L2-Switch op FPR1010, Architectuur, verificatie en probleemoplossing

Inhoud

Inleiding

In dit document wordt de L2-switch op FP1010-apparaten beschreven. Het omvat met name het gedeelte Security Services Platform (SSP)/Firepower eXtensive Operating System (FXOS) van de implementatie. Bij de release 6.5 schakelt de Firepower 1010 (desktopmodel) in op de ingebouwde L2 hardware-switch. Dit helpt u extra hardware-switches te voorkomen en de kosten worden verlaagd.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

- FP1010 is een desktopmodel voor Small Office Home-Office (SOHO) dat als vervanging dient voor ASA 5505- en ASA 5506-X-platforms.
- Softwareondersteuning voor FTD-afbeeldingen (6.4+) die worden beheerd door ofwel FireSIGHT Management Center (FMC), Firepower Devices Manager (FDM) of Cloud Defense Orchestrator (CDO).
- Softwareondersteuning voor ASA-afbeeldingen (9.13+) die worden beheerd door CSM, ASDM of CLI.
- Het besturingssysteem (OS), ASA of FTD, wordt gebundeld met FXOS (gelijk aan FP21xx).
- 8 x 10/100/1000 Mbps gegevenspoorten.
- Ondersteuning van E1/7 poorten, E1/8 PoE+
- Op de hardware-switch kan lijnsnelheidscommunicatie tussen poorten worden toegestaan (bijvoorbeeld: een cameraspeler in de lokale server).

Firepower 6.5 Toevoegingen

- Inleiding van een nieuw type interface met de naam Switched Virtual Interface (SVI).
- Gemengde modus: Interfaces kunnen worden ingesteld in een switched (L2) of niet-switched (L3) modus.
- L3 mode interfaces naar alle pakketten naar de veiligheidstoepassing doorsturen.
- L2 mode poorten kunnen in hardware switches als twee poorten deel uitmaken van hetzelfde VLAN dat de doorvoersnelheid en de latentie verbetert. En pakketten die moeten worden routeerd of overbrugd bereiken de veiligheidstoepassing (bijvoorbeeld: een camera die een nieuwe firmware vanuit het internet downloaden) en een veiligheidscontrole ondergaan volgens de configuratie.
- L2 fysieke interface kan worden gekoppeld aan een of meerdere SVI-interfaces.
- L2 mode interfaces kunnen in toegang of boomstammodus zijn.

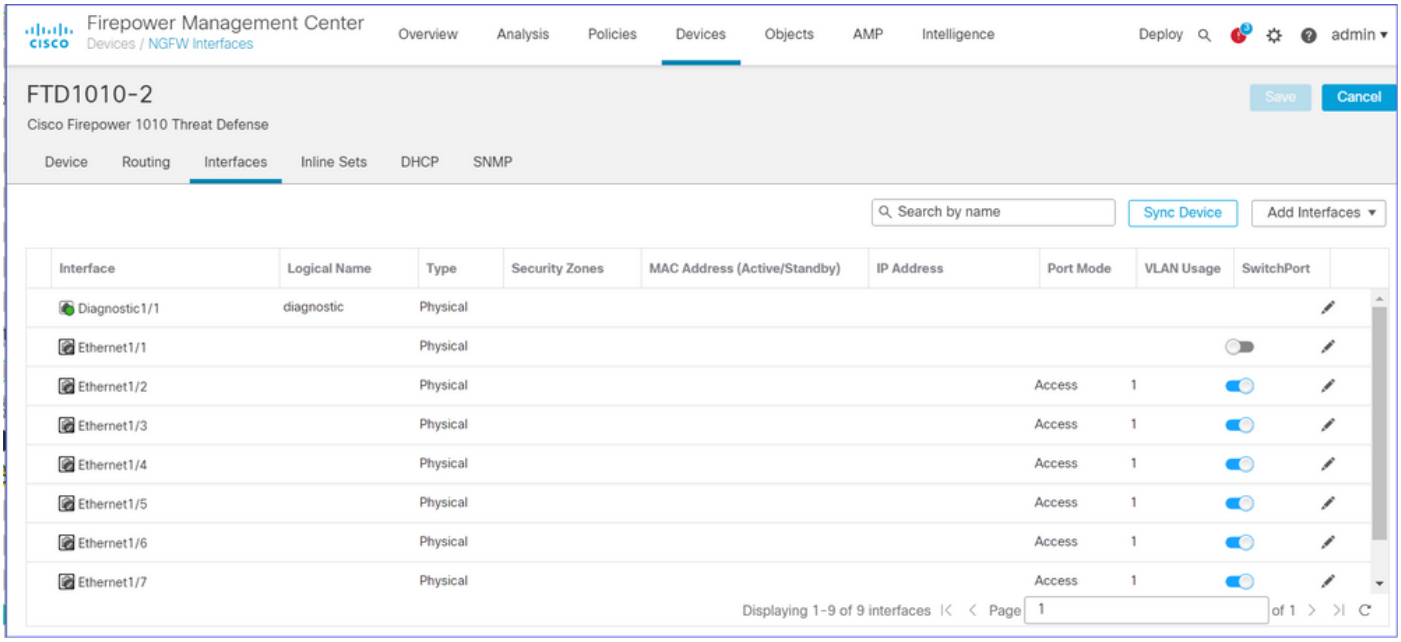
- De interface van de toegangsmodus L2 maakt alleen niet-gelabeld verkeer mogelijk.
- De interface Trunk-modus L2 maakt gelabeld verkeer mogelijk.
- Ondersteuning van native VLAN-ondersteuning voor L2-interface in de basismodus.
- ASA CLI's, ASDM, CSM, FDM en FMC worden uitgebreid ter ondersteuning van nieuwe functies.

FMC-toevoegingen

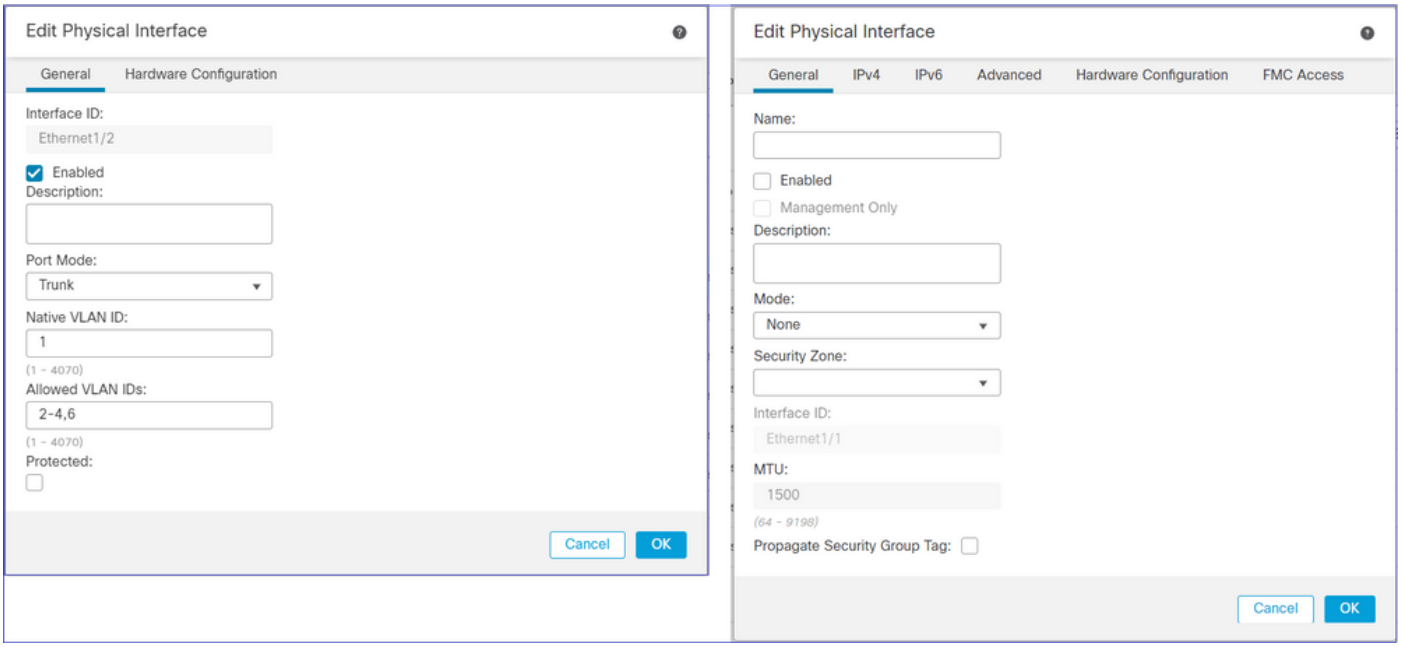
- Een nieuwe interfacemodus die schakelpoort wordt genoemd is geïntroduceerd voor een fysieke interface die wordt gebruikt om te identificeren of een fysieke interface een L3 of L2 interface is.
- L2 fysieke interface kan met één of meerdere VLAN-interfaces gekoppeld worden op basis van toegang of basismodus.
- Firepower 1010 ondersteunt Power over Ethernet (PoE)-configuratie op de laatste twee gegevensinterfaces, d.w.z. Ethernet1/7 en Ethernet1/8.
- De verandering van de interface tussen geschakeld en niet geschakeld opent alle configuraties behalve de PoE en de configuratie van de Hardware.

Hoe werkt het?

