瞭解以透明模式部署的Firepower中的事件

目錄

簡介

本檔案介紹以透明模式部署具有不同內嵌集型別的FTD時，如何顯示事件。

目標

使用內嵌集組態以透明模式部署FTD時，澄清FMC中連線事件的行為。

拓撲

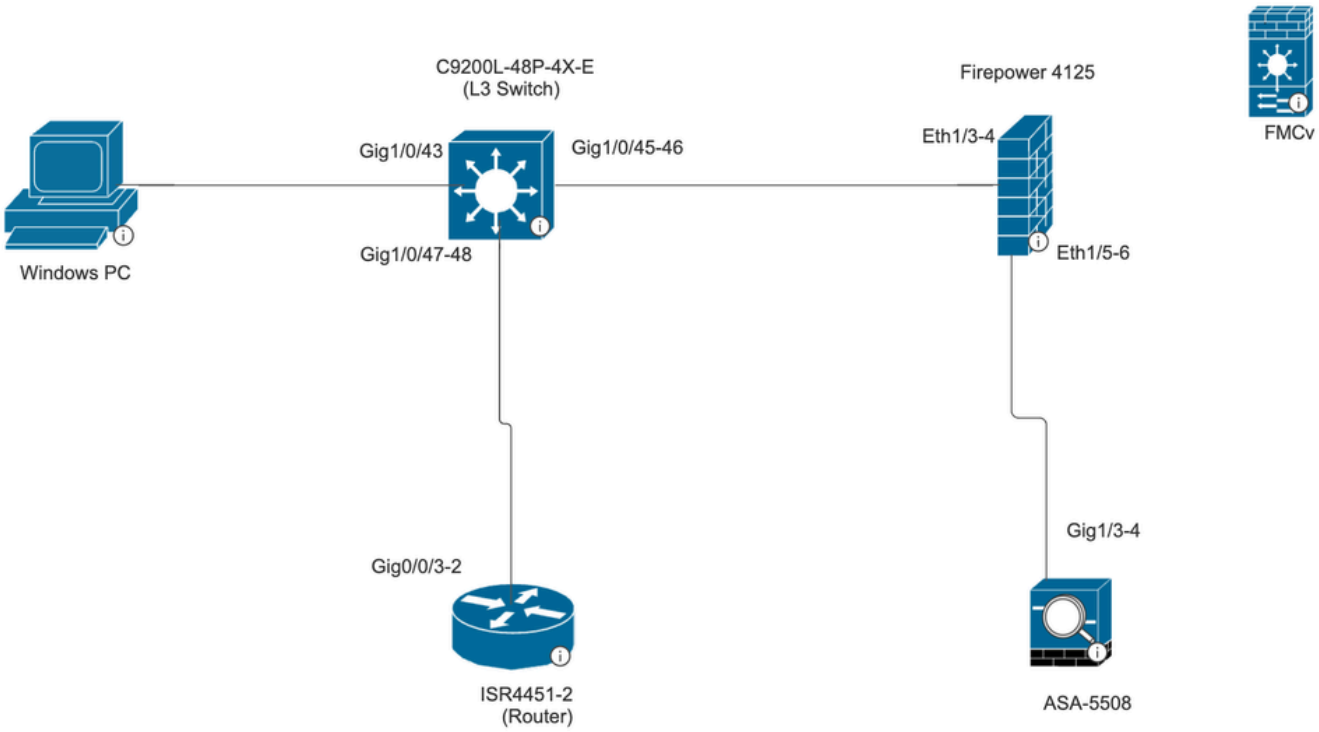


