Commutateur de couche 2 sur FPR1010, architecture, vérification et dépannage

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Informations générales](#)
[Compléments Firepower 6.5](#)
[Ajouts FMC](#)
[Comment ça fonctionne](#)
[Architecture FP1010](#)
[Traitement des paquets](#)
[Modes de port FP1010](#)
[FP1010 Cas 1. Ports routés (routage IP)](#)
[Cas 2 du FP1010. Mode Groupe de ponts (pontage)](#)
[FP1010 Cas 3. Ports de commutation (commutation matérielle) en mode d'accès](#)
[Filtrage du trafic intra-VLAN](#)
[FP1010 Cas 4. Ports de commutation (agrégation)](#)
[FP1010 Cas 5. Ports de commutation (inter-VLAN)](#)
[FP1010 Cas 6. Filtre inter-VLAN](#)
[Étude de cas - FP1010. Pontage contre commutation matérielle + pontage](#)
[Considérations relatives à la conception du FP1010](#)
[API REST FXOS](#)
[Dépannage/diagnostics](#)
[Présentation des diagnostics](#)
[Serveur principal FP1010](#)
[Collecter FPRM show tech sur FP1010](#)
[Détails des restrictions, problèmes courants et solutions de rechange](#)
[Informations connexes](#)

Introduction

Ce document décrit le commutateur L2 sur les périphériques FP1010. Plus précisément, il couvre principalement la partie de la mise en oeuvre de la plate-forme de services de sécurité (SSP)/Firepower eXtensive Operation System (FXOS). Dans la version 6.5, Firepower 1010 (modèle de bureau) a activé les fonctionnalités de commutation sur le commutateur matériel L2 intégré. Cela vous permet d'éviter des commutateurs matériels supplémentaires et de réduire les coûts.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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 votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

- FP1010 est un modèle de bureau SOHO (Small-Office Home-Office) qui remplace les plates-formes ASA5505 et ASA5506-X.
- Prise en charge logicielle des images FTD (6.4+) gérées par Firepower Management Center (FMC), Firepower Device Manager (FDM) ou Cloud Defense Orchestrator (CDO).
- Prise en charge logicielle des images ASA (9.13+) gérées par CSM, ASDM ou CLI.
- Le système d'exploitation (OS), ASA ou FTD, est fourni avec FXOS (similaire au FP21xx).
- 8 ports de données 10/100/1000 Mbits/s.
- Les ports E1/7 et E1/8 prennent en charge PoE+.
- Le commutateur matériel permet la communication de débit de ligne entre les ports (par exemple : un flux de caméra vers le serveur local).

Compléments Firepower 6.5

- Introduction d'un nouveau type d'interface appelé interface virtuelle commutée (SVI).
- Mode mixte : Les interfaces peuvent être configurées en mode commuté (L2) ou non commuté (L3).
- Les interfaces en mode L3 transmettent tous les paquets à l'application de sécurité.
- Les ports du mode L2 peuvent basculer dans le matériel si deux ports font partie du même VLAN, ce qui améliore le débit et la latence. Et les paquets qui doivent être routés ou pontés atteignent l'application de sécurité (par exemple : une caméra téléchargeant un nouveau micrologiciel depuis Internet) et subit une inspection de sécurité conformément à la configuration.
- L'interface physique de couche 2 peut être associée à une ou plusieurs interfaces SVI.
- Les interfaces du mode L2 peuvent être en mode d’accès ou d’agrégation.
- L'interface du mode d'accès L2 autorise uniquement le trafic non étiqueté.
- L’interface du mode d’agrégation L2 autorise le trafic étiqueté.
- Prise en charge du VLAN natif pour l'interface de couche 2 du mode d'agrégation.

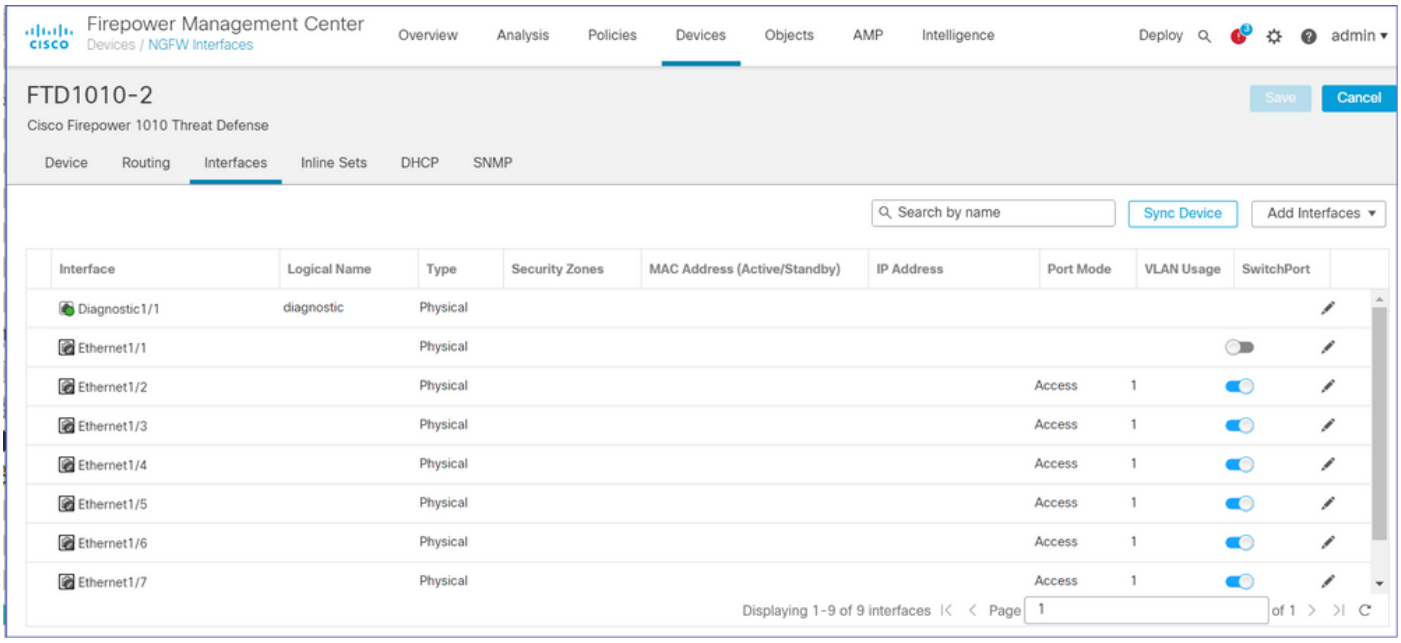
- Les CLI ASA, ASDM, CSM, FDM et FMC sont améliorés pour prendre en charge de nouvelles fonctionnalités.

Ajouts FMC

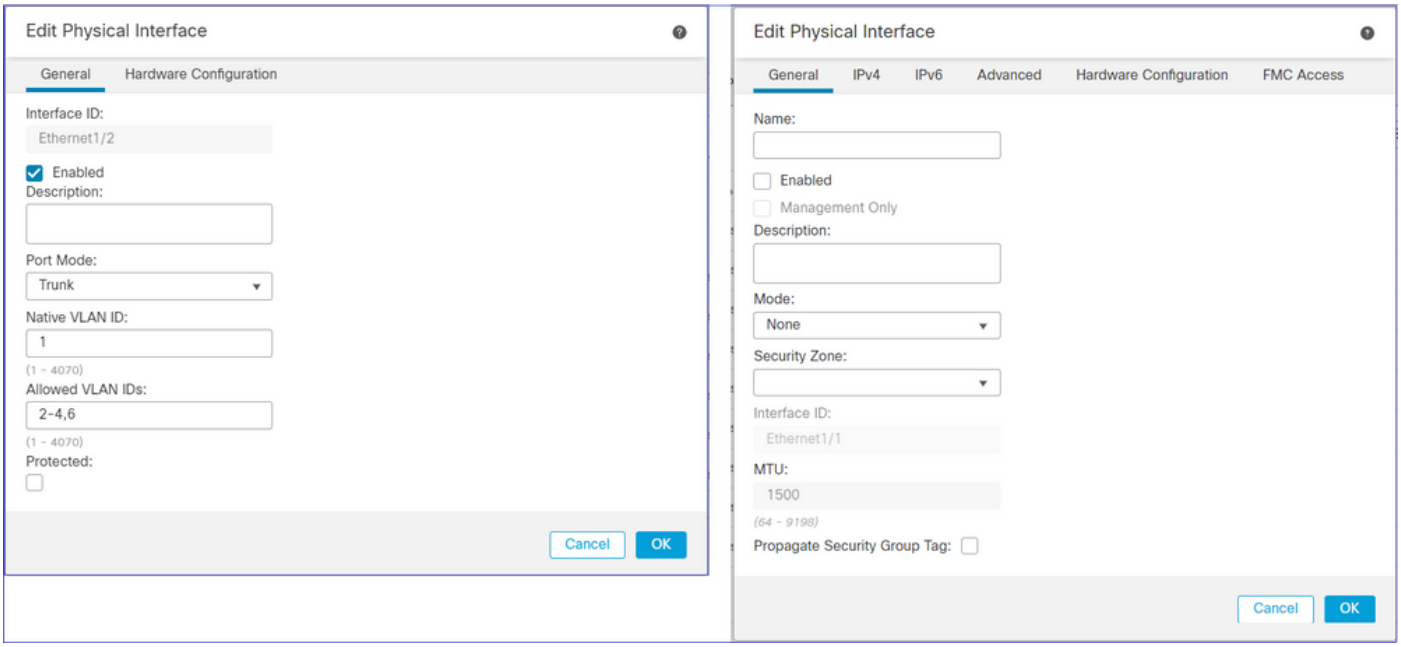
- Un nouveau mode d'interface appelé switchport a été introduit pour une interface physique qui est utilisée pour identifier si une interface physique est une interface L3 ou L2.
- L'interface physique de couche 2 peut être associée à une ou plusieurs interfaces VLAN en fonction du mode d'accès ou d'agrégation.
- Firepower 1010 prend en charge la configuration PoE (Power Over Ethernet) sur les deux dernières interfaces de données, à savoir Ethernet1/7 et Ethernet1/8.
- Le changement d'interface entre les commutateurs et les non-commutateurs efface toutes les configurations, à l'exception de la configuration PoE et matérielle.

