Hardwareumgehung für sichere Firewall 3100 FDM 7.7.0 konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Hardware-Umgehung für Inline-Sets in der von FirePOWER Device Manager (FDM) verwalteten sicheren Firewall 7.7.0 konfigurieren.

Voraussetzungen

Anforderungen

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

- Inline-Sets
- Secure Firewall der Serie 3100
- Grafische Benutzeroberfläche (GUI) des FirePOWER Gerätemanagers

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Secure Firewall 3100 mit Version 7.7.0
- Cisco Secure Firewall Device Manager 7.7.0

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

Die Funktion "Inline Sets" wurde in FDM in Version 7.4.1 hinzugefügt. Inline Sets ermöglichen die Überprüfung in einem L2-Netzwerk, ohne dass Routing erforderlich ist: FTD-Schnittstellen im Inline-Pair-Modus konfigurieren

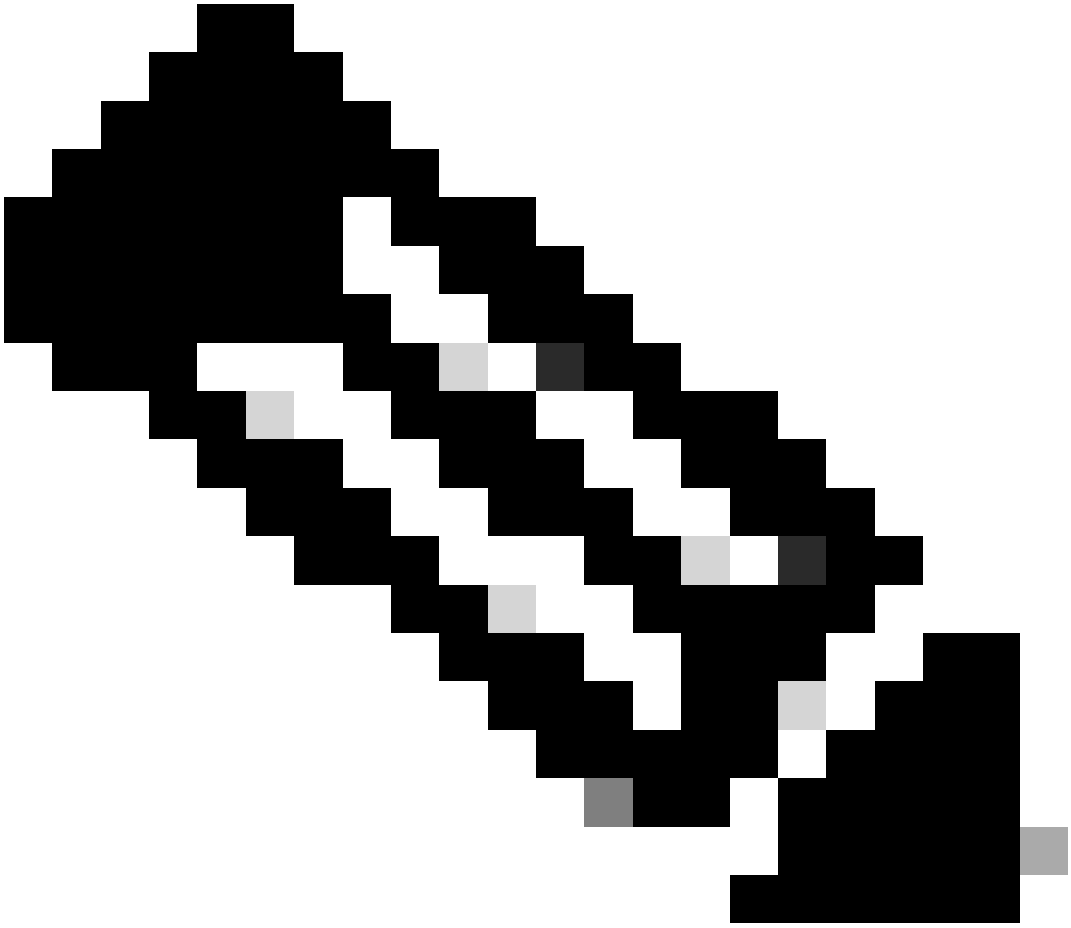
Vergleich mit Vorgängerversion

In Secure Firewall 7.6 and Below		New to Secure Firewall 7.7
• Inline Sets is available. • Hardware Bypass is not supported.		• Added support for Hardware Bypass.

Umgehungsfunktion für sichere Firewall 7.0

Neuerungen

- Hardware Inspection Bypass stellt sicher, dass der Datenverkehr während eines Stromausfalls weiterhin zwischen einem Inline-Schnittstellenpaar fließt.
- Diese Funktion wird verwendet, um die Netzwerkverbindung bei Software- oder Hardwarefehlern aufrechtzuerhalten.
- Hardware Bypass ist jetzt für Inline-Sets für Plattformen der Serie FDM 3100 verfügbar.



Hinweis: Konfigurationsleitfaden für FirePOWER Management Center

---

Bereitstellungsszenarien

- Wie würde diese Funktion in eine Produktionsumgebung passen?
  - Inline-Sets werden für einen IPS- (oder IDS-) Anwendungsfall verwendet.
  - Ermöglicht die Überprüfung des Datenverkehrs, ohne dass Routing-Konfigurationen erforderlich sind. Ermöglicht den Datenverkehrsfluss bei einem Geräteausfall über die Hardwareumgehung.
- .Praktische Beispiele:
  - Richten Sie eine Layer-2-Netzwerküberprüfung überall schnell und einfach ein - ohne dass Layer 3 erforderlich ist.
  - Kritisch für vollständig isolierte Netzwerke - kein Internetzugang.
  - Transparente Inline-Einfügung für Deep Packet Inspection für Standalone-Firewall - vorhandene Layer-2-Produktionsarchitektur.

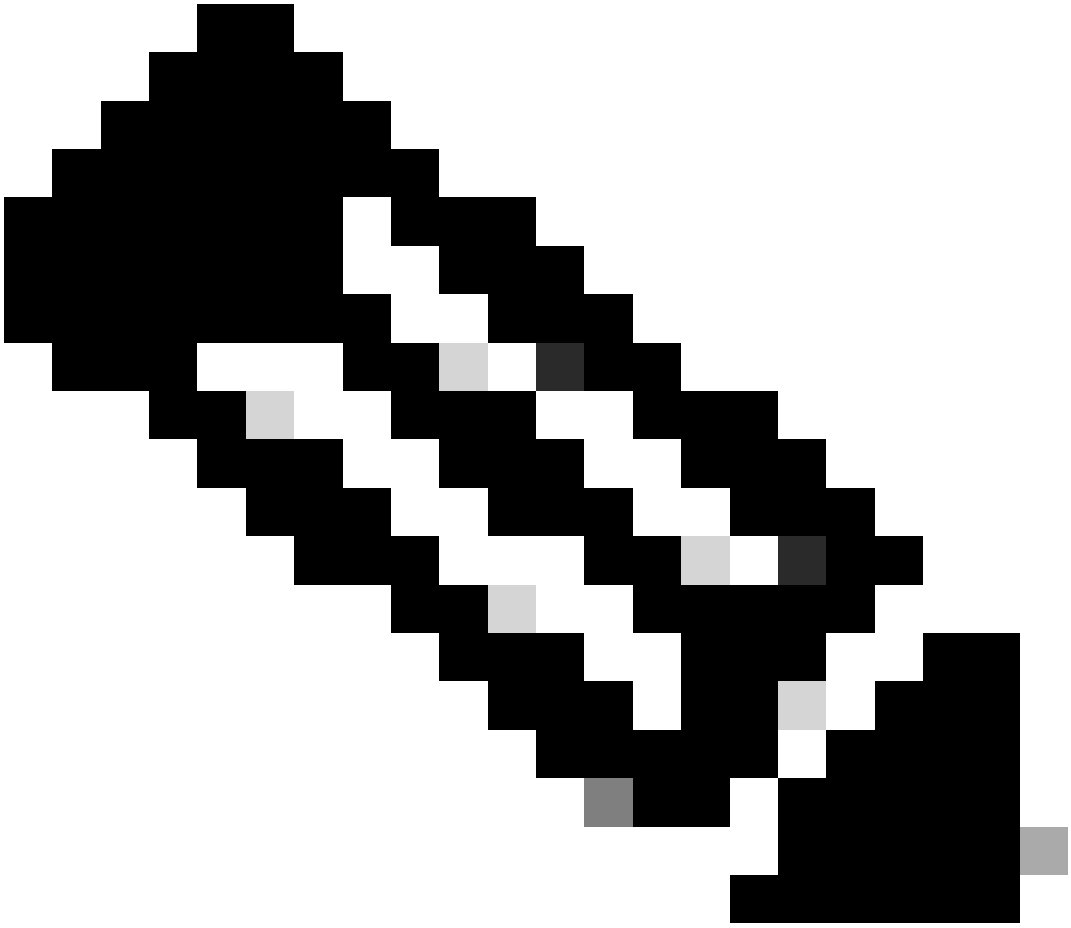
Grundlagen: Unterstützte Plattformen, Lizenzierung

Software- und Hardwareversionen

FDM		
	Inline Sets – before 7.7.0	Inline Sets with Hardware Bypass
FDM	7.4.1	7.7.0
REST API	7.4.1	7.7.0

Platforms	1000, 2100 (up to 7.4 only), and 3100 Series	3100 Series equipped with a network module:
		• 8 Ports:
		  ○ FPR-X-NM-6X1SXF
		• 6 Ports:
		  ○ FPR-X-NM-6X10SRF
		  ○ FPR-X-NM-6X10LRF
		  ○ FPR-X-NM-6X25SRF
		  ○ FPR-X-NM-6X25LRF

Software und Hardware



Anmerkung: [Informationen zur Serie 3100 und zur Hardware-Umgehung]

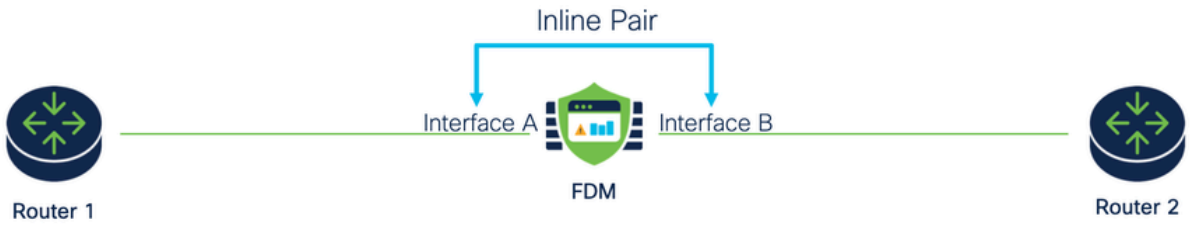
Weitere Aspekte der Unterstützung

FDM			
Inline Sets		Inline Sets with Hardware Bypass	
Licenses Required	Essentials	Licenses Required	Essentials
Works in Evaluation Mode	Yes	Works in Evaluation Mode	Yes
IP Addressing	Not required	IP Addressing	Not required
Supported with HA'd devices	Yes	Supported with HA'd devices	No
Other (only routed mode)	Yes	Other (only routed mode)	Yes
Multi-instances supported?	Not Supported on 3100 Series	Multi-instances supported?	Not Supported on 3100 Series
Supported with clustered devices?	Not Supported on 3100 Series	Supported with clustered devices?	Not Supported on 3100 Series

Funktionsbeschreibung und exemplarische Vorgehensweise

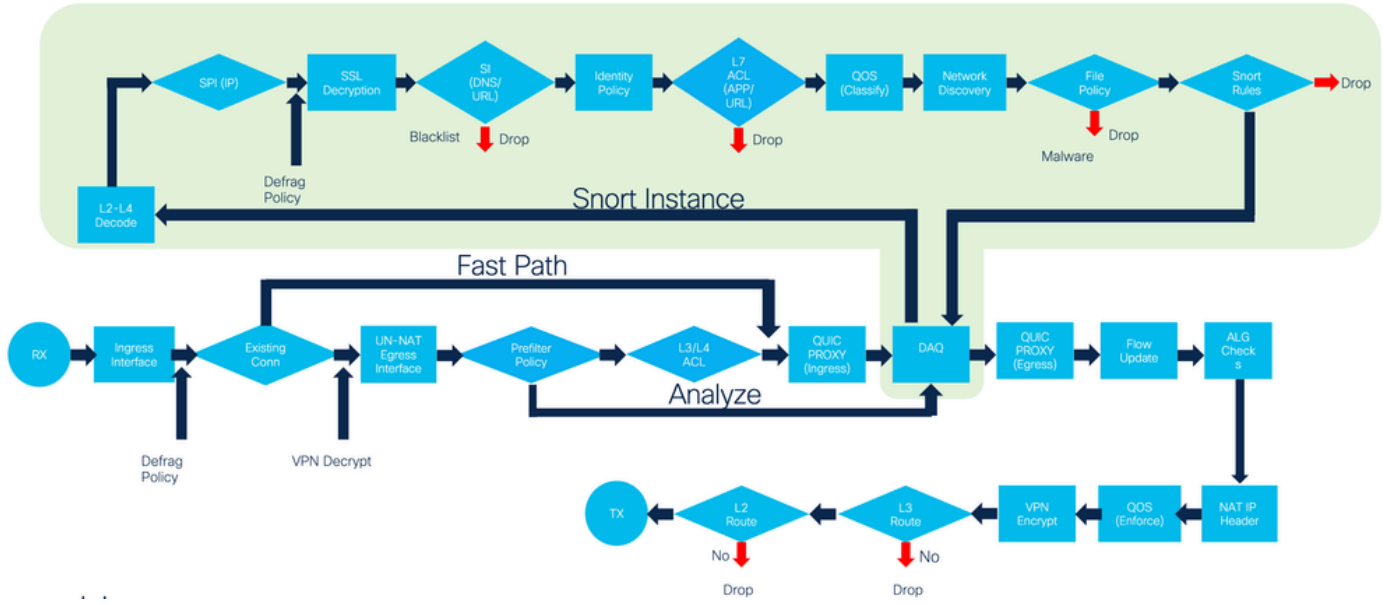
Beschreibung der Funktionsmerkmale

- Inline-Set-Netzwerkdiagramm



Inline-Set-Netzwerkdiagramm

- Der Datenverkehr fließt von Router 1 zu Router 2 über die Schnittstellen A und B und nutzt dabei nur eine physische Verbindung.
- FDM Inline Sets Paketverarbeitung - Flussdiagramm:



Flussdiagramm

- Inline-Sets:
  - Inline Sets werden auf physischen Schnittstellen und EtherChannels unterstützt.

