L2-Switch auf FPR1010, Architektur, Verifizierung und Fehlerbehebung

Inhalt

Einführung

Dieses Dokument beschreibt den L2-Switch auf FP1010-Geräten. Insbesondere deckt er den Teil der Implementierung vor allem die Security Services Platform (SSP)/FirePOWER eXtensive Operation System (FXOS) ab. In der Version 6.5 wurden mit der FirePOWER 1010 (Desktop-Modell) Switching-Funktionen auf dem integrierten L2-Hardware-Switch aktiviert. So vermeiden Sie zusätzliche Hardware-Switches, und die Kosten werden gesenkt.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

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 potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

- FP1010 ist ein Desktop-Modell für das Small Office Home Office (SOHO), das als Ersatz für die Plattformen ASA5505 und ASA5506-X erhältlich ist.
- Softwareunterstützung für FTD-Images (6.4+), die entweder vom FirePOWER Management Center (FMC), FirePOWER Device Manager (FDM) oder von Cloud Defense Orchestrator (CDO) verwaltet werden.
- Softwareunterstützung für ASA-Images (9.13+), verwaltet durch CSM, ASDM oder CLI.
- Das Betriebssystem (OS), ASA oder FTD ist FXOS gebündelt (ähnlich dem FP21xx).
- 8 x 10/100/1000-Mbit/s-Datenports.
- Die Ports E1/7, E1/8 unterstützen PoE+.
- Der Hardware-Switch ermöglicht die Kommunikation der Leitungsgeschwindigkeit zwischen Ports (z. B.: Eine Kamera wird in den lokalen Server eingespeist).

Firepower 6.5-Erweiterungen

- Einführung eines neuen Schnittstellentyps mit dem Namen Switched Virtual Interface (SVI).
- Gemischter Modus: Schnittstellen können entweder im Switch- (L2-) oder im Nicht-Switch-Modus (L3) konfiguriert werden.
- L3-Modus-Schnittstellen leiten alle Pakete an die Sicherheitsanwendung weiter.
- L2-Modus-Ports können in der Hardware umschalten, wenn zwei Ports demselben VLAN angehören, wodurch Durchsatz und Latenz verbessert werden. Pakete, die geroutet oder überbrückt werden müssen, erreichen die Sicherheitsanwendung (z.B.: eine Kamera, die eine neue Firmware aus dem Internet herunterlädt) und gemäß der Konfiguration einer Sicherheitsüberprüfung unterzogen werden.
- Die physische L2-Schnittstelle kann einer oder mehreren SVI-Schnittstellen zugeordnet werden.
- L2-Modus-Schnittstellen können sich im Zugriffs- oder Trunk-Modus befinden.

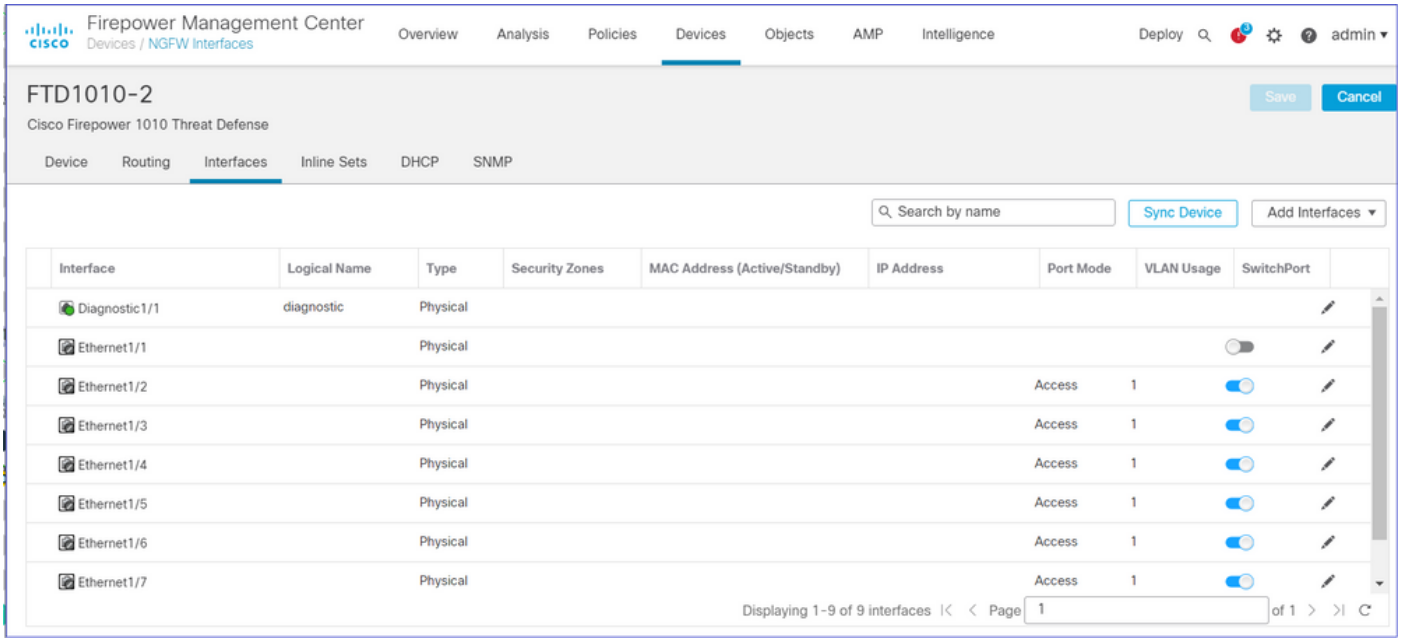
- Die L2-Schnittstelle des Zugriffsmodus unterstützt nur nicht getaggten Datenverkehr.
- Die L2-Schnittstelle des Trunk-Modus ermöglicht getaggten Datenverkehr.
- Native VLAN-Unterstützung für die L2-Schnittstelle im Trunk-Modus.
- ASA CLIs, ASDM, CSM, FDM und FMC wurden zur Unterstützung neuer Funktionen erweitert.

FMC-Ergänzungen

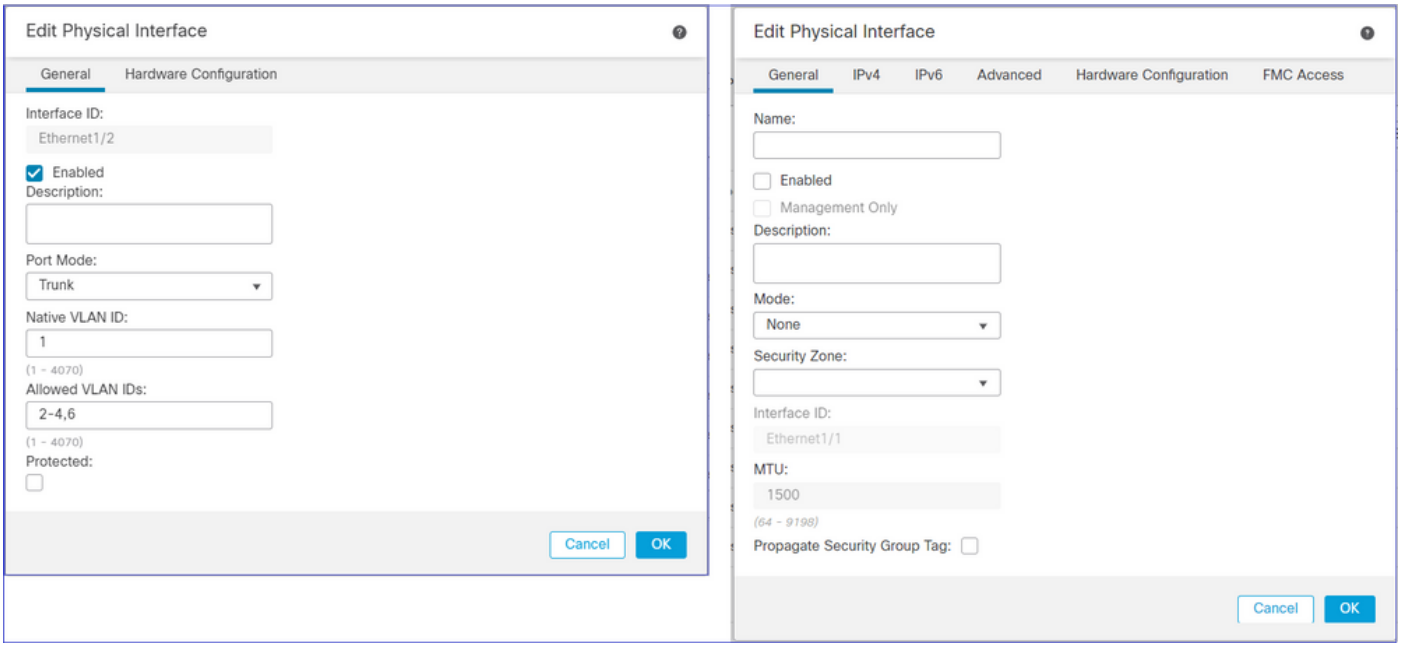
- Für eine physische Schnittstelle wurde ein neuer Schnittstellenmodus namens "switchport" eingeführt, mit dem festgestellt werden kann, ob es sich bei einer physischen Schnittstelle um eine L3- oder L2-Schnittstelle handelt.
- Die physische L2-Schnittstelle kann je nach Zugriffs- oder Trunk-Modus einer oder mehreren VLAN-Schnittstellen zugeordnet werden.
- Die FirePOWER 1010 unterstützt die PoE-Konfiguration (Power Over Ethernet) für die letzten beiden Datenschnittstellen, d. h. Ethernet1/7 und Ethernet1/8.
- Durch die Schnittstellenänderung zwischen Switch und Nicht-Switch werden alle Konfigurationen außer der PoE- und Hardwarekonfiguration gelöscht.

Funktionsweise

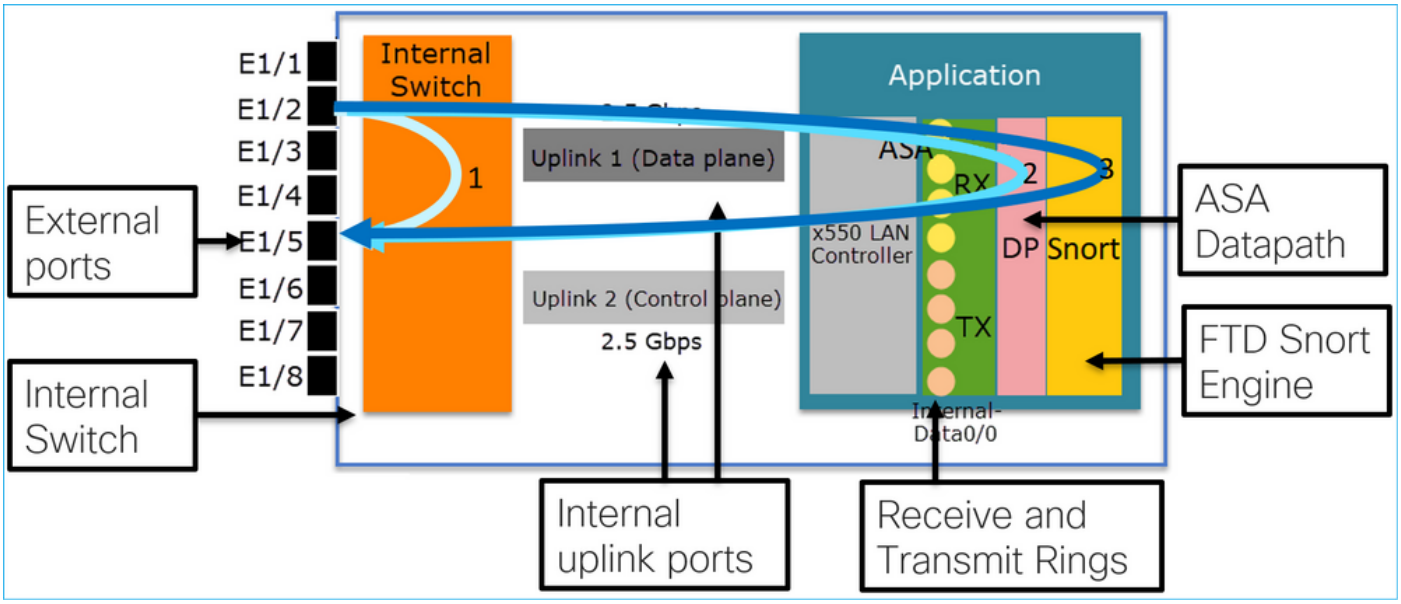
Diese Funktion ist lediglich eine Erweiterung der bestehenden Schnittstellenunterstützung auf FMC (**Gerätemanagement > Schnittstellenseite**).