Comment ça fonctionne

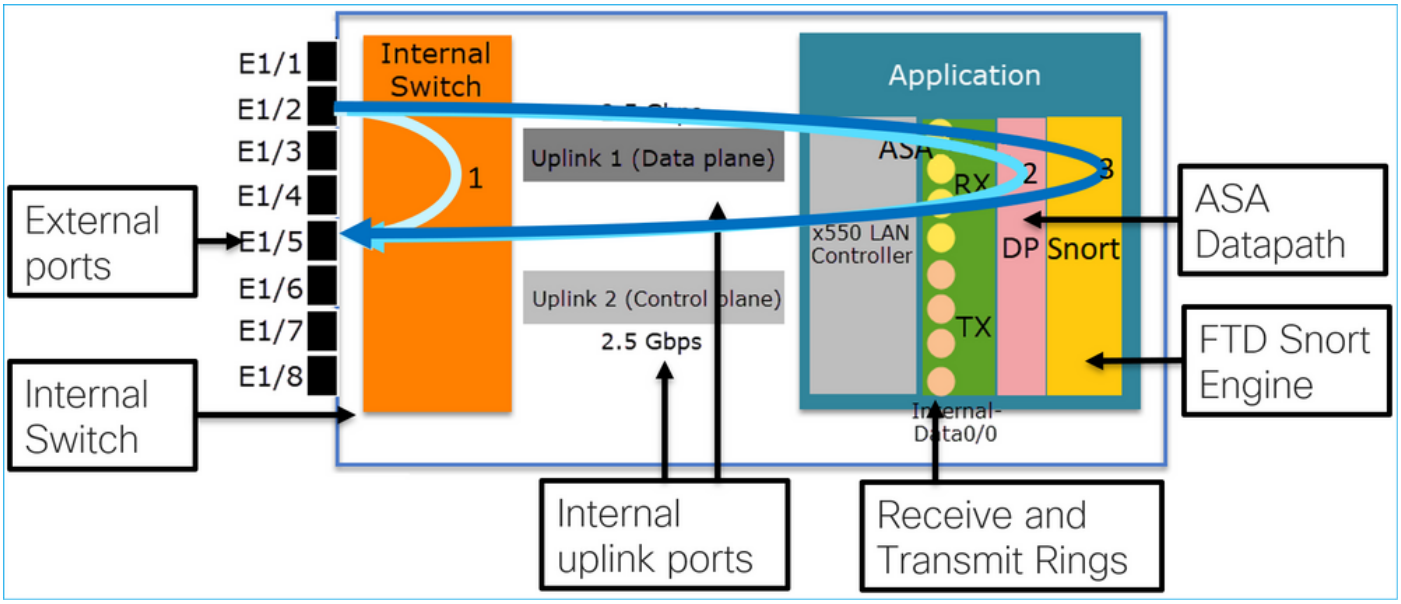
Cette fonctionnalité n'est qu'une amélioration de la prise en charge d'interface existante sur FMC (**Device Management > Interface Page**).



Vue de l'interface physique (L2 et L3)



Architecture FP1010



- 8 ports de données externes.
- 1 commutateur interne.
- 3 ports de liaison ascendante (dont 2 sur l'image), un pour le plan de données, un pour le plan de contrôle, un pour la configuration.
- Contrôleur de réseau local x550 (interface entre l'application et les liaisons ascendantes).
- 4 sonneries de réception (RX) et 4 sonneries de transmission (TX).
- Processus de chemin de données (sur ASA et FTD).
- Snort process (sur FTD).

Traitement des paquets

Deux facteurs principaux peuvent affecter le traitement des paquets :

1. Mode interface/port

2. Stratégie appliquée

Un paquet peut traverser un FP1010 de trois manières différentes :

1. Uniquement traité par le commutateur interne

2. Transféré jusqu'à l'application (ASA/FTD) et traité uniquement par le processus de chemin de données

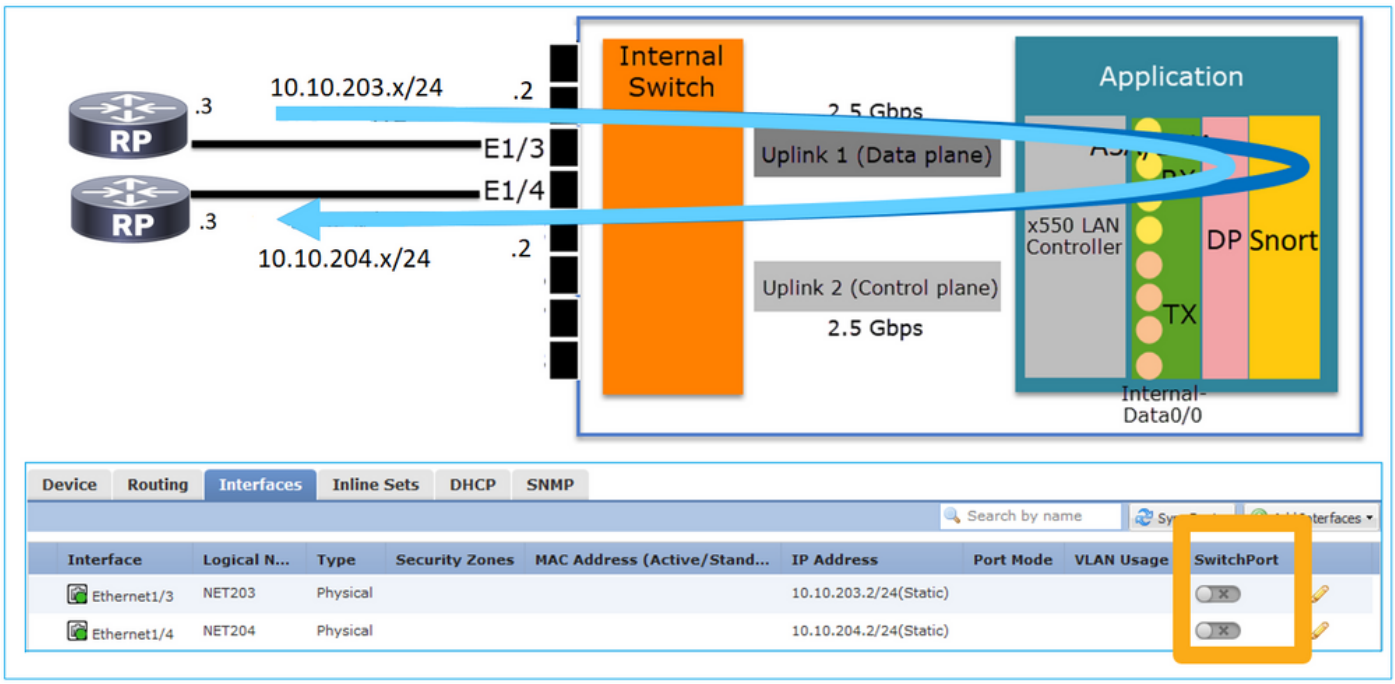
3. Transféré jusqu'à l'application (FTD) et traité par le chemin de données et le moteur Snort

Modes de port FP1010

Les exemples d'interface utilisateur sont pour FMC, les exemples CLI sont pour FTD. La plupart des concepts sont également entièrement applicables à un ASA.

FP1010 Cas 1. Ports routés (routage IP)

Configuration et fonctionnement



Points clés

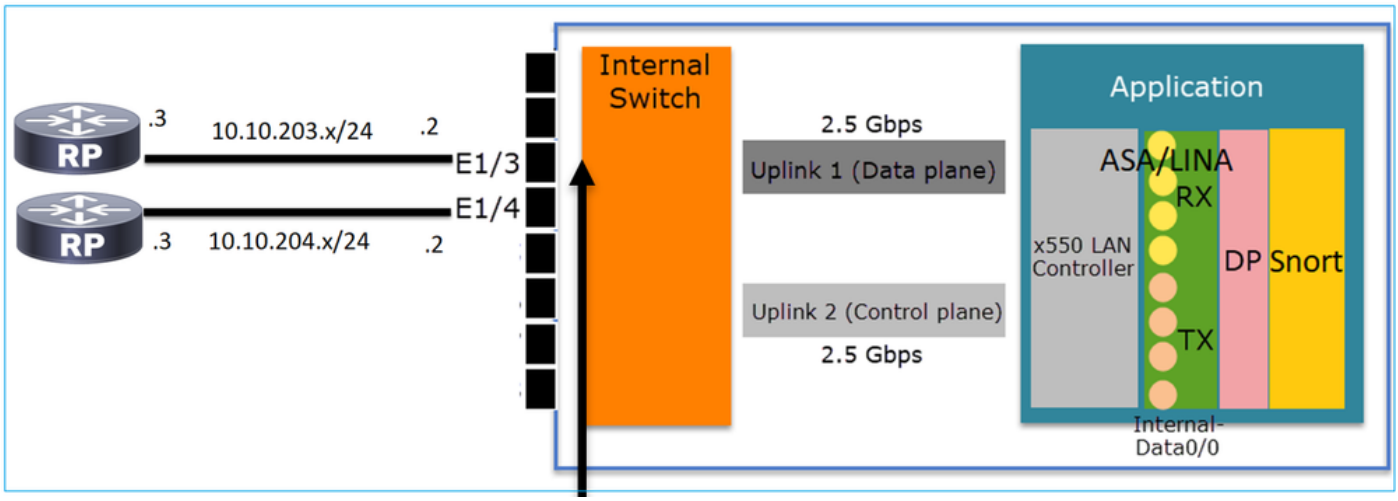
- Du point de vue de la conception, les 2 ports appartiennent à 2 sous-réseaux L2 différents.
- Lorsque les ports sont configurés en mode routé, les paquets sont traités par l'application (ASA ou FTD).
- Dans le cas de FTD, en fonction de l'action de la règle (par exemple, ALLOW), les paquets peuvent même être inspectés par le moteur Snort.