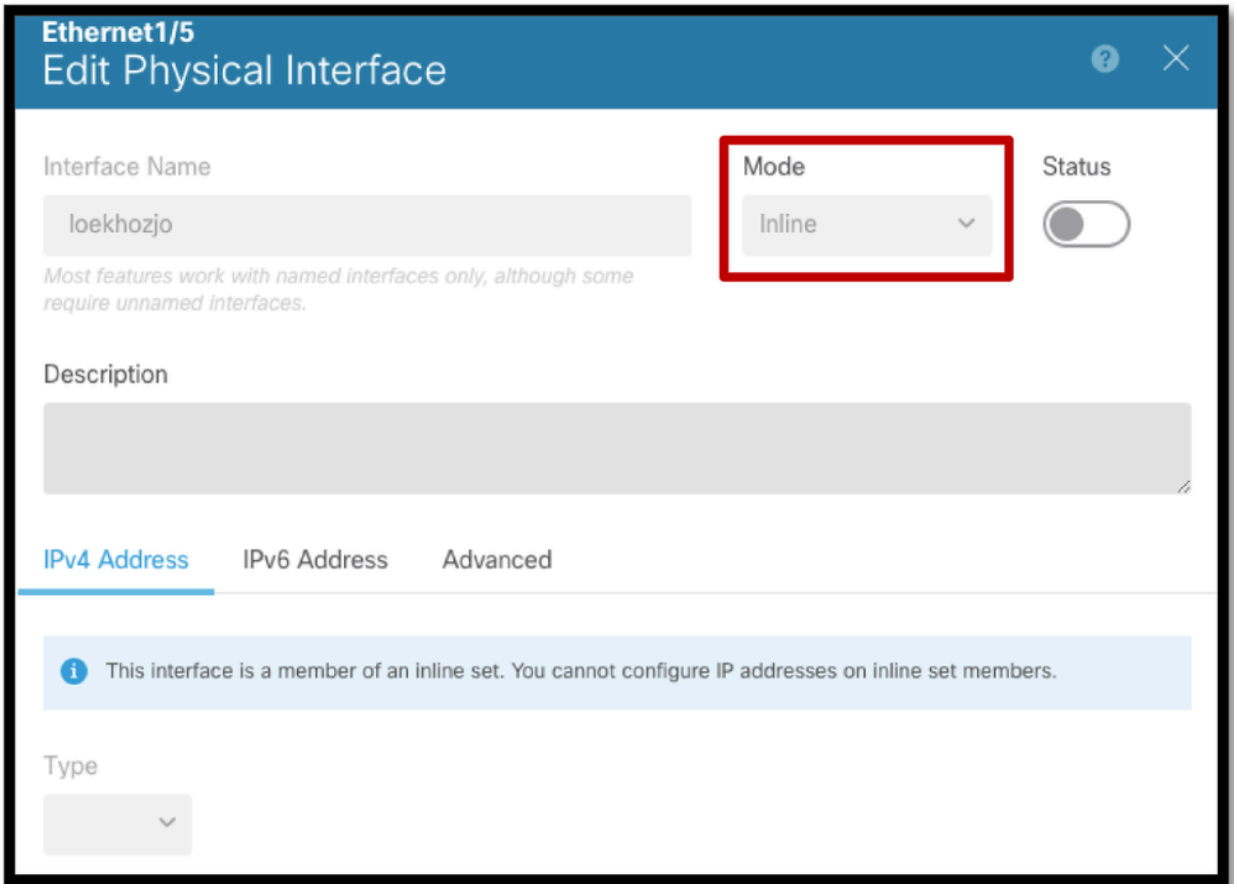
- Hardware-Umgehung:
  - Inline-Sets mit Hardwareumgehung werden von vorbestimmten physischen Schnittstellenpaaren unterstützt:
    Ethernet 1 und 2

Ethernet 2 und 3
Ethernet 4 und 5
Ethernet 5 und 6

- Schnittstellenunterstützung:
  - Schnittstellen, die Teil eines Inline-Paars sind:
    Muss benannt werden.
    Keine RisikenP-, DHCP- oder PPPoE-Konfigurationen.
    Darf sich nicht im passiven Modus befinden.
    Darf keine Management-Schnittstelle sein.
    Es darf jeweils nur in einem Inline-Paar verwendet werden.

- Details zum Inline-Modus
  - 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-Modus-GUI
  - Der Dialog Schnittstelle bearbeiten zeigt an, dass sich die Schnittstelle oder der EtherChannel im Inline-Modus befindet.
  - Änderungen sind an Schnittstellen im Inline-Modus nicht zulässig. Der Dialog Physische Schnittstelle bearbeiten (oder EtherChannel bearbeiten) ist schreibgeschützt.

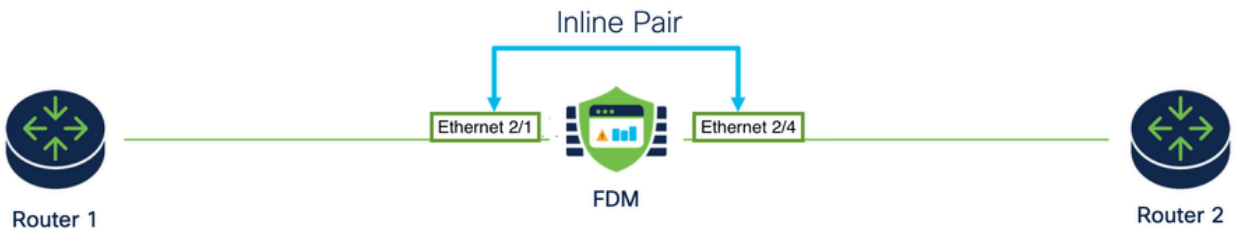


Schnittstelle in GUI bearbeiten

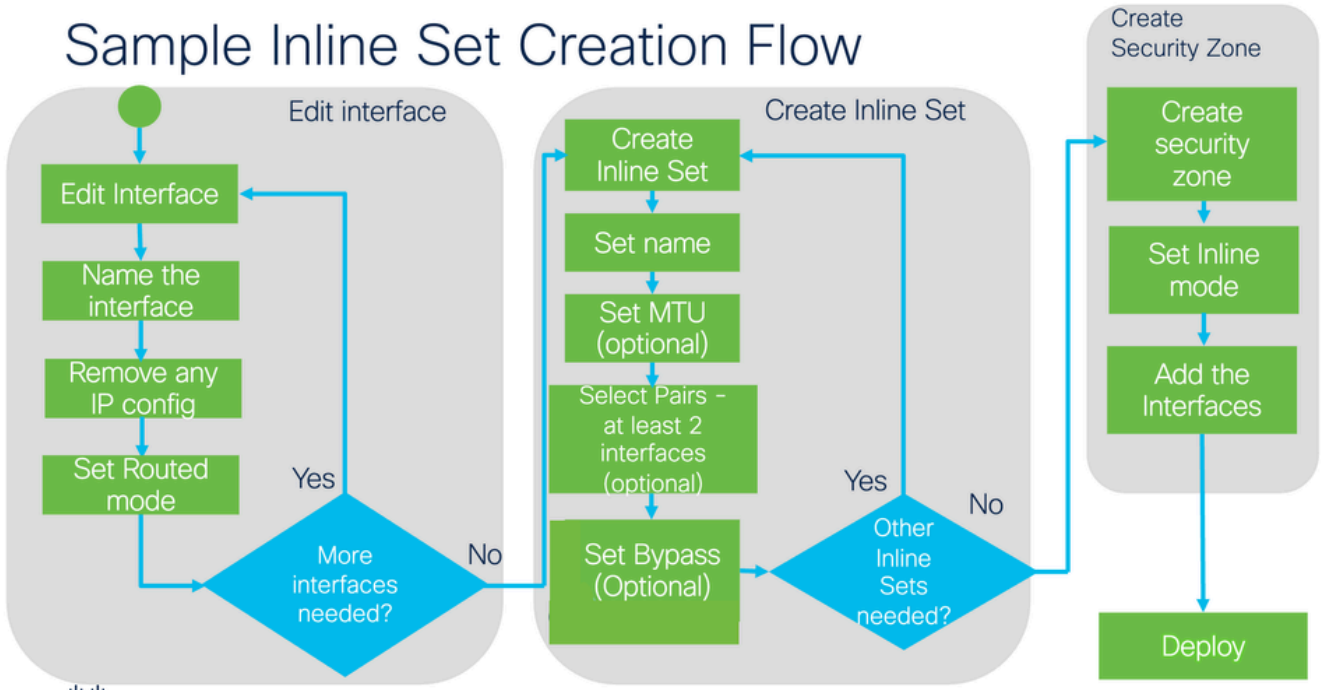
- Upgrade, Importieren/Exportieren, Sichern/Wiederherstellen, Bereitstellen
  - Auswirkungen eines Upgrades
    Der Benutzer kann FDM ohne Einschränkungen aktualisieren.
    Beim Upgrade von einer früheren Version werden vorhandene Inline Set Objects so konfiguriert, dass ihr Umgehungsfeld auf Disabled (Deaktiviert) festgelegt ist.
  - Import-/Exportauswirkungen
    Inline Set-Objekte werden importiert und exportiert.
  - Sichern/Wiederherstellen
    Inline Set-Objekte werden während der Sicherung/Wiederherstellung behandelt.
  - Bereitstellung
    Objekte werden normal bereitgestellt.
    Spezifische Fehler wurden implementiert.

Konfigurieren

Netzwerkdiagramm



Netzwerkdiagramm



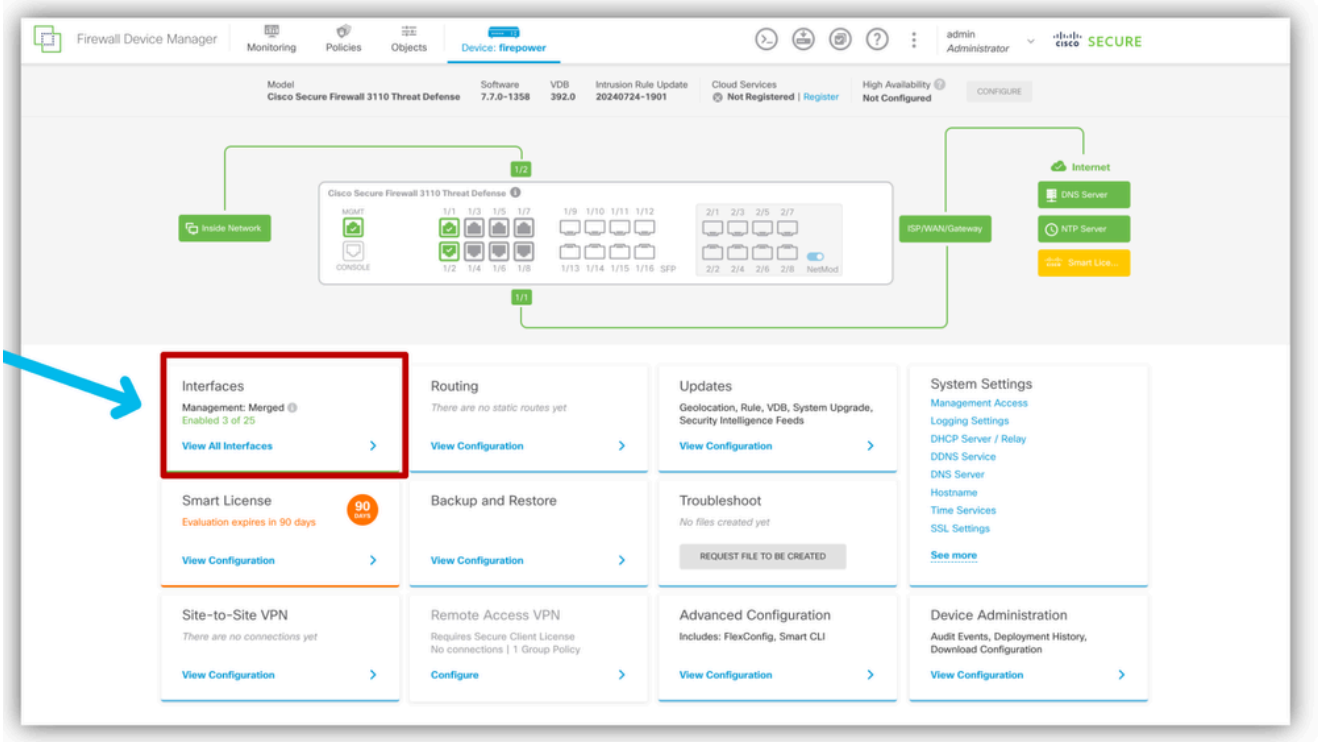
Inline Set-Erstellungsablauf

Konfigurationen

In diesem Abschnitt werden die Schritte zum Konfigurieren der Hardware-Umgehung auf FDM beschrieben.

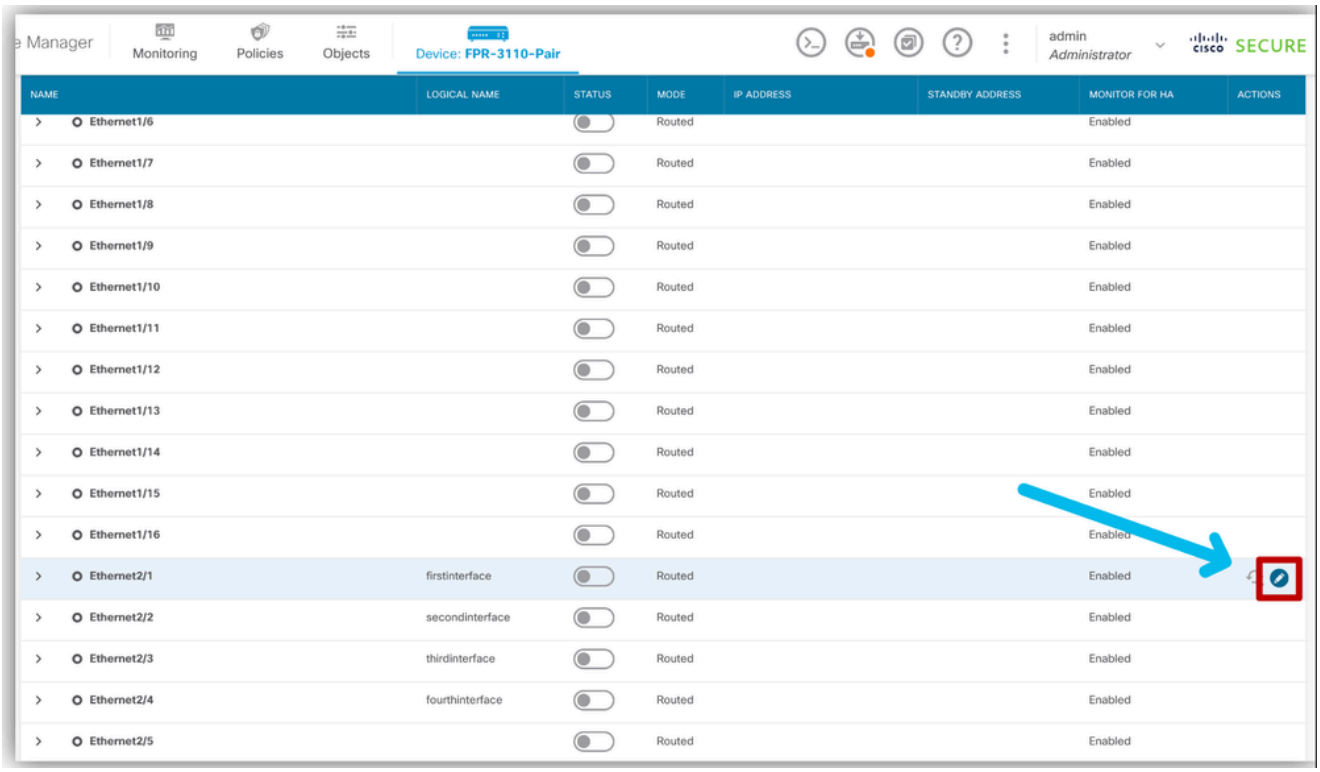
Schritt 1: Schnittstellen bearbeiten.

