Konfigurieren von FDM-Schnittstellen im Inline-Pair-Modus

Inhalt

Einleitung

In diesem Dokument werden die Inline-Sets für FDM beschrieben, die in Cisco Secure Firewall 7.4.1 hinzugefügt wurden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- FDM Konzepte und Konfiguration
- Gilt für FTDs auf den von FDM verwalteten Plattformen der Serien 1000, 2100 und 3100

Verwendete Komponenten

Die in diesem Dokument enthaltenen Informationen basieren auf FDM 7.4.2.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Ein Inline-Set stellt eine Schnittstelle zur Verfügung, die nur IPS unterstützt. Sie können nur IPS-Schnittstellen implementieren, wenn Sie über eine separate Firewall verfügen, die diese Schnittstellen schützt, und den zusätzlichen Aufwand durch die Firewall-Funktionen vermeiden möchten.

Ein Inline-Set wirkt wie eine Beule am Kabel und verbindet zwei Schnittstellen miteinander, um einen Steckplatz in einem vorhandenen Netzwerk einzurichten. Mit dieser Funktion kann das Gerät in einer beliebigen Netzwerkumgebung installiert werden, ohne dass benachbarte Netzwerkgeräte konfiguriert werden müssen. Inline-Schnittstellen empfangen den gesamten Datenverkehr ohne Einschränkungen, aber der gesamte Datenverkehr, der auf diesen Schnittstellen empfangen wird, wird aus einem Inline-Set erneut übertragen, sofern er nicht explizit fallen gelassen wird.

Richtlinien und Einschränkungen

- Sie können Inline-Sets nur auf diesen Gerätemodellen konfigurieren: Firepower der Serie 1000, Firepower 2100, Secure Firewall 3100.
- In einem Inline-Set zulässige Schnittstellentypen: physisch, EtherChannel.
- Sie können die Management-Schnittstelle nicht in ein Inline-Set integrieren.
- Sie können die Attribute der in einem Inline-Set verwendeten Schnittstellen nicht ändern: Name, Modus, Schnittstellen-ID, MTU, IP-Adresse.
- Wenn Sie den Tap-Modus aktivieren, ist Snort Fail Open deaktiviert.
- BFD-Echo-Pakete (Bidirectional Forwarding Detection) sind bei Verwendung von Inline-Sätzen nicht zulässig. Wenn auf beiden Seiten des Geräts zwei Nachbarn BFD ausführen, verwirft das Gerät BFD-Echo-Pakete, da diese die gleiche Quell- und Ziel-IP-Adresse aufweisen und Teil eines LAN-Angriffs zu sein scheinen.
- Für Inline-Sets und passive Schnittstellen unterstützt das Gerät bis zu zwei 802.1Q-Header in einem Paket (auch als Q-in-Q-Unterstützung bezeichnet).

  Anmerkung: Firewall-Schnittstellen unterstützen Q-in-Q nicht und nur einen 802.1Q-Header.

- Schnittstellen in einem Inline-Set unterstützen kein Routing, NAT, DHCP (Server, Client oder Relay), VPN, TCP Intercept, keine Anwendungsinspektion oder keinen NetFlow.

Vorbereitungen

- Es wird empfohlen, STP PortFast für STP-fähige Switches festzulegen, die mit den Inline-Pair-Schnittstellen zur Bedrohungsabwehr verbunden sind.
- Konfigurieren Sie die physischen oder EtherChannel-Schnittstellen, die Mitglieder des Inline-

Sets sein können. Sie können nur diese Werte konfigurieren: Name, Duplex, Geschwindigkeit und Routed-Modus (wählen Sie nicht "passiv" aus). Konfigurieren Sie keine Adressierungsarten, d. h. manuelle IP-Adressen, DHCP oder PoE.

Details zum Inline-Modus

- Mit dieser Funktion können Sie Inline-Sets verwenden. Dadurch wird eine Überprüfung des Datenverkehrs ohne IP-Zuweisung ermöglicht.
- Der Inline-Modus ist für physische Schnittstellen, EtherChannels und Sicherheitszonen verfügbar.
- Der Inline-Modus wird automatisch für Schnittstellen und EtherChannels festgelegt, wenn sie in einem Inline-Paar verwendet werden.
- Der Inline-Modus verhindert, dass Änderungen an den betreffenden Schnittstellen und EtherChannels vorgenommen werden, bis diese aus dem Inline-Paar entfernt werden.
- Schnittstellen, die sich im Inline-Modus befinden, können Sicherheitszonen zugeordnet werden, die auf den Inline-Modus gesetzt sind.

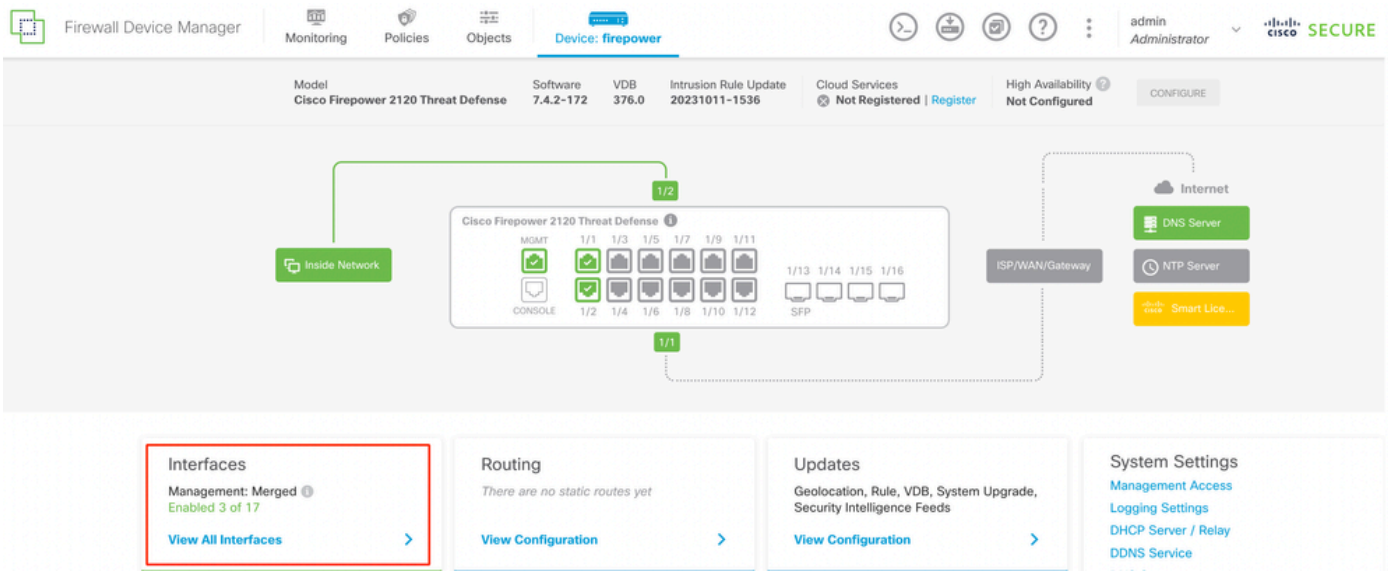
Inline-Set-Netzwerkdiagramm

Der Datenverkehr fließt von Router1 zu Router2 über die Schnittstellen A und B und nutzt dabei nur eine physische Verbindung.

