Switch L2 su FPR1010, architettura, verifica e risoluzione dei problemi

Sommario

Introduzione

In questo documento viene descritto lo switch L2 su dispositivi FP1010. In particolare, copre principalmente la parte dell'implementazione relativa a Security Services Platform (SSP)/Firepower eXtensive Operation System (FXOS). Nella versione 6.5, Firepower 1010 (modello Desktop) ha abilitato le funzionalità di commutazione sullo switch hardware L2 incorporato. In questo modo è possibile evitare switch hardware aggiuntivi e ridurre i costi.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

- FP1010 è un modello desktop Small-Office Home-Office (SOHO) che sostituisce le piattaforme ASA5505 e ASA5506-X.
- Supporto software per immagini FTD (6.4+) gestite da Firepower Management Center (FMC), Firepower Device Manager (FDM) o Cloud Defense Orchestrator (CDO).
- Supporto software per immagini ASA (9.13+) gestite da CSM, ASDM o CLI.
- Il sistema operativo (OS), ASA o FTD, è FXOS (simile a FP21xx).
- 8 porte dati 10/100/1000 Mbps.
- Le porte E1/7, E1/8 supportano PoE+.
- Lo switch hardware consente la comunicazione della velocità di linea tra le porte (ad esempio: una fotocamera viene inserita nel server locale).

Aggiunte a Firepower 6.5

- Introduzione di un nuovo tipo di interfaccia denominata SVI (Switched Virtual Interface).
- Modalità mista: Le interfacce possono essere configurate in modalità commutata (L2) o non commutata (L3).
- La modalità L3 inoltra tutti i pacchetti all'applicazione di sicurezza.
- Le porte in modalità L2 possono passare da un dispositivo hardware all'altro se due porte fanno parte della stessa VLAN, con un conseguente miglioramento del throughput e della latenza. E i pacchetti che devono essere instradati o collegati raggiungono l'applicazione di sicurezza (ad esempio: una fotocamera che scarica un nuovo firmware da Internet) e sottoporsi a un controllo di sicurezza secondo la configurazione.
- L'interfaccia fisica L2 può essere associata a una o più interfacce SVI.
- Le interfacce in modalità L2 possono essere in modalità di accesso o trunk.
- L'interfaccia L2 della modalità di accesso consente solo traffico senza tag.
- L'interfaccia L2 della modalità trunk consente il traffico con tag.

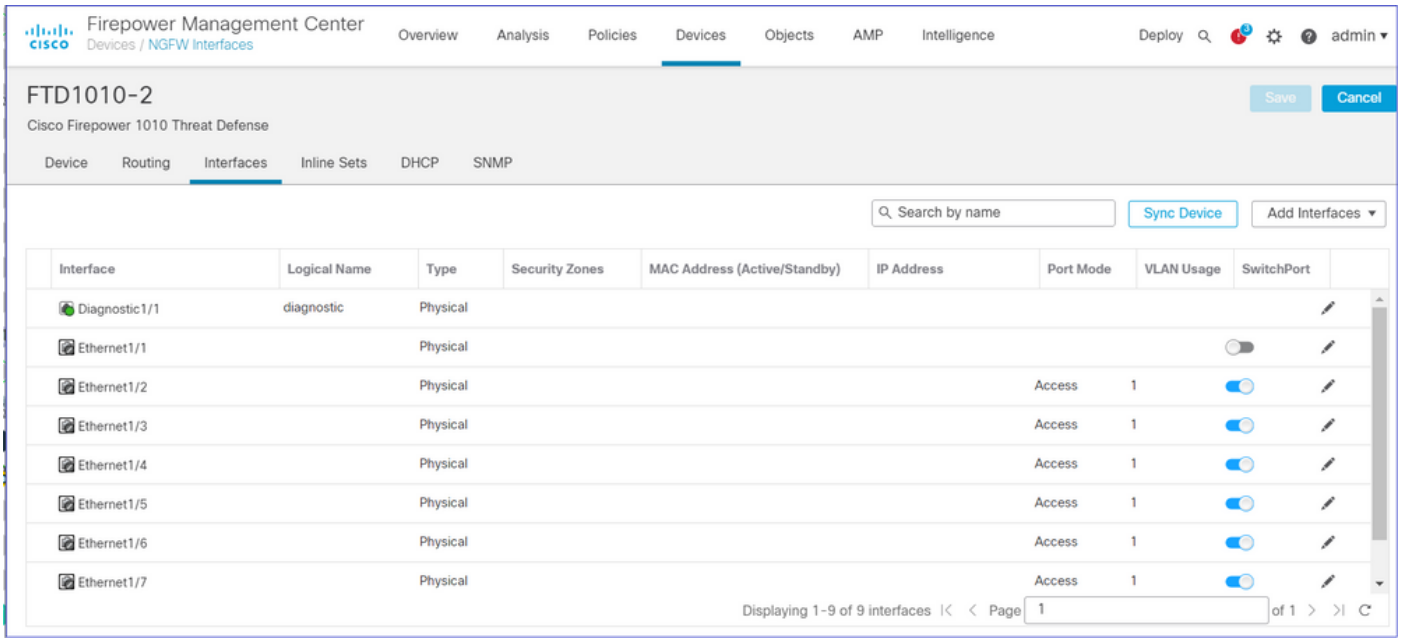
- Supporto VLAN nativa per interfaccia L2 in modalità trunk.
- ASA CLI, ASDM, CSM, FDM e FMC sono stati migliorati per supportare nuove funzionalità.

Aggiunte FMC

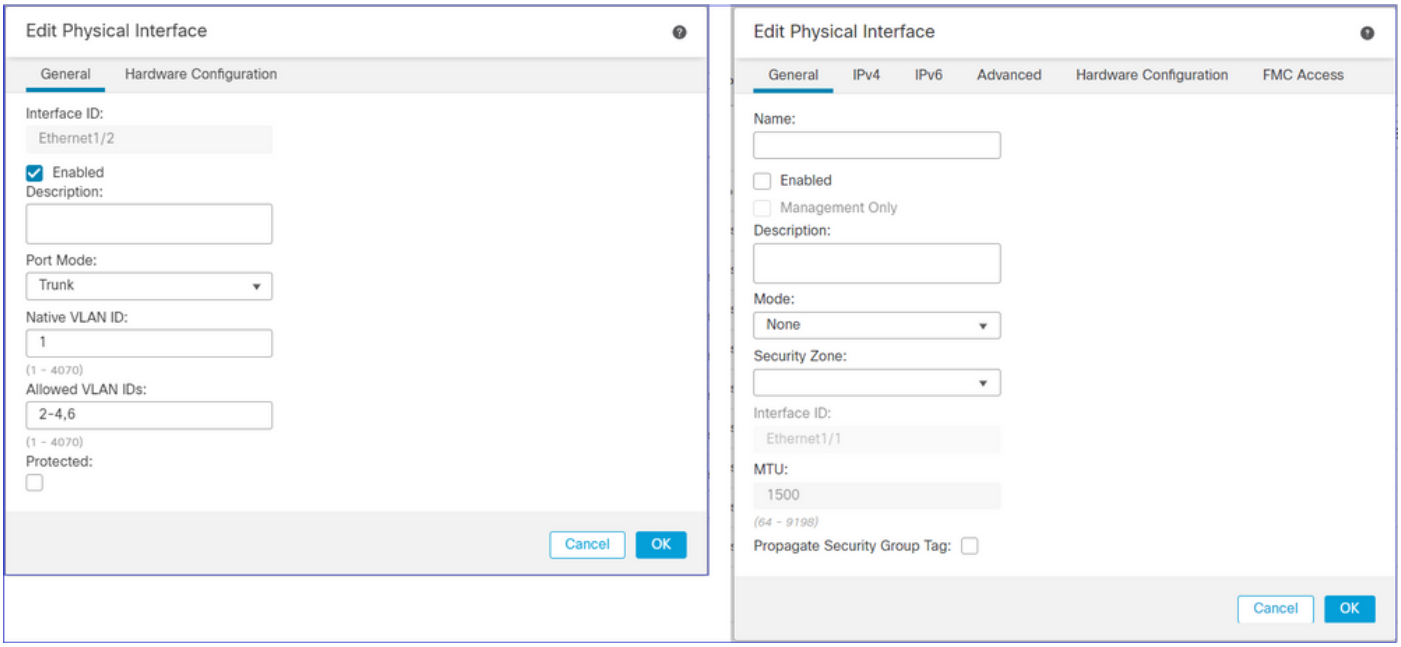
- Èstata introdotta una nuova modalità di interfaccia chiamata switchport per un'interfaccia fisica che viene utilizzata per determinare se un'interfaccia fisica è un'interfaccia L3 o L2.
- L'interfaccia fisica L2 può essere associata a una o più interfacce VLAN in base alla modalità di accesso o alla modalità trunk.
- Firepower 1010 supporta la configurazione Power Over Ethernet (PoE) sulle ultime due interfacce dati, ad esempio Ethernet1/7 ed Ethernet1/8.
- La modifica dell'interfaccia tra commutato e non commutato elimina tutte le configurazioni ad eccezione della configurazione PoE e hardware.

Come funziona

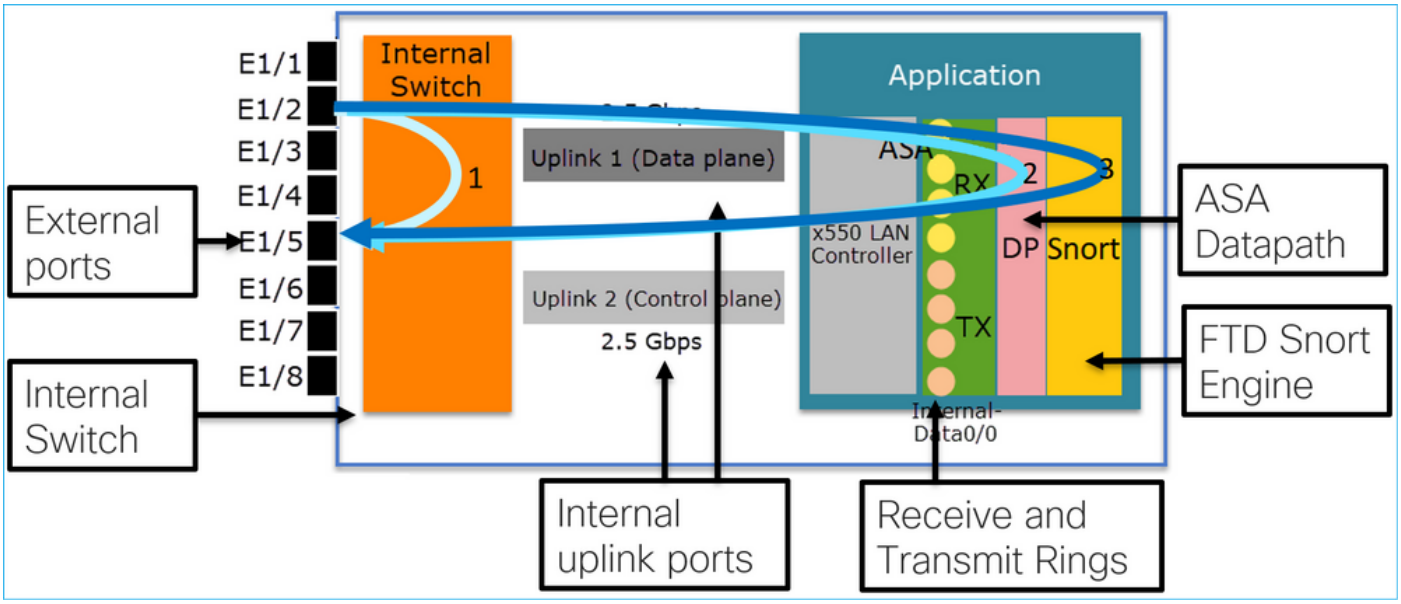
Questa funzionalità è solo un miglioramento del supporto dell'interfaccia esistente su FMC (**Gestione dispositivi > Pagina interfaccia**).



