Understanding Events in Firepower Deployed in Transparent Mode

Contents

Introduction

This document describes how events are displayed when deploying FTD in transparent mode with different types of inline sets.

Objective

To clarify the behaviour of connection events in the FMC when the FTD is deployed in transparent mode with an inline-set configuration.

Topology

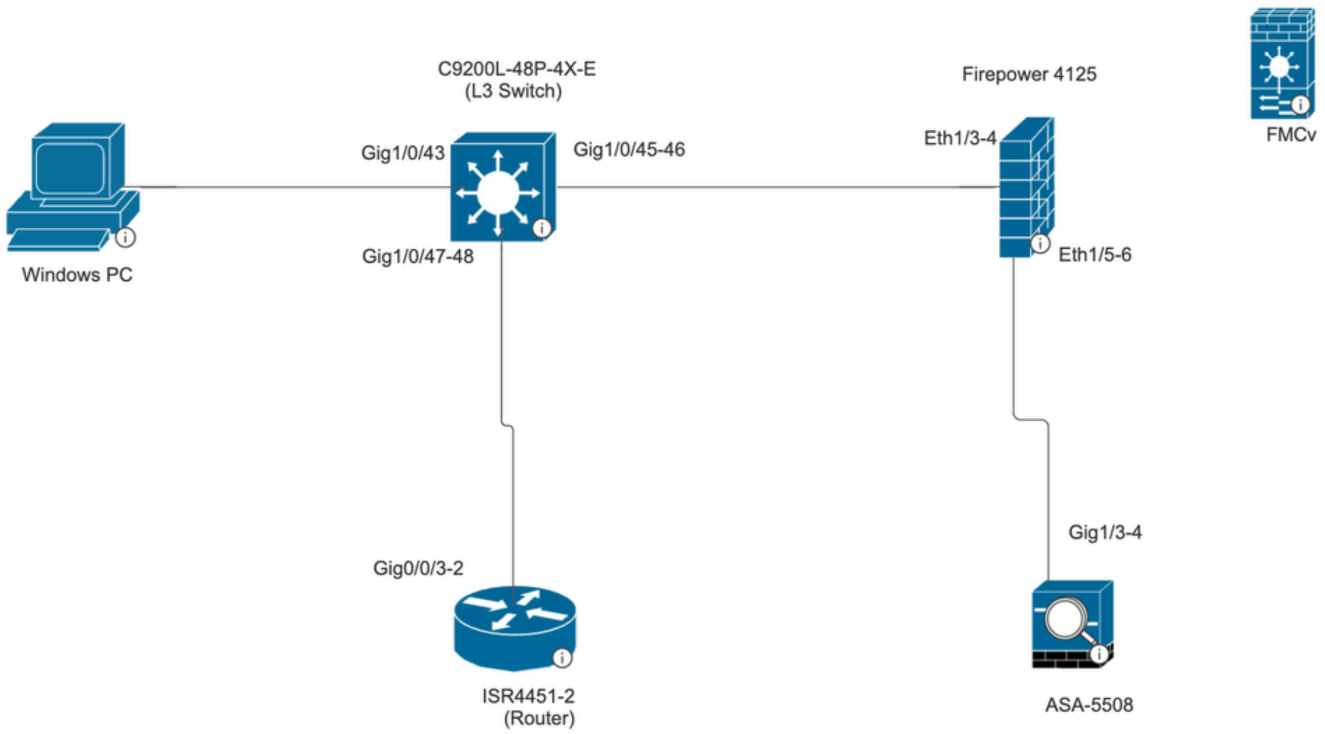


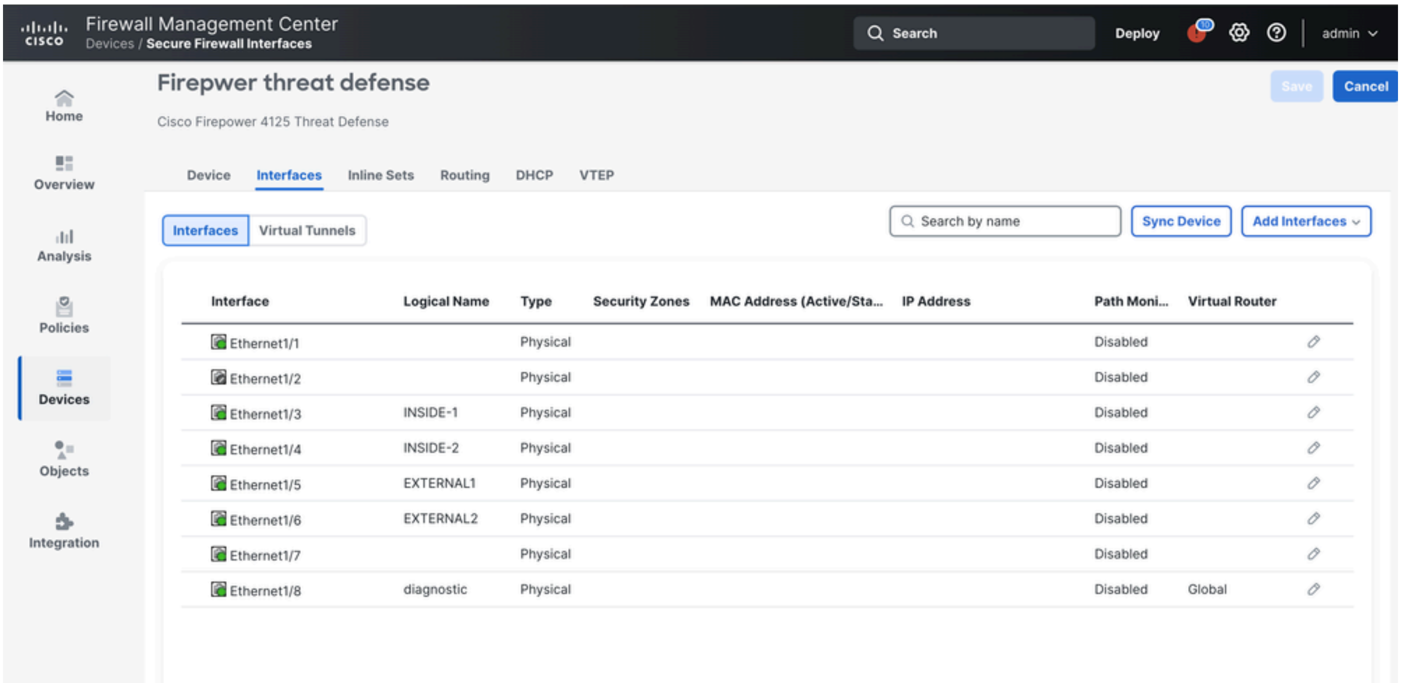
Figure 1. Topology

Components Used

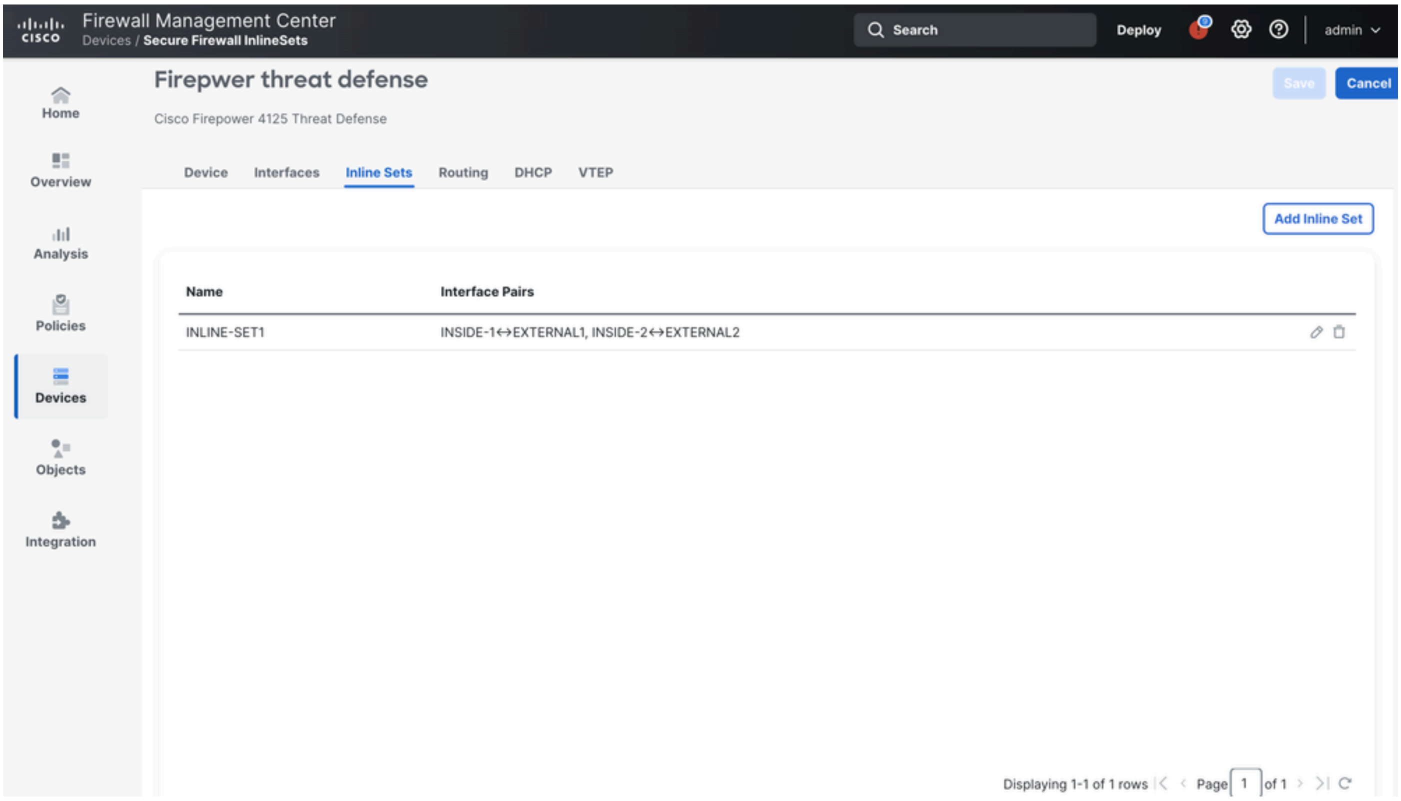
- PC-Virtual machine
- C9200L-48P-4X-E (L3 Switch)
- Firepower 4125 | 7.6
- FMCv | 7.6
- ASA 5508
- ISR4451-2 (Router)

Base Scenario

When one Inline-set configuration on Firepower 4125 contains two selected interface pairs
Ethernet 1/3 (INSIDE-1)
Ethernet 1/5 (EXTERNAL1)
Ethernet 1/4 (INSIDE-2)
Ethernet 1/6 (EXTERNAL2)