Netzwerkdiagramm

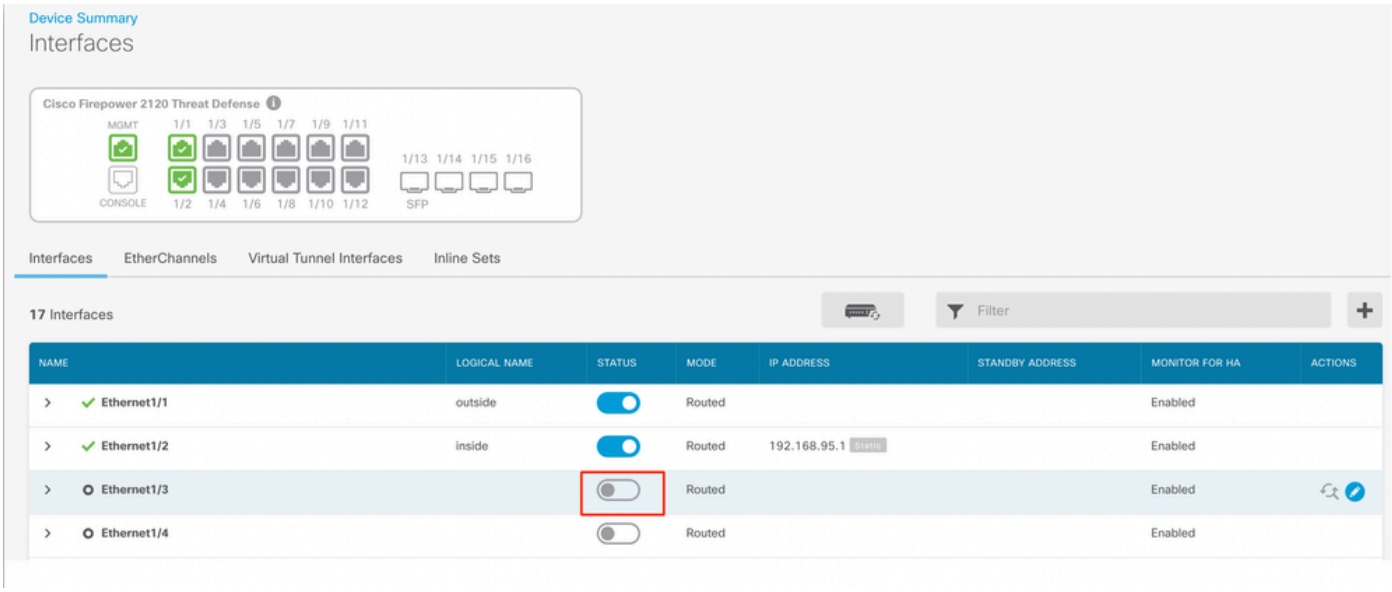
Inline-Set konfigurieren

- Navigieren Sie im FDM-Dashboard zu Schnittstellen-Karte.

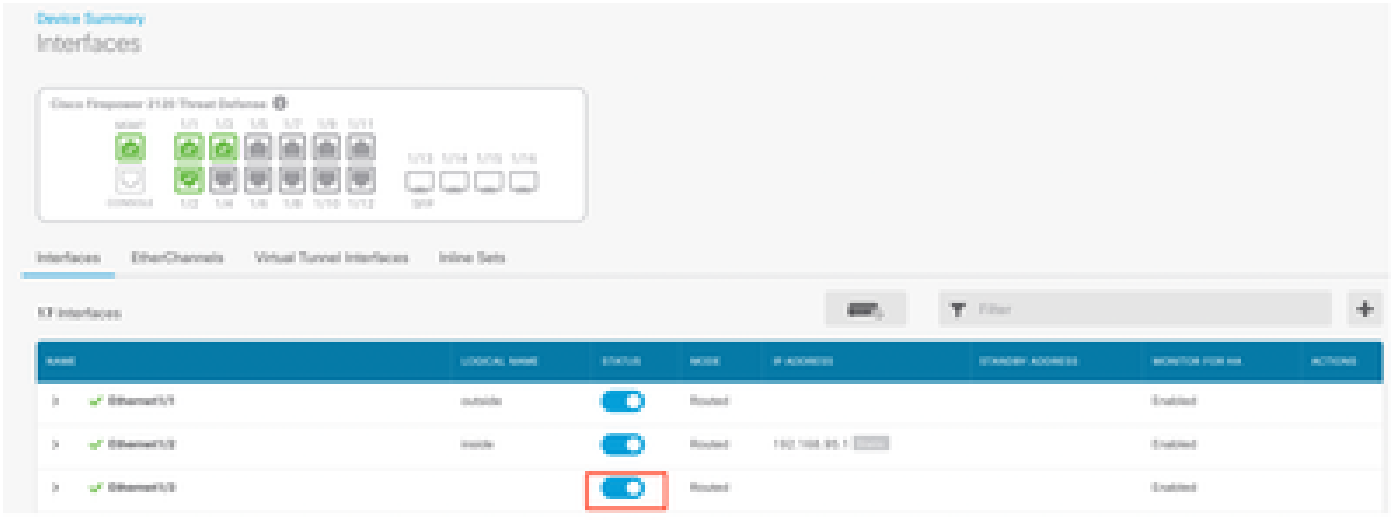


Registerkarte Schnittstellen

- Um Schnittstellen zu aktivieren, klicken Sie auf das Statussymbol der Schnittstelle.