Visualizzazione interfaccia fisica (L2 e L3)



Architettura FP1010



- 8 porte dati esterne.
- 1 Switch interno
- 3 porte di uplink (2 delle quali mostrate nella figura), una per Data-Plane, una per Control-Plane, una per Configuration.
- Controller LAN x550 (l'interfaccia tra l'applicazione e gli uplink).
- 4 squilli di ricezione (RX) e 4 di trasmissione (TX).
- Processo di datapath (su ASA e FTD).
- Avvia processo (su FTD).

Elaborazione pacchetti

L'elaborazione dei pacchetti può essere influenzata da due fattori principali:

1. Modalità interfaccia/porta

2. Politica applicata

Un pacchetto può attraversare FP1010 in 3 modi diversi:

1. Elaborato solo dal commutatore interno

2. Inoltrato all'applicazione (ASA/FTD) ed elaborato solo dal processo del percorso dati

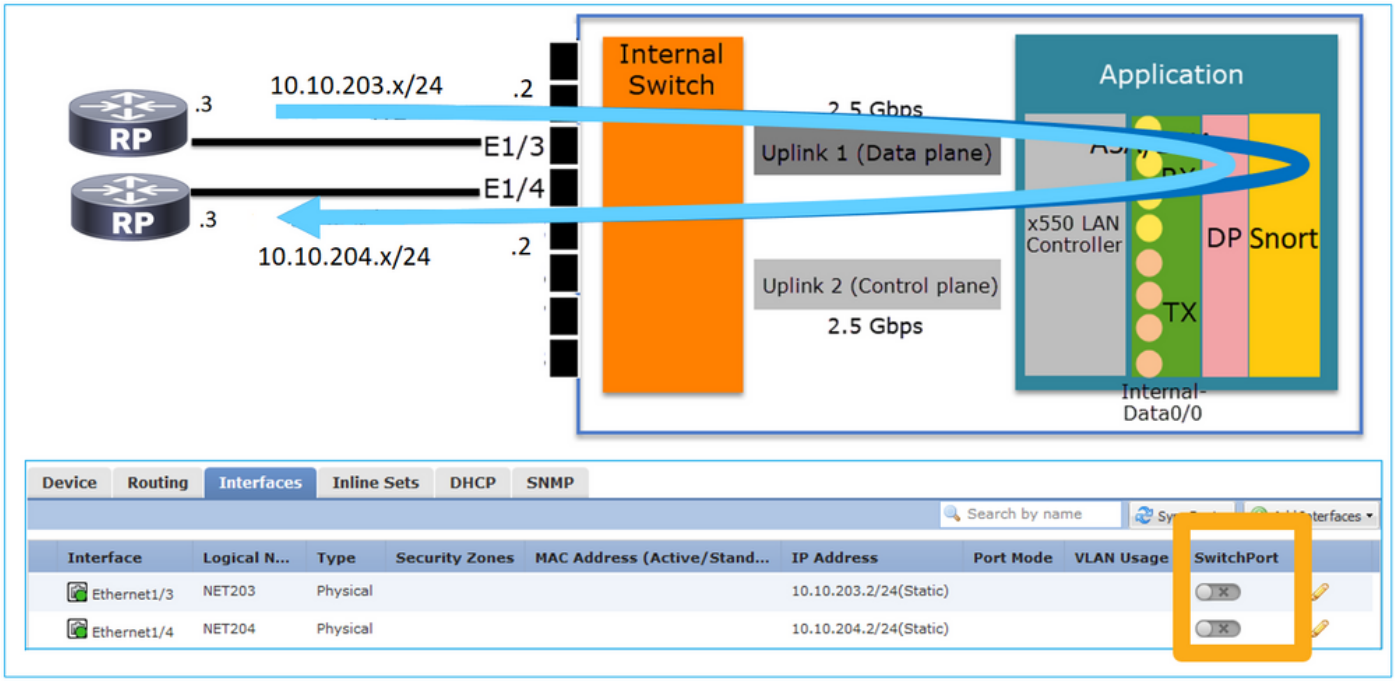
3. Inoltrato all'applicazione (FTD) ed elaborato dal datapath e dal motore Snort

Modalità porte FP1010

Gli esempi di interfaccia utente sono per FMC, gli esempi di CLI sono per FTD. La maggior parte dei concetti sono validi anche per le appliance ASA.

Caso FP1010 1. Porte di routing (routing IP)

Configurazione e funzionamento



Punti chiave

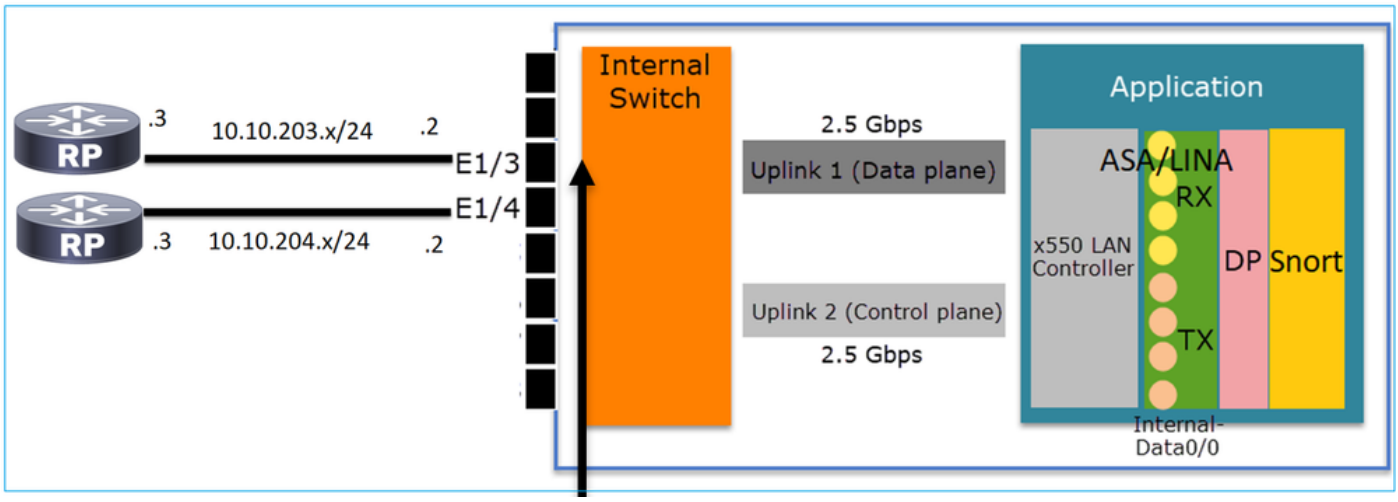
- Dal punto di vista della progettazione, le 2 porte appartengono a 2 diverse subnet L2.
- Quando le porte sono configurate in modalità di routing, i pacchetti vengono elaborati dall'applicazione (ASA o FTD).
- Nel caso dell'FTD, in base all'azione della regola (ad esempio, ALLOW), i pacchetti possono essere persino ispezionati dal motore Snort.

Configurazione interfaccia 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
```

Verifica porta di routing FP1010



Dalla CLI di FXOS è possibile controllare i contatori dell'interfaccia fisica. Nell'esempio vengono mostrati i contatori unicast in entrata e in uscita sulla porta 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
```

Èpossibile applicare acquisizioni di percorsi dati FTD e tracciare i pacchetti:

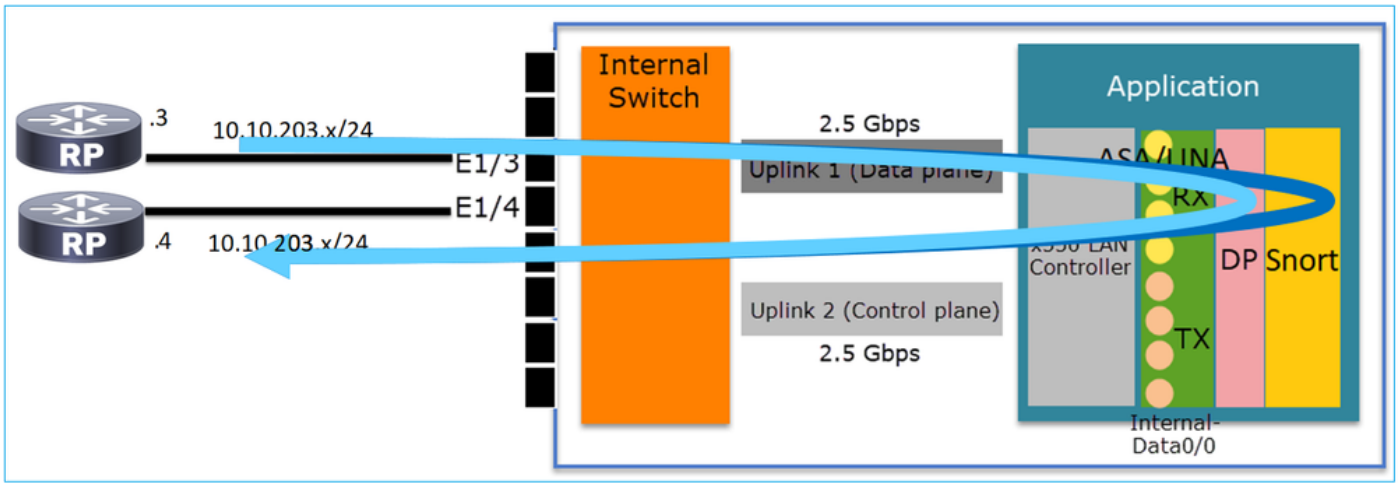
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