Physische Schnittstellenansicht (L2 und L3)



Architektur FP1010



- 8 Ports für externe Daten.
- 1 Interner Switch.
- 3 Uplink-Ports (2 davon im Bild abgebildet), einer für Datenebene, einer für Kontrollebene, einer für Konfiguration.
- x550 LAN Controller (die Schnittstelle zwischen der Anwendung und den Uplinks).
- 4 Empfangsringe (RX) und 4 Übertragungsringe (TX).
- Datapath-Prozess (auf ASA und FTD).
- Snort-Prozess (auf FTD).

Paketverarbeitung

Zwei Hauptfaktoren können sich auf die Paketverarbeitung auswirken:

1. Schnittstelle/Port-Modus

2. Angewandte Richtlinie

Ein Paket kann auf drei verschiedene Arten über ein FP1010 übertragen werden:

1. Nur über internen Switch verarbeitet

2. Zur Anwendung weitergeleitet (ASA/FTD) und nur im Datapath-Prozess verarbeitet

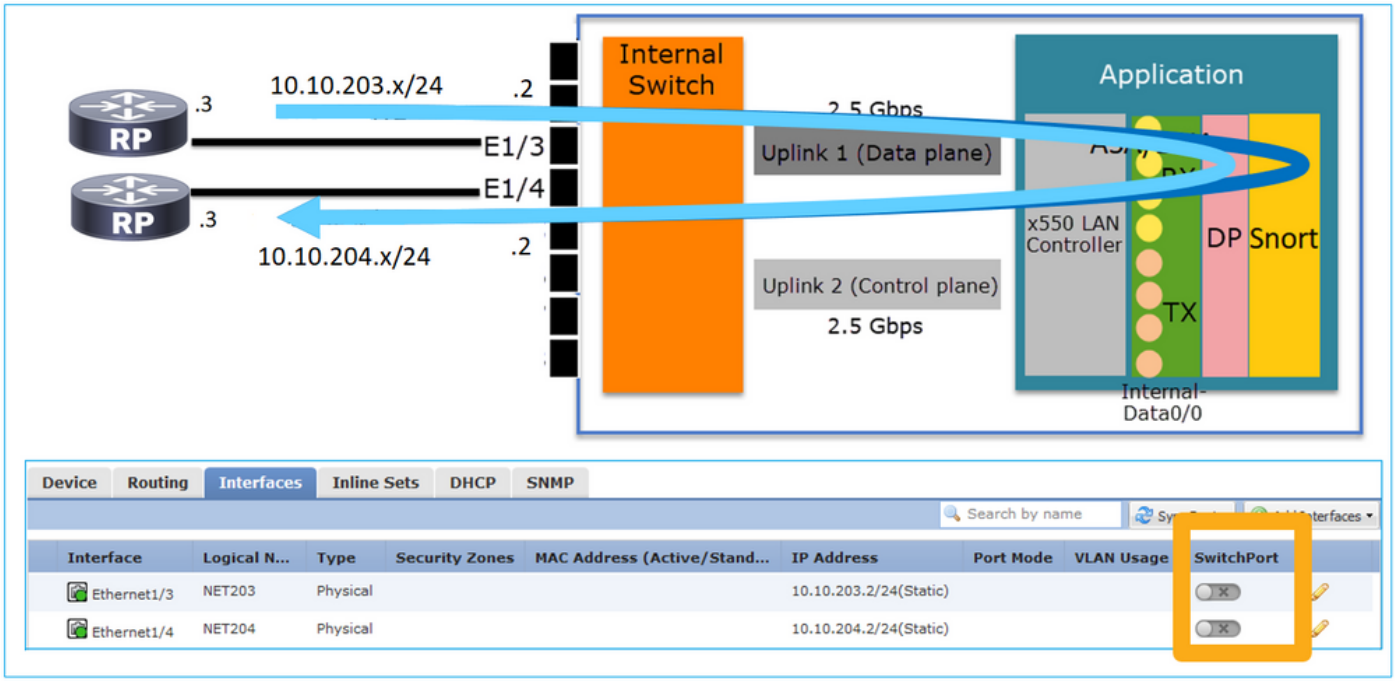
3. An die Anwendung weitergeleitet (FTD) und von der DataPath- und Snort-Engine verarbeitet

FP1010 Port-Modi

Die Beispiele für die Benutzeroberfläche gelten für FMC, die CLI-Beispiele für FTD. Die meisten Konzepte sind auch vollständig auf ASA anwendbar.

Fall 1: FP1010. Geroutete Ports (IP-Routing)

Konfiguration und Betrieb



Wichtigste Punkte

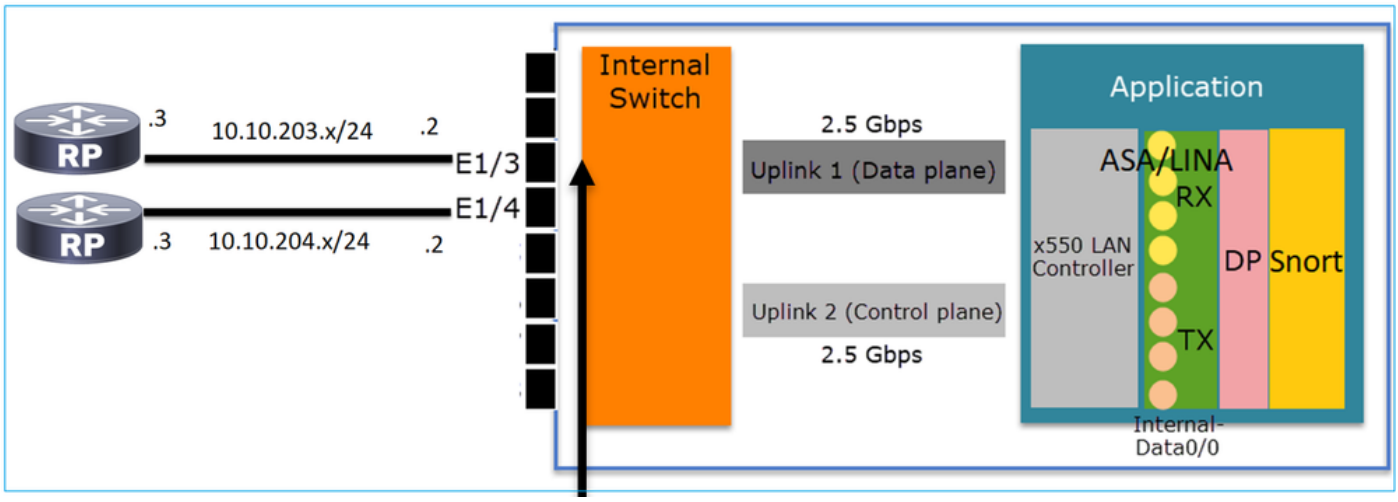
- Aus Entwurfssicht gehören die beiden Ports zu zwei verschiedenen L2-Subnetzen.
- Wenn die Ports im Routed-Modus konfiguriert sind, werden die Pakete von der Anwendung verarbeitet (ASA oder FTD).
- Bei FTD können die Pakete auf Basis der Regelaktion (z.B. ALLOW) sogar von der Snort Engine überprüft werden.

FTD-Schnittstellenkonfiguration

```
interface Ethernet1/3 nameif NET203
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
```

```
security-level 0
 ip address 10.10.203.2 255.255.255.0
!
interface Ethernet1/4 nameif NET204
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
 ip address 10.10.204.2 255.255.255.0
```

FP1010 - Überprüfung von gerouteten Ports



Über die FXOS-CLI können Sie die Zähler für die physische Schnittstelle überprüfen. Dieses Beispiel zeigt die Zähler für Unicast- und Unicast-Eingangs-Unicast und -Ausgangs-Unicast am E1/3-Port:

```
FP1010(local-mgmt)# show portmanager counters ethernet 1 3 | egrep
"stats.ing_unicastframes\|stats.egr_unicastframes"
stats.ing_unicastframes        = 3521254 stats.egr_unicastframes        = 604939
```

FTD-Datapath-Erfassungen können angewendet und Pakete nachverfolgt werden:

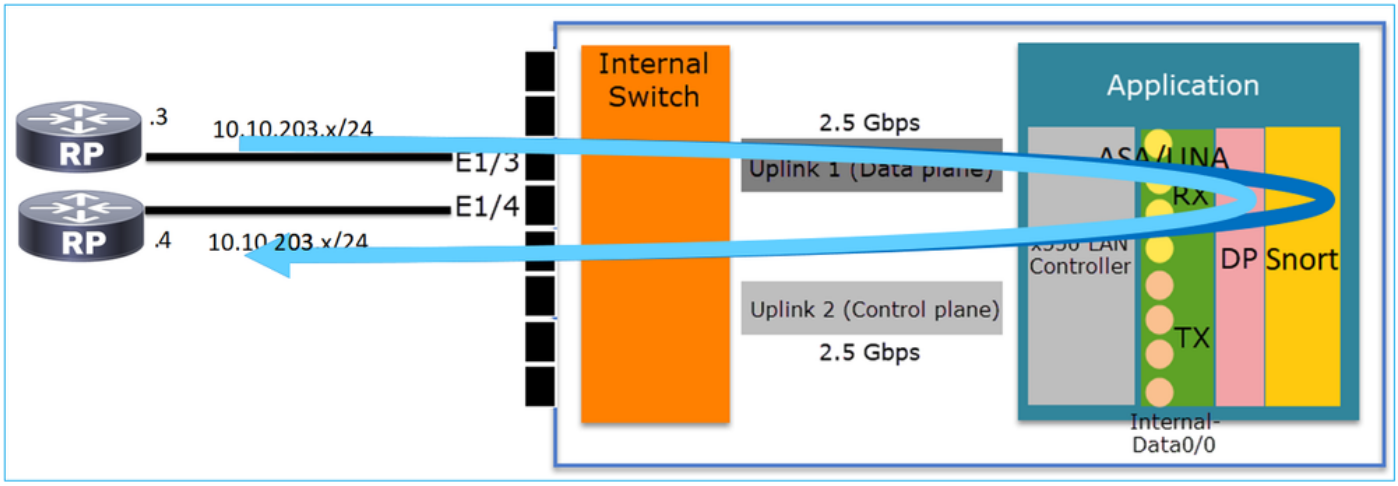
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

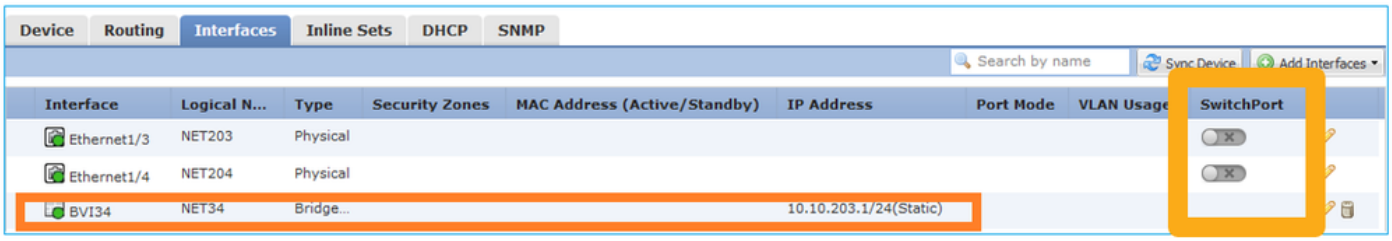
Dies ist ein Erfassungsausschnitt. Wie erwartet wird das Paket auf Grundlage einer ROUTE-SUCHE weitergeleitet:

```
FP1010# show capture CAP203 packet-number 21 trace

21: 06:25:23.924848       10.10.203.3 > 10.10.204.3 icmp: echo request
…
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.10.204.3 using egress ifc  NET204
```

Fall 2: FP1010. Bridge-Group-Modus (Bridging)

Konfiguration und Betrieb





Wichtigste Punkte

- Hinsichtlich des Designs sind die beiden Ports mit demselben L3-Subnetz (ähnlich einer transparenten Firewall), aber mit unterschiedlichen VLANs verbunden.
- Wenn die Ports im Bridging-Modus konfiguriert sind, werden die Pakete von der Anwendung verarbeitet (ASA oder FTD).
- Bei FTD können die Pakete auf Basis der Regelaktion (z.B. ALLOW) sogar von der Snort Engine überprüft werden.

