FPR1010上のL2スイッチ、アーキテクチャ、検証、およびトラブルシューティング

内容

概要
前提条件
要件
使用するコンポーネント
背景説明
Firepower 6.5の追加
FMCの追加
仕組み
FP1010アーキテクチャ
パケット処理
FP1010ポートモード
FP1010ケース1.ルーテッドポート（IPルーティング）
FP1010ケース2.ブリッジグループモード（ブリッジング）
FP1010ケース3.アクセスモードのスイッチポート（HWスイッチング）
VLAN内トラフィックのフィルタリング
FP1010ケース4.スイッチポート（トランキング）
FP1010ケース5.スイッチポート（VLAN間）
FP1010ケース6. VLAN間フィルタ
ケーススタディ – FP1010.ブリッジングとハードウェアスイッチング+ブリッジング
FP1010の設計上の考慮事項
FXOS REST API
トラブルシューティング/診断
診断の概要
FP1010バックエンド
FP1010のFPRM show techを収集します。
制限事項の詳細、一般的な問題、回避策
関連情報

概要

このドキュメントでは、FP1010デバイスのL2スイッチについて説明します。具体的には、実装のSecurity Services Platform(SSP)/Firepower eXtensive Operation System(FXOS)部分を主に対象としています。6.5リリースでは、組み込みのL2ハードウェアスイッチでFirepower 1010（デスクトップモデル）対応のスイッチング機能が有効になっています。これにより、追加のハードウェアスイッチを回避し、コストを削減できます。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

- FP1010は、ASA5505およびASA5506-Xプラットフォームに代わるデスクトップモデルのSmall-Office Home-Office(SOHO)です。
- Firepower Management Center(FMC)、Firepower Device Manager(FDM)、またはCloud Defense Orchestrator(CDO)で管理されるFTDイメージ(6.4+)のソフトウェアサポート。
- CSM、ASDM、またはCLIで管理されるASAイメージ(9.13+)のソフトウェアサポート。
- オペレーティングシステム(OS)、ASA、またはFTDは、FXOSバンドル（FP21xxと同様）です。
- 8 x 10/100/1000 Mbpsデータポート。
- ポートE1/7、E1/8はPoE+をサポートします。
- ハードウェアスイッチにより、ポート間のラインレート通信が可能になります(例：ローカルサーバへのカメラフィード)。

Firepower 6.5の追加

- Switched Virtual Interface(SVI)と呼ばれる新しいタイプのインターフェイスの導入。
- 混合モード：インターフェイスは、スイッチド(L2)モードまたは非スイッチド(L3)モードのいずれかで設定できます。
- L3モードインターフェイスは、すべてのパケットをセキュリティアプリケーションに転送します。
- 2つのポートが同じVLANに属している場合、L2モードポートはハードウェアでスイッチングできるため、スループットと遅延が向上します。ルーティングまたはブリッジする必要があるパケットは、セキュリティアプリケーションに到達します(例：新しいファームウェアをインターネットからダウンロードするカメラ)を使用して、設定に従ってセキュリティ検査を受けます。
- L2物理インターフェイスは、1つまたは複数のSVIインターフェイスに関連付けることができます。

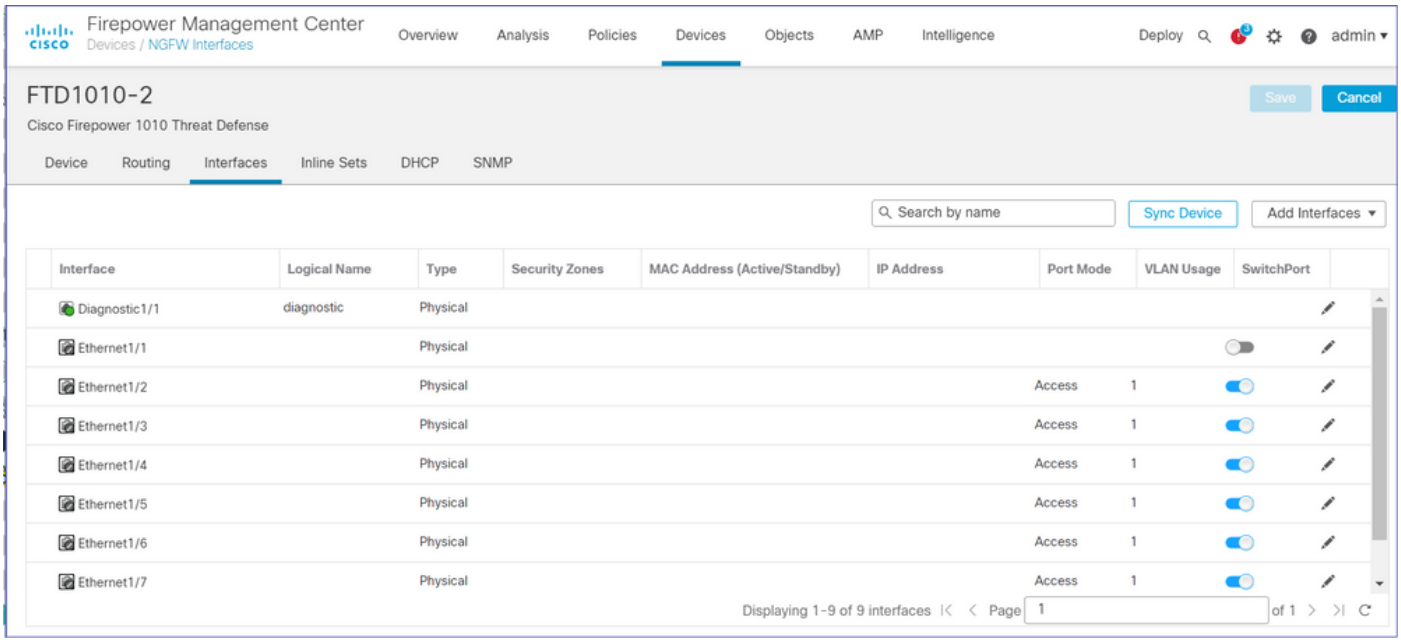
- L2モードインターフェイスは、アクセスモードまたはトランクモードにすることができます。
- アクセスモードL2インターフェイスでは、タグなしトラフィックだけが許可されます。
- トランクモードL2インターフェイスでは、タグ付きトラフィックが許可されます。
- トランクモードL2インターフェイスのネイティブVLANサポート。
- ASA CLI、ASDM、CSM、FDM、FMCは、新しい機能をサポートするように強化されています。

FMCの追加

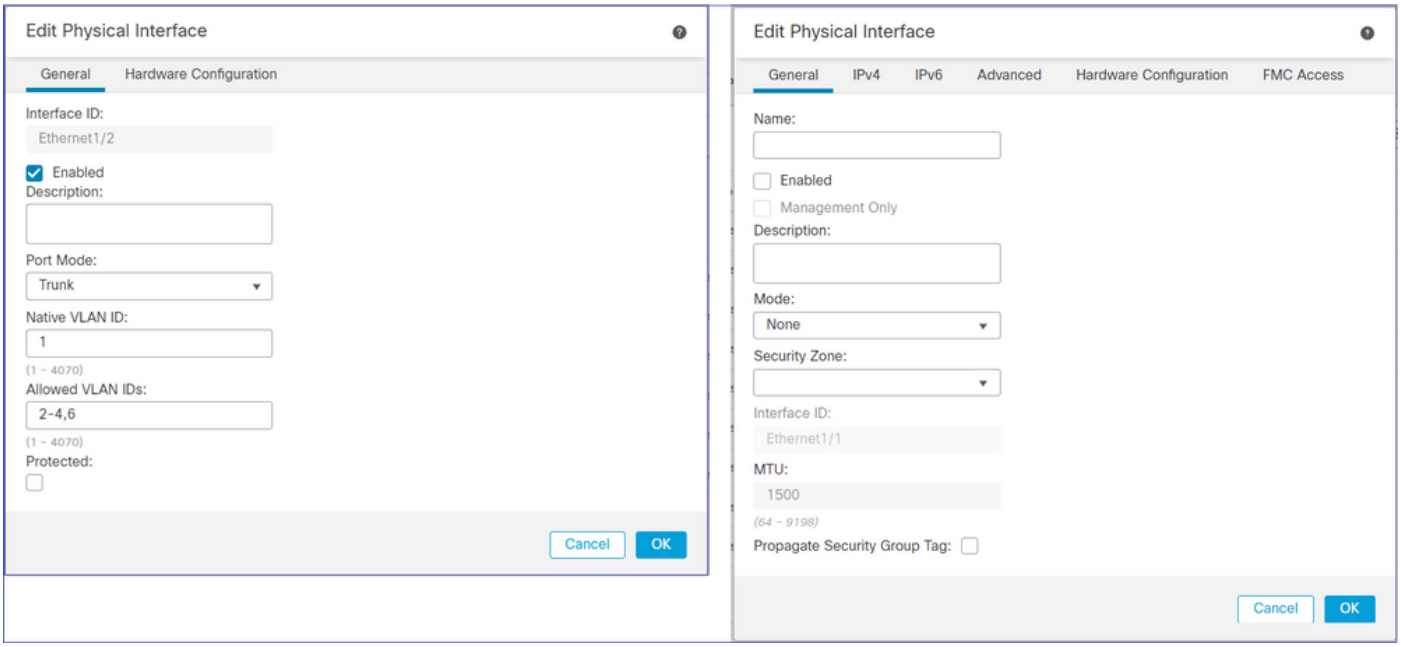
- 物理インターフェイスがL3インターフェイスかL2インターフェイスかを識別するために使用される物理インターフェイスに対して、switchportという新しいインターフェイスモードが導入されました。
- L2物理インターフェイスは、アクセスモードまたはトランクモードに基づいて、1つまたは複数のVLANインターフェイスに関連付けることができます。
- Firepower 1010は、Ethernet1/7およびEthernet1/8などの最後の2つのデータインターフェイスでPower over Ethernet(PoE)設定をサポートしています。
- スイッチドと非スイッチド間のインターフェイスの変更は、PoEとハードウェアの設定以外のすべての設定をクリアします。

