了解以透明模式部署的Firepower中的事件

目录

简介

目标

拓扑

使用的组件

基本场景

配置概述

- L3交换机
- FMCv

观察到的行为

- 场景 1
- 场景 2

简介

本文档介绍在透明模式下使用不同类型的内联集部署FTD时如何显示事件。

目标

当FTD以透明模式部署且使用内联集配置时，在FMC中明确连接事件的行为。

拓扑

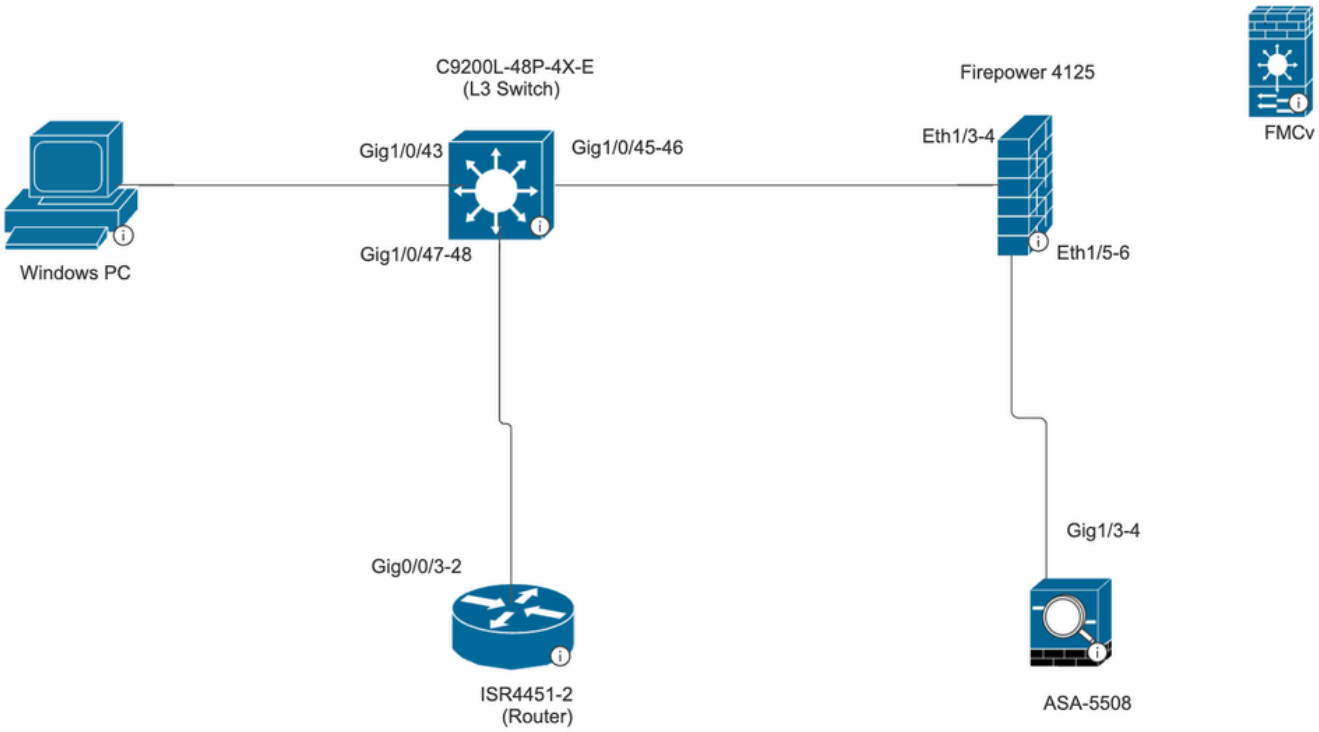


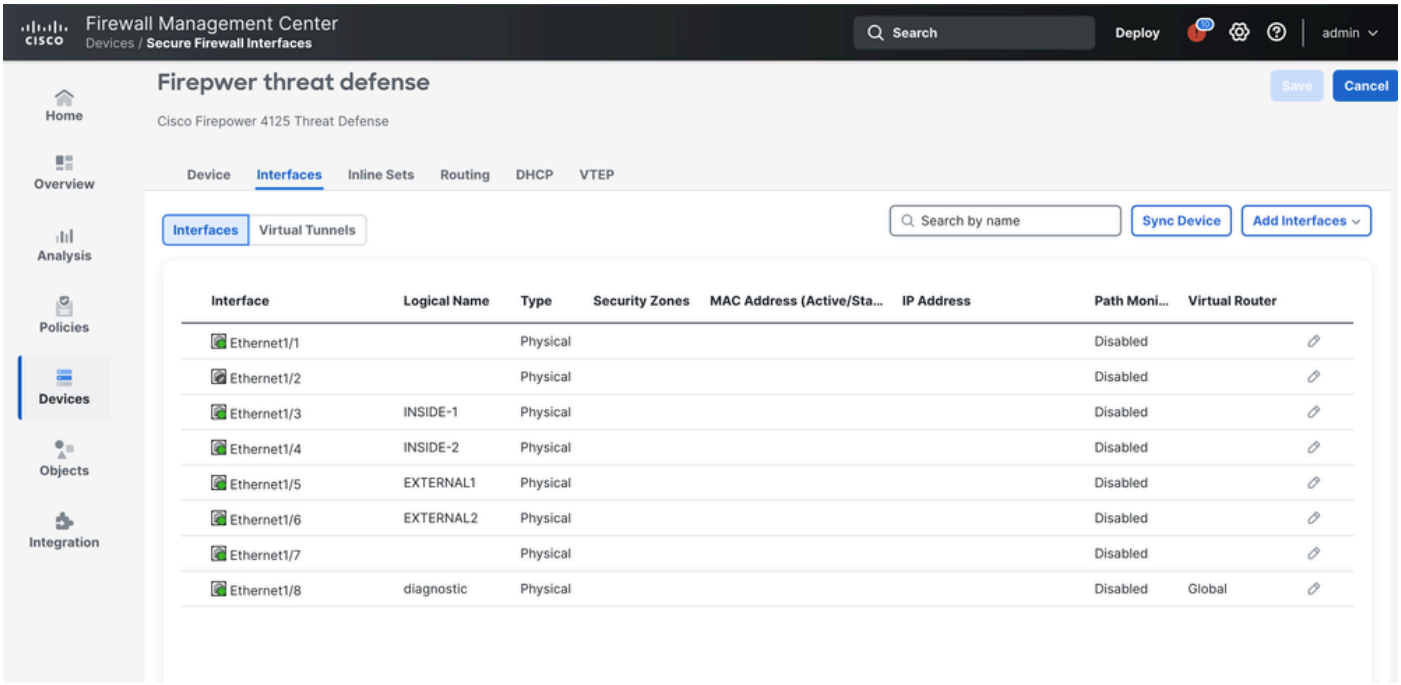
Figure 1. Topology

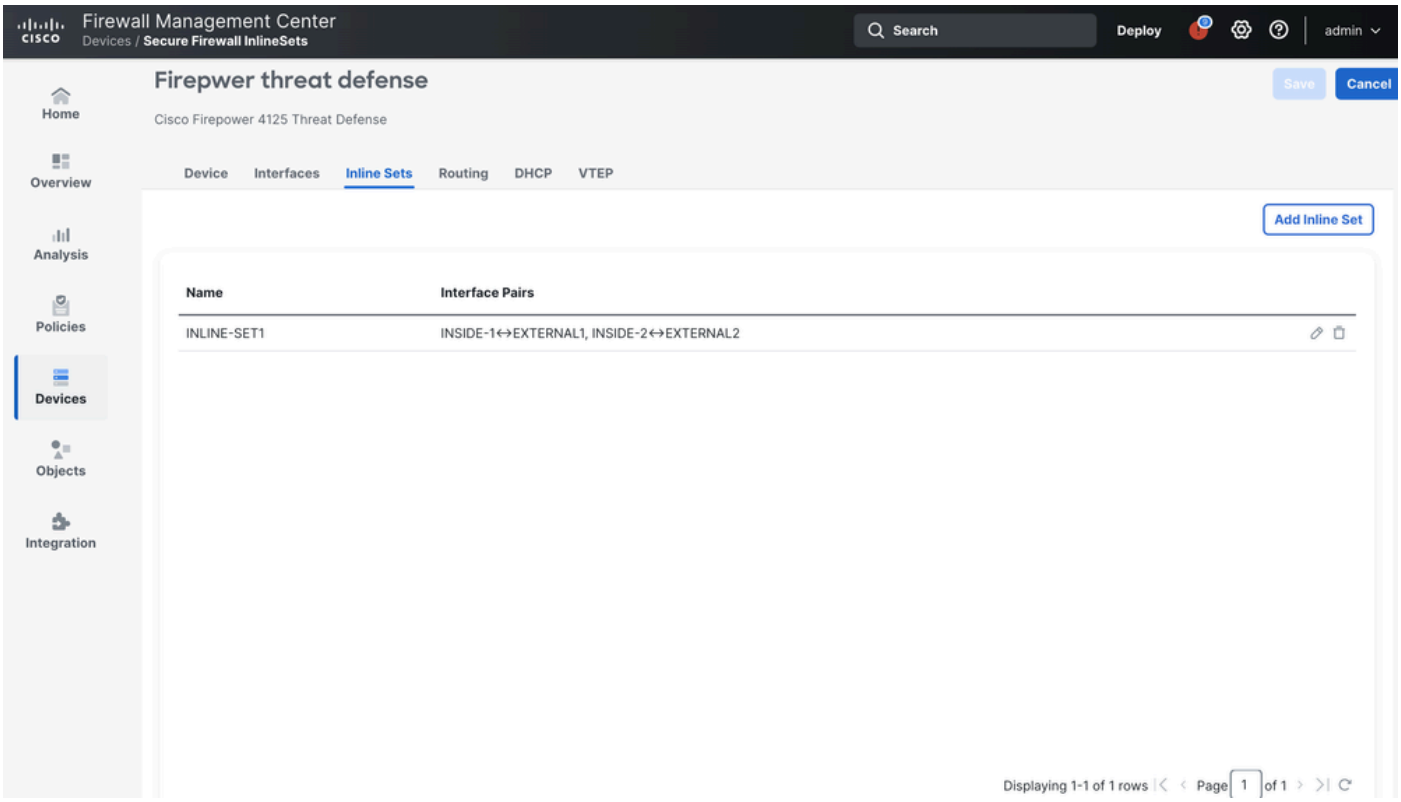
使用的组件

- PC虚拟机
- C9200L-48P-4X-E（L3交换机）
- Firepower 4125 | 7.6
- FMCv | 7.6
- ASA 5508
- ISR4451-2（路由器）

基本场景

当Firepower 4125上的一个内联集配置包含两个选定的接口对时
以太网1/3（内部–1）
以太网1/5（外部1）
以太网1/4（内部–2）
以太网1/6（外部2）





