Switch L2 no FPR1010, arquitetura, verificação e solução de problemas

Contents

Introduction

Este documento descreve o switch L2 em dispositivos FP1010. Especificamente, ele abrange principalmente a parte da implementação da Plataforma de Serviços de Segurança (SSP - Security Services Platform)/Sistema de Operação Extensiva Firepower (FXOS - eXtensive Operation System). Na versão 6.5, o Firepower 1010 (modelo de desktop) ativou os recursos de comutação no switch de hardware L2 integrado. Isso ajuda a evitar switches de hardware extras e o custo é reduzido.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

- O FP1010 é um modelo de desktop Small-Office Home-Office (SOHO) que substitui as plataformas ASA5505 e ASA5506-X.
- Suporte de software para imagens FTD (6.4+) gerenciadas pelo Firepower Management Center (FMC), pelo Firepower Device Manager (FDM) ou pelo Cloud Defense Orchestrator (CDO).
- Suporte de software para imagens ASA (9.13+) gerenciadas pelo CSM, ASDM ou CLI.
- O sistema operacional (SO), ASA ou FTD, é um pacote FXOS (semelhante ao FP21xx).
- 8 portas de dados de 10/100/1000 Mbps.
- As portas E1/7, E1/8 suportam PoE+.
- O switch de hardware permite a comunicação de taxa de linha entre portas (por exemplo: uma câmera é alimentada no servidor local).

Adições do Firepower 6.5

- Introdução de um novo tipo de Interface chamada Interface Virtual Comutada (SVI - Switched Virtual Interface).
- Modo misto: As interfaces podem ser configuradas no modo comutado (L2) ou não comutado (L3).
- As interfaces do modo L3 encaminham todos os pacotes para o aplicativo de segurança.
- As portas do modo L2 podem comutar no hardware se duas portas fizerem parte da mesma VLAN, o que melhora o throughput e a latência. E os pacotes que precisam ser roteados ou interligados acessam o aplicativo de segurança (por exemplo: uma câmera baixando um novo firmware da Internet) e passando por uma inspeção de segurança de acordo com a configuração.
- A interface física L2 pode ser associada a uma ou várias interfaces SVI.
- As interfaces do modo L2 podem estar no modo de acesso ou tronco.
- A interface L2 do modo de acesso permite somente tráfego não marcado.

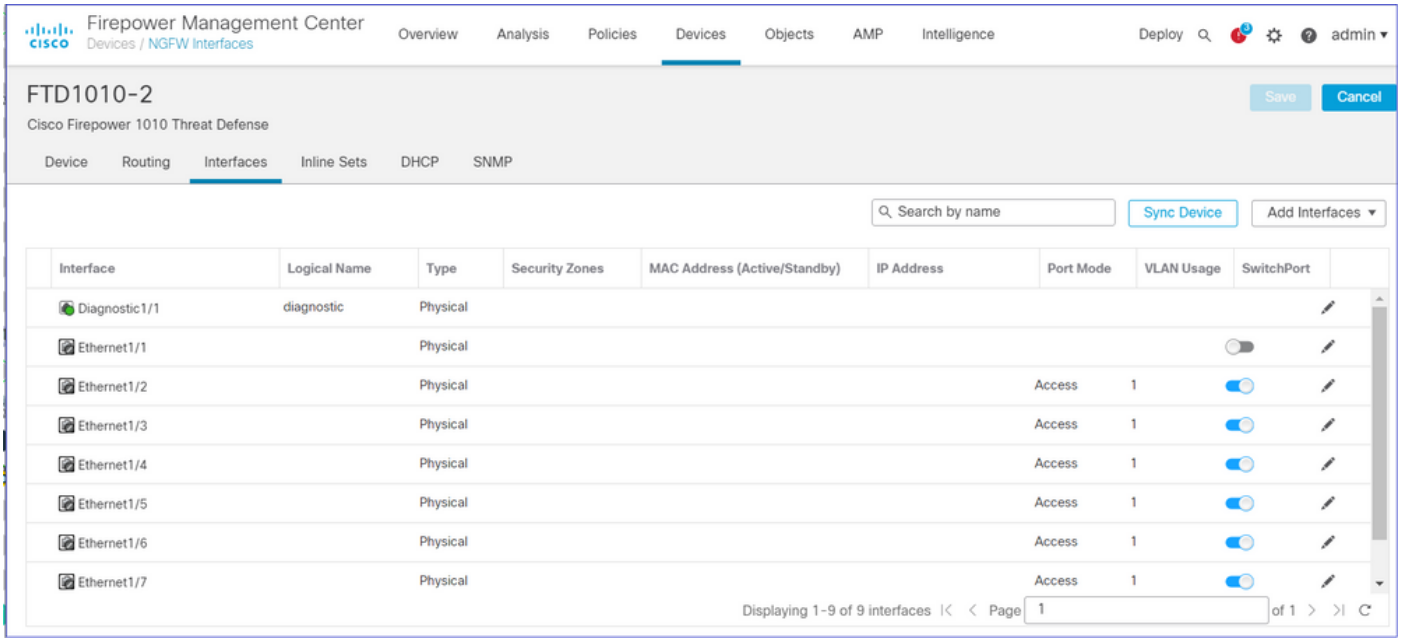
- A interface L2 do modo de tronco permite tráfego marcado.
- Suporte a VLAN nativa para interface L2 de modo de tronco.
- As CLIs ASA, ASDM, CSM, FDM, FMC são aprimoradas para oferecer suporte a novos recursos.