- Anmeldung bei FDM undfliegen nach Schnittstellenverwaltung:
- Klicken Sie im FDM-Dashboard auf die Karte Schnittstellen.



Schnittstelle auswählen

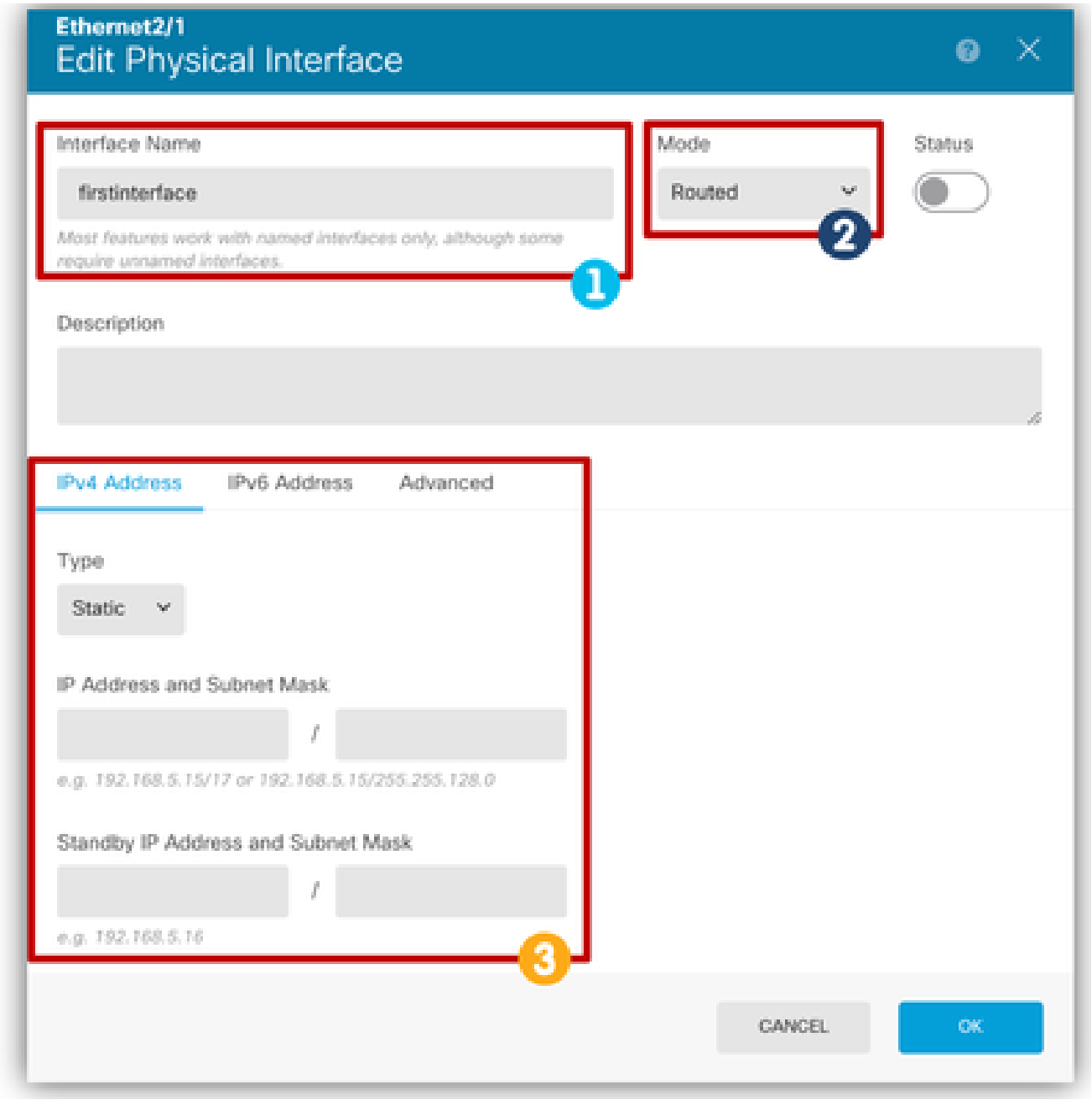
- Bearbeiten Sie die Schnittstellen, die im Inline-Set verwendet werden.
- Um Schnittstellen zu bearbeiten, klicken Sie auf das Bleistiftsymbol für die Schnittstelle.



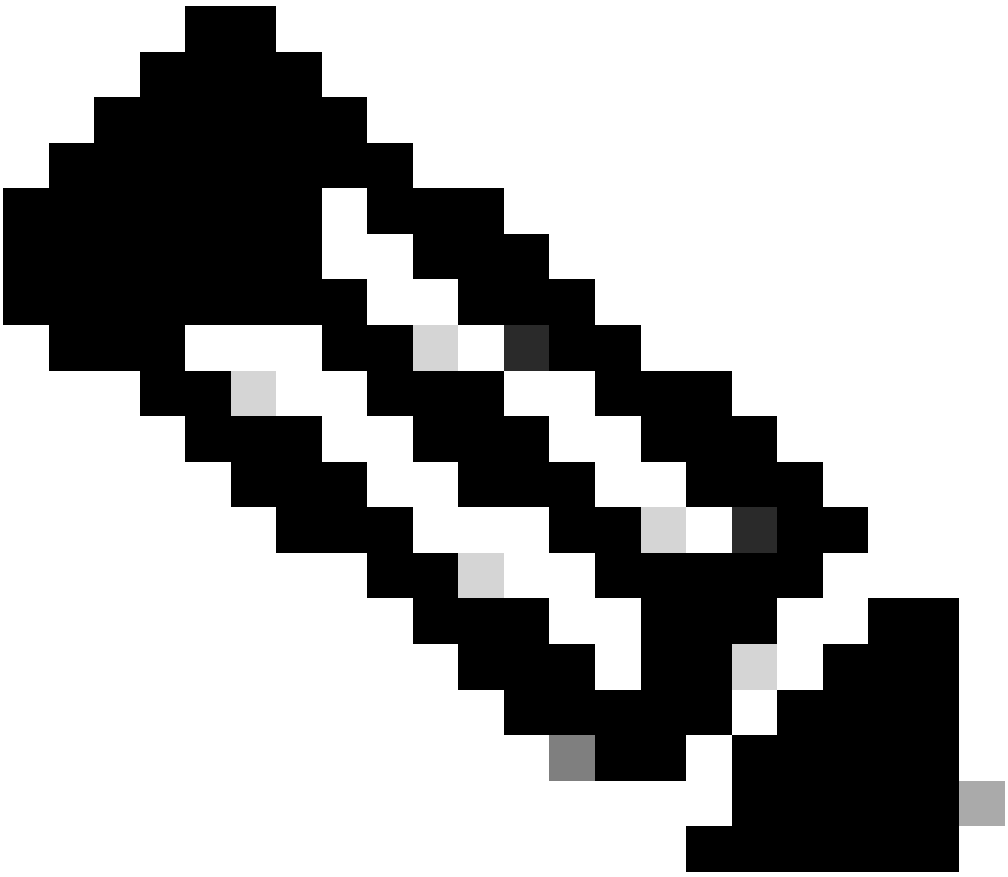
Schnittstelle bearbeiten

- Physische Schnittstelle bearbeiten:
  1. Benennen Sie die Schnittstelle.

2. Wählen Sie Routed Mode (Gerouteten Modus).
3. Entfernen Sie alle IP-Konfigurationen.



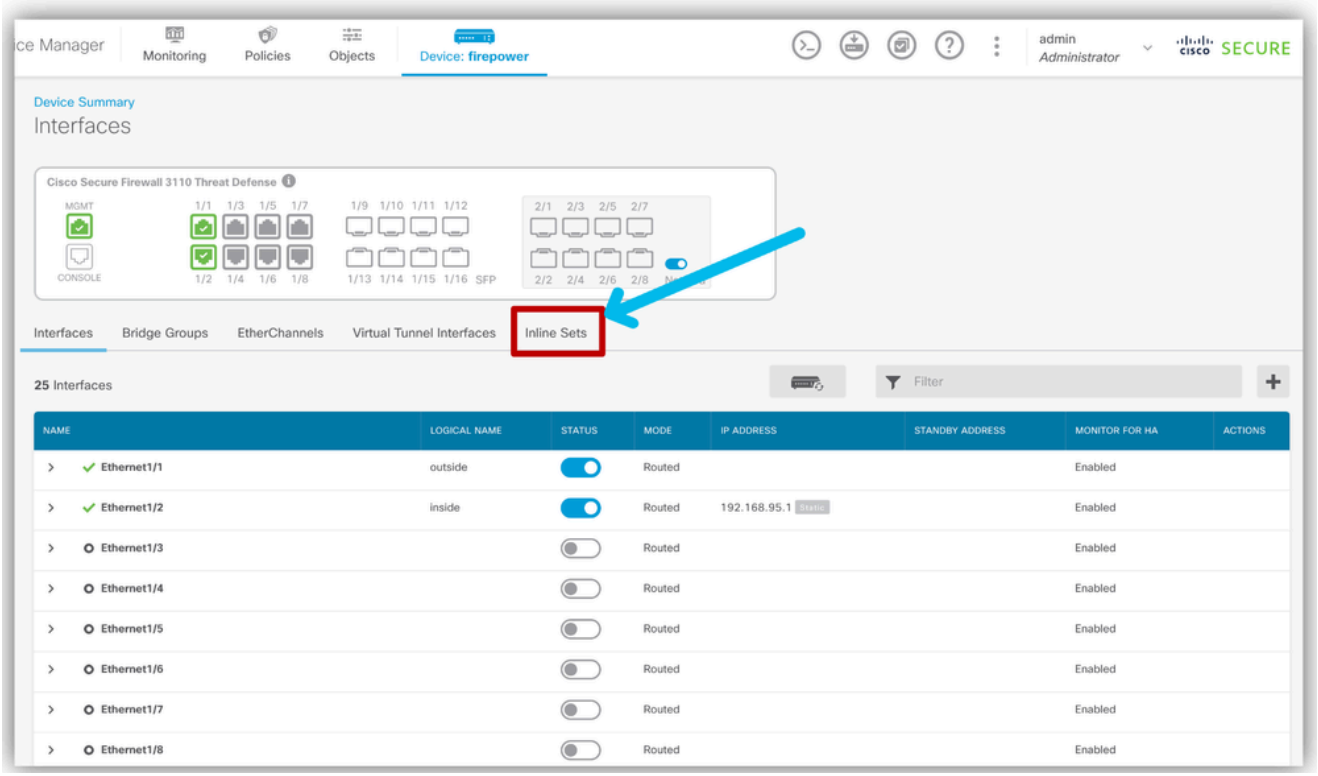
Parameter konfigurieren



Anmerkung: Der Modus wird automatisch in "Inline" geändert, nachdem die Schnittstelle einem Inline-Paar hinzugefügt wurde.

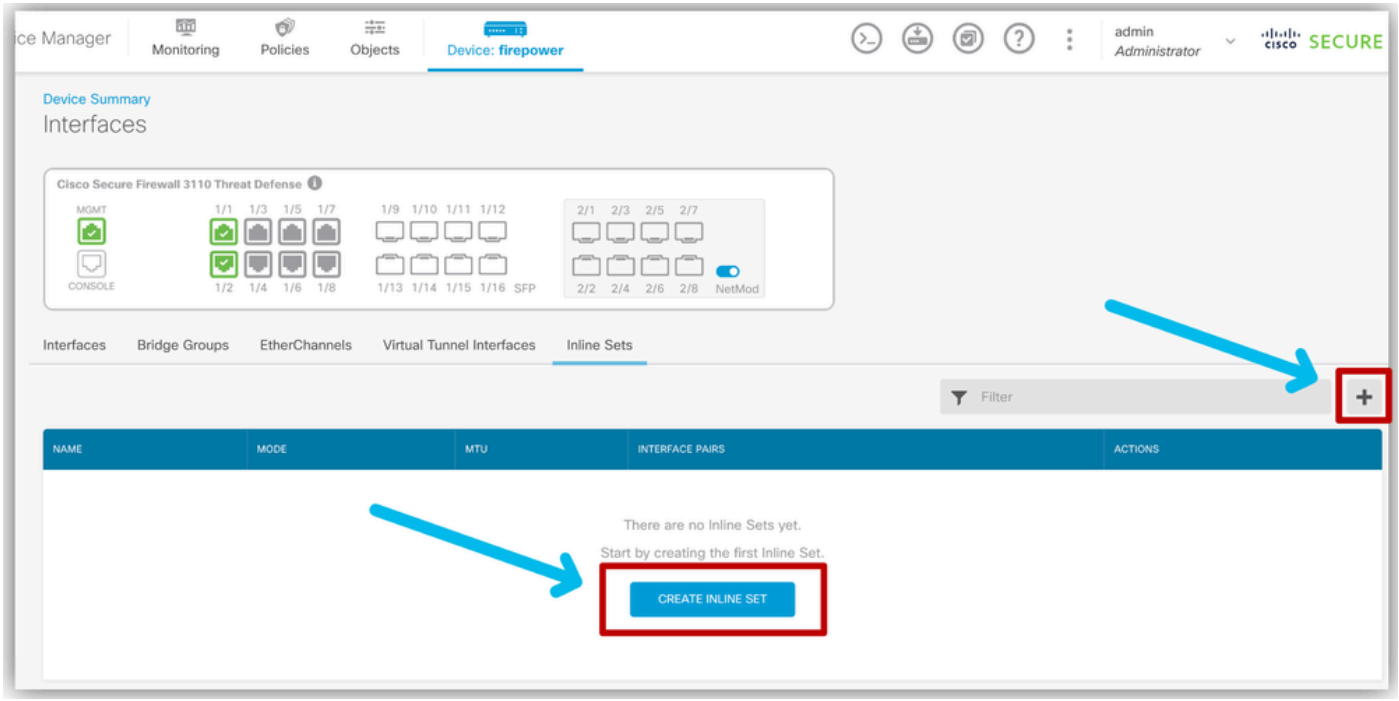
Phase 2: Erstellen eines Inline-Sets

- Navigieren Sie zur Registerkarte Device > Interfaces > Inline Sets.