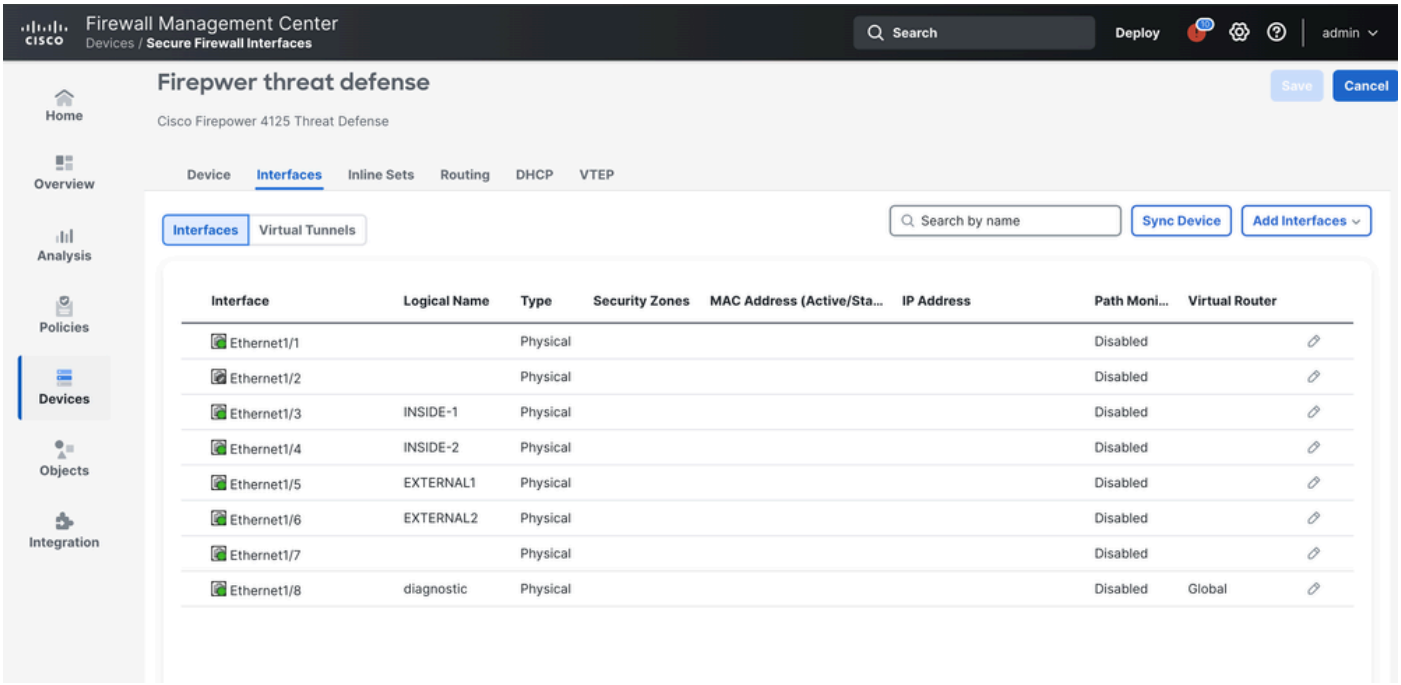
Figure 1. Topology

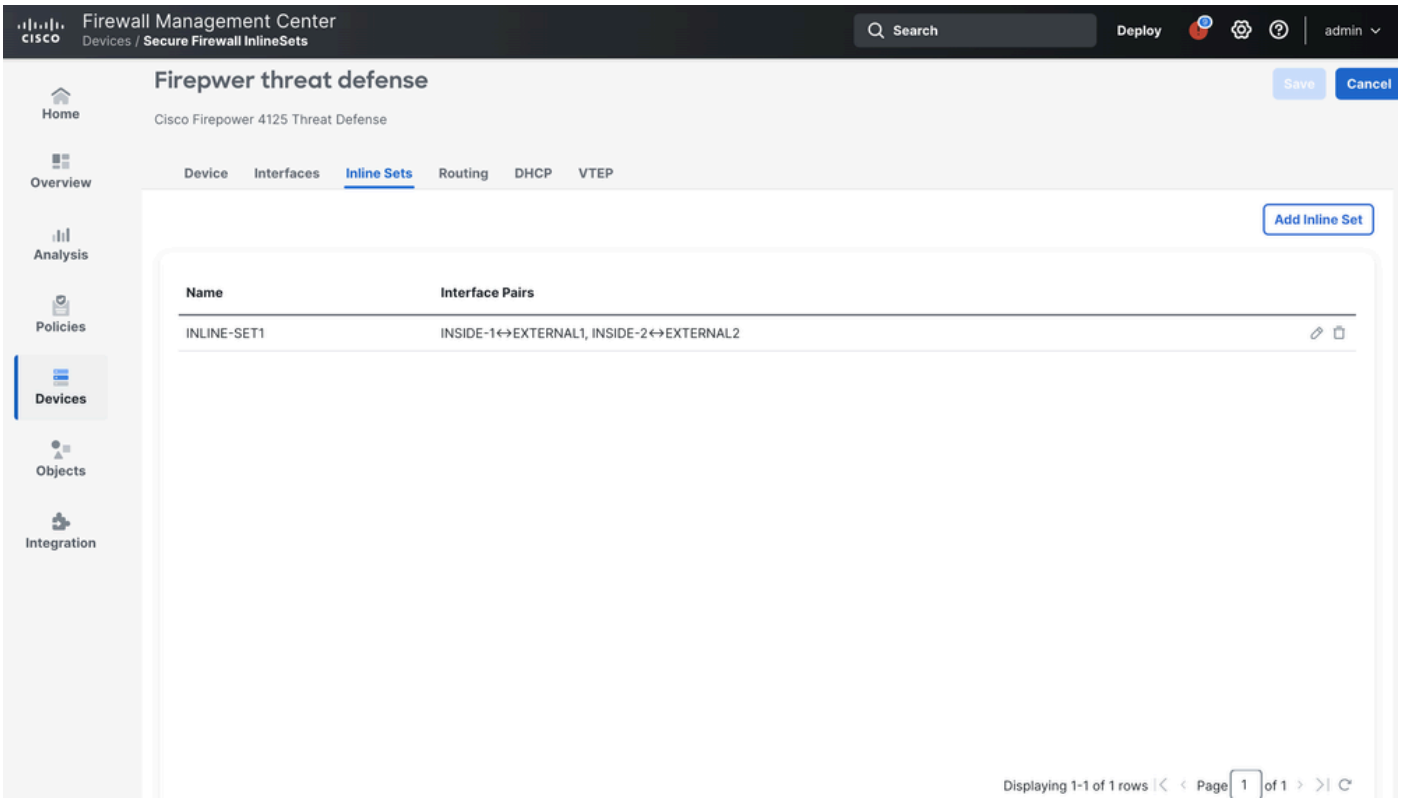
採用元件

- PC虛擬機器
- C9200L-48P-4X-E（L3交換器）
- Firepower 4125 | 7.6
- FMCv | 7.6
- ASA 5508
- ISR4451-2（路由器）

基本方案

當Firepower 4125上的一個內聯集配置包含兩個選定的介面對時
Ethernet 1/3(INSIDE-1)
Ethernet 1/5(EXTERNAL1)
Ethernet 1/4(INSIDE-2)
Ethernet 1/6(EXTERNAL2)