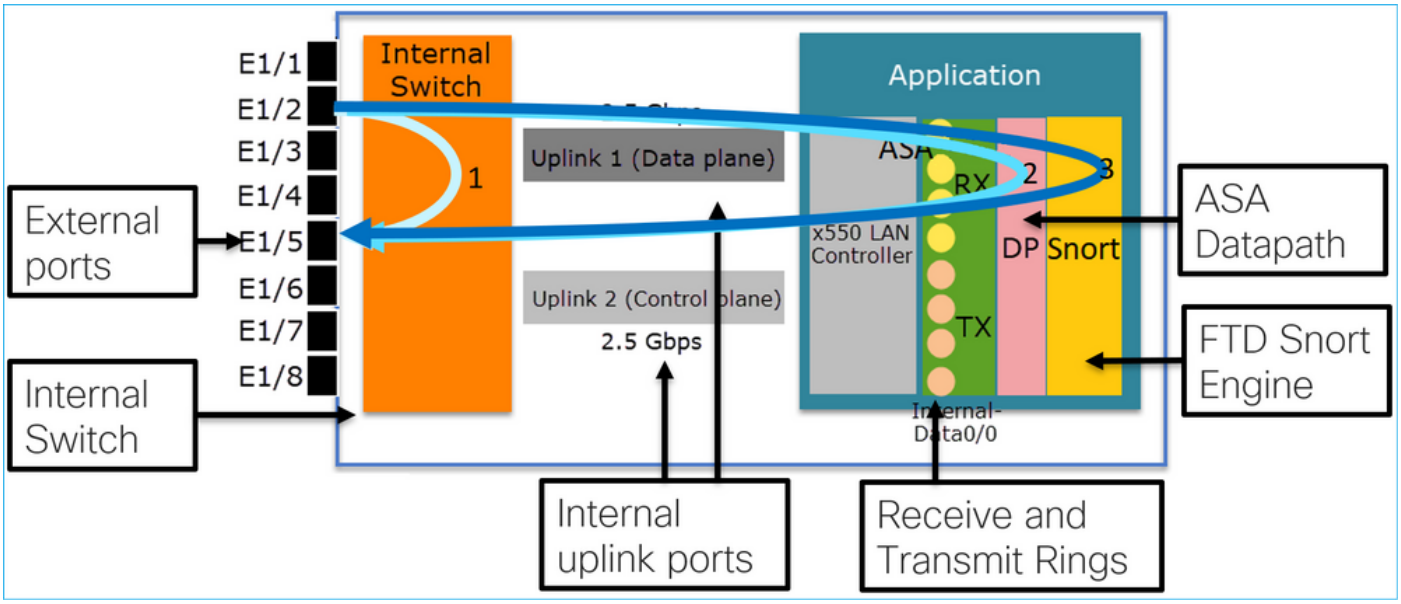
Deze optie is slechts een versterking van bestaande interfaceondersteuning op FMC (**Apparaatbeheer > Interfacepagina**).



Fysieke interfaceweergave (L2 en L3)



FP1010-architectuur



- 8 Externe gegevenspoorten.
- 1 Interne Switch.
- 3 Uplink-poorten (waarvan er twee in het beeld worden weergegeven), één voor datacenter, één voor besturingsplane en één voor configuratie.
- x550 LAN controller (de interface tussen de toepassing en de uplinks).
- 4 Ontvang (RX) en 4 transmissies (TX).
- Datapath-proces (op ASA en FTD).
- Snellproces (op FTD).

PacketProcessing

Twee belangrijke factoren kunnen de pakketverwerking beïnvloeden:

1. Interface/poortmodus

2. Toepasselijk beleid

Een pakket kan een FP1010 op 3 verschillende manieren doorlopen:

1. Alleen verwerkt door de interne switch

2. Alleen doorgestuurd naar de applicatie (ASA/FTD) en alleen verwerkt door het datapath-proces

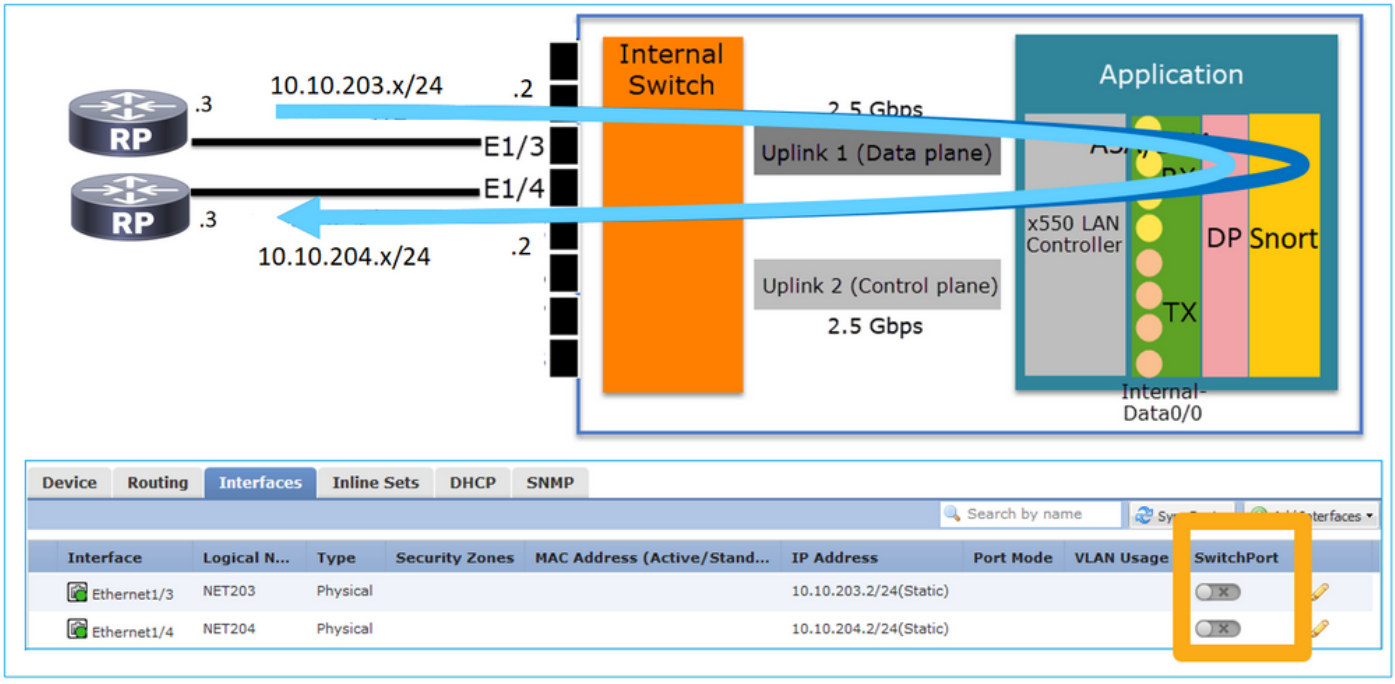
3. Verstuurd naar de aanvraag (FTD) en verwerkt door de datapath- en Snort-motor

FP1010-poortmodules

De UI-voorbeelden zijn voor FMC, de CLI-voorbeelden zijn voor FTD. De meeste concepten zijn ook volledig van toepassing op een ASA.

FP1010 Case 1.0 Routed Port (IP-routing)

Configuratie en werking



Belangrijkste punten

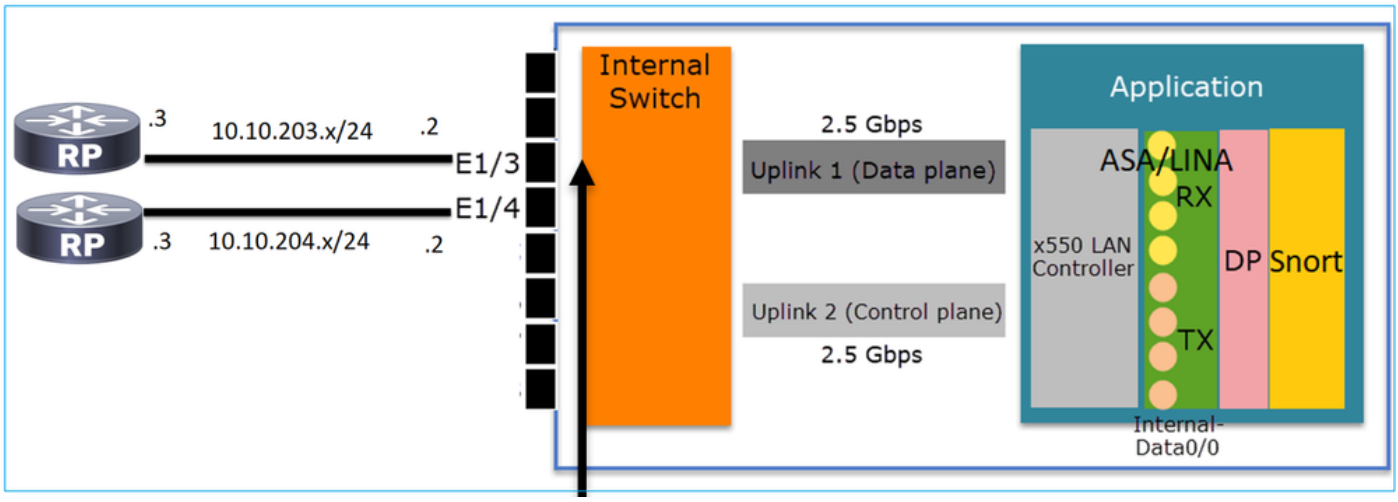
- Vanuit het oogpunt van het ontwerp behoren de twee havens tot 2 verschillende L2 subnetten.
- Wanneer de poorten in Routed Mode zijn ingesteld, worden de pakketten verwerkt door de toepassing (ASA of FTD).
- In het geval van FTD, op basis van de regelactie (bijv. ALLOW), kunnen de pakketten zelfs worden geïnspecteerd door de sorteermachine.

FTD-interfaceconfiguratie

```
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 routepoortverificatie



Van FXOS CLI kunt u de fysieke interfacetellers controleren. Dit voorbeeld toont de ingress unicast- en egress unicast-loketten op de E1/3-poort:

```
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 Captures kan worden toegepast en pakketten kunnen worden gevolgd:

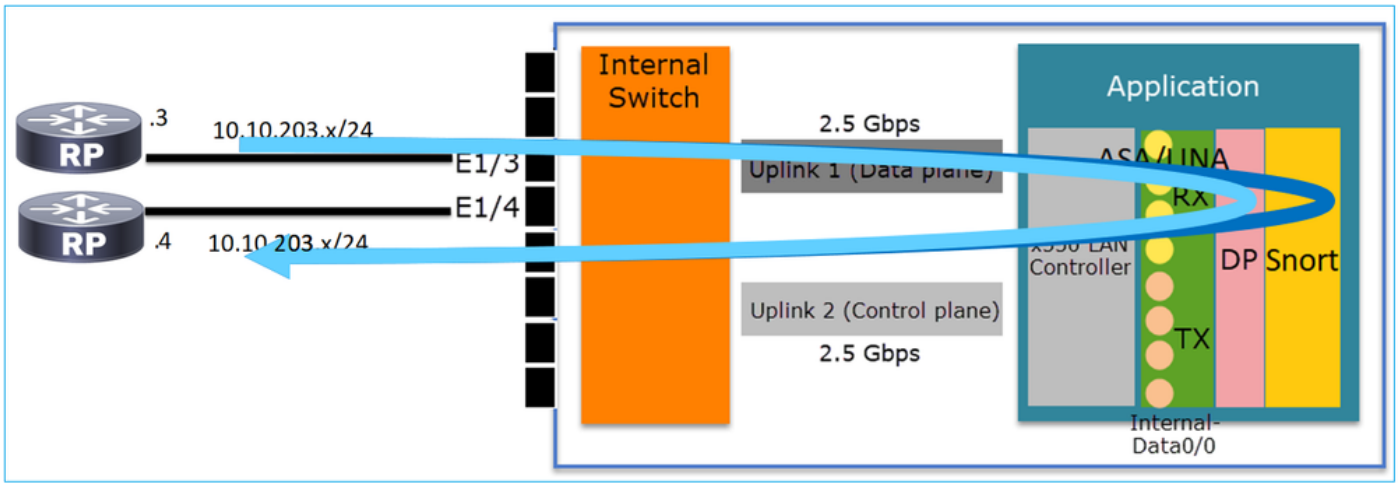
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