Navigieren zur Registerkarte "Inline Sets"

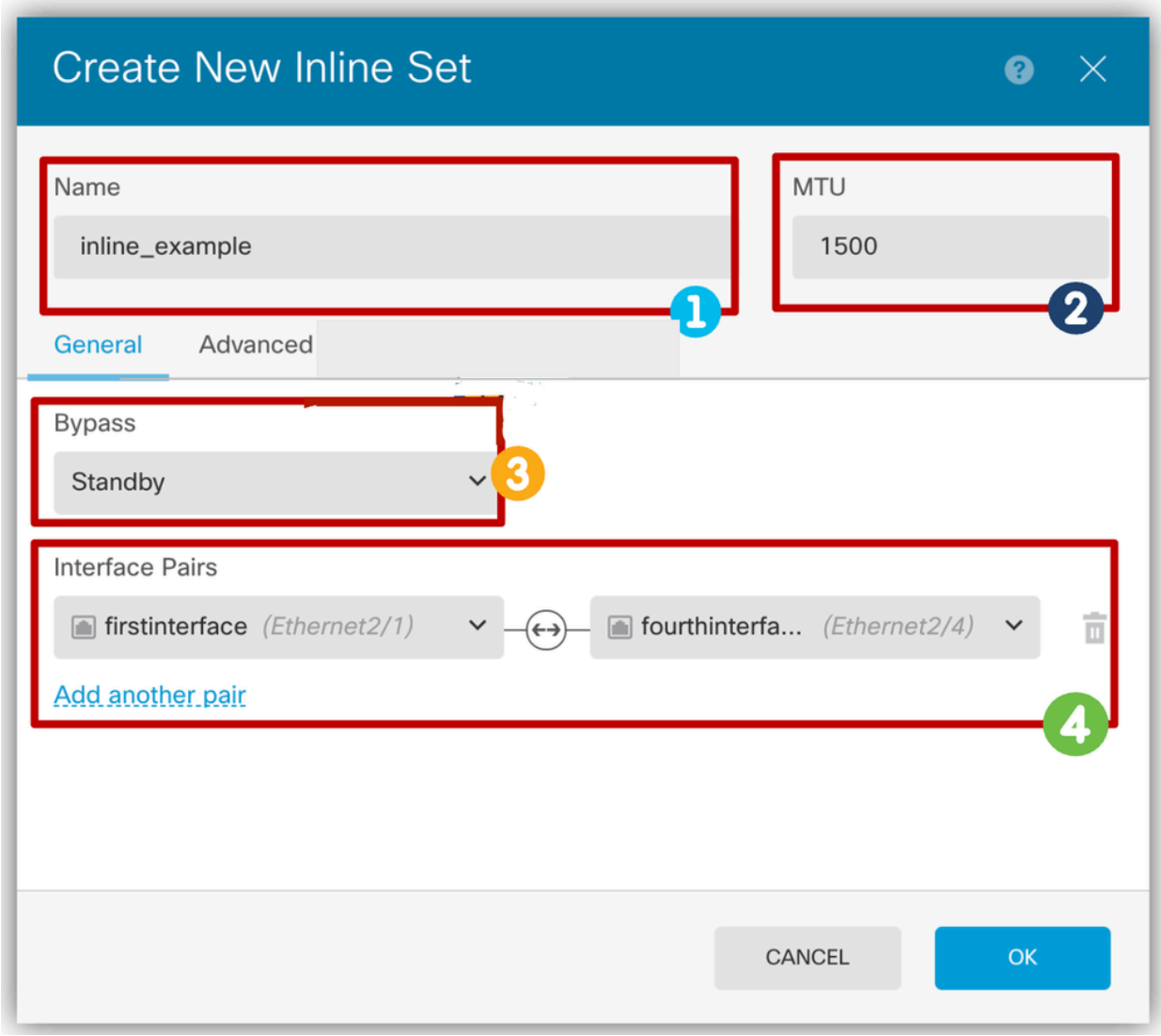
- Fügen Sie einen neuen Inline-Satz hinzu.
- Klicken Sie auf + Symbol oder auf die Schaltfläche "Inline-Set erstellen".



Inline-Set erstellen

.

- Konfigurieren der Grundeinstellungen
    1. Legen Sie einen Namen fest.
    2. Legen Sie die gewünschte MTU fest (optional). Der Standardwert ist 1500, die minimale unterstützte MTU.
    3. Wählen Sie Hardware Bypass (Details im nächsten Abschnitt verfügbar) aus. Für Bypass wurde ein neues Dropdown-Menü hinzugefügt.
    4. Wählen Sie im Abschnitt Schnittstellenpaare die Option Schnittstellen aus.
    5. Benannte Schnittstellen stehen zur Auswahl. Wenn mehr Paare erforderlich sind, klicken Sie auf den Link Weiteres Paar hinzufügen.



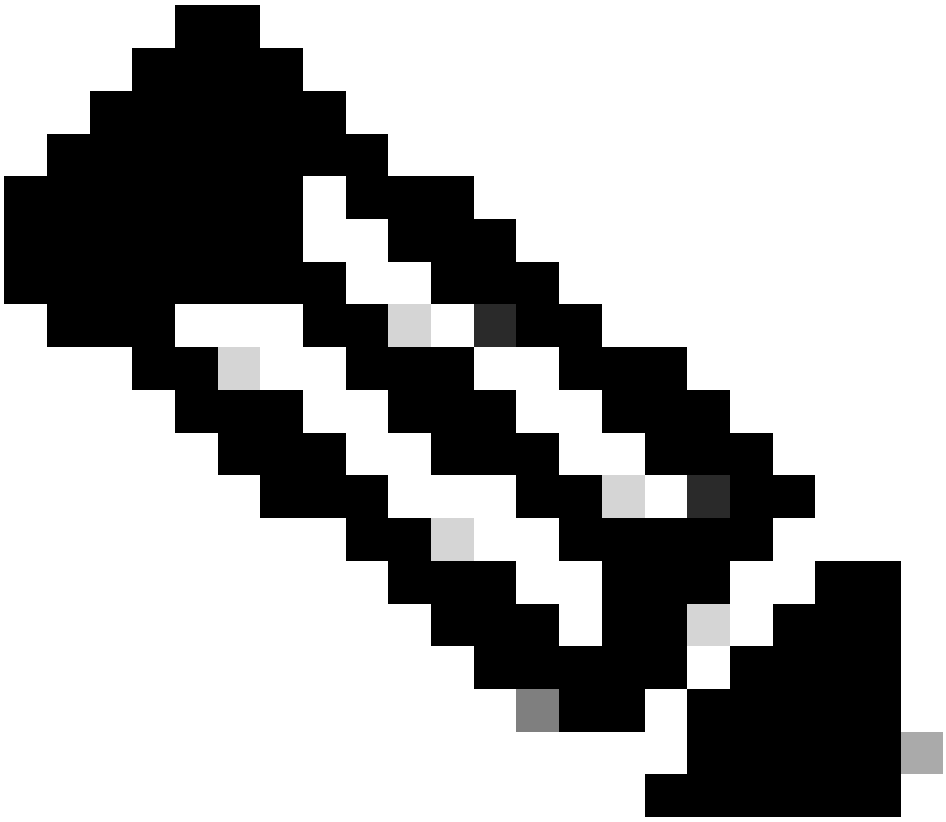
Einstellungen konfigurieren

Hardware-Umgehung

Funktionen und Einschränkungen

- Hardware Bypass stellt sicher, dass der Datenverkehr während eines Stromausfalls

weiterhin zwischen einem Inline-Schnittstellenpaar fließt. Diese Funktion kann verwendet werden, um die Netzwerkverbindung bei Software- oder Hardwarefehlern aufrechtzuerhalten.
- Hardware-Bypass-Ports werden nur für Inline-Sets unterstützt.
- Hardware Bypass wird im Hochverfügbarkeitsmodus NICHT unterstützt.
- Hardware-Umgehungsmodi:
  - DISABLED - Deaktiviert die Umgehung auf unterstützten Schnittstellen. Standardmodus für nicht unterstützte Schnittstellen.
  - STANDBY - Im Standby-Zustand bleiben die Schnittstellen im Normalbetrieb, bis ein Triggerereignis eintritt.
  - BYPASS FORCE - Zwingt das Schnittstellenpaar manuell dazu, die Überprüfung zu umgehen.



Anmerkung: Informationen zu FTD-Schnittstellentypen und Hardware-Umgehung

---

Snort Fail Open und Hardware Bypass

- Die Funktion "Hardware Bypass" (Hardware-Umgehung) ermöglicht den Datenverkehrsfluss während eines Hardwareausfalls, einschließlich eines vollständigen Stromausfalls, und

bestimmter begrenzter Softwareausfälle.
- Ein Softwarefehler, der Snort Fail Open auslöst, löst keine Hardware-Umgehung aus.

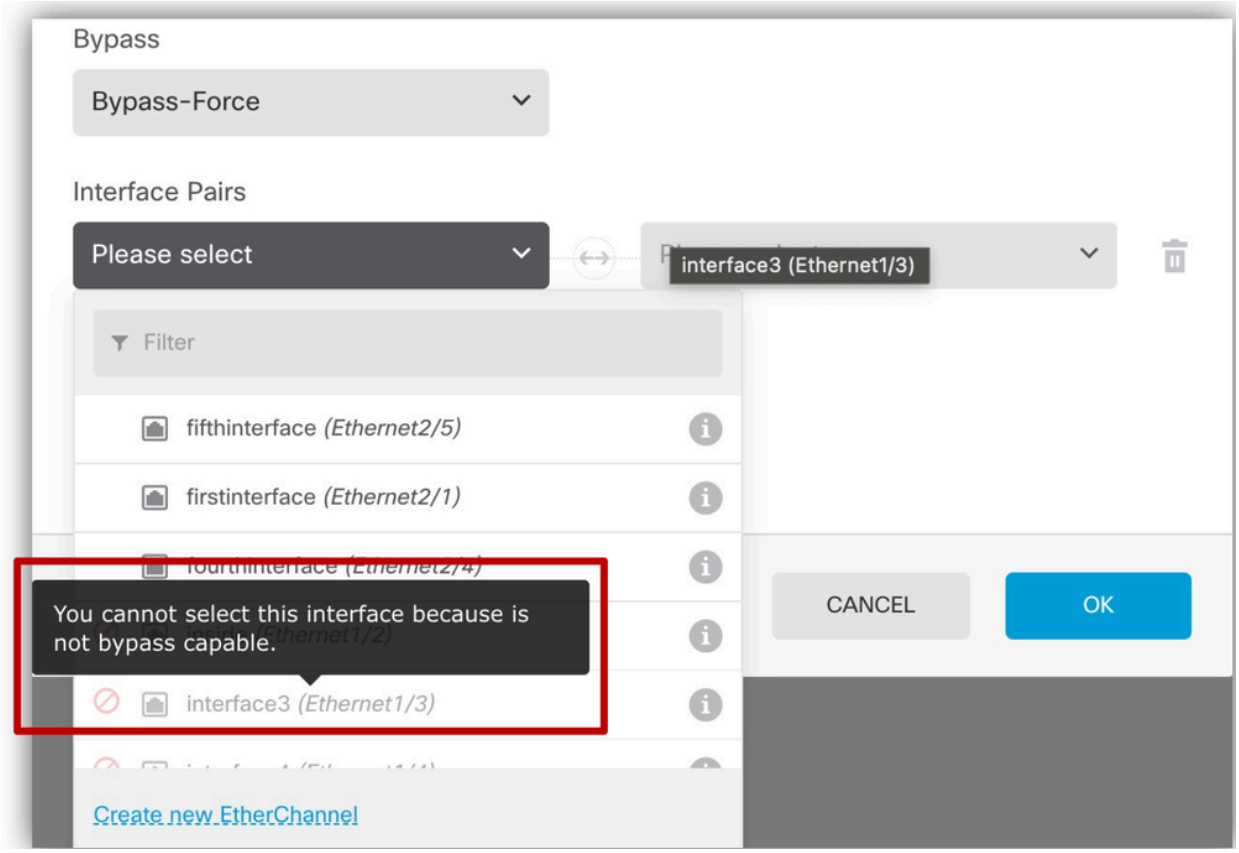
Hardware-BypassTrigger

Die Hardware-Umgehung kann in folgenden Szenarien ausgelöst werden:

- Anwendungsabsturz
- Anwendungsneustart
- Geräteabsturz
- Neustart oder Upgrade von Geräten
- Stromausfall bei Geräten
- Manueller Trigger

So zeigen Sie an, welche Schnittstellen Hardware Bypass unterstützen:

- Wenn in der FDM-GUI Bypass (Umgehung) ausgewählt ist:
  - Schnittstellen, die diese unterstützen, sind auswählbar.
  - Nicht unterstützte Schnittstellen sind ausgegraut.
  - Bei diesem Beispiel ist Ethernet1/3 in der folgenden Abbildung abgeblendet:

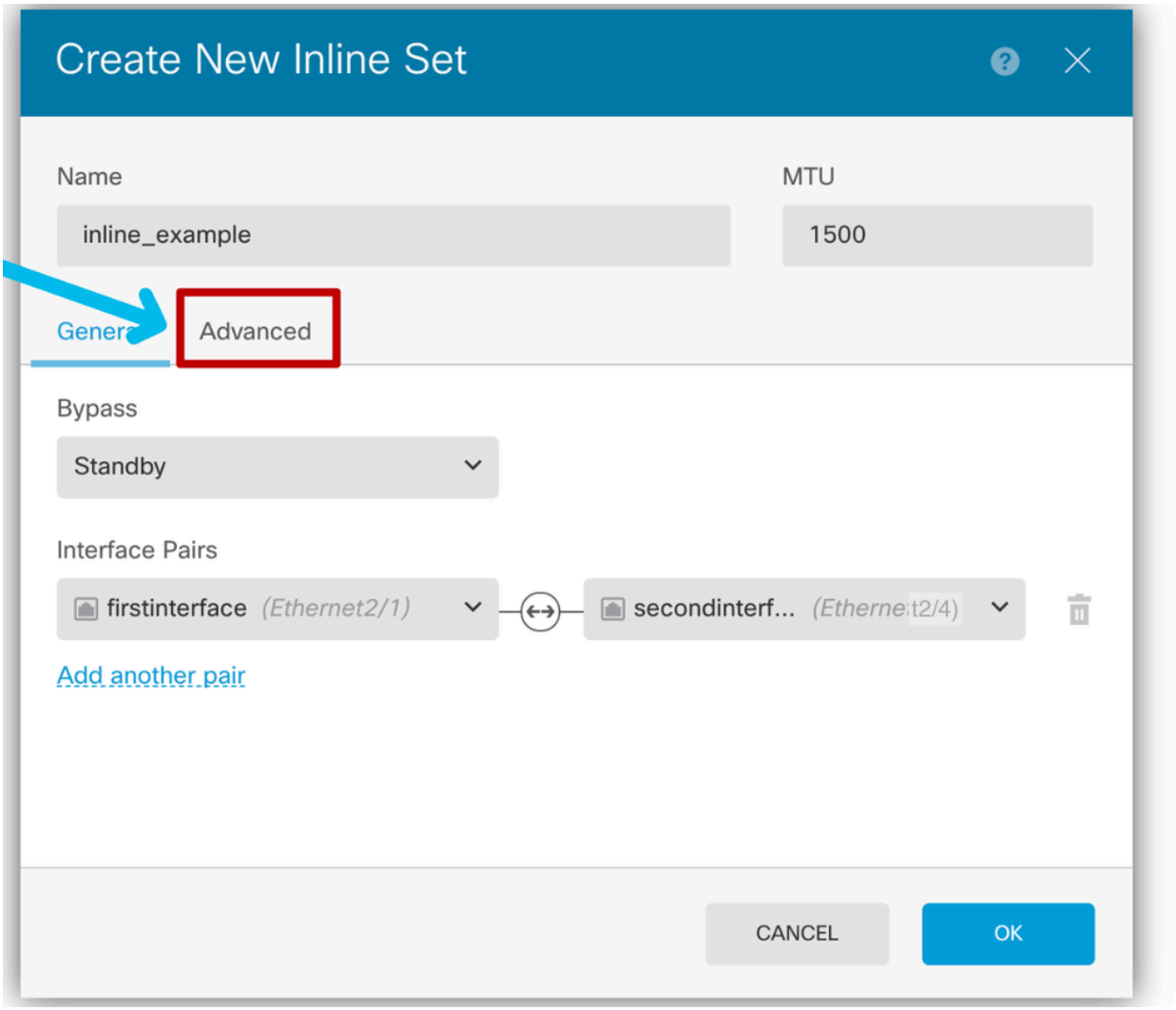


Überprüfung der Unterstützung für Hardwareumgehung

Schritt 3: Konfigurieren Sie die erweiterten Einstellungen für Inlinesets.