Configuration de l'interface 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
```

Vérification du port routé FP1010



Àpartir de l'interface de ligne de commande FXOS, vous pouvez vérifier les compteurs d'interface physique. Cet exemple montre les compteurs de monodiffusion d'entrée et de sortie sur le port 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
```

Les captures de chemin de données FTD peuvent être appliquées et les paquets peuvent être suivis :

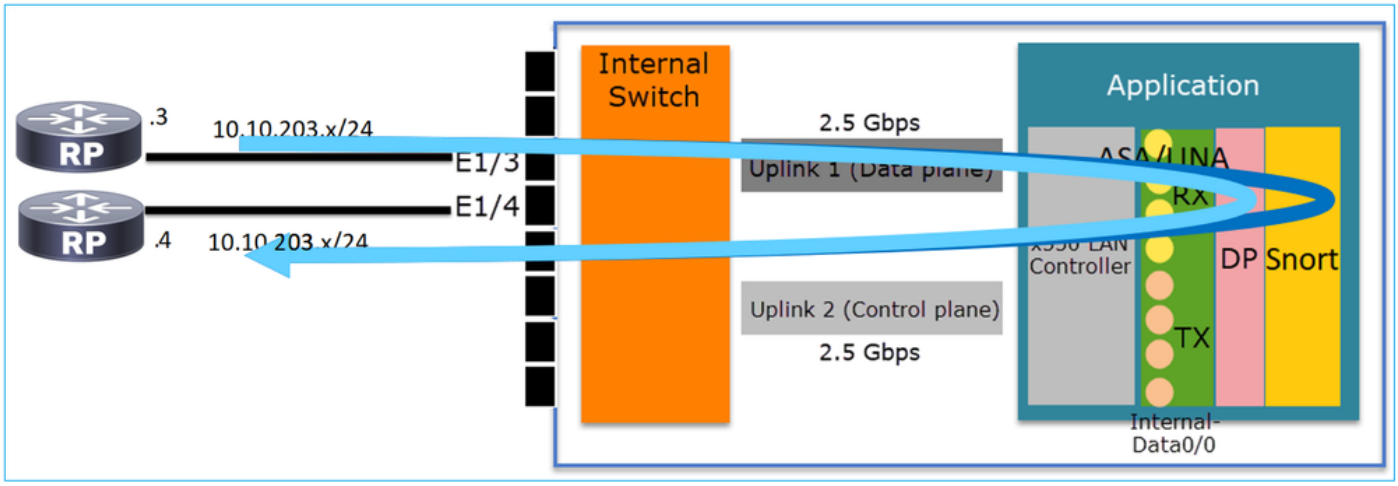
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

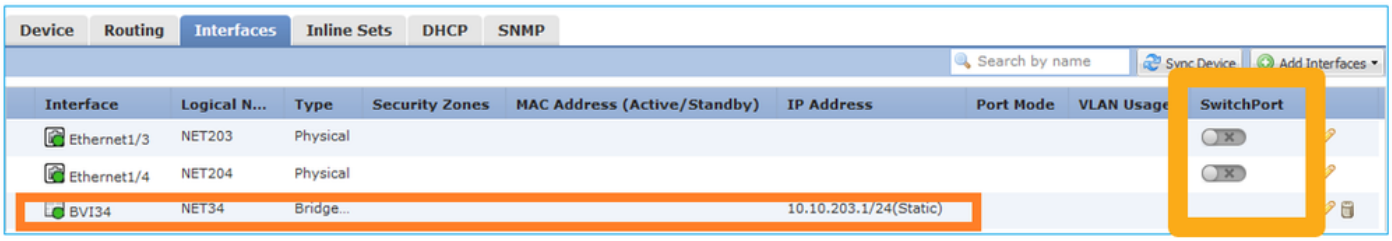
Voici un extrait de capture. Comme prévu, le paquet est transféré en fonction d'une RECHERCHE DE ROUTE :

```
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
```

Cas 2 du FP1010. Mode Groupe de ponts (pontage)

Configuration et fonctionnement





Points clés

- Du point de vue de la conception, les 2 ports sont connectés au même sous-réseau de couche 3 (similaire à un pare-feu transparent), mais à un VLAN différent.
- Lorsque les ports sont configurés en mode pontage, les paquets sont traités par l'application (ASA ou FTD).
- Dans le cas de FTD, en fonction de l'action de la règle (par exemple, ALLOW), les paquets peuvent même être inspectés par le moteur Snort.

Configuration de l'interface 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
```

Vérification du port du groupe de ponts FP1010

Cette commande affiche les membres d'interface 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
```

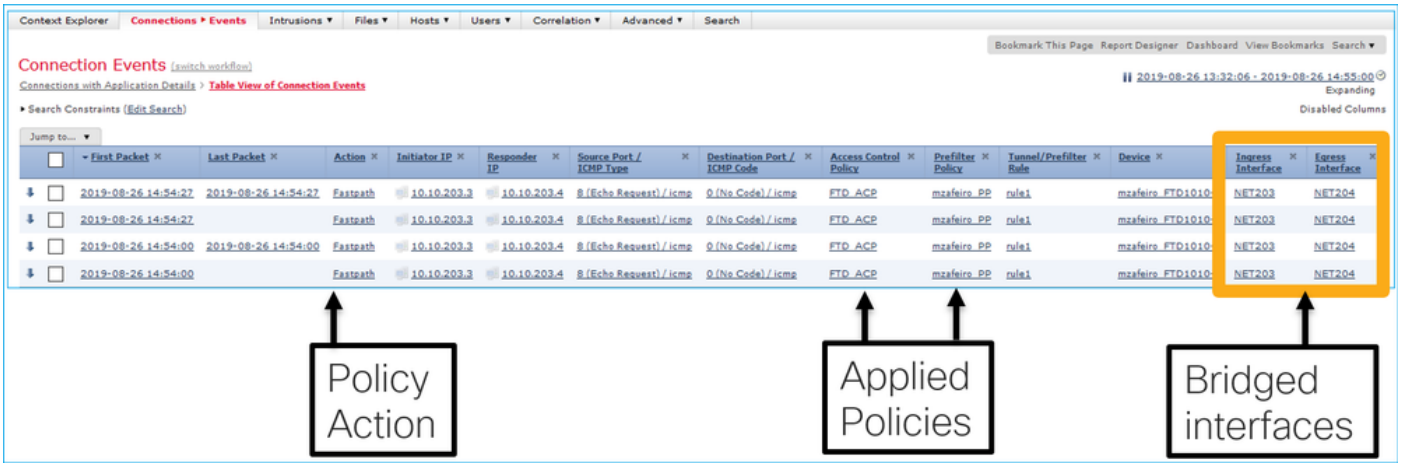
Cette commande affiche la table CAM (Content Addressable Memory) ASA/FTD :

```
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 extrait de trace de paquet indique que le paquet est transféré en fonction de la recherche de couche 2 MAC de destination :

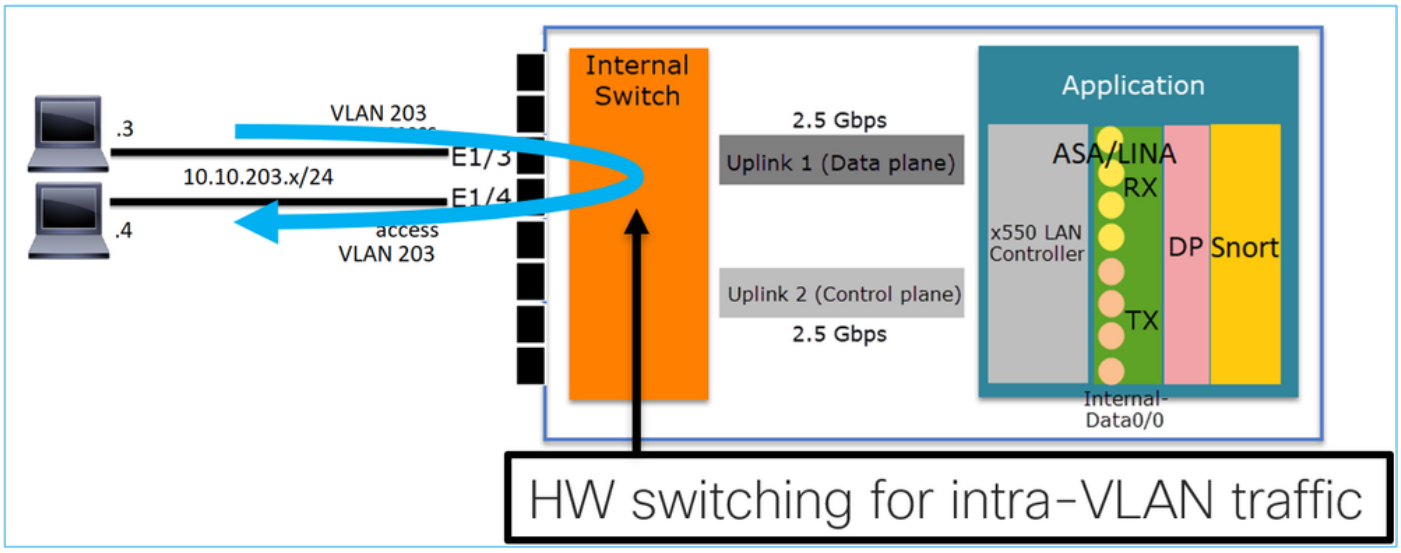
```
FP1010# show cap CAP203 packet-number 1 trace

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
```

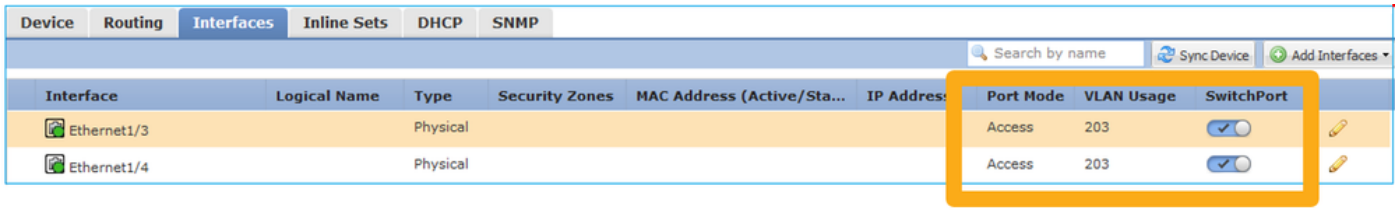
Dans le cas de FTD, les événements de connexion FMC peuvent également fournir des informations sur l'inspection de flux et les interfaces de groupe de ponts de transit :



FP1010 Cas 3. Ports de commutation (commutation matérielle) en mode d'accès

Configuration et fonctionnement





Points clés

- La commutation matérielle est une fonctionnalité FTD **6.5+** et ASA **9.13+**.
- Du point de vue de la conception, les 2 ports sont connectés au même sous-réseau de couche 3 et au même VLAN.
- Les ports de ce scénario fonctionnent en mode Accès (trafic non étiqueté uniquement).
- Les ports de pare-feu configurés en mode SwitchPort n'ont pas de nom logique (nom) configuré.
- Lorsque les ports sont configurés en mode de commutation et appartiennent au même VLAN (trafic intra-VLAN), les paquets sont traités uniquement par le commutateur interne FP1010.

Configuration de l'interface FTD

Du point de vue de l'interface de ligne de commande, la configuration ressemble beaucoup à celle d'un commutateur de couche 2 :

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

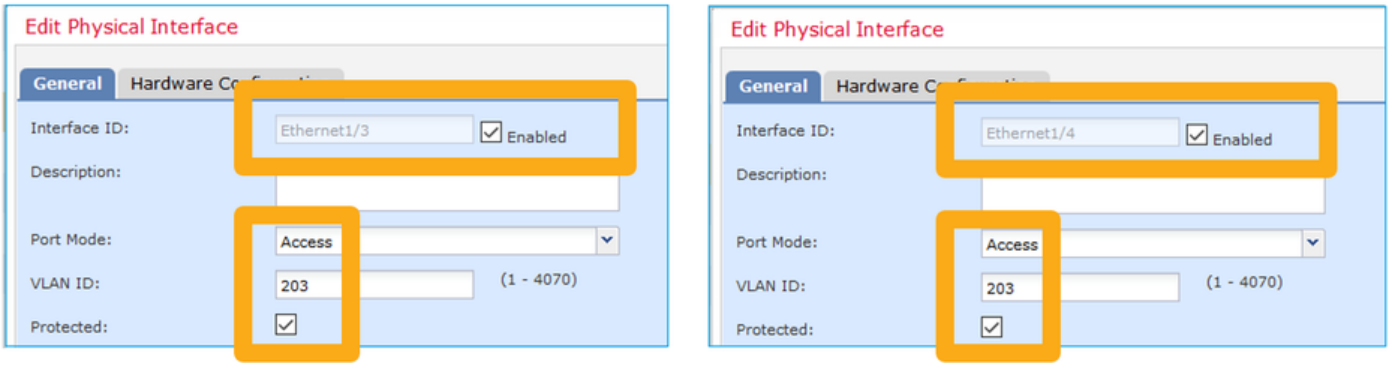
Filtrage du trafic intra-VLAN

Le défi : **Une liste de contrôle d'accès ne peut pas filtrer le trafic intra-VLAN !**

La solution : Ports **protégés**

Le principe est très simple : 2 ports configurés en tant que Protected ne peuvent pas communiquer entre eux.

Interface utilisateur FMC en cas de ports protégés :



Configuration de l'interface FTD

La commande **switchport protected** est configurée sous l'interface :

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

Vérification du port de commutation FP1010

Dans cet exemple, 1 000 paquets de monodiffusion (ICMP) sont envoyés avec une taille spécifique (1 100 octets) :

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

Pour vérifier les compteurs de monodiffusion d'entrée et de sortie des interfaces de transit, utilisez cette commande :