仕組み

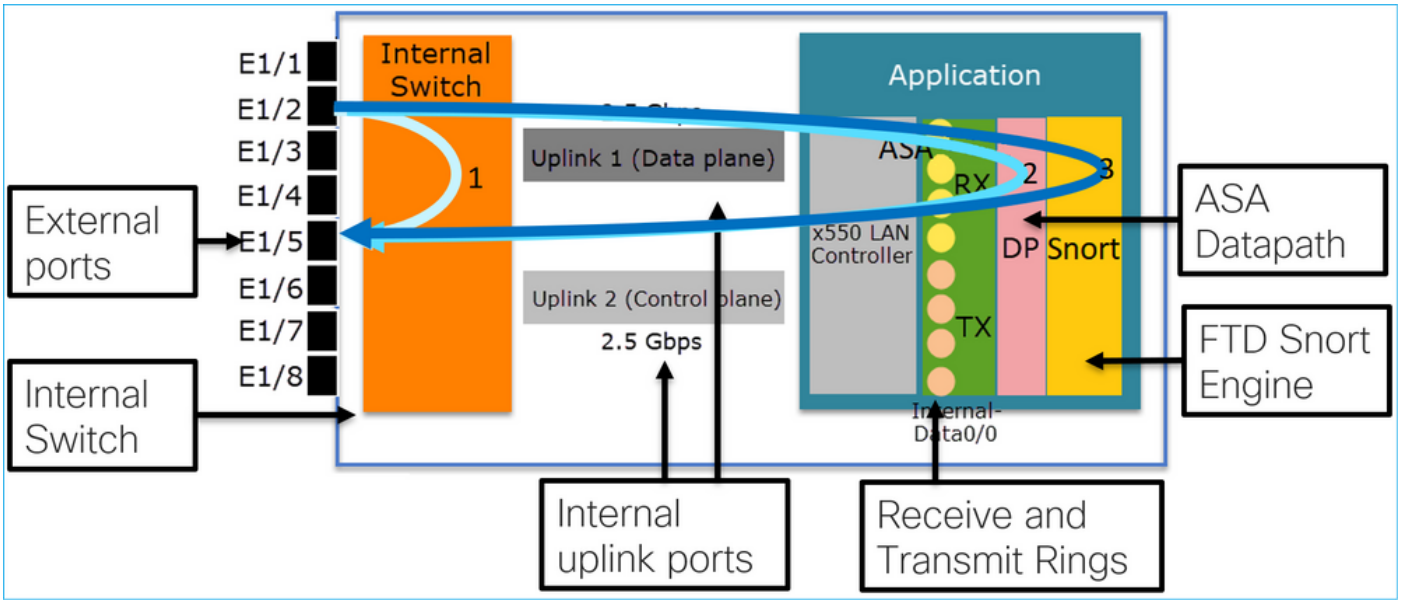
この機能は、FMC上の既存のインターフェイスのサポートを強化したにすぎません([Device Management] > [Interface Page])。



物理インターフェイスビュー（L2およびL3）



FP1010アーキテクチャ



- 8個の外部データポート。
- 1内部スイッチ
- 3つのアップリンクポート（図に示す2つのポート）、1つはデータプレーン用、1つはコントロールプレーン用、もう1つは設定用です。
- x550 LANコントローラ（アプリケーションとアップリンク間のインターフェイス）。
- 4受信(RX)リングと4送信(TX)リング。
- データパスプロセス（ASAおよびFTD上）。
- Snortプロセス（FTD上）。

パケット処理

パケット処理に影響を与える主な要因は次の2つです。

1.インターフェイス/ポートモード

2.適用ポリシー

パケットは、次の3つの方法でFP1010を通過できます。

1.内部スイッチでのみ処理

2.アプリケーション(ASA/FTD)に転送され、データパスプロセスでのみ処理される

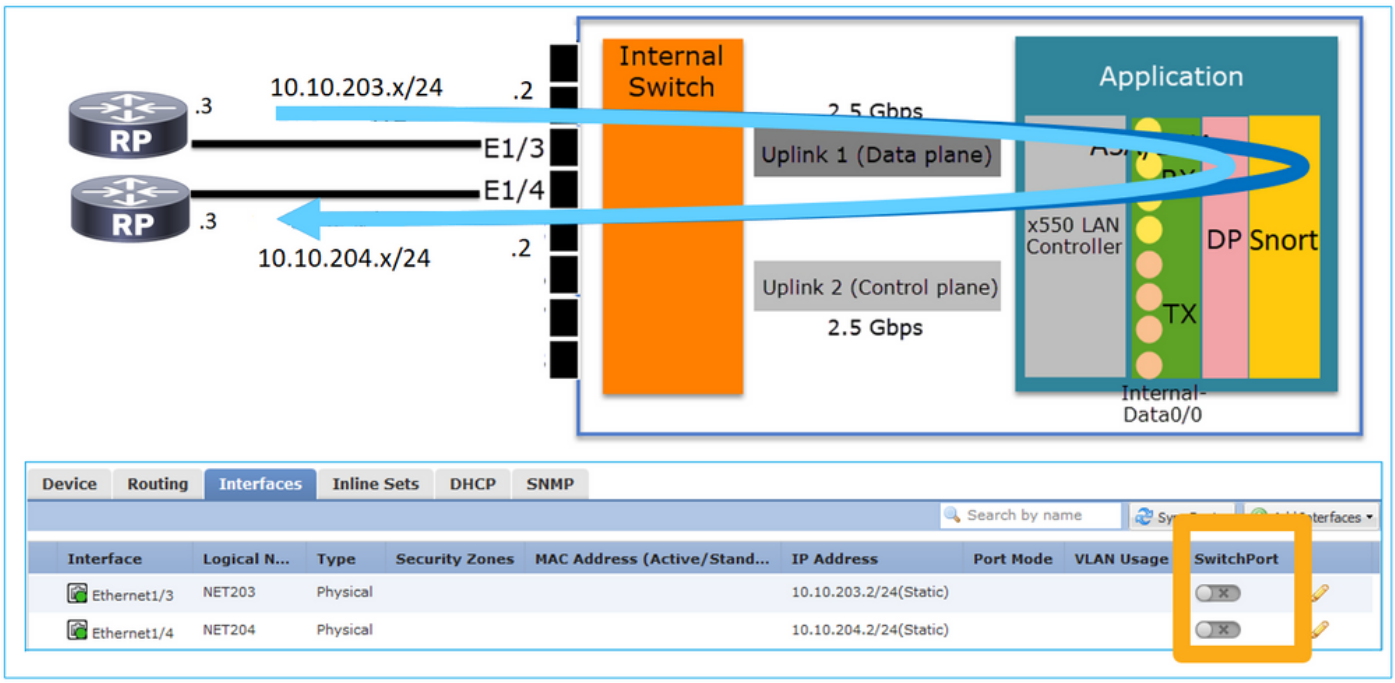
3.アプリケーション(FTD)に転送され、データパスとSnortエンジンによって処理される

FP1010ポートモード

UIの例はFMC用、CLIの例はFTD用です。ほとんどの概念は、ASAにも完全に適用できます。

FP1010ケース1.ルーテッドポート（IPルーティング）

設定と操作



要点

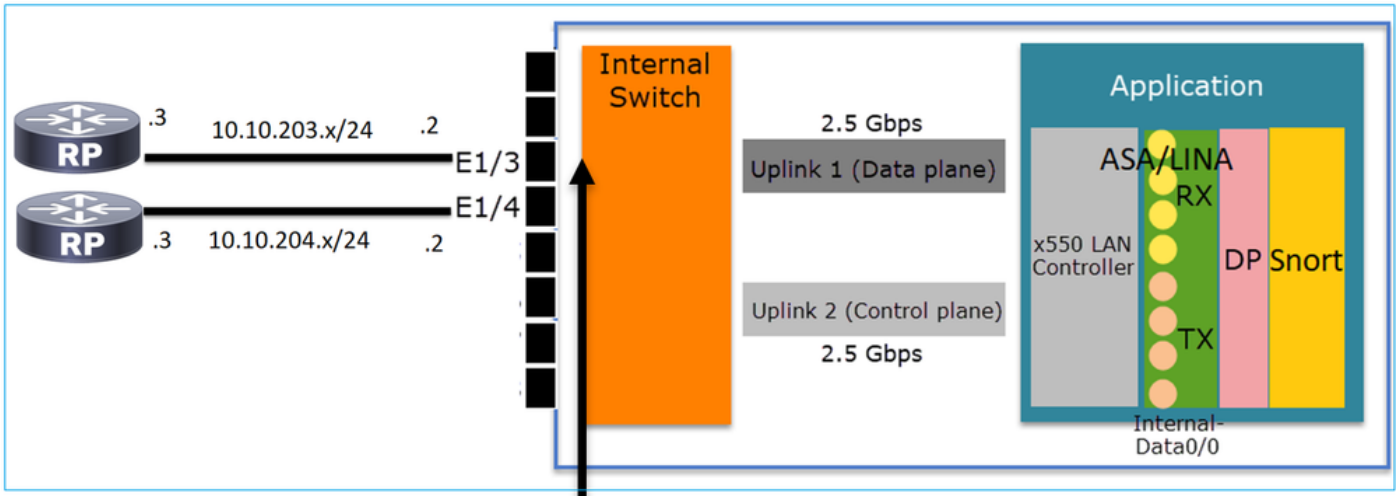
- 設計上、2つのポートは2つの異なるL2サブネットに属します。
- ポートがルーテッドモードに設定されると、パケットはアプリケーション（ASAまたはFTD）によって処理されます。
- FTDの場合、ルールアクション（ALLOWなど）に基づいて、パケットをSnortエンジンで検査することもできます。

FTDインターフェイスの設定

```
interface Ethernet1/3 nameif NET203
 cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
```

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

FP1010ルーテッドポートの確認



FXOS CLIから、物理インターフェイスカウンタを確認できます。次の例は、E1/3ポートの入力ユニキャストおよび出力ユニキャストカウンタを示しています。

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

FTDデータパスキャプチャを適用し、パケットをトレースできます。

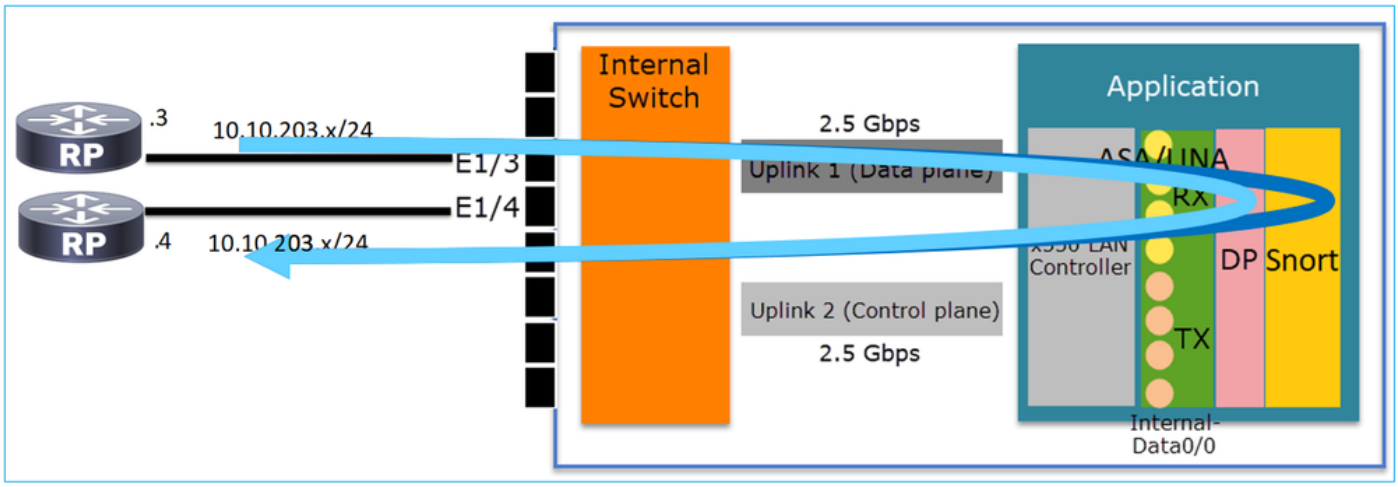
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

