Switch L2 en FPR1010, arquitectura, verificación y resolución de problemas

Contenido

Introducción

Este documento describe el switch L2 en los dispositivos FP1010. Específicamente, cubre principalmente la parte de implementación de la plataforma de servicios de seguridad (SSP)/Firepower eXtensive Operation System (FXOS). En la versión 6.5, Firepower 1010 (modelo de escritorio) habilitó las capacidades de switching en el switch de hardware L2 integrado. Esto le ayuda a evitar switches de hardware adicionales y a reducir el coste.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

- FP1010 es un modelo de escritorio para pequeñas oficinas en casa (SOHO) que se sustituye por las plataformas ASA5505 y ASA5506-X.
- Compatibilidad con software para imágenes FTD (6.4+) gestionadas por Firepower Management Center (FMC), Firepower Device Manager (FDM) o Cloud Defense Orchestrator (CDO).
- Compatibilidad de software para imágenes ASA (9.13+) gestionadas por CSM, ASDM o CLI.
- El sistema operativo (OS), ASA o FTD, se incluye en FXOS (similar a FP21xx).
- 8 puertos de datos de 10/100/1000 Mbps.
- Los puertos E1/7, E1/8 admiten PoE+.
- El switch de hardware permite la comunicación de velocidad de línea entre los puertos (por ejemplo: una fuente de cámara en el servidor local).

Agregaciones de Firepower 6.5

- Introducción de un nuevo tipo de interfaz denominada Interfaz virtual conmutada (SVI).
- Modo mixto: Las interfaces se pueden configurar en modo conmutado (L2) o no conmutado (L3).
- Las interfaces de modo L3 reenvían todos los paquetes a la aplicación de seguridad.
- Los puertos de modo L2 pueden conmutar en hardware si dos puertos forman parte de la misma VLAN, lo que mejora el rendimiento y la latencia. Y los paquetes que deben enrutarse o puentearse alcanzan la aplicación de seguridad (por ejemplo: una cámara que descarga un nuevo firmware de Internet) y se somete a una inspección de seguridad según la configuración.
- La interfaz física L2 se puede asociar con una o varias interfaces SVI.
- Las interfaces de modo L2 pueden estar en modo de acceso o tronco.
- La interfaz L2 del modo de acceso permite solamente el tráfico sin etiquetas.
- La interfaz L2 del modo troncal permite el tráfico etiquetado.

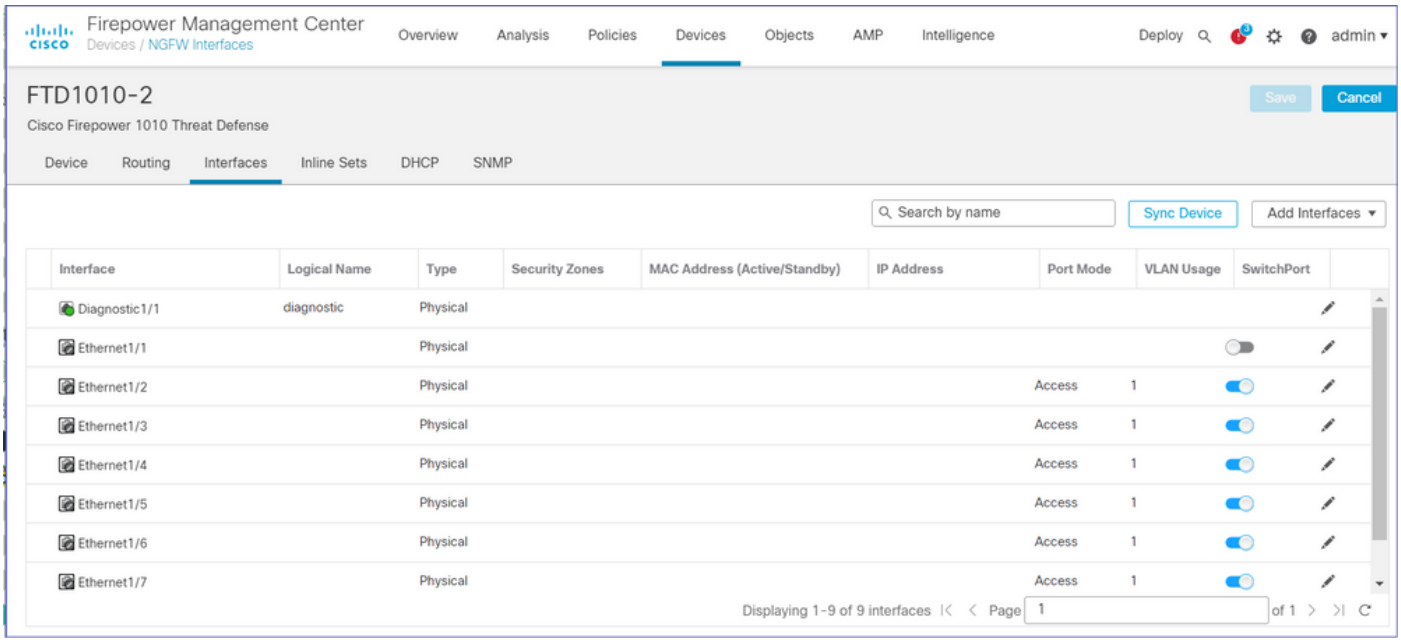
- Compatibilidad de VLAN nativa para la interfaz L2 del modo troncal.
- Las CLI de ASA, ASDM, CSM, FDM y FMC se han mejorado para admitir nuevas funciones.

Adiciones de FMC

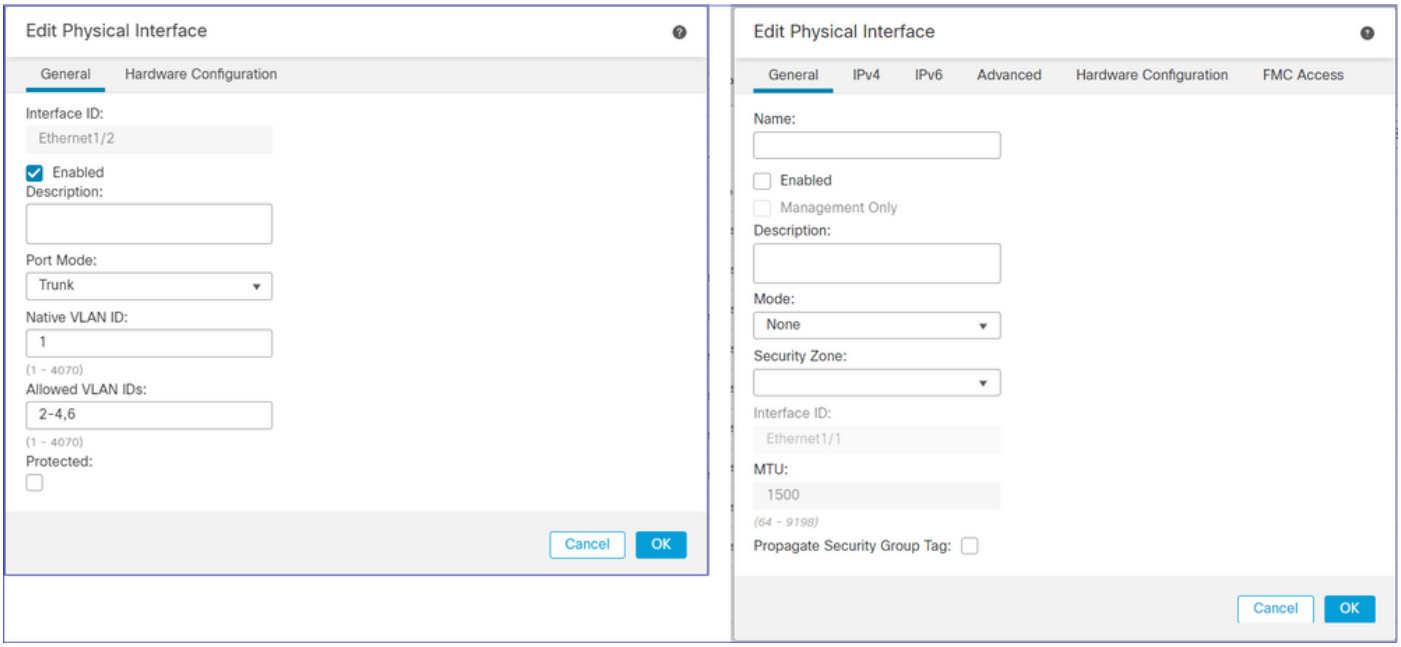
- Se ha introducido un nuevo modo de interfaz denominado switchport para una interfaz física que se utiliza para identificar si una interfaz física es una interfaz L3 o L2.
- La interfaz física L2 se puede asociar con una o varias interfaces VLAN basadas en el modo de acceso o tronco.
- Firepower 1010 admite la configuración de alimentación a través de Ethernet (PoE) en las dos últimas interfaces de datos, es decir, Ethernet1/7 y Ethernet1/8.
- El cambio de interfaz entre conmutado y no conmutado borra todas las configuraciones excepto la configuración de PoE y Hardware.

Cómo funciona

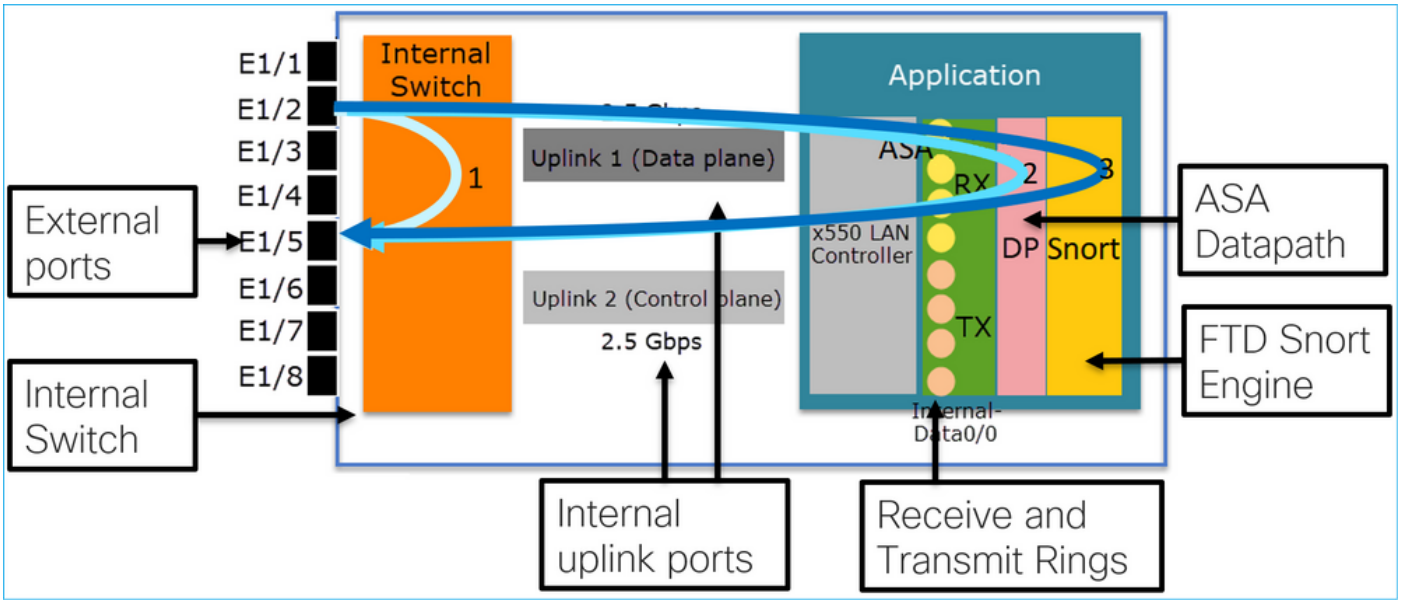
Esta función es sólo una mejora del soporte de interfaz existente en FMC (**Administración de dispositivos > Página de interfaz**).