```
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
```

Cette commande affiche l'état du VLAN du commutateur interne :

```
FP1010# show switch vlan
```

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

L'état d'un VLAN est UP tant qu'au moins un port est attribué au VLAN

Si un port est désactivé par l'administrateur ou si le port de commutateur connecté est désactivé/déconnecté par câble et qu'il s'agit du seul port attribué au VLAN, l'état du VLAN est également désactivé :

```
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
```

Cette commande affiche la table CAM du commutateur interne :

```
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
```

La durée de vieillissement par défaut de la table CAM du commutateur interne est de 5 min 30 s.

FP1010 contient 2 tables CAM :

1. **Table CAM interne du commutateur** : Utilisé en cas de commutation matérielle
2. **Table CAM du chemin de données ASA/FTD** : Utilisé en cas de pontage

Chaque paquet/trame traversant le FP1010 est traité par une seule table CAM (commutateur interne ou chemin de données FTD) basée sur le mode de port.

> **Attention** : Ne confondez pas la table CAM interne du commutateur **show switch mac-address-table** utilisée en mode SwitchPort avec la table CAM **show mac-address-table** FTD datapath utilisée en mode ponté

Commutation matérielle : Autres éléments à prendre en compte

Les journaux de chemin de données ASA/FTD n'affichent pas d'informations sur les flux commutés matériel :

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

La table de connexion de chemin de données ASA/FTD n'affiche pas les flux commutés matériel :

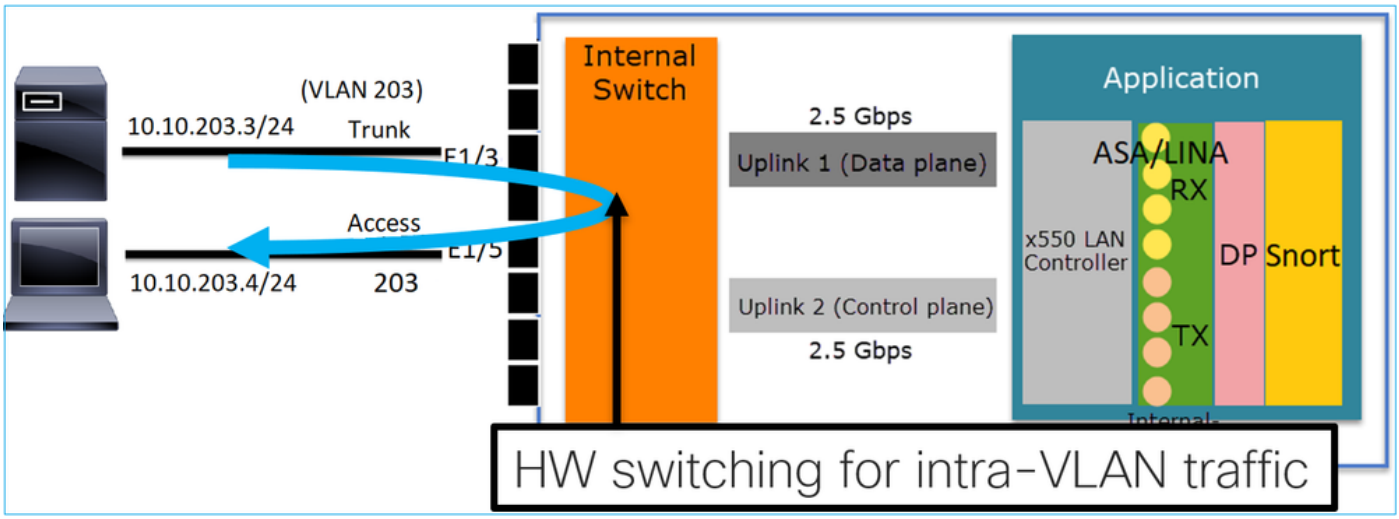
```
FP1010# show conn
0 in use, 3 most used
Inspect Snort:
```

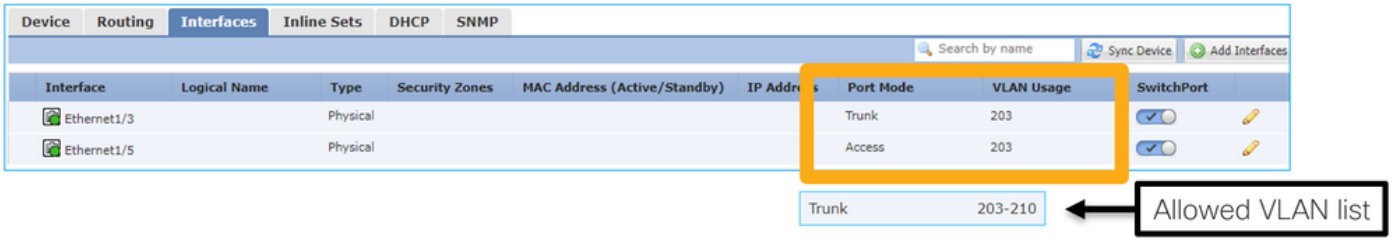
```
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

En outre, les événements de connexion FMC n'affichent pas de flux commutés matériel.

FP1010 Cas 4. Ports de commutation (agrégation)

Configuration et fonctionnement





Points clés

- La commutation matérielle est une fonctionnalité FTD **6.5+** et ASA **9.13+**.
- Du point de vue de la conception, les 2 ports sont connectés au même sous-réseau de couche 3 et au même VLAN.
- Le port agrégé accepte les trames étiquetées et non étiquetées (dans le cas d'un VLAN natif).
- Lorsque les ports sont configurés en mode de commutation et appartiennent au même VLAN (trafic intra-VLAN), les paquets sont traités uniquement par le commutateur interne.

