Ereignisse in FirePOWER im transparenten Modus

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Ereignisse angezeigt werden, wenn FTD im transparenten Modus mit verschiedenen Arten von Inline-Sets bereitgestellt wird.

Ziel

Zur Verdeutlichung des Verhaltens von Verbindungsereignissen im FMC bei Bereitstellung des FTD im transparenten Modus mit einer Inline-Set-Konfiguration.

Topologie

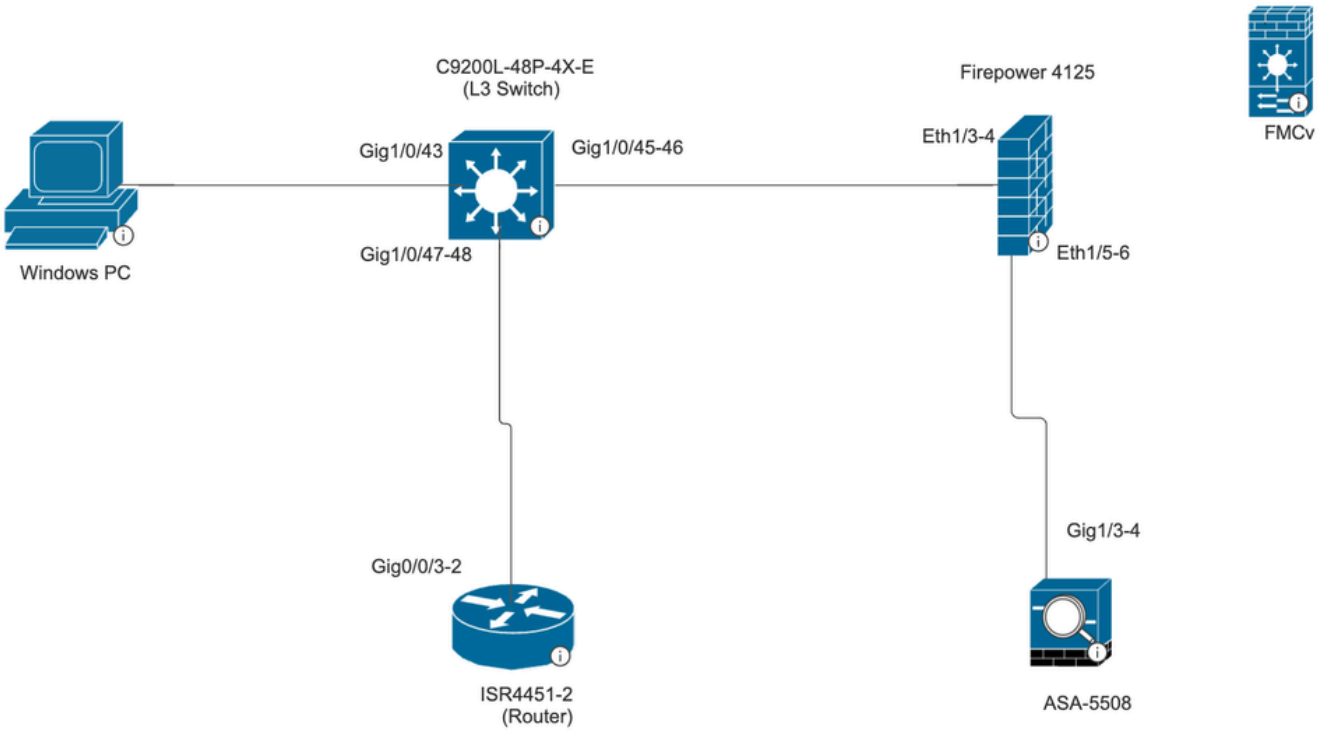


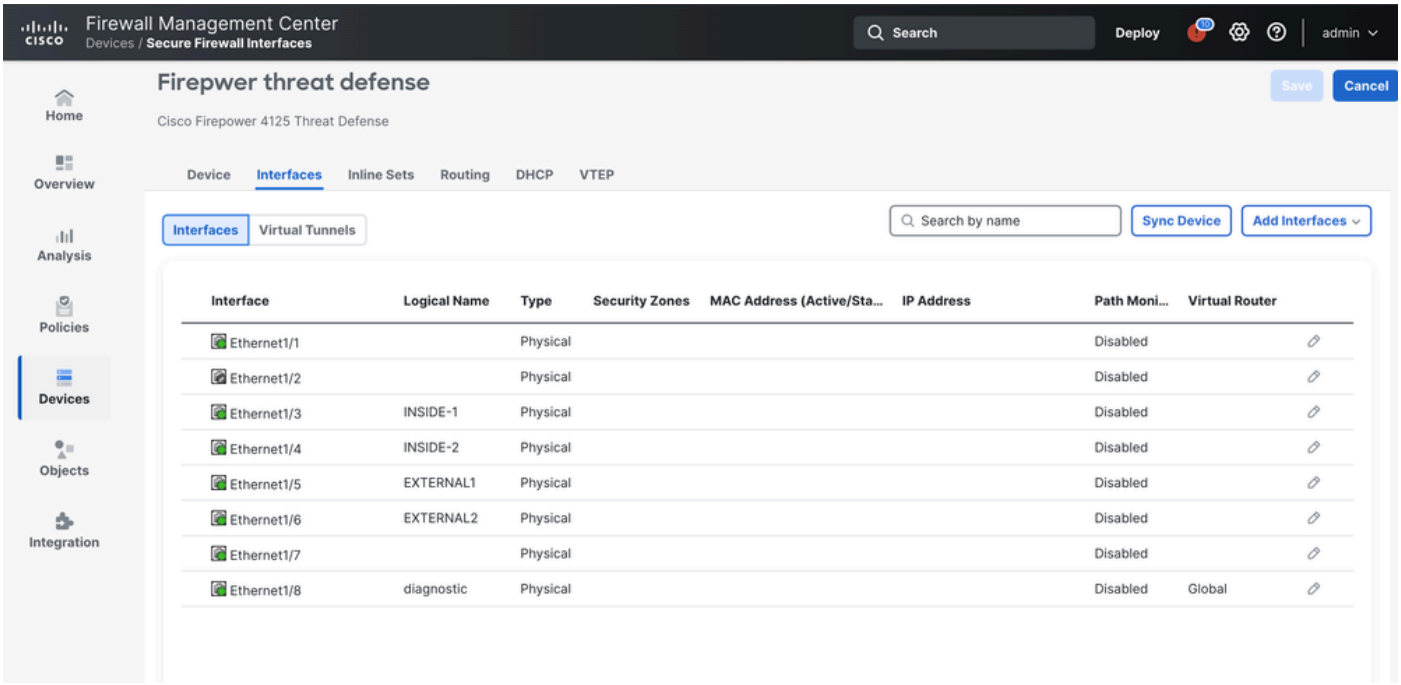
Figure 1. Topology

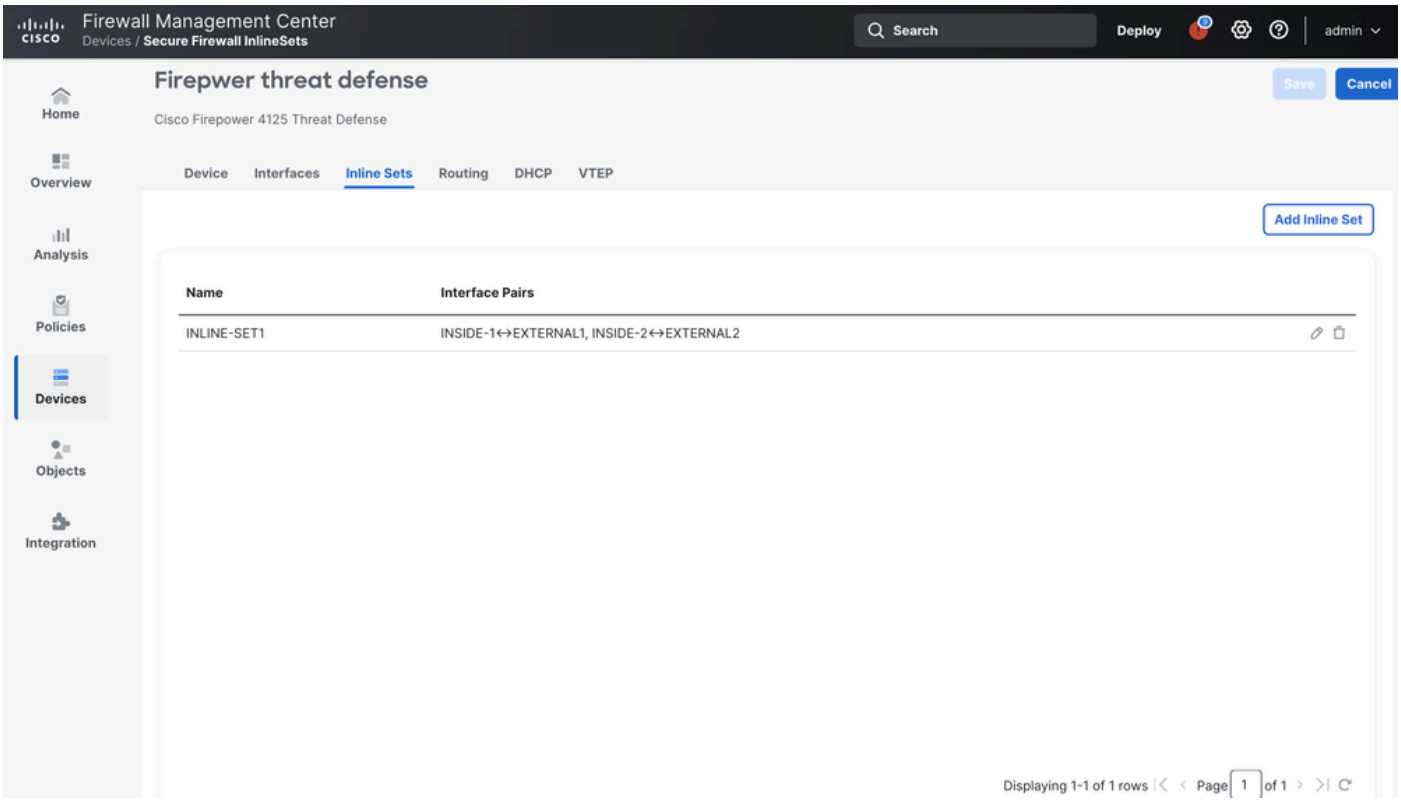
Verwendete Komponenten

- PC-virtuelles System
- C9200L-48P-4X-E (L3-Switch)
- FirePOWER 4125 | 7,6
- FMC V | 7,6
- ASA 5508
- ISR 4451-2 (Router)

Basisszenario

Wenn eine Inline-Set-Konfiguration auf Firepower 4125 zwei ausgewählte Schnittstellenpaare enthält
Ethernet 1/3 (INNEN-1)
Ethernet 1/5 (EXTERN1)
Ethernet 1/4 (INNEN-2)
Ethernet 1/6 (EXTERN2)





