Présentation des événements dans Firepower déployé en mode transparent

Table des matières

Introduction

Ce document décrit comment les événements sont affichés lors du déploiement de FTD en mode transparent avec différents types de jeux en ligne.

Objectif

Clarifier le comportement des événements de connexion dans le FMC lorsque le FTD est déployé en mode transparent avec une configuration en ligne.

Topologie

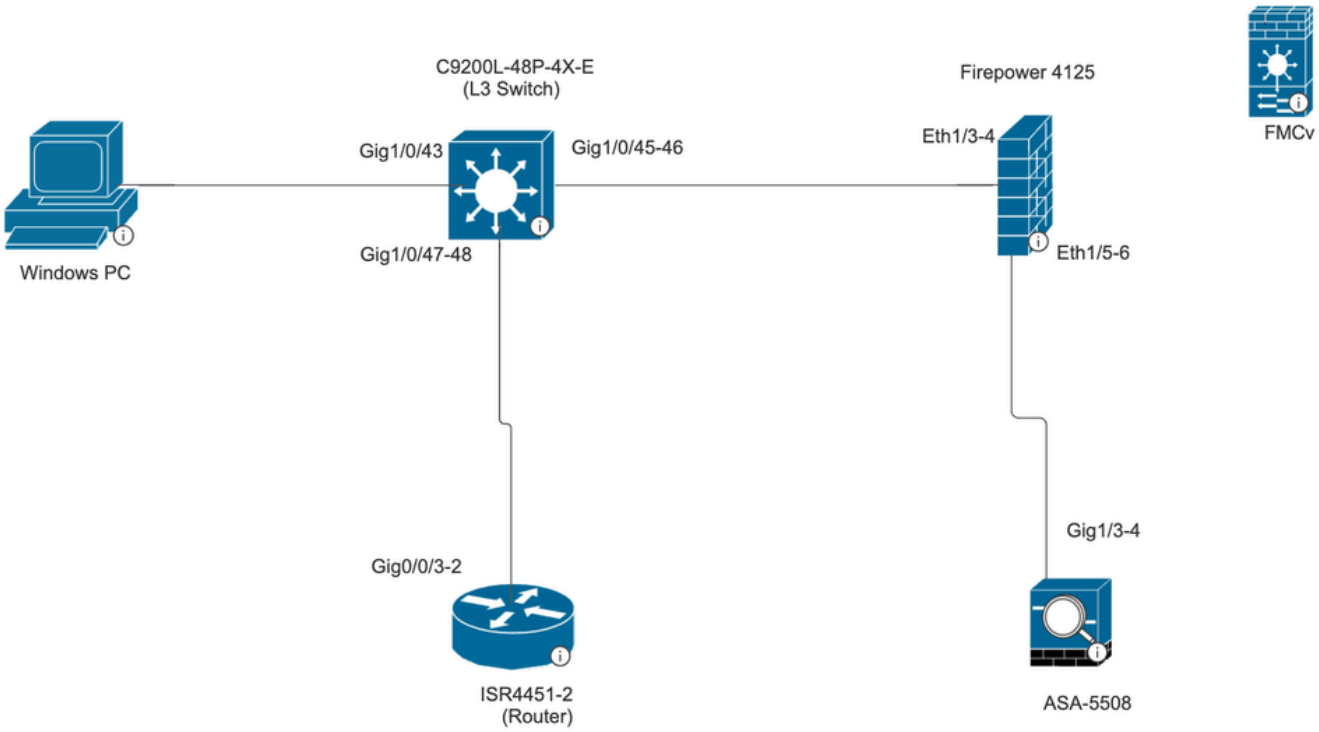


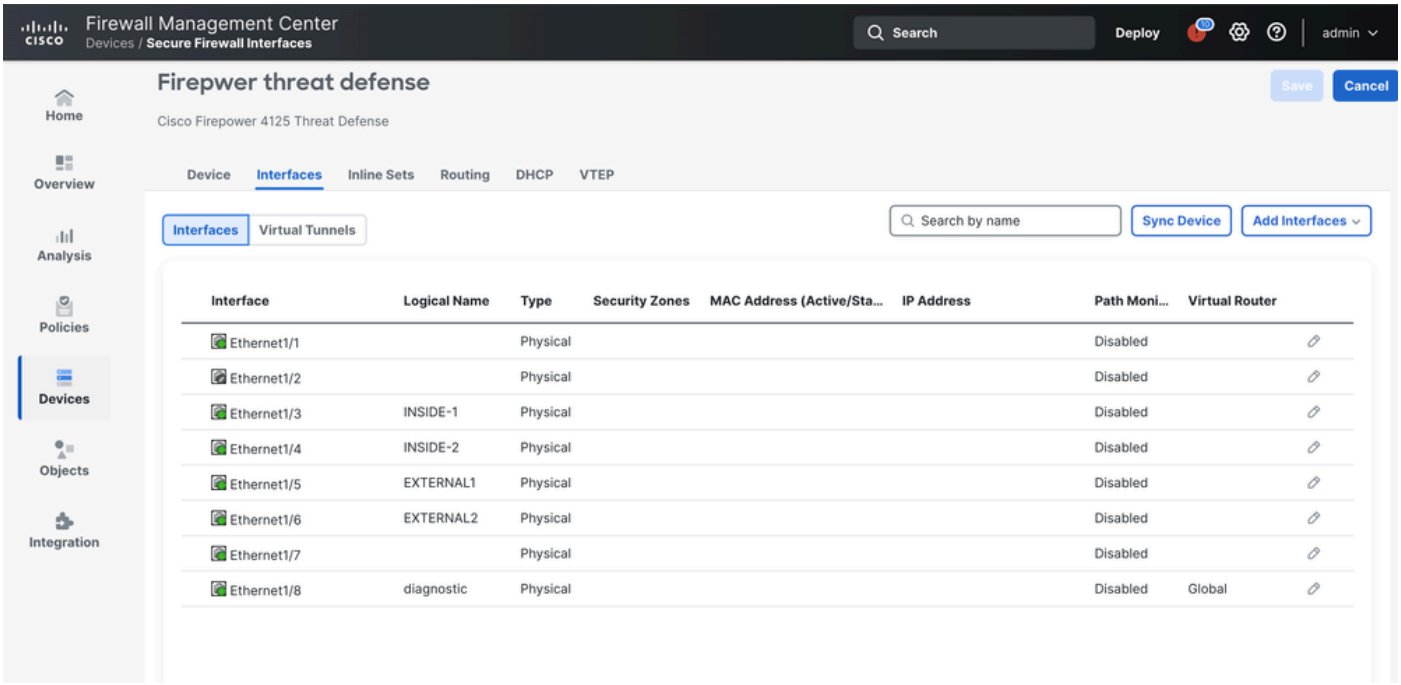
Figure 1. Topology

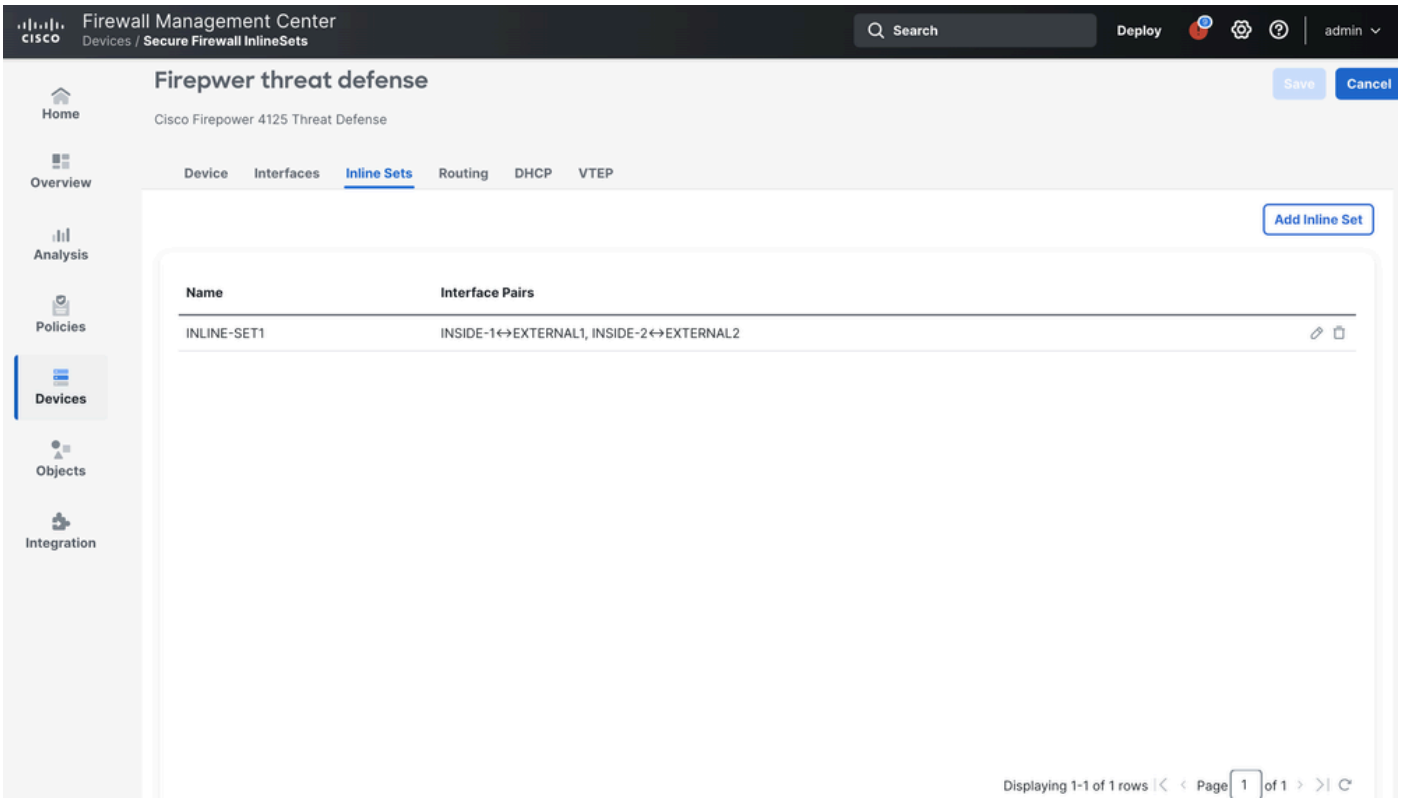
Composants utilisés

- PC-Machine virtuelle
- C9200L-48P-4X-E (commutateur L3)
- Firepower 4125 | 7,6
- FMCv | 7,6
- ASA 5508
- ISR4451-2 (routeur)

Scénario de base

Lorsqu'une configuration Inline-set sur Firepower 4125 contient deux paires d'interfaces sélectionnées
Ethernet 1/3 (INSIDE-1)
Ethernet 1/5 (EXTERNE1)
Ethernet 1/4 (INTERNE-2)
Ethernet 1/6 (EXTERNE2)