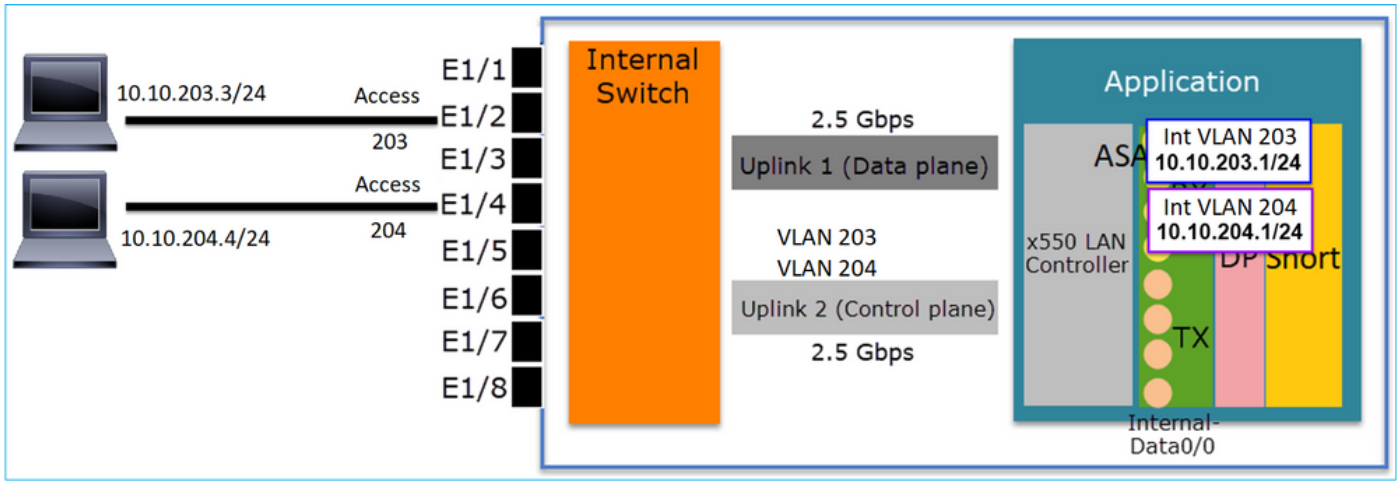
Configuration de l'interface FTD

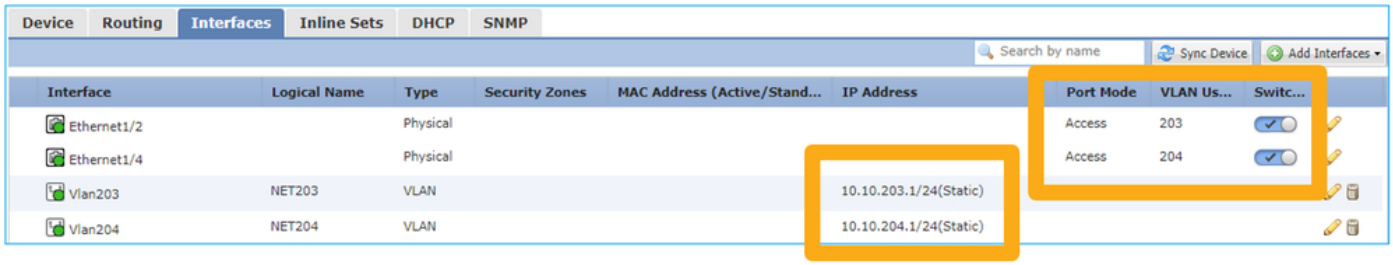
La configuration est similaire à celle d'un port de commutateur de couche 2 :

```
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 Cas 5. Ports de commutation (inter-VLAN)

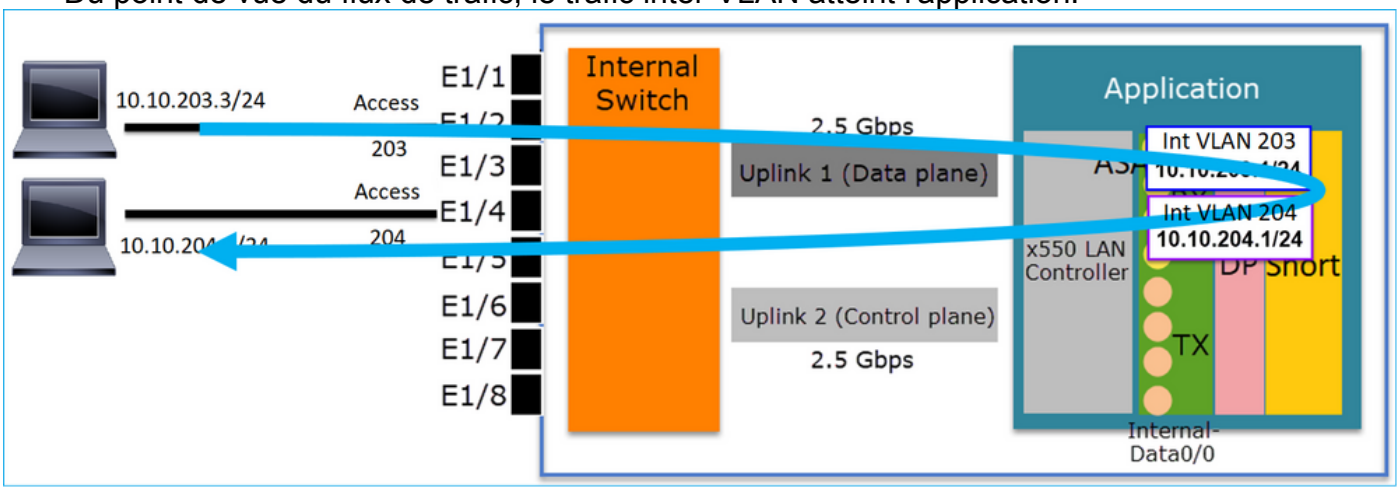
Configuration et fonctionnement





Points clés

- Du point de vue de la conception, les 2 ports sont connectés à 2 sous-réseaux L3 différents et 2 VLAN différents.
- Le trafic entre les VLAN passe par les interfaces VLAN (similaires aux SVI).
- Du point de vue du flux de trafic, le trafic inter-VLAN atteint l'application.



Configuration de l'interface FTD

La configuration est similaire à une interface virtuelle de commutateur (SVI) :

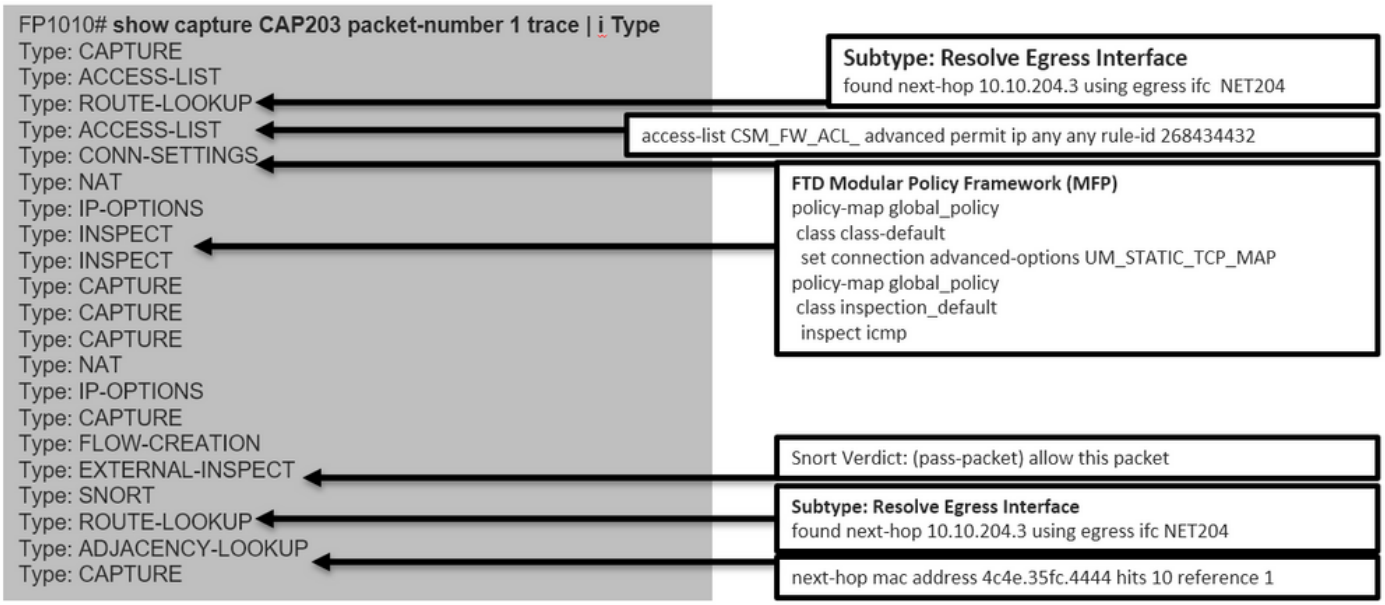
```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

Traitement des paquets pour le trafic entre VLAN

Il s’agit d’une trace d’un paquet qui traverse deux VLAN différents :

```
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
```

Les principales phases du processus de paquet :



FP1010 Cas 6. Filtre inter-VLAN

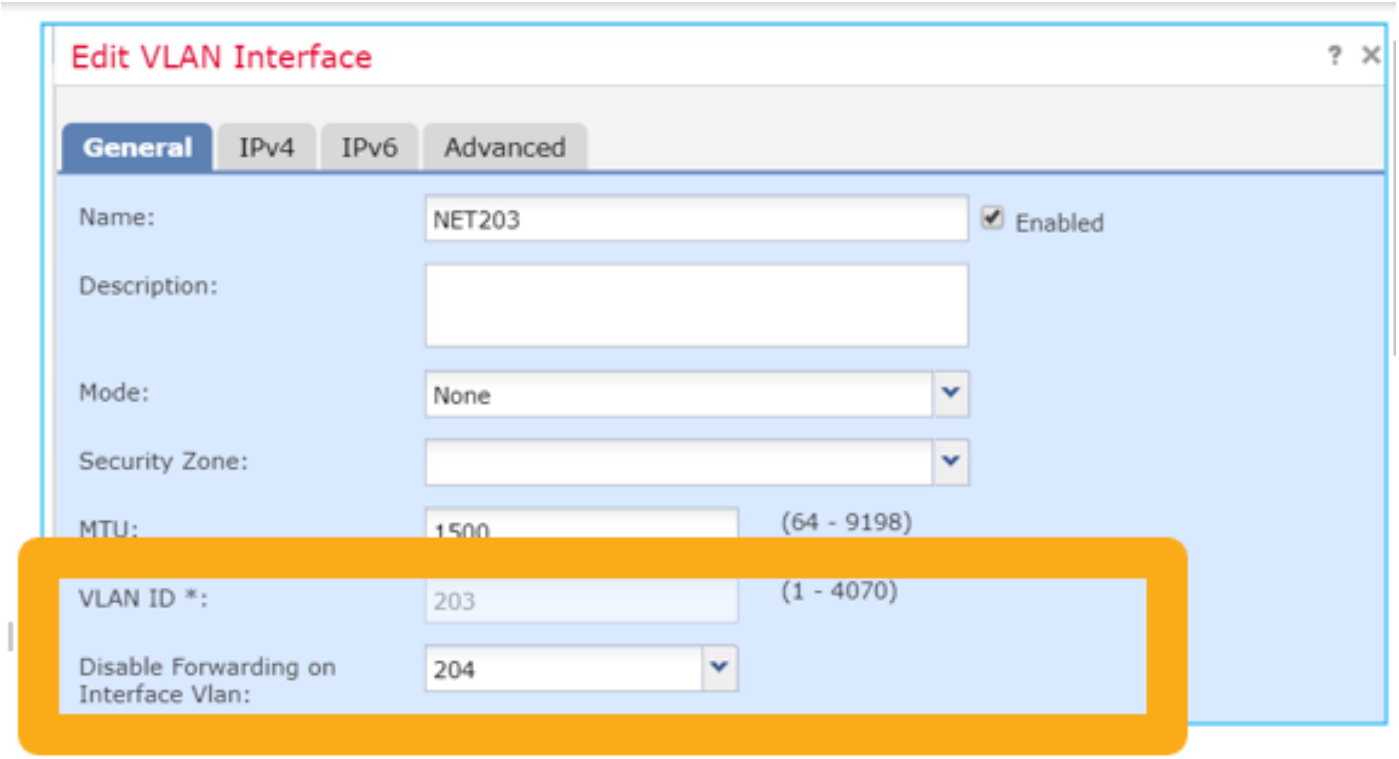
Configuration et fonctionnement

Il existe deux options principales pour filtrer le trafic entre VLAN :

1. Stratégie de contrôle d'accès
2. **no forward**, commande

Filtrer le trafic inter-VLAN à l'aide de la commande 'no forward'

Configuration de l'interface FMC :



Points clés

- La liste déroulante no forward est unidirectionnelle.
- Il ne peut pas être appliqué aux deux interfaces VLAN.
- La vérification no forward est effectuée avant la vérification de la liste de contrôle d'accès.