FTD-Schnittstellenkonfiguration

```
interface Ethernet1/3 bridge-group 34 nameif NET203
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
!
interface Ethernet1/4 bridge-group 34 nameif NET204
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
 security-level 0
!
interface BVI34 nameif NET34 security-level 0 ip address 10.10.203.1 255.255.255.0
```

FP1010 Portüberprüfung für Bridge-Gruppen

Dieser Befehl zeigt die Schnittstellenmember von BVI 34 an:

```
FP1010# show bridge-group 34
 Interfaces:
 Ethernet1/3 Ethernet1/4
 Management System IP Address:  10.10.203.1 255.255.255.0
```

```
 Management Current IP Address: 10.10.203.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):    N/A
 Static mac-address entries:  0
 Dynamic mac-address entries: 13
```

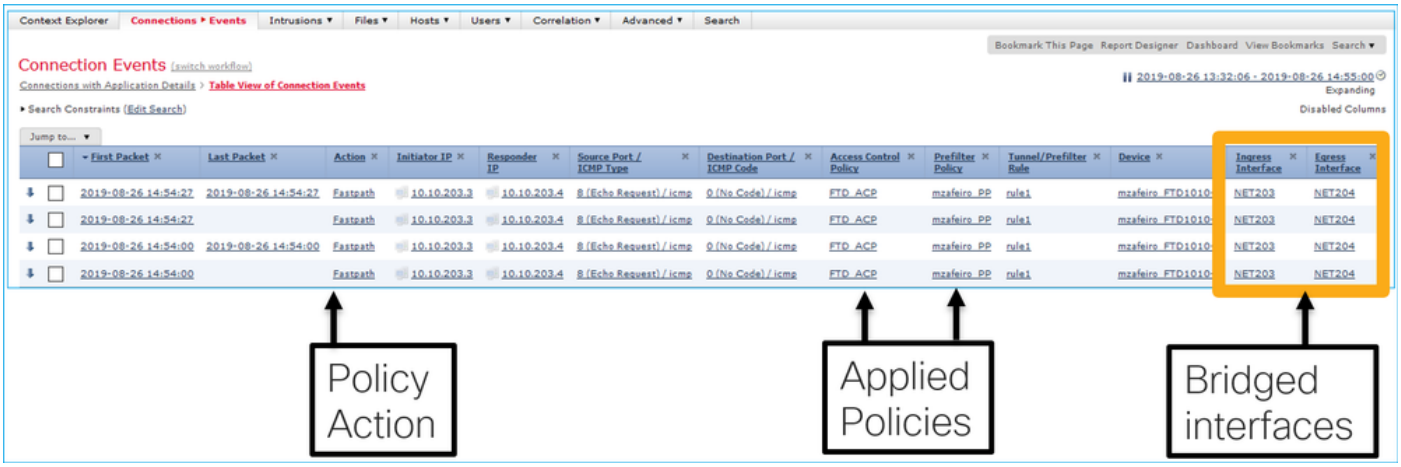
Dieser Befehl zeigt die Tabelle ASA/FTD DataPath Content Addressable Memory (CAM) (CAM)):

```
FP1010# show mac-address-table
interface mac address     type       Age(min)    bridge-group
-----------------------------------------------------------------
NET203 0050.5685.43f1   dynamic      1             34
NET204 4c4e.35fc.fcd8   dynamic      3             34
NET203                    0050.56b6.2304   dynamic      1             34
NET204                    0017.dfd6.ec00   dynamic      1             34
NET203                    0050.5685.4fda   dynamic      1             34
```

Ein Paket-Ablaufverfolgungsausschnitt zeigt, dass das Paket basierend auf der Ziel-MAC-L2-Suche weitergeleitet wird:

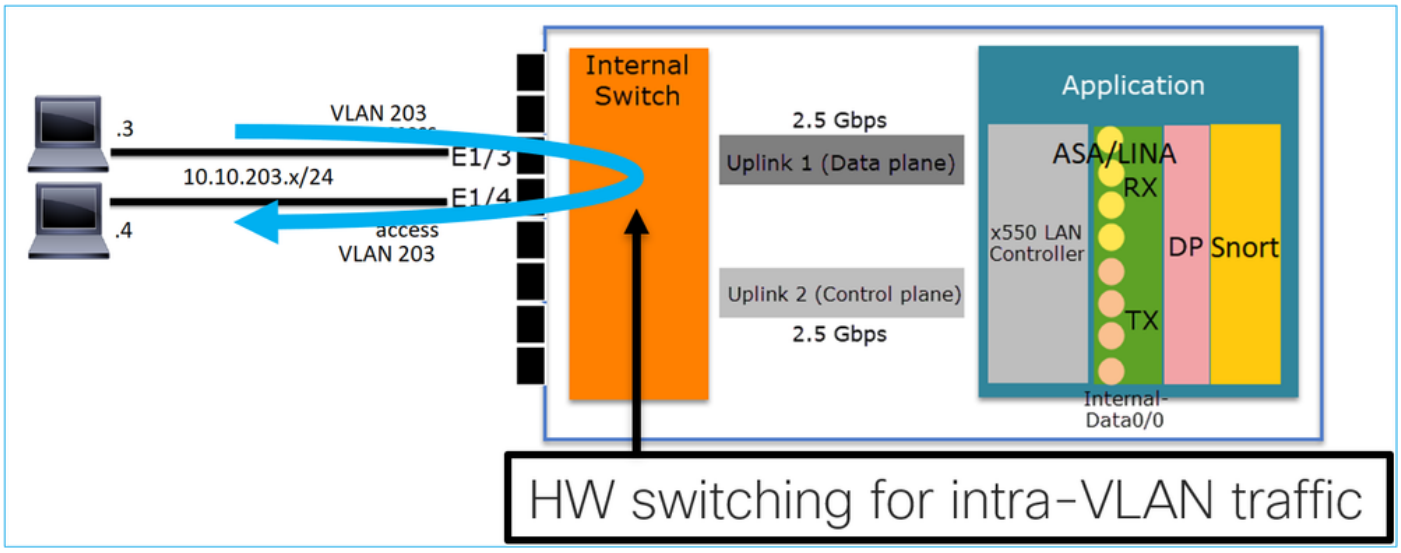
```
FP1010# show cap CAP203 packet-number 1 trace

2 packets captured

1: 11:34:40.277619 10.10.203.3 > 10.10.203.4 icmp: echo request
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
DestinationMAC lookup resulted in egress ifc NET204
```

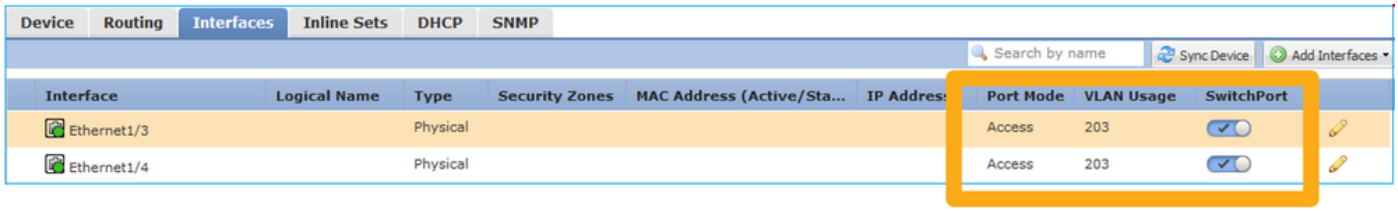
Im Falle von FTD können FMC Connection Events auch Informationen über die Flusskontrolle und die Transit-Bridge-Gruppen-Schnittstellen bereitstellen:



Fall 3: FP1010. Switchports (HW-Switching) im Zugriffsmodus

Konfiguration und Betrieb





Wichtigste Punkte

- HW Switching ist eine FTD **6.5+-** und ASA **9.13+-**Funktion.
- Hinsichtlich des Designs sind die beiden Ports mit demselben L3-Subnetz und demselben VLAN verbunden.
- Die Ports in diesem Szenario arbeiten im Zugriffsmodus (nur nicht markierter Datenverkehr).
- Für die im SwitchPort-Modus konfigurierten Firewall-Ports ist kein logischer Name (name) konfiguriert.
- Wenn die Ports im Switching-Modus konfiguriert sind und demselben VLAN (Intra-VLAN-Verkehr) angehören, werden die Pakete nur vom internen FP1010-Switch verarbeitet.

FTD-Schnittstellenkonfiguration

Aus CLI-Sicht ähnelt die Konfiguration einem L2-Switch sehr:

```
interface Ethernet1/3 switchport switchport access vlan 203 ! interface Ethernet1/4 switchport switchport access vlan 203
```

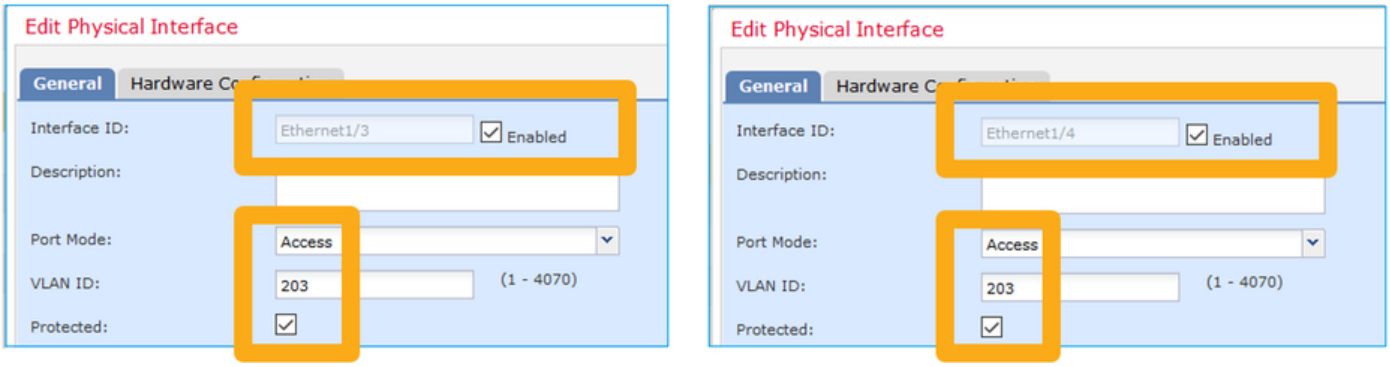
Filtern des VLAN-internen Datenverkehrs

Die Herausforderung: **Eine ACL kann den VLAN-internen Datenverkehr nicht filtern!**

Die Lösung: **Geschützte** Ports

Das Prinzip ist sehr einfach: Zwei als "Protected" konfigurierte Ports können nicht miteinander kommunizieren.