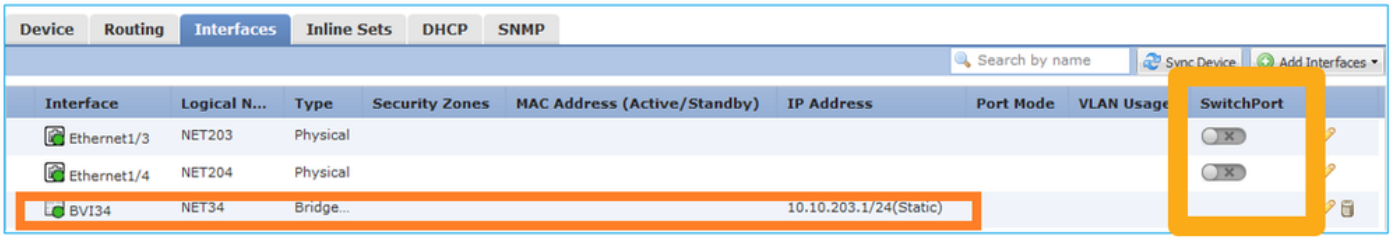
Dit is een vangnet. Zoals verwacht wordt het pakket verzonden op basis van een ROUTE LOOKUP:

```
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
```

FP1010 Case 2. Bridge-Group mode (overbrugging)

Configuratie en werking





Belangrijkste punten

- Vanuit een ontwerpstandpunt worden de 2 poorten aangesloten op dezelfde L3-subvorm (gelijk aan een transparante firewall) maar op verschillende VLAN's.
- Wanneer de poorten in overbruggingsmodus zijn ingesteld, worden de pakketten verwerkt door de toepassing (ASA of FTD).
- In het geval van FTD, op basis van de regelactie (bijv. ALLOW), kunnen de pakketten zelfs worden geïnspecteerd door de sorteermachine.

FTD-interfaceconfiguratie

```
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 Bridge-Group poortverificatie

Deze opdracht toont de interfaceleden van BVI 34:

```
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
```

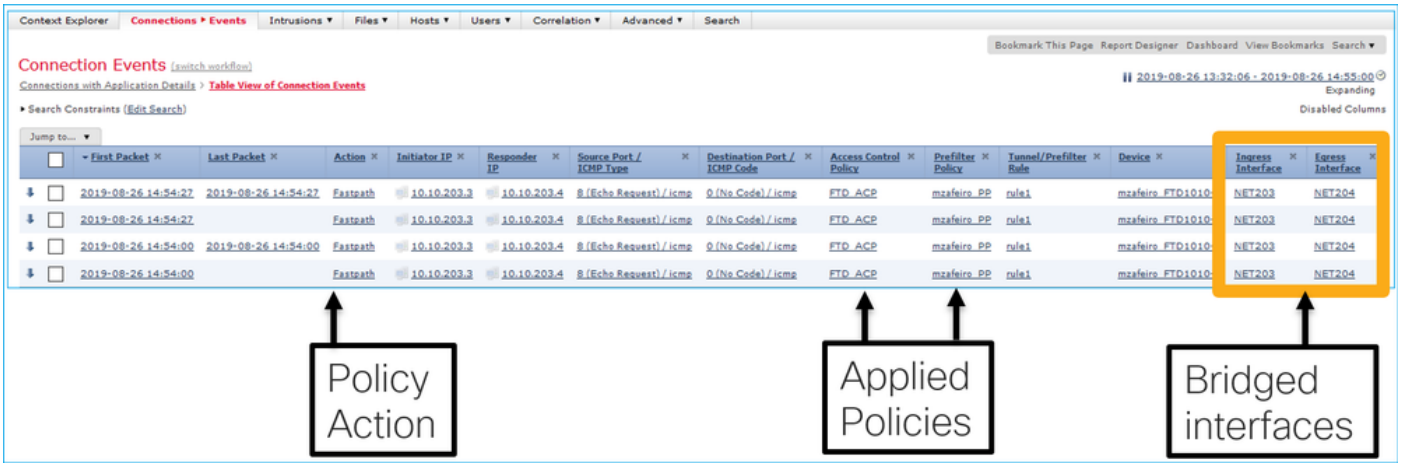
Deze opdracht toont de ASA/FTD Data Content Adresseerbare Geheugen (CAM) tabel:

```
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
```

Een pakketsporenfragment toont dat het pakket is doorgestuurd op basis van de MAC L2-favoriet van de bestemming:

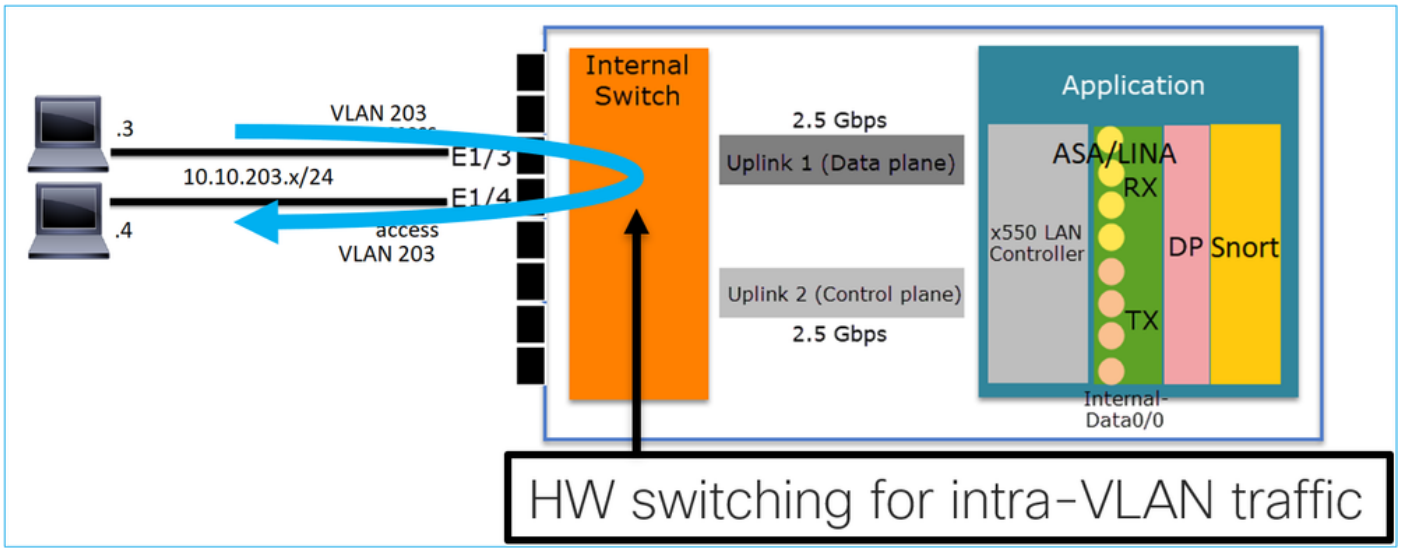
```
FP1010# show cap CAP203 packet-number 1 trace

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
```

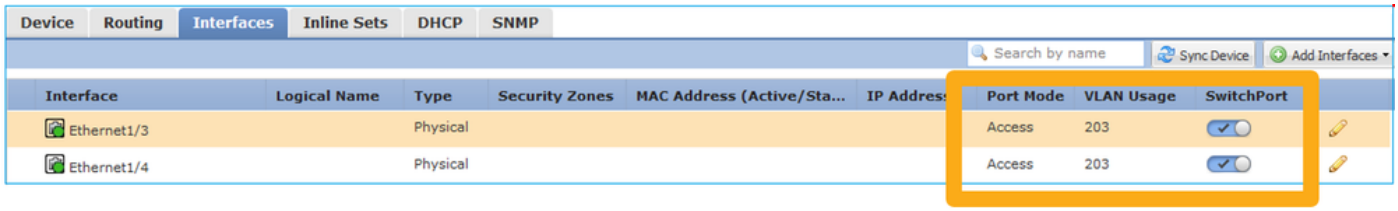
In het geval van FTD kunnen FMC Connection-evenementen ook informatie verstrekken over de stroominspectie en de overloopbrug-groepsinterfaces:



FP1010 Case 3. Switches (HW-switching) in toegangsmodus

Configuratie en werking





Belangrijkste punten

- HW-switching is een FTD **6.5+** en ASA **9.13+** optie.
- Vanuit een ontwerpstandpunt worden de 2 poorten aangesloten op dezelfde L3-bits en hetzelfde VLAN.
- De poorten in dit scenario werken in de toegangsmodus (alleen zonder tag).
- De firewallpoorten die in SwitchPort-modus zijn ingesteld, hebben geen logische naam (naam indien) ingesteld.
- Wanneer de poorten in switchingmodus worden geconfigureerd en tot hetzelfde VLAN (intra-VLAN-verkeer) behoren, worden de pakketten alleen verwerkt door de FP1010 interne switch.

FTD-interfaceconfiguratie

Vanuit een CLI-standpunt ziet de configuratie er sterk uit als een L2-switch:

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

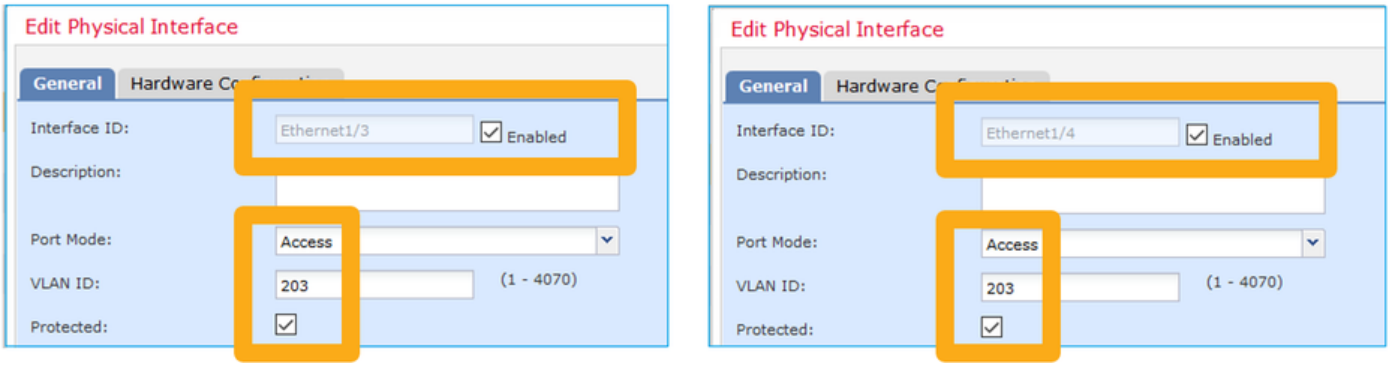
Filtering van verkeer binnen VLAN

De uitdaging: **ACL kan verkeer binnen VLAN niet filteren!**

De oplossing: **Beschermde** poorten

Het principe is heel eenvoudig: 2 poorten die zijn geconfigureerd als beveiligd, kunnen niet met elkaar praten.

FMC UI in het geval van beschermde havens:



FTD-interfaceconfiguratie

De opdracht **switchpoort die beveiligd** is, wordt ingesteld onder de interface:

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

FP1010 switchingverificatie

In dit voorbeeld worden er 1000 pakketten met een specifieke grootte (1100 bytes) verzonden:

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

Gebruik deze opdracht om de ingangen en reling te controleren op eenastloketten van de transitinterfaces:

```
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
```

Deze opdracht toont de status Interne switch VLAN:

```
FP1010# show switch vlan
VLAN Name            Status    Ports
```

```
---- -------------- --------- ----------------------
1    -              down
203 - up Ethernet1/3, Ethernet1/4
```

De status van een VLAN is UP zolang minimaal één poort is toegewezen aan het VLAN

Als een poort administratief wordt ingedrukt of de aangesloten poort op de switch is afgesloten/kabel is losgekoppeld en dit is de enige poort die aan VLAN is toegewezen, is de VLAN-status ook minder:

```
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
```

Deze opdracht toont de CAM-tabel van de interne switch:

```
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
```

De standaard verouderingstijd van de interne switch CAM-tabel is 5 min 30 seconden.

FP1010 bevat 2 CAM-tabellen:

1. Inwendige CAM-tabel van Switch: Gebruikt in geval van HW-switching
2. ASA/FTD datapath CAM-tabel: Gebruikt bij overbrugging

Elk pakket/kader dat over FP1010 loopt wordt verwerkt door één enkele CAM-tabel (interne switch of FTD datapath) op basis van de poortmodus.

> Voorzichtig: Verwar de in SwitchPort-modus gebruikte interne switch CAM-tabel van de show switch niet met de CAM-tabel met hoofdadres waarvoor een FTD-datapath wordt gebruikt in een overbrugde modus

Hoe switching: Extra dingen om te weten te komen

ASA/FTD datapath-blogs tonen geen informatie over HW-switched stromen:

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

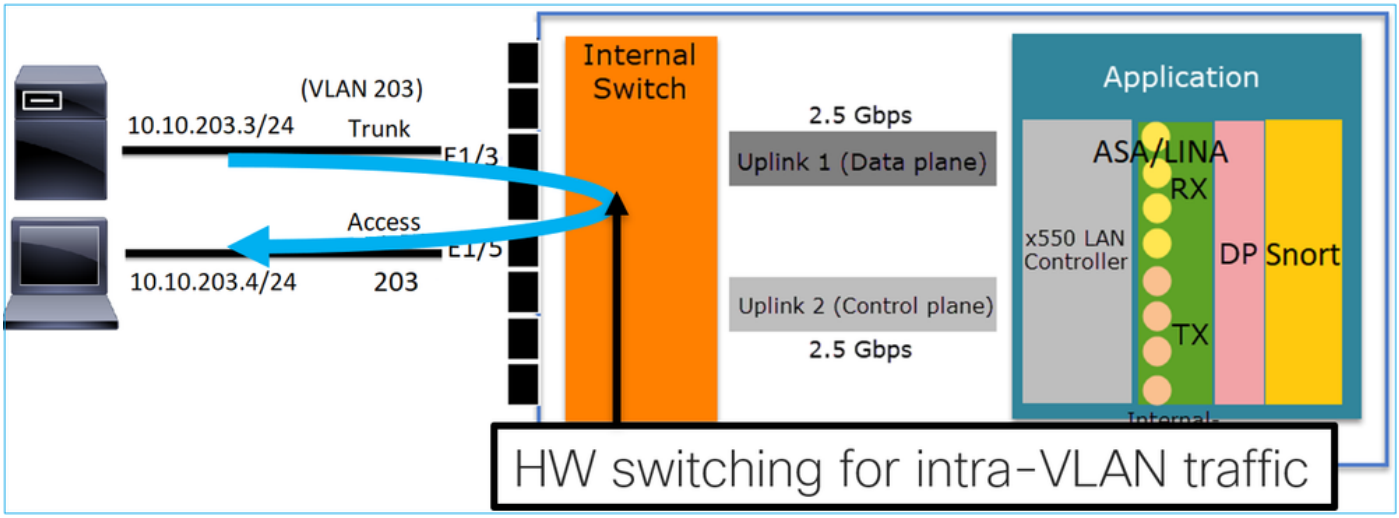
ASA/FTD datapath-verbindingstabel bevat geen HW-switched stromen:

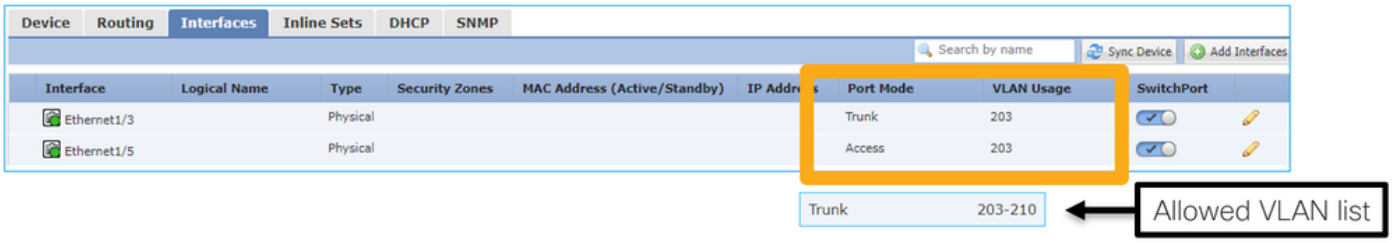
```
FP1010# show conn
0 in use, 3 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

Bovendien tonen de gebeurtenissen van de verbinding van FMC geen HW-switched stromen.

FP1010 Case 4.0 Switches (trunking)

Configuratie en werking





Belangrijkste punten

- HW-switching is een FTD **6.5+** en ASA **9.13+** optie.
- Vanuit een ontwerpstandpunt worden de 2 poorten aangesloten op dezelfde L3-bits en hetzelfde VLAN.
- Trunk-poort accepteert gekoppelde frames en untagged (in het geval van een inheems VLAN).
- Wanneer de poorten in switchingmodus zijn geconfigureerd en tot hetzelfde VLAN (intra-VLAN-verkeer) behoren, worden de pakketten alleen door de interne switch verwerkt.

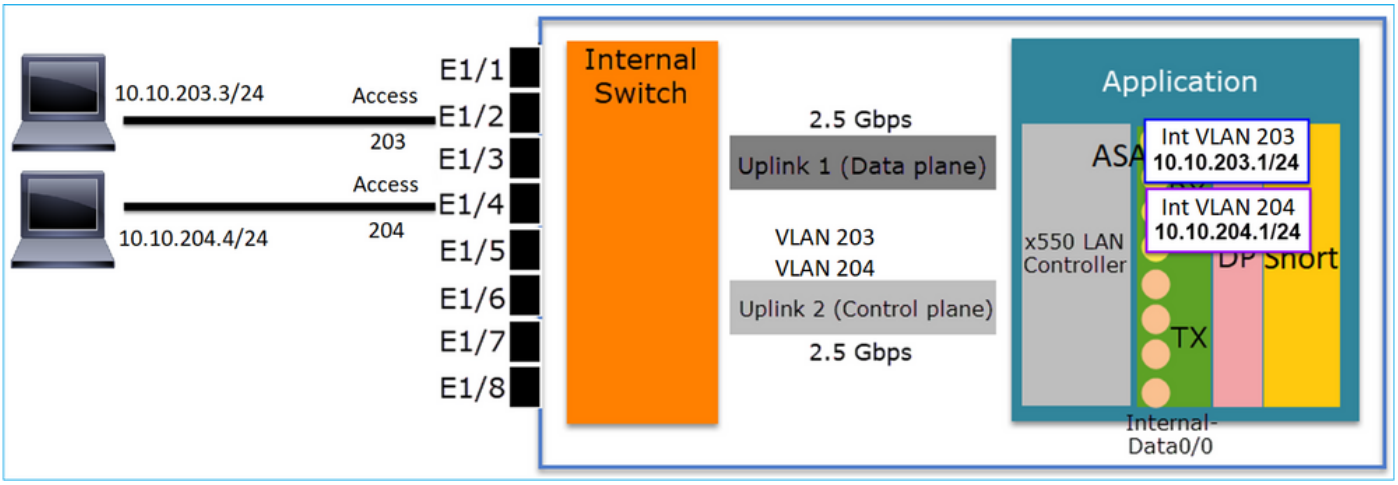
FTD-interfaceconfiguratie

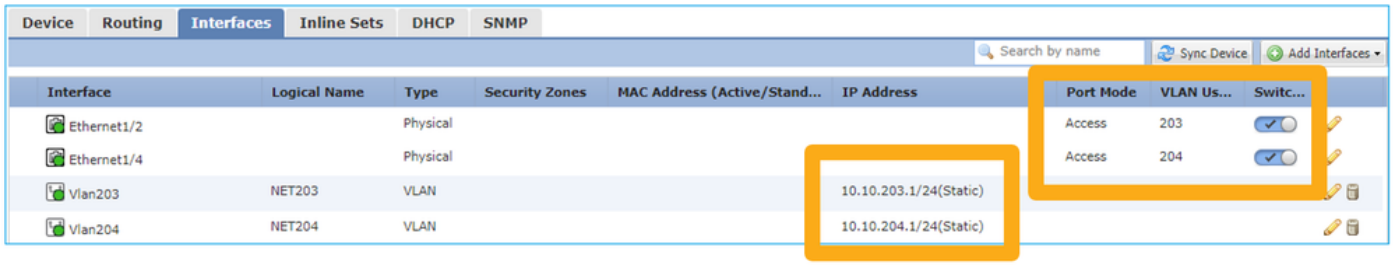
De configuratie is vergelijkbaar met een Layer 2 switch poort:

```
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
```

FP1010 Case 5.0 Switches (Inter-VLAN)