Configuration de l'interface FTD

Dans ce cas, la configuration CLI est la suivante :

```
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
```

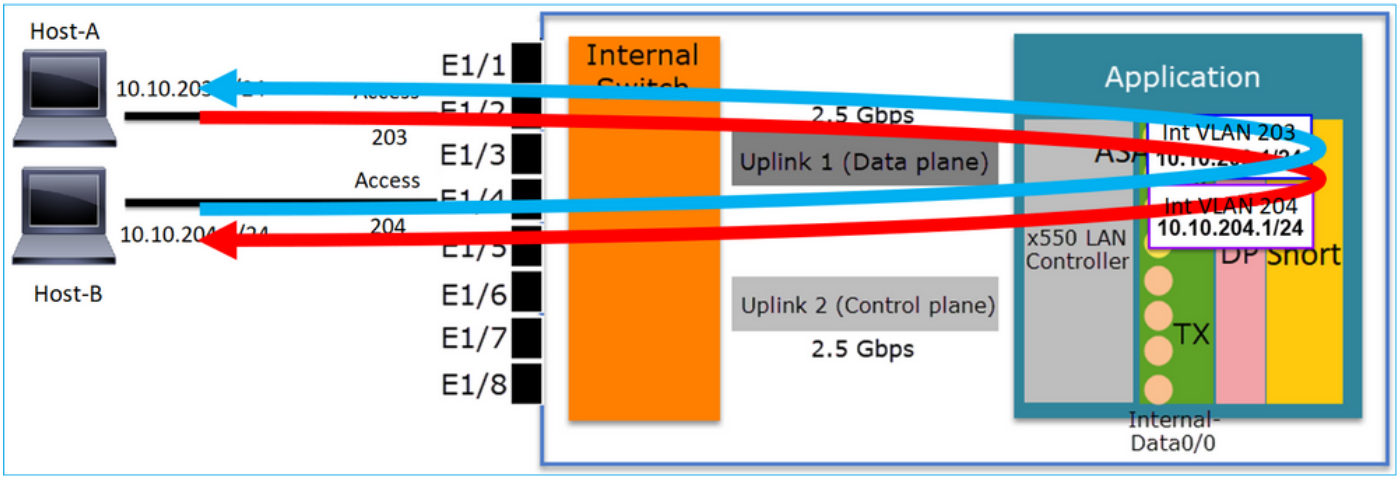
Si un paquet est abandonné par la fonction no forward, un message Syslog de chemin de données ASA/FTD est généré :

```
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)
```

Du point de vue de l'accélération du chemin de sécurité (ASP), il est considéré comme une perte de liste de contrôle d'accès :

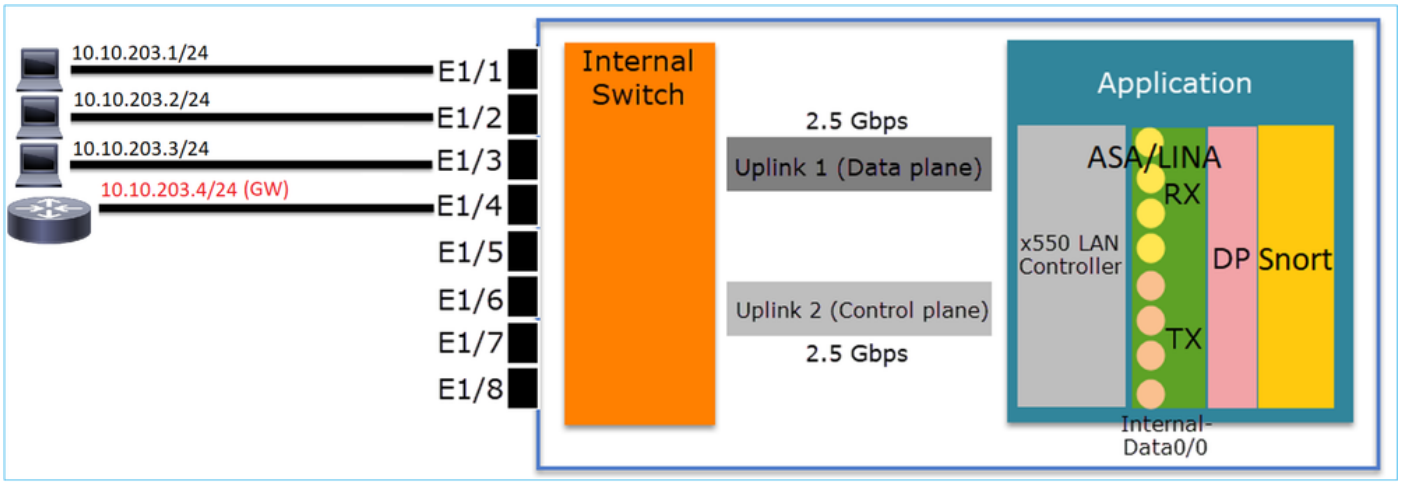
```
FP1010-2# show asp drop
Frame drop:
Flow is denied by configured rule (acl-drop) 1
```

Puisque la perte est unidirectionnelle, l'hôte A (VLAN 203) ne peut pas initier le trafic vers l'hôte B (VLAN 204), mais le contraire est autorisé :



Étude de cas - FP1010. Pontage contre commutation matérielle + pontage

Considérez la topologie suivante :



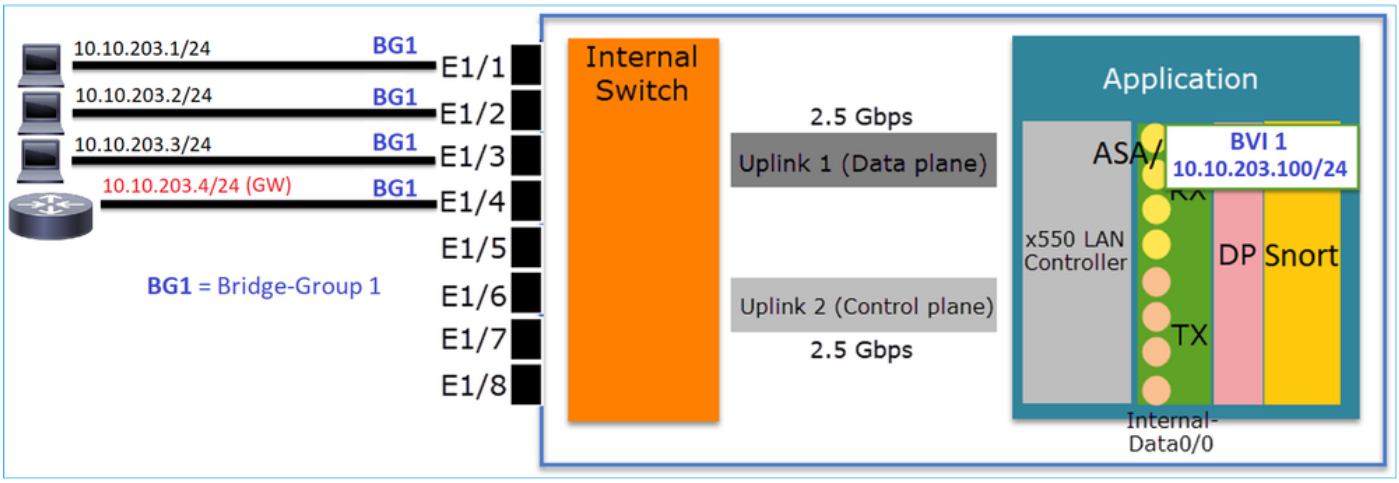
Dans cette topologie :

- Trois hôtes finaux appartiennent au même sous-réseau de couche 3 (10.10.203.x/24).
- Le routeur (10.10.203.4) agit en tant que GW dans le sous-réseau.

Dans cette topologie, il existe deux principales options de conception :

1. Pontage
2. Commutation matérielle + pontage

Option de conception 1. Pontage

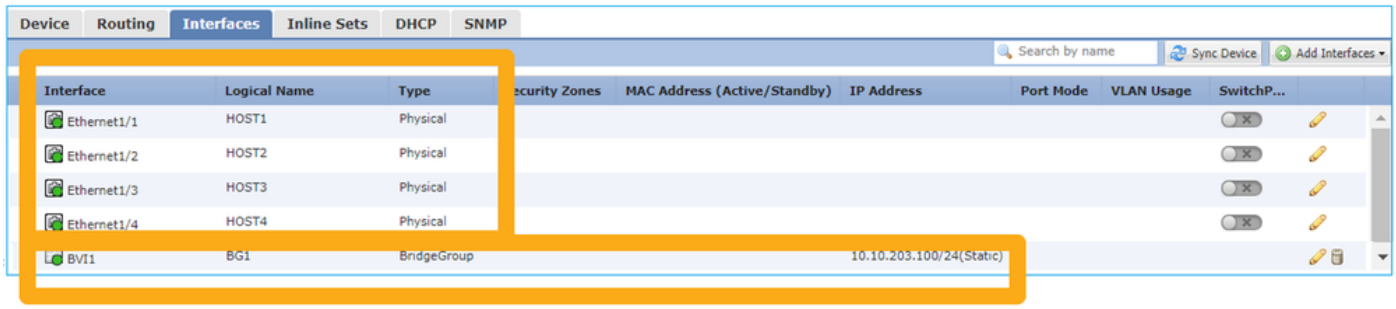


Points clés

Les principaux points de cette conception sont les suivants :

- BVI 1 est créé avec une adresse IP dans le même sous-réseau (10.10.203.x/24) que les 4 périphériques connectés.
- Les quatre ports appartiennent au même groupe de ponts (groupe 1 dans ce cas).
- Chacun des quatre ports a un nom configuré.
- La communication hôte-hôte et hôte-GW passe par l'application (par exemple, FTD).

Du point de vue de l'interface FMC, la configuration est la suivante :