Konfigurationsübersicht

L3-Switch

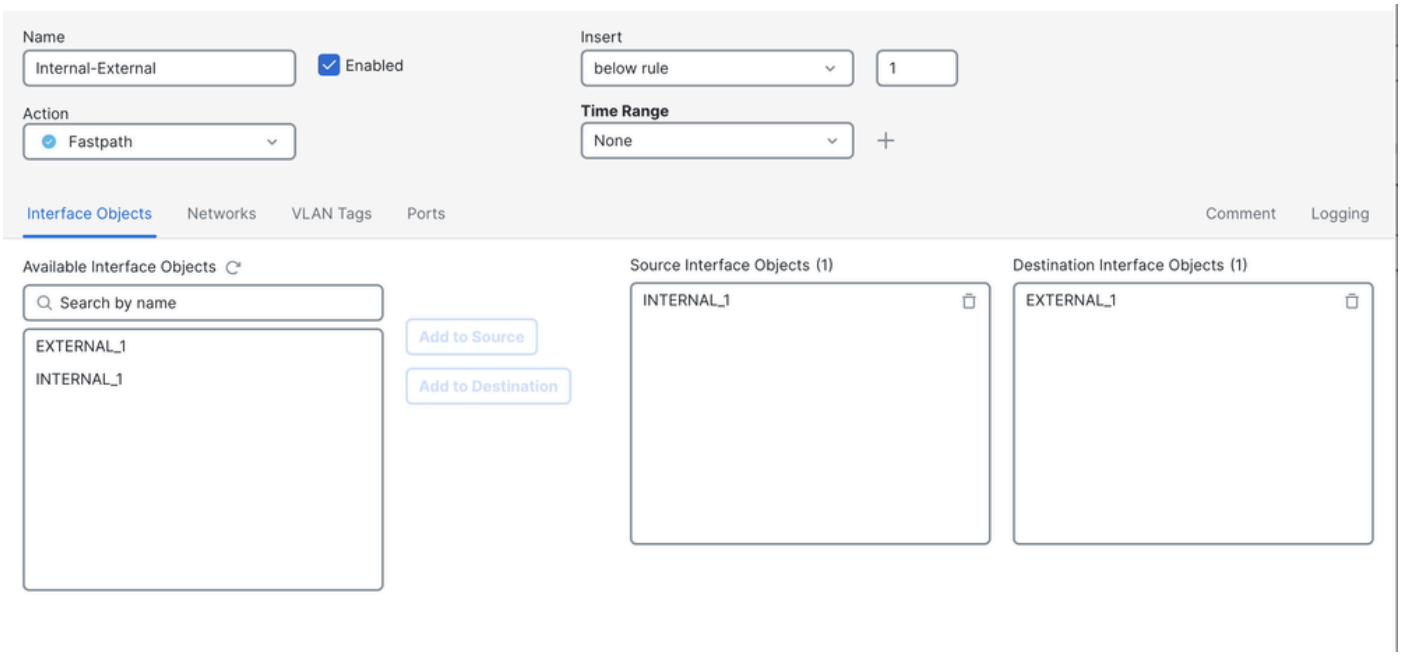
Port-Channel 2 (GB 1/0/45-46)

ASA 5508
Port-Channel 2 (Gigabit 1/3-4)

ASA wird im One-Arm-Modus bereitgestellt, d. h. der Datenverkehr läuft über denselben Port-Channel, nämlich Port-Channel 2, in die ASA ein und aus der ASA.
Port-Channel wird auf ASA und Switch konfiguriert, um den Datenverkehr zwischen den beiden Systemen auszugleichen.
Firepower 4125 ist für FMCv registriert.

FMC V

Konfigurieren
Vorfilterrichtlinie:
Vorfilterregel intern-extern mit Aktion Fastpath.
Quellschnittstellenobjekt: INTERNAL_1 Zielschnittstellenobjekt: EXTERN_1.



Die Zugriffskontrollrichtlinie wird so konfiguriert, dass "Alle beliebigen zulassen" aktiviert ist.

Beobachtetes Verhalten

Szenario 1

ICMP-Datenverkehr von VM-PC generiert und an ISR4451-2(Router) gerichtet:

Der ICMP-Datenverkehr verläuft über den folgenden Pfad:

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

Im FMC-Verbindungsereignis wird nur ein Verbindungsereignis erkannt, da der ICMP-Datenverkehr über dasselbe Inline-Paar (INSIDE-2 >>EXTERNAL2) auf dem FPR 4125 ein- und ausgeht.