Vista de interfaz física (L2 y L3)



Arquitectura FP1010



- 8 puertos de datos externos.
- 1 switch interno.
- 3 puertos de enlace ascendente (2 de ellos se muestran en la imagen), uno para el plano de datos, uno para el plano de control y otro para la configuración.
- x550 LAN Controller (la interfaz entre la aplicación y los enlaces ascendentes).
- 4 anillos de recepción (RX) y 4 de transmisión (TX).
- Proceso Datapath (en ASA y FTD).
- Proceso Snort (en FTD).

Procesamiento de paquetes

Dos factores principales pueden afectar al procesamiento de paquetes:

1. Modo de interfaz/puerto

2. Política aplicada

Un paquete puede atravesar un FP1010 de 3 maneras diferentes:

1. Sólo procesado por el switch interno

2. Reenviado hasta la aplicación (ASA/FTD) y procesado únicamente por el proceso de datapath

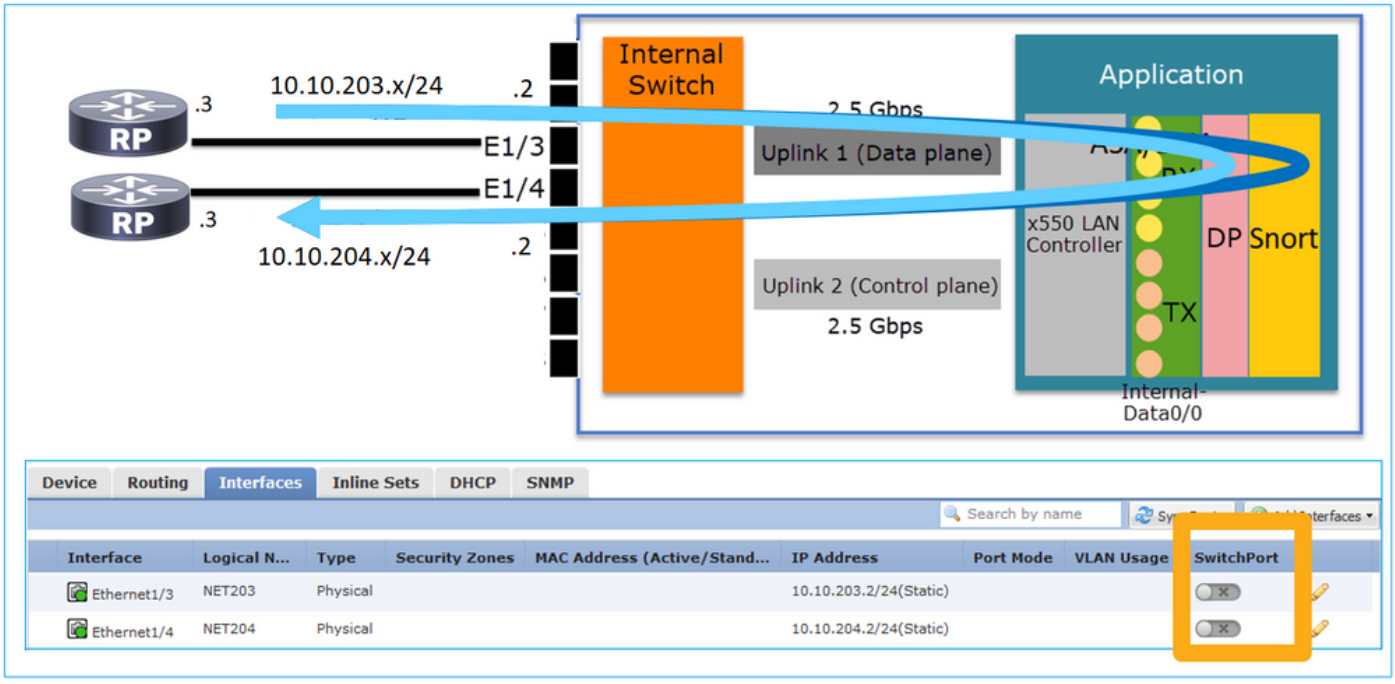
3. Reenviado hasta la aplicación (FTD) y procesado por el motor de datapath y Snort

Modos de puerto FP1010

Los ejemplos de interfaz de usuario son para FMC, los ejemplos de CLI son para FTD. La mayoría de los conceptos también se aplican completamente a un ASA.

FP1010 Caso 1. Puertos enrutados (routing IP)

Configuración y funcionamiento



Puntos clave

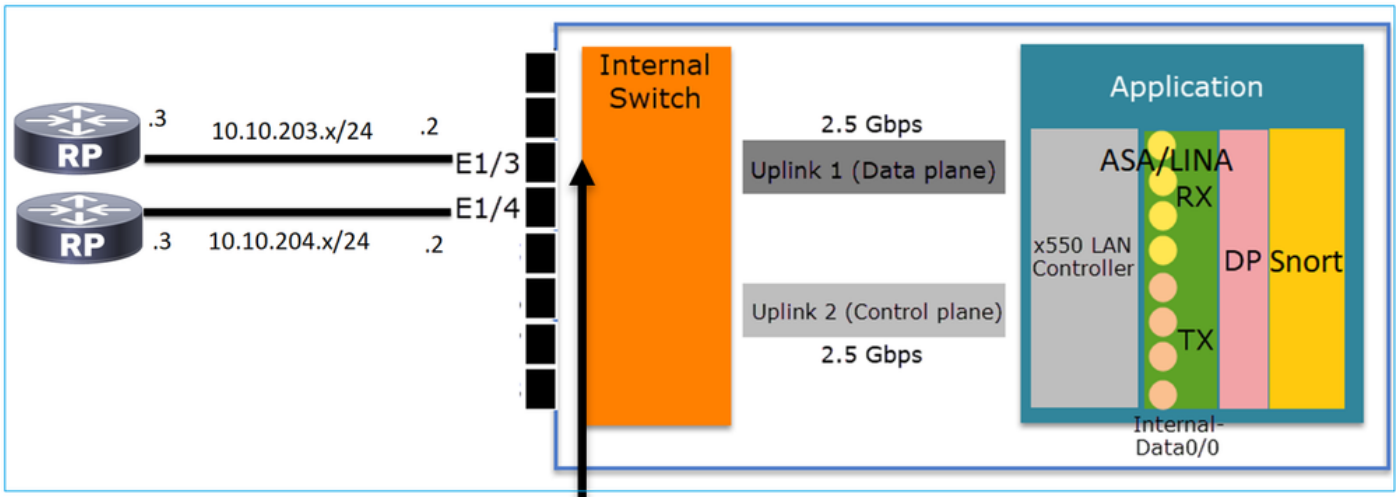
- Desde el punto de vista del diseño, los 2 puertos pertenecen a 2 subredes L2 diferentes.
- Cuando los puertos se configuran en modo ruteado, la aplicación (ASA o FTD) procesa los paquetes.
- En el caso de FTD, basado en la acción de regla (por ejemplo, PERMITIR), el motor Snort puede incluso inspeccionar los paquetes.

configuración de interfaz FTD

```
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
```

Verificación de puerto enrutado FP1010



Desde FXOS CLI puede verificar los contadores de interfaz física. Este ejemplo muestra los contadores de unidifusión de entrada y salida en el puerto E1/3:

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

Se pueden aplicar capturas de datapath de FTD y se pueden rastrear los paquetes:

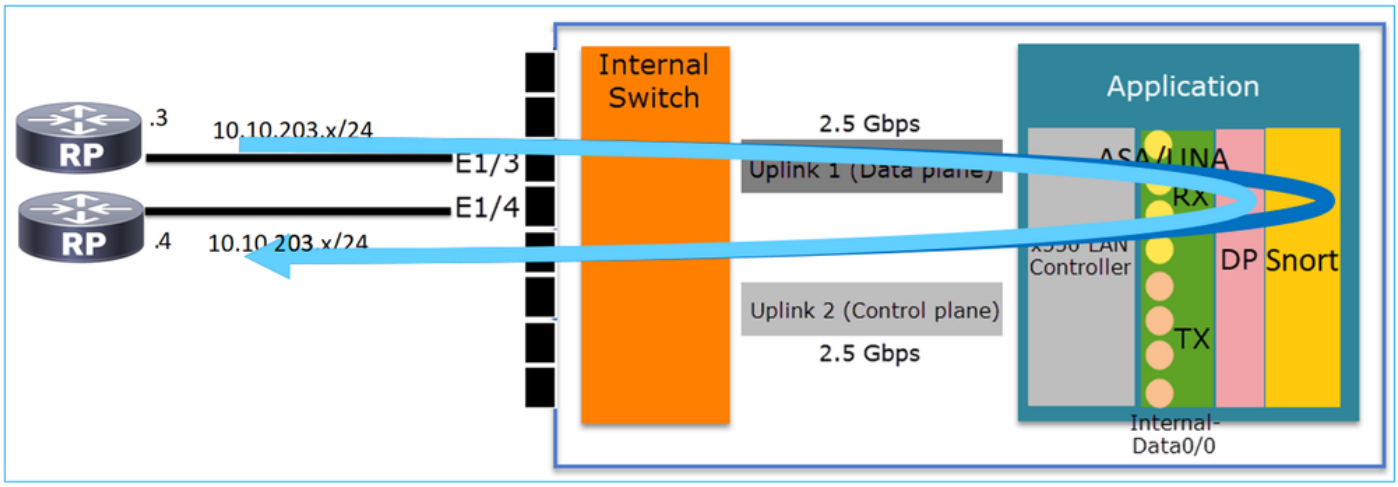
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