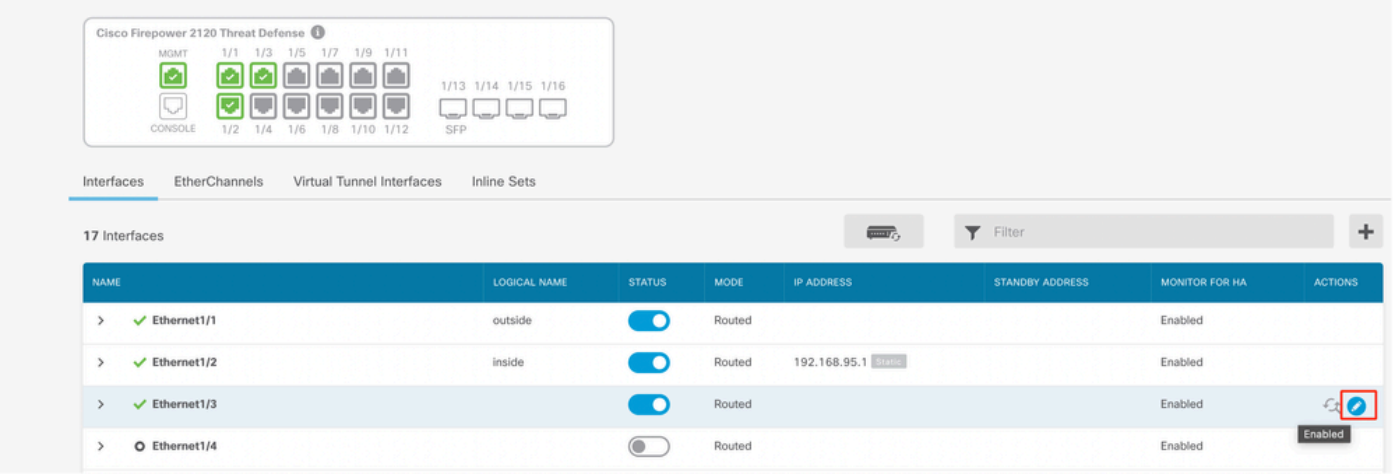


Statussymbol



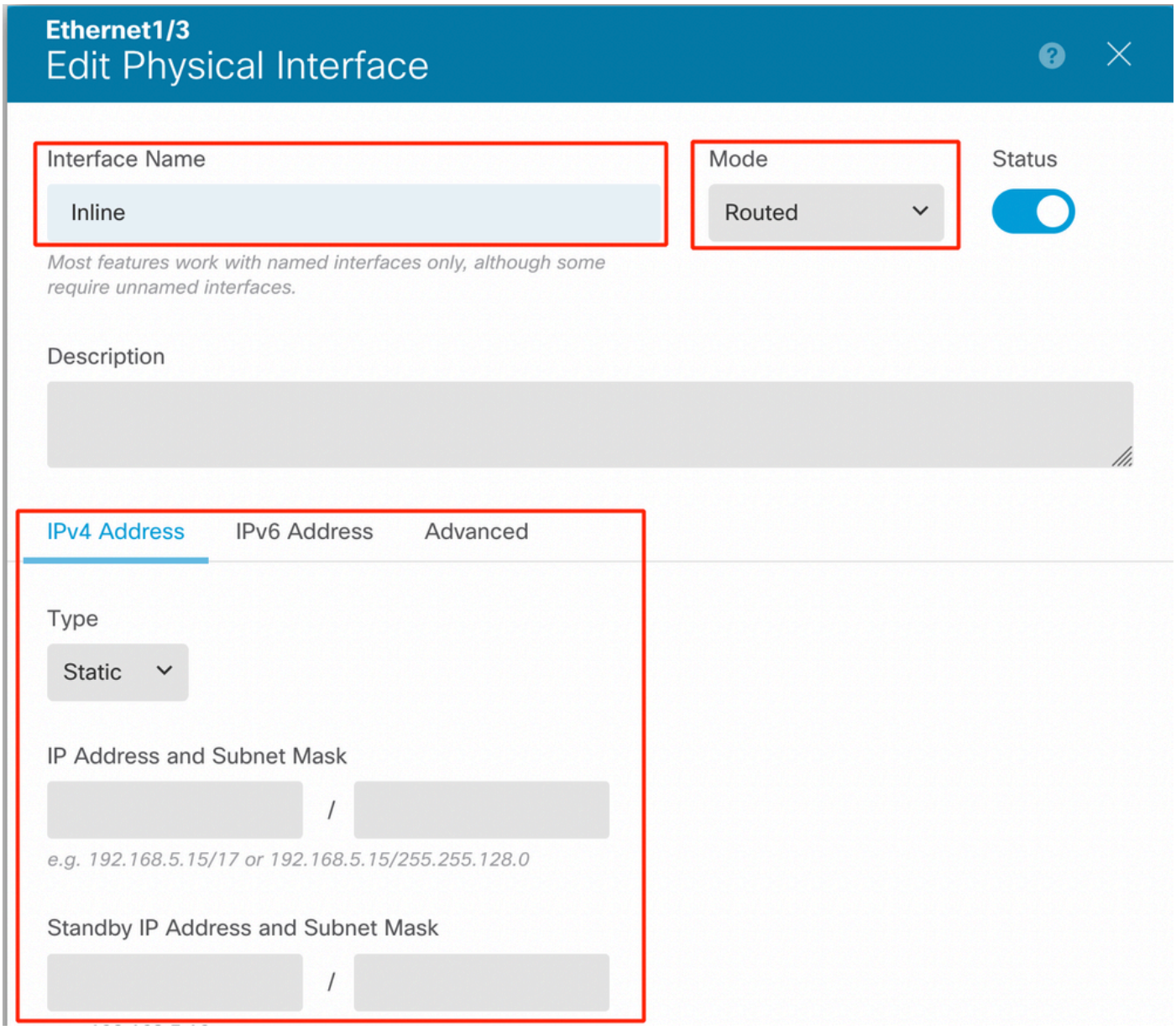
Schnittstelle aktivieren

- Um Schnittstellen zu bearbeiten, klicken Sie für die Schnittstelle auf das Bleistiftsymbol für Edit (Bearbeiten).



