

Noções básicas sobre eventos no Firepower implantados no modo transparente

Contents

[Introdução](#)

[Objetivo](#)

[Topologia](#)

[Componentes Utilizados](#)

[Cenário base](#)

[Visão geral sobre a configuração](#)

[Switch L3](#)

[FMCv](#)

[Comportamento observado](#)

[Cenário 1](#)

[Cenário 2](#)

Introdução

Este documento descreve como os eventos são exibidos ao implantar o FTD no modo transparente com diferentes tipos de conjuntos em linha.

Objetivo

Clarificar o comportamento dos eventos de ligação no CVP quando o DTF é implantado em modo transparente com uma configuração em linha.

Topologia

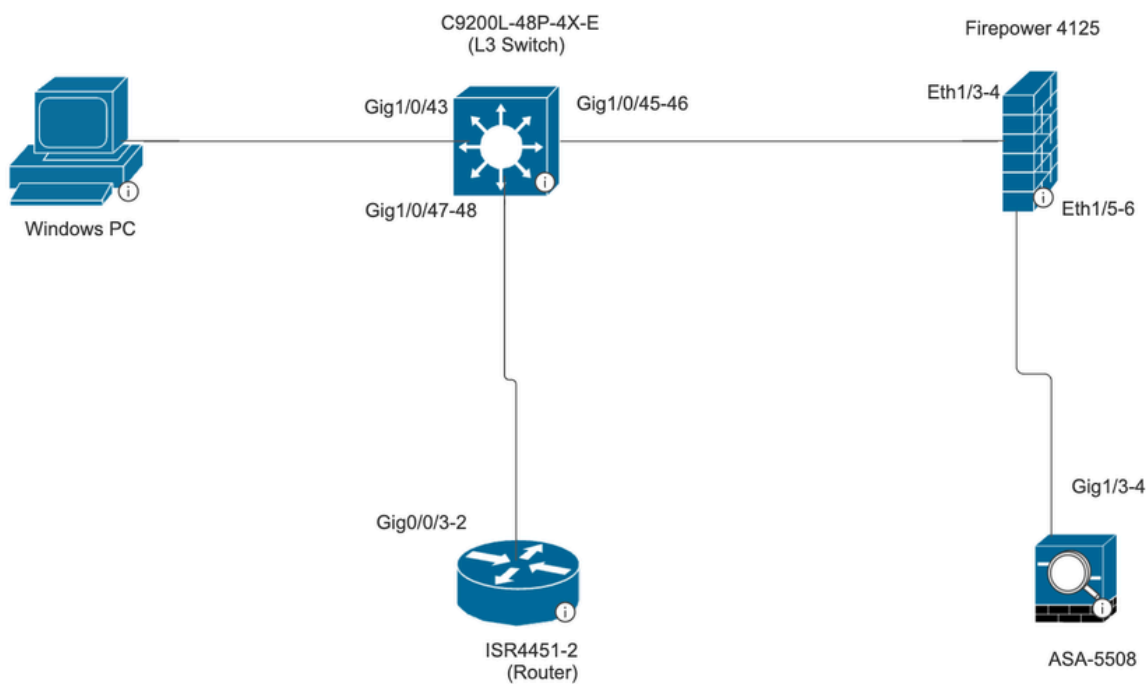


Figure 1. Topology

Componentes Utilizados

- PC-máquina virtual
- C9200L-48P-4X-E (Switch L3)
- Firepower 4125 | 7,6
- FMCv | 7,6
- ASA 5508
- ISR4451-2 (roteador)

Cenário base

Quando uma configuração em linha no Firepower 4125 contiver dois pares de interfaces selecionados
Ethernet 1/3 (INSIDE-1)
Ethernet 1/5 (EXTERNA1)
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

Visão geral sobre a configuração

Switch L3

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

ASA 5508

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

O ASA é implantado no modo de um braço, o que significa que o tráfego entra e sai do ASA através do mesmo canal de porta, que é o canal de porta 2.

O canal de porta é configurado no ASA e no switch para balancear a carga do tráfego entre os dois.

O Firepower 4125 está registrado no FMCv.

FMCv

Configurar

Política de pré-filtro:

Regra de pré-filtragem interna-externa com ação Fastpath.

Objeto de interface de origem: INTERNAL_1 Objeto de interface de destino : EXTERNAL_1.

The screenshot shows the configuration page for a rule in the FMCv interface. The rule is named 'Internal-External' and is currently enabled. The action is set to 'Fastpath'. The source interface object is 'INTERNAL_1' and the destination interface object is 'EXTERNAL_1'. The rule is configured to be 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'.

A política de controle de acesso é configurada com permitir todos, qualquer um.

Comportamento observado

Cenário 1

Tráfego ICMP gerado de VM-PC destinado a ISR4451-2(roteador) :

O tráfego ICMP segue o caminho:

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

Apenas um evento de conexão é visto no evento de conexão FMC porque o tráfego ICMP entra e sai através do mesmo par em linha (INSIDE-2 >>EXTERNAL2) no FPR 4125.