Adições de FMC

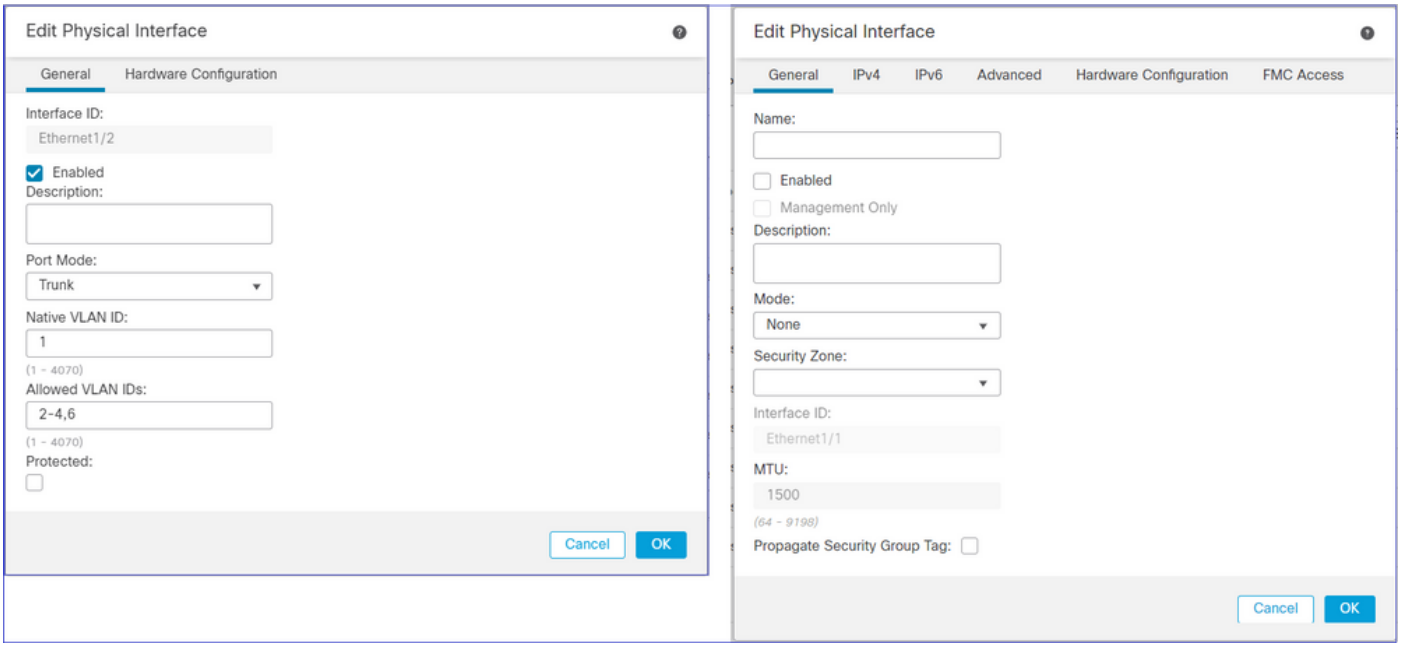
- Um novo modo de interface chamado switchport foi introduzido para uma interface física que é usada para identificar se uma interface física é uma interface L3 ou L2.
- A interface física L2 pode ser associada a uma ou várias interfaces VLAN com base no modo de acesso ou tronco.
- O Firepower 1010 suporta a configuração Power Over Ethernet (PoE) nas duas últimas interfaces de dados, por exemplo, Ethernet1/7 e Ethernet1/8.
- A alteração de interface entre comutado e não comutado limpa todas as configurações, exceto a configuração de PoE e hardware.

Como funciona

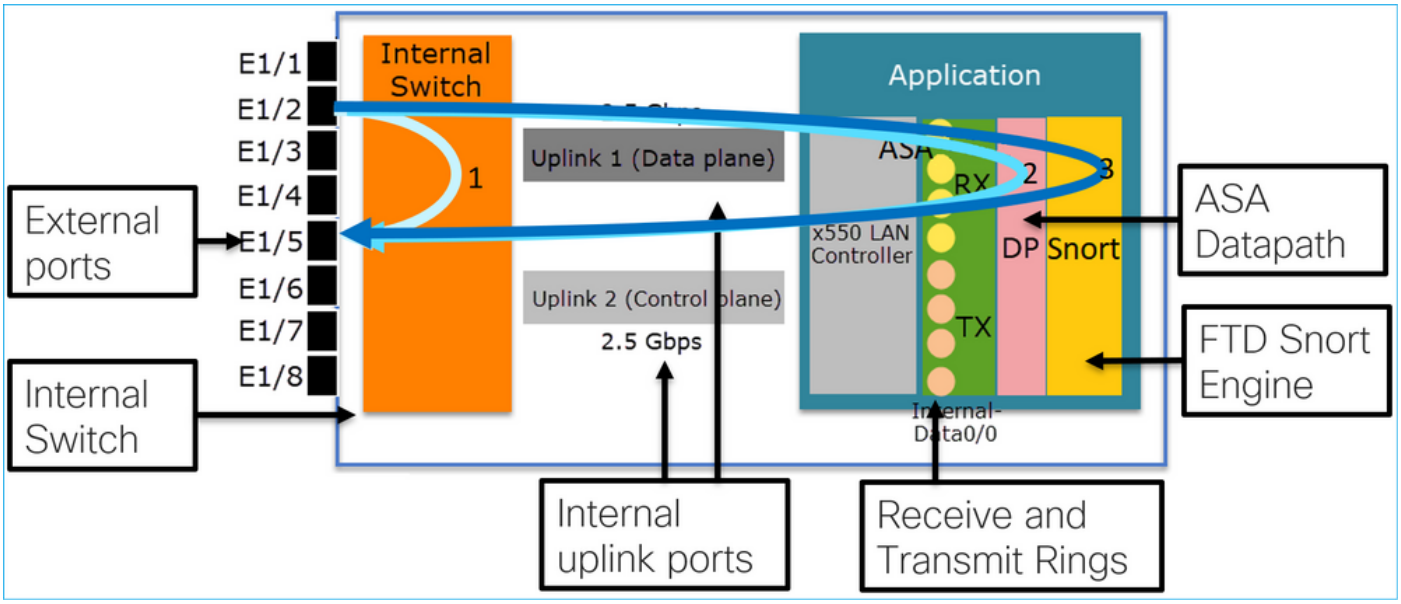
Este recurso é apenas um aprimoramento do suporte à Interface existente no FMC (**Gerenciamento de dispositivos > Página de interface**).