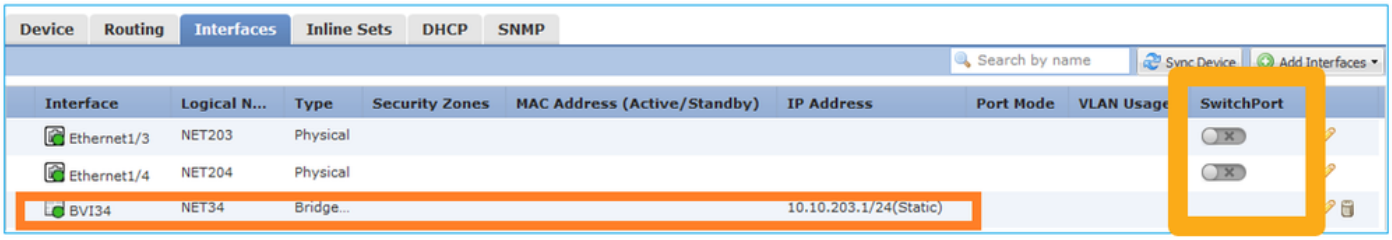
Questo è un frammento di codice di acquisizione. Come previsto, il pacchetto viene inoltrato in base a una ricerca route:

```
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. Modalità Bridge-Group (Bridging)

Configurazione e funzionamento





Punti chiave

- Da un punto di vista progettuale, le 2 porte sono connesse alla stessa subnet L3 (simile a un firewall trasparente), ma a una VLAN diversa.
- Quando le porte sono configurate in modalità Bridging, i pacchetti vengono elaborati dall'applicazione (ASA o FTD).
- Nel caso dell'FTD, in base all'azione della regola (ad esempio, ALLOW), i pacchetti possono essere persino ispezionati dal motore Snort.

Configurazione interfaccia 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
```

Verifica porta gruppo di bridge FP1010

Questo comando visualizza i membri di interfaccia di 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
```

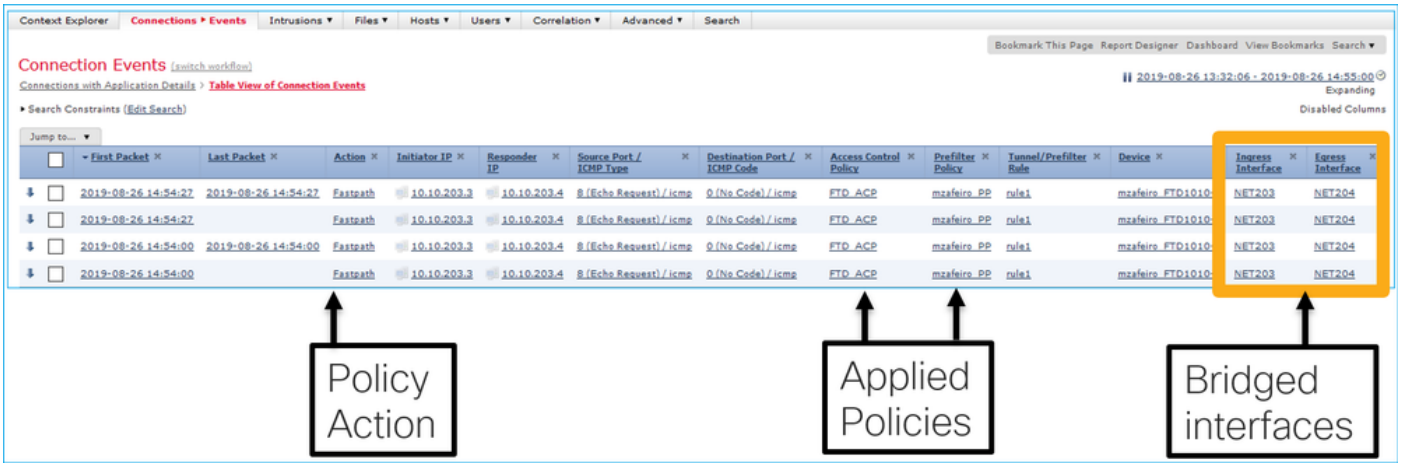
Questo comando mostra la tabella ASA/FTD datapath Content Addressable Memory (CAM):

```
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
```

Un frammento di traccia del pacchetto mostra che il pacchetto viene inoltrato in base alla ricerca MAC L2 di destinazione:

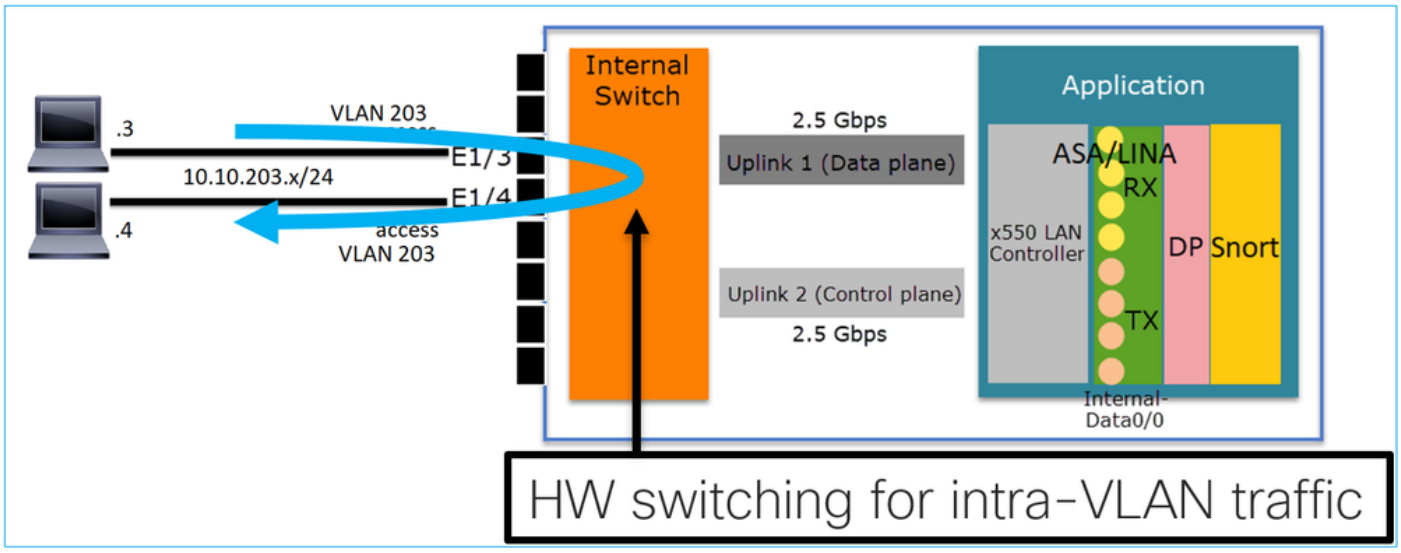
```
FP1010# show cap CAP203 packet-number 1 trace

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
```

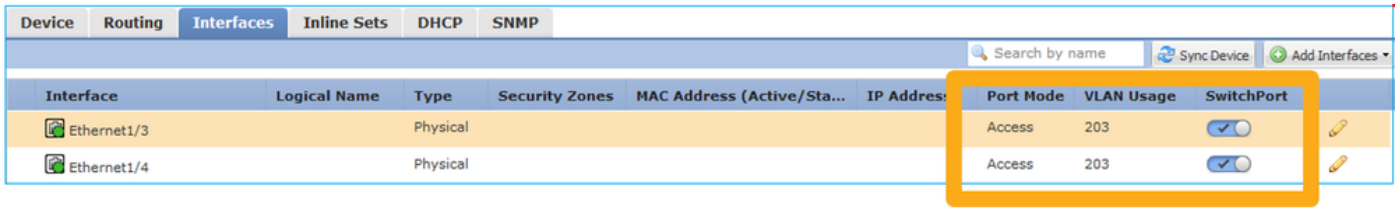
Nel caso di FTD, gli eventi di connessione FMC possono anche fornire informazioni sull'ispezione di flusso e sulle interfacce del gruppo-ponte di transito:



FP1010 Case 3. Porte dello switch (commutazione hardware) in modalità di accesso

Configurazione e funzionamento





Punti chiave

- Lo switching HW è una funzionalità FTD **6.5+** e ASA **9.13+**.
- Da un punto di vista progettuale, le due porte sono connesse alla stessa subnet L3 e alla stessa VLAN.
- Le porte in questo scenario funzionano in modalità di accesso (solo traffico senza tag).
- Per le porte del firewall configurate in modalità SwitchPort non è configurato un nome logico (nameif).
- Quando le porte sono configurate in modalità Switching e appartengono alla stessa VLAN (traffico intra VLAN), i pacchetti vengono elaborati solo dallo switch interno FP1010.

Configurazione interfaccia FTD

Dal punto di vista della CLI, la configurazione sembra molto simile a uno switch L2:

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

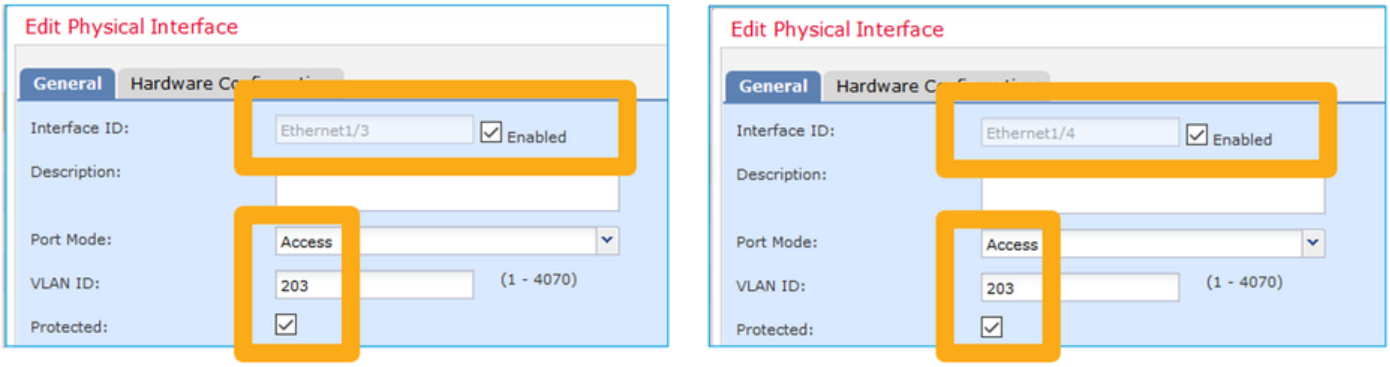
Filtraggio del traffico tra VLAN

La sfida: **Un ACL non è in grado di filtrare il traffico interno alla VLAN.**

La soluzione: Porte **protette**

Il principio è molto semplice: 2 le porte configurate come protette non possono comunicare tra loro.

Interfaccia utente FMC in caso di porte protette:



Configurazione interfaccia FTD

Il comando **switchport protected** viene configurato nell'interfaccia:

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

Verifica porta switch FP1010

Nell'esempio, vengono inviati 1000 pacchetti unicast (ICMP) con una dimensione specifica (1100 byte):

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

Per controllare i contatori unicast in entrata e in uscita delle interfacce di transito, utilizzare questo 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
```