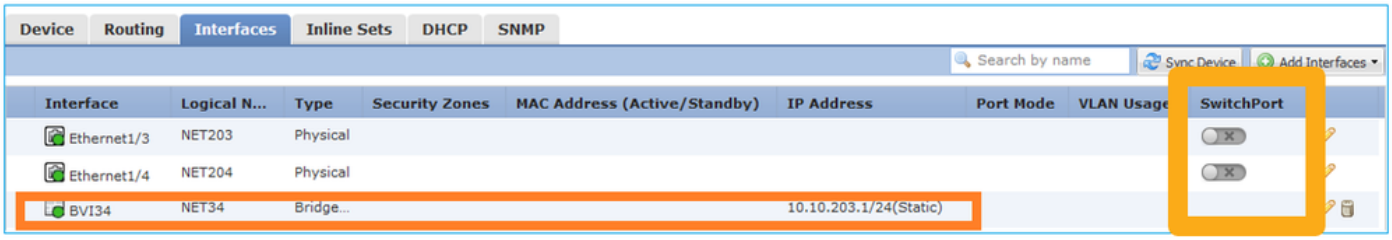
これはキャプチャス二ペットです。予想どおり、パケットはROUTE LOOKUP:

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

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

FP1010ケース2.ブリッジグループモード（ブリッジング）

設定と操作





要点

- 設計上、2つのポートは同じL3サブネット（トランスペアレントファイアウォールと同様）に接続されますが、異なるVLANに接続されます。
- ポートがブリッジモードに設定されると、パケットはアプリケーション（ASAまたはFTD）によって処理されます。
- FTDの場合、ルールアクション（ALLOWなど）に基づいて、パケットをSnortエンジンで検査することもできます。

FTDインターフェイスの設定

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

FP1010ブリッジグループポートの確認

次のコマンドは、BVI 34のインターフェイスメンバを表示します。

```
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
```

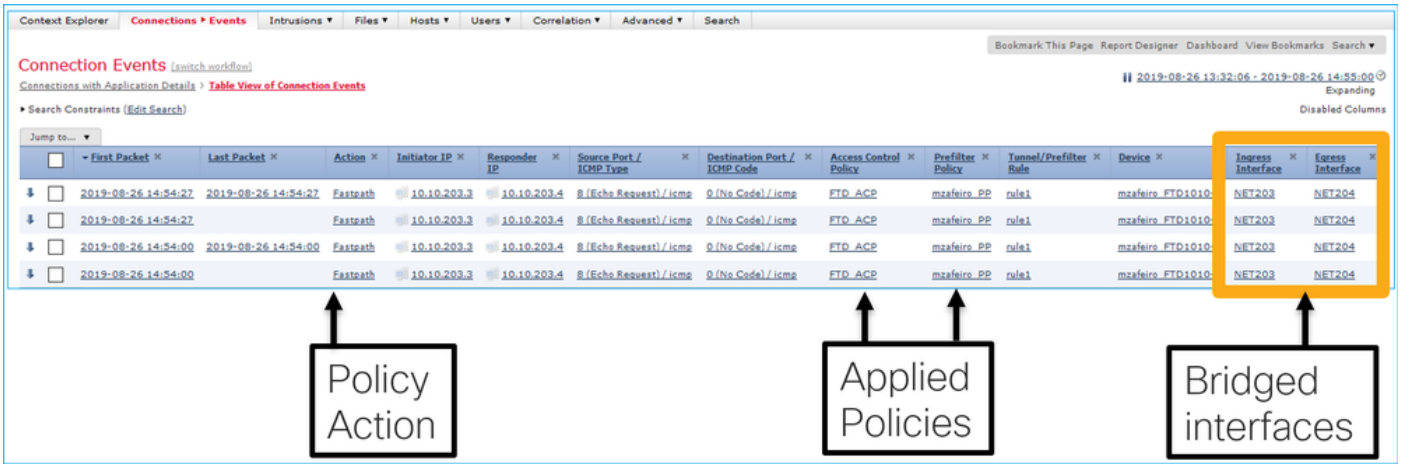
次のコマンドは、ASA/FTDデータパスのContent Addressable Memory(CAM)テーブルを示します。

```
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
```

パケットトレーススニペットは、パケットが宛先MAC L2ルックアップに基づいて転送されることを示します。

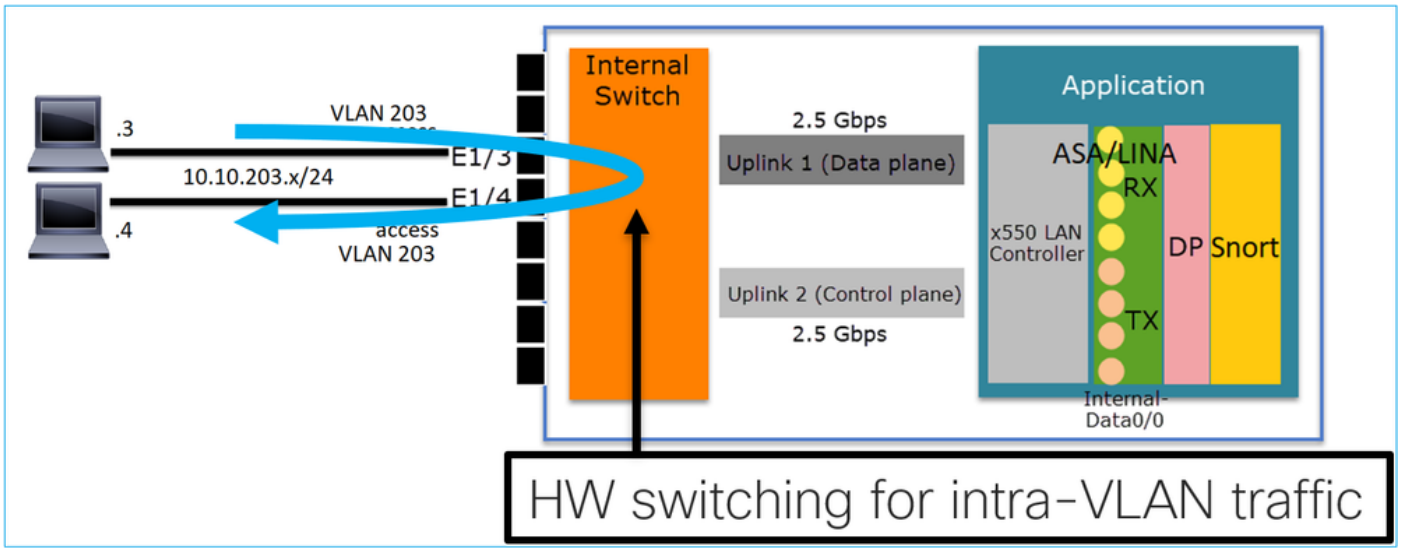
```
FP1010# show cap CAP203 packet-number 1 trace

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
```

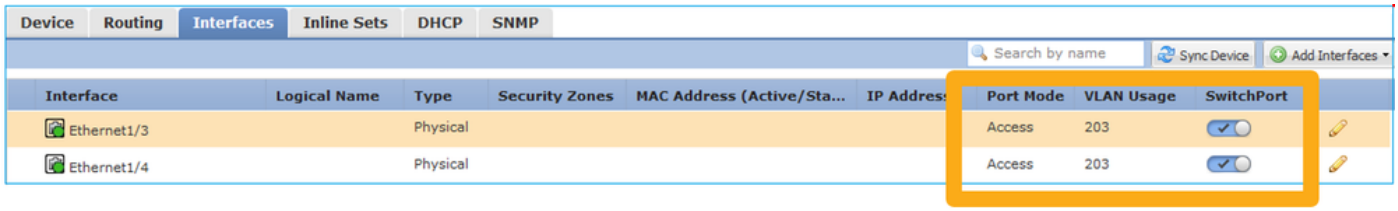
FTDの場合、FMC接続イベントは、フロー検査とトランジットブリッジグループインターフェイスに関する情報も提供できます。



FP1010ケース3.アクセスモードのスイッチポート（HWスイッチング）

設定と操作





要点

- HWスイッチングは、FTD **6.5+およ**びASA **9.13+機能**です。
- 設計上、2つのポートは同じL3サブネットと同じVLANに接続されます。
- このシナリオのポートは、アクセスモードで動作しています（タグなしトラフィックのみ）。
- SwitchPortモードで設定されたファイアウォールポートには、論理名(nameif)が設定されていません。
- ポートがスイッチングモードで設定され、同じVLAN（VLAN内トラフィック）に属している場合、パケットはFP1010内部スイッチでのみ処理されます。

FTDインターフェイスの設定

CLIから見ると、設定はL2スイッチに非常によく似ています。

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

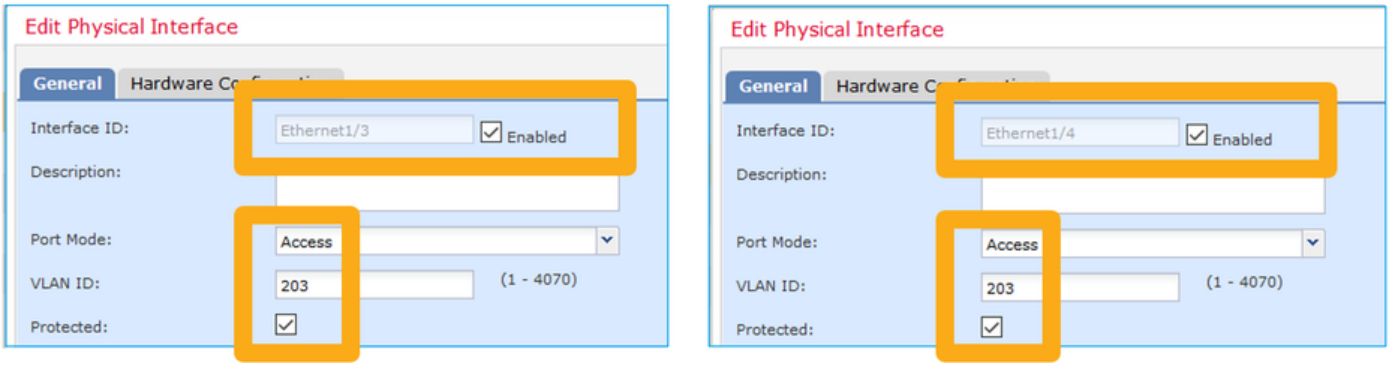
VLAN内トラフィックのフィルタリング

課題：**ACLはVLAN内トラフィックをフィルタリングできません。**

ソリューション:**保護ポート**

原理は非常に単純です。保護ポートとして設定されている2つのポートは相互に通信できません。

保護ポートの場合のFMC UI:



FTDインターフェイスの設定

switchport protectedコマンドは、インターフェイスで設定します。

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

FP1010スイッチポートの検証

この例では、1000個のユニキャストパケット(ICMP)が特定のサイズ（1100バイト）で送信されています。

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

中継インターフェイスの入力および出力ユニキャストカウンタを確認するには、次のコマンドを使用します。

```
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
```

次のコマンドは、内部スイッチのVLANステータスを示します。

```
FP1010# show switch vlan
```

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

少なくとも1つのポートがVLANに割り当てられている限り、VLANのステータスはUPです

ポートが管理上ダウンしているか、接続されているスイッチポートがdown/cable disconnectedで、これがVLANに割り当てられている唯一のポートである場合、VLANステータスもdownになります。

```
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
```

次のコマンドは、内部スイッチのCAMテーブルを表示します。

```
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
```

内部スイッチのCAMテーブルのデフォルトのエージングタイムは5分30秒です。

FP1010には2つのCAMテーブルがあります。

1. **内部スイッチCAMテーブル**:ハードウェアスイッチングの場合に使用
2. **ASA/FTDデータパスCAMテーブル**:ブリッジングの場合に使用

FP1010を通過する各パケット/フレームは、ポートモードに基づいて1つのCAMテーブル（内部スイッチまたはFTDデータパス）で処理されます。

> **注意**：SwitchPortモードで使用される**show switch mac-address-table内部スイッチのCAMテーブル**と、ブリッジモードで使用される**show mac-address-table** FTDデータパスのCAMテーブルを混同しないでください

ハードウェアスイッチング：その他の注意点

ASA/FTDデータパスログには、ハードウェアスイッチドフローに関する情報が表示されません。

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

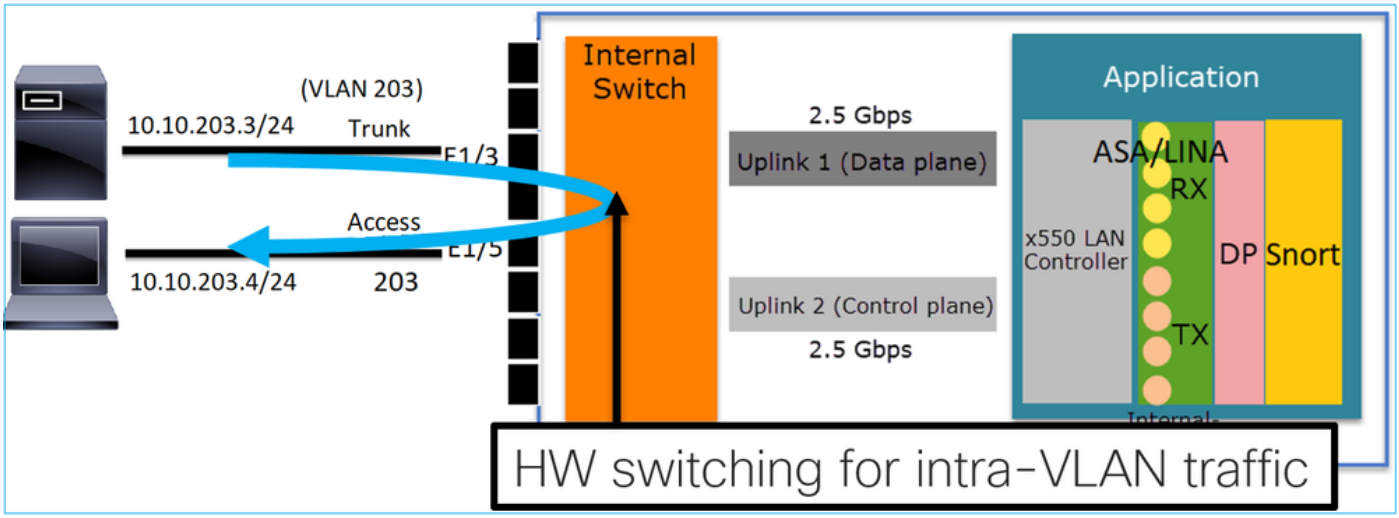
ASA/FTDデータパス接続テーブルには、ハードウェアスイッチドフローが表示されません。

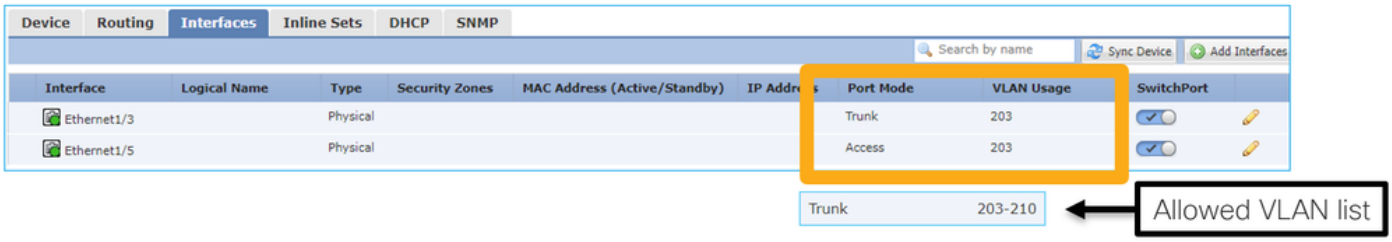
```
FP1010# show conn
0 in use, 3 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

さらに、FMC接続イベントには、ハードウェアによってスイッチングされるフローは表示されません。

FP1010ケース4.スイッチポート（トランキング）

設定と操作





要点

- HWスイッチングは、FTD 6.5+およびASA 9.13+機能です。
- 設計上、2つのポートは同じL3サブネットと同じVLANに接続されます。
- トランクポートは、タグ付きフレームとタグなし（ネイティブVLANの場合）を受け入れます。
- ポートがスイッチングモードで設定され、同じVLAN（VLAN内トラフィック）に属している場合、パケットは内部スイッチでのみ処理されます。

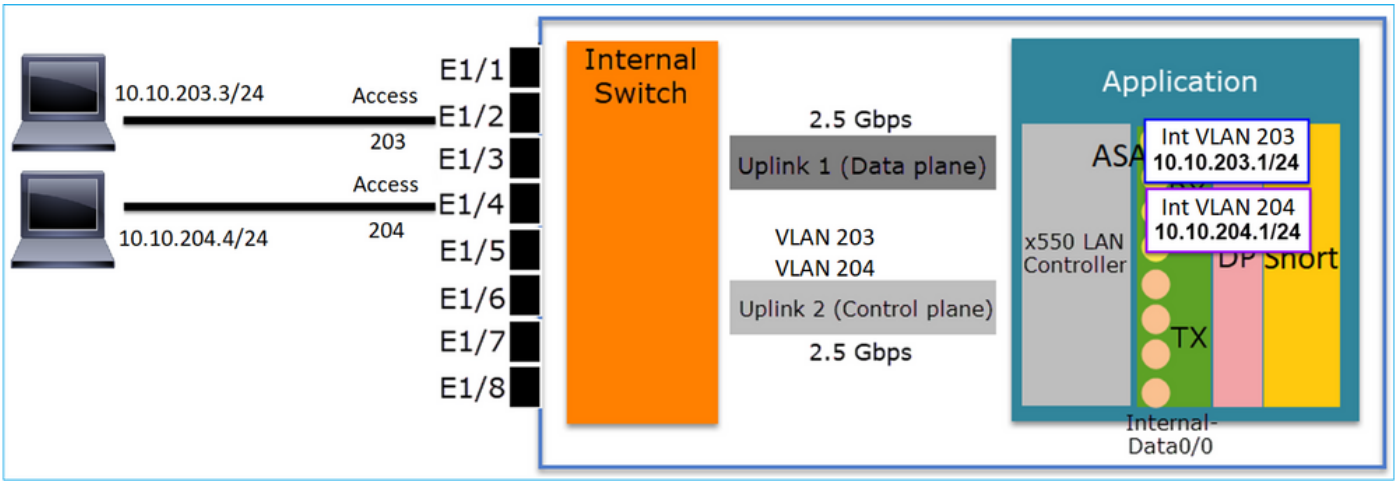
FTDインターフェイスの設定

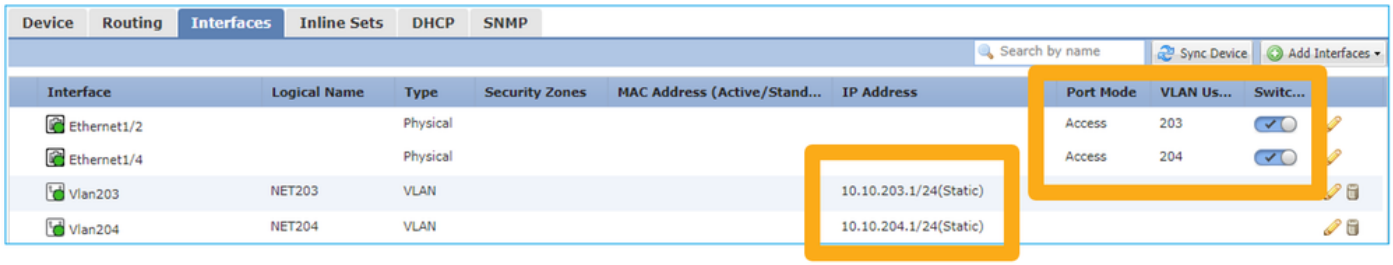
設定は、レイヤ2スイッチポートに似ています。