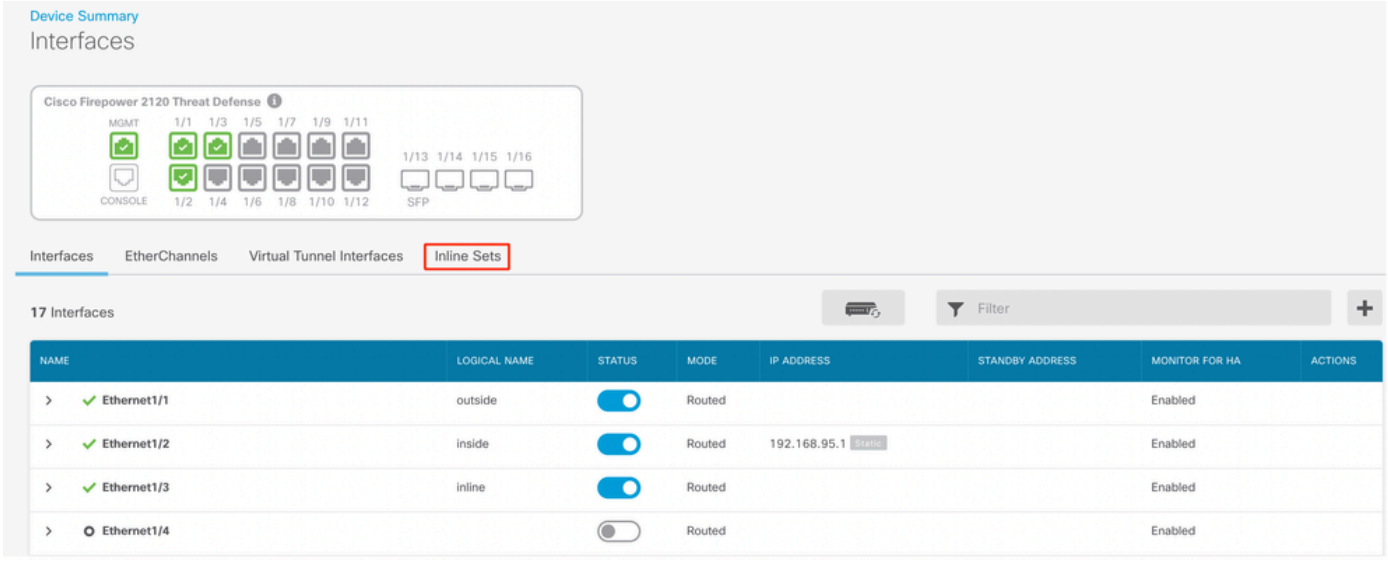
Schnittstelle bearbeiten

- Geben Sie den Schnittstellennamen ein, und wählen Sie den Modus "Routed" aus. Konfigurieren Sie keine IP-Adressen.



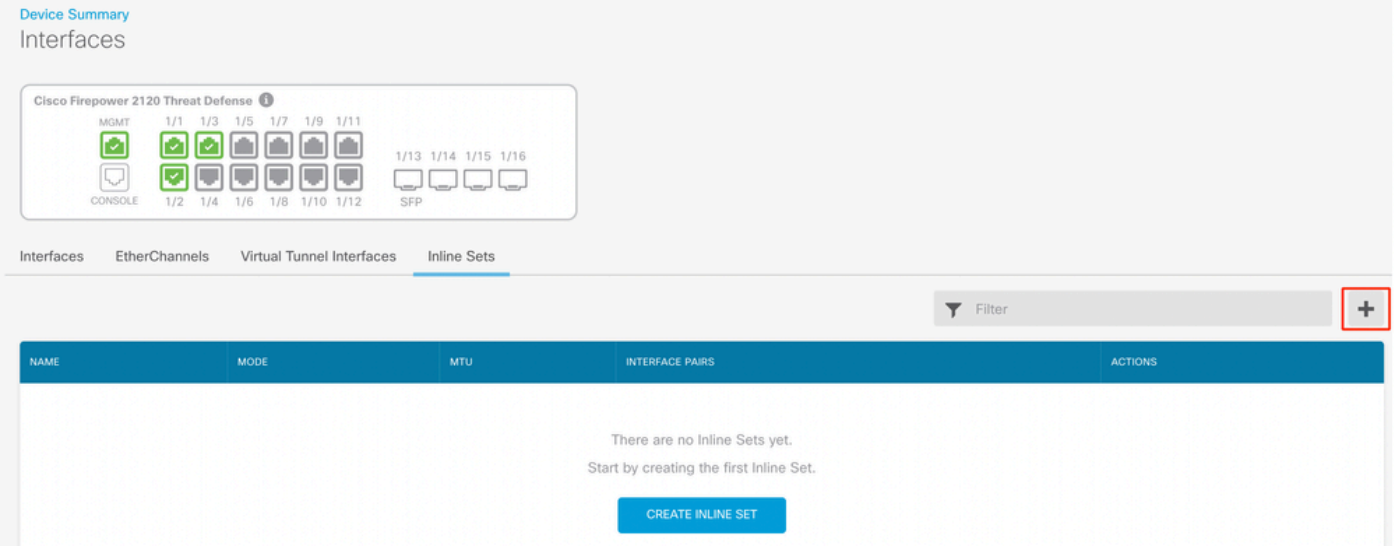
Schnittstelle bearbeiten

- Um ein Inline-Set zu erstellen, navigieren Sie zur Registerkarte Inline-Sets.