Questo comando mostra lo stato della VLAN dello switch interno:

```
FP1010# show switch vlan
```

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

Lo stato di una VLAN è ATTIVO se almeno una porta è assegnata alla VLAN

Se una porta è disattivata a livello amministrativo o la porta dello switch connesso è disattivata/cavo disconnesso e questa è l'unica porta assegnata alla VLAN, anche lo stato della VLAN sarà inattivo:

```
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
```

Questo comando mostra la tabella CAM dello 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
```

Il tempo di aging predefinito della tabella CAM dello switch interno è di 5 min 30 sec.

FP1010 contiene 2 tabelle CAM:

1. **Tabella CAM switch interno**: Utilizzato in caso di commutazione HW
2. **Tabella CAM datapath ASA/FTD**: Utilizzato in caso di bridging

Ogni pacchetto/frame che attraversa FP1010 viene elaborato da una singola tabella CAM (switch interno o datapath FTD) in base alla modalità della porta.

> **Attenzione:** Non confondere la tabella **show switch mac-address-table** interna dello switch CAM utilizzata in modalità SwitchPort con la tabella **show mac-address-table** FTD datapath CAM utilizzata in modalità bridge

Switching hardware: Ulteriori informazioni

I log del percorso dati ASA/FTD non mostrano informazioni sui flussi con commutazione a livello di hardware:

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

La tabella di connessione del percorso dati ASA/FTD non mostra i flussi con commutazione a livello di hardware:

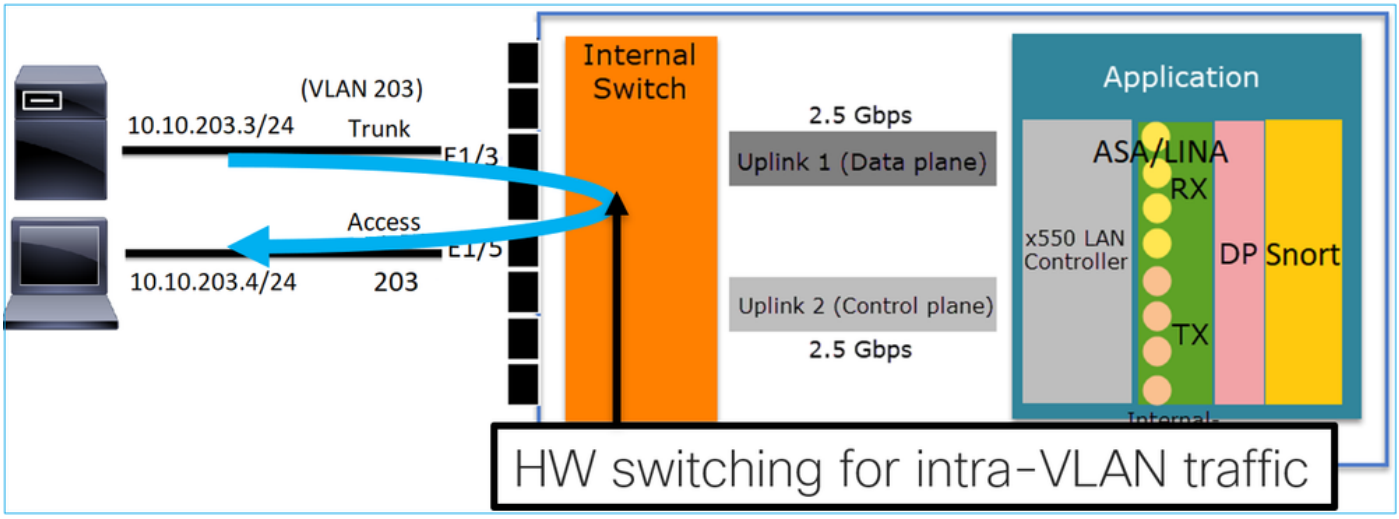
```
FP1010# show conn
```

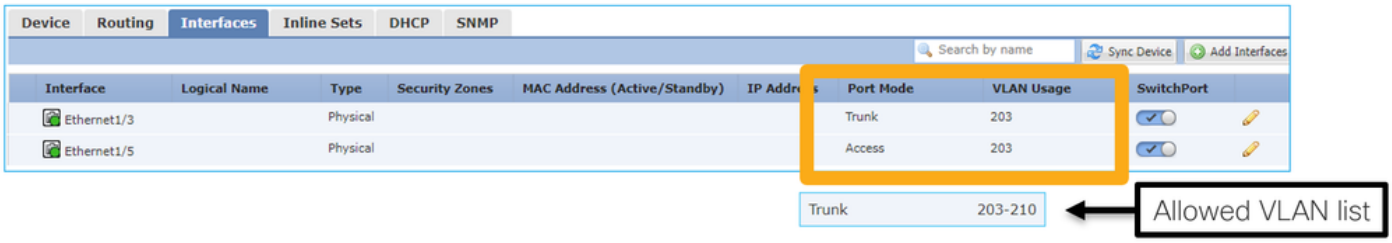
```
0 in use, 3 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

Inoltre, gli eventi di connessione FMC non mostrano i flussi a commutazione di hardware.

FP1010 Case 4. Porte dello switch (trunking)

Configurazione e funzionamento





Punti chiave

- Lo switching HW è una funzionalità FTD **6.5+** e ASA **9.13+**.
- Da un punto di vista progettuale, le due porte sono connesse alla stessa subnet L3 e alla stessa VLAN.
- La porta trunk accetta frame con tag e senza tag (in caso di una VLAN nativa).
- Quando le porte sono configurate in modalità Switching e appartengono alla stessa VLAN (traffico intra VLAN), i pacchetti vengono elaborati solo dallo switch interno.

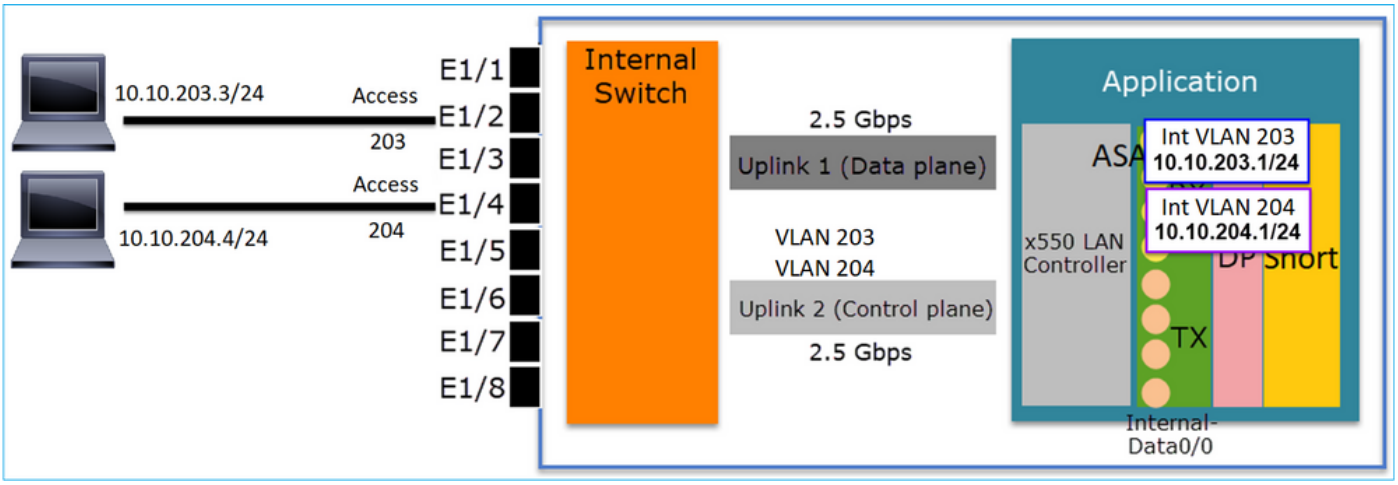
Configurazione interfaccia FTD

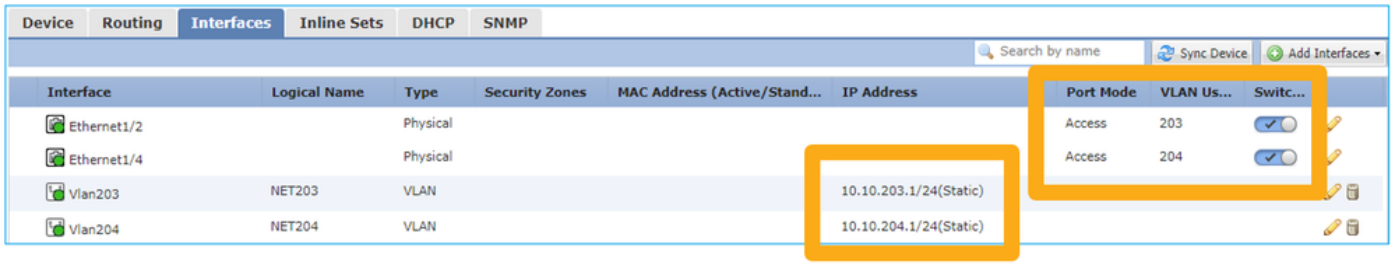
La configurazione è simile a una porta dello switch di layer 2:

```
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
```

FP1010 Case 5. Porte dello switch (inter-VLAN)