Présentation de la configuration

Commutateur L3

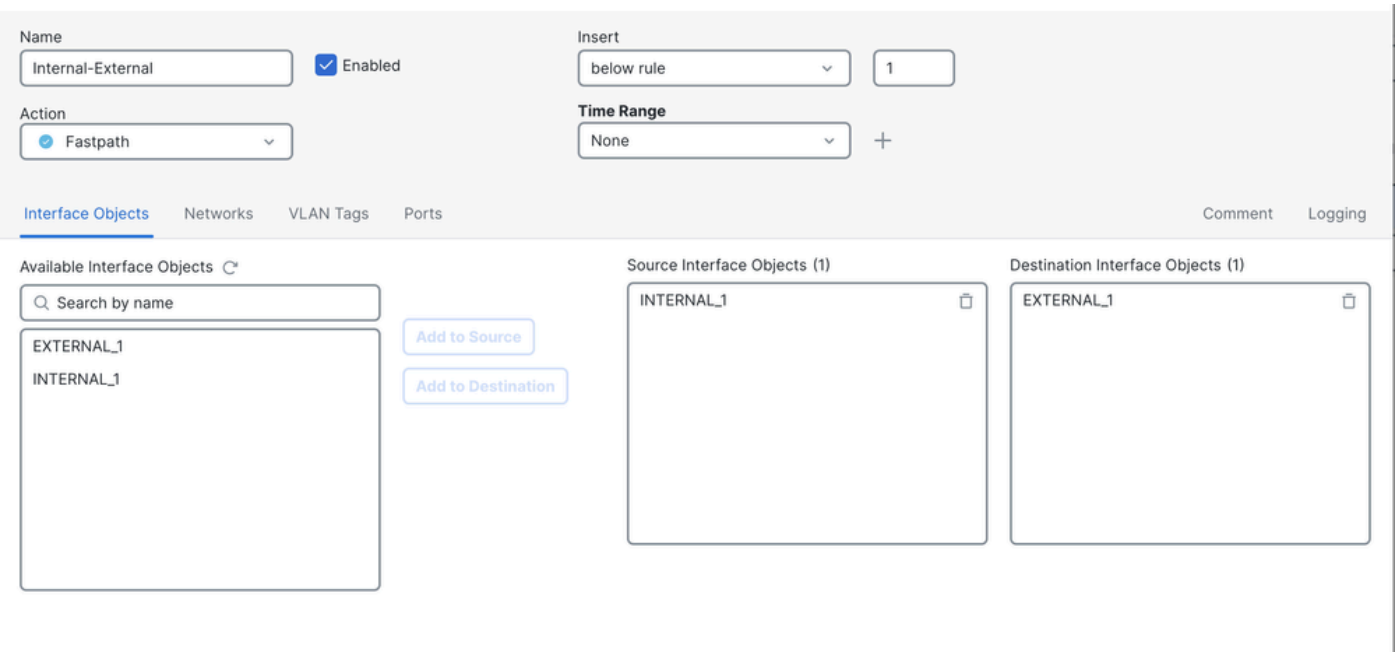
Port-channel 2 (Gig 1/0/45-46)

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

ASA est déployé en mode Un bras, ce qui signifie que le trafic entre et sort de l'ASA par le même port-channel qui est le port-channel 2.
Port-channel est configuré sur ASA et le commutateur pour équilibrer la charge du trafic entre les deux.
Firepower 4125 est enregistré auprès de FMCv.

FMCv

Configurer
Politique de préfiltrage :
Règle de préfiltrage interne-externe avec action FastPath.
Objet interface source : INTERNAL_1 Objet interface de destination : EXTERNE_1.



La stratégie de contrôle d'accès est configurée avec l'option autoriser tous les accès sans restriction.

Comportement observé

Scénario 1

Trafic ICMP généré à partir de VM-PC destiné à ISR4451-2(Router) :

Le trafic ICMP emprunte le chemin suivant :

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

Un seul événement de connexion est vu dans l'événement de connexion FMC, car le trafic ICMP entre et sort par la même paire en ligne (INSIDE-2 >>EXTERNAL2) sur le FPR 4125.