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

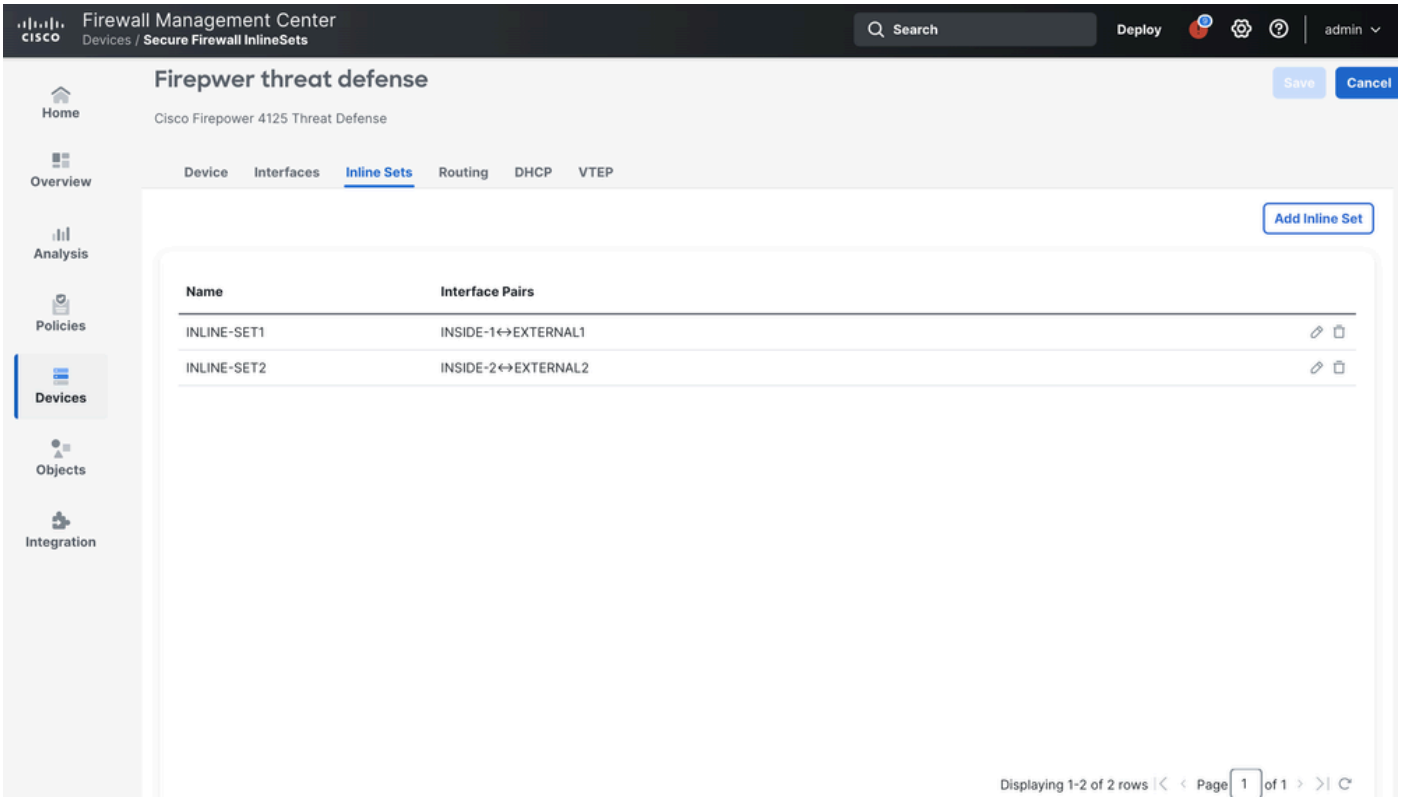
Um unsere Anforderung zu erfüllen, den Datenverkehr über FTD zu überprüfen, mussten wir PBR konfigurieren, um den Datenverkehr (sowohl Anfragen als auch Antworten) über FTD umzuleiten. Daher wurde PBR auf den Switch-Schnittstellen konfiguriert, die mit dem PC und Router verbunden sind.

Szenario 2

ICMP-Datenverkehr von VM-PC generiert und an ISR4451-2(Router) gerichtet:

Der ICMP-Datenverkehr verläuft über den folgenden Pfad:

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



Wenn wir die Inline-Paar-Konfiguration in zwei verschiedene Inline-Sets unterteilen, wie in der Abbildung oben

gezeigt. Der Datenverkehr tritt über INSIDE-1 aus der FTD aus und über EXTERN2 ein.
Daher werden zwei Inline-Sets verwendet.

Beim Beobachten der Verbindungsereignisse auf dem FMC werden zwei Verbindungsereignisse angezeigt, eines für den ausgehenden und eines für den eingehenden Datenverkehr.

Der Grund für ein solches Verhalten ist, dass immer dann, wenn der Datenverkehr auf FTD zwei verschiedene Inline-Paare für den gleichen Datenverkehr nutzt, auf dem FMC zwei Verbindungsereignisse angezeigt werden.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.