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

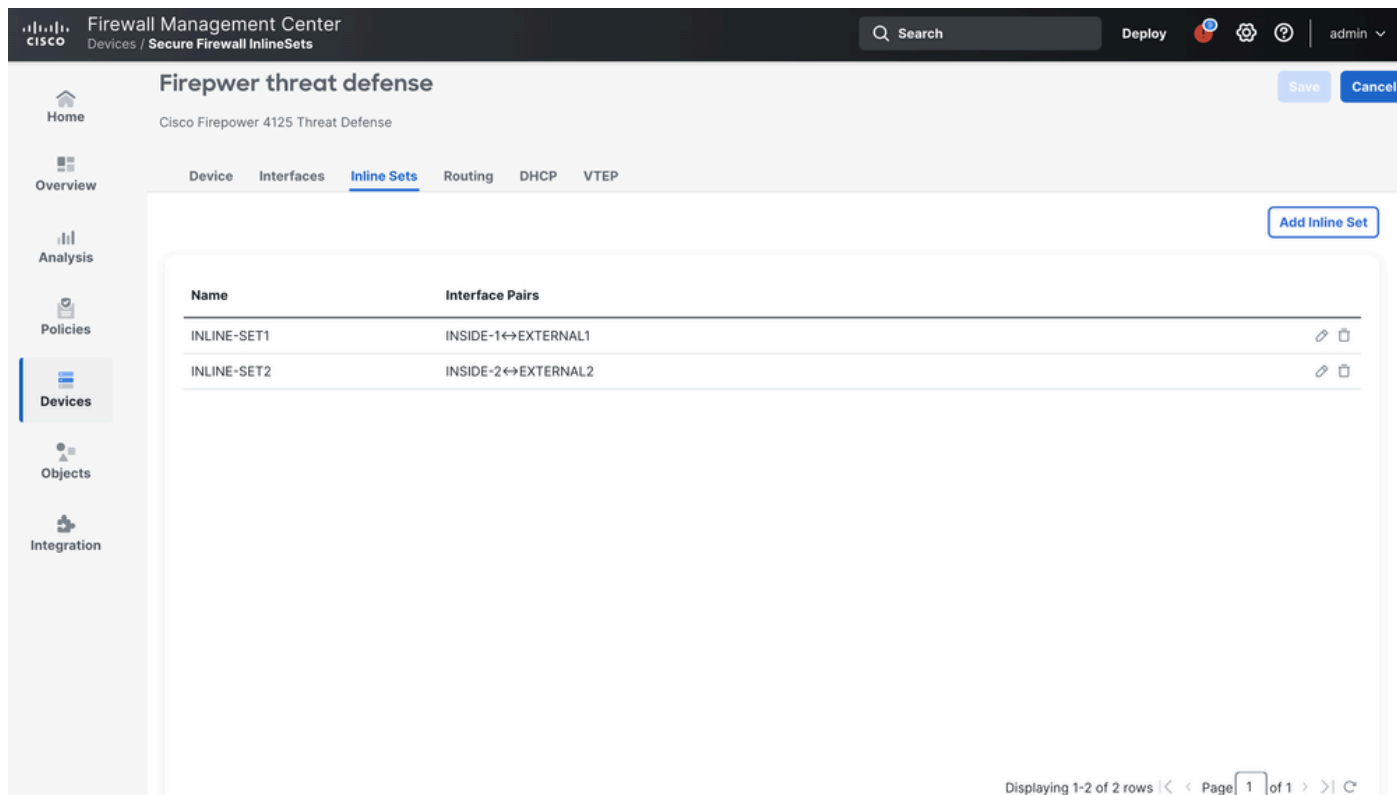
Para atender à nossa exigência de inspeção do tráfego por meio do FTD, precisamos configurar o PBR para redirecionar o tráfego (solicitações e respostas) por meio do FTD. Portanto, configuramos o PBR nas interfaces do switch conectadas ao PC e ao roteador.

Cenário 2

Tráfego ICMP gerado de VM-PC destinado a ISR4451-2(roteador) :

O tráfego ICMP segue o caminho:

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



The screenshot shows the Cisco Firewall Management Center (FMC) interface for 'Firepower threat defense'. The main content area displays a table of inline sets:

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

At the bottom of the page, it indicates 'Displaying 1-2 of 2 rows | Page 1 of 1'.

Quando separamos a configuração de par em linha em dois conjuntos em linha diferentes, como mostrado na figura acima. O tráfego sai do FTD através do INSIDE-1 e entra através do EXTERNAL2. Portanto, dois conjuntos em linha são utilizados .

Ao observar os eventos de conexão no FMC, vemos dois eventos de conexão , um para o tráfego de saída e outro para o de entrada.

A razão por trás de tal comportamento é sempre que o tráfego no FTD utiliza dois pares em linha diferentes para o mesmo tráfego , sempre vemos dois eventos de conexão no FMC.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.