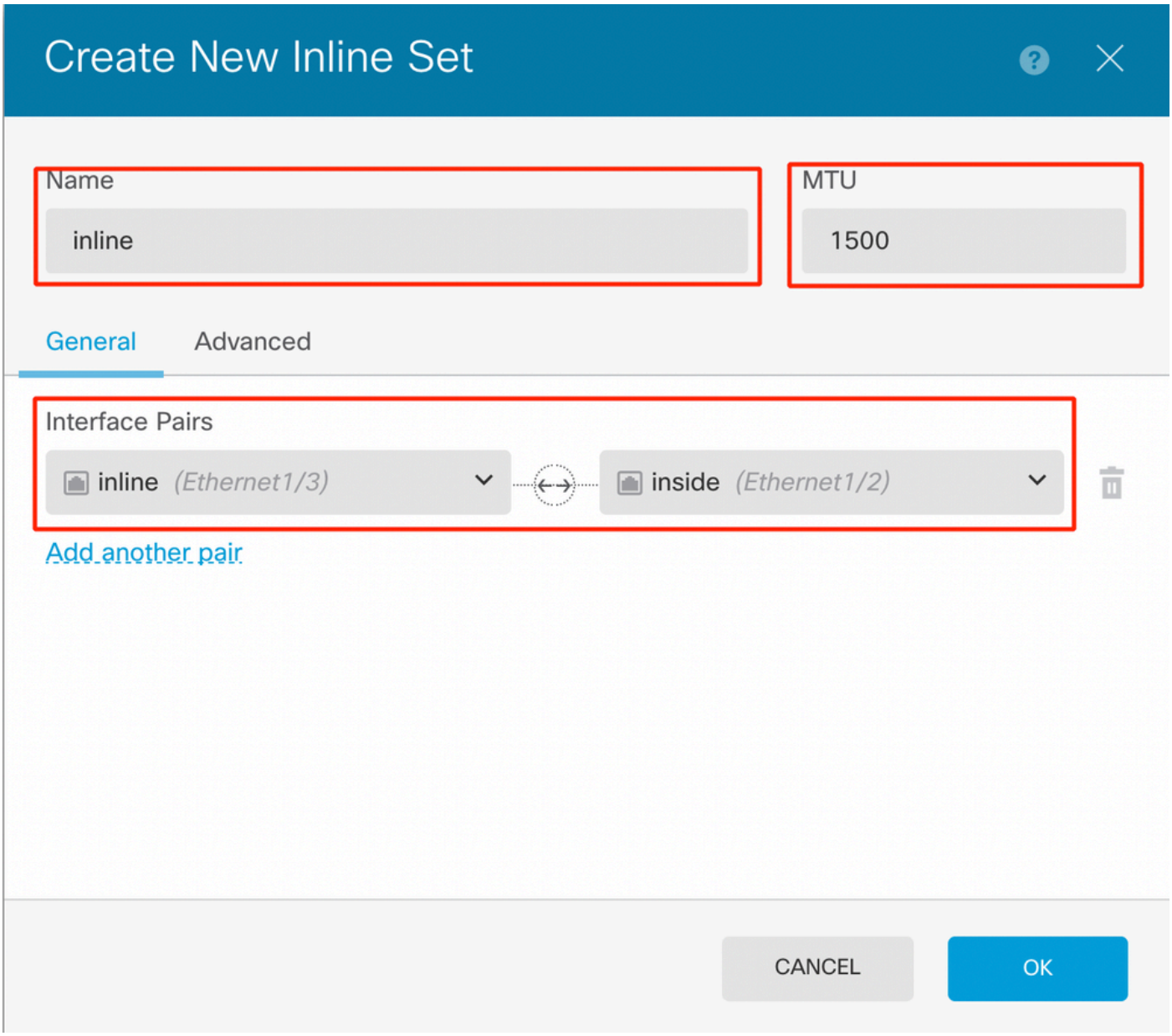
Inline-Set erstellen

Um ein Inline-Set hinzuzufügen, klicken Sie auf Hinzufügen (Symbol +).



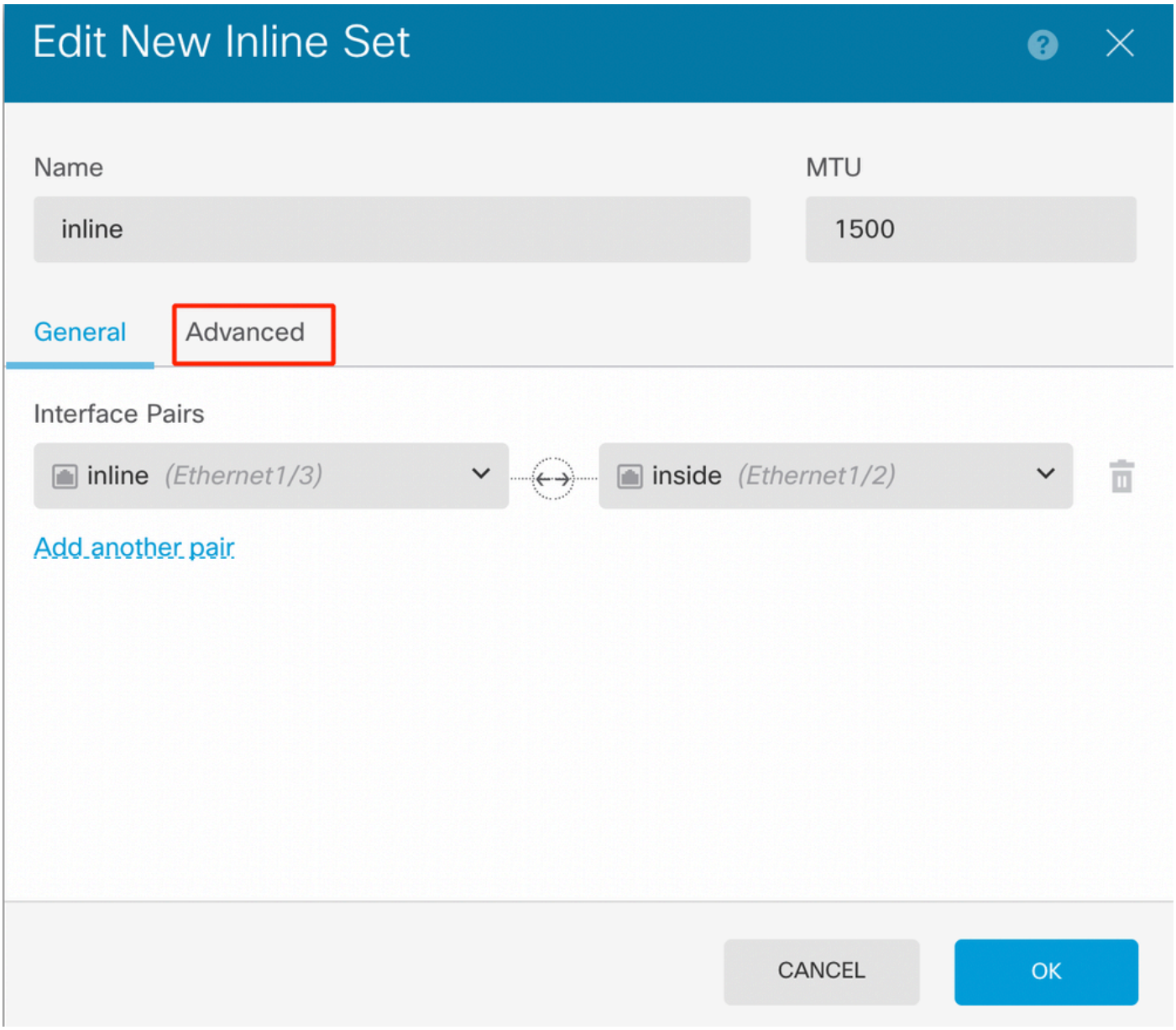
Inline-Satz hinzufügen

- Legen Sie einen Namen für den Inline-Satz fest.
- Stellen Sie die gewünschte MTU ein (optional). Der Standardwert ist 1500 (dies ist die mindestens unterstützte MTU).
- Wählen Sie im Abschnitt Schnittstellenpaare die Schnittstellen aus. Wenn mehr Paare erforderlich sind, klicken Sie auf Add another pair link.