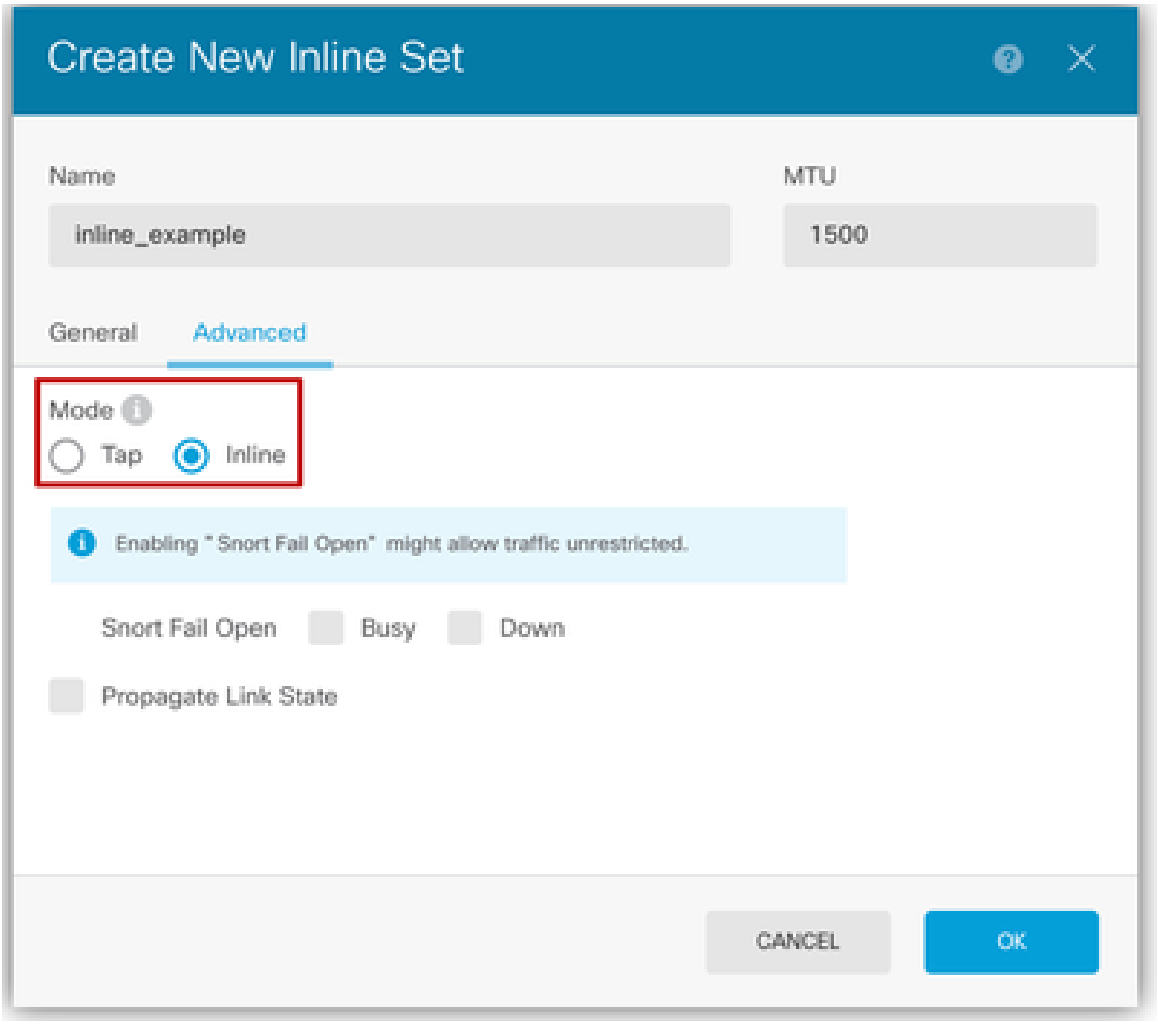
- Navigieren Sie zur Registerkarte Gerät > Schnittstellen > Inline-Sets, oder bearbeiten Sie ein bereits erstelltes Inline-Set.

- Navigieren Sie zur Registerkarte Erweitert.
  - Auf der Registerkarte Erweitert können Sie die Einstellung von Optionen für Inline-Sets konfigurieren.
  - Klicken Sie auf die Registerkarte Advanced (Erweitert).



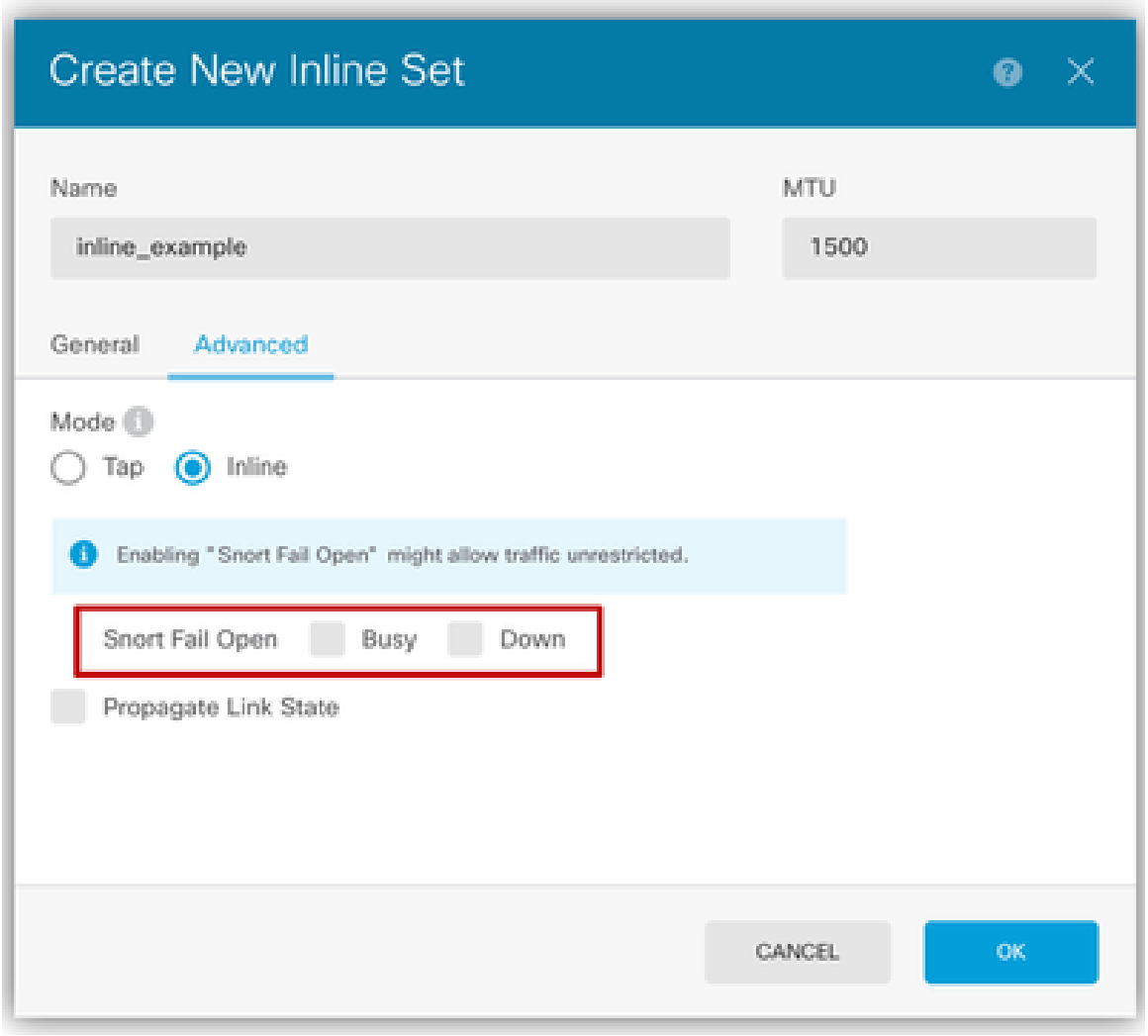
Inline-Set konfigurieren

  - Modus
    - Tippen: Stellt den Inline-Tipp-Modus ein.Wenn der Tap-Modus aktiviert ist, ist Snort Fail Open deaktiviert.
    - Inline



Modus auswählen

- Open-Einstellungen für Snort fehlgeschlagen.
  - Wählen Sie die gewünschten Snort Fail Open-Einstellungen aus.
  - Keine, eine oder beide. Die Optionen Besetzt und Abwärts können eingestellt werden.
  - 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.

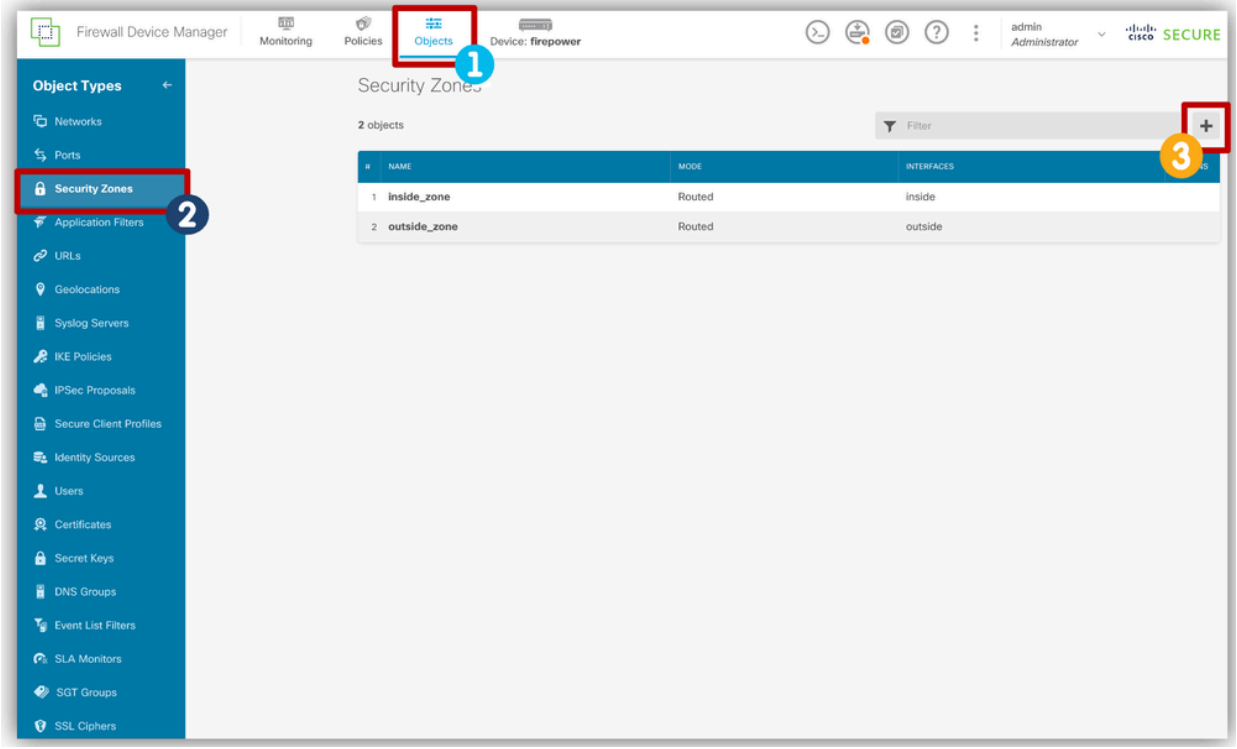


Snort Fail Open und Propagate Link State

- Verknüpfungsstatus propagieren.
  - Propagate Link State (Verbindungsstatus propagieren) deaktiviert automatisch die zweite Schnittstelle im Inline-Paar, wenn eine der Schnittstellen ausfällt. Wenn die ausgefallene Schnittstelle wieder verfügbar ist, wird auch die zweite Schnittstelle automatisch wieder aktiviert.
- Klicken Sie auf OK, um den Inline-Satz zu erstellen.

Schritt 4: Auf eine Sicherheitszone anwenden (optional).