配置概述

L3交换机

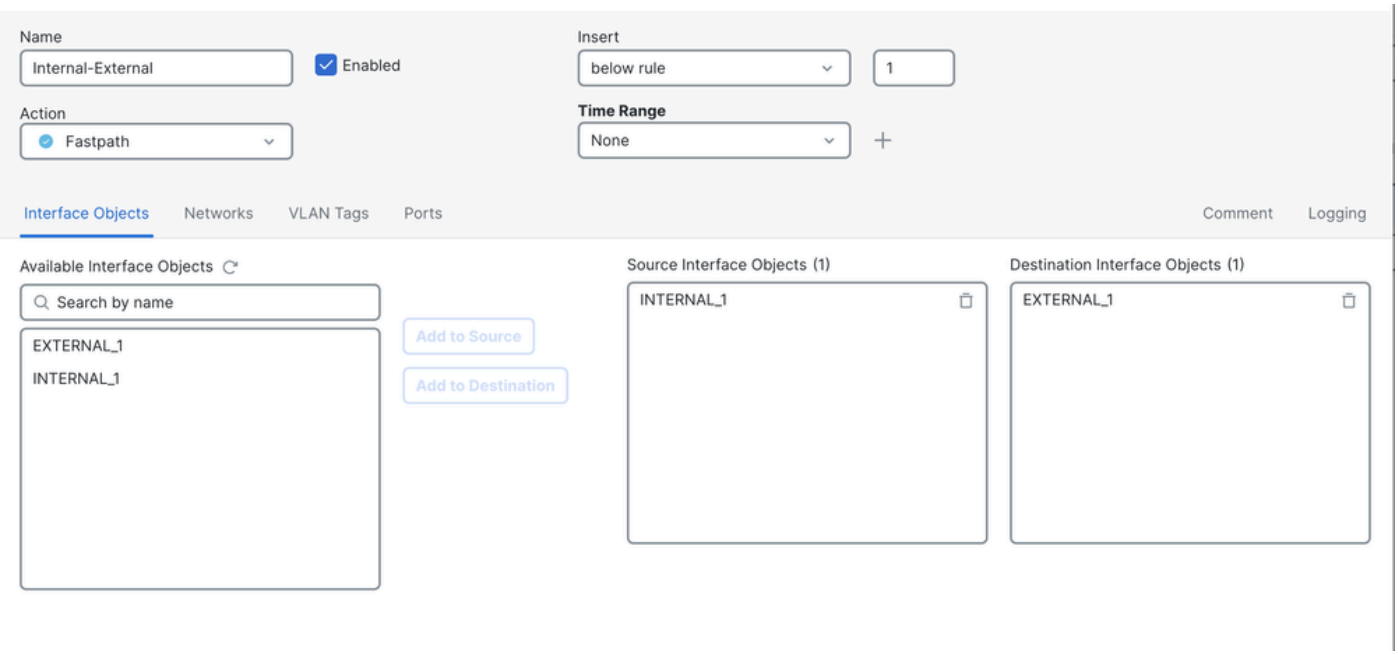
端口通道2(Gig 1/0/45-46)

ASA 5508
端口通道2(Gig 1/3-4)

ASA以单臂模式部署，这意味着流量通过与port-channel 2相同的端口通道进出ASA。
在ASA和交换机上配置端口通道，以在两者之间对流量进行负载均衡。
Firepower 4125已注册到FMCv。

FMCv

配置
预过滤器策略：
使用操作Fastpath预过滤规则内部 — 外部。
源接口对象：INTERNAL_1目标接口对象：EXTERNAL_1。



访问控制策略配置为allow all any-any。

观察到的行为

场景 1

从VM-PC生成的发往ISR4451-2（路由器）的ICMP流量：

ICMP流量采用以下路径：

VM-PC ------ L3交换机------- FPR4125 ------- ASA 5508 ------FPR4125 ------ L3交换机----ISR路由器。