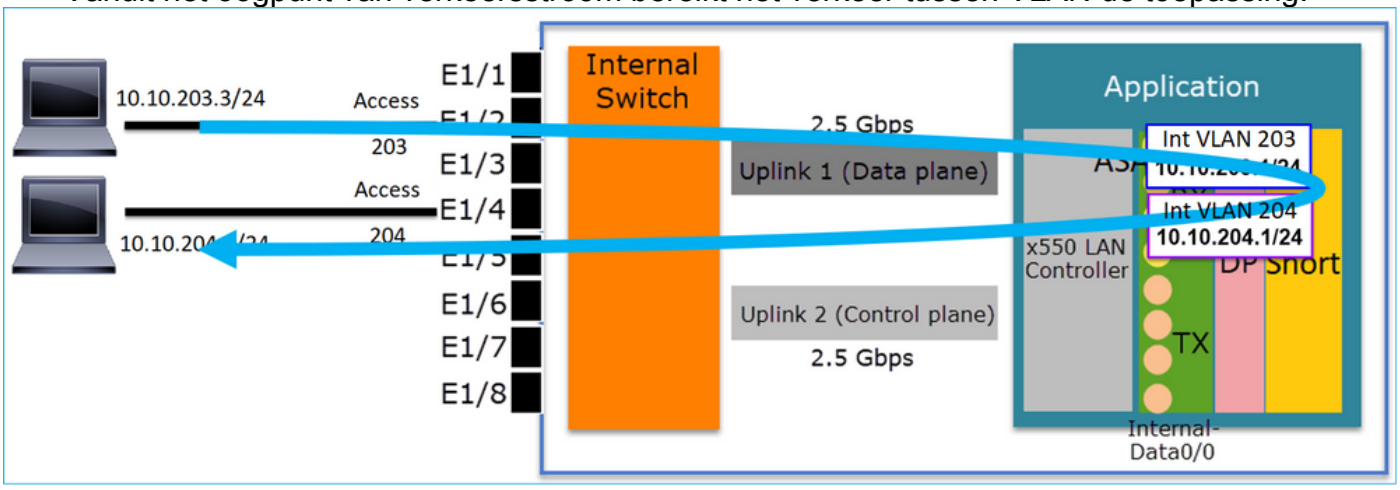
Configuratie en werking





Belangrijkste punten

- Vanuit ontwerpstandpunt worden de 2 poorten aangesloten op 2 verschillende L3 subnetten en 2 verschillende VLAN's.
- Het verkeer tussen de VLAN's gaat door de VLAN-interfaces (gelijk aan SVIs).
- Vanuit het oogpunt van verkeersstroom bereikt het verkeer tussen VLAN de toepassing.



FTD-interfaceconfiguratie

De configuratie is vergelijkbaar met een Switch virtuele interface (SVI):

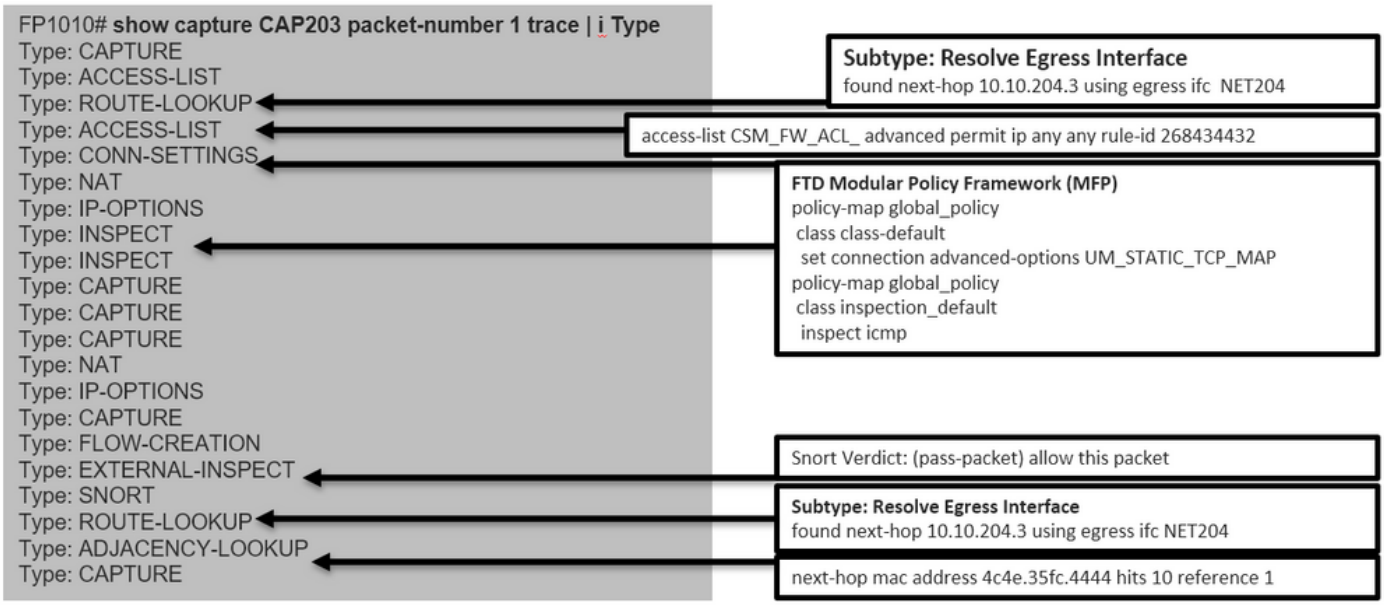
```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

Packet Processing voor interVLAN-verkeer

Dit is een spoor van een pakje dat door 2 verschillende VLAN's overschrijdt:

```
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
```

De belangrijkste fasen in het pakketproces:



FP1010 Case 6. Inter-VLAN-filter

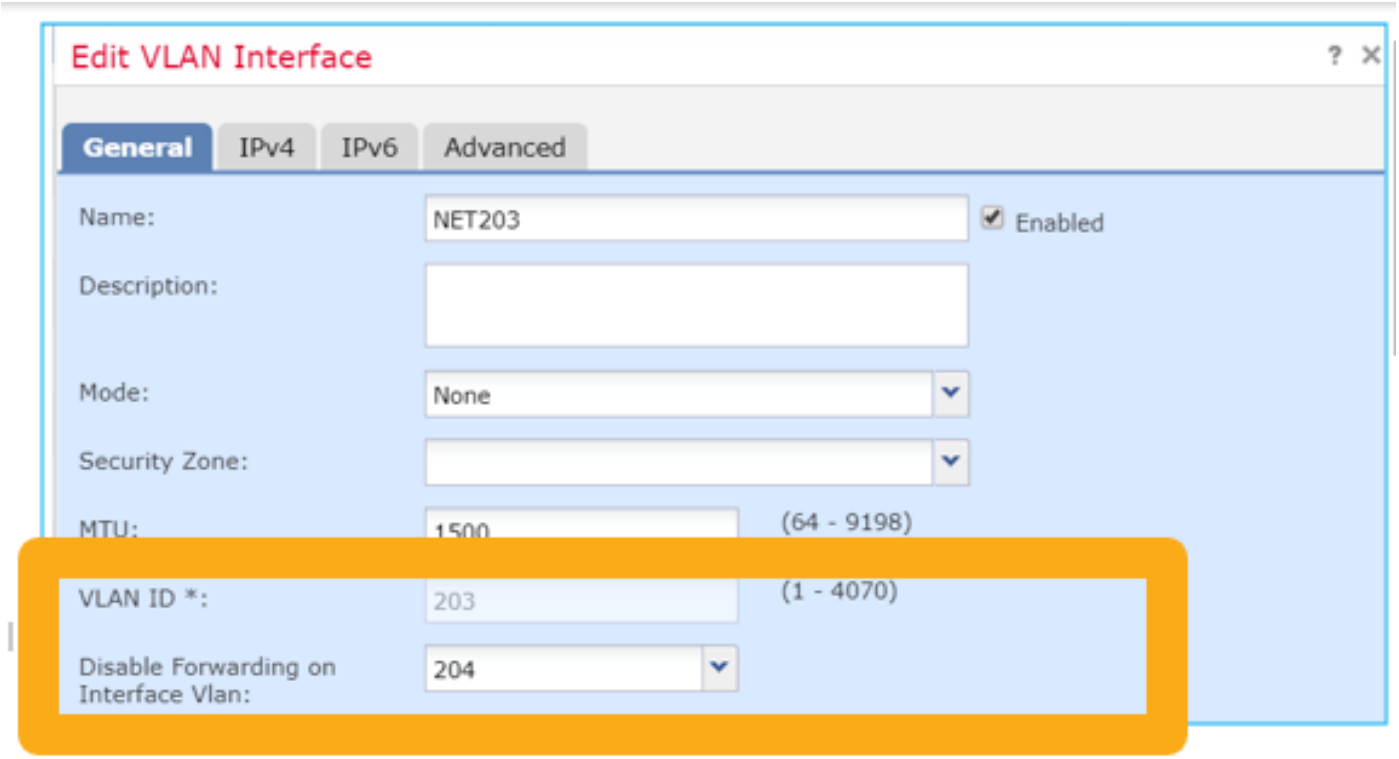
Configuratie en werking

Er zijn 2 hoofdopties om verkeer tussen VLAN's te filteren:

1. Toegangsbeheerbeleid
2. commando '**geen voorwaartse**'

Filter verkeer tussen VLAN met het gebruik van de "no-forward" opdracht

configuratie FMC UI:



Belangrijkste punten

- De no-forward-daling is in één richting gericht.
- Het kan niet op beide interfaces van VLAN worden toegepast.
- De niet-voorwaartse controle wordt uitgevoerd vóór de ACL-controle.

FTD-interfaceconfiguratie

De CLI-configuratie in dit geval is:

```
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
```

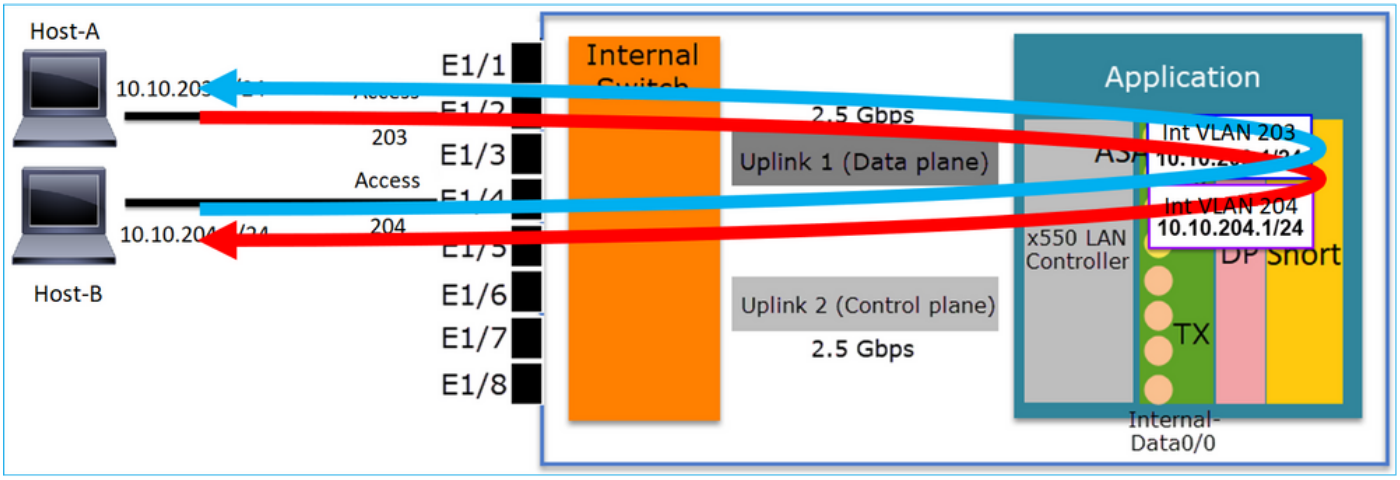
Als een pakje door de optie Geen voorwaartse voorziening wordt verbroken, wordt een ASA/FTD Data Syslog-bericht gegenereerd:

```
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)
```

Vanuit het vervolgkeuzepunt Accelerated Security Path (ASP) wordt het beschouwd als een ACL-daling:

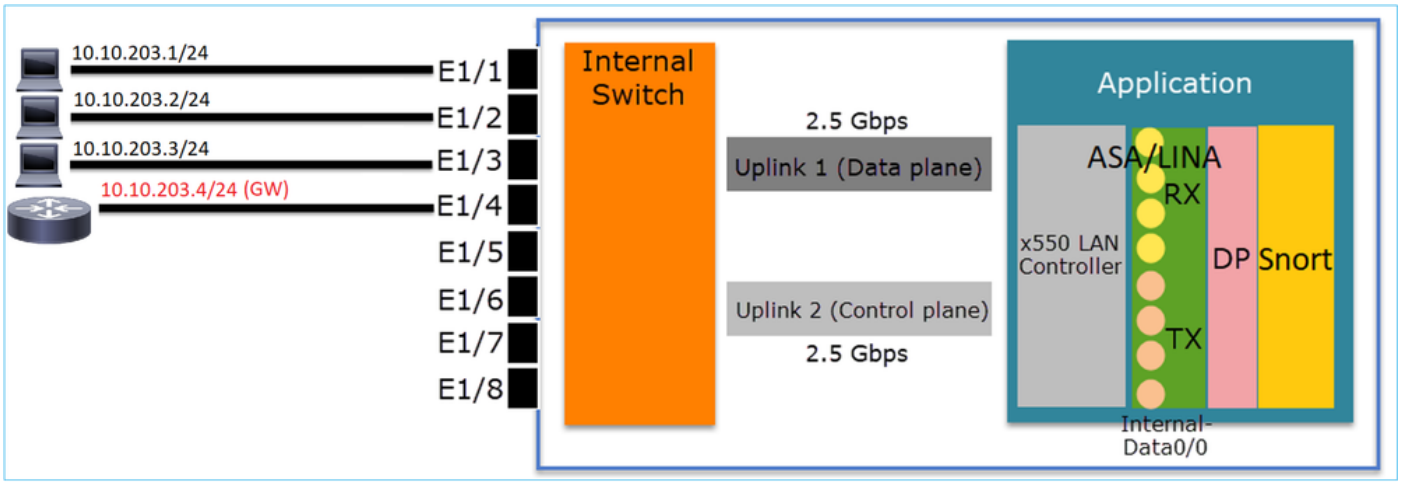
```
FP1010-2# show asp drop
Frame drop:
Flow is denied by configured rule (acl-drop) 1
```

Aangezien de druppel unidirectioneel is, kan Host-A (VLAN 203) geen verkeer naar Host-B (VLAN 204) initiëren, maar het tegenovergestelde is toegestaan:



Case Studie - FP1010. Overbrugging vs HW-switching + Overbrugging

Overweeg de volgende topologie:



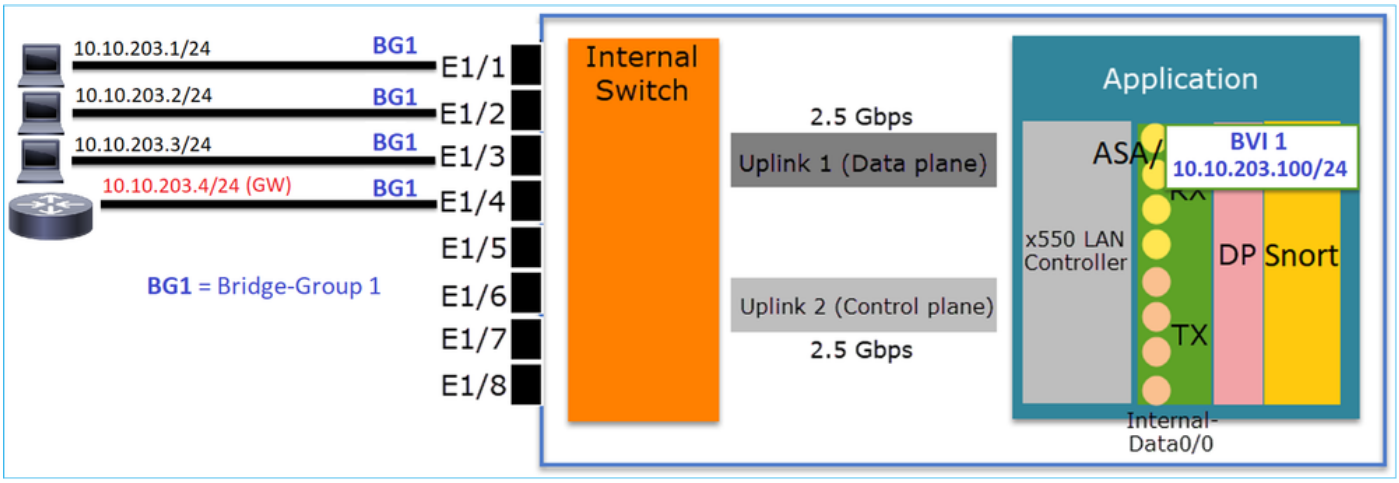
In deze topologie:

- Drie end-hosts behoren tot hetzelfde L3-net (10.10.203.x/24).
- De router (10.10.203.4) werkt als een GW in Subnet.

In deze topologie zijn er twee belangrijke ontwerpopties:

1. overbrugging
2. HW-switching + overbrugging

Ontwerpoptie 1. Overbrugging

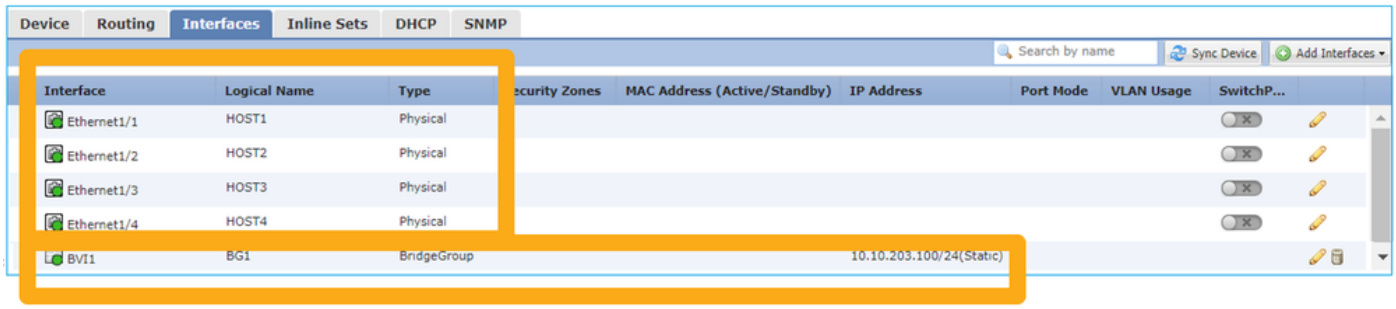


Belangrijkste punten

De belangrijkste punten van dit ontwerp zijn:

- Er is BVI 1 gemaakt met een IP in hetzelfde subnetwerk (10.10.203.x/24) als de 4 aangesloten apparaten.
- Alle vier havens behoren tot dezelfde Bridge-Group (in dit geval groep 1).
- Elk van de vier poorten heeft een naam ingesteld.
- Host-to-host en host-to-GW communicatie gaat door de toepassing (bv. FTD).

Vanuit het standpunt van FMC UI is de configuratie:

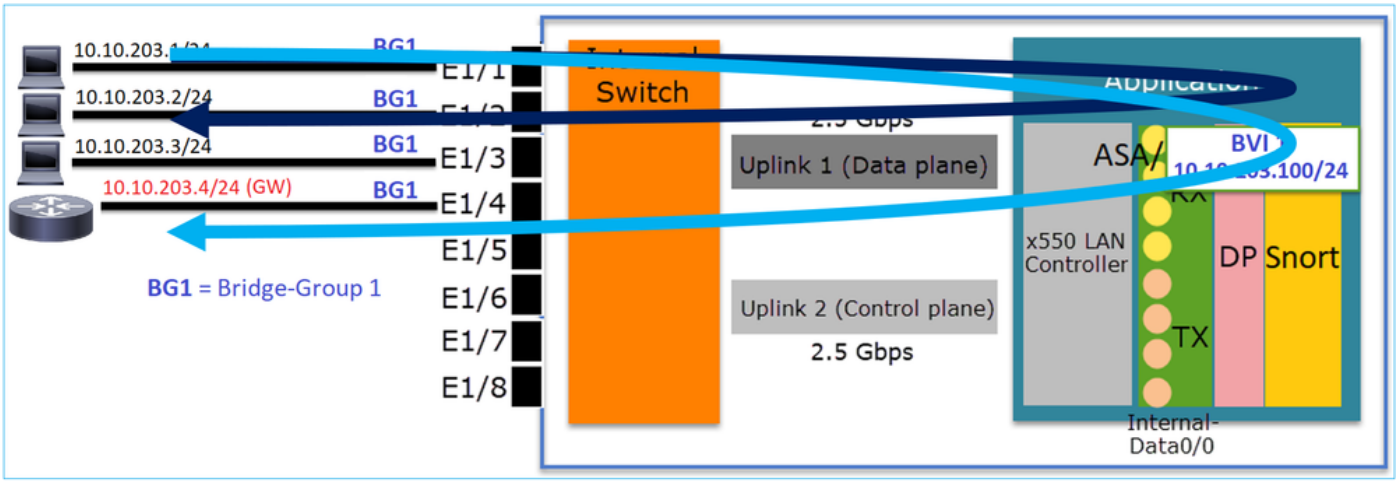


FTD-interfaceconfiguratie

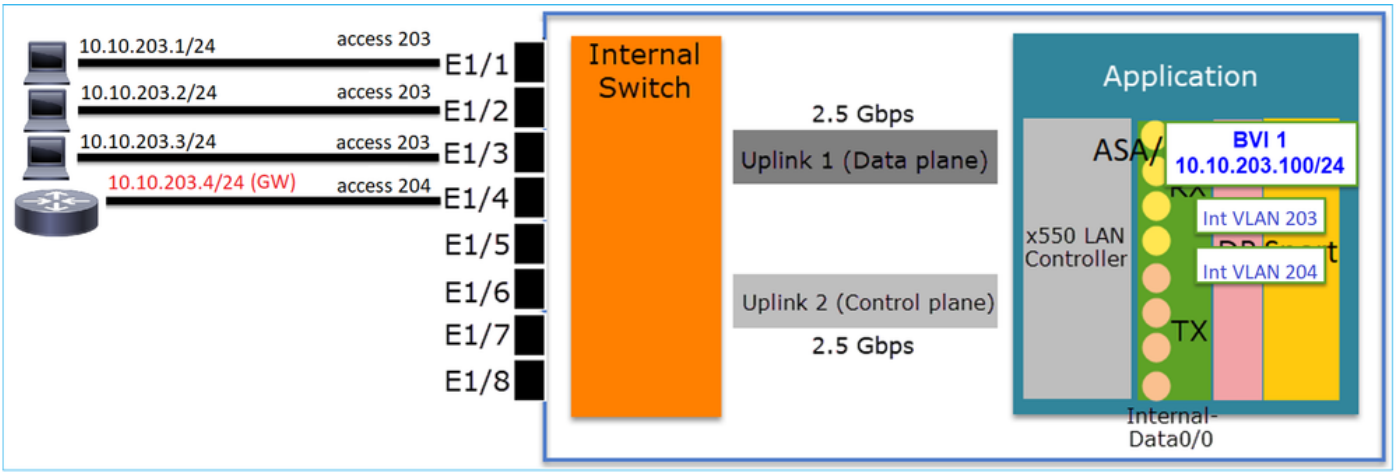
In dit geval is de configuratie:

```
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
```

De verkeersstroom in dit scenario:



Ontwerpoptie 2. W-switching + overbrugging

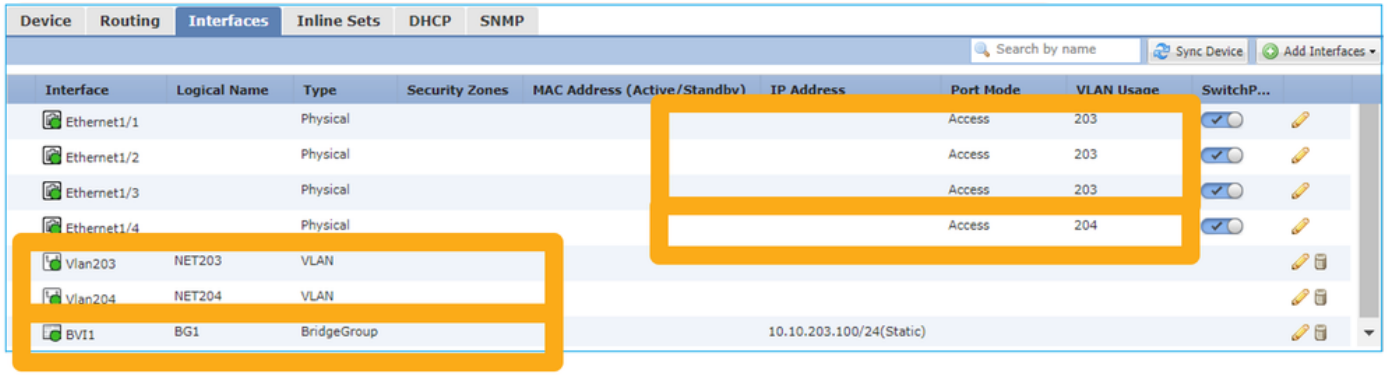


Belangrijkste punten

De belangrijkste punten van dit ontwerp zijn:

- Er is BVI 1 gemaakt met een IP in hetzelfde subnetwerk (10.10.203.x/24) als de 4 aangesloten apparaten.
- De poorten die aan de end-hosts zijn gekoppeld, worden geconfigureerd in SwitchPort-modus en behoren tot hetzelfde VLAN (203).
- De poort die aan de GW is aangesloten is ingesteld in SwitchPort-modus en behoort tot een ander VLAN (204).
- Er zijn 2 VLAN-interfaces (2003, 204). De 2 interfaces van VLAN hebben geen IP toegewezen en behoren tot Bridge-Group 1.
- Host-to-host communicatie gaat alleen door de interne switch.
- Host-to-GW-communicatie gaat door de toepassing (bijvoorbeeld FTD).

FMC UI-configuratie:

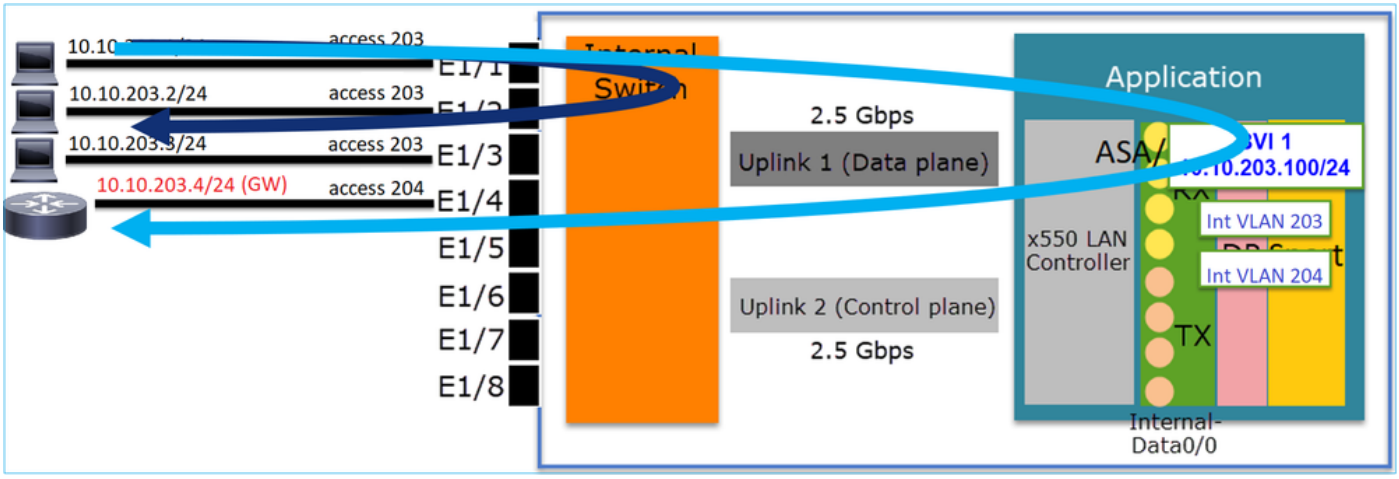


FTD-interfaceconfiguratie

In dit geval is de configuratie:

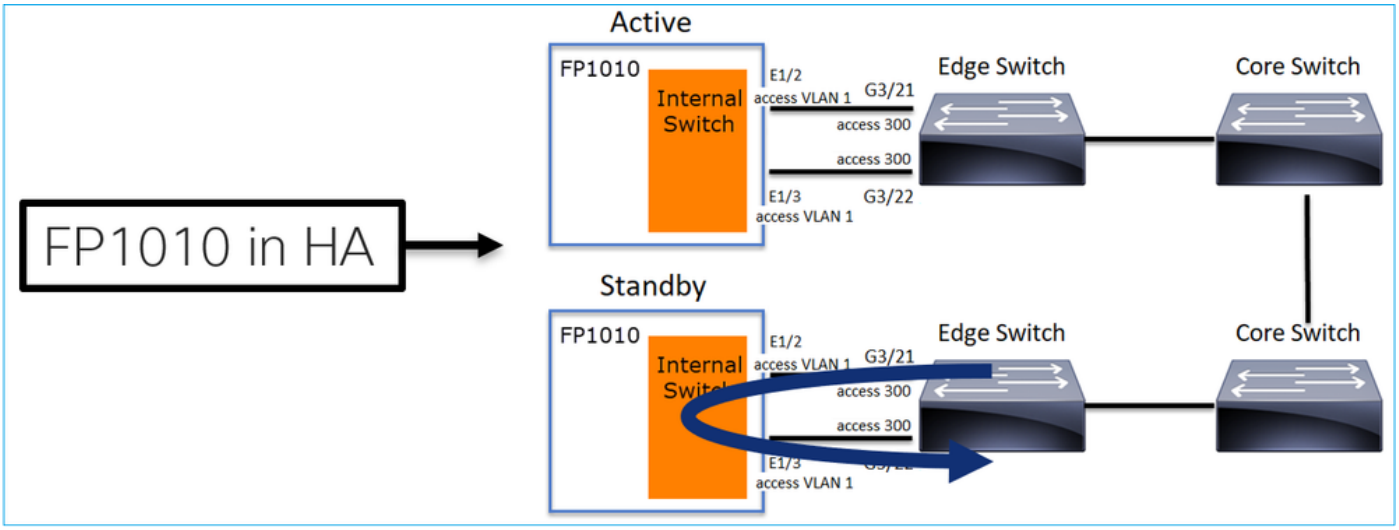
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1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

Host-to-host communicatie vs host-to-GW communicatie:



FP1010 Ontwerpoverwegingen

Switching en hoge beschikbaarheid (HA)

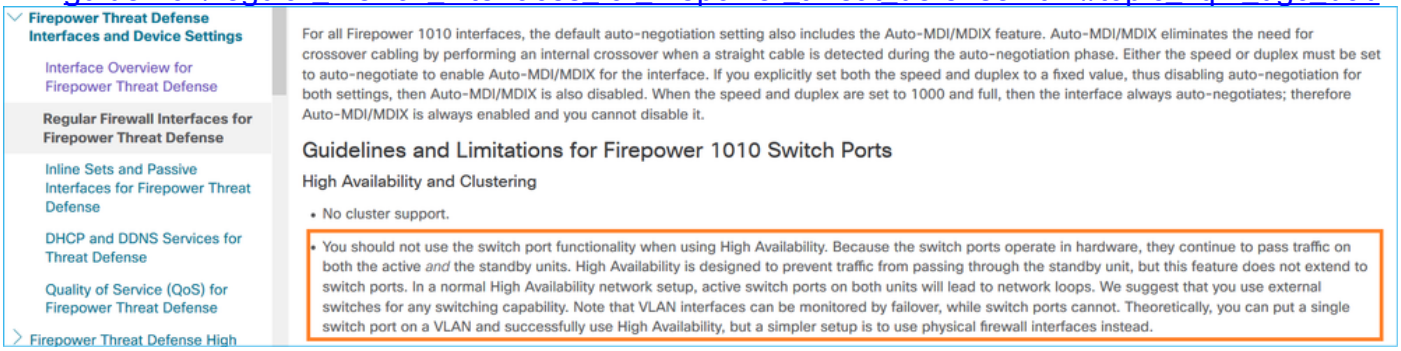


Er zijn twee belangrijke problemen wanneer HW Switching is ingesteld in een HA-omgeving:

1. HW-switching op de Standby-unit sturen pakketten door het apparaat door. Dit kan een netwerk veroorzaken.
2. Switch-poorten worden niet gecontroleerd door HA

Ontwerpvereisten

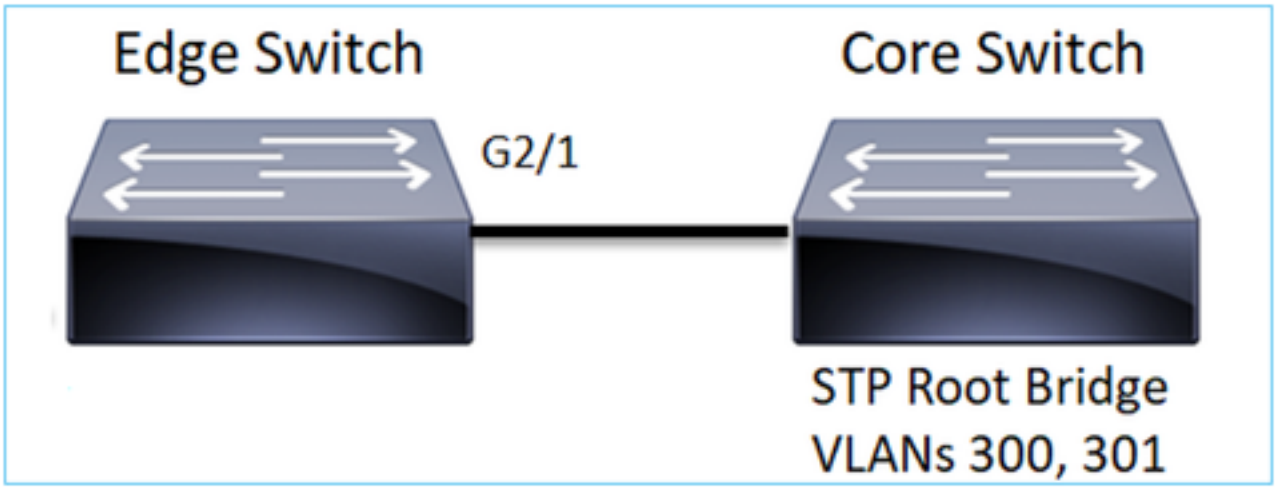
- U mag de SwitchPort-functie niet gebruiken met een hoge beschikbaarheid van ASA/FTD. Dit wordt gedocumenteerd in de configuratie van het FMC: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b



Interactie met Spanning Tree Protocol (STP)

De FP1010 interne switch voert geen STP uit.

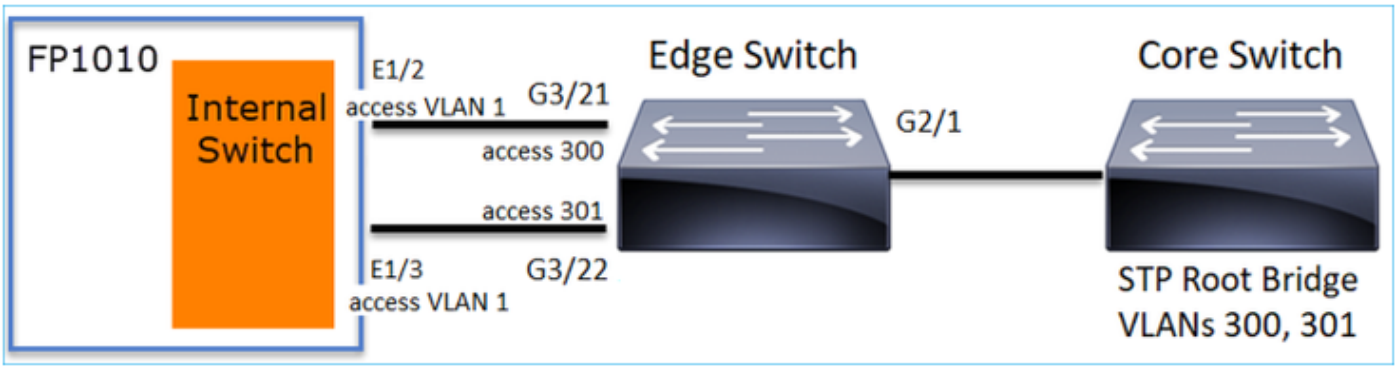
Neem dit scenario in overweging:



Op de Edge-Switch is de Root Port voor beide VLAN's 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
```