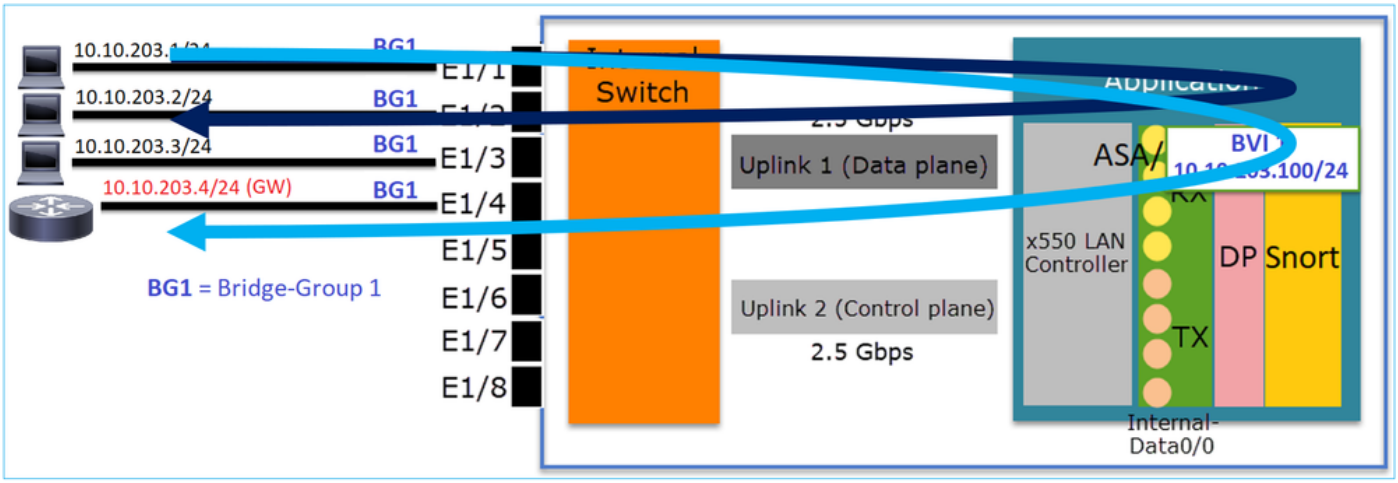


Configuration de l'interface FTD

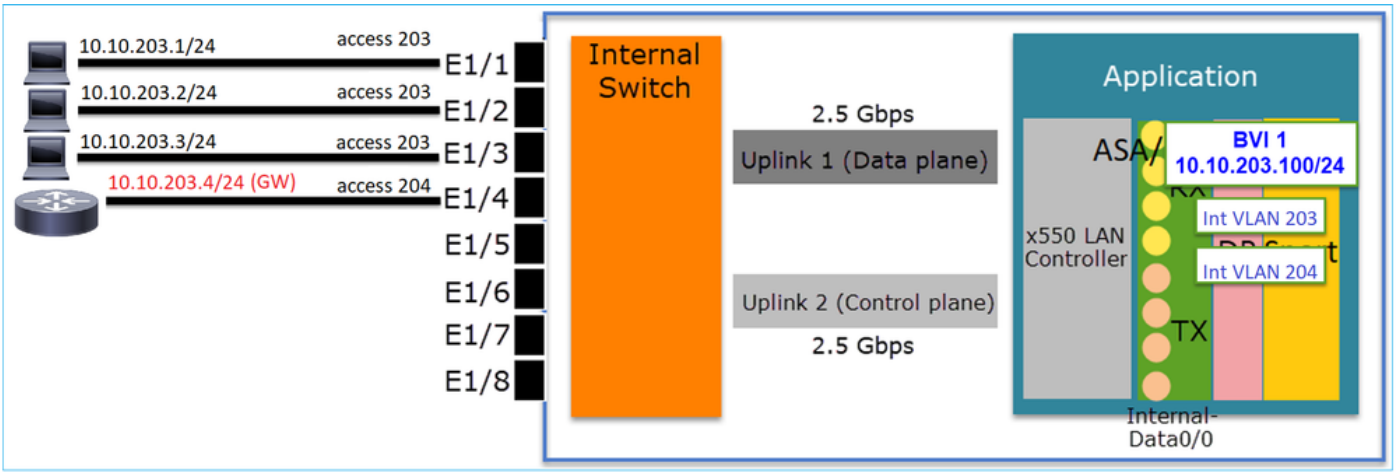
Dans ce cas, la configuration est la suivante :

```
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
```

Flux de trafic dans ce scénario :



Option de conception 2. Commutation matérielle + pontage

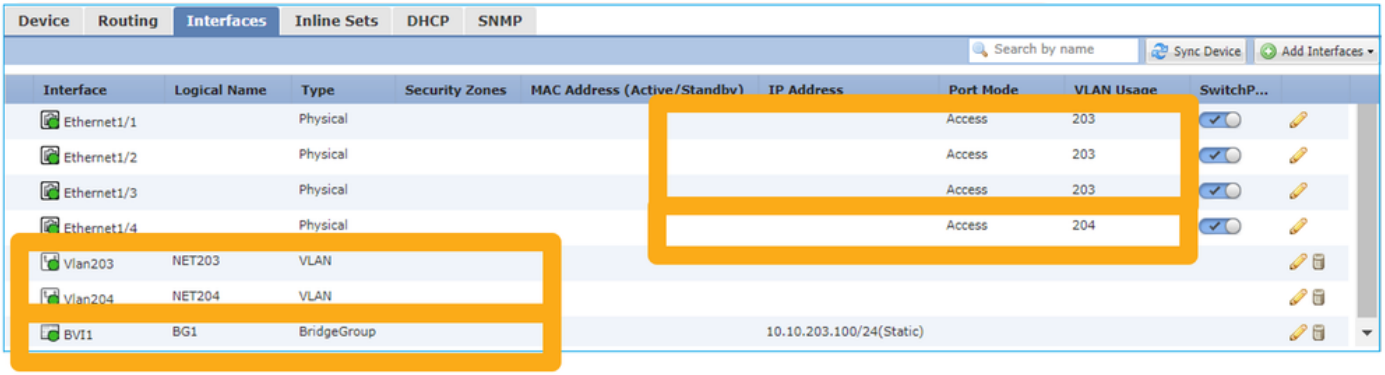


Points clés

Les principaux points de cette conception sont les suivants :

- BVI 1 est créé avec une adresse IP dans le même sous-réseau (10.10.203.x/24) que les 4 périphériques connectés.
- Les ports connectés aux hôtes finaux sont configurés en mode SwitchPort et appartiennent au même VLAN (203).
- Le port connecté au GW est configuré en mode SwitchPort et appartient à un autre VLAN (204).
- Il existe 2 interfaces VLAN (203, 204). Les 2 interfaces VLAN n'ont pas d'adresse IP attribuée et appartiennent au groupe de ponts 1.
- La communication hôte-hôte passe uniquement par le commutateur interne.
- La communication hôte-GW passe par l'application (par exemple, FTD).

Configuration de l'interface utilisateur FMC :

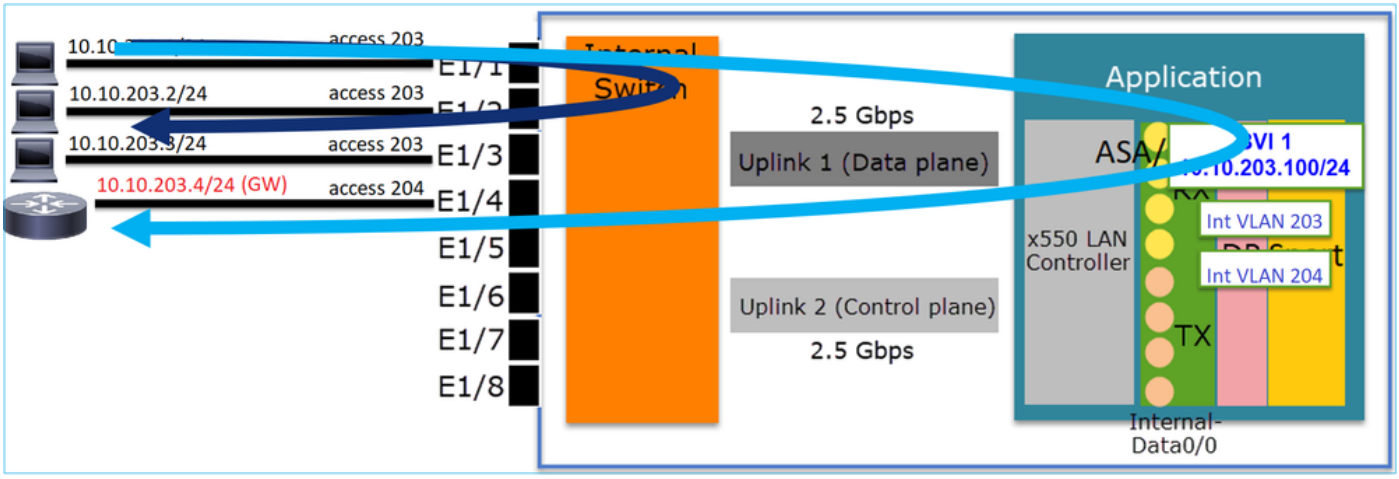


Configuration de l'interface FTD

Dans ce cas, la configuration est la suivante :

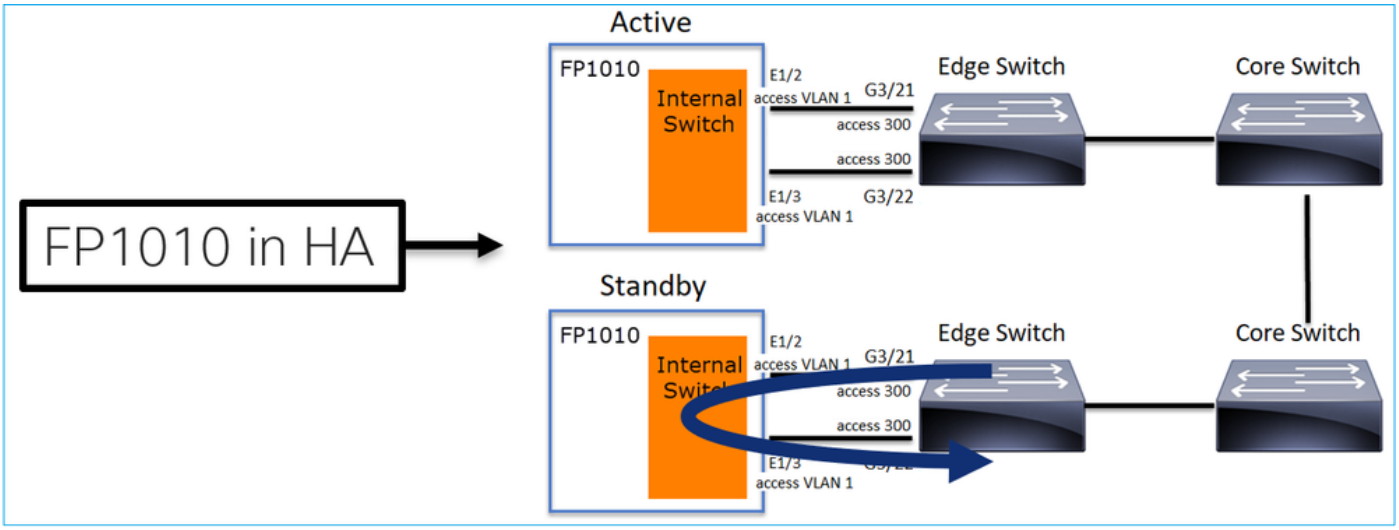
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1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

Communication hôte-hôte et communication hôte-GW :



Considérations relatives à la conception du FP1010

Commutation et haute disponibilité (HA)

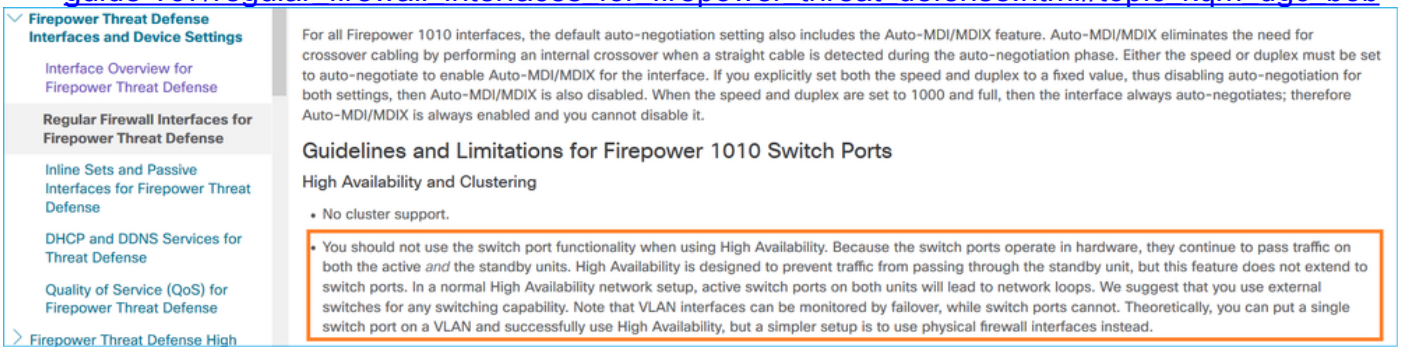


Deux problèmes principaux se posent lorsque la commutation matérielle est configurée dans un environnement haute disponibilité :

