

# Inzicht in gebeurtenissen in FirePOWER die in transparante modus zijn geïmplementeerd

## Inhoud

---

[Inleiding](#)

[Doel](#)

[Topologie](#)

[Gebruikte componenten](#)

[basisscenario](#)

[Configuratieoverzicht](#)

[L3-Switch](#)

[VCCv](#)

[geobserveerd gedrag](#)

[Scenario 1](#)

[Scenario 2](#)

---

## Inleiding

Dit document beschrijft hoe gebeurtenissen worden weergegeven wanneer FTD in de transparante modus wordt geïmplementeerd met verschillende typen inline sets.

## Doel

Het gedrag van verbindingsevenementen in het VCC verduidelijken wanneer de FTD in transparante modus wordt ingezet met een inline-set configuratie.

## Topologie

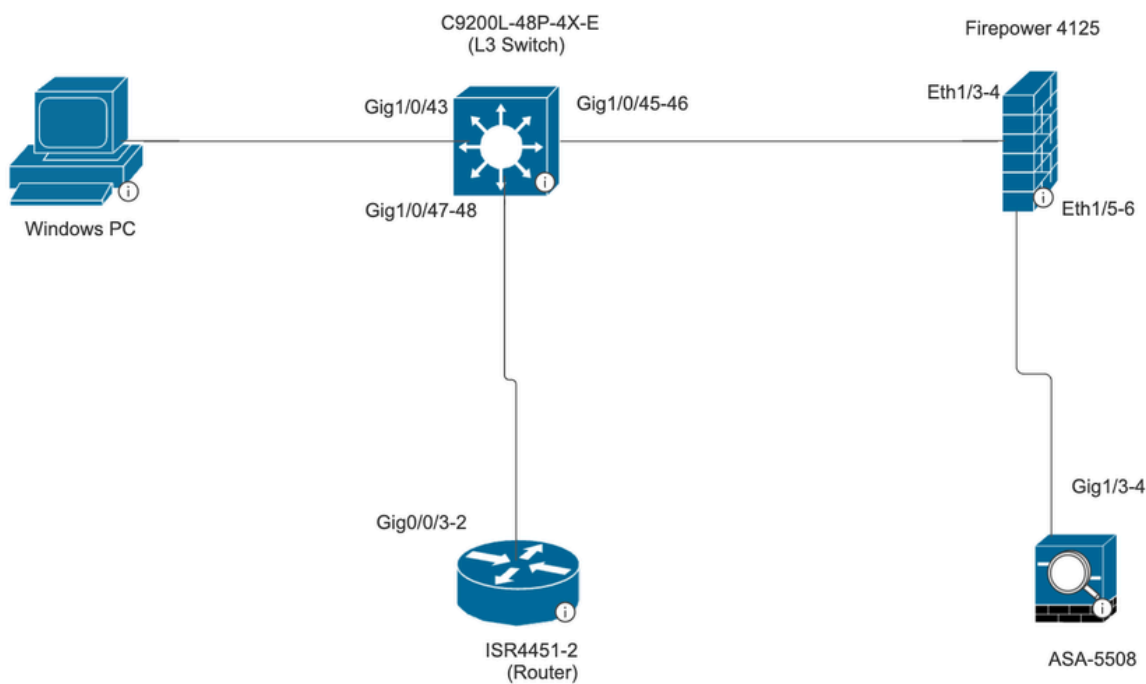


Figure 1. Topology

## Gebruikte componenten

- PC-Virtuele machine
- C9200L-48P-4X-E (L3-Switch)
- FirePOWER-applicatie 4125 | 7.6
- VCCv | 7.6
- ASA 5508 router
- ISR 4451-2 (router)

## basisscenario

Wanneer één Inline-set configuratie op Firepower 4125 twee geselecteerde interfaceparen bevat

- Ethernet 1/3 (BINNENKANT-1)
- Ethernet 1/5 (EXTERN1)
- Ethernet 1/4 (BINNENKANT-2)
- Ethernet 1/6 (EXTERN2)

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

## Configuratieoverzicht

L3-Switch

Poortkanaal 2 (Gig 1/0/45-46)

ASA 5508 router  
Poortkanaal 2 (Gig 1/3-4)

ASA wordt ingezet in de modus één arm, wat betekent dat het verkeer de ASA binnenkomt en verlaat via hetzelfde poortkanaal, namelijk poortkanaal 2.

Port-channel is geconfigureerd op ASA en switch om het verkeer tussen de twee te verdelen.  
Firepower 4125 is geregistreerd bij FMCv.

## VCCv

Configureren

Prefilterbeleid:

Pre-filter regel intern-extern met actie FastPath.

Bron-interfaceobject : Internal\_1 Doelbestemming interfaceobject : EXTERN\_1.

The screenshot shows the configuration page for a rule named "Internal-External". The rule is enabled. The action is set to "Fastpath". The "Insert" position is "below rule" and the "Time Range" is "None". Below the rule configuration, there are tabs for "Interface Objects", "Networks", "VLAN Tags", and "Ports". The "Interface Objects" tab is active, showing a search box and a list of available interface objects: "EXTERNAL\_1" and "INTERNAL\_1". There are "Add to Source" and "Add to Destination" buttons. The "Source Interface Objects (1)" list contains "INTERNAL\_1" and the "Destination Interface Objects (1)" list contains "EXTERNAL\_1".

Toegangscontrolebeleid is ingesteld op alle willekeurige opties.

## geobserveerd gedrag

### Scenario 1

ICMP-verkeer gegenereerd van VM-PC voor ISR4451-2(router) :

ICMP-verkeer volgt het pad:

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

In de FMC-verbindingsebeurtenis wordt slechts één verbindingsebeurtenis weergegeven,

omdat het ICMP-verkeer via hetzelfde inline-paar (INSIDE-2 >>EXTERNAL2) op de FPR 4125 binnendringt en uitloopt.

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

Om te voldoen aan onze eis van het inspecteren van het verkeer via de FTD, moesten we PBR configureren om het verkeer (zowel verzoeken als antwoorden) via de FTD opnieuw te sturen. Daarom hebben we PBR geconfigureerd op de switch-interfaces die zijn aangesloten op de PC en de router.

## Scenario 2

ICMP-verkeer gegenereerd van VM-PC voor ISR4451-2(router) :

ICMP-verkeer volgt het pad:

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

The screenshot shows the Cisco Firewall Management Center (FMC) interface for a Cisco Firepower 4125 Threat Defense device. The main content area displays the 'Inline Sets' configuration page. There are two inline sets listed:

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 sidebar on the left contains navigation options: Home, Overview, Analysis, Policies, Devices, Objects, and Integration. The bottom right corner indicates 'Displaying 1-2 of 2 rows | Page 1 of 1'.

Wanneer we de inline paarconfiguratie in twee verschillende inline-sets scheiden zoals in de afbeelding hierboven. Het verkeer betreft de FTD via INSIDE-1 en betreft zich via EXTERN2.

Daarom worden twee inline-sets gebruikt.

Bij de waarneming van de aansluitingen op het VCC zien we twee aansluitingen , één voor het uitgaande verkeer en één voor het inkomende verkeer.

De reden voor dit gedrag is wanneer verkeer op FTD twee verschillende inline-paren voor hetzelfde verkeer gebruikt, we altijd zien twee verbidingsgebeurtenissen op het FMC.

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.