配置概述

L3交換機

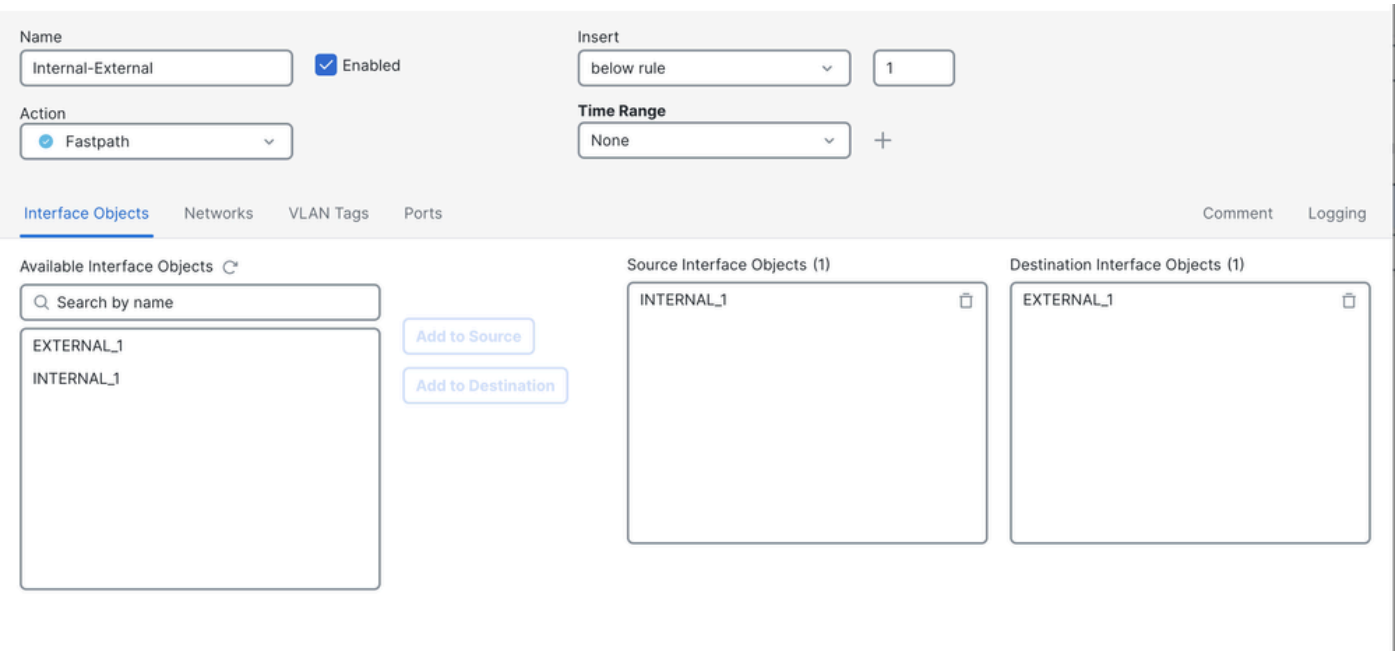
埠通道2(Gig 1/0/45-46)

ASA 5508
埠通道2(Gig 1/3-4)

ASA以單臂模式部署，這意味著流量通過與port-channel 2相同的埠通道進入和退出ASA。
在ASA和交換機上配置埠通道以平衡兩者之間的流量。
Firepower 4125已註冊到FMCv。

FMCv

設定
Prefilter-policy:
使用操作Fastpath預篩選規則internal-external。
源介面對象：INTERNAL_1目標介面對象：EXTERNAL_1。



訪問控制策略配置為allow all any-any。

觀察到的行為

案例 1

從VM-PC產生的發往ISR4451-2（路由器）的ICMP流量：

ICMP流量採用路徑：

VM-PC ------ L3交換機------- FPR4125 ------- ASA 5508 ------FPR4125 ------ L3交換機---- ISR路由器。