Vista da interface física (L2 e L3)



Arquitetura FP1010



- 8 portas de dados externos.
- 1 Switch interno.
- 3 portas de uplink (2 delas exibidas na figura), uma para plano de dados, uma para plano de controle, outra para configuração.
- Controlador de LAN x550 (a interface entre o aplicativo e os uplinks).
- 4 Anéis de recepção (RX) e 4 de transmissão (TX).
- Processo de datapath (no ASA e FTD).
- Processo Snort (no FTD).

Processamento de pacote

Dois fatores principais podem afetar o processamento de pacotes:

1. Modo de interface/porta

2. Política aplicada

Um pacote pode atravessar um FP1010 de três maneiras diferentes:

1. Somente processado pelo switch interno

2. Encaminhado até o aplicativo (ASA/FTD) e processado somente pelo processo de datapath

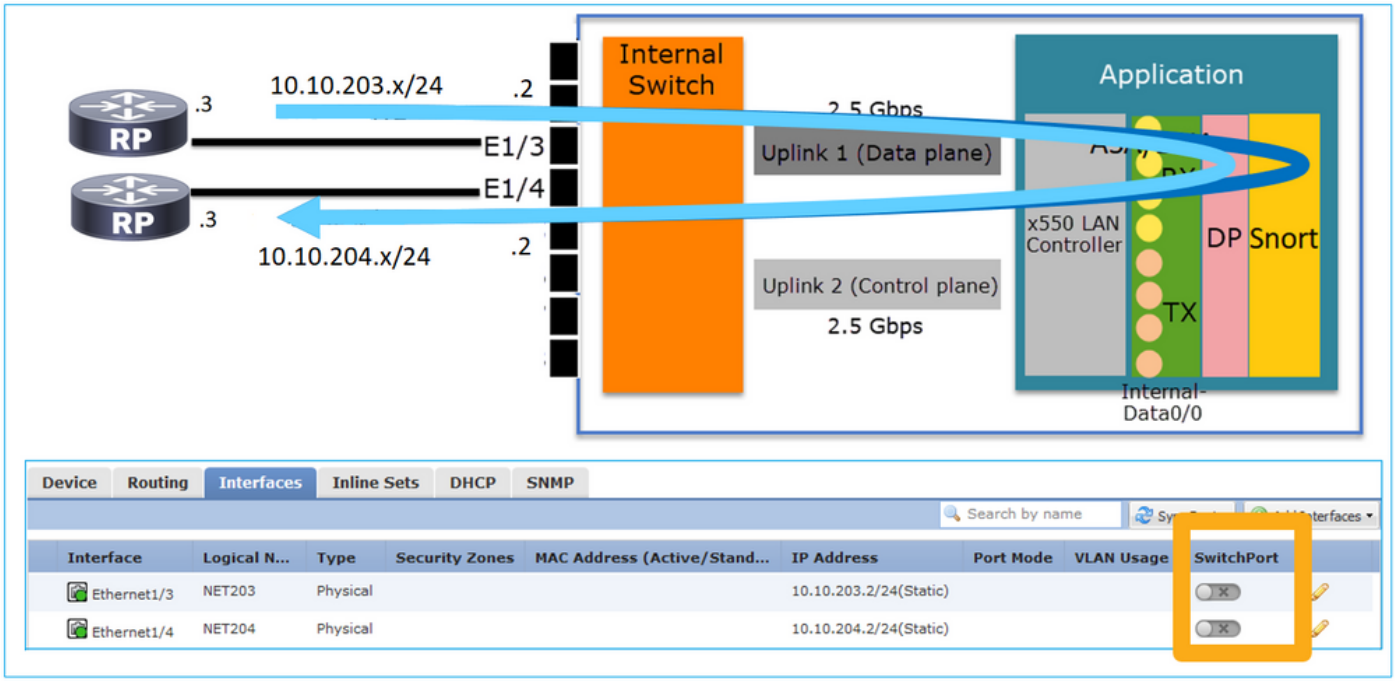
3. Encaminhado até o aplicativo (FTD) e processado pelo datapath e pelo mecanismo Snort

Modos de porta FP1010

Os exemplos de IU são para o FMC; os exemplos de CLI são para o FTD. A maioria dos conceitos também é totalmente aplicável a um ASA.

FP1010 Caso 1. Portas roteadas (roteamento IP)