```
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ケース5.スイッチポート（VLAN間）

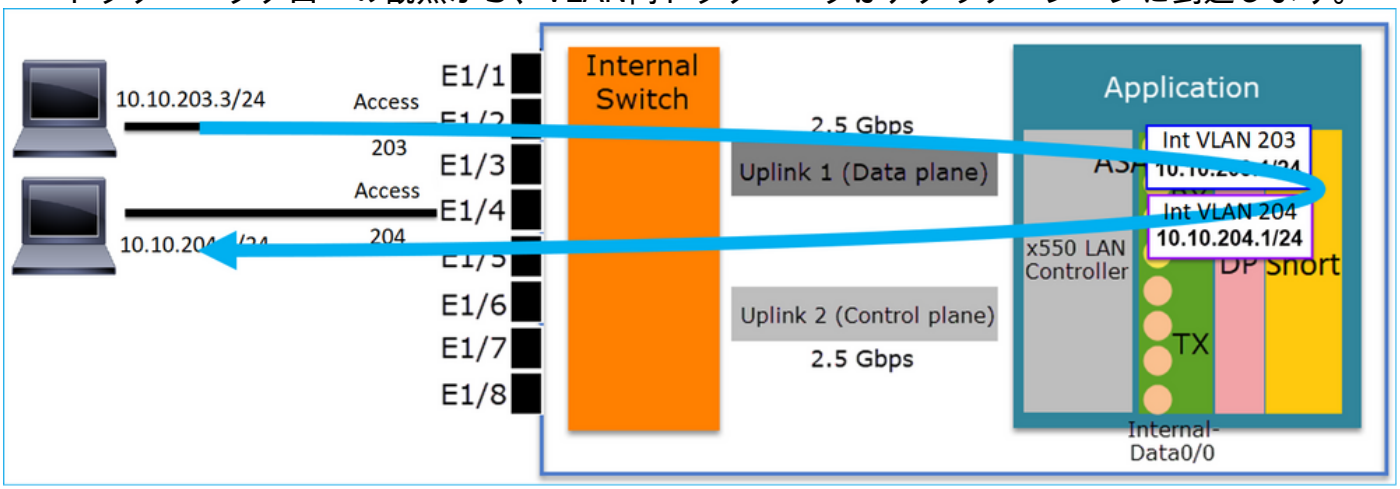
設定と操作





要点

- 設計上、2つのポートは2つの異なるL3サブネットと2つの異なるVLANに接続されます。
- VLAN間のトラフィックは、VLANインターフェイス（SVIと同様）を通過します。
- トラフィックフローの観点から、VLAN間トラフィックはアプリケーションに到達します。



FTDインターフェイスの設定

この設定は、スイッチ仮想インターフェイス(SVI)に似ています。

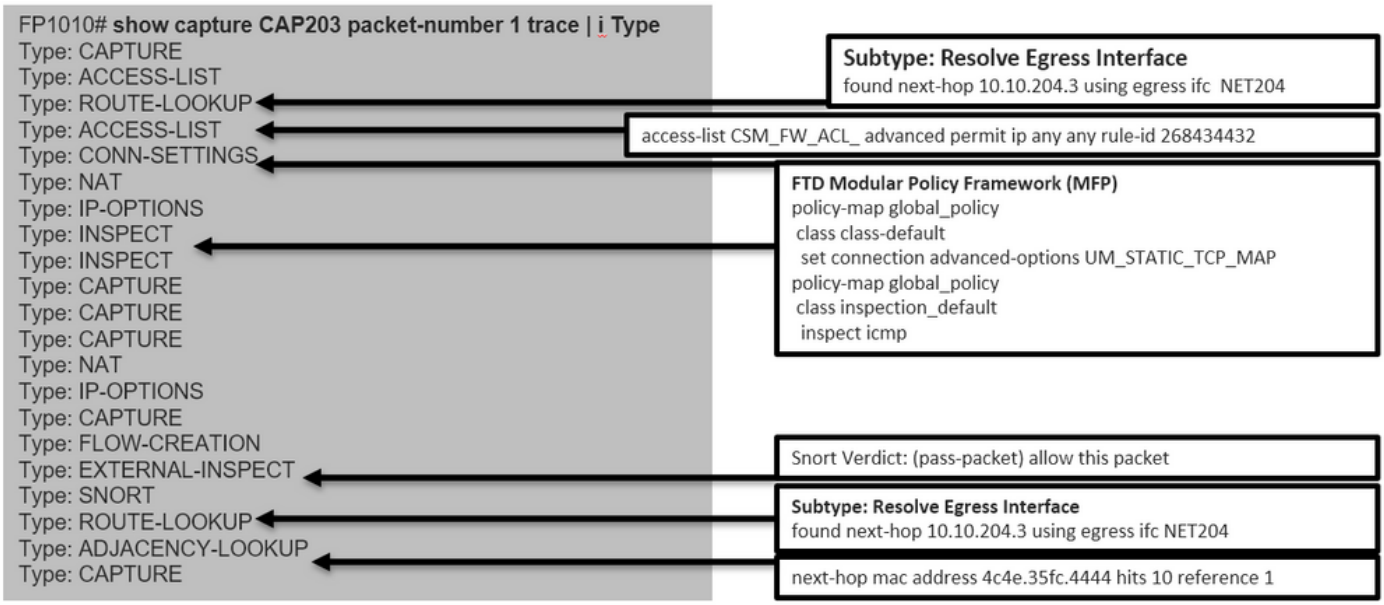
```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

VLAN間トラフィックのパケット処理

これは、2つの異なるVLANを通過するパケットのトレースです。

```
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
```

パケットプロセスの主なフェーズ：



FP1010ケース6. VLAN間フィルタ

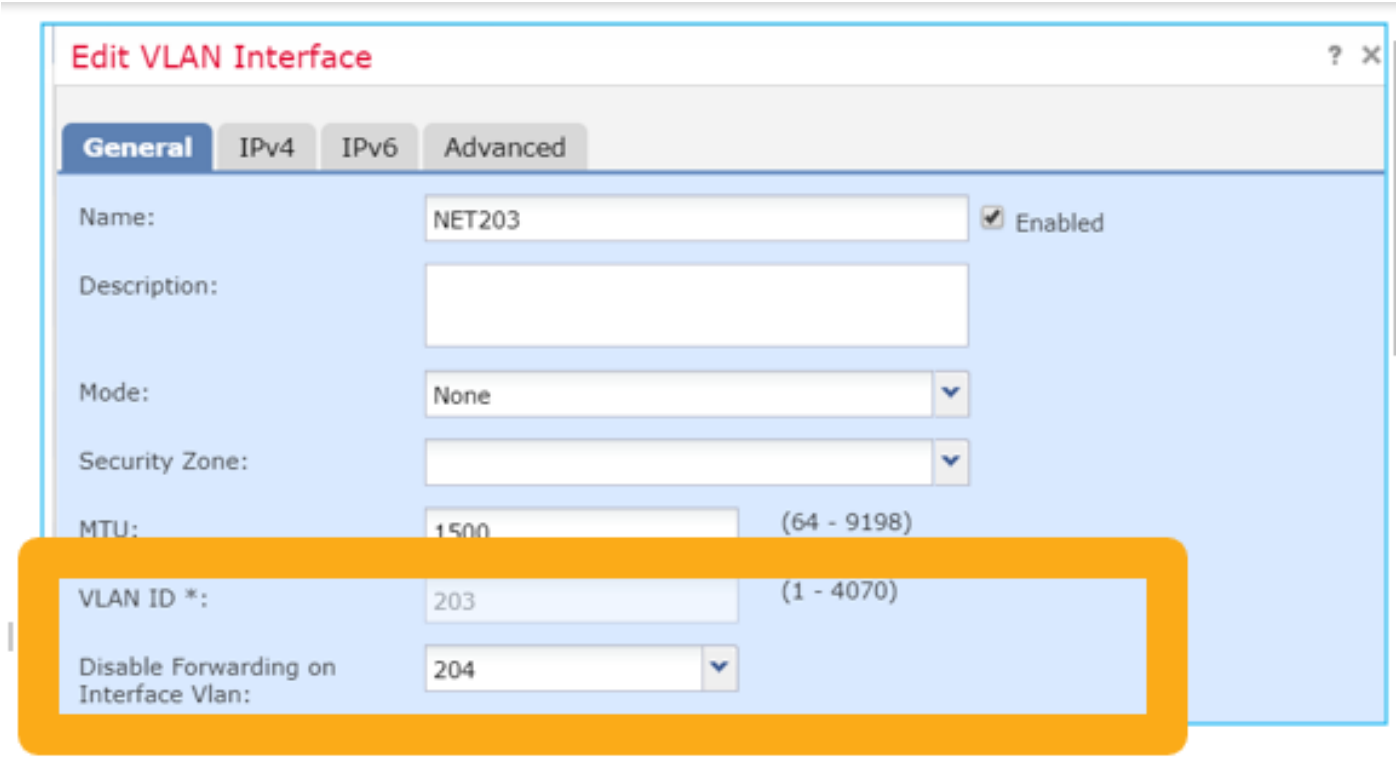
設定と操作

VLAN間トラフィックをフィルタリングするには、主に2つのオプションがあります。

1. アクセス コントロール ポリシー
2. 'no forward'コマンド

「no forward」コマンドを使用してVLAN間トラフィックをフィルタリングする

FMC UIの設定：



要点

- no forward dropは単方向です。
- 両方のVLANインターフェイスに適用することはできません。
- no forwardチェックは、ACLチェックの前に実行されます。

FTDインターフェイスの設定

この場合のCLI設定は次のとおりです。

```
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
```

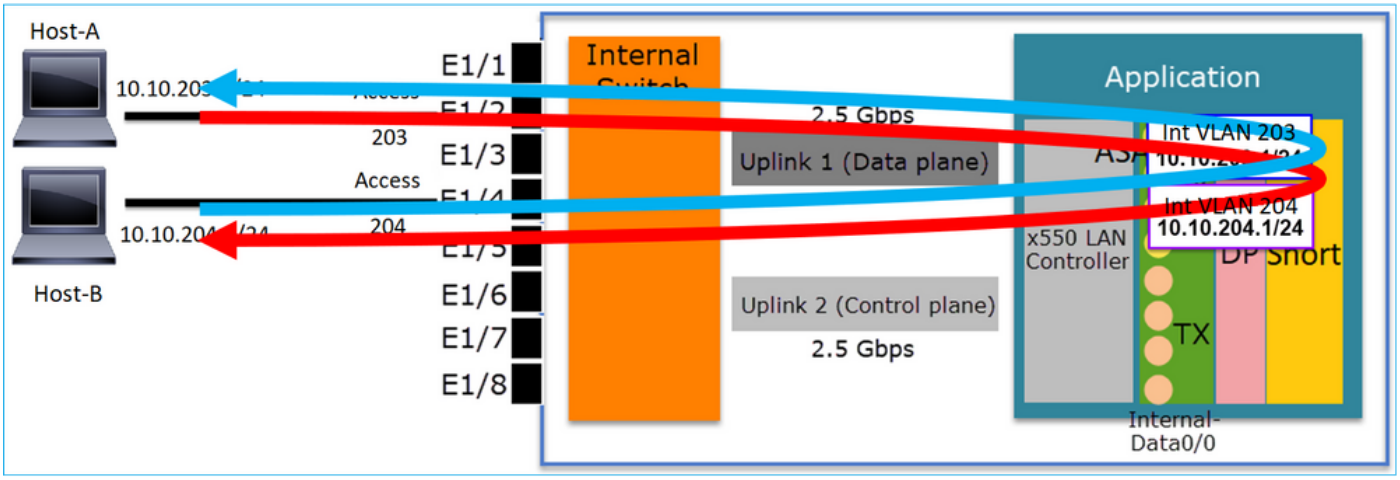
no forward機能によってパケットがドロップされると、ASA/FTDデータパスSyslogメッセージが生成されます。

