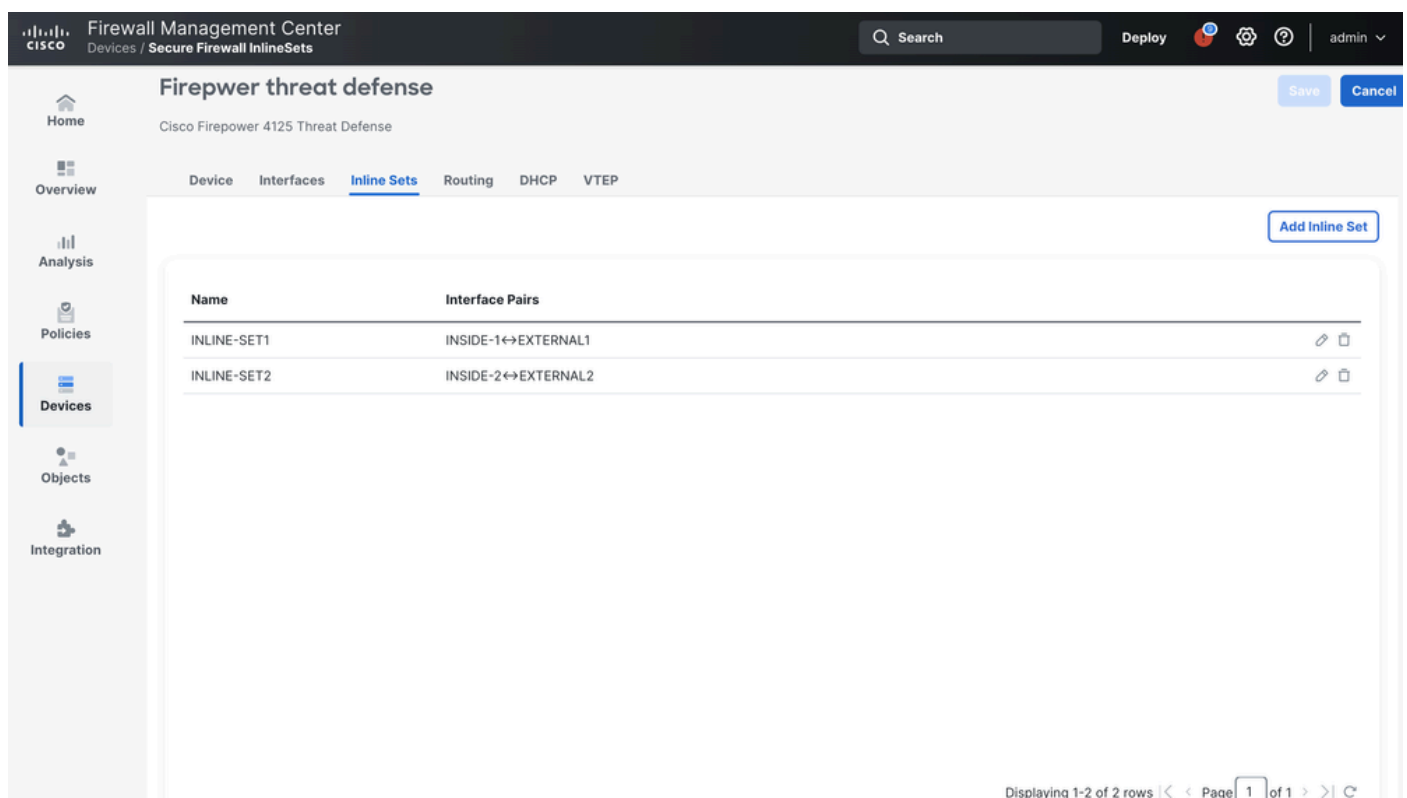
Per soddisfare il nostro requisito di ispezionare il traffico attraverso l'FTD, dovevamo configurare PBR per reindirizzare il traffico (sia le richieste che le risposte) attraverso l'FTD. Pertanto, è stato configurato il PBR sulle interfacce dello switch collegate al PC e al router.

## Scenario 2

Traffico ICMP generato da VM-PC destinato a ISR4451-2(router) :

Il traffico ICMP ha il seguente percorso:

VM-PC — L3Switch — FPR4125 — ASA 5508 — FPR4125 — L3 Switch — Router ISR.



Quando si separa la configurazione della coppia inline in due diversi insiemi Inline, come illustrato nella figura precedente. Il traffico aumenta l'FTD attraverso INSIDE-1 e passa attraverso EXTERNAL2. Vengono quindi utilizzati due set in linea.

Osservando gli eventi di connessione sul FMC vengono visualizzati due eventi di connessione, uno per il traffico in

uscita e uno per quello in entrata.

Il motivo di tale comportamento è che ogni volta che il traffico su FTD utilizza due coppie in linea diverse per lo stesso traffico, vengono sempre visualizzati due eventi di connessione sul FMC.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).