由於ICMP流量通過FPR 4125上的相同內嵌配對(INSIDE-2 >>EXTERNAL2)傳入和傳出，因此在FMC連線事件中只能看到一個連線事件。

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

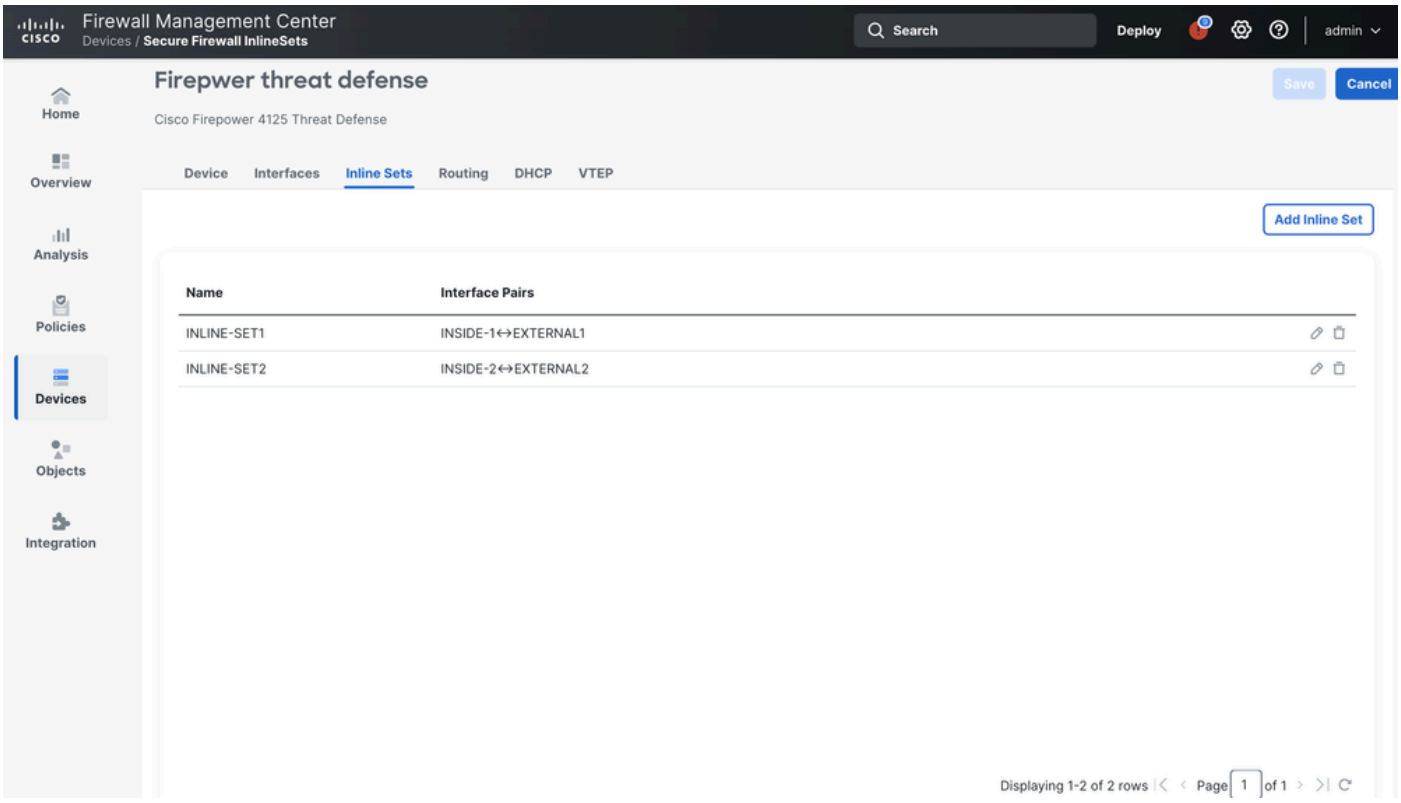
為了滿足我們檢查通過FTD的流量的要求，我們需要配置PBR以通過FTD重新定向流量（包括請求和響應）。因此，我們在連線到PC和路由器的交換機介面上配置了PBR。

案例 2

從VM-PC產生的發往ISR4451-2（路由器）的ICMP流量：

ICMP流量採用路徑：

VM-PC ------ L3交換機------- FPR4125 ------- ASA 5508 ------FPR4125 ------ L3交換機---- ISR路由器。



將內嵌配對組態分隔成兩個不同的內嵌集時，如上圖所示。流量通過INSIDE-1從FTD進入，並通過EXTERNAL2進入。
因此，使用了兩個內嵌集。

觀察FMC上的連線事件時，我們看到兩個連線事件，一個用於傳出流量，另一個用於傳入流量。

出現此行為的原因在於，每當FTD上的流量針對相同流量使用兩個不同的內嵌配對（我們總是在FMC上看到兩個連線事件）。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。