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



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

Displaying 1-1 of 1 rows Page 1 of 1

Configuration overview

L3 Switch

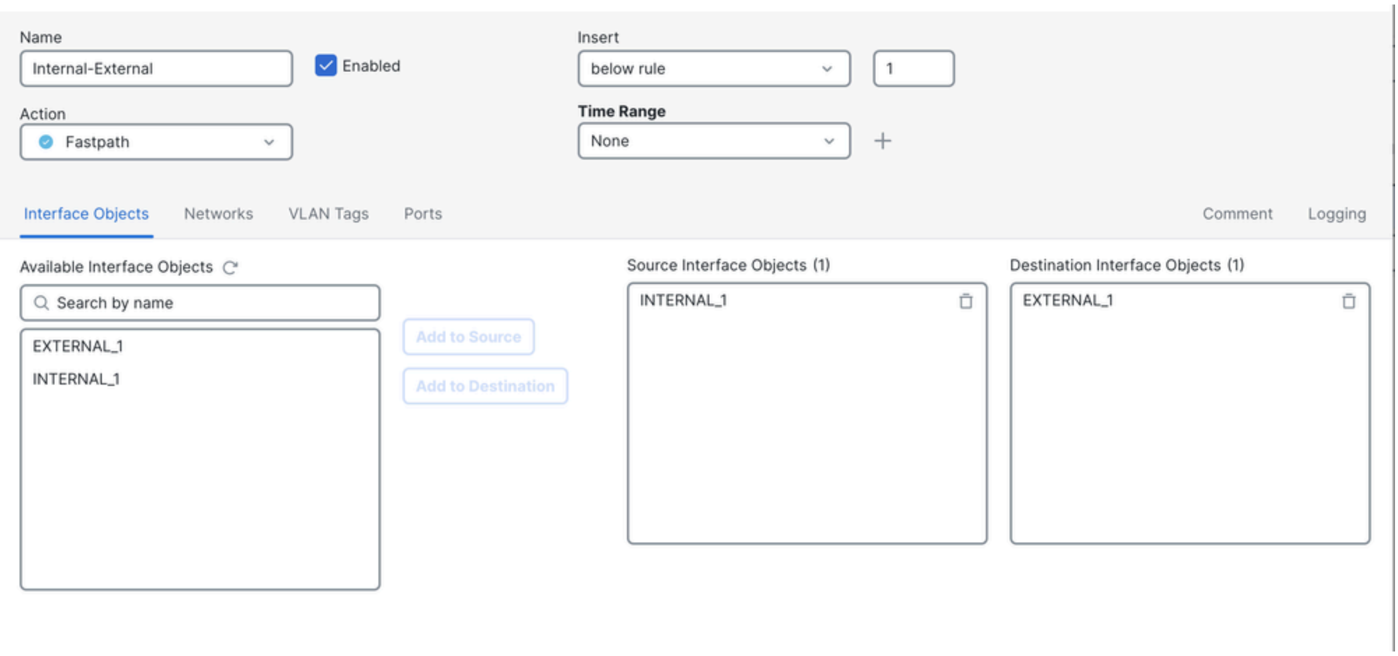
Port-channel 2 (Gig 1/0/45-46)

ASA 5508
Port-channel 2 (Gig 1/3-4)

ASA is deployed in One arm mode which means the traffic enters and exits the ASA through same port-channel which is port-channel 2.
Port-channel is configured on ASA and switch to load balance the traffic between the two.
Firepower 4125 is registered to FMCv.

FMCv

Configure
Prefilter-policy:
Pre-filter rule internal-external with action Fastpath.
Source interface object : INTERNAL_1 Destination interface object : EXTERNAL_1.



Name: Internal-External
☑ Enabled
Insert: below rule 1
Action: Fastpath
Time Range: None

Available Interface Objects: EXTERNAL_1, INTERNAL_1
Source Interface Objects (1): INTERNAL_1
Destination Interface Objects (1): EXTERNAL_1

Access Control policy is configured with allow all any-any.

Observed Behaviour

Scenario 1

ICMP Traffic generated from VM-PC destined to ISR4451-2(Router) :

ICMP traffic takes the path:

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

Only one connection event is seen in the FMC connection event because the ICMP traffic ingresses and egresses through the same inline pair (INSIDE-2 >>EXTERNAL2) on the FPR 4125.