FMC-Benutzeroberfläche bei geschützten Ports:



FTD-Schnittstellenkonfiguration

Der Befehl **switchport protected** wird unter der Schnittstelle konfiguriert:

```
interface Ethernet1/3
 switchport
 switchport access vlan 203
 switchport protected
!
interface Ethernet1/4
 switchport
 switchport access vlan 203
 switchport protected
```

FP1010 Switch-Port-Verifizierung

In diesem Beispiel werden 1000 Unicast-Pakete (ICMP) mit einer bestimmten Größe (1100 Byte) gesendet:

```
router# ping 10.10.203.4 re 1000 timeout 0 size 1100
```

Um die Unicast-Zähler für Ein- und Ausgang der Transit-Schnittstellen zu überprüfen, verwenden Sie den folgenden Befehl:

```
FP1010(local-mgmt)# show portmanager counters ethernet 1 3 | egrep
"stats.ing_unicastframes\|stats.bytes_1024to1518_frames"
stats.ing_unicastframes         = 146760
stats.bytes_1024to1518_frames   = 0
FP1010(local-mgmt)# show portmanager counters ethernet 1 4 | egrep
"stats.egr_unicastframes\|stats.bytes_1024to1518_frames"
stats.bytes_1024to1518_frames   = 0
stats.egr_unicastframes         = 140752
FP1010(local-mgmt)# show portmanager counters ethernet 1 3 | egrep
"stats.ing_unicastframes\|stats.bytes_1024to1518_frames"
stats.ing_unicastframes         = 147760 <------------------ Ingress Counters got increased by
1000
stats.bytes_1024to1518_frames   = 1000 <------------------ Ingress Counters got increased by 1000
FP1010(local-mgmt)# show portmanager counters ethernet 1 4 | egrep
"stats.egr_unicastframes\|stats.bytes_1024to1518_frames"
stats.bytes_1024to1518_frames   = 0 <------------------ No egress increase
stats.egr_unicastframes         = 140752 <------------------ No egress increase
```

Dieser Befehl zeigt den VLAN-Status des internen Switches an:

```
FP1010# show switch vlan
```

```
VLAN Name           Status    Ports
---- -------------- --------- ---------------------
1    -              down
203 - up Ethernet1/3, Ethernet1/4
```

Der Status eines VLAN ist UP, solange dem VLAN mindestens ein Port zugewiesen ist

Wenn ein Port administrativ ausgefallen ist oder der verbundene Switch-Port ausgefallen ist/das Kabel getrennt ist und dies der einzige Port ist, der dem VLAN zugewiesen wurde, ist der VLAN-Status ebenfalls nicht verfügbar:

```
FP1010-2# show switch vlan
VLAN Name                            Status    Ports
---- ------------------------------- --------- ------------------------------
1    -                               down 201  net201                          down
Ethernet1/1 <--- e1/1 was admin down 202  net202                         down Ethernet1/2 <---
upstream switch port is admin down
```

Dieser Befehl zeigt die CAM-Tabelle des internen Switches an:

```
FP1010-2# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |            Type          | Age | Port
-------------------------------------------------------------
 4c4e.35fc.0033 | 0203 |          dynamic         | 282 | Et1/3
 4c4e.35fc.4444 | 0203 |          dynamic         | 330 | Et1/4
```

Die Standardverweilzeit der internen Switch-CAM-Tabelle beträgt 5 Min. 30 Sek.

FP1010 enthält 2 CAM-Tabellen:

1. Interne Switch CAM-Tabelle: Wird bei HW-Switching verwendet
2. ASA/FTD DataPath CAM-Tabelle: Wird bei Bridging verwendet

Jedes Paket/Frame, das den FP1010 passiert, wird auf Basis des Portmodus von einer einzigen CAM-Tabelle (interner Switch oder FTD-Datenpfad) verarbeitet.

> Vorsicht: Verwechseln Sie nicht die im SwitchPort-Modus verwendete MAC-Adresstabelle für internen Switch CAM mit der show mac-address-table FTD datapath CAM-Tabelle für den FTD, die im Bridge-Modus verwendet wird.

HW-Switching: Zusätzliche Dinge zu beachten

ASA/FTD-Datenath-Protokolle enthalten keine Informationen zu HW-Switched-Datenflüssen:

```
FP1010# show log
FP1010#
```

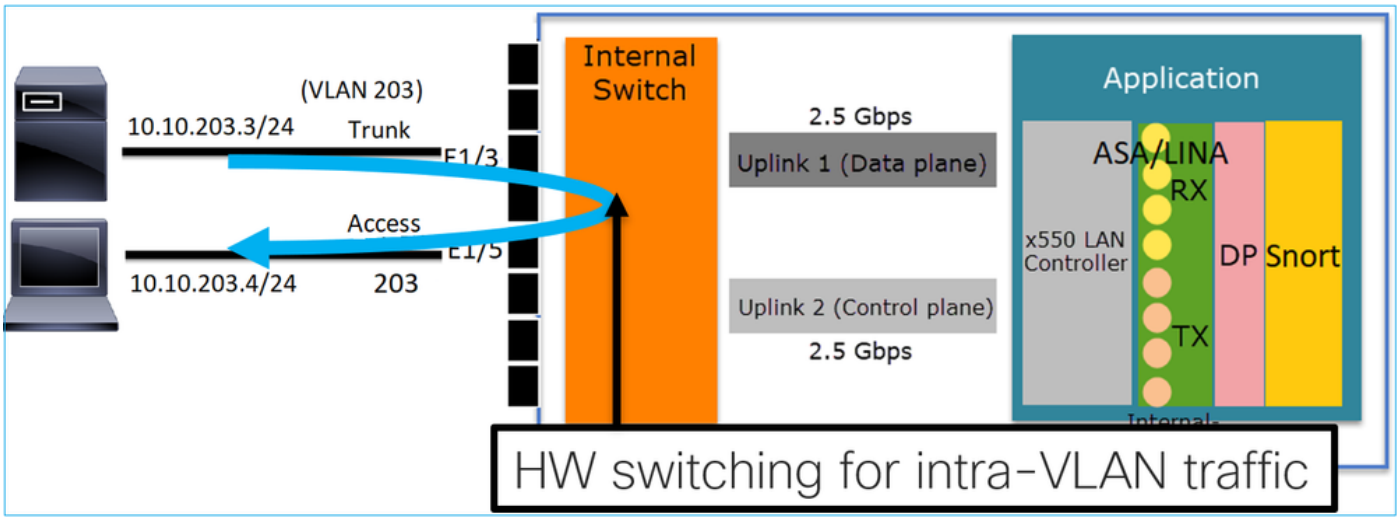
ASA/FTD Datapath-Verbindungstabelle zeigt keine HW-Switched Flows:

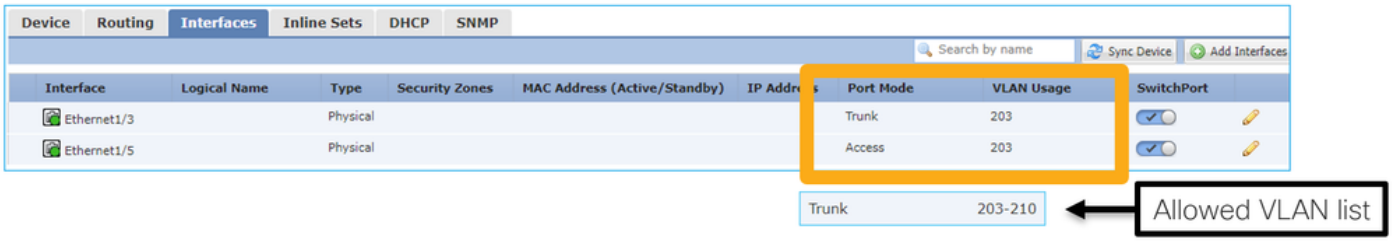
```
FP1010# show conn
0 in use, 3 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

Außerdem werden bei den FMC Connection Events keine HW-Switched-Flows angezeigt.

Fall 4: FP1010. Switchports (Trunking)

Konfiguration und Betrieb





Wichtigste Punkte

- HW Switching ist eine FTD **6.5+-** und ASA **9.13+-**Funktion.
- Hinsichtlich des Designs sind die beiden Ports mit demselben L3-Subnetz und demselben VLAN verbunden.
- Der Trunk-Port akzeptiert getaggte und nicht getaggte Frames (bei einem nativen VLAN).
- Wenn die Ports im Switching-Modus konfiguriert sind und demselben VLAN (Intra-VLAN-Verkehr) angehören, werden die Pakete nur vom internen Switch verarbeitet.

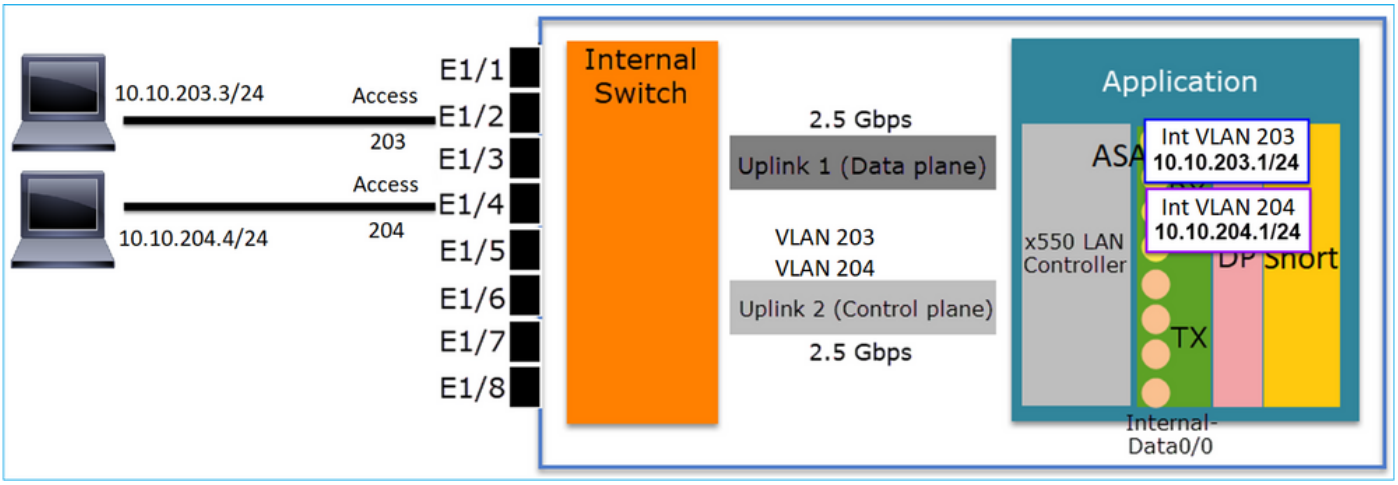
FTD-Schnittstellenkonfiguration

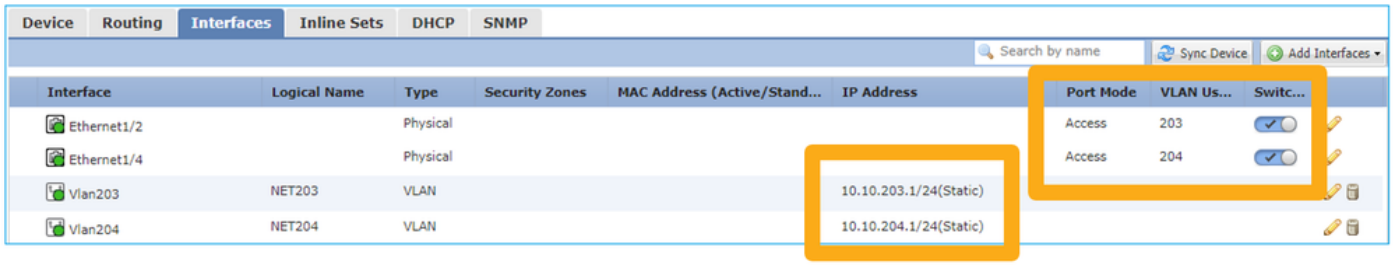
Die Konfiguration ähnelt einem Switch-Port auf Layer 2:

```
interface Ethernet1/3 switchport switchport trunk allowed vlan 203 switchport trunk native vlan
1 switchport mode trunk
!
interface Ethernet1/5
 switchport
 switchport access vlan 203
```

Fall 5: FP1010. Switchports (Inter-VLAN)

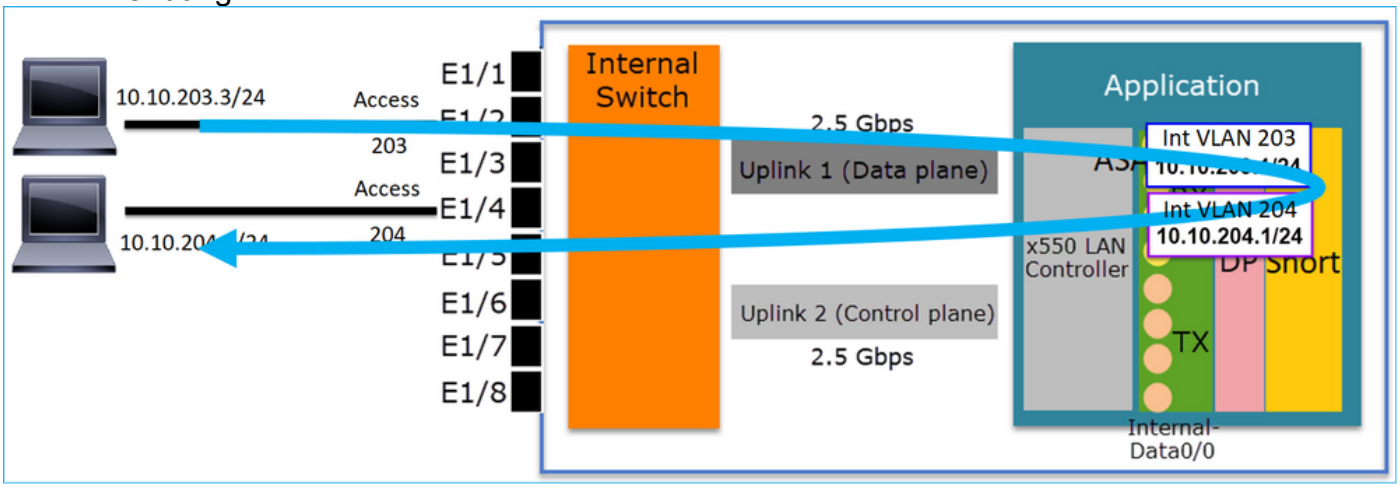
Konfiguration und Betrieb





Wichtigste Punkte

- Hinsichtlich des Designs sind die beiden Ports mit zwei verschiedenen L3-Subnetzen und zwei verschiedenen VLANs verbunden.
- Der Datenverkehr zwischen den VLANs verläuft über die VLAN-Schnittstellen (ähnlich wie bei SVIs).
- Aus Sicht des Datenverkehrsflusses erreicht der VLAN-übergreifende Datenverkehr die Anwendung.



FTD-Schnittstellenkonfiguration

Die Konfiguration ähnelt einer Switch Virtual Interface (SVI):

```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
```

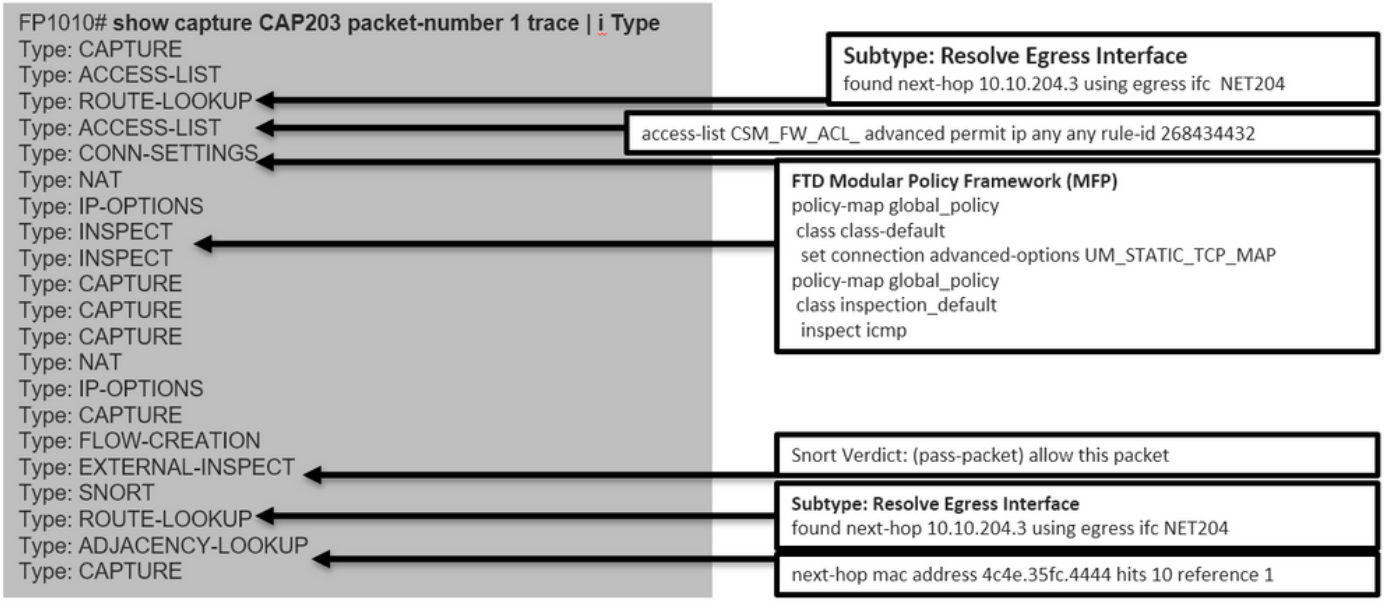
```
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

Paketverarbeitung für Inter-VLAN-Datenverkehr

Dies ist eine Spur eines Pakets, das durch zwei verschiedene VLANs geleitet wird:

```
FP1010# show capture CAP203 packet-number 1 trace | include Type
Type: CAPTURE
Type: ACCESS-LIST
Type: ROUTE-LOOKUP
Type: ACCESS-LIST
Type: CONN-SETTINGS
Type: NAT
Type: IP-OPTIONS
Type: INSPECT
Type: INSPECT
Type: CAPTURE
Type: CAPTURE
Type: CAPTURE
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: FLOW-CREATION
Type: EXTERNAL-INSPECT
Type: SNORT
Type: ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

Die Hauptphasen des Paketprozesses:



Fall 6: FP1010. Inter-VLAN-Filter

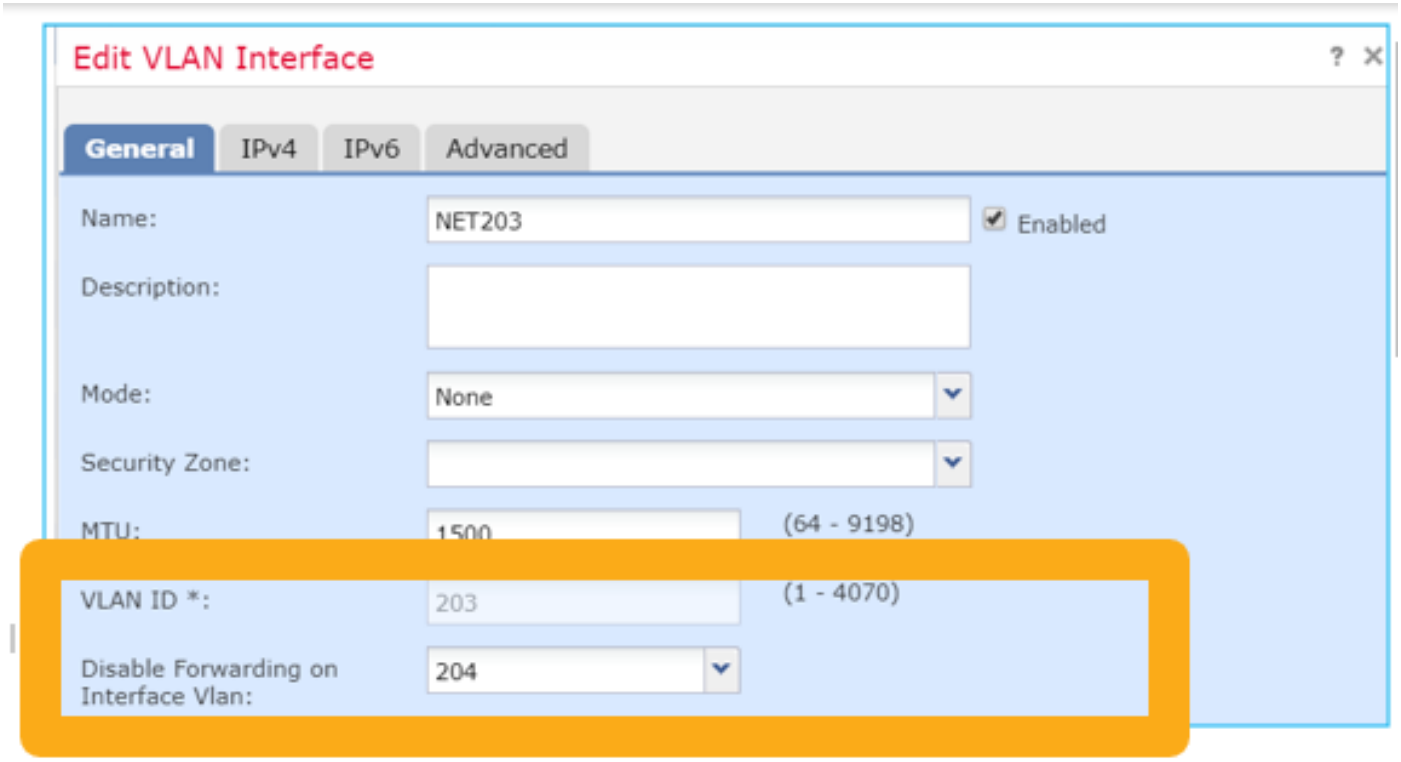
Konfiguration und Betrieb

Es gibt zwei Hauptoptionen zum Filtern des VLAN-Datenverkehrs:

1. Zugriffskontrollrichtlinie
2. Befehl "no forward"

Filtern des VLAN-übergreifenden Datenverkehrs mithilfe des Befehls "no forward"

Konfiguration der FMC-Benutzeroberfläche:



Wichtigste Punkte

- Der "no forward"-Befehl ist unidirektional.
- Sie kann nicht auf beide VLAN-Schnittstellen angewendet werden.
- Vor der ACL-Prüfung wird die Überprüfung der Vorwärtskompatibilität durchgeführt.

FTD-Schnittstellenkonfiguration

Die CLI-Konfiguration in diesem Fall ist:

```
interface Vlan203
no forward interface Vlan204
 nameif NET203
 security-level 0
 ip address 10.10.203.1 255.255.255.0
!
interface Vlan204
 nameif NET204
 security-level 0
 ip address 10.10.204.1 255.255.255.0
```

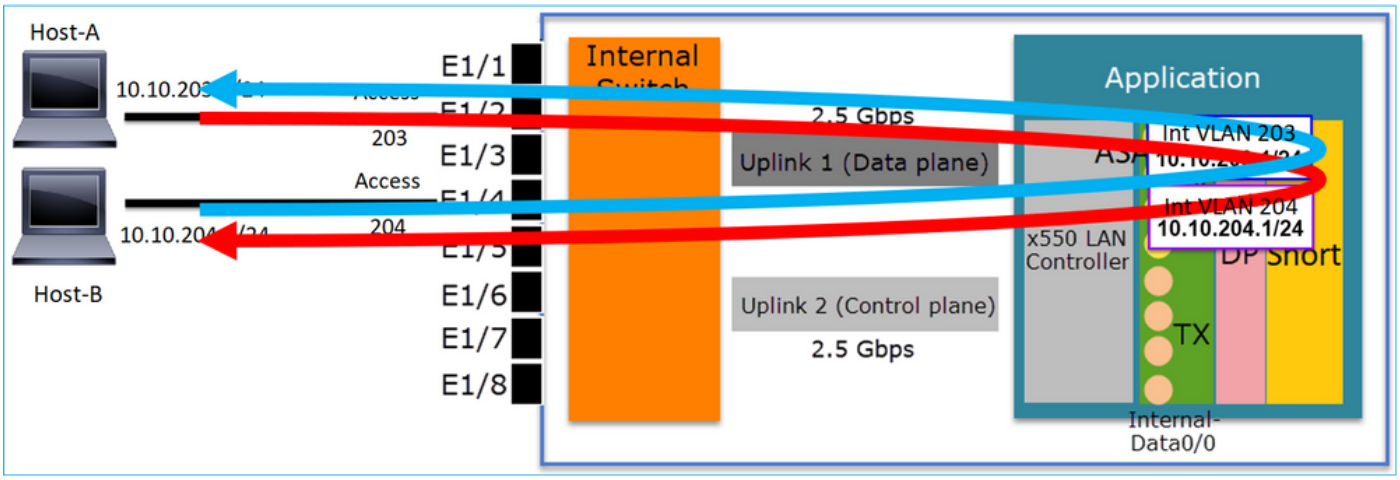
Wenn ein Paket durch die Weiterleitungsfunktion verworfen wird, wird eine ASA/FTD-Datenath-Syslog-Meldung generiert:

```
FP1010# show log
Sep 10 2019 07:44:54: %FTD-5-509001: Connection attempt was prevented by "no forward" command:
icmp src NET203:10.10.203.3 dst NET204:10.10.204.3 (type 8, code 0)
```

Aus der Sicht des Accelerated Security Path (ASP)-Dropdown-Menüs wird dies als ACL-Drop betrachtet:

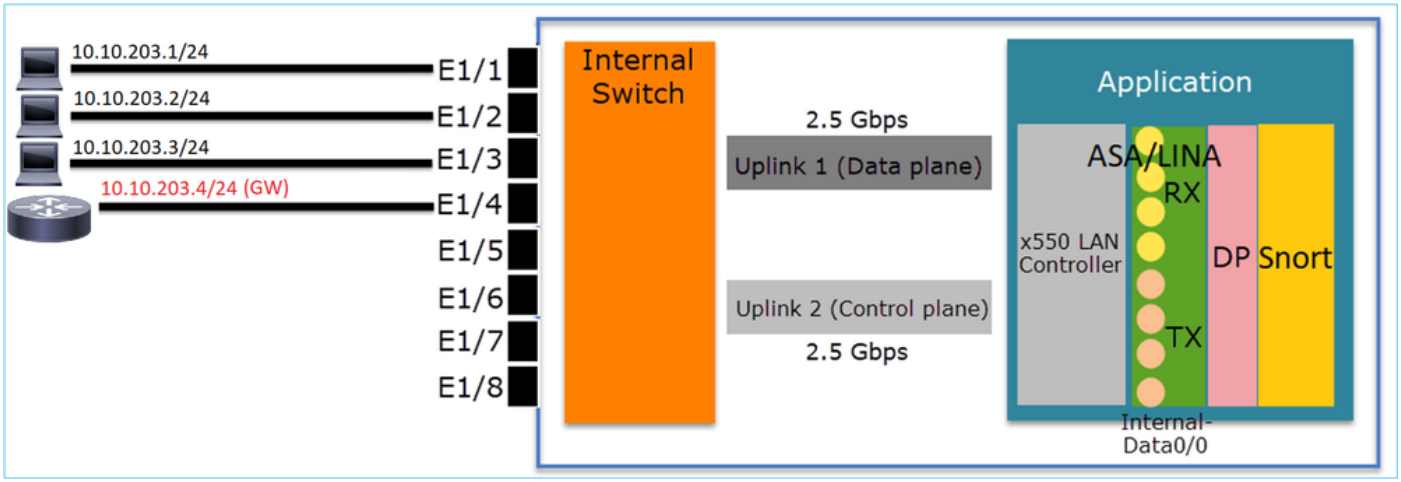
```
FP1010-2# show asp drop
Frame drop:
Flow is denied by configured rule (acl-drop) 1
```

Da der Drop unidirektional ist, kann Host-A (VLAN 203) keinen Datenverkehr zu Host-B (VLAN 204) initiieren. Das Gegenteil ist jedoch möglich:



Fallstudie - FP1010. Bridging und HW-Switching + Bridging

Betrachten Sie die folgende Topologie:



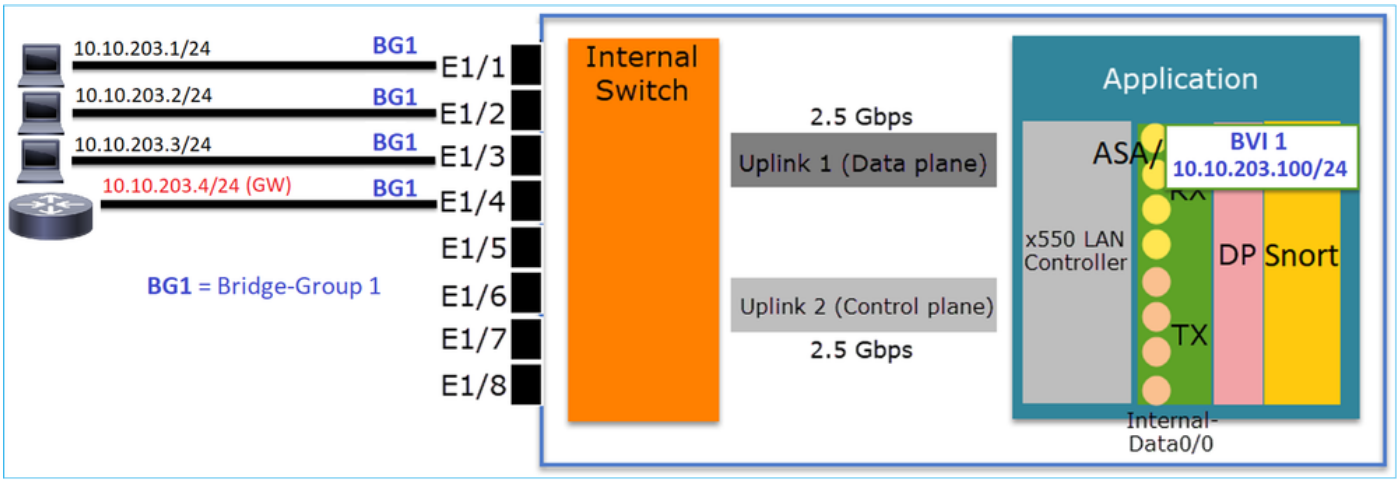
In dieser Topologie:

- Drei End-Hosts gehören demselben L3-Subnetz an (10.10.203.x/24).
- Der Router (10.10.203.4) agiert im Subnetz als GW.

In dieser Topologie gibt es zwei Hauptdesigns-Optionen:

1. Überbrückung
2. HW-Switching + Bridging

Designoption 1: Überbrückung

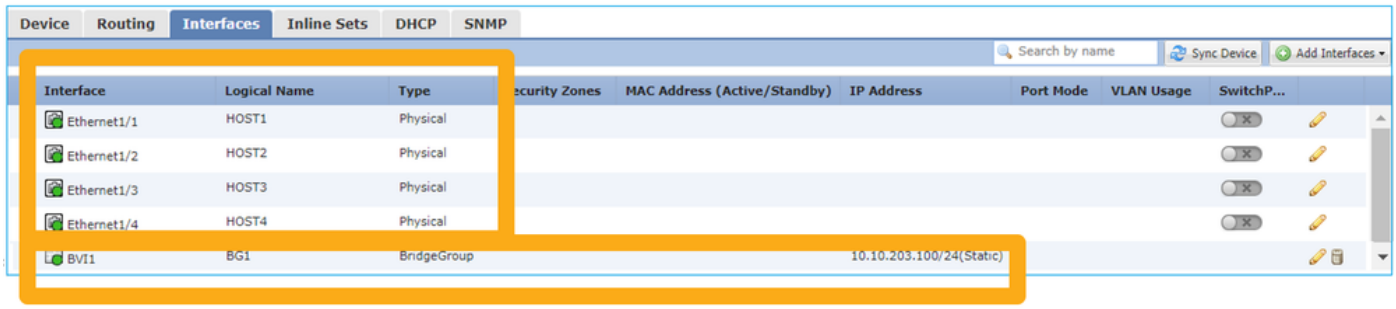


Wichtigste Punkte

Die wichtigsten Punkte dieses Designs sind:

- Es wird BVI 1 mit einer IP-Adresse im gleichen Subnetz (10.10.203.x/24) wie die vier angeschlossenen Geräte erstellt.
- Alle vier Ports gehören zur gleichen Bridge-Gruppe (in diesem Fall Gruppe 1).
- Für jeden der vier Ports ist ein Name konfiguriert.
- Host-zu-Host- und Host-zu-GW-Kommunikation erfolgt über die Anwendung (z. B. FTD).

Aus Sicht der FMC-Benutzeroberfläche lautet die Konfiguration wie folgt:

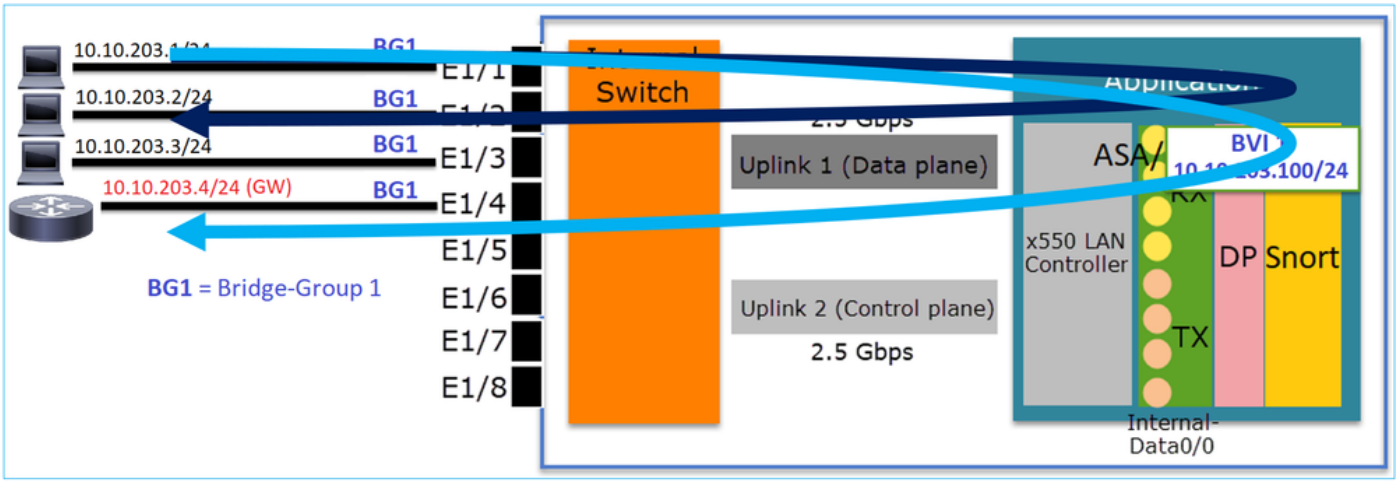


FTD-Schnittstellenkonfiguration

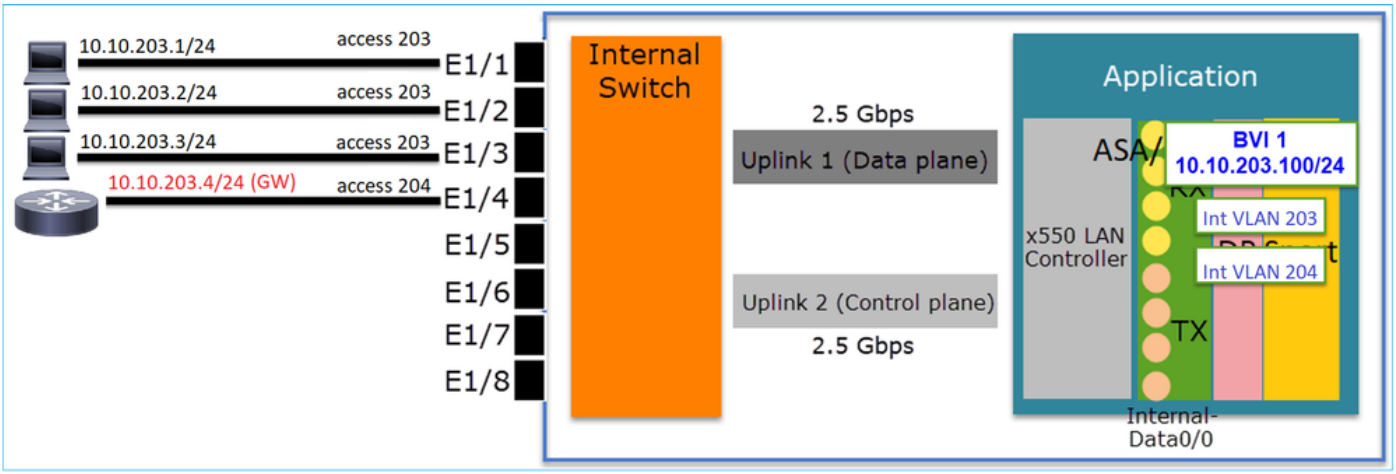
Die Konfiguration in diesem Fall ist:

```
interface BVI1 nameif BG1 security-level 0 ip address 10.10.203.100 255.255.255.0
interface Ethernet1/1
 no switchport bridge-group 1 nameif HOST1
interface Ethernet1/2
 no switchport
 bridge-group 1
 nameif HOST2
interface Ethernet1/3
 no switchport
 bridge-group 1
 nameif HOST3
interface Ethernet1/4
 no switchport
 bridge-group 1
 nameif HOST4
```

Der Datenverkehrsfluss in diesem Szenario:



Designoption 2: HW-Switching + Bridging

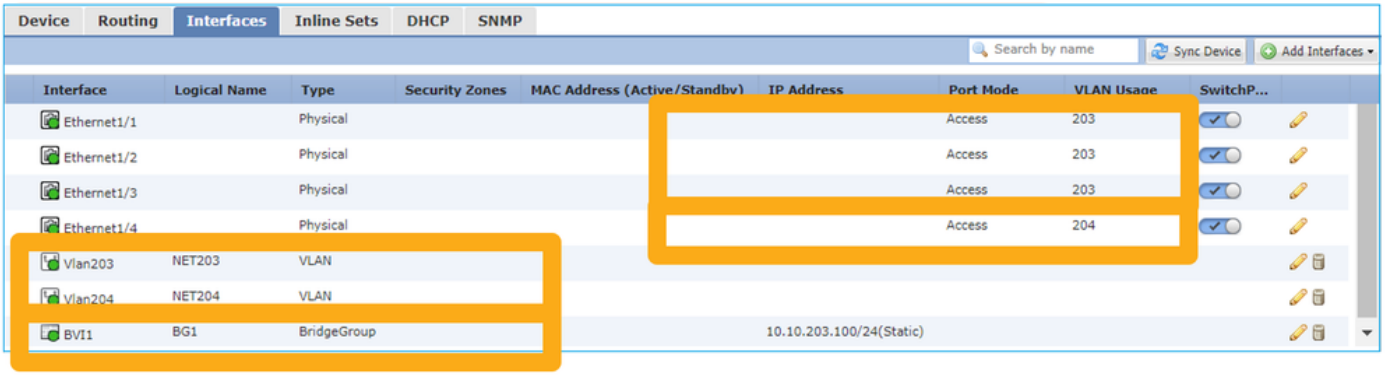


Wichtigste Punkte

Die wichtigsten Punkte dieses Designs sind:

- Es wird BVI 1 mit einer IP-Adresse im gleichen Subnetz (10.10.203.x/24) wie die vier angeschlossenen Geräte erstellt.
- Die mit den End-Hosts verbundenen Ports werden im SwitchPort-Modus konfiguriert und gehören zum gleichen VLAN (203).
- Der an das GW angeschlossene Port wird im SwitchPort-Modus konfiguriert und gehört zu einem anderen VLAN (204).
- Es gibt zwei VLAN-Schnittstellen (203, 204). Den beiden VLAN-Schnittstellen wurde keine IP zugewiesen, und sie gehören zur Bridge-Gruppe 1.
- Die Kommunikation zwischen Host erfolgt nur über den internen Switch.
- Die Host-zu-GW-Kommunikation erfolgt über die Anwendung (z. B. FTD).

FMC-UI-Konfiguration:

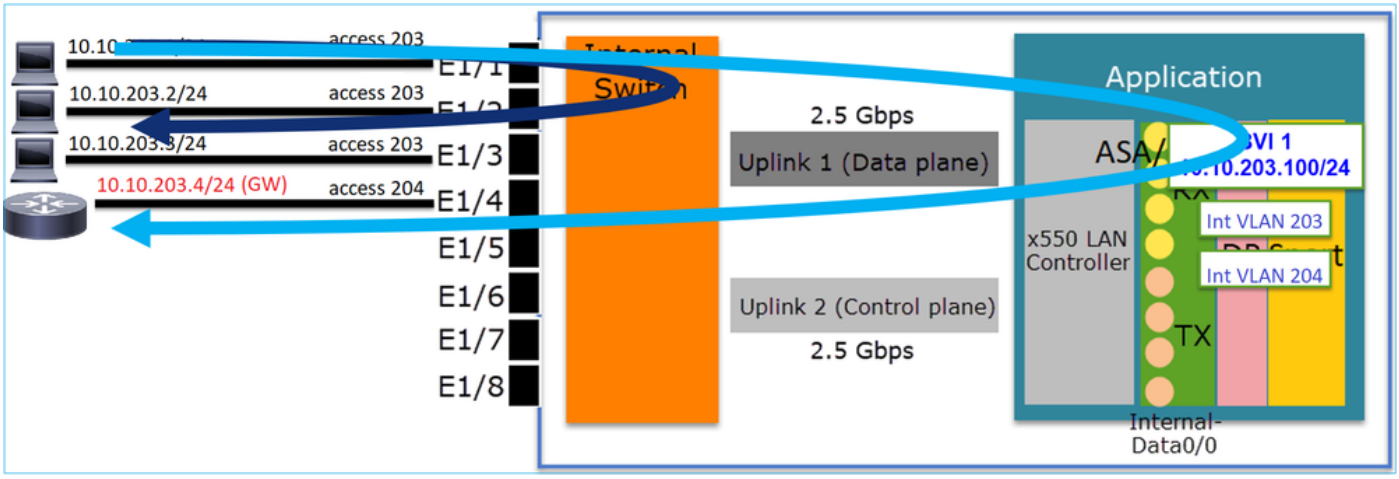


FTD-Schnittstellenkonfiguration

Die Konfiguration in diesem Fall ist:

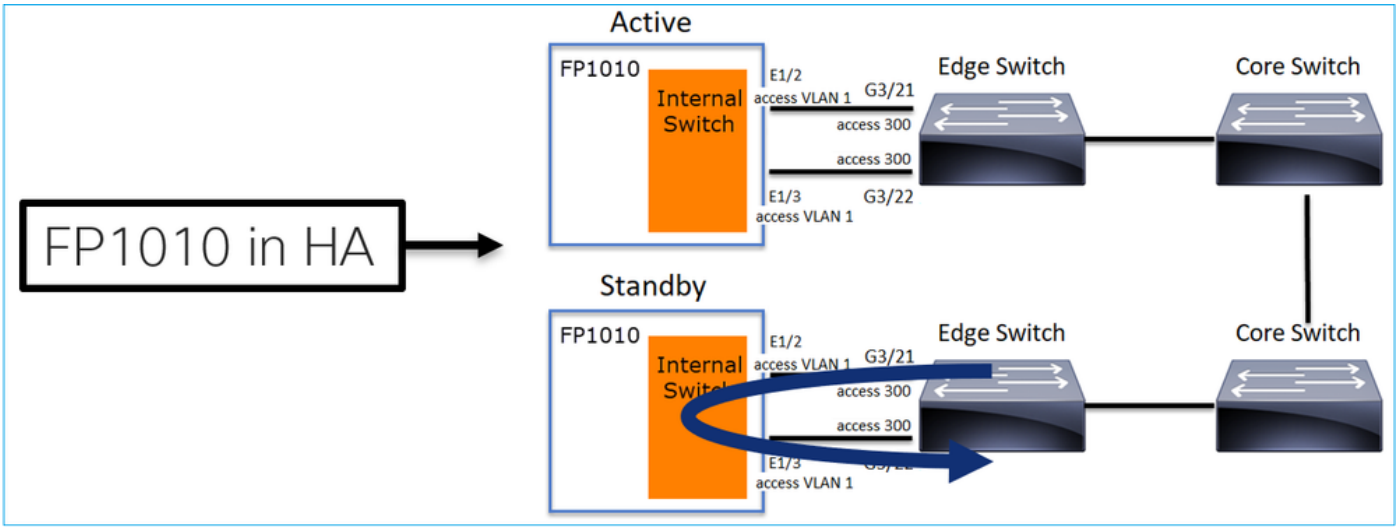
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1 nameif BG1 ip address 10.10.203.100 255.255.255.0
```

Host-zu-Host-Kommunikation und Host-zu-GW-Kommunikation:



FP1010 - Designüberlegungen

Switching und Hochverfügbarkeit (HA)

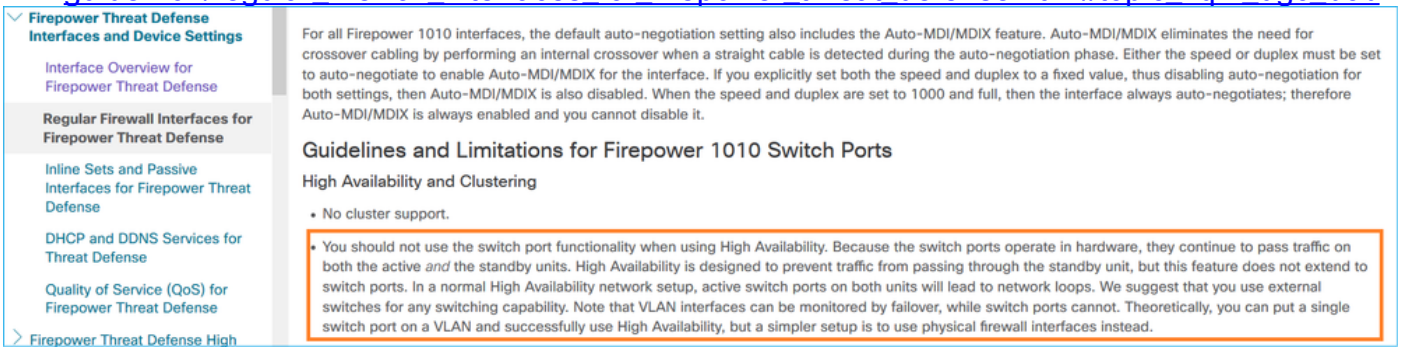


Wenn HW-Switching in einer HA-Umgebung konfiguriert ist, gibt es zwei Hauptprobleme:

1. Beim HW-Switching auf der Standby-Einheit werden Pakete über das Gerät weitergeleitet. Dies kann Datenverkehrsschleifen verursachen.
2. Switch-Ports werden nicht durch HA überwacht

Design-Anforderungen

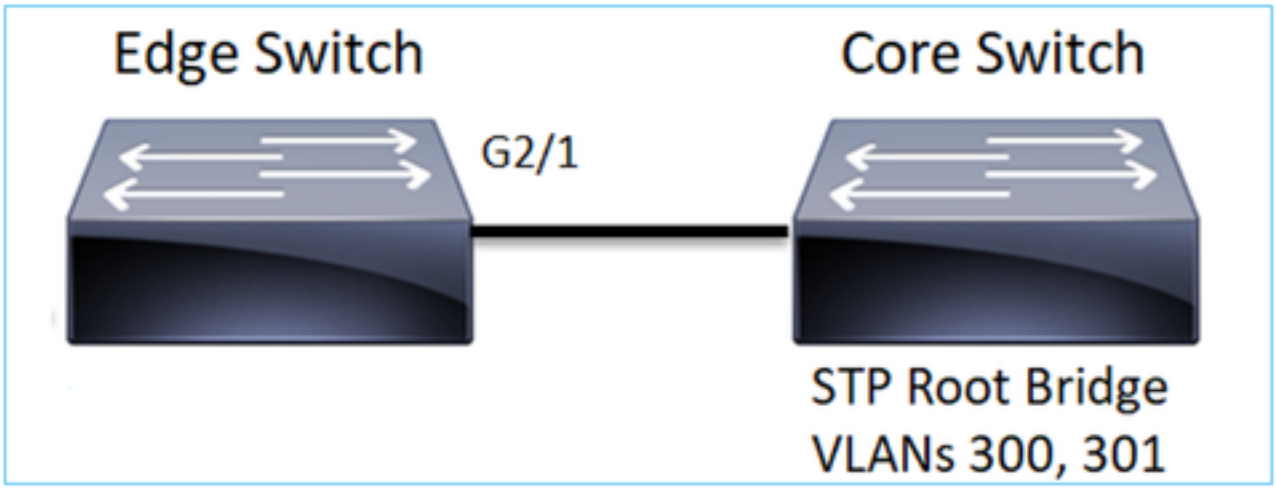
- Sie dürfen die SwitchPort-Funktionalität nicht mit ASA/FTD High Availability verwenden. Dies ist im FMC-Konfigurationsleitfaden dokumentiert: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b



Interaktion mit Spanning Tree Protocol (STP)

Der interne Switch FP1010 führt STP nicht aus.