```
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)
```

Accelerated Security Path（ASP；高速セキュリティパス）ドロップポイントの観点からは、ACLドロップと見なされます。

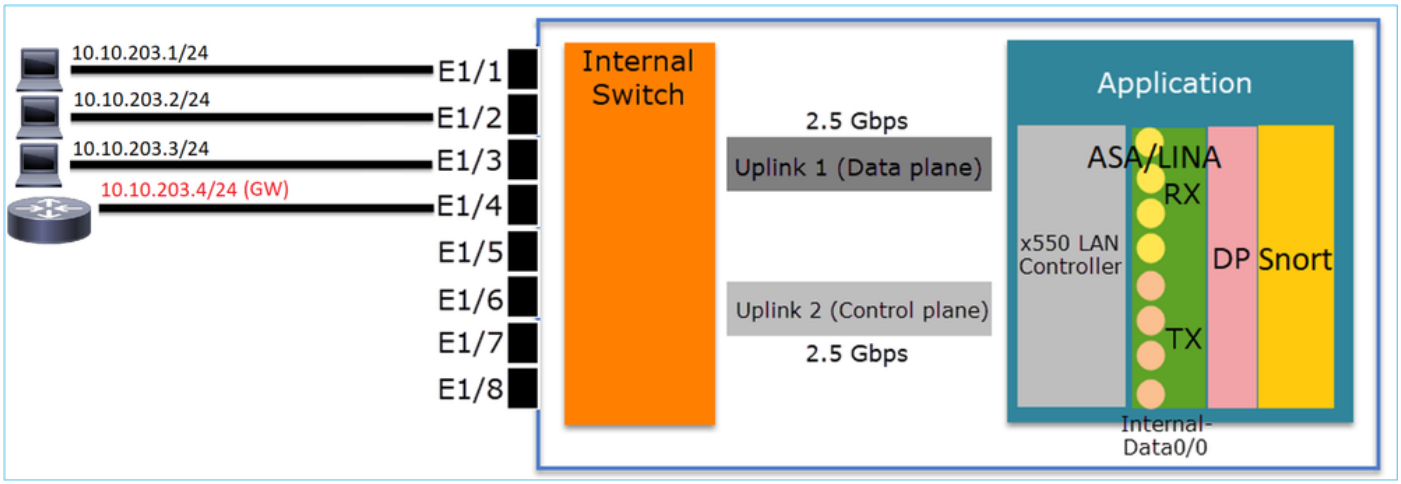
```
FP1010-2# show asp drop
Frame drop:
Flow is denied by configured rule (acl-drop) 1
```

ドロップは単方向であるため、Host-A(VLAN 203)はHost-B(VLAN 204)へのトラフィックを開始できませんが、逆が許可されます。



ケーススタディ – FP1010.ブリッジングとハードウェアスイッチング+ブリッジング

次のトポロジを考えてみます。



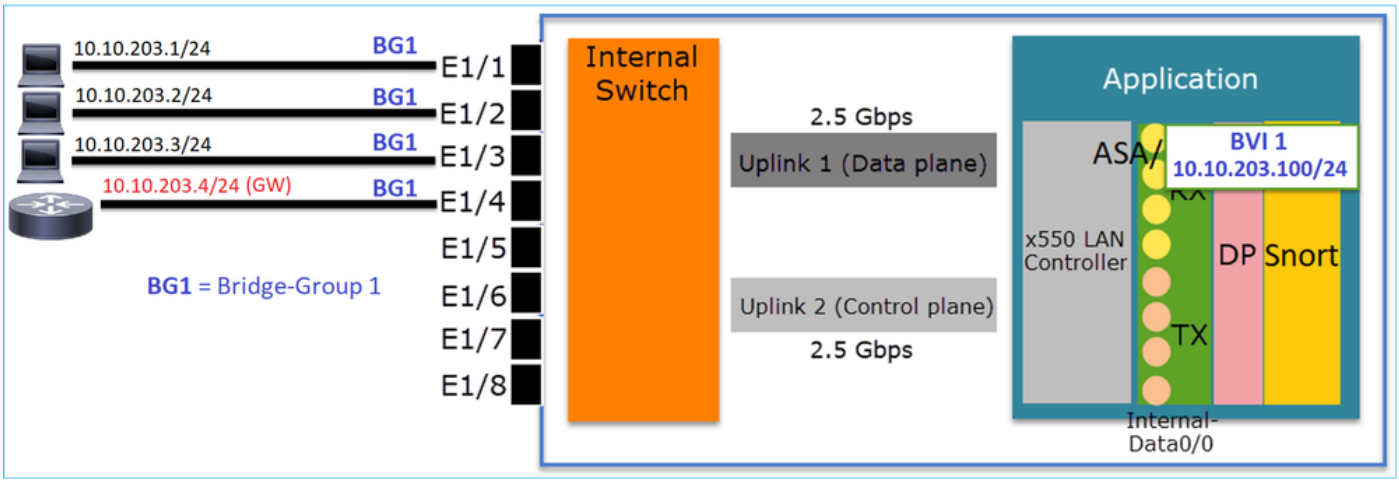
このトポロジでは、次のようになります。

- 同じL3サブネット(10.10.203.x/24)に属する3つのエンドホスト。
- ルータ(10.10.203.4)は、サブネット内でGWとして機能します。

このトポロジには、主に2つの設計オプションがあります。

1. ブリッジング
2. ハードウェアスイッチング+ブリッジング

設計オプション1.ブリッジング

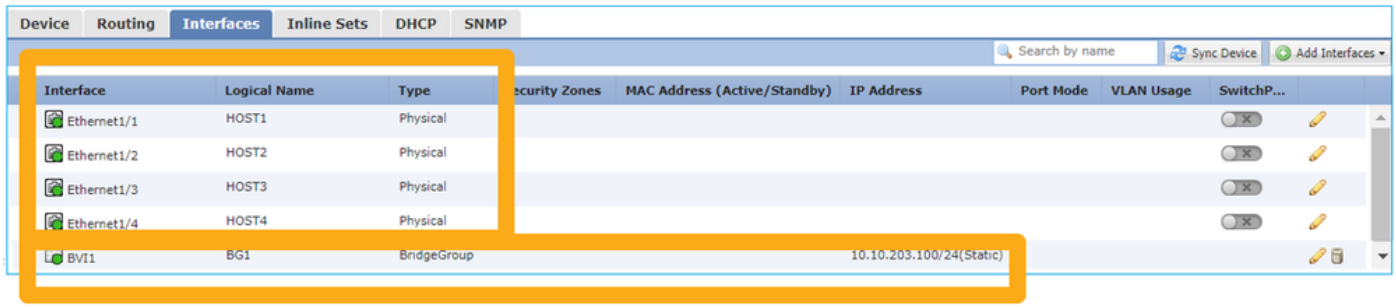


要点

この設計の主なポイントは次のとおりです。

- 4台の接続デバイスと同じサブネット(10.10.203.x/24)にIPを使用して作成されたBVI 1があります。
- 4つのポートはすべて同じブリッジグループ（この場合はグループ1）に属しています。
- 4つのポートにはそれぞれ名前が設定されています。
- ホスト間およびホストとゲートウェイ間の通信は、アプリケーション（FTDなど）を経由します。

FMC UIの観点から見ると、設定は次のようになります。

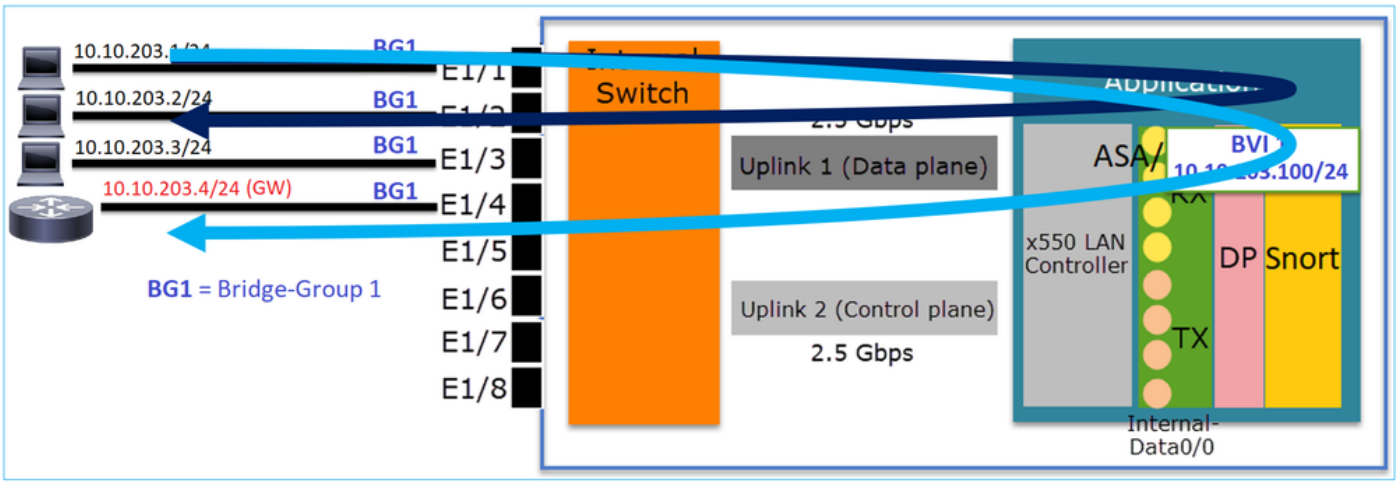


FTDインターフェイスの設定

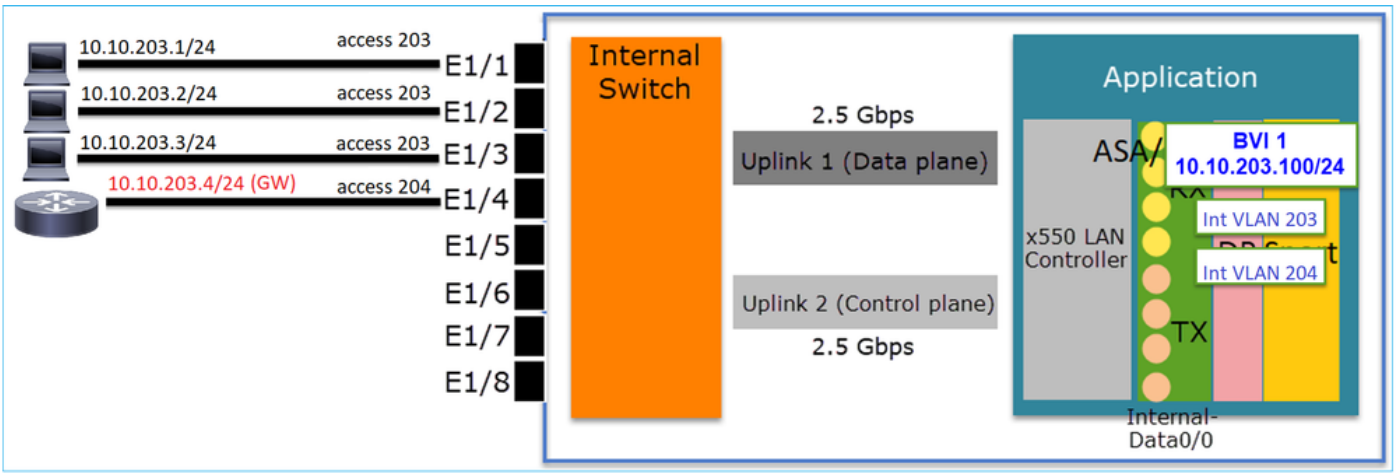
この場合の設定は次のとおりです。