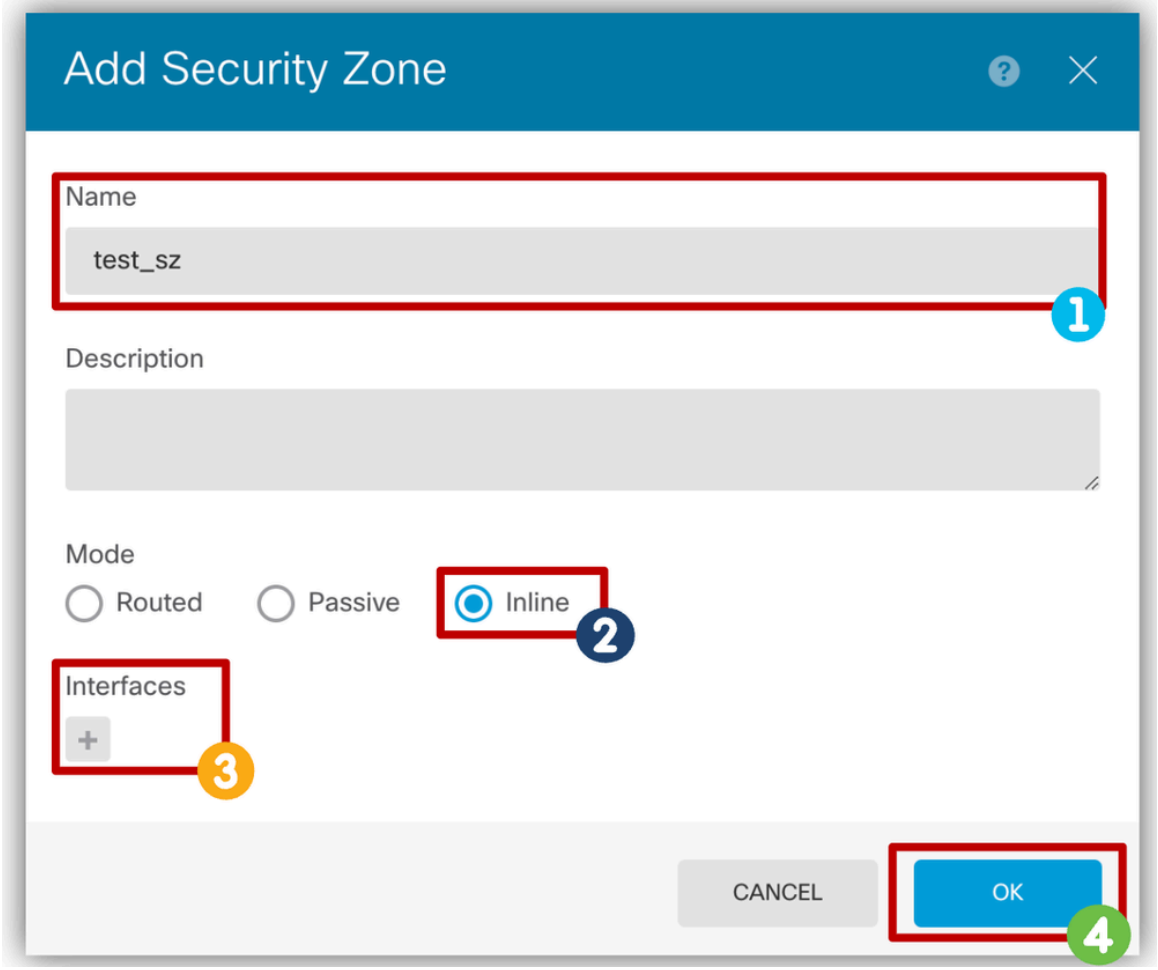
1. Navigieren Sie in der oberen Navigationsleiste zu Objekte.
2. Wählen Sie in der linken Navigationsleiste Sicherheitszonen aus:
   - Klicken Sie auf +, um eine Sicherheitszone hinzuzufügen.



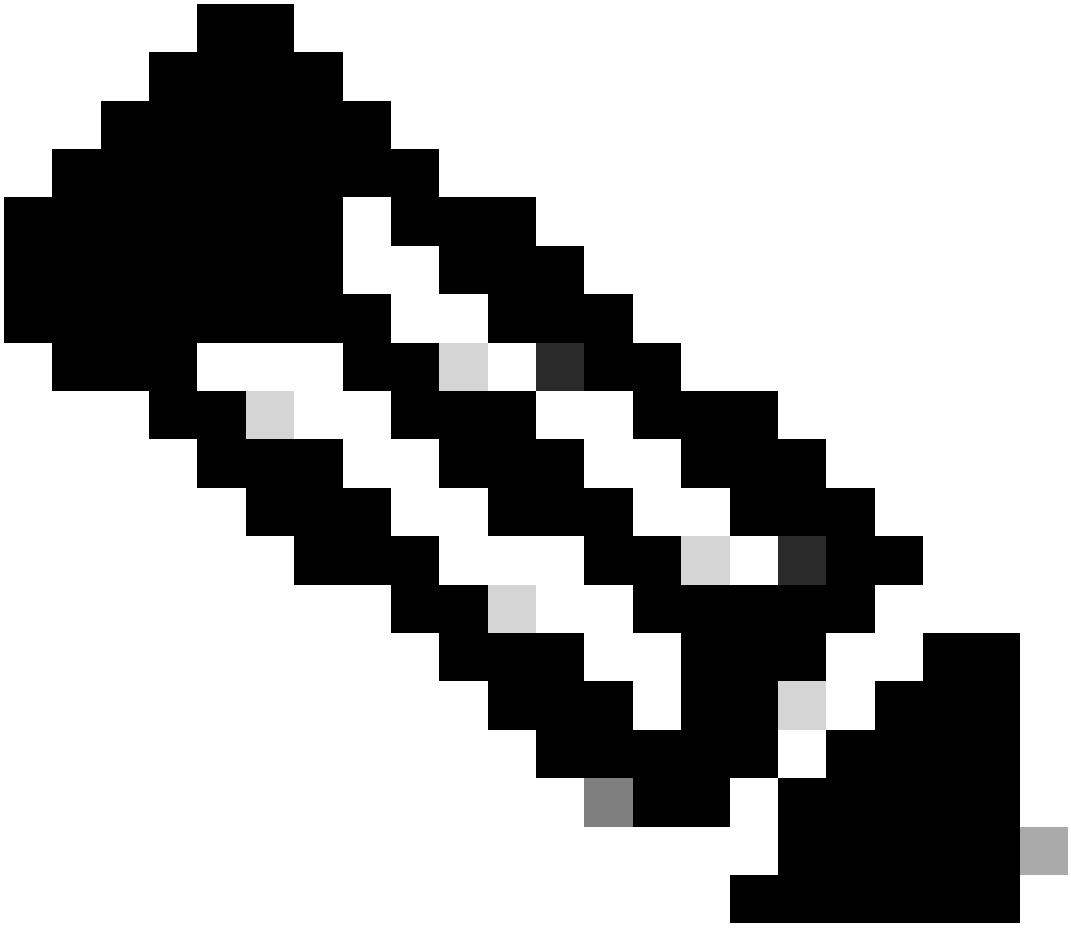
Hinzufügen einer Sicherheitszone

Konfigurieren der Sicherheitszone (optional)

1. Nennen Sie die Sicherheitszone.
2. Wählen Sie den Inline-Modus aus.
   Sicherheitszonen und -schnittstellen müssen den gleichen Modus haben.
3. Wählen Sie Schnittstellen aus, die Teil des Inline-Sets sind.
4. Klicken Sie auf OK.



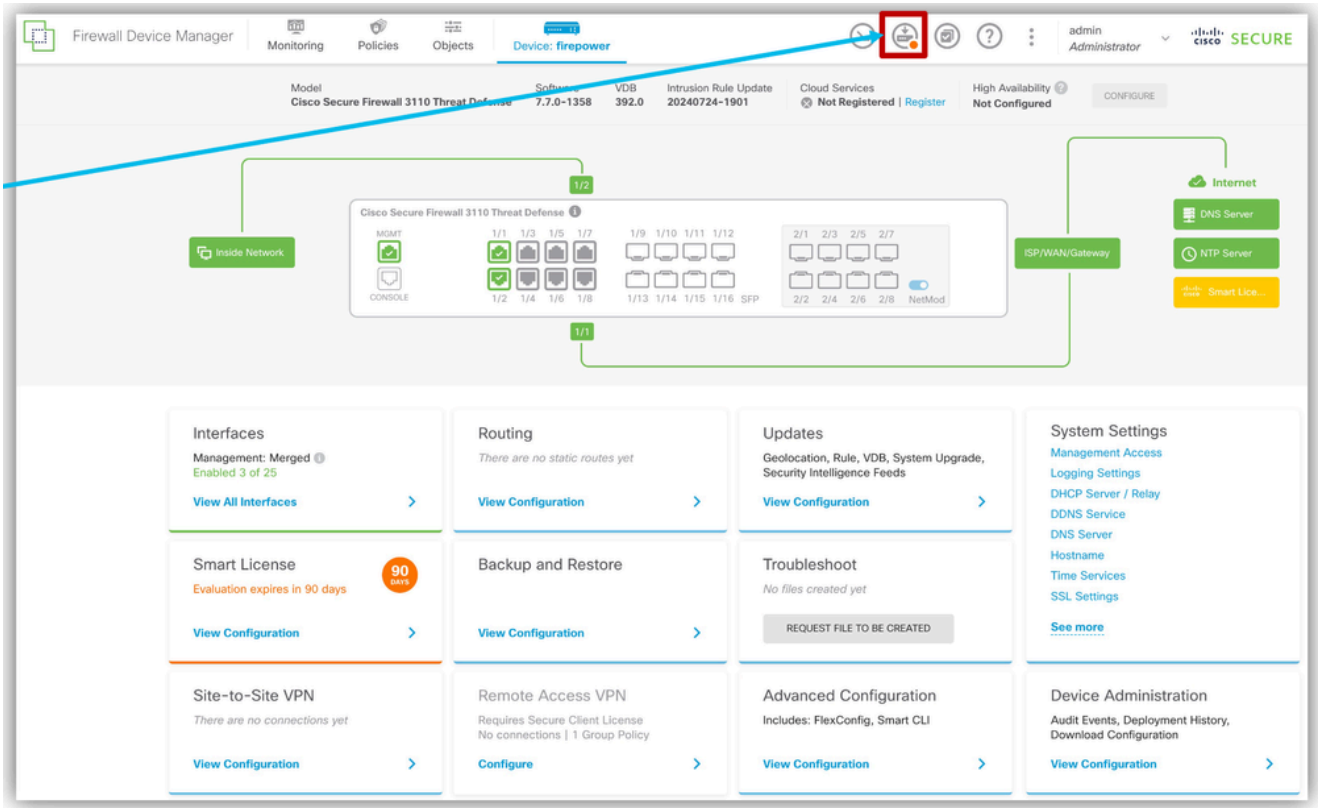
Sicherheitszone konfigurieren



Anmerkung: Bei Schnittstellen wurde der Modus automatisch in "Inline" geändert, nachdem die Schnittstelle einem Inline-Paar hinzugefügt wurde.

Schritt 4: Bereitstellung

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



Änderungen bereitstellen

- Inlinesätze bearbeiten und löschen.
  - Navigieren Sie zur Registerkarte Device > Interfaces > Inline Sets.
  - Schaltflächen zum Bearbeiten und Löschen stehen für Inline-Sets zur Verfügung.

Inline-Sets bearbeiten und löschen

REST-APIs für FDM-Geräte

REST-API-Endpunkte

- GET: /devices/default/inlinesets
  Abrufen einer Liste aller vorhandenen Inline-Sets

- GET:/devices/default/inlinesets/{objID}
  Abrufen eines bestimmten Inline-Set-Objekts anhand seiner ID
- POST: /devices/default/inlinesets
  Erstellen Sie einen neuen Inline-Satz.
- PUT: /devices/default/inlinesets/{objID}
  Vorhandenes Inline-Set-Objekt anhand seiner ID aktualisieren
- LÖSCHEN:/devices/default/inlinesets/{objID}
  Vorhandenes Inline-Set-Objekt anhand seiner ID löschen.
- GET:/operating/interface/objID}
  Abrufen einer Liste aller InterfaceInfoentity.
- Zur Unterstützung von Hardware Bypass wurde der InterfaceInfo-API ein neues Feld hinzugefügt.

Schnittstelleninfo REST API-Modelle

- Ein neues Feld "bypassInterfacePeerId" wurde hinzugefügt, um die Integration der Hardwareumgehung zu unterstützen.
- Dieses Feld stellt die ID des Schnittstellenpaars Hardwareumgehung für die aktuelle Schnittstelle dar.
- Werte:
  - Null - Schnittstelle unterstützt keine Umgehung.
  - ID - Schnittstelle unterstützt Umgehung.

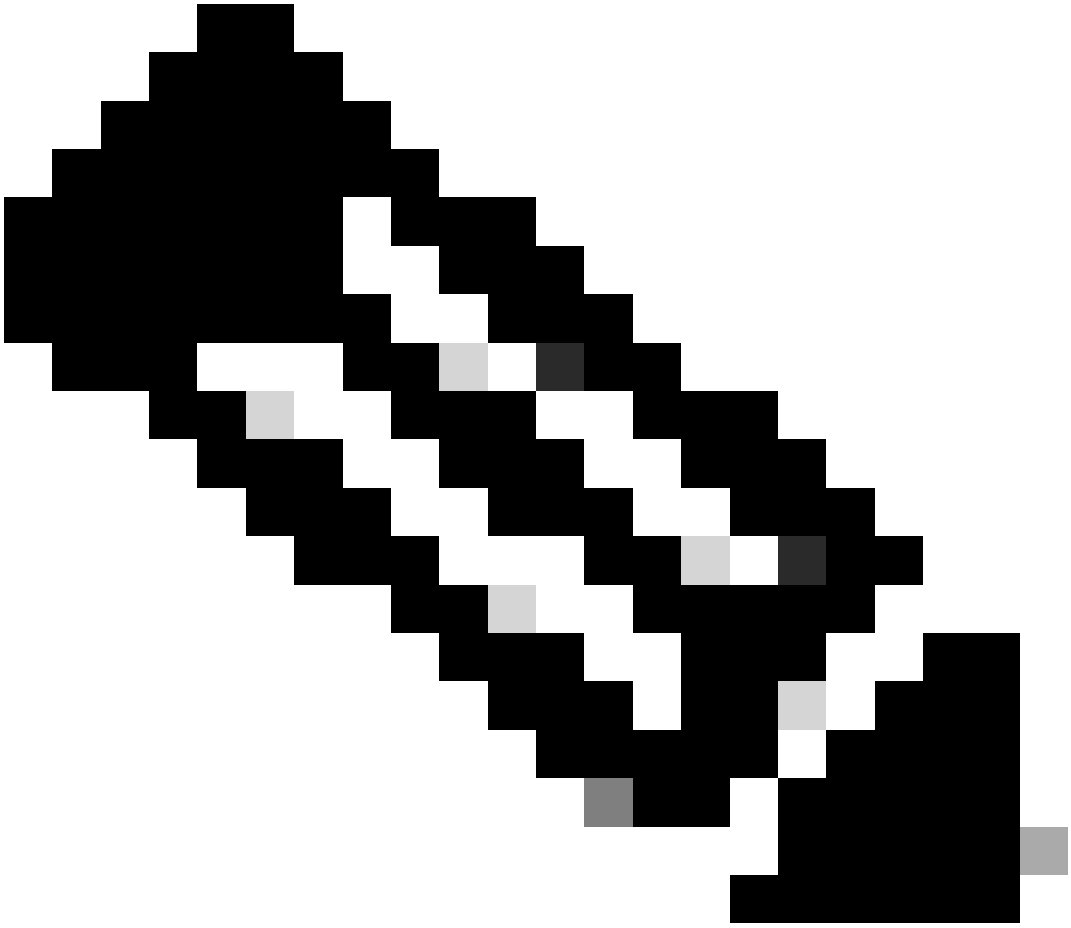
REST-API für Schnittstelleninformationen

Beispiel für REST-API für Schnittstelleninfo

- Schnittstelle Info REST API-Beispiel.
  - Schnittstelle ohne Hardware-Bypass-Unterstützung (Ethernet 1/4).
  - Schnittstellenpaar mit Unterstützung für Hardwareumgehung (Ethernet2/1 und Ethernet 2/2).

```
{ "interfaceInfoList": [
    {
        "interfaceId": "da9edc2d-58ba-11ef-b764-ffea0b8d9fa2",
        "hardwareName": "Ethernet1/4",
        "bypassInterfacePeerId": null,
        ...
    },
    {
        "interfaceId": "dbe9d2c1-58ba-11ef-b764-396644d1c752",
        "hardwareName": "Ethernet2/1",
        "bypassInterfacePeerId": "dc74fbc3-58ba-11ef-b764-11d423dbcbd7",
        ...
    },
    {
        "interfaceId": "dc74fbc3-58ba-11ef-b764-11d423dbcbd7",
        "hardwareName": "Ethernet2/2",
        "bypassInterfacePeerId": "dbe9d2c1-58ba-11ef-b764-396644d1c752",
        ...
    }],
  "id": "default",
  "type": "interfaceinfo",
  "links": { "self": "https://u90c04p02-
vrouter.cisco.com:25455/api/fdm/v6/operational/interfaceinfo/1/default"
    }
}
```


Beispiel für REST-API für Schnittstelleninfo



Anmerkung: Dies ist ein Ausschnitt aus dem vollständigen Aufruf, aufgrund seiner Größe.