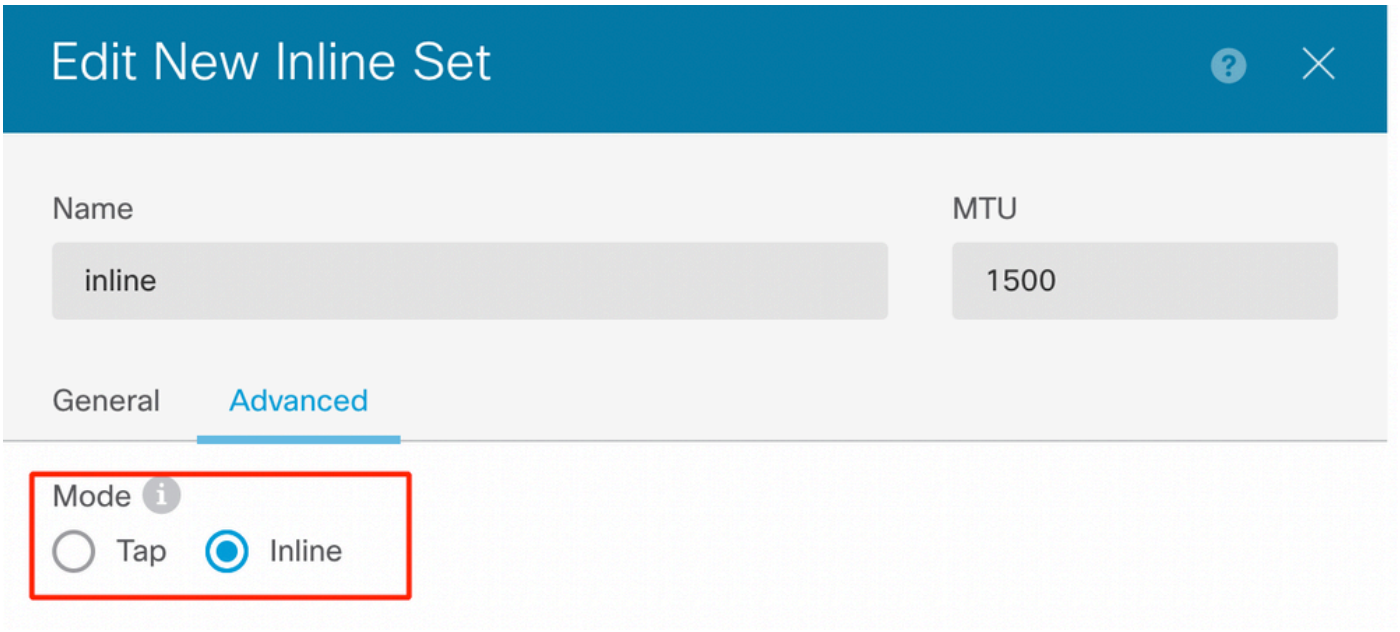
Schnittstellenpaare

- Um die erweiterten Einstellungen für das Inline-Set zu konfigurieren, navigieren Sie zur Registerkarte Erweitert.



Erweiterte Einstellungen

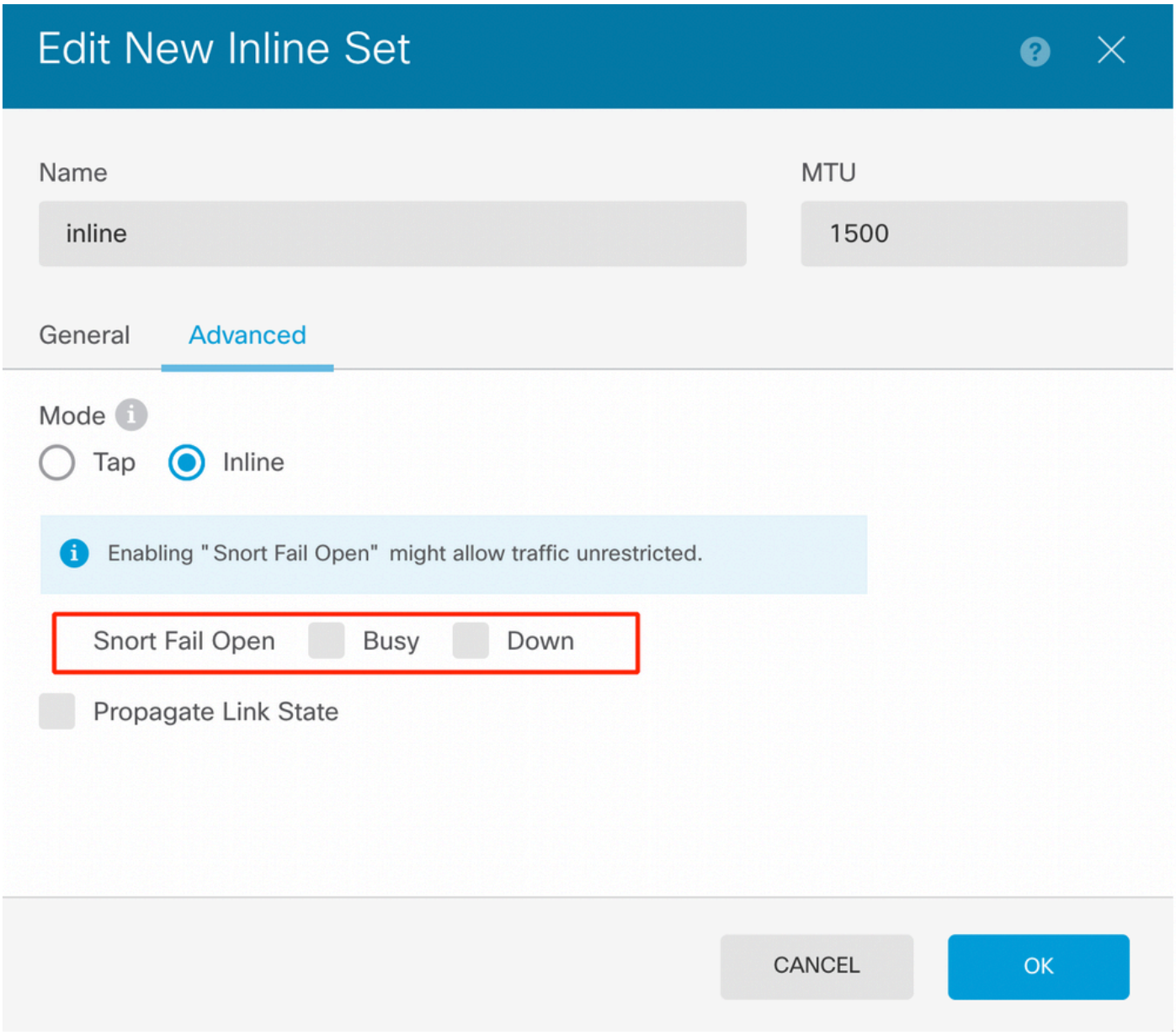
- Wählen Sie den Modus als Inline aus. Wenn der Tap-Modus aktiviert ist, ist Snort Fail Open deaktiviert.