1. La commutation matérielle sur l'unité de secours transfère les paquets via le périphérique. Cela peut entraîner des boucles de trafic.
2. Les ports de commutation ne sont pas surveillés par HA

Exigences de conception

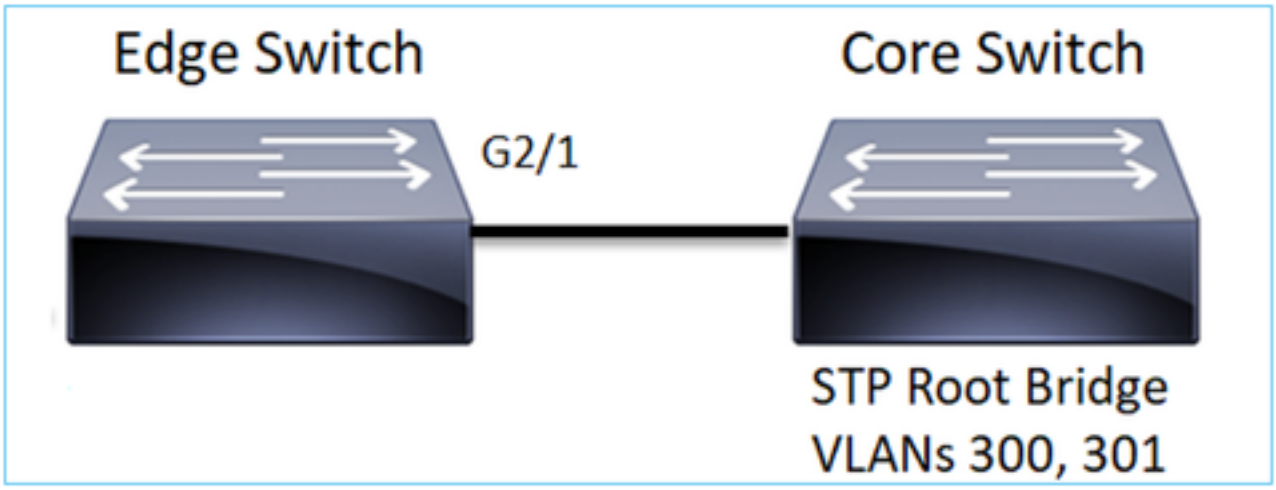
- Vous ne devez pas utiliser la fonctionnalité SwitchPort avec la haute disponibilité ASA/FTD. Ceci est documenté dans le guide de configuration FMC : https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b



Interaction avec le protocole STP (Spanning Tree Protocol)

Le commutateur interne FP1010 n'exécute pas STP.

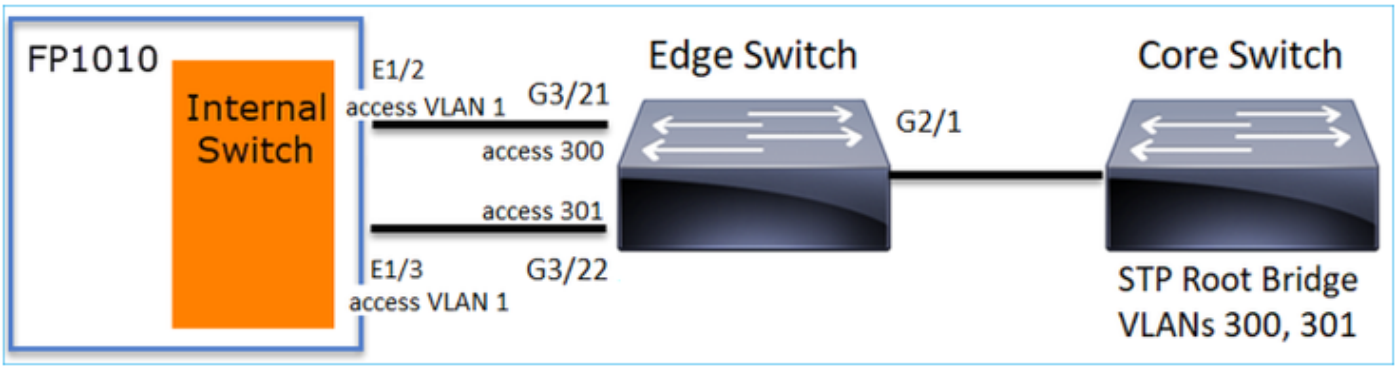
Considérez ce scénario:



Sur le commutateur Edge, le port racine des deux VLAN est 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
```

Connectez un FP1010 au commutateur de périphérie et configurez les deux ports dans le même VLAN (commutation matérielle) :



Le problème

- En raison d'une **fuite de** BPDU supérieure **VLAN** pour VLAN 301 reçu sur 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
```

> **Avertissement :** Si vous connectez un commutateur L2 au FP1010, vous pouvez affecter le domaine STP

Ceci est également documenté dans le guide de configuration 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 REST FMC

Voici les API REST pour cette prise en charge des fonctionnalités :

- Interface physique de couche 2 [PUT/GET pris en charge]

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

- Interface VLAN [POST/PUT/GET/DELETE pris en charge]

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

Dépannage/diagnostics

Présentation des diagnostics

- Les fichiers journaux sont capturés dans un dépannage FTD/NGIPS ou dans la sortie show tech. Voici les éléments à rechercher pour plus de détails en cas de dépannage :
- /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

Collecte de données à partir de FXOS (périphérique) - CLI

Dans le cas 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)#
```

Dans le cas de 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)#
```

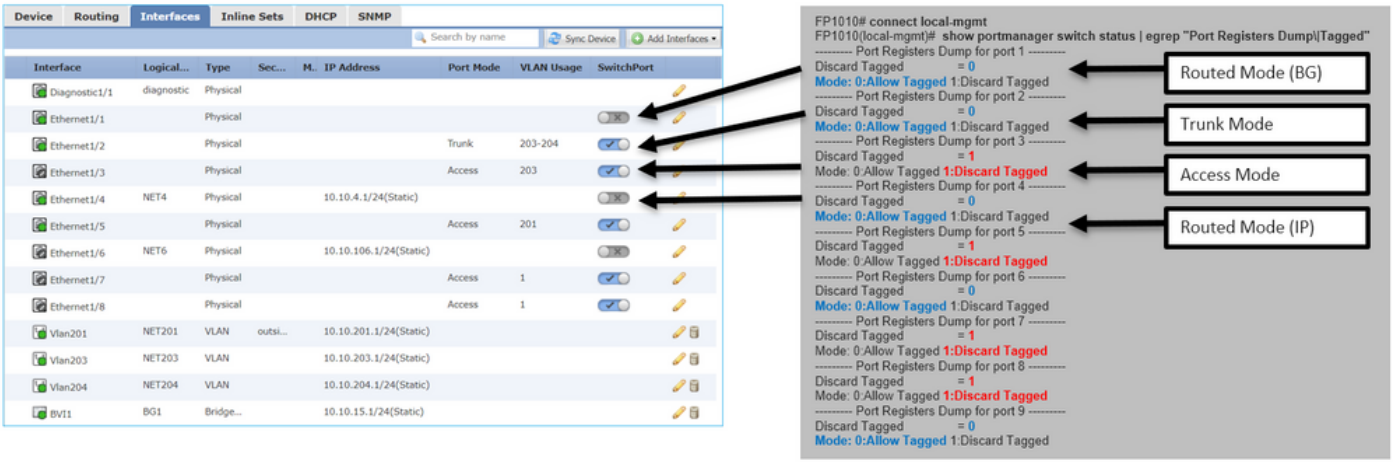
Serveur principal FP1010

Les registres de ports définissent toutes les fonctions de commutateur et de port internes.

Dans cette capture d'écran, la section 'Contrôle de port' des registres de port s'affiche et plus précisément le registre qui détermine si le trafic étiqueté reçu sur l'interface doit être ignoré (1) ou autorisé (0). Voici la section de registre complète pour un port :

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

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

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

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

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

Dans cette capture d'écran, vous pouvez voir les différentes valeurs de registre Discard Tagged pour les différents modes de port :

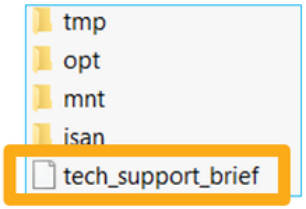


Collecter FPRM show tech sur FP1010

Pour générer un bundle FPRM et le télécharger sur un serveur 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
```

Le bundle FPRM contient un fichier appelé tech_support_brief. Le fichier tech_support_brief contient une série de commandes show. L'une d'elles est la **commande show portmanager switch status** :



Détails des restrictions, problèmes courants et solutions de rechange

Limitations de la mise en oeuvre de la version 6.5

- Les protocoles de routage dynamique ne sont pas pris en charge pour les interfaces SVI.
- Multi-contexte non pris en charge sur 1010.
- Plage d'ID VLAN SVI limitée à 1-4070.
- Port-channel pour L2 n'est pas pris en charge.
- Le port de couche 2 en tant que liaison de basculement n'est pas pris en charge.

Limites liées aux fonctionnalités du commutateur

Fonctionnalité	Description	Limite
Nombre d’interfaces VLAN	Nombre total d’interfaces VLAN pouvant être créées	60
VLAN en mode Trunk	Nombre maximal de VLAN autorisés sur un port en mode trunk	20
VLAN natif	Mappe tous les paquets non balisés Atteindre un port au VLAN natif configuré sur le port	1
Interfaces nommées	Inclut toutes les interfaces nommées (VLAN d'interface, sous-interface, port-channel, interface physique, etc)	60

Autres limitations

- Les sous-interfaces et le VLAN d'interface ne peuvent pas utiliser le même VLAN.
- Toutes les interfaces qui participent à BVI doivent appartenir à la même classe d'interface.
- Une BVI peut être créée avec une combinaison de ports de mode L3 et de sous-interfaces de ports de mode L3.
- Une BVI peut être créée avec une combinaison de VLAN d'interface.
- Une BVI ne peut pas être créée en mélangeant les ports du mode L3 et les VLAN d'interface.

Informations connexes

- Appliance de sécurité Cisco Firepower 1010
- Guides de configuration