```
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
```

このシナリオのトラフィックフロー：



設計オプション2.ハードウェアスイッチング+ブリッジング

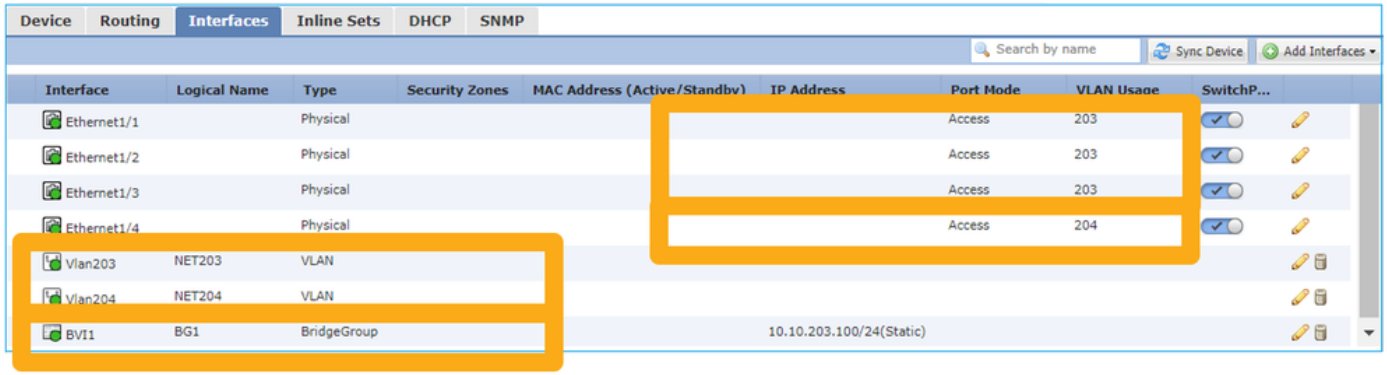


要点

この設計の主なポイントは次のとおりです。

- 4台の接続デバイスと同じサブネット(10.10.203.x/24)にIPを使用して作成されたBVI 1があります。
- エンドホストに接続されたポートは、SwitchPortモードで設定され、同じVLAN(203)に属しています。
- GWに接続されたポートはSwitchPortモードで設定され、別のVLAN(204)に属しています。
- 2つのVLANインターフェイス(203、204)があります。 2つのVLANインターフェイスにはIPが割り当てられておらず、ブリッジグループ1に属しています。
- ホスト間通信は、内部スイッチのみを経由します。
- ホストからゲートウェイへの通信は、アプリケーション（FTDなど）を経由します。

FMC UIの設定：

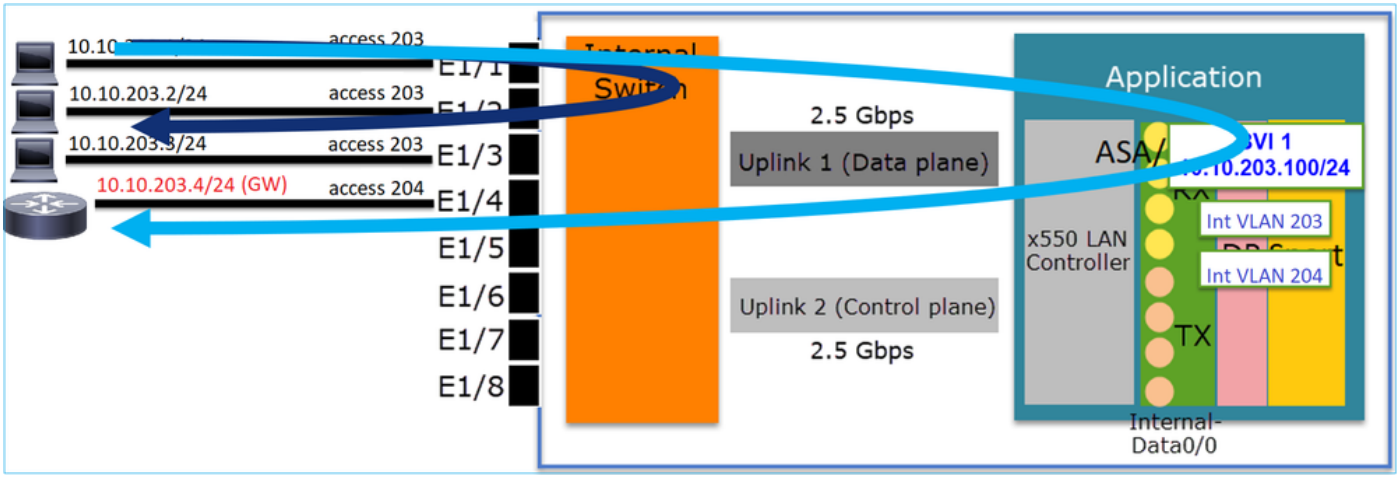


FTDインターフェイスの設定

この場合の設定は次のとおりです。

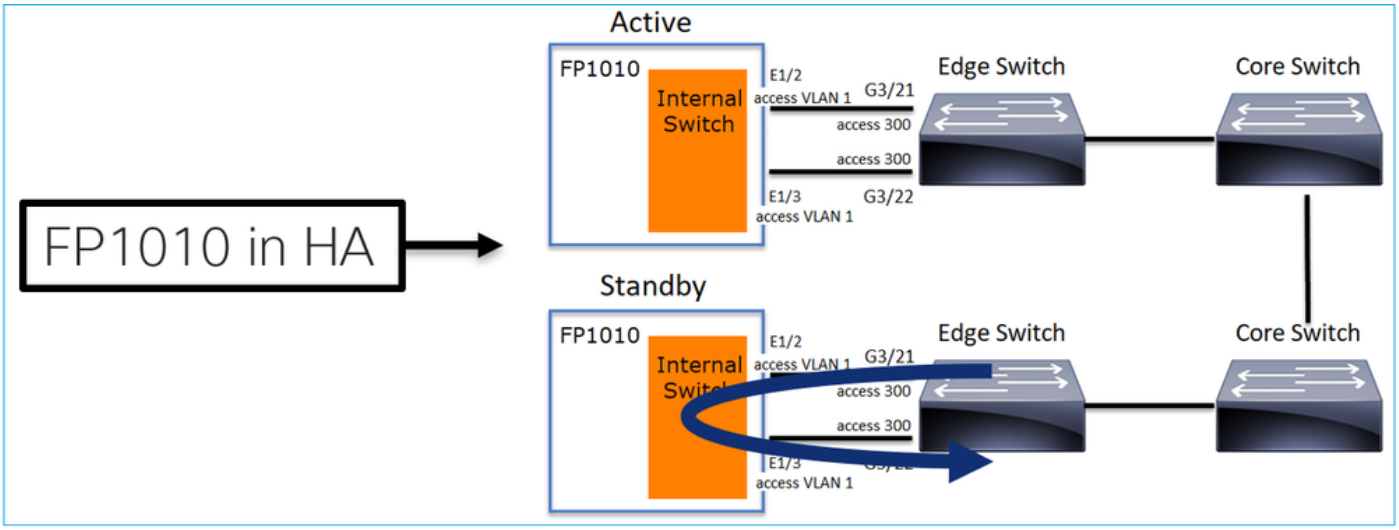
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1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

ホスト間通信とホスト間通信のGW間通信：



FP1010の設計上の考慮事項

スイッチングおよびハイアベイラビリティ(HA)

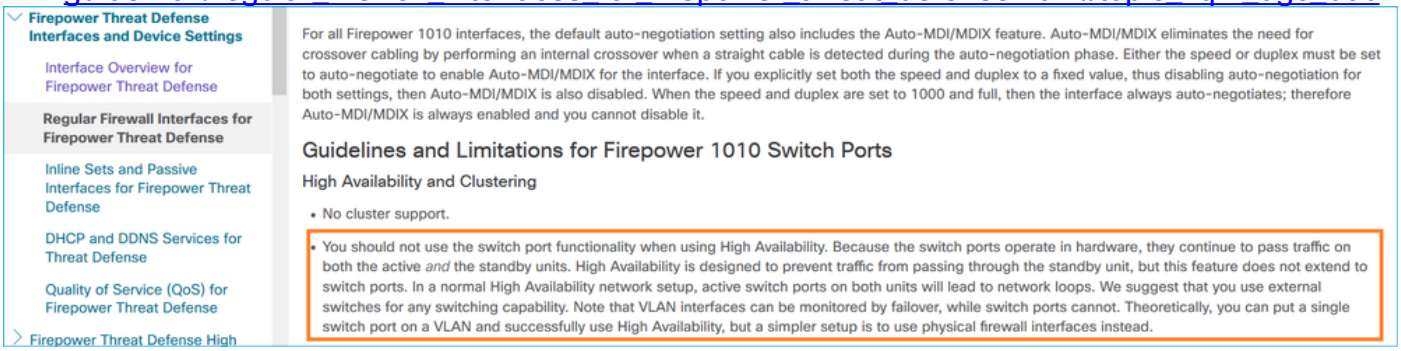


HA環境でHWスイッチングを設定する場合、主に2つの問題があります。

1. スタンバイユニットのハードウェアスイッチングは、デバイスを介してパケットを転送します。これにより、トラフィックループが発生する可能性があります。
2. スイッチポートはHAでモニタされない

設計要件

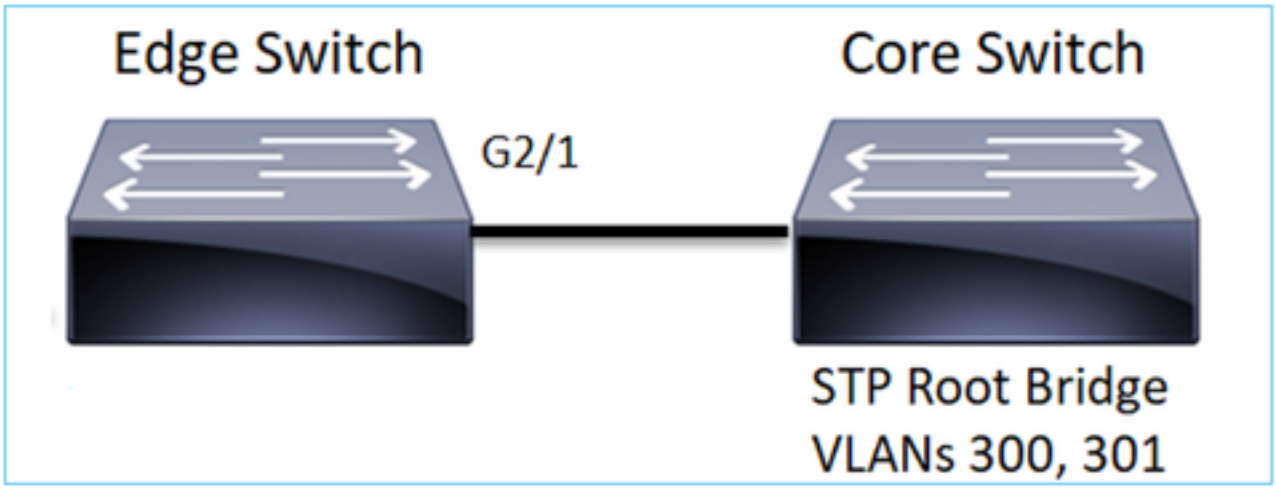
- ASA/FTDハイアベイラビリティでは、SwitchPort機能を使用しないでください。これは、FMC設定ガイドに記載されています。
  https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b



スパニングツリープロトコル(STP)とのインタラクション

FP1010内部スイッチではSTPが実行されません。

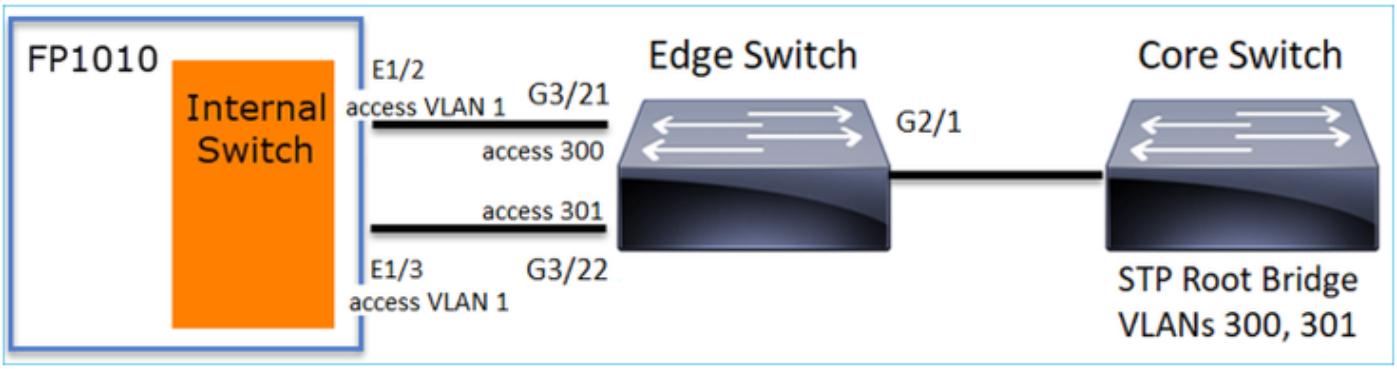
次のシナリオについて考えます。



エッジスイッチでは、両方のVLANのルートポートはG2/1です。