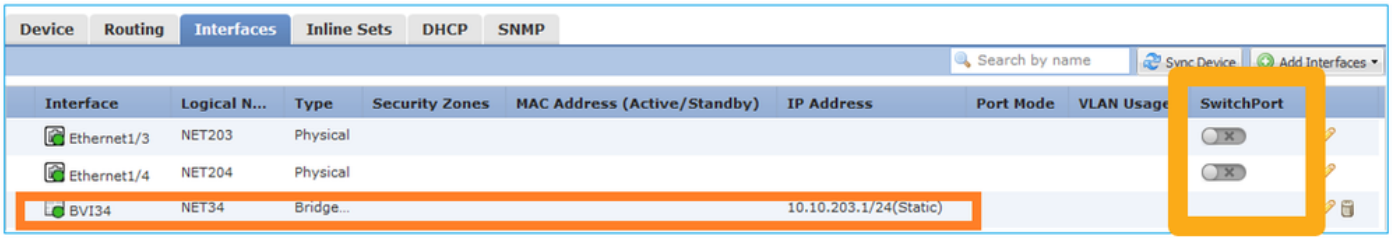
Este es un fragmento de captura. Como se esperaba, el paquete se reenvía en función de una BÚSQUEDA DE RUTAS:

```
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 Caso 2. Modo Bridge-Group (Bridging)

Configuración y funcionamiento





Puntos clave

- Desde el punto de vista del diseño, los 2 puertos están conectados a la misma subred L3 (similar a un firewall transparente), pero VLAN diferentes.
- Cuando los puertos se configuran en modo de puente, la aplicación (ASA o FTD) procesa los paquetes.
- En el caso de FTD, basado en la acción de regla (por ejemplo, PERMITIR), el motor Snort puede incluso inspeccionar los paquetes.

configuración de interfaz FTD

```
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
```

Verificación del puerto del grupo de puentes FP1010

Este comando muestra los miembros de la interfaz de 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
```

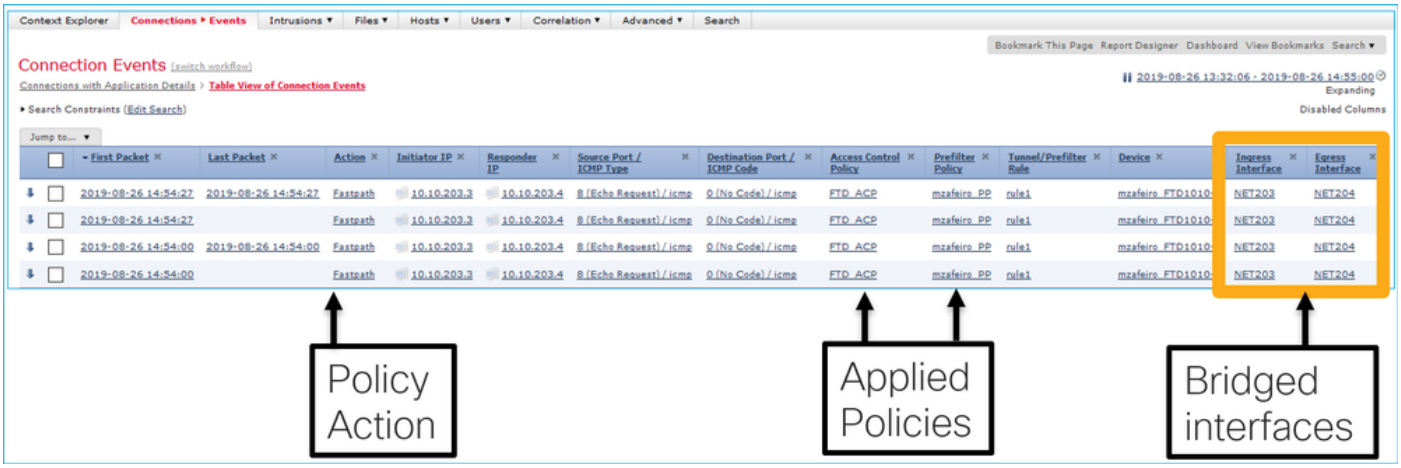
Este comando muestra la tabla de Memoria direccionable de contenido (CAM) de la ruta de datos ASA/FTD:

```
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
```

Un fragmento de seguimiento de paquetes muestra que el paquete se reenvía en función de la búsqueda de destino MAC L2:

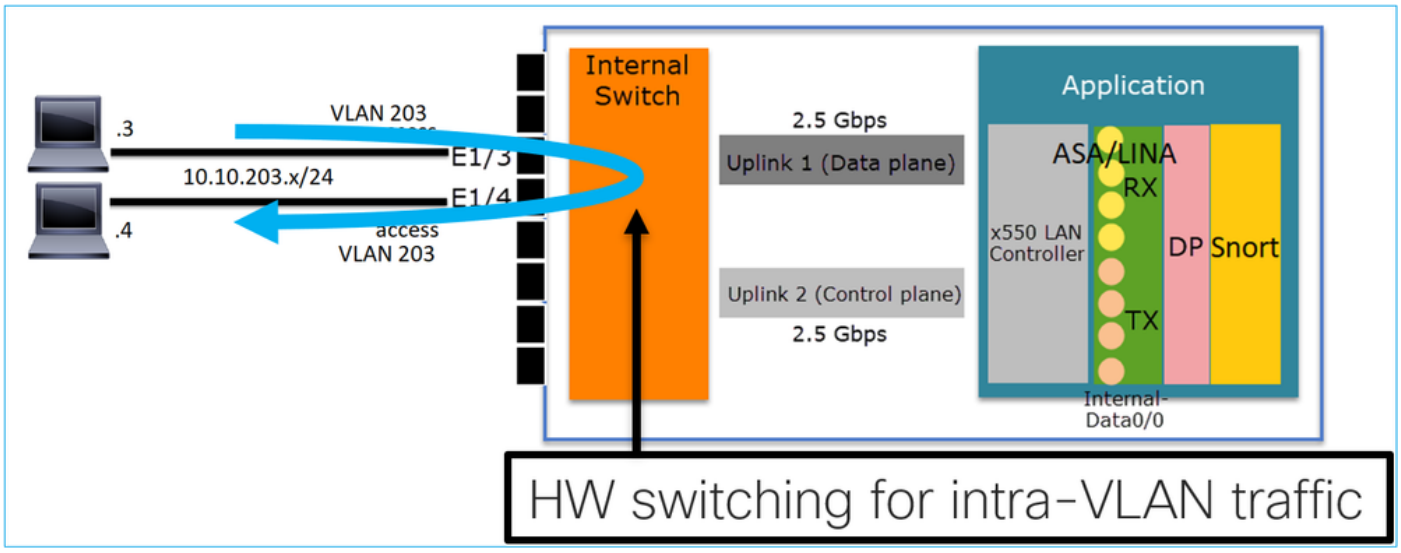
```
FP1010# show cap CAP203 packet-number 1 trace

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
```

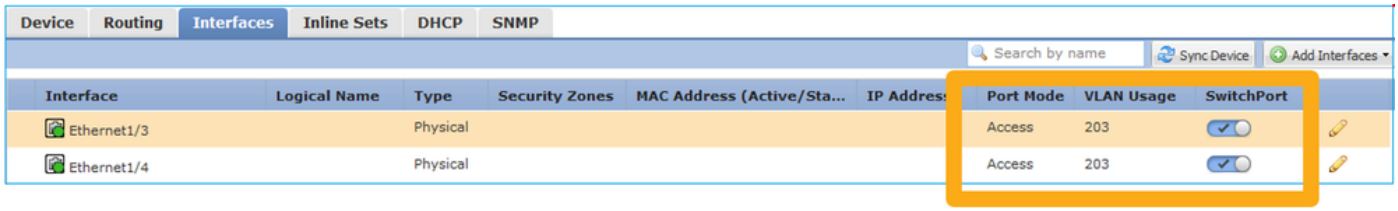
En el caso de FTD, los eventos de conexión FMC también pueden proporcionar información sobre la inspección de flujo y las interfaces de grupo de puente de tránsito:



FP1010 Caso 3. Puertos de switch (HW switching) en modo de acceso

Configuración y funcionamiento





Puntos clave

- HW Switching es una función FTD **6.5+** y ASA **9.13+**.
- Desde el punto de vista del diseño, los 2 puertos están conectados a la misma subred L3 y a la misma VLAN.
- Los puertos en esta situación funcionan en modo de acceso (sólo tráfico sin etiquetas).
- Los puertos de firewall configurados en el modo SwitchPort no tienen un nombre lógico (nameif) configurado.
- Cuando los puertos se configuran en modo Switching y pertenecen a la misma VLAN (tráfico dentro de VLAN), los paquetes son procesados solamente por el switch interno FP1010.

configuración de interfaz FTD

Desde un punto de vista de CLI, la configuración se parece mucho a un switch L2:

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

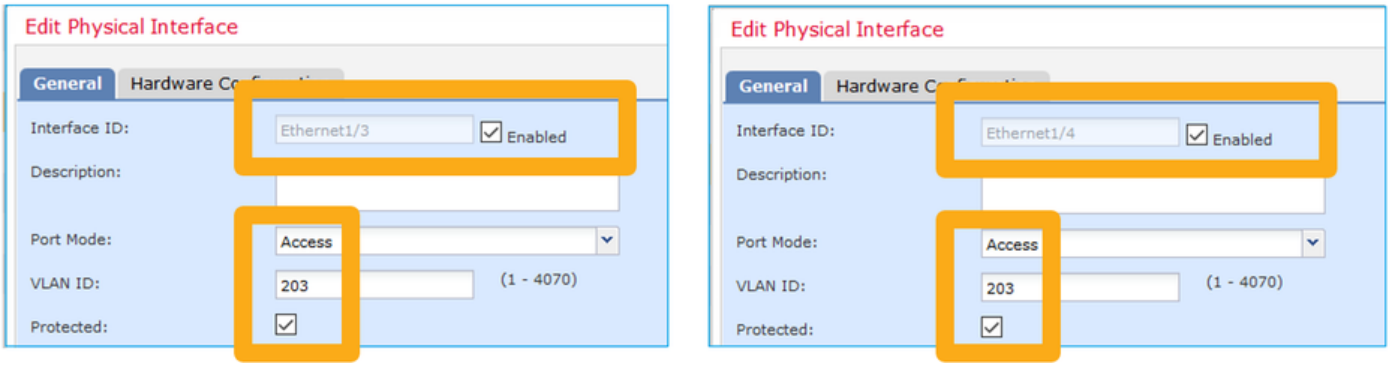
Filtrado del Tráfico Intra-VLAN

El reto: **Una ACL no puede filtrar el tráfico dentro de VLAN.**

La solución: Puertos **protegidos**

El principio es muy simple: 2 puertos configurados como protegidos no pueden comunicarse entre sí.