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

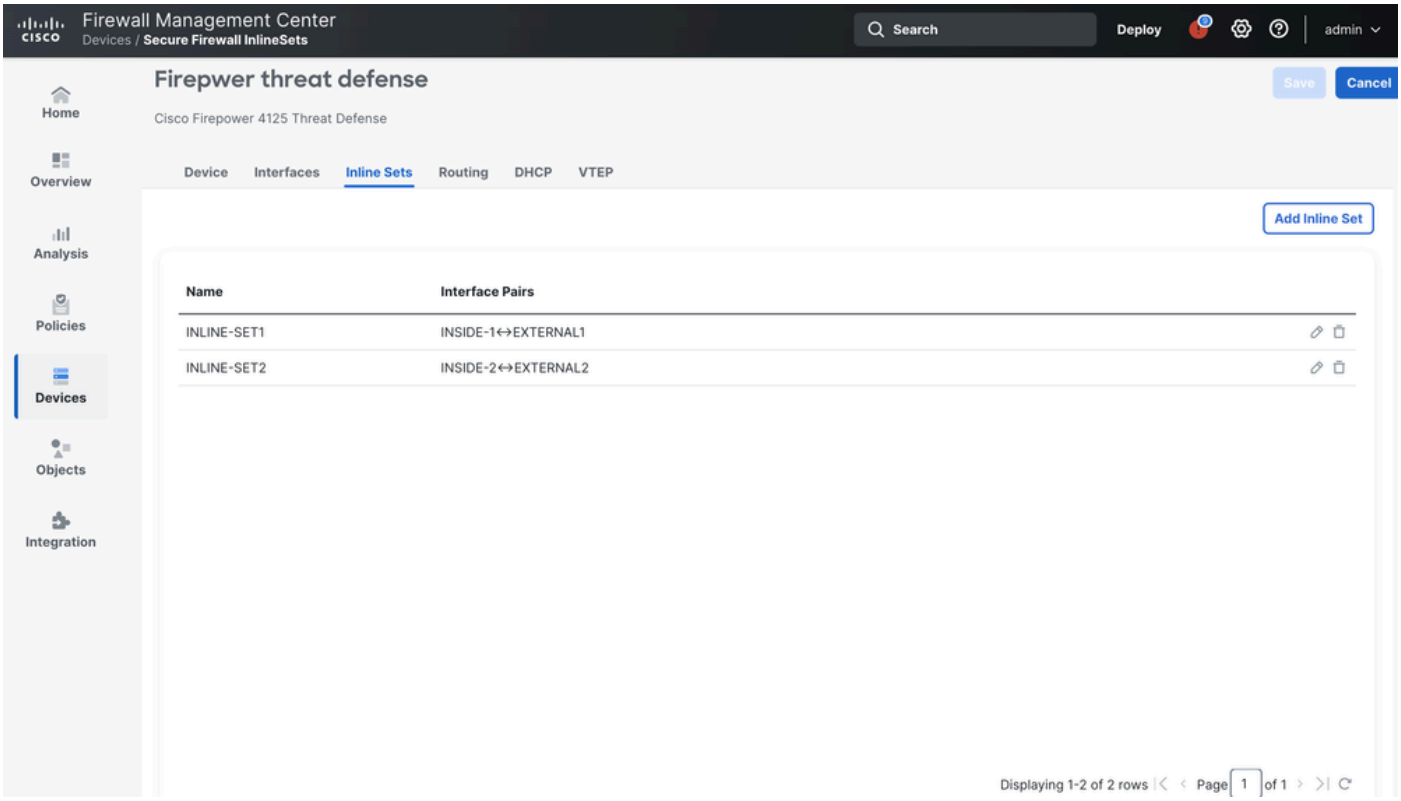
Pour répondre à notre exigence d'inspection du trafic via le FTD, nous devions configurer PBR pour rediriger le trafic (à la fois les requêtes et les réponses) via le FTD. Par conséquent, nous avons configuré PBR sur les interfaces de commutateur connectées au PC et au routeur.

Scénario 2

Trafic ICMP généré à partir de VM-PC destiné à ISR4451-2(Router) :

Le trafic ICMP emprunte le chemin suivant :

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



Lorsque nous séparons la configuration de la paire en ligne en deux jeux en ligne différents, comme illustré dans la figure ci-dessus. Le trafic sort du FTD via INSIDE-1 et entre via EXTERNAL2.

On utilise donc deux ensembles en ligne .

En observant les événements de connexion sur le FMC, nous voyons deux événements de connexion , un pour le trafic sortant et un pour le trafic entrant.

La raison derrière un tel comportement est chaque fois que le trafic sur FTD utilise deux paires en ligne différentes pour le même trafic , nous voyons toujours deux événements de connexion sur le FMC.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.