Configuração e operação



Principais pontos

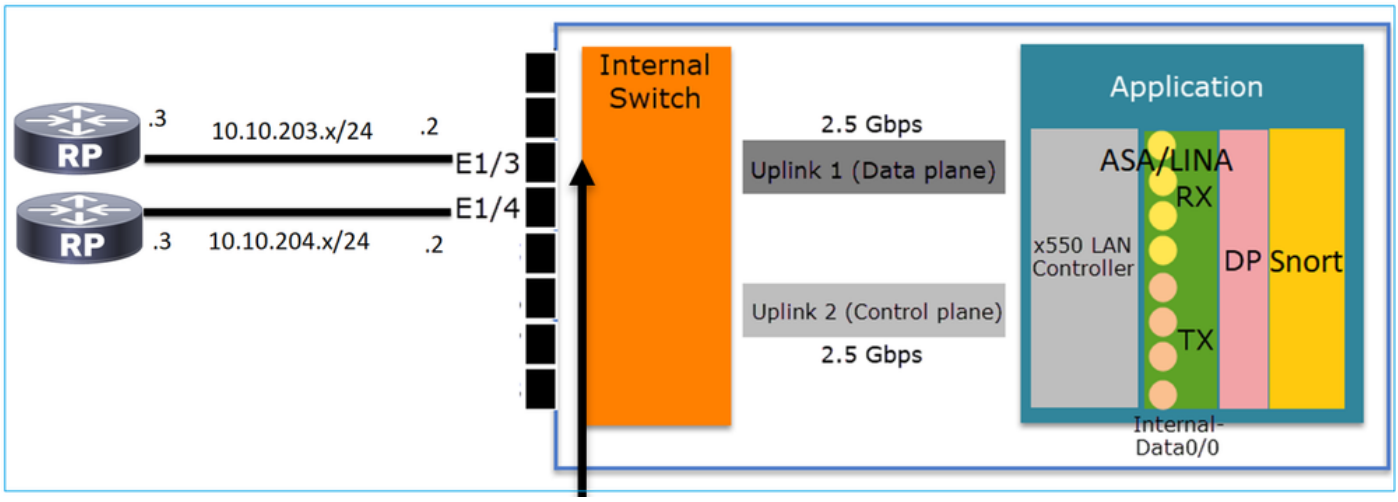
- Do ponto de vista do projeto, as 2 portas pertencem a 2 sub-redes L2 diferentes.
- Quando as portas são configuradas no modo roteado, os pacotes são processados pelo aplicativo (ASA ou FTD).
- No caso do FTD, com base na ação da regra (por exemplo, ALLOW), os pacotes podem até ser inspecionados pelo mecanismo Snort.

configuração de 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
```

Verificação de porta roteada FP1010



Na CLI do FXOS, você pode verificar os contadores da interface física. Este exemplo mostra os contadores unicast de entrada e unicast de saída na 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
```

Capturas de dados FTD podem ser aplicadas e os pacotes podem ser rastreados:

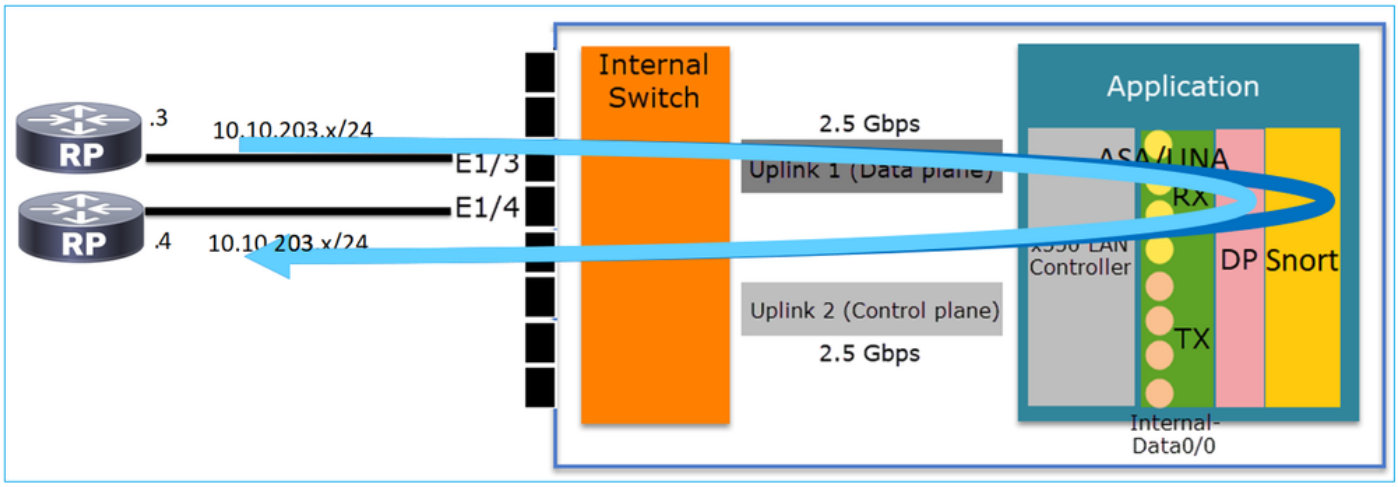
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

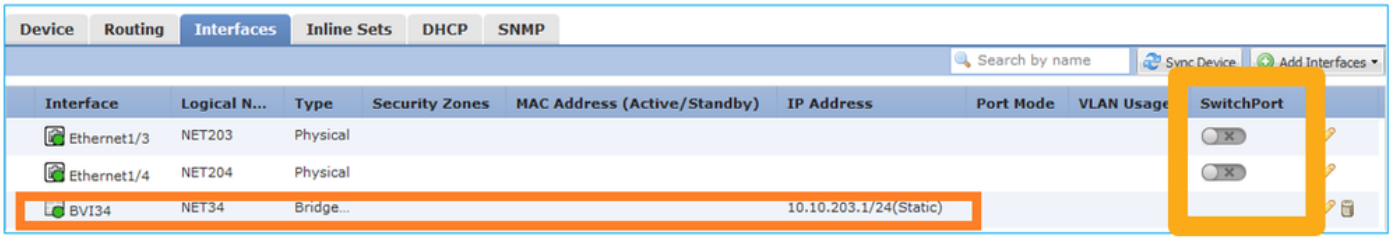
Este é um trecho de captura. Como esperado, o pacote é encaminhado com base em uma PESQUISA DE ROTA:

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

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

FP1010 Caso 2. Modo de Grupo de Bridge (Bridging)

Configuração e operação





Principais pontos

- Do ponto de vista do projeto, as 2 portas são conectadas à mesma sub-rede L3 (semelhante a um firewall transparente), mas com VLAN diferente.
- Quando as portas são configuradas no modo Bridging, os pacotes são processados pelo aplicativo (ASA ou FTD).
- No caso do FTD, com base na ação da regra (por exemplo, ALLOW), os pacotes podem até ser inspecionados pelo mecanismo Snort.

configuração de 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
```

Verificação de porta de grupo de ponte FP1010

Esse comando mostra os membros da interface da BVI 34:

```
FP1010# show bridge-group 34
 Interfaces:
 Ethernet1/3 Ethernet1/4
 Management System IP Address:  10.10.203.1 255.255.255.0
 Management Current IP Address: 10.10.203.1 255.255.255.0
 Management IPv6 Global Unicast Address(es):    N/A
```

```
 Static mac-address entries:  0
 Dynamic mac-address entries: 13
```

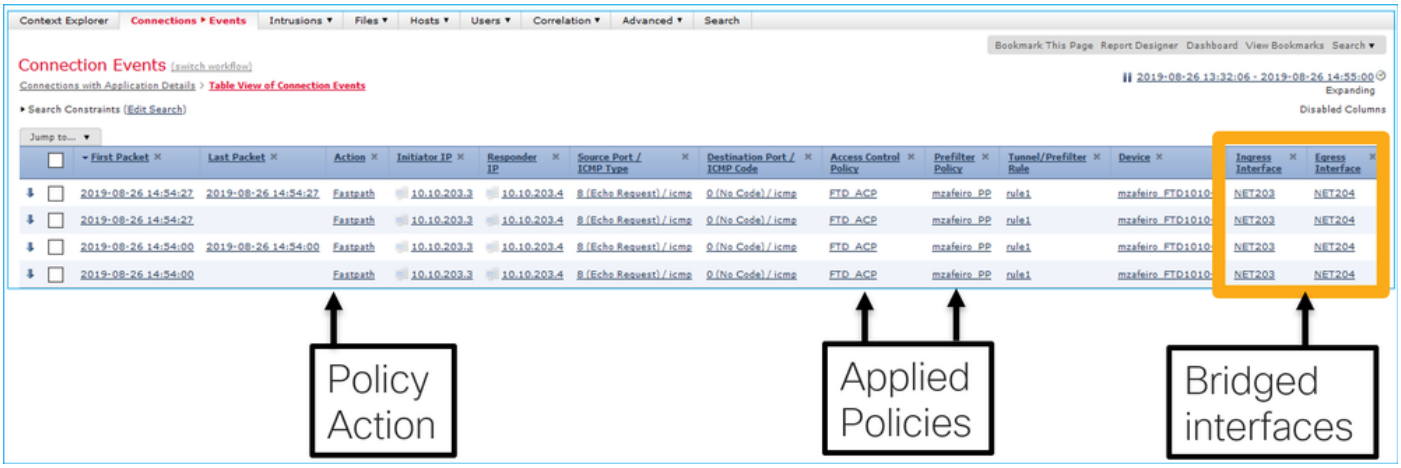
Este comando mostra a tabela CAM (Content Addressable Memory, memória endereçável de conteúdo) do ASA/FTD:

```
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
```

Um snippet de rastreamento de pacote mostra que o pacote é encaminhado com base na pesquisa de destino MAC L2:

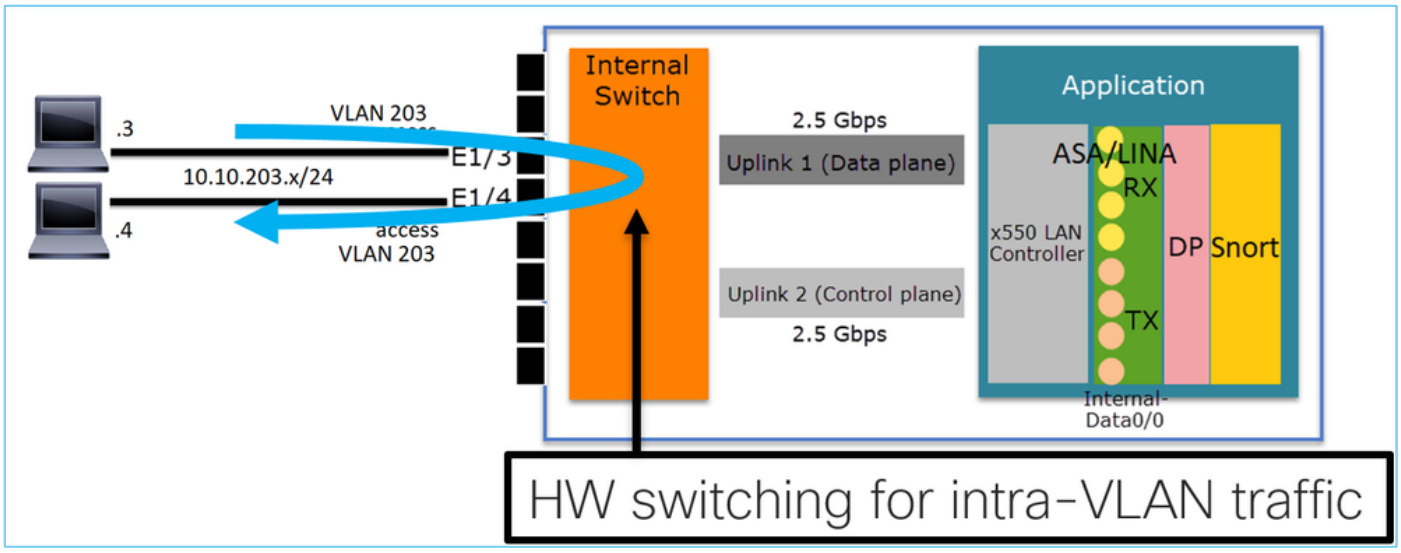
```
FP1010# show cap CAP203 packet-number 1 trace