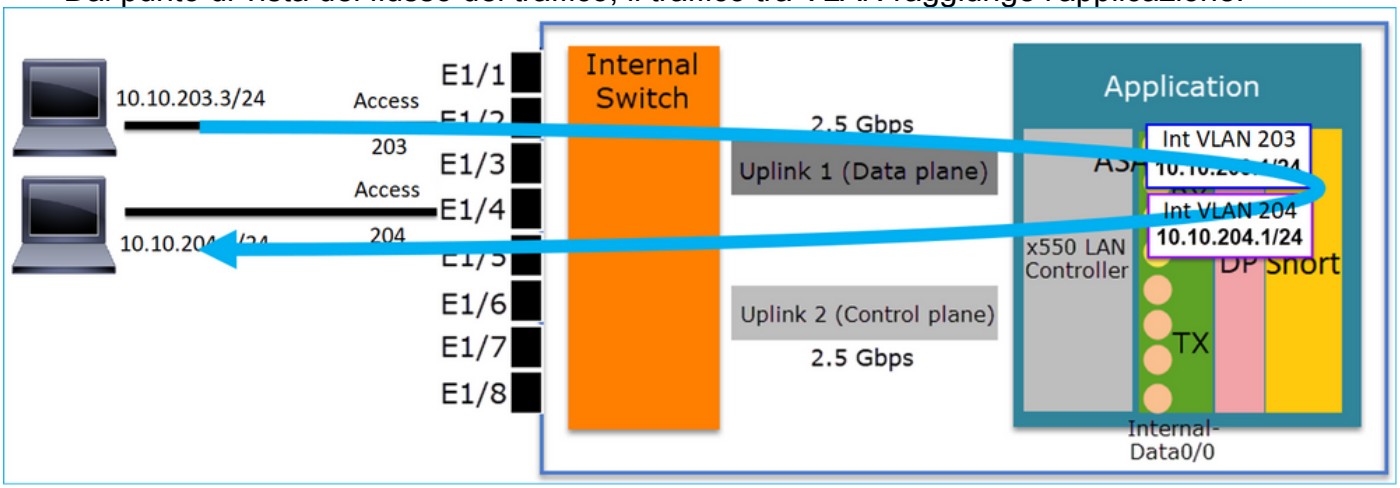
Configurazione e funzionamento





Punti chiave

- Da un punto di vista progettuale, le 2 porte sono connesse a 2 diverse subnet L3 e 2 diverse VLAN.
- Il traffico tra le VLAN passa attraverso le interfacce VLAN (simile alle SVI).
- Dal punto di vista del flusso del traffico, il traffico tra VLAN raggiunge l'applicazione.



Configurazione interfaccia FTD

La configurazione è simile a quella di un'interfaccia virtuale di switch (SVI):

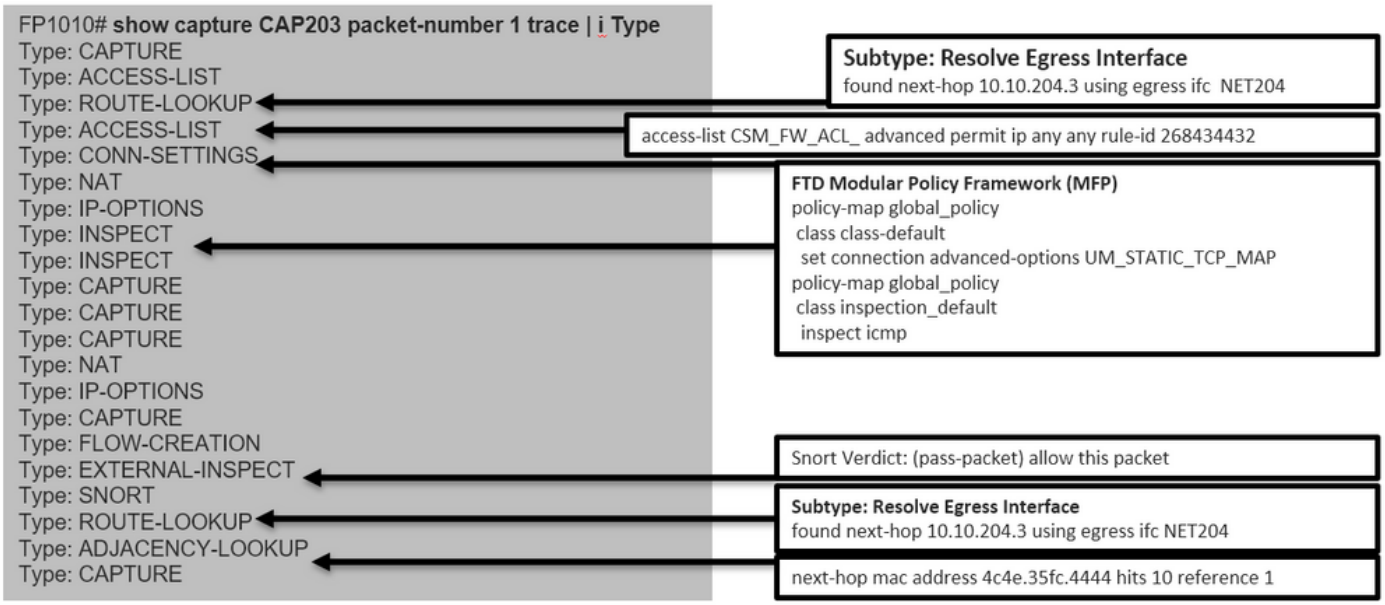
```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

Elaborazione dei pacchetti per il traffico tra VLAN

Questa è la traccia di un pacchetto che attraversa 2 VLAN diverse:

```
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
```

Le fasi principali del processo del pacchetto:



FP1010 Caso 6. Filtro inter-VLAN

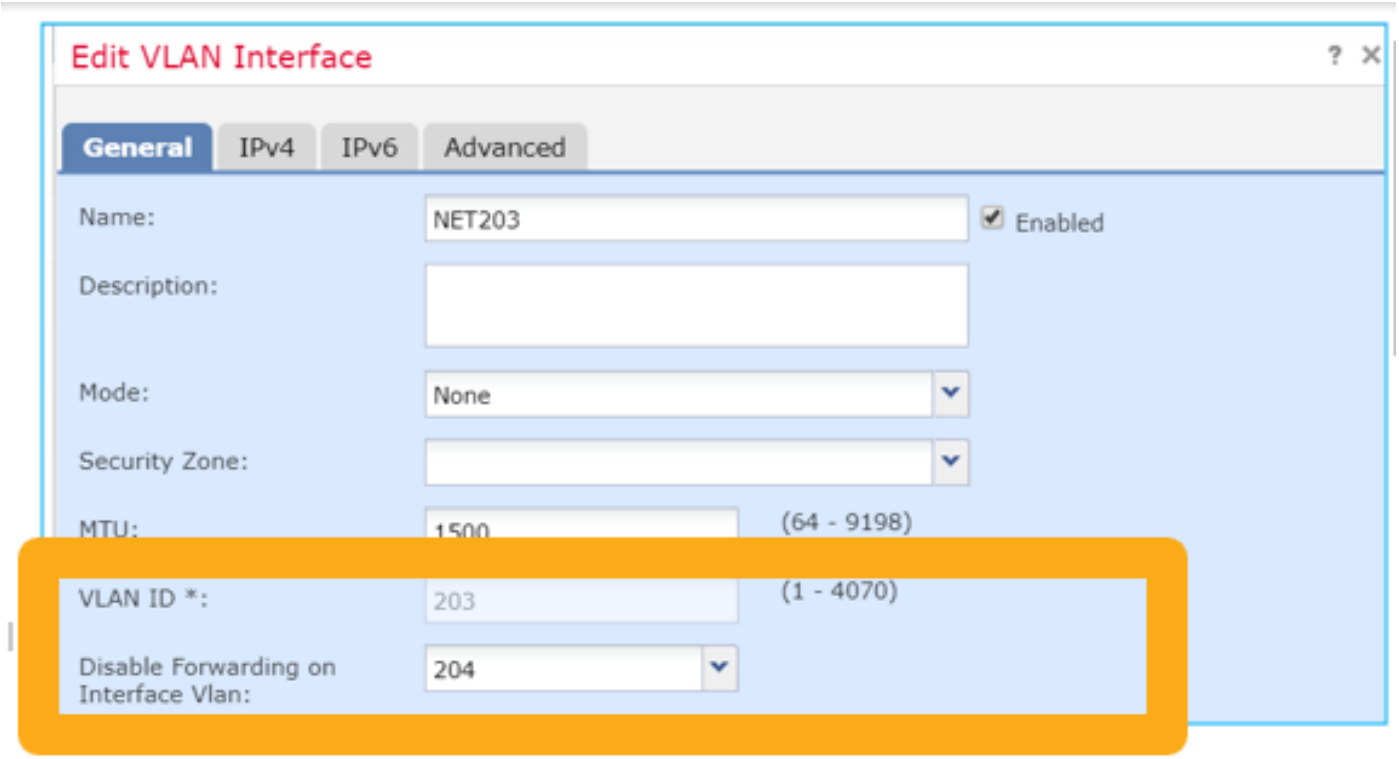
Configurazione e funzionamento

Per filtrare il traffico tra VLAN, sono disponibili due opzioni principali:

1. Policy di controllo dell'accesso
2. comando "no forward"

Filtrare il traffico tra VLAN con il comando "no forward"

Configurazione interfaccia utente FMC:



Punti chiave

- Il rilascio in avanti è unidirezionale.
- Non può essere applicato a entrambe le interfacce VLAN.
- Il controllo in avanti viene eseguito prima del controllo ACL.

Configurazione interfaccia FTD

In questo caso, la configurazione CLI è:

```
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
```

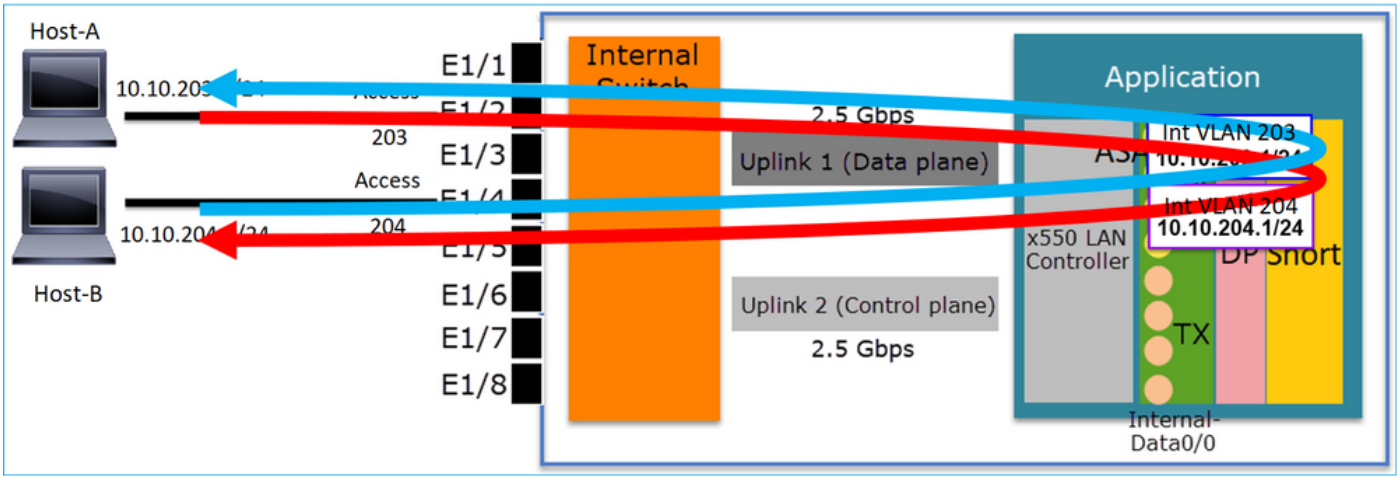
Se un pacchetto viene scartato dalla funzione no forward, viene generato un messaggio Syslog datapath ASA/FTD:

```
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)
```

Dal punto di vista della visualizzazione Accelerated Security Path (ASP), è considerato un rilascio ACL:

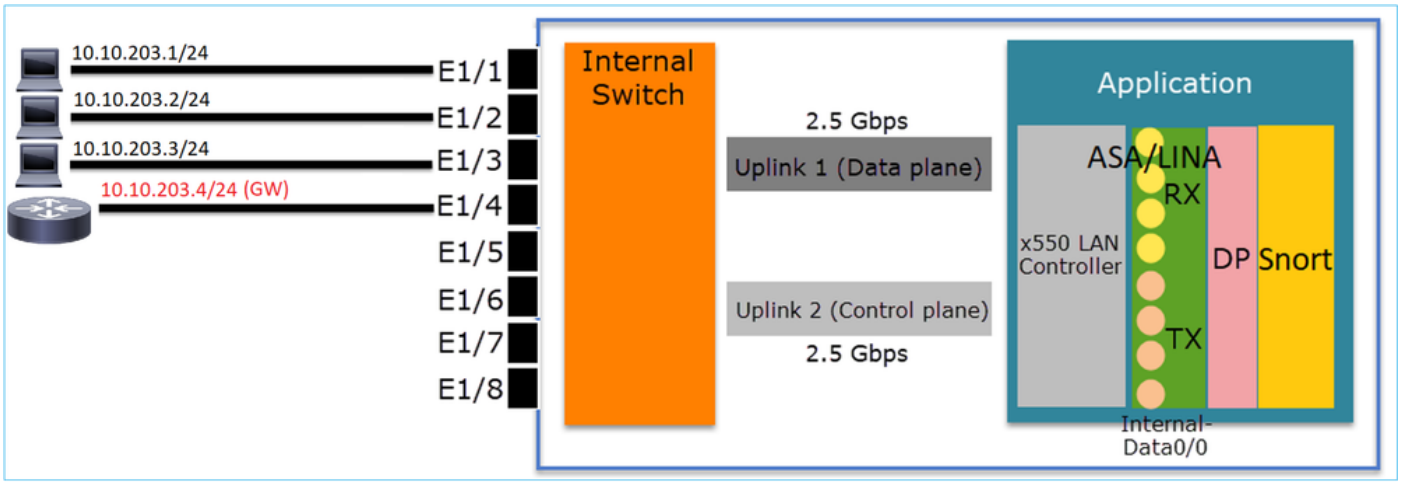
```
FP1010-2# show asp drop
Frame drop:
Flow is denied by configured rule (acl-drop) 1
```

Poiché il rilascio è unidirezionale, l'host A (VLAN 203) non può avviare il traffico verso l'host B (VLAN 204), ma è consentito il contrario:



Case study - FP1010. Bridging e switching hardware + Bridging

Considerare la topologia seguente:



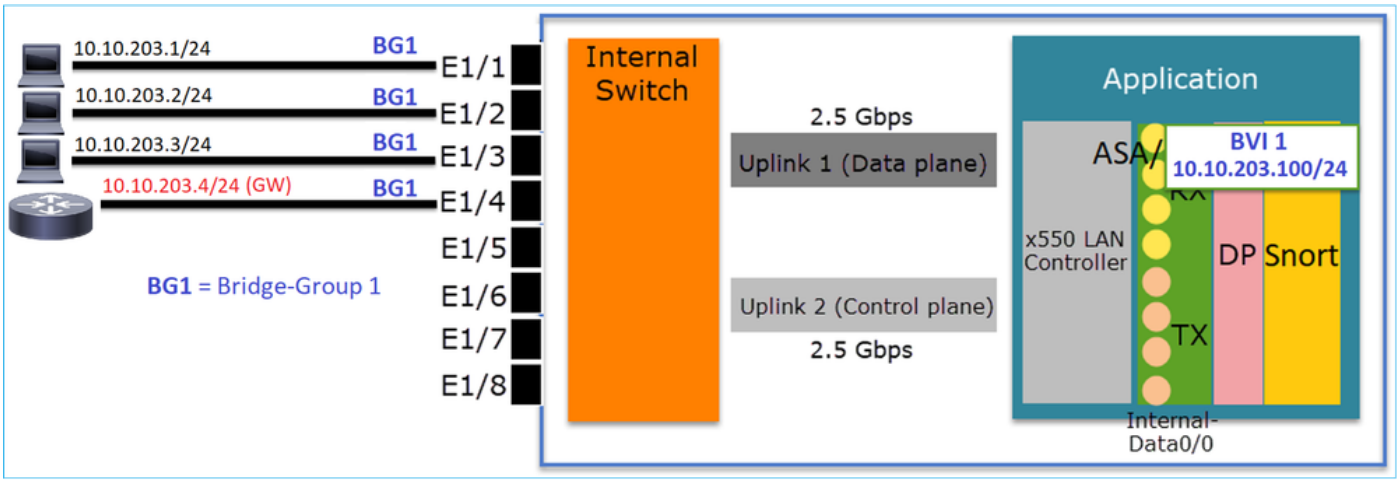
In questa topologia:

- Tre host terminali appartengono alla stessa subnet L3 (10.10.203.x/24).
- Il router (10.10.203.4) funziona come GW nella subnet.

In questa topologia sono disponibili due opzioni di progettazione principali:

1. Bridging
2. Switching HW + Bridging

Opzione di progettazione 1. Bridging

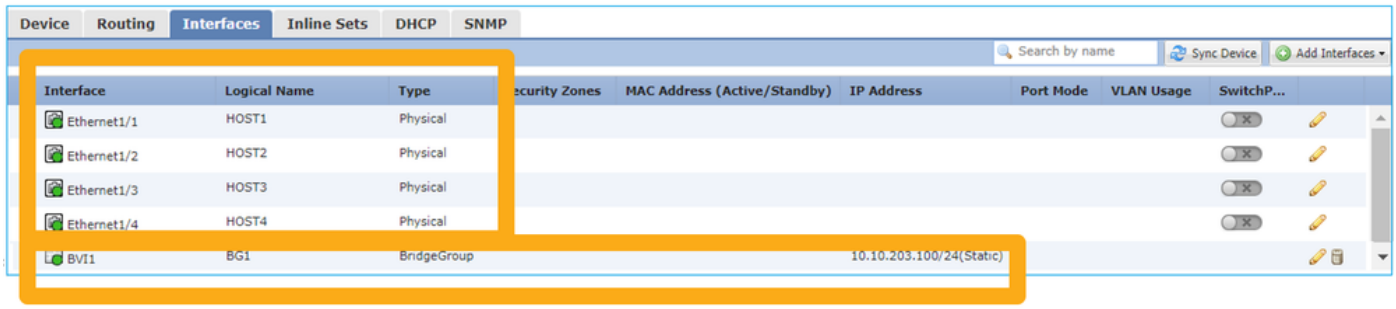


Punti chiave

I punti principali di questo progetto sono:

- Èpresente una BVI 1 creata con un IP nella stessa subnet (10.10.203.x/24) dei 4 dispositivi collegati.
- Tutte e quattro le porte appartengono allo stesso Bridge-Group (in questo caso il gruppo 1).
- A ciascuna delle quattro porte è configurato un nome.
- La comunicazione host-host e host-GW passa attraverso l'applicazione (ad esempio, FTD).

Dal punto di vista dell'interfaccia utente di FMC, la configurazione è:

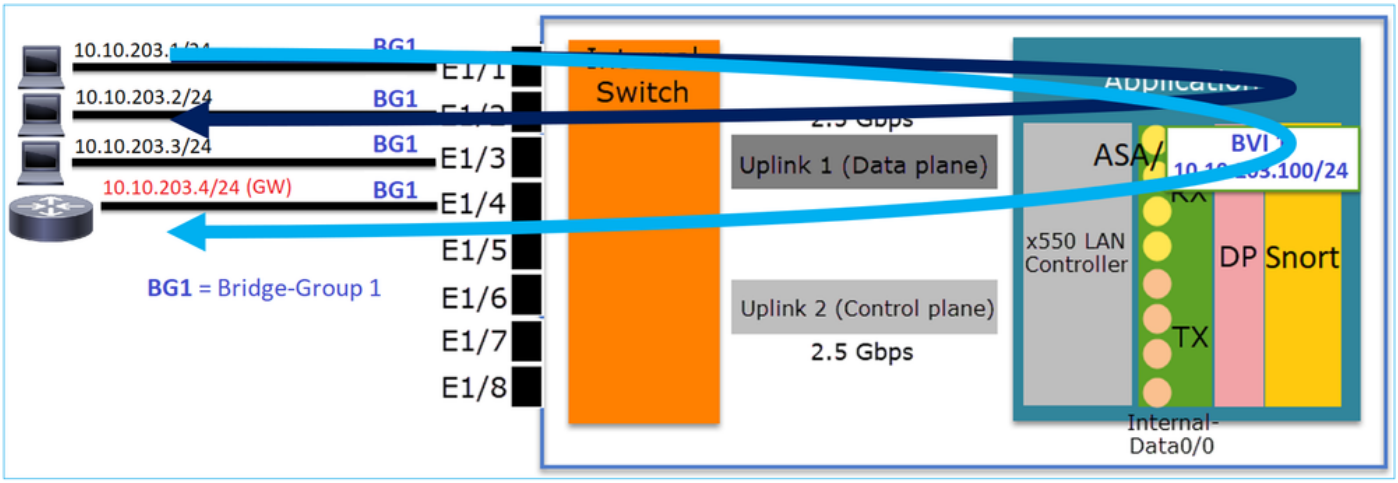


Configurazione interfaccia FTD

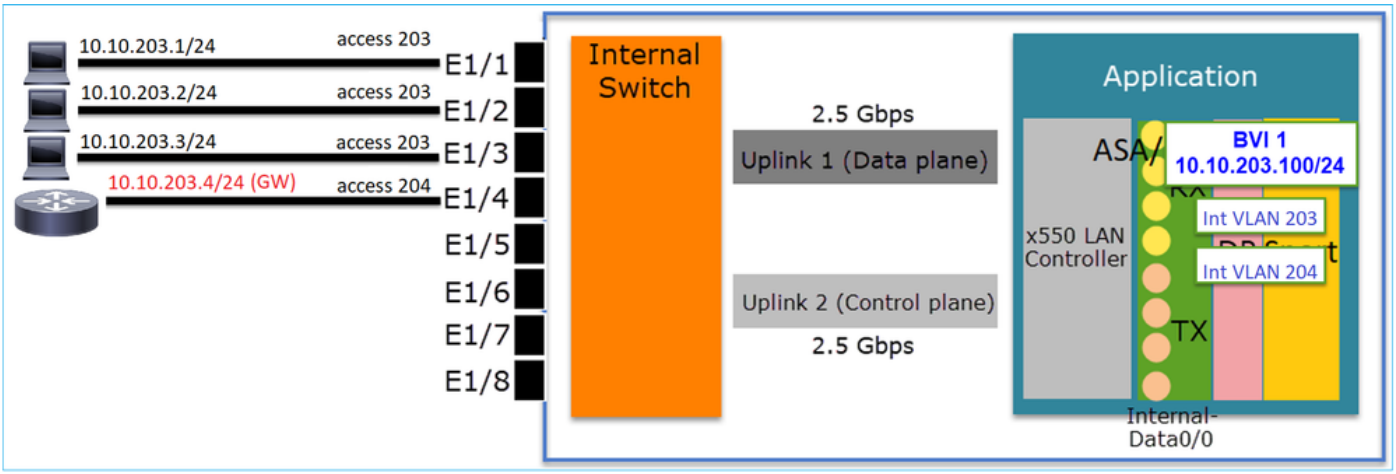
In questo caso, la configurazione è:

```
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
```

Flusso del traffico in questo scenario:



Opzione di progettazione 2. Switching hardware + Bridging

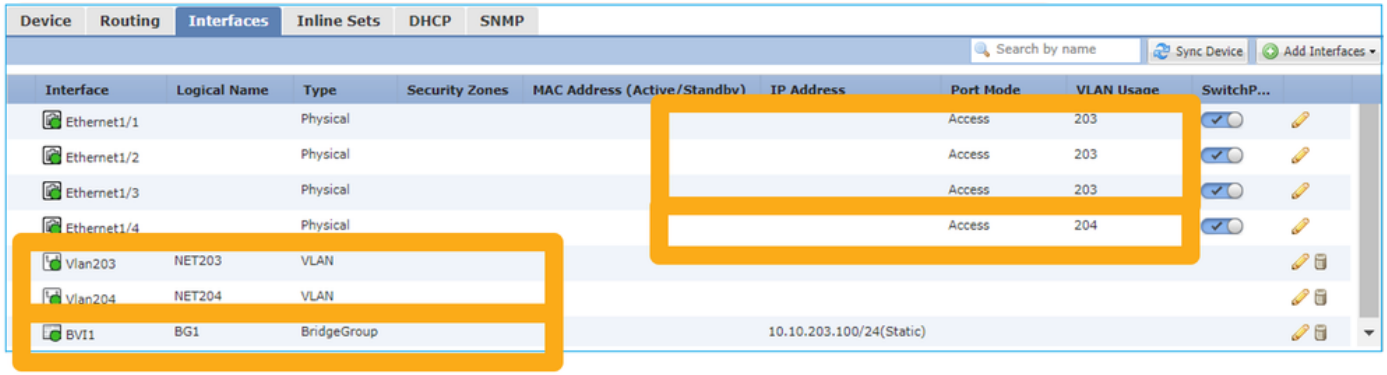


Punti chiave

I punti principali di questo progetto sono:

- Èpresente una BVI 1 creata con un IP nella stessa subnet (10.10.203.x/24) dei 4 dispositivi collegati.
- Le porte collegate agli host terminali sono configurate in modalità SwitchPort e appartengono alla stessa VLAN (203).
- La porta collegata al GW è configurata in modalità SwitchPort e appartiene a una VLAN diversa (2004).
- Sono disponibili 2 interfacce VLAN (203, 204). Alle due interfacce VLAN non è assegnato un indirizzo IP e appartengono al gruppo di bridge 1.
- La comunicazione host-host passa solo attraverso lo switch interno.
- La comunicazione host-GW avviene attraverso l'applicazione (ad esempio, FTD).

Configurazione interfaccia utente FMC:

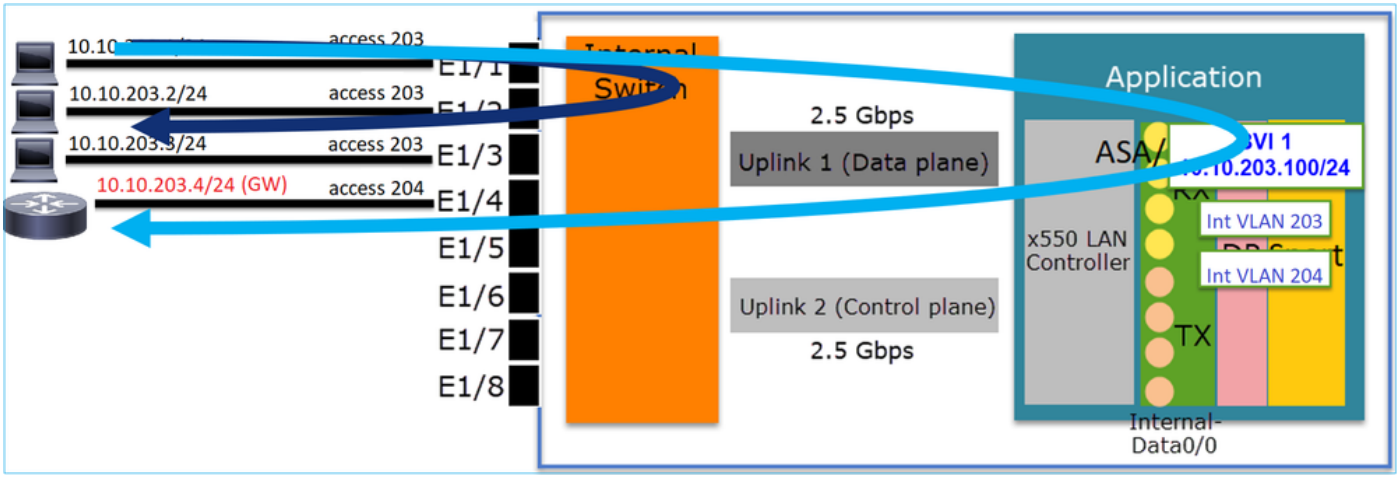


Configurazione interfaccia FTD

In questo caso, la configurazione è:

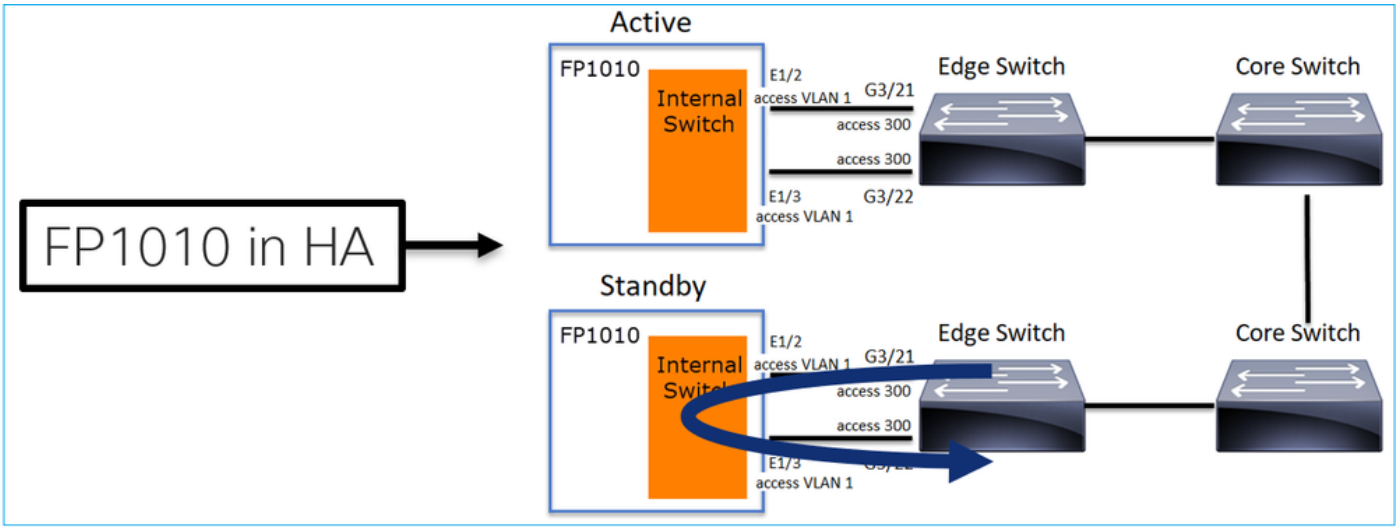
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1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

Comunicazione host-host e host-GW:



Considerazioni sulla progettazione di FP1010

Switching e alta disponibilità (HA)

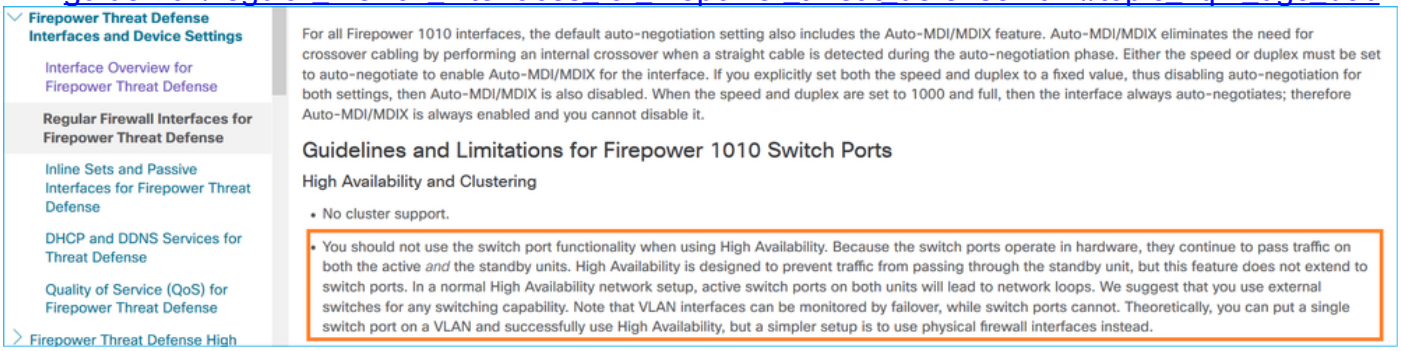


Esistono due problemi principali quando lo switching hardware è configurato in un ambiente HA:

1. HW Quando si accende l'unità di standby, i pacchetti vengono inoltrati attraverso il dispositivo. Questo può causare loop di traffico.
2. Le porte degli switch non sono monitorate da HA

Requisiti di progettazione

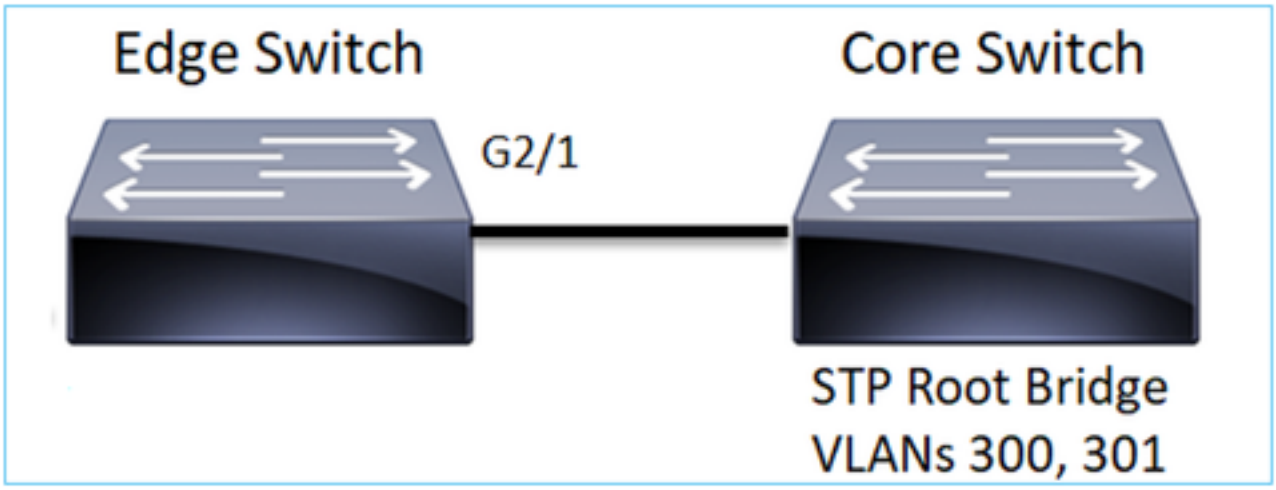
- Non utilizzare la funzionalità SwitchPort con ASA/FTD High Availability. Questa condizione è documentata nella guida alla configurazione del CCP: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b



Interazione con Spanning Tree Protocol (STP)

Lo switch interno FP1010 non esegue STP.

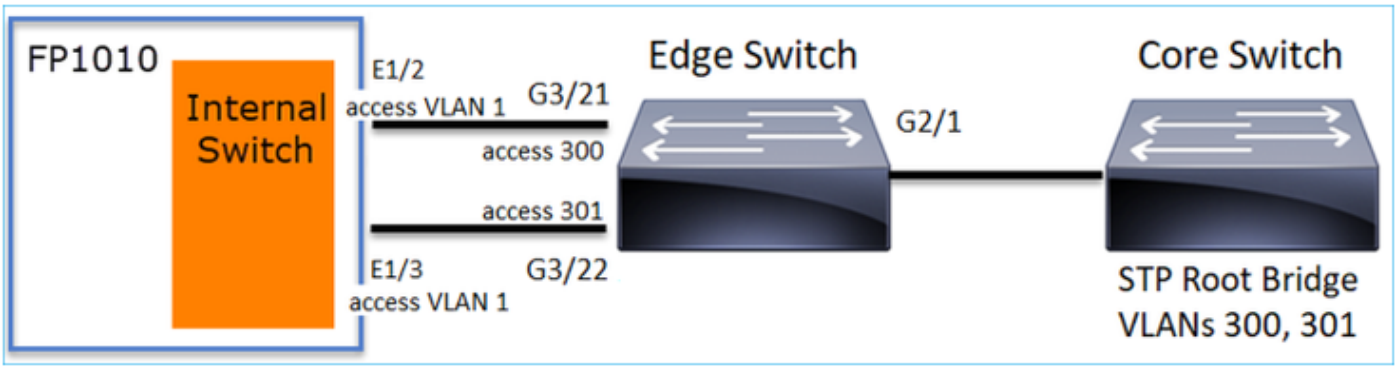
Considerare questo scenario:



Sullo switch perimetrale, la porta radice per entrambe le VLAN è 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
```