Inline Set REST APIs-Modell

- Das Inline Set-Modell besteht aus:
  - Typ
  - Name
  - Tap-Modus
  - MTU
  - Verknüpfungsstatus propagieren
  - Fehler bei geöffnetem Snort bei Besetzt
  - Bypass-Werte: DISABLED, STANDBY, BYPASS_FORCE

Inline Set REST-API

Inline Set REST API - Beispiel

- Grundlegende Inline Set-Beispiele:

- Ein Inline-Paar
- Standby umgehen

```
{
  "name": "inline_set_example",
  "type": "inlineset",
  "tapMode": false,
  "mtu": 1500,
  "propagateLinkState": false,
  "failOpenSnortBusy": false,
  "failOpenSnortDown": true,
  "bypass": "STANDBY",
  "inlinePairs": [
    {
      "first": {
        "id": "12345-6789-1234-56789",
        "type": "physicalinterface"
      },
      "second": {
        "id": "12345-6789-1234-56789",
        "type": "physicalinterface"
      },
      "type": "inlinesetpair"
    }
  ]
}
```

Bei anderen Bypass-Modi muss STANDBY durch DISABLED oder BYPASS_FORCE ersetzt werden.

Konfigurieren und Bereitstellen eines Inline-Sets

1.Schnittstellen-IDs abrufen (Payload-Beispiele finden Sie im API-Explorer).

GET/Geräte/Standard/Schnittstellen
2.Create Inline Set (Payload-Beispiele finden Sie im API Explorer).

POST/Geräte/Standard/Inlinesets
3.Erstellen Sie eine Sicherheitszone (Payload-Beispiele finden Sie im API-Explorer) (optional).
POST/Objekt/Sicherheitszonen
4.Deploy auf Gerät (siehe API Explorer für Payload-Beispiele).
POST/Betrieb/Bereitstellung

Konfiguration und Bereitstellung eines Inline-Sets mit Hardware-Bypass

1.Laden Sie Schnittstellen-IDs und Informationen zu Hardware Bypass-Schnittstellenpaaren herunter (Payload-Beispiele finden Sie im API-Explorer).
GET/Operational/Interfaceinfo/{objId}
2.Create Inline Set (Payload-Beispiele finden Sie im API Explorer).
POST/Geräte/Standard/Inlinesets
3.Erstellen Sie eine Sicherheitszone (Payload-Beispiele finden Sie im API-Explorer) (optional).
POST/Objekt/Sicherheitszonen
4.Deploy auf Gerät (siehe API Explorer für Payload-Beispiele).
POST/Betrieb/Bereitstellung

Bearbeiten eines Inlinesatzes

1. Schnittstellen-IDs abrufen (Payload-Beispiele finden Sie im API-Explorer).
GET/Geräte/Standard/Schnittstellen
2. Inline-Sets abrufen.
GET/devices/default/inlinesets
3. Bearbeiten Sie den Inline-Satz (Beispiele für Payloads finden Sie im API-Explorer).
PUT/devices/default/inlinesets/{objId}
4. Bereitstellung auf Gerät (Payload-Beispiele finden Sie im API-Explorer).
POST/Betrieb/Bereitstellung

Überprüfung

<#root>

```
> show running-config inline-set
```

```
inline-set test_inline_0
    interface-pair test2 test1
inline-set test_inline_1
```

hardware-bypass standby

```
    interface-pair test27 test28
inline-set test_inline_2
    hardware-bypass bypass
    interface-pair test26 test25
```

> show inline-set

```
 Inline-set test_inline_0
   Mtuis 1600 bytes
   Fail-open for snort down is off
   Fail-open for snort busy is off
   Tap mode is off
   Propagate-link-state option is off
```

hardware-bypass mode is disabled

```
   Interface-Pair[1]:
     Interface: Ethernet1/3 "test1"
       Current-Status: DOWN
     Interface: Ethernet1/4 "test2"
       Current-Status: DOWN
     Bridge Group ID: 519
```

> show inline-set

```
Inline-set test_inline_1
Mtuis 1500 bytes
Fail-open for snort down is off
Fail-open for snort busy is off
Tap mode is off
Propagate-link-state option is off
hardware-bypass mode is standby
Interface-Pair[1]:
Interface: Ethernet2/7 "test27"
Current-Status: DOWN
Interface: Ethernet2/8 "test28"
Current-Status: DOWN
Bridge Group ID: 618
```

> show inline-set

```
Inline-set test_inline_1
Mtuis 1500 bytes
Fail-open for snort down is off
Fail-open for snort busy is off
Tap mode is off
Propagate-link-state option is off
```

```
hardware-bypass mode is bypass


Interface-Pair[1]:
Interface: Ethernet2/6 "test26"
Current-Status: DOWN
Interface: Ethernet2/5 "test25"
Current-Status: DOWN
Bridge Group ID: 610


> show interface



...
Interface Ethernet1/7 "", is admin down, line protocol is down
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec
Available but not configured via nameif

...
Interface Ethernet2/7 "", is admin down, line protocol is down
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec

Hardware bypass is supported with interface Ethernet2/8


Available but not configured via nameif

...
Interface Ethernet2/8 "", is admin down, line protocol is down
Hardware is EtherSVI, BW 1000 Mbps, DLY 10 usec

Hardware bypass is supported with interface Ethernet2/7


Available but not configured via nameif
```

Fehlerbehebung

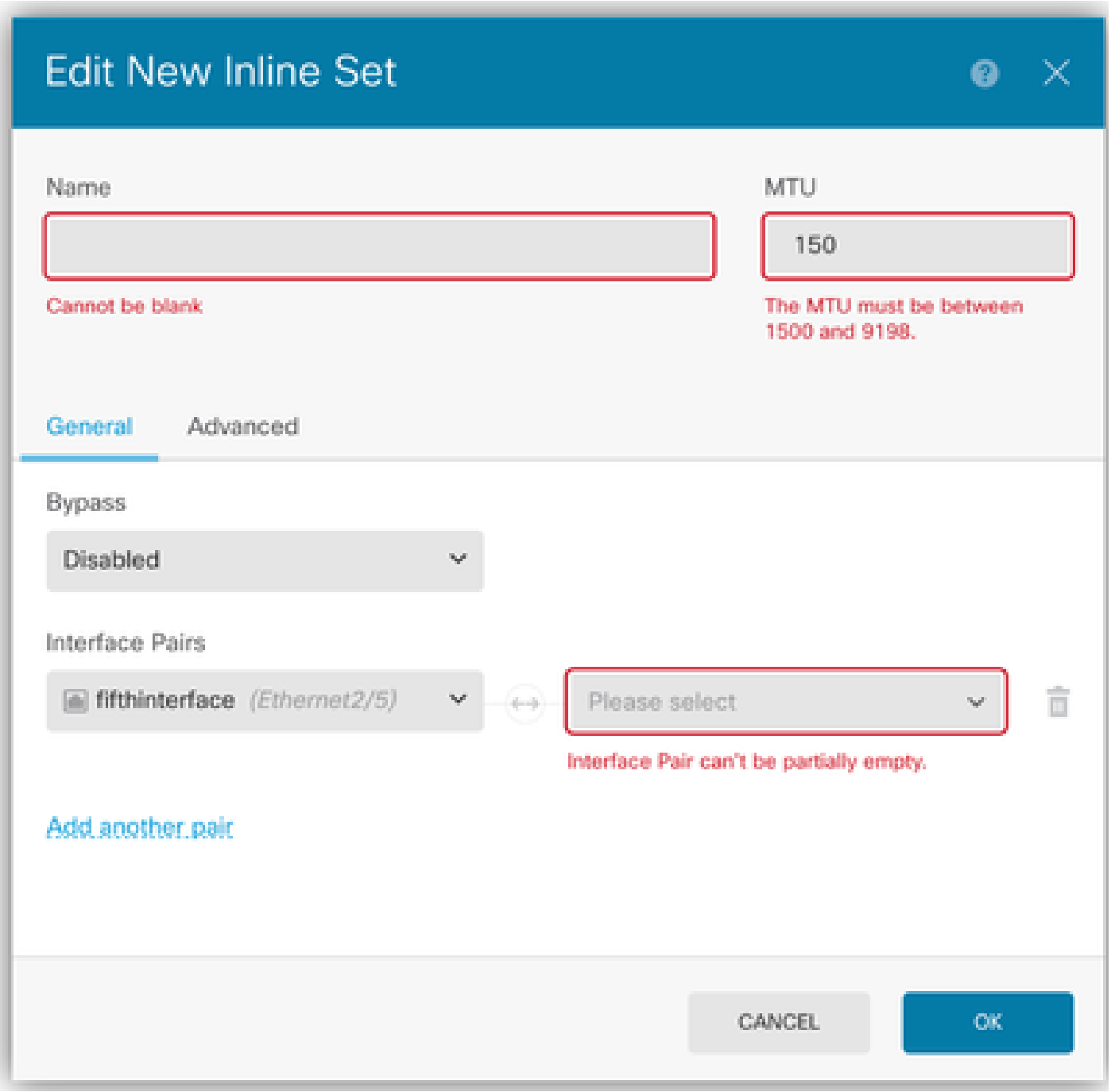
Befehle

- show running-config inline-set
- Inline-Set anzeigen
- show interface
- System-Support-Trace

Inline-Set - Validierungen beim Erstellen

- In der GUI werden Fehler für jedes Feld angezeigt.
    - Der Name muss ausgefüllt werden.

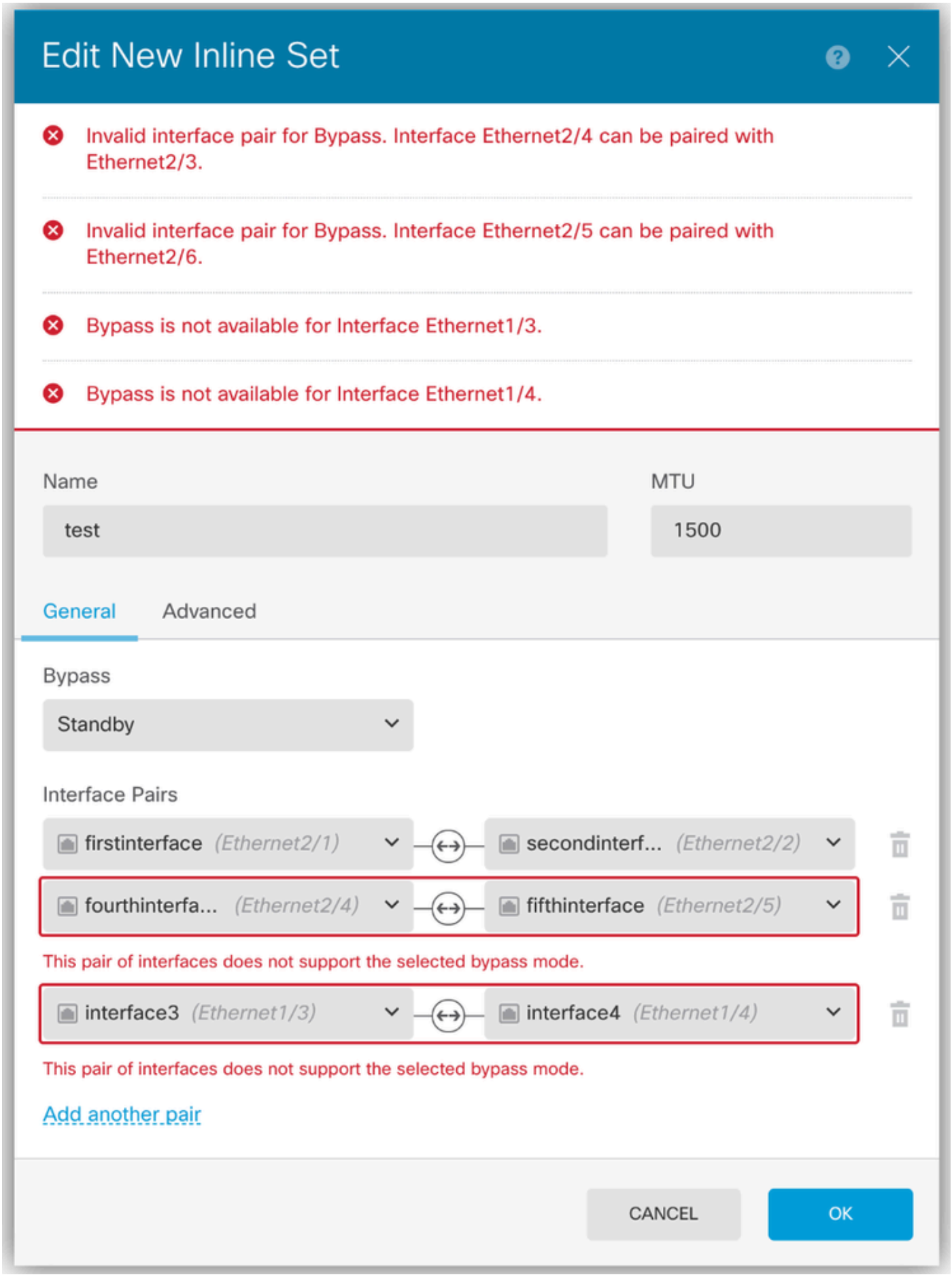
- Die MTU-Größe muss mindestens 1500 betragen.
- Beide Schnittstellen eines Paares müssen ausgewählt werden.