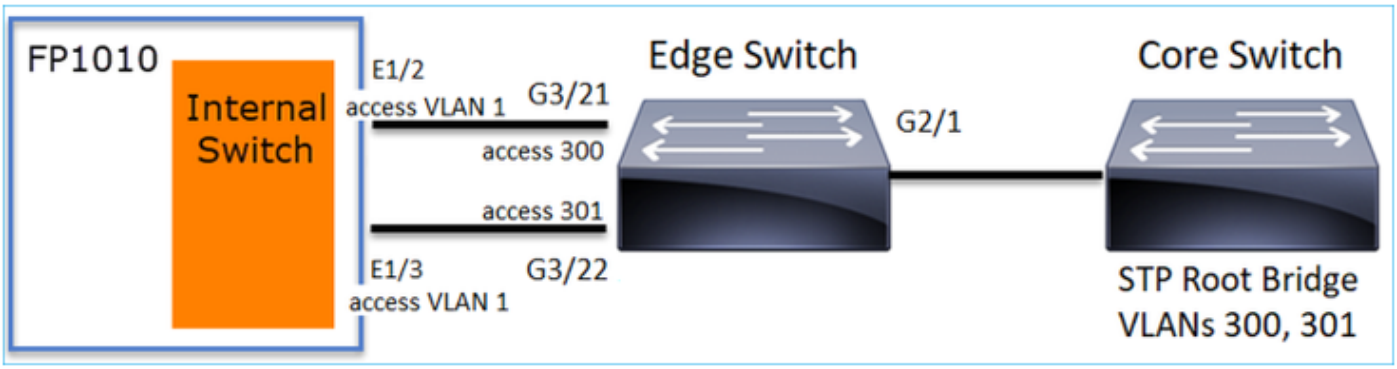
Betrachten Sie dieses Szenario:



Am Edge-Switch ist der Root-Port für beide VLANs G2/1:

```
Edge-Switch# show spanning-tree root | i 300|301
VLAN0300         33068 0017.dfd6.ec00         4    2   20  15  Gi2/1
VLAN0301  33069 0017.dfd6.ec00         4    2   20  15  Gi2/1
```

Verbinden Sie einen FP1010 mit dem Edge-Switch, und konfigurieren Sie beide Ports im gleichen VLAN (HW-Switching):



Das Problem

- Aufgrund der **VLAN-Auslagerung** überlegener BPDUs für VLAN 301, die auf G3/22 empfangen wurden

```
Edge-Switch# show spanning-tree root | in 300|301
VLAN0300         33068 0017.dfd6.ec00         4    2   20  15  Gi2/1
VLAN0301         33068 0017.dfd6.ec00         8    2   20  15  Gi3/22
```

> **Warnung:** Wenn Sie einen L2-Switch mit FP1010 verbinden, können Sie die STP-Domäne beeinflussen.

Dies ist auch im FMC-Konfigurationsleitfaden dokumentiert:

https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#task_rzl_bfc_b3b

> **Note** The Firepower 1010 does not support Spanning Tree Protocol for loop detection in the network. Therefore you must ensure that any connection with the FTD does not end up in a network loop.

FXOS REST-APIs

FMC REST-APIs

Dies sind die REST-API(s) für diese Funktionsunterstützung:

- L2 Physische Schnittstelle [Unterstützte PUT/GET]

/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/physicalinterfaces/{objectId}

- VLAN-Schnittstelle [Unterstützter POST/PUT/GET/DELETE]

/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUUID}/vlaninterfaces/{objectId}

Fehlerbehebung/Diagnose

Diagnoseübersicht

- Protokolldateien werden in einer FTD/NGIPS-Fehlerbehebung oder in der Ausgabe des "show tech" erfasst. Dies sind die Punkte, die bei der Fehlerbehebung näher erläutert werden müssen:
- /opt/cisco/platform/logs/portmgr.out
- /var/sysmgr/sam_logs/svc_sam_dme.log
- /var/sysmgr/sam_logs/svc_sam_portAG.log
- /var/sysmgr/sam_logs/svc_sam_appAG.log
- Asa running-config
- /mnt/disk0/log/asa-appagent.log

Erfassen von Daten von FXOS (Gerät) - CLI

Bei FTD (SSH):

```
> connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

...

FP1010-2# connect local-mgmt
FP1010-2(local-mgmt)#
```

Bei FTD (Konsole):

```
> connect fxos
You came from FXOS Service Manager. Please enter 'exit' to go back.
> exit FP1010-2# connect local-mgmt
FP1010-2(local-mgmt)#
```

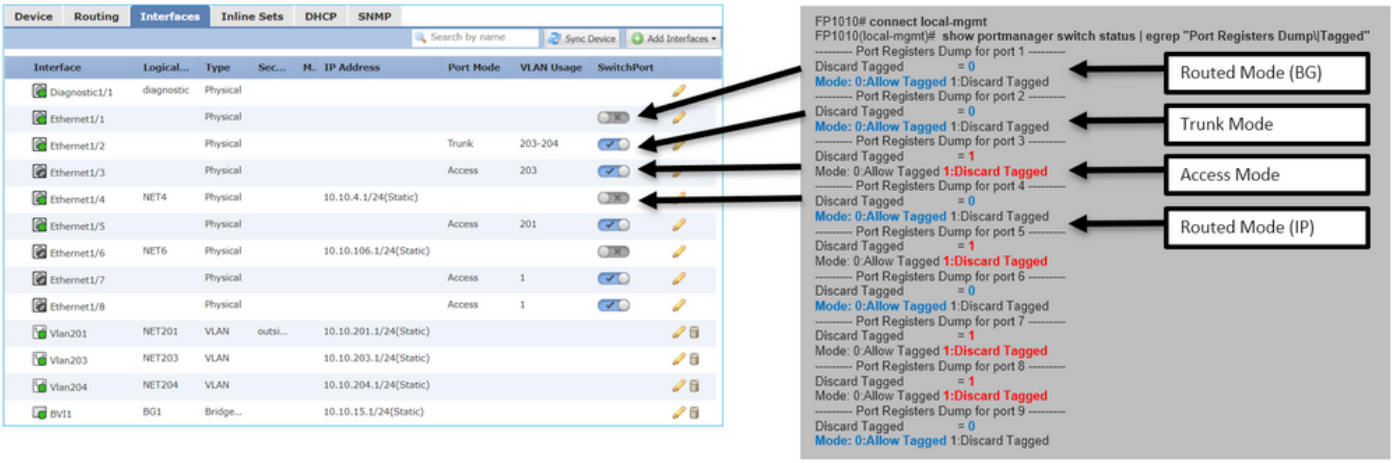
FP1010-Backend

Portregister definieren alle internen Switch- und Port-Funktionen.

In diesem Screenshot wird der Abschnitt 'Port Control' der Portregister und insbesondere das Register angezeigt, das vorgibt, ob markierter Datenverkehr, der an der Schnittstelle empfangen wird, verworfen (1) oder zugelassen (0) werden muss. Im Folgenden finden Sie den vollständigen Registerabschnitt für einen Port:

```
FP1010-2# connect local-mgmt
FP1010-2(local-mgmt)# show portmanager switch status
...
---Port Control 2            regAddr=8 data=2E80--

Jumbo Mode                    = 2
Mode: 0:1522 1:2048 2:10240

802.1q mode                   = 3
Mode: 0:Disable 1:Fallback 2:Check 3:Secure

Discard Tagged = 1 Mode: 0:Allow Tagged 1:Discard Tagged

Discard Untagged = 0 Mode: 0:Allow Untagged 1:Discard Untagged ARP Mirror = 0 Mode: 1:Enable
0:Disable Egress Monitor Source = 0 Mode: 1:Enable 0:Disable Ingress Monitor Source = 0 Mode:
1:Enable 0:Disable Port default QPri = 0
```

In diesem Screenshot sehen Sie die verschiedenen Werte für die mit Discard Tagged gekennzeichneten Register für die verschiedenen Portmodi:

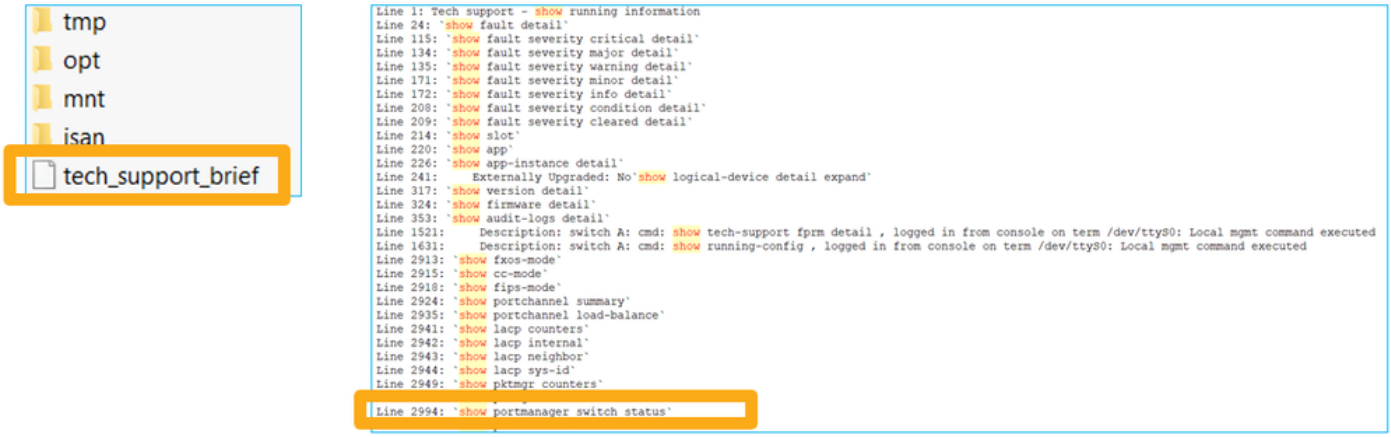


Erfassung von FPRM-Showtech auf FP1010

So generieren Sie ein FPRM-Paket und laden es auf einen FTP-Server hoch:

```
FP1010(local-mgmt)# show tech-support fprm detail
FP1010(local-mgmt)# copy workspace:///techsupport/20190913063603_FP1010-2_FPRM.tar.gz
ftp://ftp@10.229.20.96
```

Das FPRM-Paket enthält die Datei tech_support_brief. Die Datei tech_support_brief enthält eine Reihe von Anzeigebefehlen. Einer davon ist der **Switch-Status** von **show portmanager**:



Details zu Einschränkungen, häufige Probleme und Problemumgehungen

Einschränkungen der Implementierung für Version 6.5

- Dynamische Routing-Protokolle werden für SVI-Schnittstellen nicht unterstützt.
- Multi-Context wird auf 1010 nicht unterstützt.
- Der SVI-VLAN-ID-Bereich ist auf 1-4070 beschränkt.
- Port-Channel für L2 wird nicht unterstützt.
- L2-Port als Failover-Verbindung wird nicht unterstützt.

Einschränkungen in Bezug auf Switch-Funktionen

Funktion	Beschreibung	Begrenzung
Anzahl der VLAN-Schnittstellen	Gesamtzahl der VLAN-Schnittstellen, die erstellt werden können	60
VLAN im Trunk-Modus	Maximale Anzahl zulässiger VLANs an einem Port im Trunk-Modus	20
Natives VLAN	Ordnet alle nicht markierten Pakete zu Erreichen eines Ports zu nativem VLAN, das auf dem Port konfiguriert ist	1
Benannte Schnittstellen	Beinhaltet alle benannten Schnittstellen (VLAN-Schnittstelle, Subschnittstelle, Port-Channel, physische Schnittstelle usw.)	60

Weitere Einschränkungen

- Sub-Schnittstellen und Schnittstellen-VLAN können nicht dasselbe VLAN verwenden.
- Alle Schnittstellen, die an der BVI teilnehmen, müssen derselben Schnittstellenklasse angehören.
- Eine BVI kann mit einer Kombination aus L3-Modus-Ports und L3-Modus-Port-Subschnittstellen erstellt werden.
- Eine BVI kann mit einer Kombination von Schnittstellen-VLANs erstellt werden.

- Eine BVI kann nicht erstellt werden, indem L3-Modus-Ports und Schnittstellen-VLANs kombiniert werden.

Zugehörige Informationen

- Cisco FirePOWER 1010 Security Appliance
- Konfigurationsanleitungen