```
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
```

FP1010をエッジスイッチに接続し、両方のポートを同じVLAN（ハードウェアスイッチング）に設定します。



問題

- G3/22で**受信した**VLAN 301の上位BPDUがVLANリークにより発生

```
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
```

警告：L2スイッチをFP1010に接続すると、STPドメインに影響する可能性があります

これは、FMC設定ガイドにも記載されています。

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

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

FXOS REST API

FMC REST API

この機能をサポートするREST APIは次のとおりです。

- L2物理インターフェイス（サポートされるPUT/GET）

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

- VLANインターフェイス（サポートされるPOST/PUT/GET/DELETE）

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

トラブルシューティング/診断

診断の概要

- ログファイルは、FTD/NGIPSのトラブルシューティングまたはshow techの出力でキャプチャされます。トラブルシューティングの場合に詳細を調べる必要がある項目を次に示します。
- /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

FXOS（デバイス）からのデータ収集 – CLI

FTD(SSH)の場合：

```
> 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)#
```

FTD（コンソール）の場合：

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

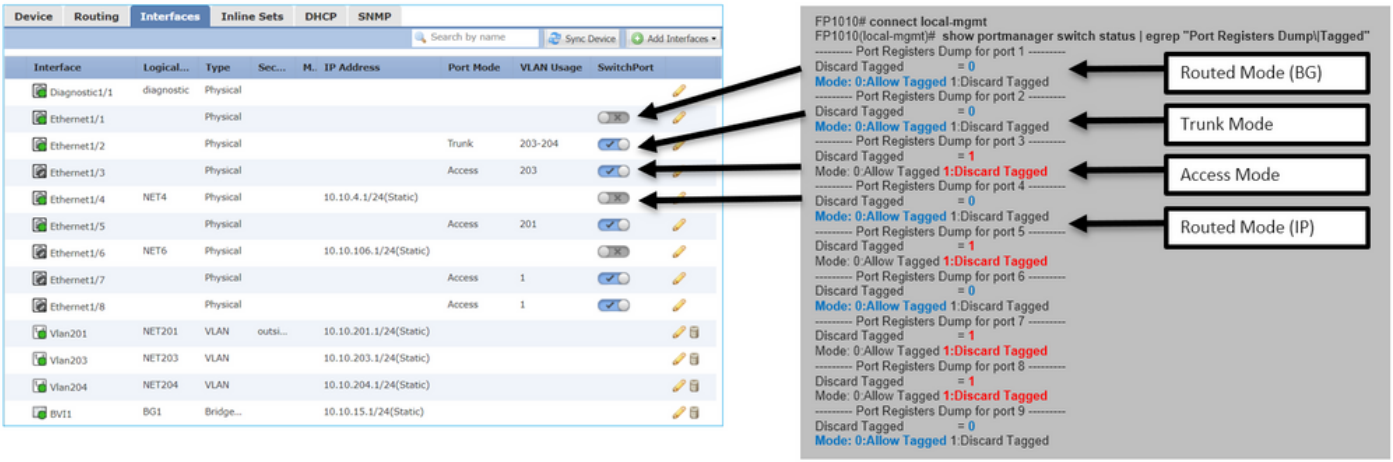
FP1010バックエンド

ポートレジスタは、すべての内部スイッチおよびポート機能を定義します。

このスクリーンショットは、ポートレジスタの「Port Control」セクションを示しています。特に、インターフェイスで受信されたタグ付きトラフィックを廃棄(1)するか、許可(0)するかを指定するレジスタが示されています。 1つのポートの完全な登録セクションを次に示します。

```
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
```

次のスクリーンショットでは、さまざまなポートモードのさまざまなタグ付き廃棄(DNA)レジスタ値を確認できます。

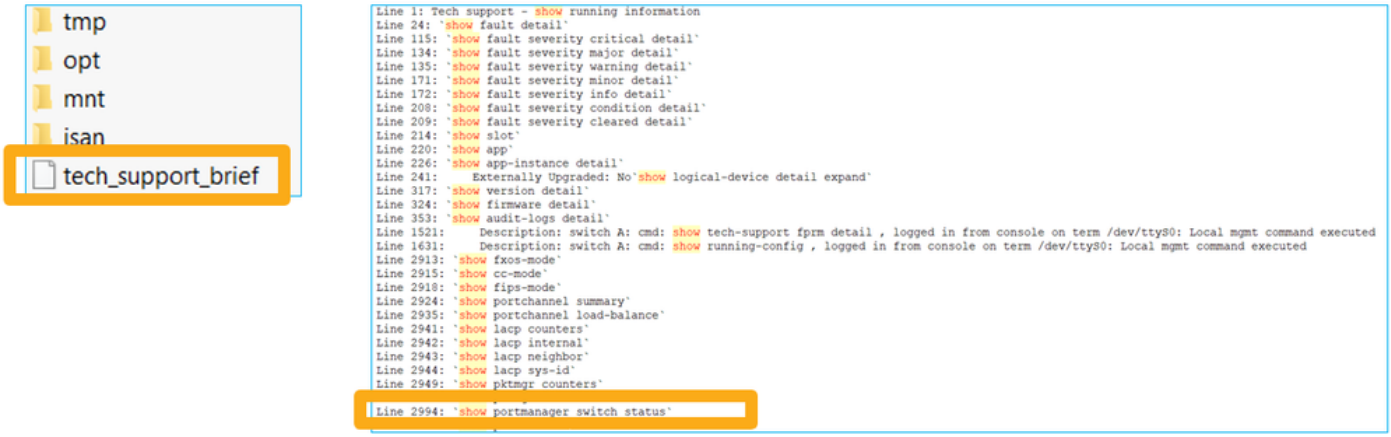


FP1010のFPRM show techを収集します。

FPRMバンドルを生成し、FTPサーバにアップロードするには、次の手順を実行します。

```
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
```

FPRMバンドルには、tech_support_briefというファイルが含まれています。tech_support_briefファイルには、一連のshowコマンドが含まれています。そのうちの1つが**show portmanager switch statusです**。



制限事項の詳細、一般的な問題、回避策

6.5リリースの実装の制限

- ダイナミックルーティングプロトコルは、SVIインターフェイスではサポートされていません。
- マルチコンテキストは1010ではサポートされていません。
- SVI VLAN IDの範囲は1 ~ 4070に制限されます。
- L2のポートチャネルはサポートされていません。
- フェールオーバーリンクとしてのL2ポートはサポートされていません。

スイッチ機能に関する制限

機能	説明	制限
VLANインターフェイスの数	作成可能なVLANインターフェイスの総数	60
トランクモードVLAN	トランクモードのポートで許可されるVLANの最大数	20
ネイティブVLAN	すべてのタグなしパケットをマップ ポート上で、ポート上で設定されたネイティブVLANに到達する	1
名前付きインターフェイス	すべての名前付きインターフェイスを含む (インターフェイスVLAN、サブインターフェイス、ポートチャネル、 物理インターフェイスなど)	60

その他の制限

- サブインターフェイスとインターフェイスVLANは、同じVLANを使用できません。
- BVIに参加しているすべてのインターフェイスは、同じクラスのインターフェイスに属している必要があります。
- BVIは、L3モードポートとL3モードポートサブインターフェイスを組み合わせて作成できます。
- インターフェイスVLANを組み合わせてBVIを作成できます。
- L3モードポートとインターフェイスVLANを混在させてBVIを作成することはできません。

関連情報

- Cisco Firepower 1010セキュリティアプライアンス
- 設定ガイド