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

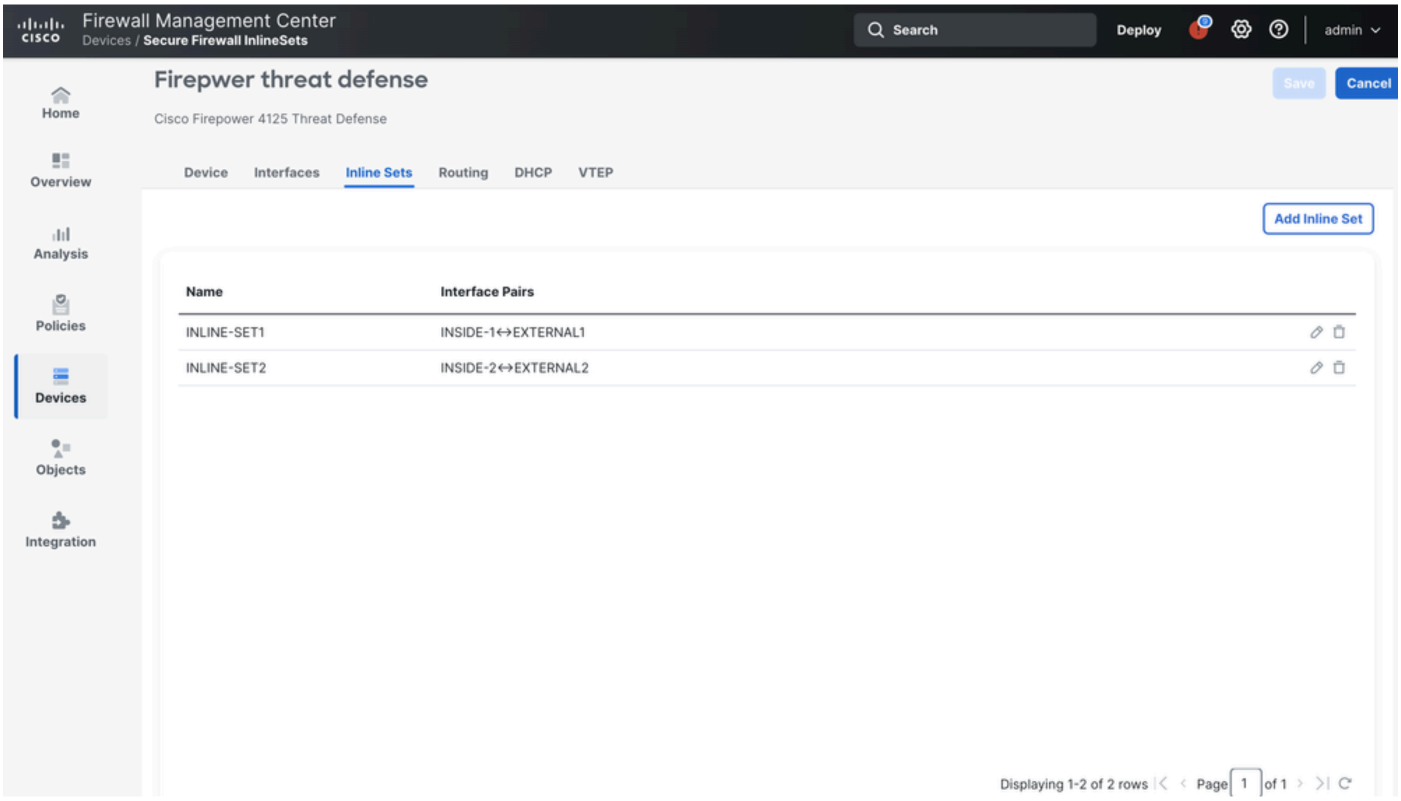
To meet our requirement of inspecting the traffic through the FTD, we needed to configure PBR to re-direct the traffic (both requests and responses) via the FTD. Therefore, we configured PBR on the switch interfaces connected to the PC and router.

Scenario 2

ICMP Traffic generated from VM-PC destined to ISR4451-2(Router) :

ICMP traffic takes the path:

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



Firepwer threat defense

Cisco Firepower 4125 Threat Defense

Name	Interface Pairs
INLINE-SET1	INSIDE-1↔EXTERNAL1
INLINE-SET2	INSIDE-2↔EXTERNAL2

When we separate the inline pair configuration in to two different Inline-sets as shown in the figure above. The traffic egresses the FTD thorugh INSIDE-1 and ingresses through EXTERNAL2.
Hence two inline-sets are utilized .

When observing the connection events on the FMC we see two connection events , one for the outgoing traffic and one for the incoming.

The reason behind such behaviour is whenever traffic on FTD utilises two different inline-pairs for the same traffic , we always see two connection events on the FMC.