在FMC连接事件中只能看到一个连接事件，因为ICMP流量通过FPR 4125上的同一内联对(INSIDE-2 >>EXTERNAL2)进入和退出。

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

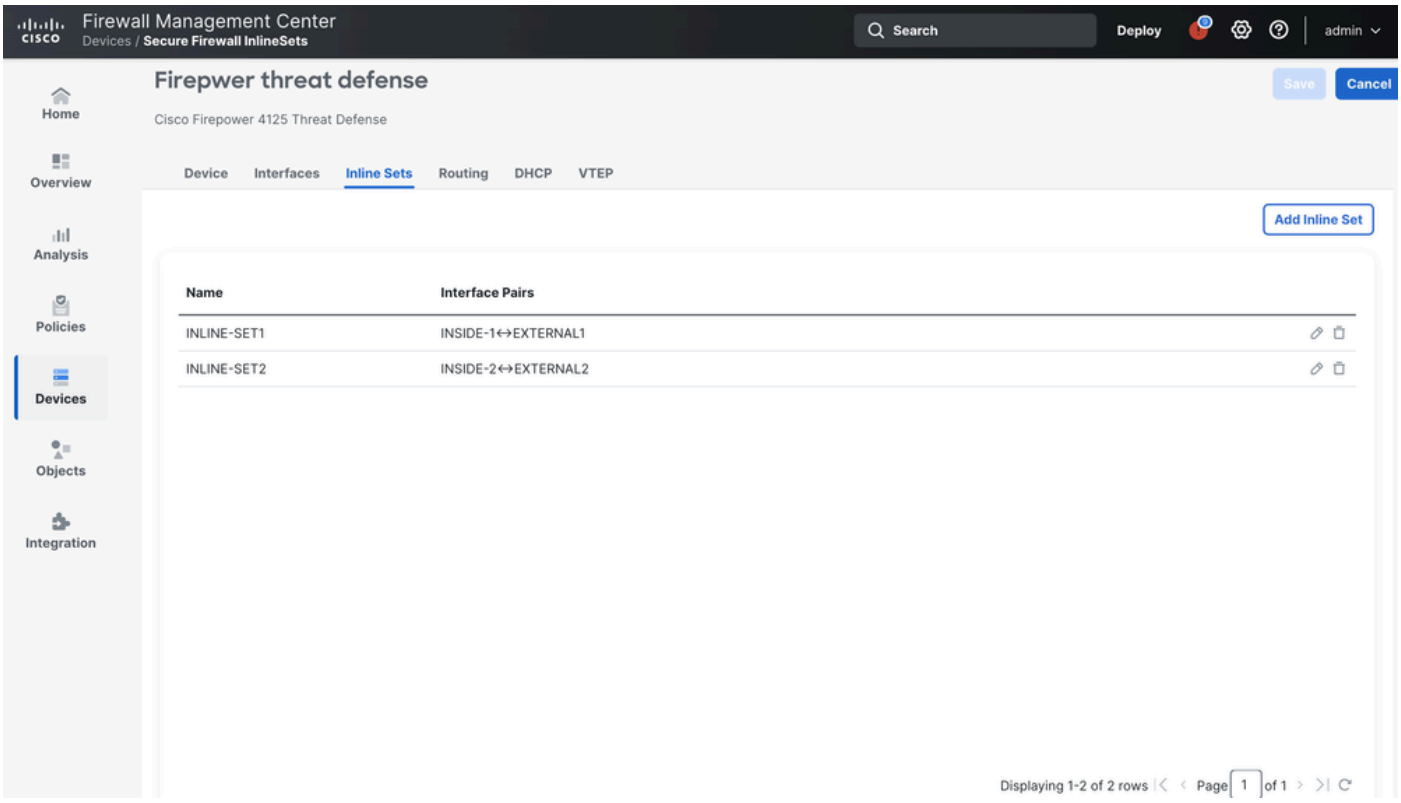
为了满足通过FTD检查流量的要求，我们需要配置PBR以通过FTD重定向流量（包括请求和响应）。因此，我们在连接到PC和路由器的交换机接口上配置了PBR。

场景 2

从VM-PC生成的发往ISR4451-2（路由器）的ICMP流量：

ICMP流量采用以下路径：

VM-PC ------ L3交换机------- FPR4125 ------- ASA 5508 ------FPR4125 ------ L3交换机----ISR路由器。



将内联对配置分为两个不同的内联集时，如上图所示。流量通过INSIDE-1从FTD进入，并通过EXTERNAL2进入。
因此，使用了两个内联集。

观察FMC上的连接事件时，我们会看到两个连接事件，一个用于传出流量，另一个用于传入。

出现此行为的原因在于，每当FTD上的流量为同一流量使用两个不同的内联对（FMC上始终显示两个连接事件）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。