Interfaz de usuario de FMC en caso de puertos protegidos:



configuración de interfaz FTD

El comando **switchport protected** se configura bajo la interfaz:

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

Verificación de puerto de switch FP1010

En este ejemplo, hay 1000 paquetes unicast (ICMP) enviados con un tamaño específico (1100 bytes):

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

Para verificar los contadores de unicast de ingreso y egreso de las interfaces de tránsito, utilice este comando:

```
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
```

Este comando muestra el estado de VLAN del switch interno:

```
FP1010# show switch vlan
```

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

El estado de una VLAN es ACTIVO siempre y cuando se asigne al menos un puerto a la VLAN

Si un puerto está administrativamente inactivo o el puerto del switch conectado está inactivo/el cable desconectado y éste es el único puerto asignado a la VLAN, el estado de la VLAN también está inactivo:

```
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
```

Este comando muestra la tabla CAM del switch interno:

```
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
```

El tiempo de envejecimiento predeterminado de la tabla CAM del switch interno es de 5min 30 s.

FP1010 contiene 2 tablas CAM:

1. Tabla CAM del switch interno: Se utiliza en caso de switching de hardware
2. Tabla CAM de ruta de datos ASA/FTD: Se utiliza en caso de conexión en puente

Cada paquete/trama que atraviesa el FP1010 es procesado por una única tabla CAM (switch interno o datapath FTD) basada en el modo de puerto.

> **Precaución:** No confunda la tabla **show switch mac-address-table** interna CAM del switch utilizada en el modo SwitchPort con la tabla **show mac-address-table** FTD datapath CAM utilizada en el modo puenteado

Switching de hardware: Aspectos adicionales que deben tenerse en cuenta

Los registros de la ruta de datos ASA/FTD no muestran información sobre los flujos conmutados por HW:

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

La tabla de conexión de la ruta de datos ASA/FTD no muestra los flujos conmutados por HW:

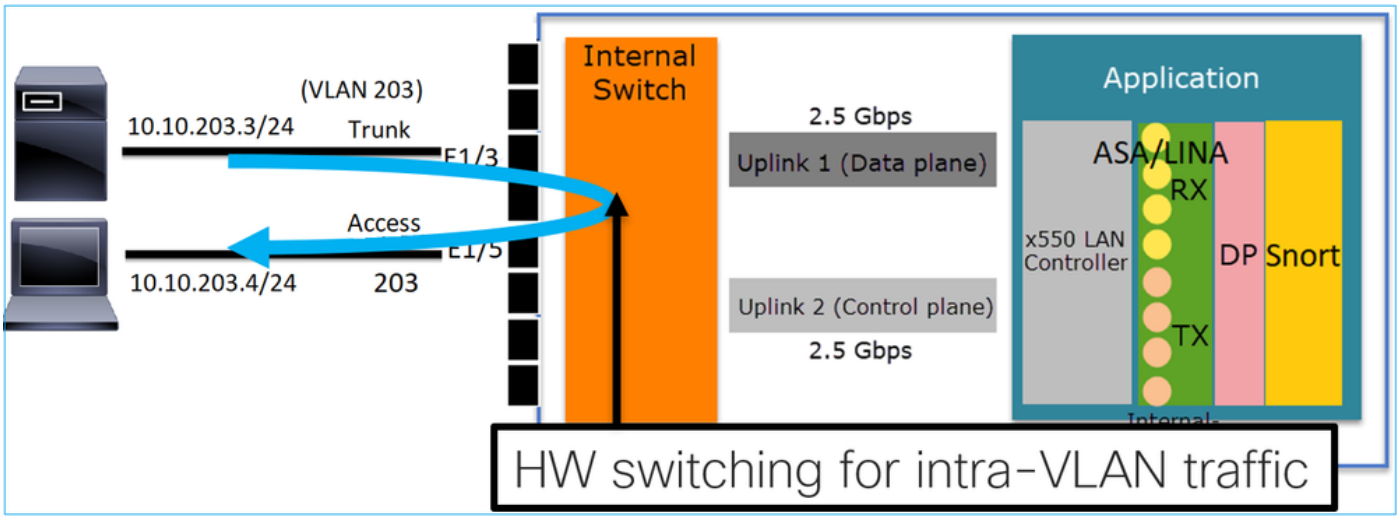
```
FP1010# show conn
0 in use, 3 most used
Inspect Snort:
```

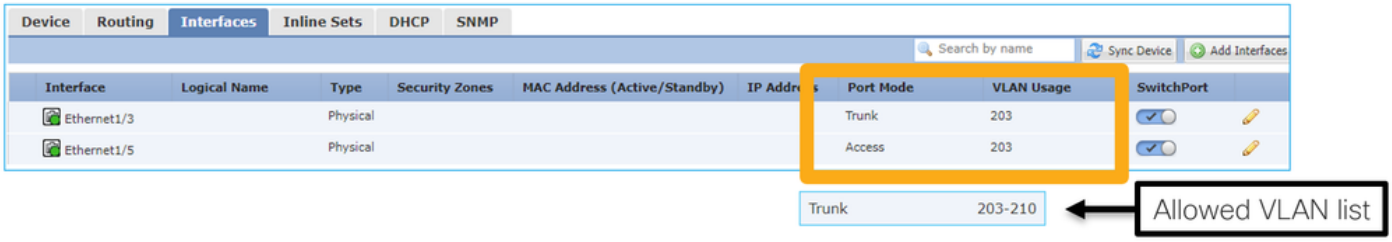
```
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

Además, los eventos de conexión FMC no muestran los flujos conmutados por HW.

FP1010 Caso 4. Puertos de switch (enlace troncal)

Configuración y funcionamiento





Puntos clave

- HW Switching es una función FTD **6.5+** y ASA **9.13+**.
- Desde el punto de vista del diseño, los 2 puertos están conectados a la misma subred L3 y a la misma VLAN.
- El puerto troncal acepta tramas etiquetadas y sin etiquetar (en el caso de una VLAN nativa).
- Cuando los puertos se configuran en modo de switching y pertenecen a la misma VLAN (tráfico dentro de VLAN), los paquetes son procesados solamente por el switch interno.

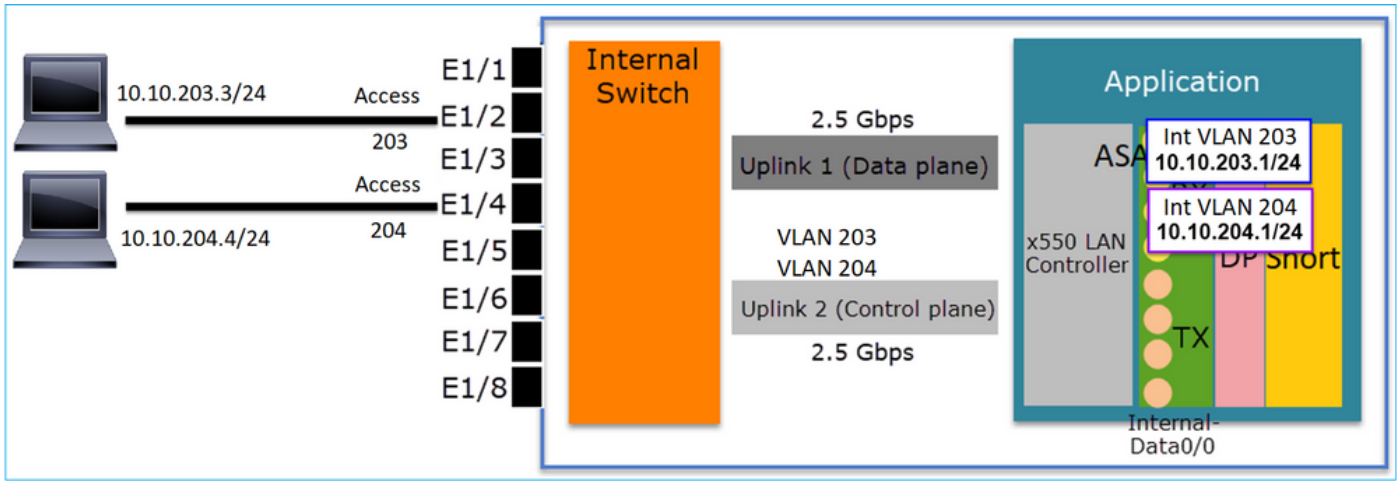
configuración de interfaz FTD

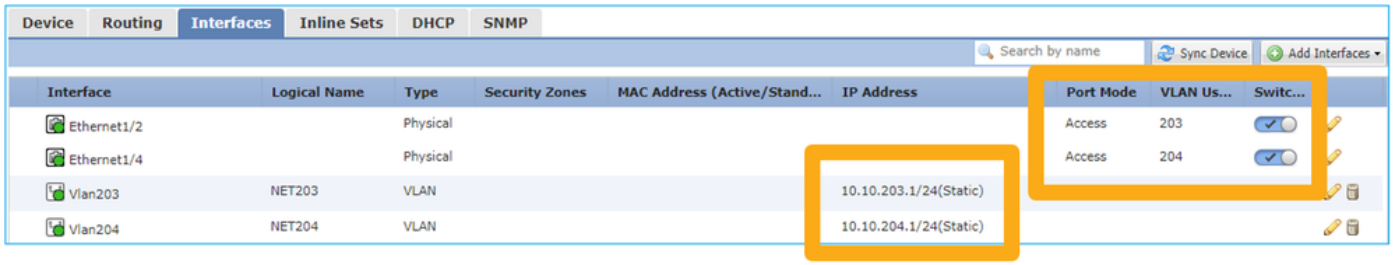
La configuración es similar a un puerto de switch de capa 2:

```
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
```

FP1010, caso 5. Puertos de switch (Inter-VLAN)

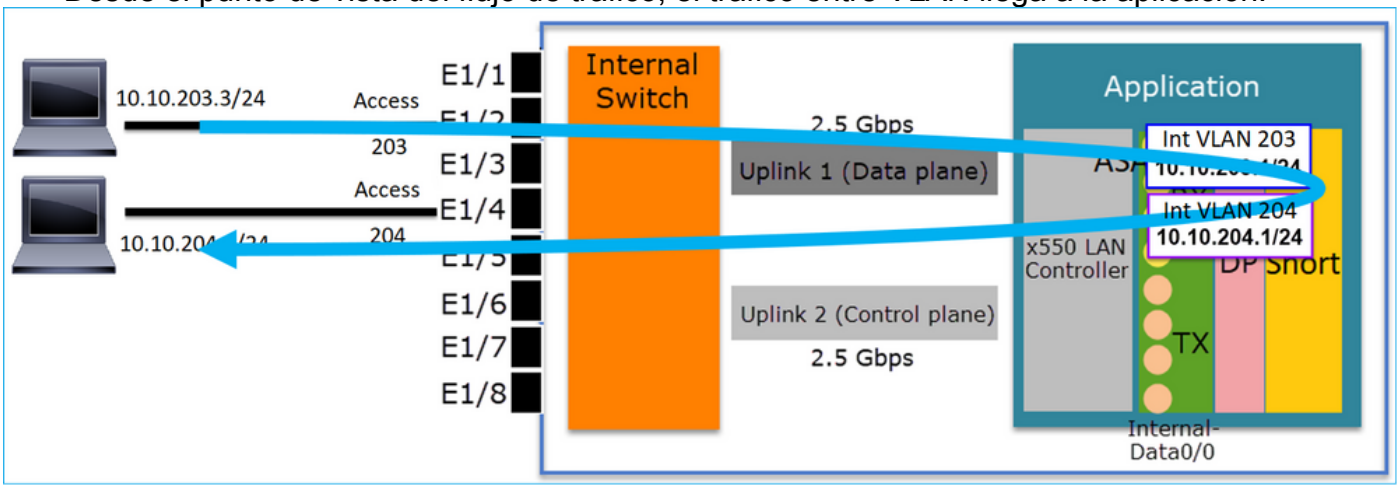
Configuración y funcionamiento





Puntos clave

- Desde el punto de vista del diseño, los 2 puertos están conectados a 2 subredes L3 diferentes y 2 VLAN diferentes.
- El tráfico entre las VLAN pasa a través de las interfaces VLAN (similares a las SVI).
- Desde el punto de vista del flujo de tráfico, el tráfico entre VLAN llega a la aplicación.



configuración de interfaz FTD

La configuración es similar a una interfaz virtual de switch (SVI):

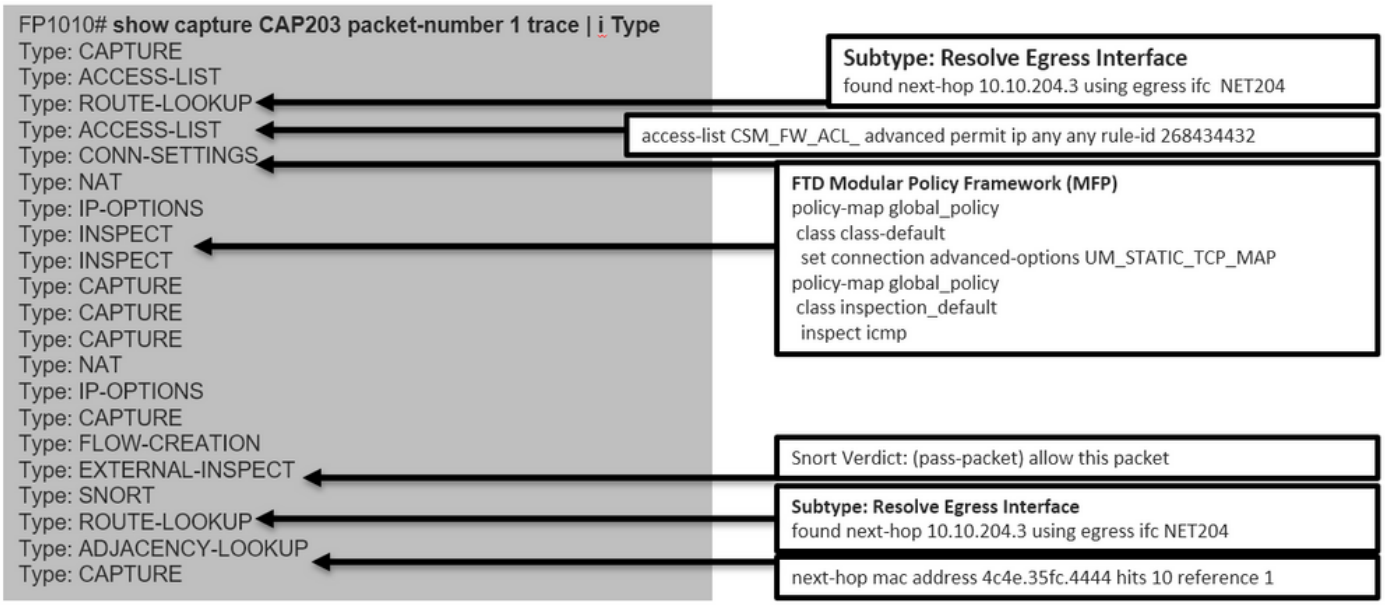
```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

Procesamiento de paquetes para tráfico entre VLAN

Este es un seguimiento de un paquete que atraviesa 2 VLAN diferentes:

```
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
```

Las fases principales del proceso de paquetes:



FP1010 Caso 6. Filtro entre VLAN

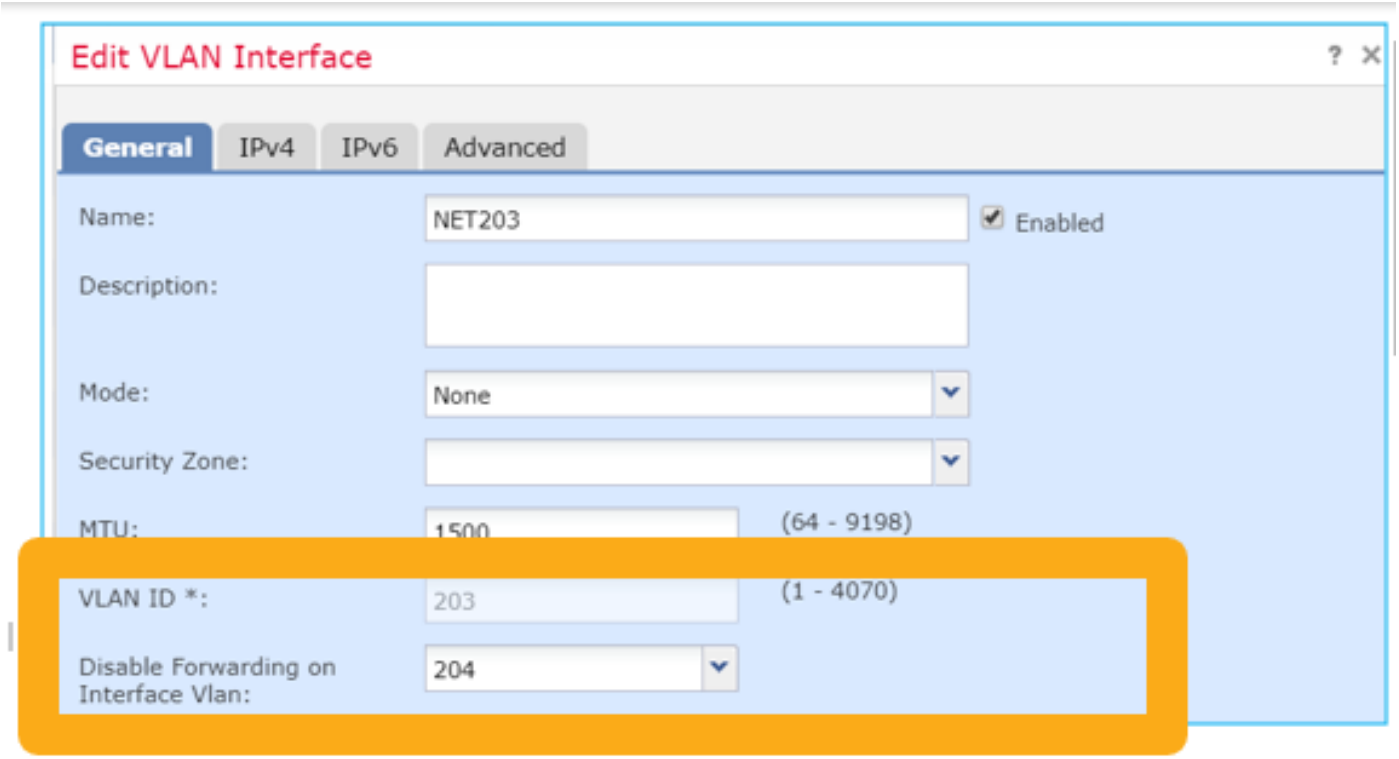
Configuración y funcionamiento

Hay dos opciones principales para filtrar el tráfico entre VLAN:

1. Política de control de acceso
2. comando **"no forward"**

Filtrar el tráfico entre VLAN con el uso del comando 'no forward'

Configuración de la interfaz de usuario de FMC:



Puntos clave

- La caída sin reenvío es unidireccional.
- No se puede aplicar a ambas interfaces VLAN.
- La verificación sin reenvío se realiza antes de la verificación ACL.

configuración de interfaz FTD

La configuración CLI en este caso es:

```
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
```

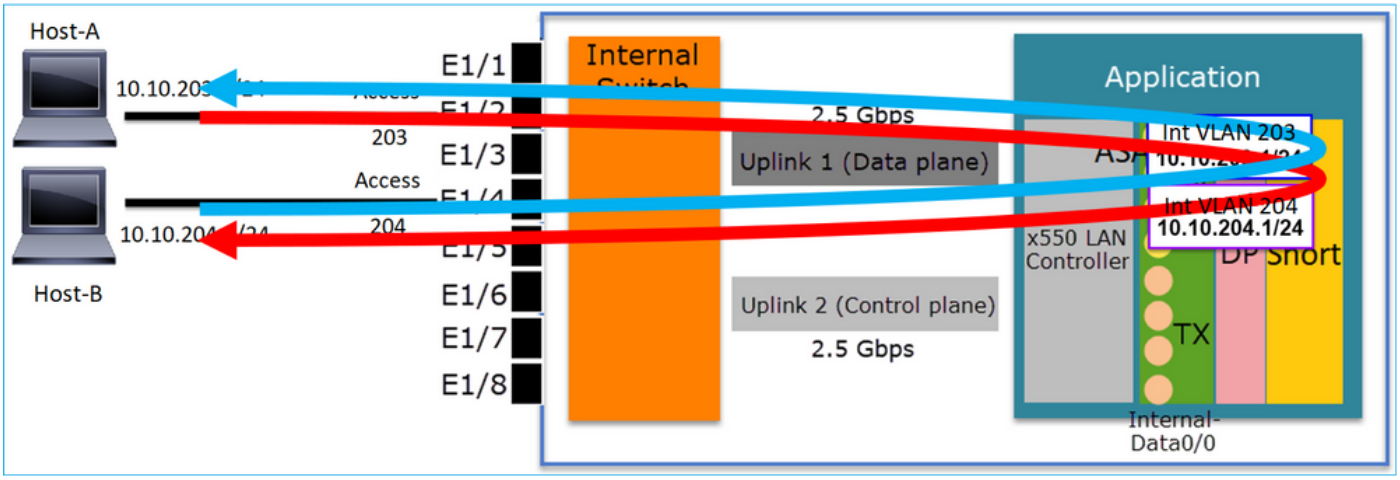
Si una función de no reenvío descarta un paquete, se genera un mensaje de Syslog de datos ASA/FTD:

```
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)
```