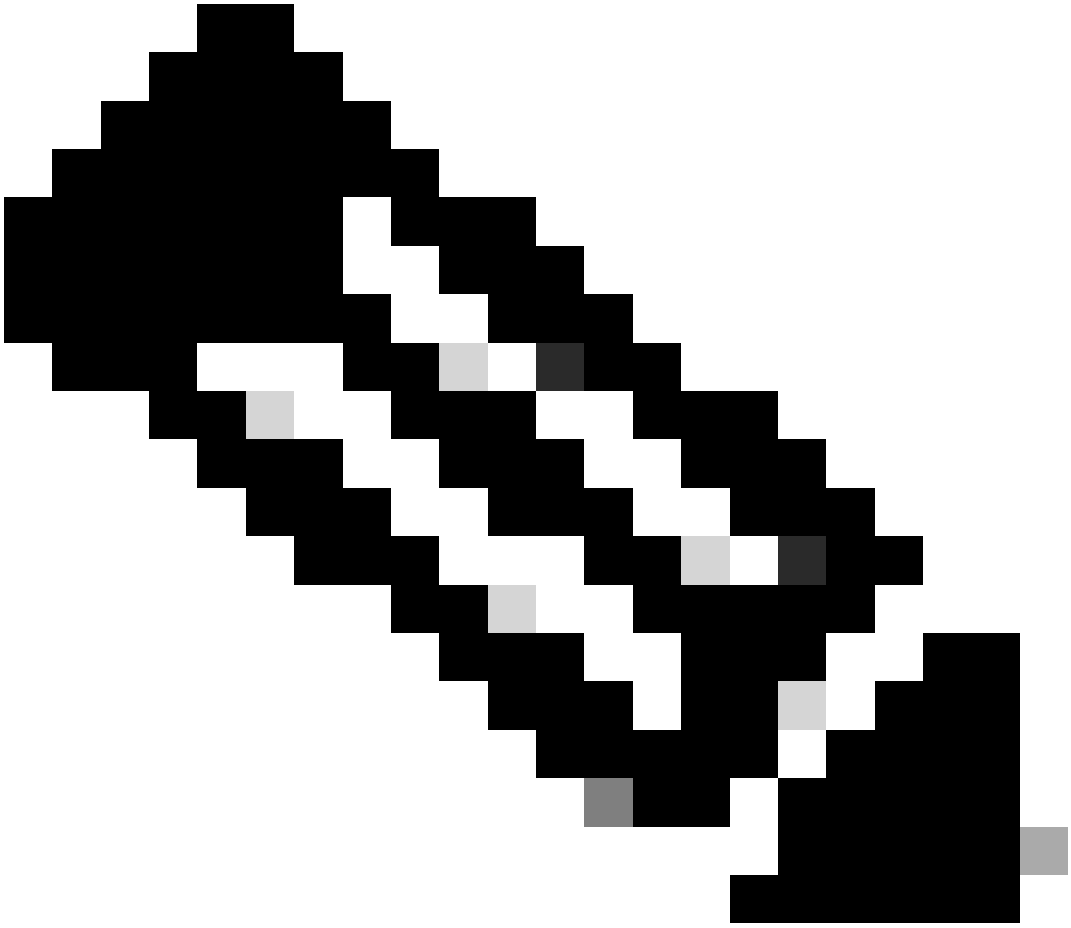
MTU-Größe

Hardware-Umgehung - Validierung beim Erstellen

- Neue Fehler werden in der GUI für jedes der Felder angezeigt, wenn Umgehung aktiviert ist:
  - Alle Schnittstellen müssen Bypass unterstützen.
    - Der Fehler zeigt nicht unterstützte Schnittstellen an.
  - Alle Paare müssen das vorbestimmte Schnittstellenpaar verwenden.
    - In der Fehlermeldung werden verfügbare Bypass-Schnittstellenpaare angegeben.



GUI-Validierung



Anmerkung: Das erste Paar (Ethernet2/1-Ethernet2/2) ist gültig.

REST API-Antwort zeigt Fehler an

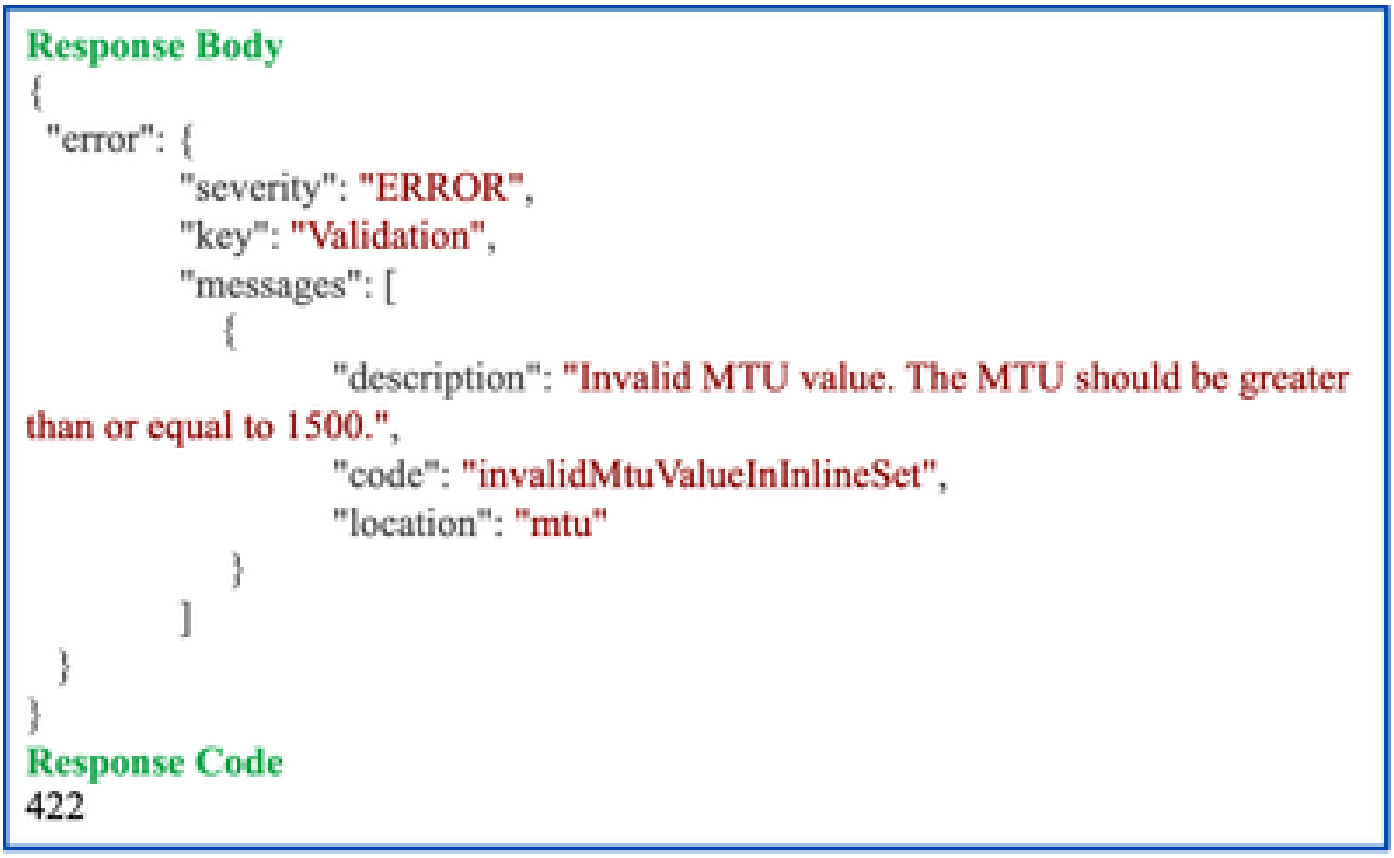
- Fehler werden in der REST-API-Antwort angezeigt.
  - Hier ist der MTU-Wert ungültig.

Response Body


```
{
  "error": {
            "severity": "ERROR",
            "key": "Validation",
            "messages": [
                {
                        "description": "Invalid MTU value. The MTU should be greater
than or equal to 1500.",
                        "code": "invalidMtuValueInInlineSet",
                        "location": "mtu"
                }
            ]
    }
}
```


Response Code

422



REST-API-Validierung

Einschränkungen der Implementierung für diese Version

- Inline-Sets: Funktioniert nur mit physischen Schnittstellen und EtherChannel.
- Inline-Sets mit Hardwareumgehung: Funktioniert nur mit physischen Schnittstellen und erfordert ein Netzwerkmodul.

Nicht unterstützte Firewall-Funktionen an Inline-Schnittstellen

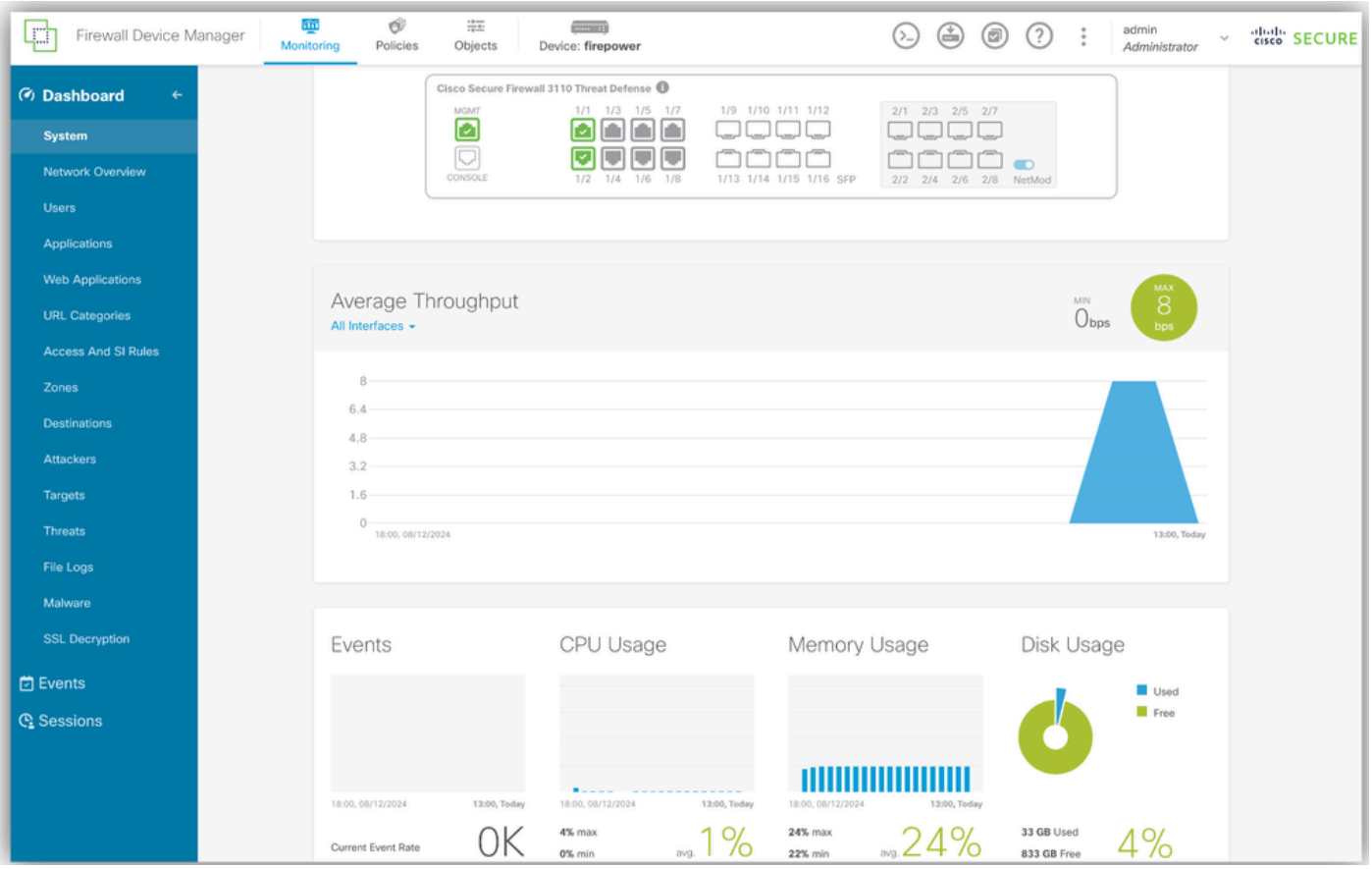
- DHCP-Server
- DHCP-Relay
- DHCP-Client
- TCP-Intercept
- Routing
- NAT
- VPN
- Anwendung
- Inspektion
- QoS
- NetFlow

Protokolle von CLI überprüfen

- Protokollieren.
    - Protokolle finden Sie unter /ngfw/var/log/cisco/ngfw-onbox.log.
    - Suchen Sie nach Inline Set.
    - Beispiel für mögliche Fehler in Protokollen:
        - Zwei Schnittstellen unterstützen keinen Bypass.
        - Zwei Schnittstellen sind kein gültiges Bypass-Paar.

```
root@FPR-3110-Pair:/home/admin# cd /ngfw/var/log/cisco/

root@FPR-3110-Pair:/ngfw/var/log/cisco# cat ngfw-onbox.log | grep "InlineSet"

2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator: 548 - Invalid

interface pair for Bypass. Interface Ethernet2/4 can be paired with Ethernet2/3.

2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:548 - Invalid

interface pair for Bypass. Interface Ethernet2/5 can be paired with Ethernet2/6.

2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:541 - Bypass

is not available for Interface Ethernet1/3.

2024-08-28 12:35:00 ajp-nio-8009-exec-1: ERROR InlineSetValidator:541 - Bypass

is not available for Interface
```

- Überprüfen des Datenverkehrs von der GUI
    - Ereignisse werden in der Benutzeroberfläche angezeigt.
    - Hier kann die Richtigkeit des Verkehrsflusses überwacht werden.
    - Navigieren Sie zu Überwachung > System.



FDM-Überwachung

- Überprüfen der Korrektheit des Datenverkehrs über die CLI

<#root>

```
> system support trace
Enable firewall-engine-debug too? [n]:
Please specify an IP protocol: ICMP
Please specify a client IP address:
Please specify a server IP address:
Monitoring packet tracer debug messages
```

[packets show up here]

Häufig gestellte Fragen

F: Wird Hochverfügbarkeit bei Inline-Sets von FDM unterstützt?
A: Inline-Sets ohne Bypass werden unterstützt.
  Inline-Sets mit Bypass werden NICHT unterstützt.
F: Werden die Spanning-Tree-BPDUs für das Inline-Set-Paar blockiert?
A : Nein, sie sind nicht blockiert.
F: Werden FTW-Karten von 3100 unterstützt?

A : Ja, FTW-Netzwerkmodule werden seit der Einführung der Serie 3100 mit 7.1/9.17 unterstützt. Hardware Bypass ist ab 7.7.0 verfügbar.
F: Wird für 3100 FTW-Karten der Bypass-Modus "Disabled" (Deaktiviert), "Standby" (Standby) oder "Bypass-Force" (Umgehungsstärke) wie auf FMC unterstützt oder nicht?
A : Hardware Bypass ist ab 7.7.0 auf 3100 Geräten mit FTW-Karten verfügbar.
F: Werden Inline-Sets mit Port-Channels unterstützt, bei denen der Datenverkehr auch über die Port-Channels asymmetrisch ist?
A : Für die konfigurierte Port-Channel-Geschwindigkeit wird keine Validierung durchgeführt. Solange sie von der FTD unterstützt wird, muss sie unterstützt werden.
F: Wird Failopen unterstützt, falls Snort die Inspektion nicht durchführen kann?
A : Weitere Informationen finden Sie in der Dokumentation zu dieser Einstellung im Konfigurationsleitfaden für FirePOWER Management Center.

Zugehörige Informationen

- FTD-Schnittstellen im Inline-Pair-Modus konfigurieren
- Konfigurationsleitfaden für FirePOWER Management Center, Version 6.3
- Cisco Secure Firewall der Serie 3100 - Hardware-Installationshandbuch
- Cisco Secure Firewall der Serie 3100 - Datenblatt

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.