2 packets captured

1: 11:34:40.277619 10.10.203.3 > 10.10.203.4 icmp: echo request
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP Subtype: Destination MAC L2 Lookup
Result: ALLOW
Config:
Additional Information:
DestinationMAC lookup resulted in egress ifc NET204
```

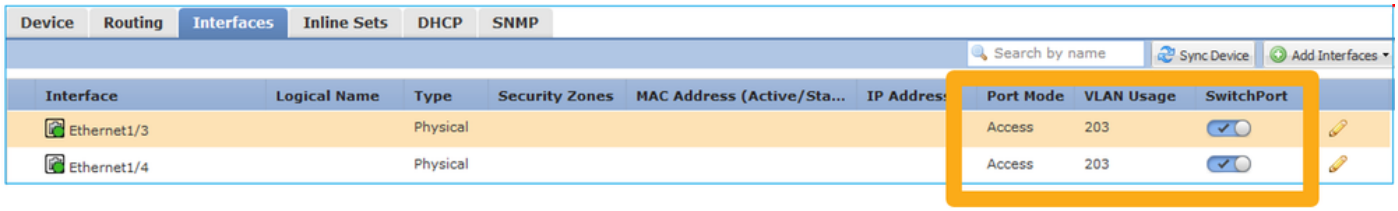
No caso do FTD, os eventos de conexão do FMC também podem fornecer informações sobre a inspeção de fluxo e as interfaces do grupo de ponte de trânsito:



FP1010 Caso 3. Switchports (HW switching) no modo de acesso

Configuração e operação





Principais pontos

- O HW Switching é um recurso FTD **6.5+** e ASA **9.13+**.
- Do ponto de vista do projeto, as 2 portas são conectadas à mesma sub-rede L3 e à mesma VLAN.
- As portas neste cenário estão operando no modo de acesso (somente tráfego não marcado).
- As portas de firewall configuradas no modo SwitchPort não têm um nome lógico (nome se) configurado.
- Quando as portas são configuradas no modo de switching e pertencem à mesma VLAN (tráfego intra-VLAN), os pacotes são processados somente pelo switch interno FP1010.

configuração de interface FTD

Do ponto de vista da CLI, a configuração é muito semelhante a um switch L2:

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

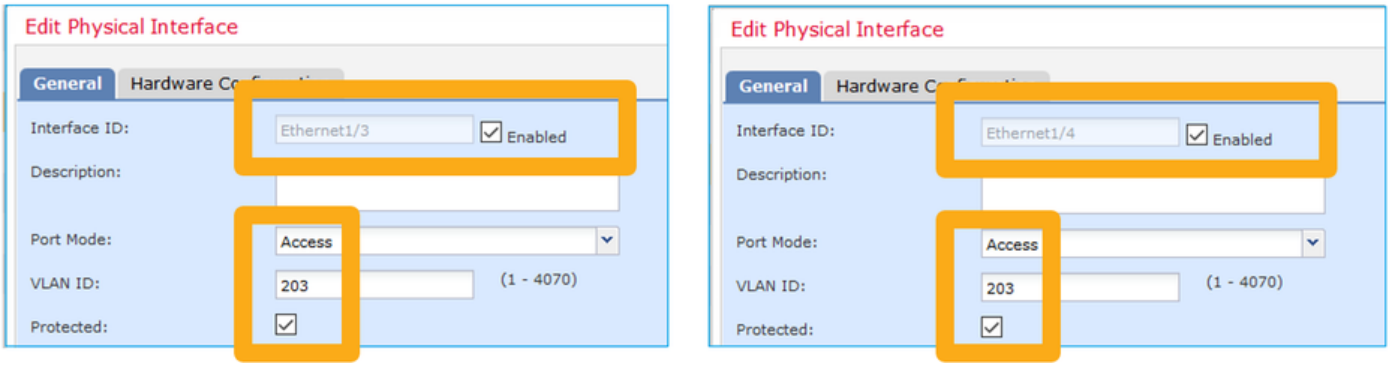
Filtrando tráfego entre VLANs

O desafio: **Uma ACL não pode filtrar o tráfego entre VLANs!**

A solução: Portas **protegidas**

O princípio é muito simples: 2 portas configuradas como Protegidas não podem se comunicar entre si.

IU do FMC no caso de portas protegidas:



configuração de interface FTD

O comando **switchport protected** está configurado na interface:

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

Verificação de porta do switch FP1010

Neste exemplo, há 1.000 pacotes unicast (ICMP) enviados com um tamanho específico (1.100 bytes):

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

Para verificar os contadores unicast de entrada e saída das interfaces de trânsito, use este comando:

```
FP1010(local-mgmt)# show portmanager counters ethernet 1 3 | egrep
"stats.ing_unicastframes\|stats.bytes_1024to1518_frames"
stats.ing_unicastframes         = 146760
stats.bytes_1024to1518_frames   = 0
FP1010(local-mgmt)# show portmanager counters ethernet 1 4 | egrep
"stats.egr_unicastframes\|stats.bytes_1024to1518_frames"
stats.bytes_1024to1518_frames   = 0
stats.egr_unicastframes         = 140752
FP1010(local-mgmt)# show portmanager counters ethernet 1 3 | egrep
"stats.ing_unicastframes\|stats.bytes_1024to1518_frames"
stats.ing_unicastframes         = 147760 <------------------ Ingress Counters got increased by
1000
stats.bytes_1024to1518_frames   = 1000 <------------------ Ingress Counters got increased by 1000
FP1010(local-mgmt)# show portmanager counters ethernet 1 4 | egrep
"stats.egr_unicastframes\|stats.bytes_1024to1518_frames"
stats.bytes_1024to1518_frames   = 0 <------------------ No egress increase
stats.egr_unicastframes         = 140752 <------------------ No egress increase
```

Este comando mostra o status da VLAN do switch interno:

```
FP1010# show switch vlan
```

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

O status de uma VLAN é UP desde que pelo menos uma porta seja atribuída à VLAN

Se uma porta estiver administrativamente inativa ou a porta do switch conectado estiver inativa/desconectada por cabo e esta for a única porta atribuída à VLAN, o status da VLAN também estará inoperante:

```
FP1010-2# show switch vlan
VLAN Name                            Status    Ports
---- ------------------------------- --------- -----------------------------
1    -                               down 201  net201                              down
Ethernet1/1 <--- e1/1 was admin down 202  net202                            down Ethernet1/2 <---
upstream switch port is admin down
```

Este comando mostra a tabela CAM do 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
```

O tempo de envelhecimento padrão da tabela CAM do switch interno é de 5 minutos e 30 segundos.