Collegare un FP1010 allo switch edge e configurare entrambe le porte nella stessa VLAN (switching hardware):



Il problema

- A causa di **perdite** di **VLAN**, BPDU superiori per la VLAN 301 ricevute il 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
```

Avviso: Se si collega uno switch L2 a FP1010, è possibile che il dominio STP

Questa condizione è documentata anche nella guida alla configurazione del CCP:

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 REST FMC

Queste sono le API REST per il supporto di questa funzione:

- Interfaccia fisica L2 [PUT/GET supportato]

/api/fmc_config/v1/domain/{domainUUID}/devices/devicerecords/{containerUID}/physical interfaces/{objectId}

- Interfaccia VLAN [Supported POST/PUT/GET/DELETE]

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

Risoluzione dei problemi/Diagnostica

Panoramica sulla diagnostica

- I file di log vengono acquisiti in un'operazione di risoluzione dei problemi FTD/NGIPS o nell'output show tech. Di seguito sono elencati gli elementi da cercare per ulteriori dettagli in caso di risoluzione dei problemi:
- /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

Raccogli dati da FXOS (dispositivo) - CLI

Nel caso di 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)#
```

Nel caso di 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)#
```

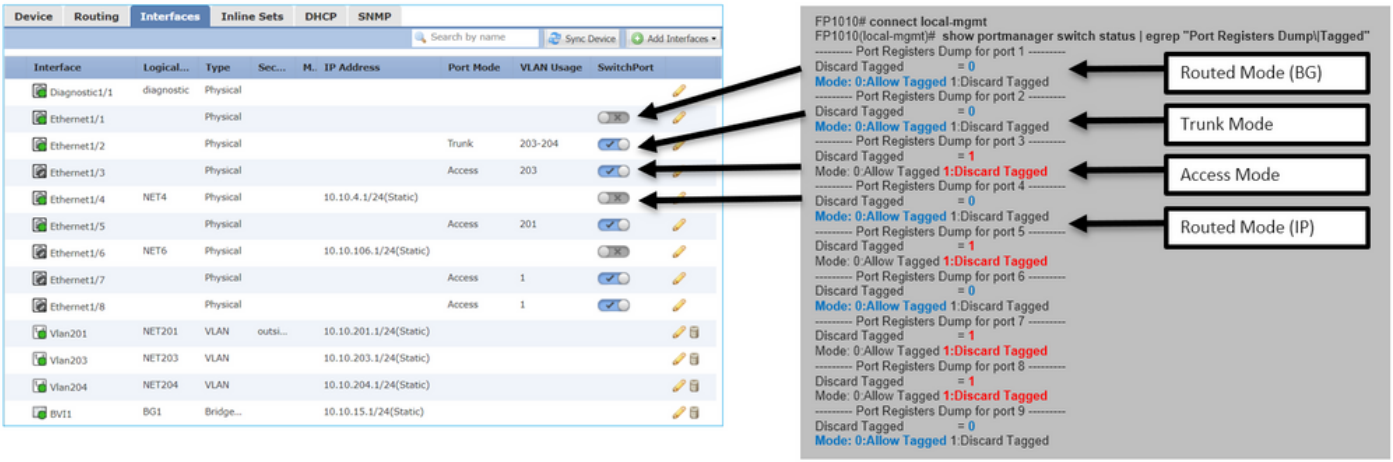
Back-end FP1010

I registri delle porte definiscono tutte le funzioni interne delle porte e degli switch.

In questa schermata viene mostrata la sezione 'Port Control' dei registri delle porte e in particolare il registro che determina se il traffico contrassegnato ricevuto sull'interfaccia deve essere scartato (1) o autorizzato (0). Di seguito è riportata la sezione completa del registro per una porta:

```
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 questa schermata è possibile vedere i vari valori di registro Discard Tagged per le varie modalità di porta:

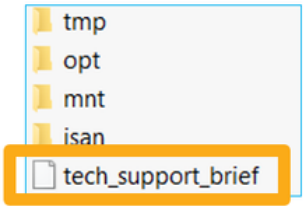


Raccogliere FPRM show tech su FP1010

Per generare un bundle FPRM e caricarlo su un server 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
```

Il bundle FPRM contiene un file denominato tech_support_brief. Il file tech_support_brief contiene una serie di comandi show. Uno di questi è lo **stato** dello **switch show portmanager**:



Dettagli su limitazioni, problemi comuni e soluzioni

Limitazioni dell'implementazione per la release 6.5

- I protocolli di routing dinamico non sono supportati per le interfacce SVI.
- Multi-context non supportato in 1010.
- La gamma di ID della VLAN SVI è limitata a 1-4070.
- Port-channel per L2 non supportato.
- La porta L2 come collegamento di failover non è supportata.

Limiti relativi alle funzioni dello switch

Funzionalità	Descrizione	Limite
Numero di interfacce VLAN	Numero totale di interfacce VLAN che possono essere create	60
VLAN modalità trunk	Numero massimo di VLAN consentite su una porta in modalità trunk	20
VLAN nativa	Esegue il mapping di tutti i pacchetti senza tag collegamento su una porta alla VLAN nativa configurata sulla porta	1
Interfacce denominate	Include tutte le interfacce denominate (interfaccia VLAN, sottointerfaccia, port-channel, interfaccia fisica, ecc.)	60

Altre limitazioni

- Le sottointerfacce e la VLAN di interfaccia non possono usare la stessa VLAN.
- Tutte le interfacce che partecipano a BVI devono appartenere alla stessa classe di interfacce.
- Èpossibile creare un BVI con una combinazione di porte in modalità L3 e sottointerfacce di porte in modalità L3.
- Èpossibile creare una BVI con una combinazione di VLAN di interfaccia.
- Non è possibile creare un BVI combinando porte in modalità L3 e VLAN di interfaccia.

Informazioni correlate

- Cisco Firepower 1010 Security Appliance
- Guide alla configurazione