Sluit een FP1010 aan op de edge switch en bevestig beide poorten in hetzelfde VLAN (HW-switching):



Het probleem

- Als gevolg van het lekken van VLAN superieure BPDU's voor VLAN 301 die op G3/22 zijn ontvangen

```
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
```

> **Waarschuwing**: Als u een L2-switch aansluit op FP1010, kunt u het STP-domein beïnvloeden

Dit wordt ook gedocumenteerd in de configuratie-handleiding van het FMC:

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 API's

FMC REST API's

Dit zijn de REST API(s) voor deze functieondersteuning:

- L2 fysieke interface [Ondersteunde PUT/GET]

/api/fmc_fig/v1/domein/ {domeinUID}/apparaten/apparaten/ {containerUID}/fysieke interfaces/ {objectID}

- VLAN-interface [Ondersteunde POST/PUT/GET/DELETE]

/api/fmc_fig/v1/domein/ {domeinUID}/apparaten/apparaten/ {containerUID}/vlaninterfaces/ {objectID}

Problemen oplossen/diagnostiek

Overzicht van de diagnostiek

- Logbestanden worden opgenomen in een FTD/NGIPS-probleemoplossing of in de resultaten van de show-technologie. Dit zijn de items die moeten worden geraadpleegd voor meer informatie in het geval van een oplossing:
- /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-in werking stellen van de configuratie
- /mnt/disk0/log/asa-appagent.log

Verzamel gegevens van FXOS (apparaat) - CLI

In het geval van 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)#
```

In het geval van FTD (console):

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

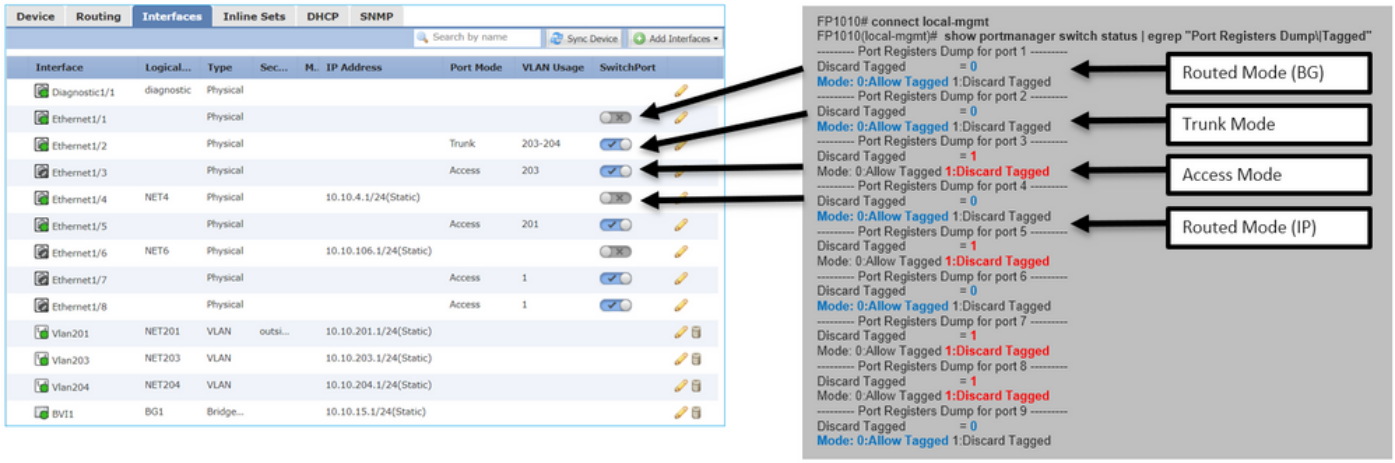
Ondersteuning van FP1010

Poortregisters definiëren alle interne switch- en poortfuncties.

In dit screenshot wordt het gedeelte "Port Control" van de havenregisters getoond en in het bijzonder het register dat voorschrijft wanneer het op de interface ontvangen getagde verkeer wordt getagd, moet worden weggegooid (1) of toegestaan (0). Hier is het volledige registratiegedeelte voor één poort:

```
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 dit screenshot kunt u de verschillende kadavers van de kaart voor de verschillende poortmodi zien:

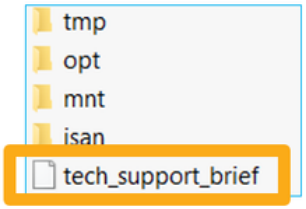


Verzamel FPRM-show technologie op FP1010

U kunt als volgt een FPRM-bundel genereren en het uploaden naar een FTP-server:

```
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
```

De FPRM bundel bevat een bestand dat tech_support_brief heet. Het tech_support_short bestand bevat een reeks showopdrachten. Eén daarvan is de **status van switch van showportmanager**:



Beperkingen in details, gemeenschappelijke problemen en problemen

Beperkingen van de implementatie voor 6.5 release

- Dynamische routingprotocollen worden niet ondersteund voor SVI-interfaces.
- Multi-context niet ondersteund op 1010.
- SVI VLAN-id bereik beperkt tot 1-4070.
- Poortkanaal voor L2 wordt niet ondersteund.
- L2 poort als een failover-link wordt niet ondersteund.

Limieten ten aanzien van de Switch

Functie	Beschrijving	Limiet
Aantal VLAN-interfaces	Totaal aantal VLAN-interfaces dat kan worden gemaakt	60
Trunkmodus VLAN	Maximum aantal VLAN's toegestaan op een poort in hoofdmodus Maps zonder tag	20
Native VLAN	Het bereiken op een haven aan inheems VLAN gevormd op de haven	1
Benoemde interfaces	Omvat alle genoemde interfaces (interface VLAN, subinterface, poortkanaal, fysieke interface enz)	60

Overige beperkingen

- Subinterfaces en interface VLAN kunnen niet hetzelfde VLAN gebruiken.
- Alle interfaces die aan BVI deelnemen, moeten tot dezelfde interfaceklasse behoren.
- Een BVI kan worden gemaakt met een combinatie van L3 mode-poorten en L3 mode-subinterfaces.
- Een BVI kan worden gemaakt met een combinatie van interface-VLAN's.
- Een BVI kan niet worden gemaakt door L3-modempoorten en interface-VLAN's te mengen.

Gerelateerde informatie

- Cisco Firepower 1010 security applicatie
- Configuratiehandleidingen