FP1010 contém 2 tabelas CAM:

1. **Tabela CAM do Switch interno**: Usado no caso de switching de hardware
2. **Tabela CAM de dados ASA/FTD**: Usado em caso de Bridging

Cada pacote/quadro que atravessa o FP1010 é processado por uma única tabela CAM (switch interno ou datapath FTD) com base no modo de porta.

> **Caution**: Não confunda a tabela CAM do switch interno **show switch mac-address-table** usada no modo SwitchPort com a tabela CAM de dados **show mac-address-table** FTD usada no modo de ponte

Comutação de HW: Coisas adicionais que devem estar cientes

Os registros de dados do ASA/FTD não mostram informações sobre os fluxos comutados por HW:

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

A tabela de conexão de dados ASA/FTD não mostra os fluxos comutados por HW:

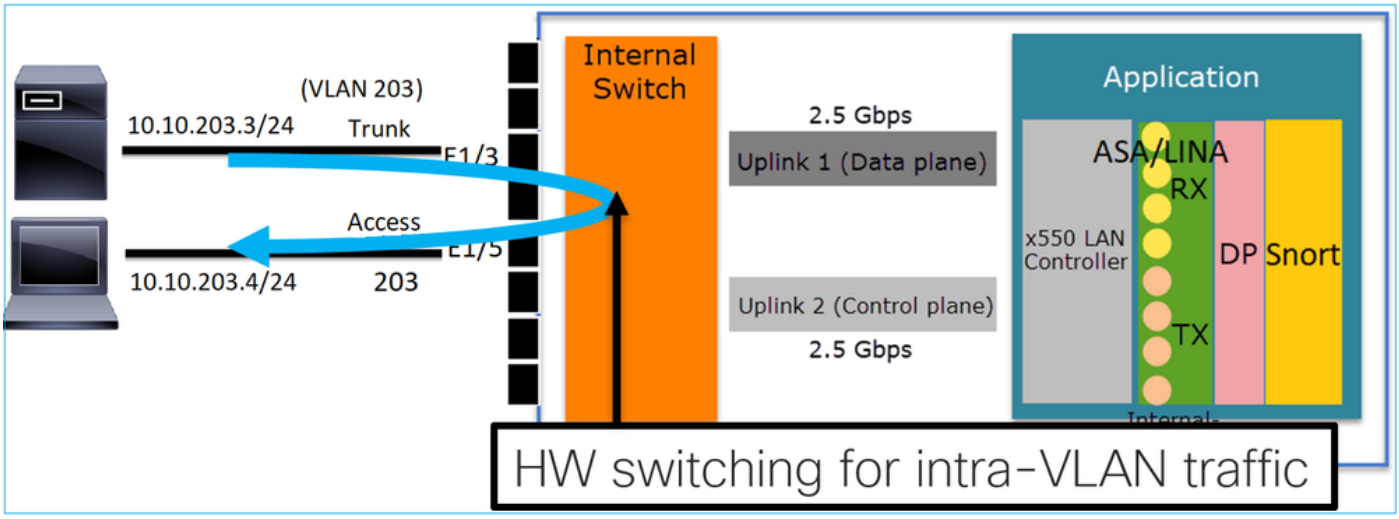
```
FP1010# show conn
```

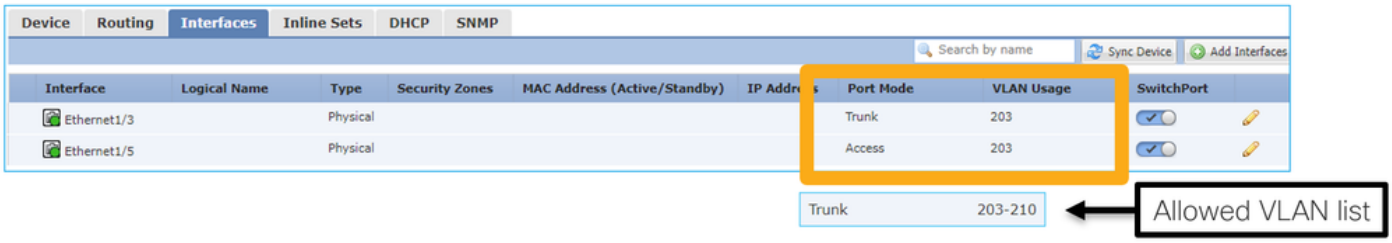
```
0 in use, 3 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

Além disso, os eventos de conexão do FMC não mostram fluxos comutados por HW.

FP1010 Caso 4. Portas de switch (entroncamento)

Configuração e operação





Principais pontos