Modus Inline

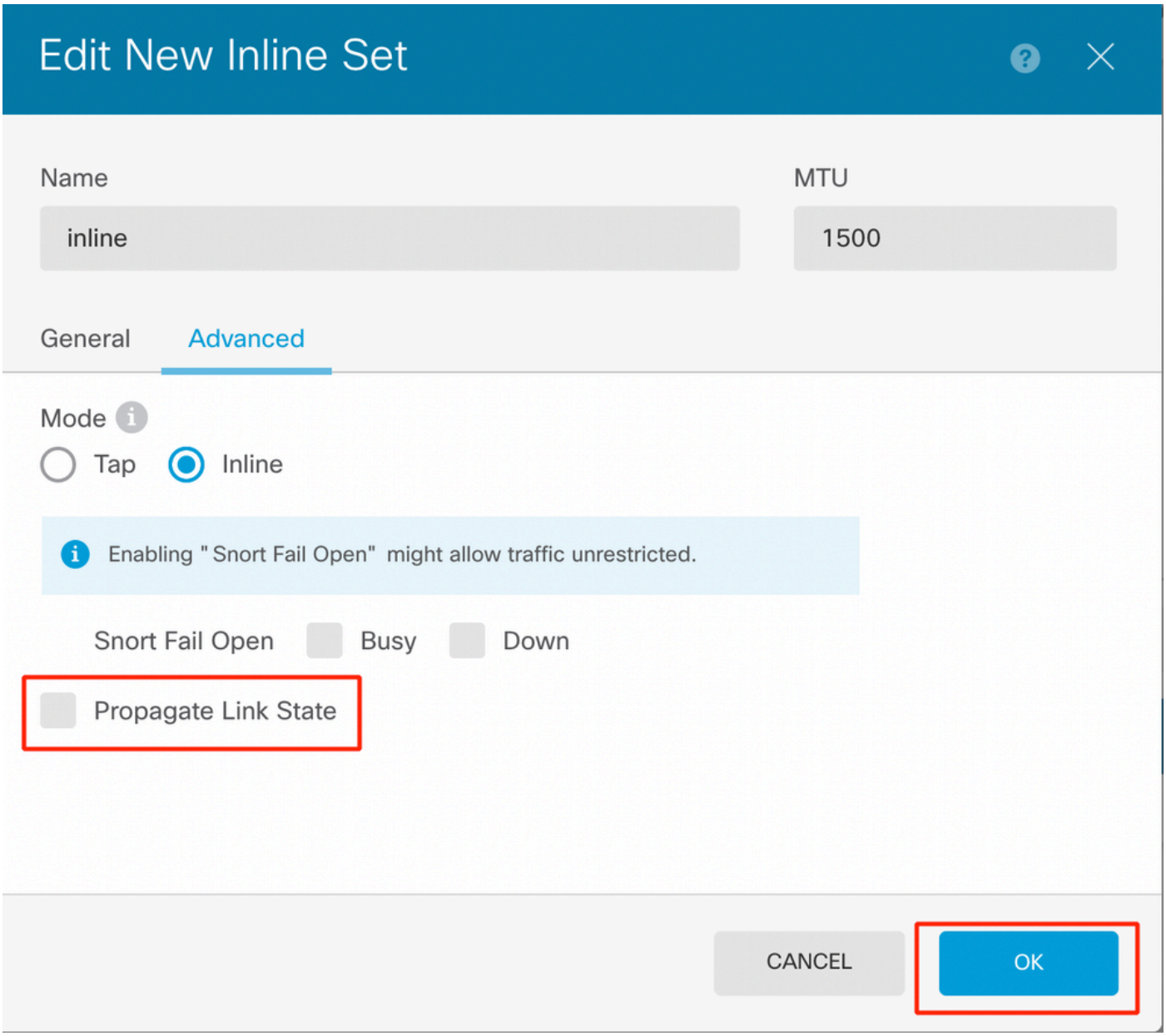
- Snort Fail Open lässt zu, dass neuer und vorhandener Datenverkehr ohne Prüfung (aktiviert) oder Abwurf (deaktiviert) weitergeleitet wird, wenn der Snort-Prozess ausgelastet oder ausgefallen ist.

- Wählen Sie die gewünschten Snort Fail Open-Einstellungen aus.
- Es können keine, eine oder beide Optionen Besetzt und Abwärts eingestellt werden.



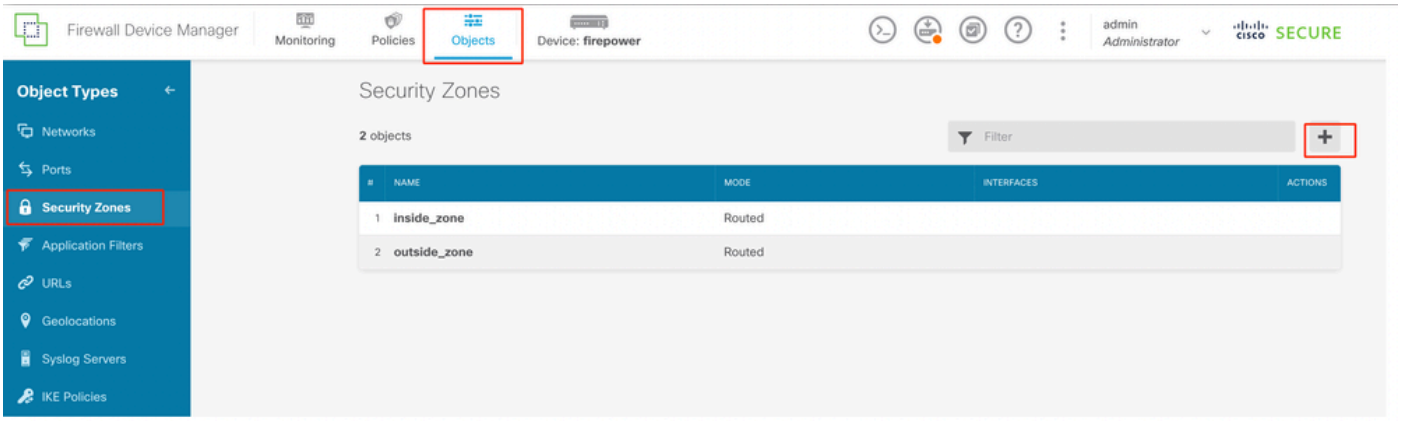
Snort Fail Open

- Mit der Option Link-Zustand propagieren wird die zweite Schnittstelle im Inline-Paar automatisch deaktiviert, wenn eine der Schnittstellen ausfällt. Wenn die ausgefallene Schnittstelle wieder verfügbar ist, wird auch die zweite Schnittstelle automatisch wieder aktiviert.
- Wenn Sie alle Einstellungen vorgenommen haben, klicken Sie auf OK, um die Konfiguration zu speichern.