Desde el punto de vista de destino de la ruta de seguridad acelerada (ASP), se considera una caída de ACL:

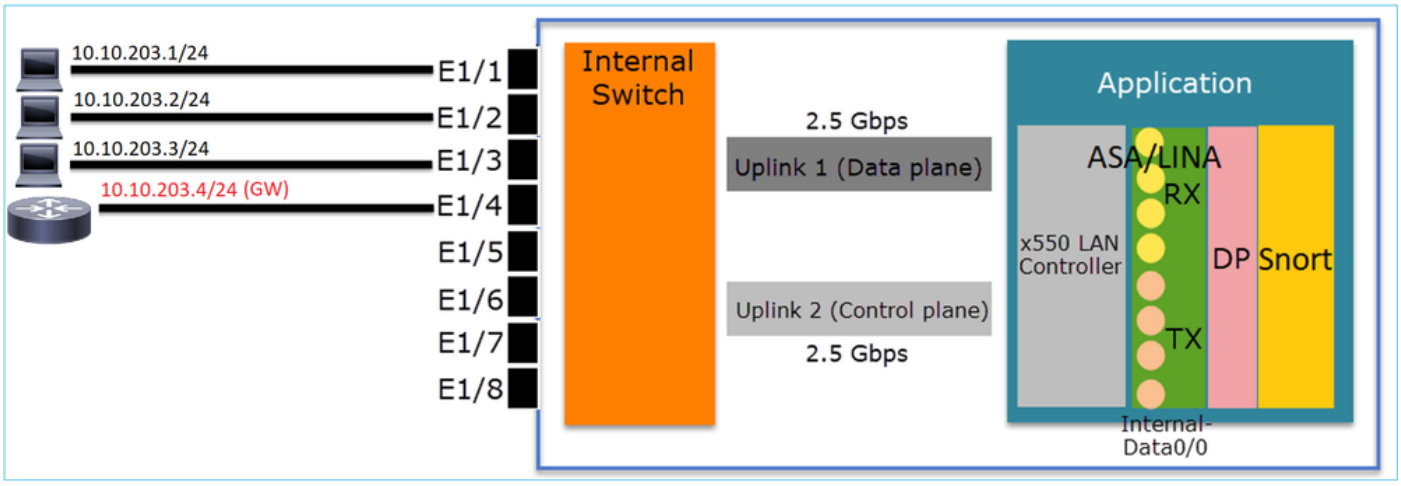
```
FP1010-2# show asp drop
Frame drop:
Flow is denied by configured rule (acl-drop) 1
```

Dado que la caída es unidireccional, el Host-A (VLAN 203) no puede iniciar el tráfico al Host-B (VLAN 204), pero se permite lo contrario:



Caso práctico: FP1010. Bridging vs HW Switching + Bridging

Tenga en cuenta la siguiente topología:



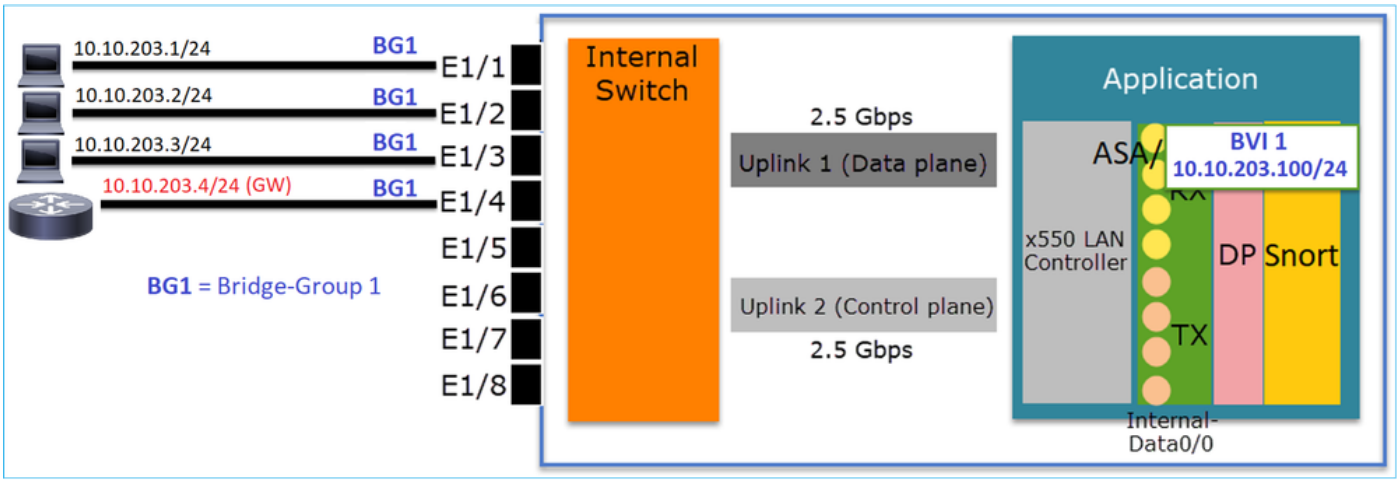
En esta topología:

- Tres hosts finales pertenecen a la misma subred L3 (10.10.203.x/24).
- El router (10.10.203.4) actúa como GW en la subred.

En esta topología hay dos opciones de diseño principales:

1. Conexión en puente
2. HW Switching + Bridging

Opción de diseño 1. Conexión en puente

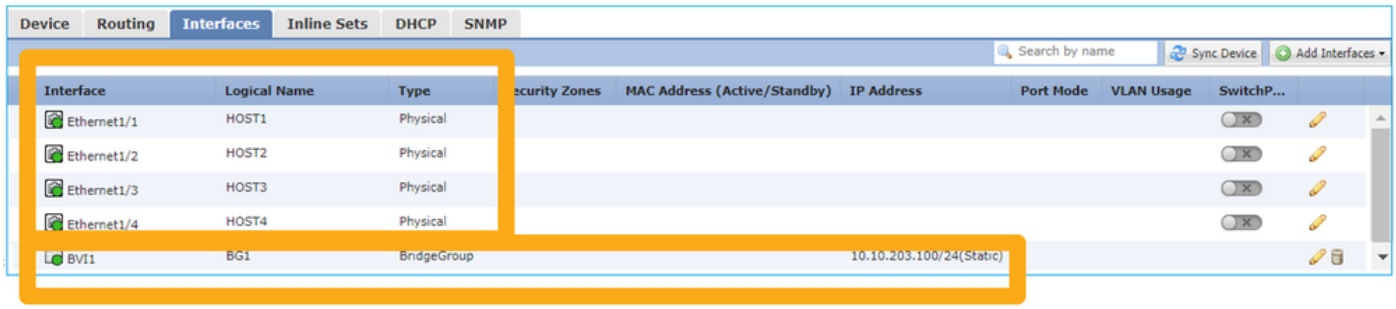


Puntos clave

Los principales puntos de este diseño son:

- Hay BVI 1 creado con una IP en la misma subred (10.10.203.x/24) que los 4 dispositivos conectados.
- Los cuatro puertos pertenecen al mismo grupo de puente (grupo 1 en este caso).
- Cada uno de los cuatro puertos tiene un nombre configurado.
- La comunicación de host a host y de host a GW pasa por la aplicación (por ejemplo, FTD).

Desde el punto de vista de la interfaz de usuario de FMC, la configuración es:

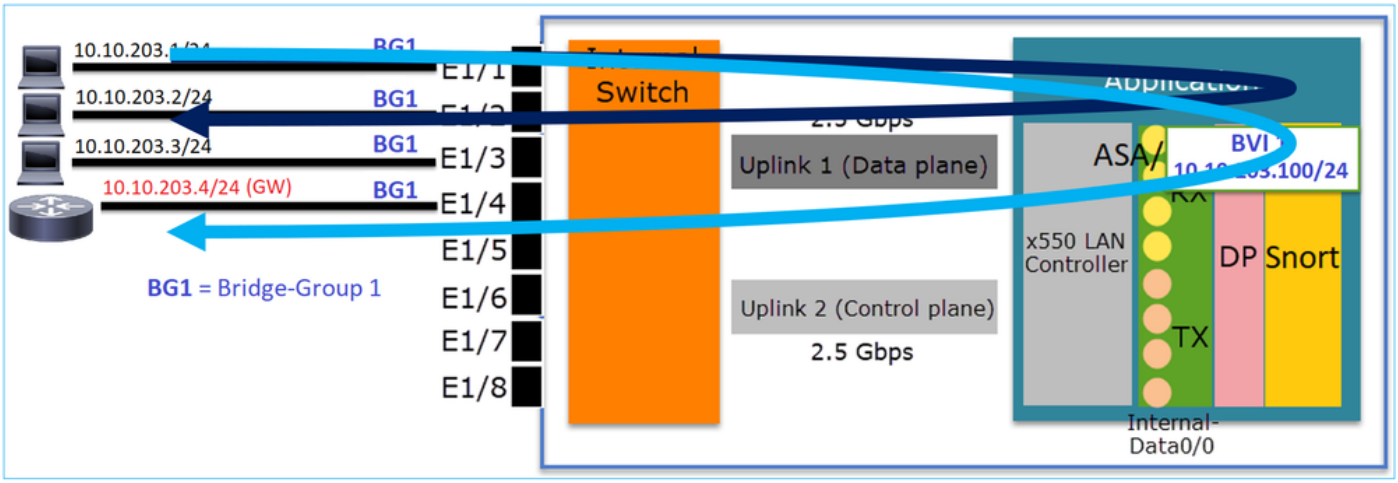


configuración de interfaz FTD

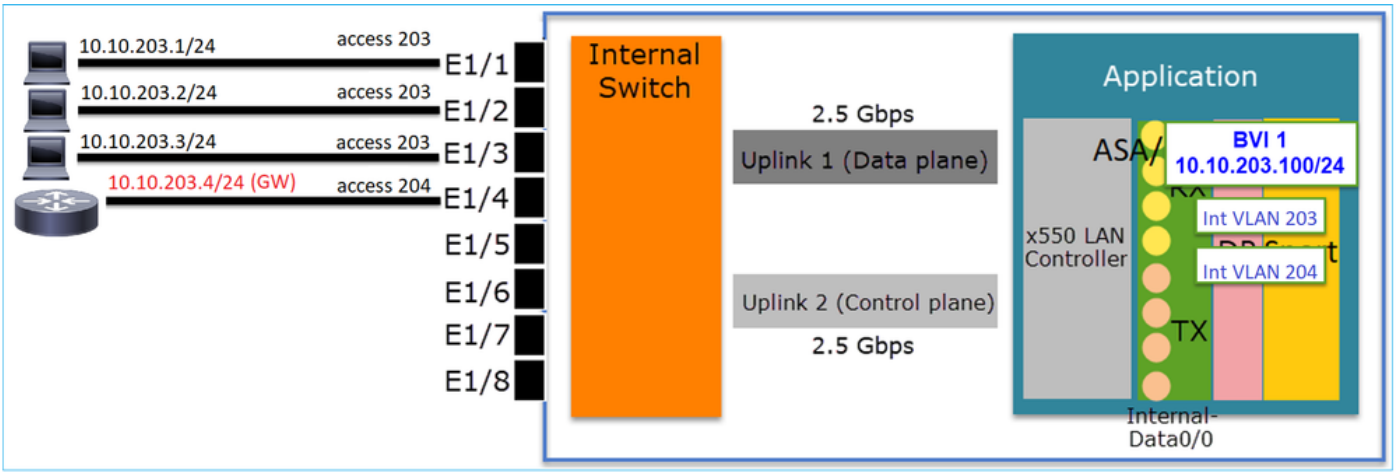
La configuración en este caso es:

```
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
```

El flujo de tráfico en este escenario:



Opción de diseño 2. HW Switching + Bridging

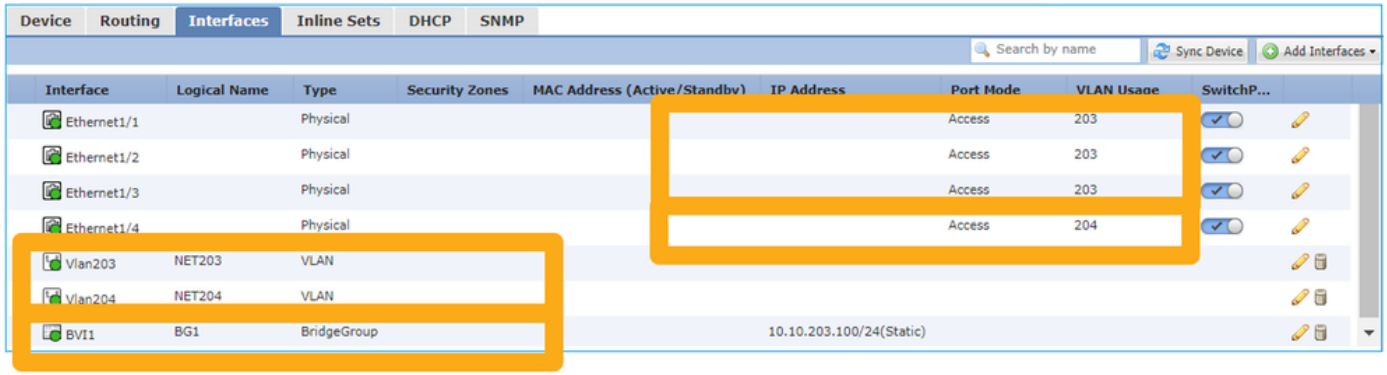


Puntos clave

Los principales puntos de este diseño son:

- Hay BVI 1 creado con una IP en la misma subred (10.10.203.x/24) que los 4 dispositivos conectados.
- Los puertos conectados a los hosts extremos se configuran en modo SwitchPort y pertenecen a la misma VLAN (203).
- El puerto conectado al GW se configura en modo SwitchPort y pertenece a una VLAN diferente (204).
- Hay 2 interfaces VLAN (203, 204). Las 2 interfaces VLAN no tienen una IP asignada y pertenecen al Grupo de Bridge 1.
- La comunicación de host a host sólo pasa por el switch interno.
- La comunicación de host a GW pasa por la aplicación (por ejemplo, FTD).

Configuración de la interfaz de usuario de FMC:

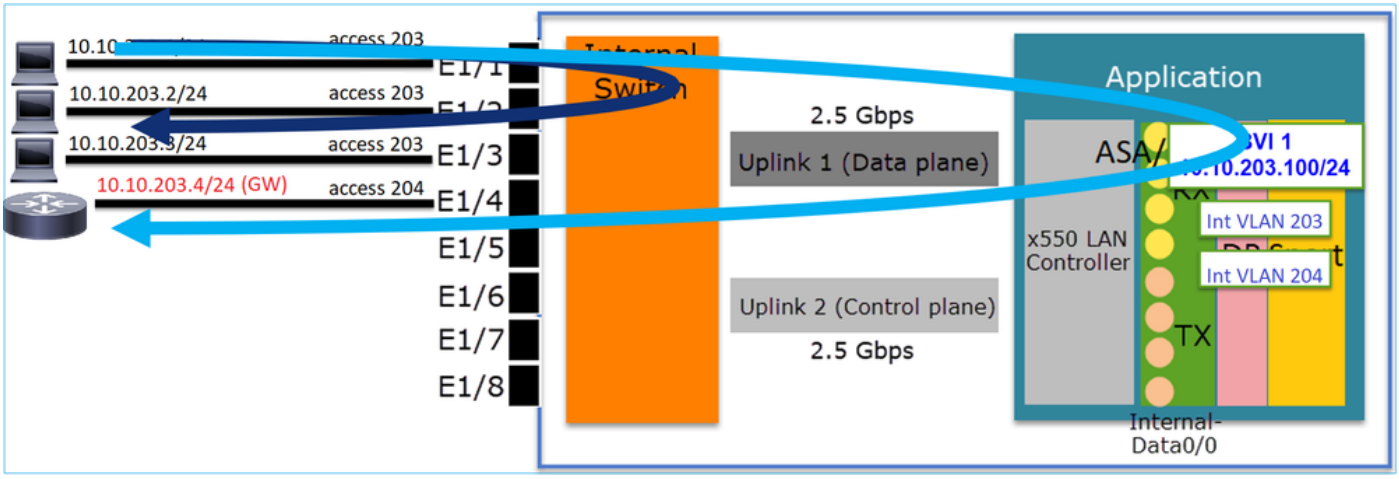


configuración de interfaz FTD

La configuración en este caso es:

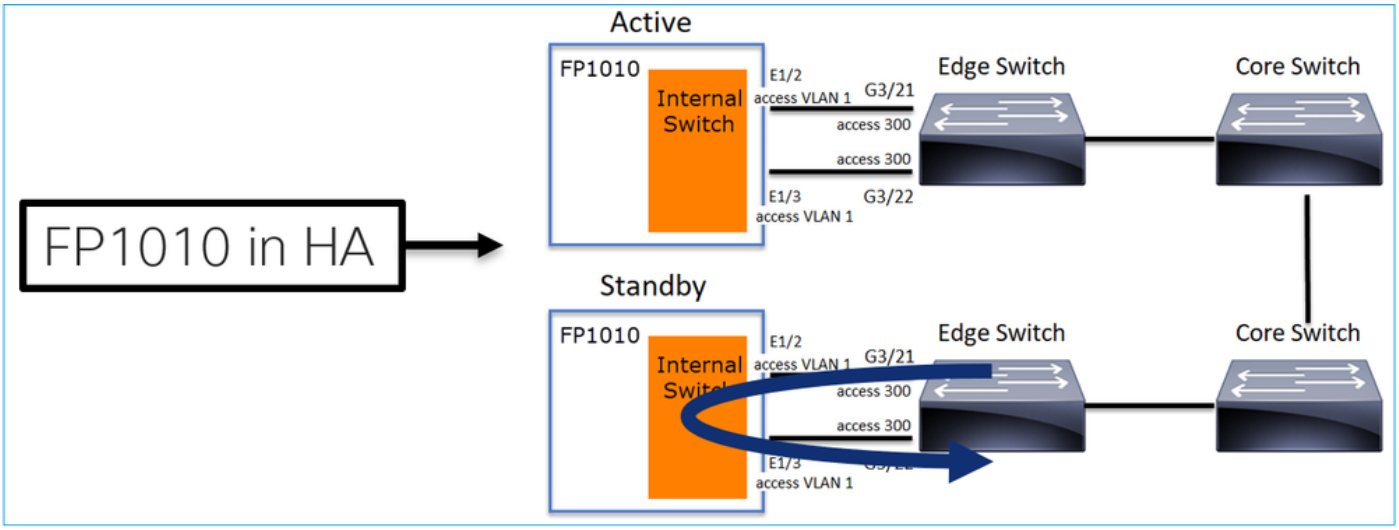
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1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

Comunicación de host a host frente a comunicación de host a GW:



Consideraciones de diseño de FP1010

Switching y alta disponibilidad (HA)

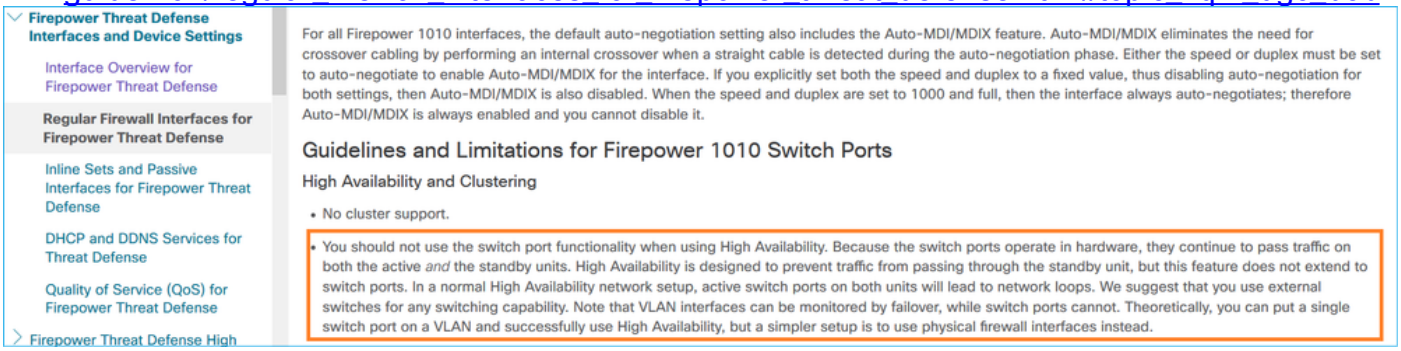


Hay 2 problemas principales cuando se configura el switching de hardware en un entorno HA:

1. HW Switching en la unidad en espera reenvía paquetes a través del dispositivo. Esto puede provocar loops de tráfico.
2. Los puertos de switch no son supervisados por HA

Requisito de diseño

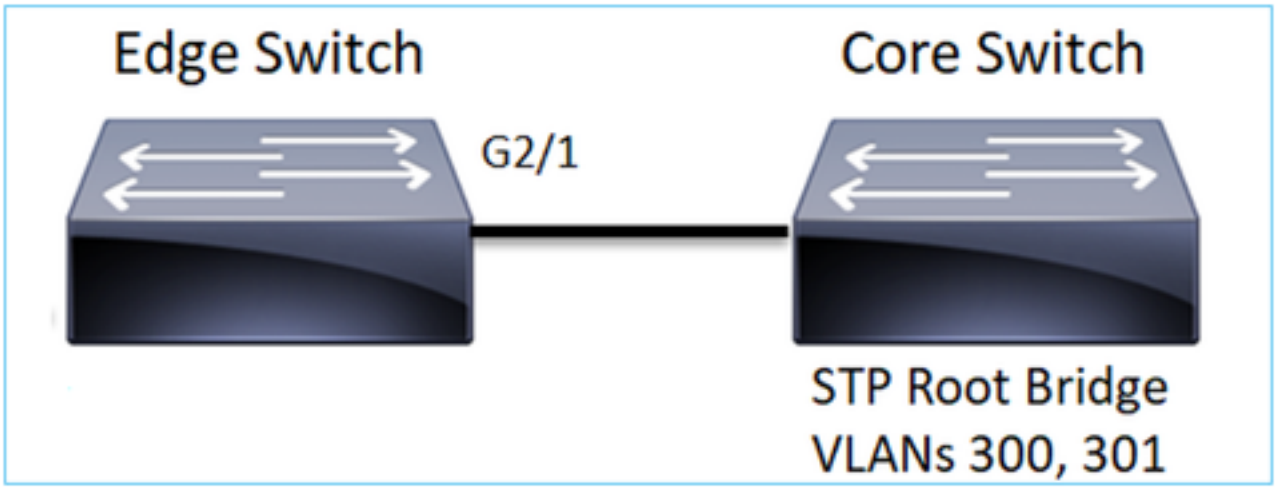
- No debe utilizar la funcionalidad de SwitchPort con alta disponibilidad ASA/FTD. Esto se documenta en la guía de configuración de FMC: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b



Interacción con el protocolo de árbol de extensión (STP)

El switch interno FP1010 no ejecuta STP.

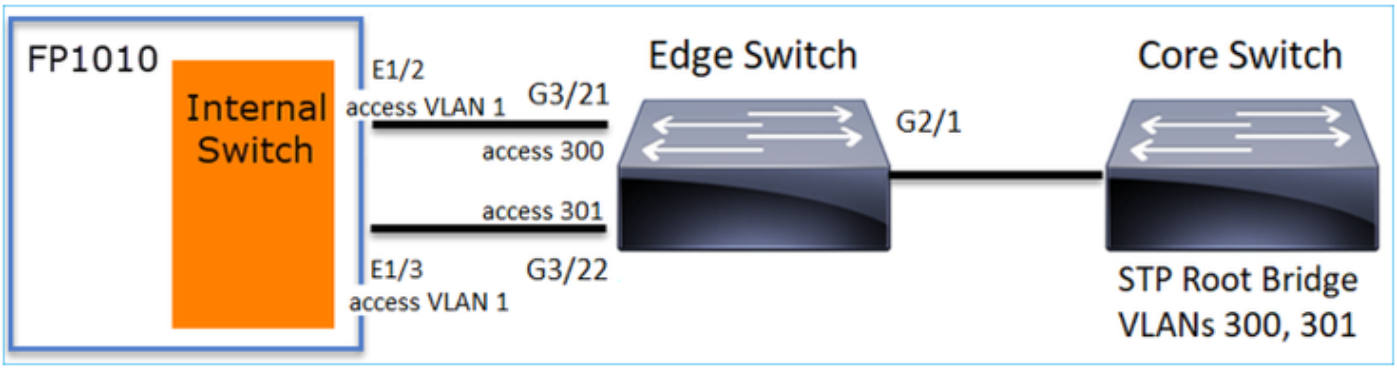
Tenga en cuenta esta situación:



En el switch de borde, el puerto raíz para ambas VLAN es 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
```

Conecte un FP1010 al switch de borde y configure ambos puertos en la misma VLAN (switching de hardware):



El problema

- Debido a la **fuga de VLAN** BPDU superiores para VLAN 301 recibidas en G3/22

```
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
```

Advertencia: Si conecta un switch L2 a FP1010, puede afectar al dominio STP

Esto también se documenta en la guía de configuración de 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.

API REST FXOS

API FMC REST

Estas son las API REST para esta compatibilidad con funciones:

- Interfaz física L2 [PUT/GET soportado]

/api/fmc_config/v1/domain/{domainUUID}/devices/deviceerecords/{containerUUID}/físiccalinterfaces/{objectId}

- Interfaz VLAN [POST/PUT/GET/DELETE admitidos]

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

Resolución de problemas/Diagnóstico

Descripción general de los diagnósticos

- Los archivos de registro se capturan en una solución de problemas de FTD/NGIPS o en la salida show tech. Estos son los elementos que se deben buscar para obtener más detalles en caso de resolución de problemas:
- /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

Recopilación de datos de FXOS (dispositivo) - CLI

En el caso de 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)#
```

En el caso de FTD (consola):

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

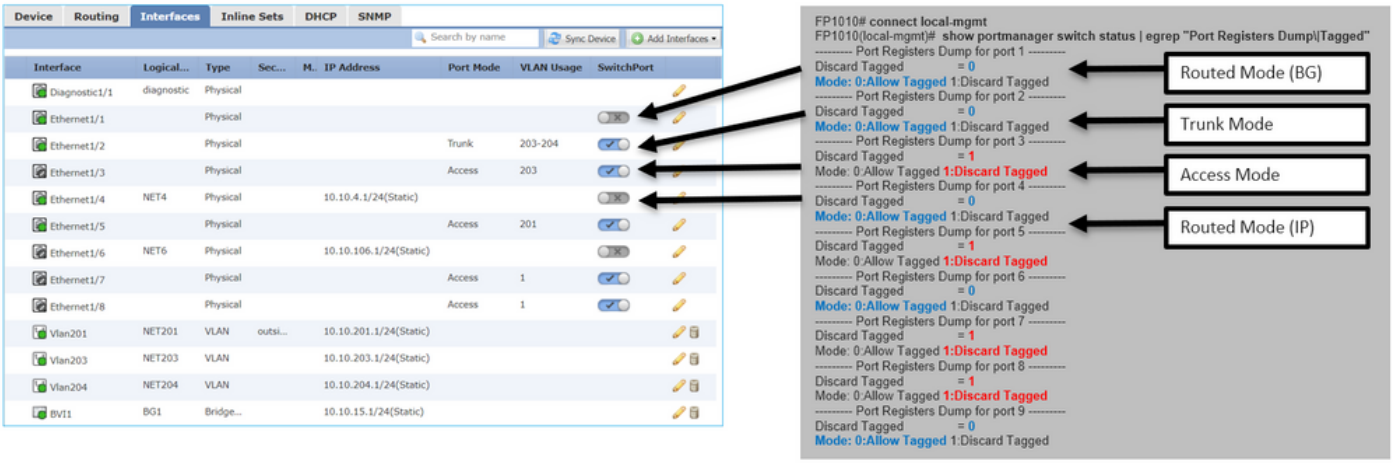
Motor FP1010

Los registros de puertos definen todas las funciones de puerto y switch internas.

En esta captura de pantalla, se muestra la sección 'Control de puerto' de los registros de puerto y específicamente el registro que dicta si el tráfico etiquetado recibido en la interfaz debe ser descartado (1) o permitido (0). Esta es la sección de registro completo de un puerto:

```
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
```

En esta captura de pantalla puede ver los diversos valores de registro de descarte etiquetado para los diversos modos de puerto:

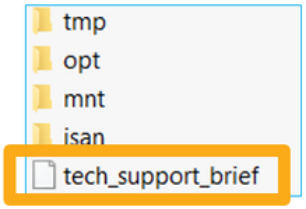


Recopile FPRM show tech en FP1010

Para generar un paquete FPRM y cargarlo en un servidor FTP:

```
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
```

El paquete FPRM contiene un archivo llamado tech_support_brief. El archivo tech_support_brief contiene una serie de comandos show. Uno de ellos es el **estado del switch show portmanager**:



Detalles de limitaciones, problemas comunes y soluciones

Limitaciones de la implementación de la versión 6.5

- Los protocolos de ruteo dinámicos no se soportan para las interfaces SVI.
- Multicontexto no admitido en 1010.
- Rango de ID de VLAN SVI limitado a 1-4070.
- El canal de puerto para L2 no es soportado.
- El puerto L2 como link de failover no es soportado.

Límites relacionados con las funciones del switch

Función	Descripción	Límite
Número de interfaces VLAN	Número total de interfaces VLAN que se pueden crear	60
VLAN de modo troncal	Número máximo de VLAN permitidas en un puerto en modo troncal	20
VLAN nativa	Asigna todos los paquetes sin etiqueta alcanzar en un puerto a la VLAN nativa configurada en el puerto	1
Interfaces con nombre	Incluye todas las interfaces con nombre (interfaz VLAN, subinterfaz, canal de puerto, interfaz física, etc)	60

Otras limitaciones

- Las subinterfaces y la interfaz VLAN no pueden utilizar la misma VLAN.
- Todas las interfaces que participan en BVI deben pertenecer a la misma clase de interfaz.
- Se podría crear una BVI con una combinación de puertos de modo L3 y subinterfaces de puerto de modo L3.
- Se podría crear una BVI con una combinación de VLAN de interfaz.
- No se puede crear una BVI mediante la mezcla de puertos de modo L3 y VLAN de interfaz.

Información Relacionada

- Dispositivo de seguridad Cisco Firepower 1010
- Guías de Configuración