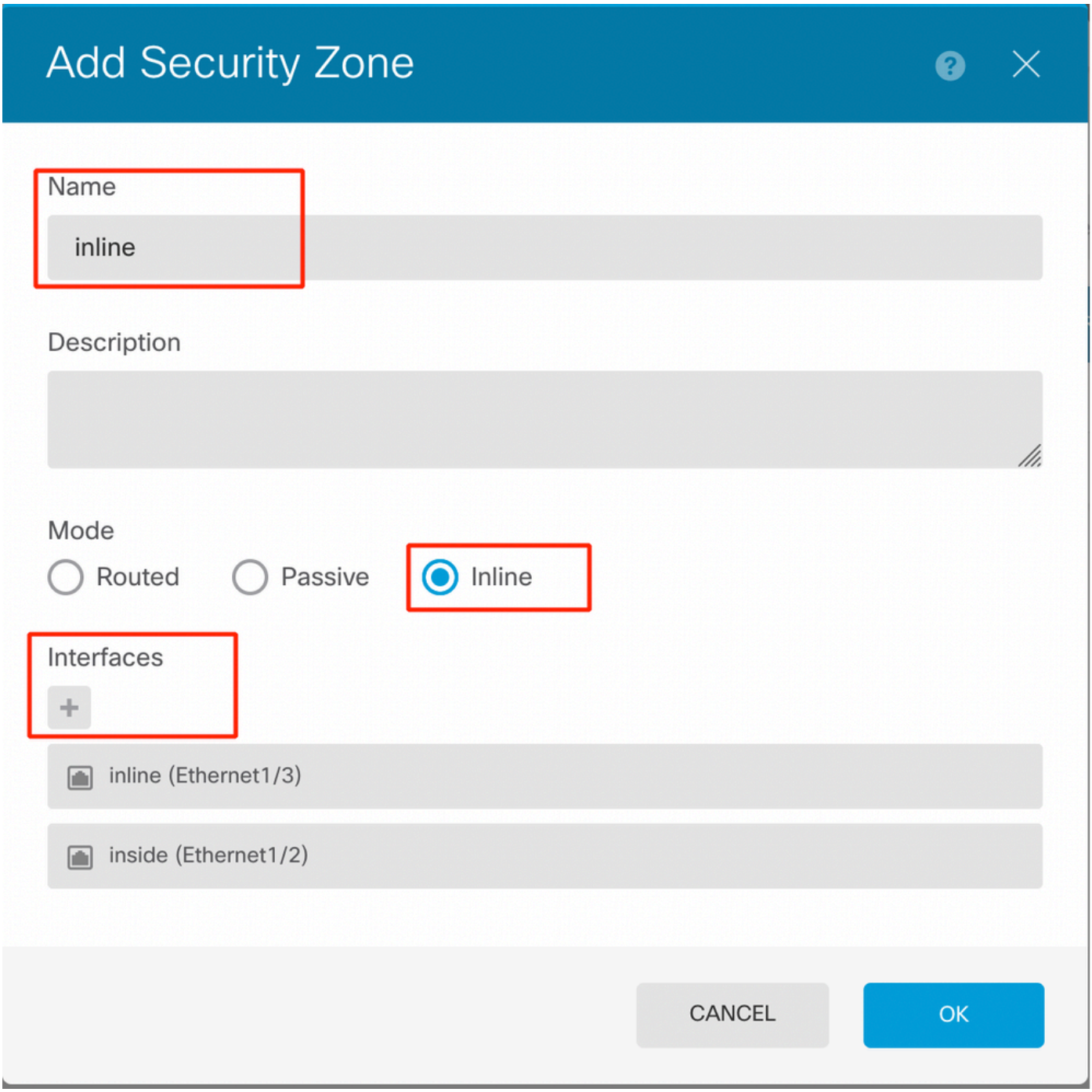
Verknüpfungsstatus propagieren

- Um diese Inline-Gruppe einer Sicherheitszone hinzuzufügen, navigieren Sie zu Objekte > Sicherheitszonen.
- Klicken Sie auf Hinzufügen, um eine neue Sicherheitszone zu erstellen.



Sicherheitszone hinzufügen

- Legen Sie einen Namen fest, wählen Sie den Modus als Inline aus, und fügen Sie die Schnittstellen des Inline Sets hinzu. Klicken Sie dann auf OK, um zu speichern.

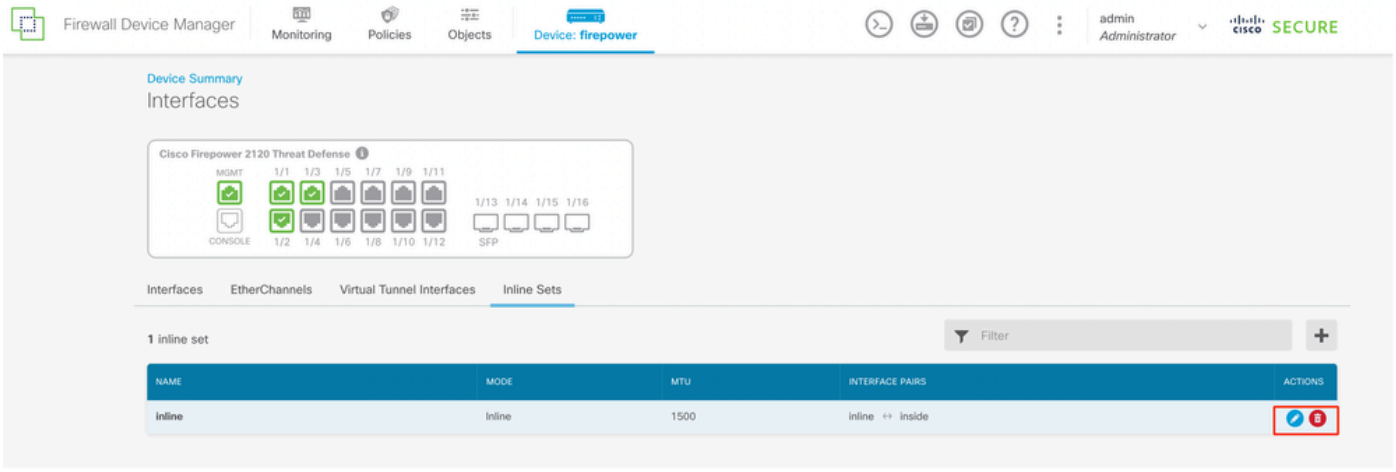


Schnittstellen hinzufügen

- Navigieren Sie zur Registerkarte "Bereitstellung", und stellen Sie die Änderungen bereit.

Ändern oder Löschen eines Inline-Sets

Für die Inline Sets sind Bearbeitungs- und Löschaktionen verfügbar.



Aktionen des Inline-Sets

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.