- O HW Switching é um recurso FTD **6.5+** e ASA **9.13+**.
- Do ponto de vista do projeto, as 2 portas são conectadas à mesma sub-rede L3 e à mesma VLAN.
- A porta de tronco aceita quadros marcados e não marcados (no caso de uma VLAN nativa).
- Quando as portas são configuradas no modo de switching e pertencem à mesma VLAN (tráfego intra-VLAN), os pacotes são processados somente pelo switch interno.

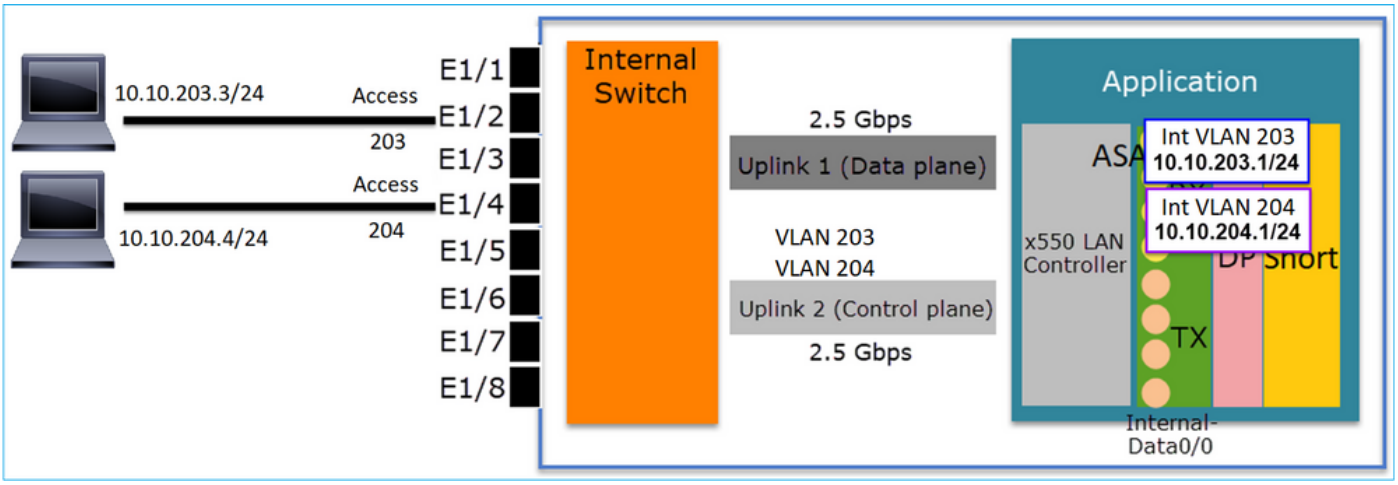
configuração de interface FTD

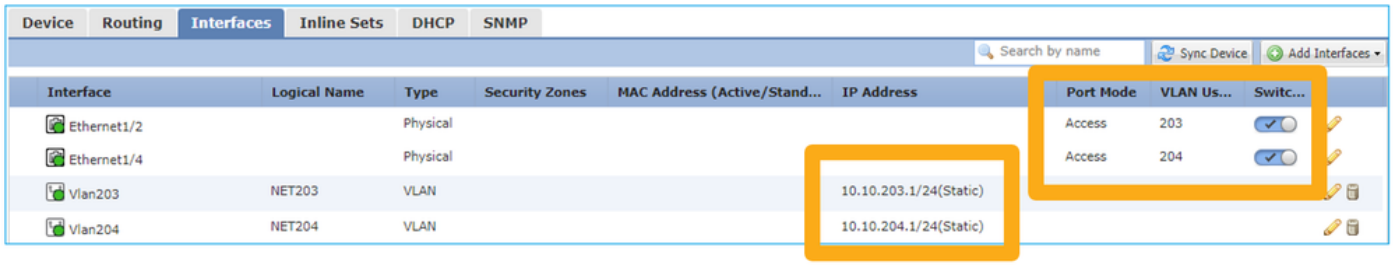
A configuração é semelhante a uma porta de switch da camada 2:

```
interface Ethernet1/3 switchport switchport trunk allowed vlan 203 switchport trunk native vlan
1 switchport mode trunk
!
interface Ethernet1/5
 switchport
 switchport access vlan 203
```

FP1010 Caso 5. Portas de switch (Inter-VLAN)

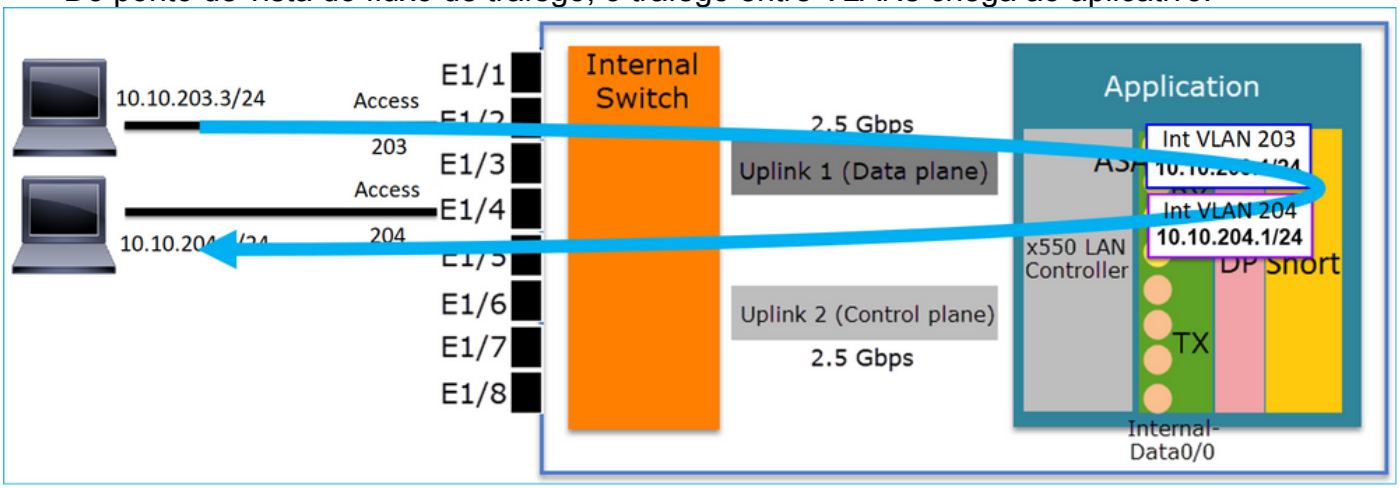
Configuração e operação





Principais pontos

- Do ponto de vista do projeto, as 2 portas são conectadas a 2 sub-redes L3 diferentes e 2 VLANs diferentes.
- O tráfego entre as VLANs passa pelas interfaces de VLAN (semelhantes às SVIs).
- Do ponto de vista do fluxo de tráfego, o tráfego entre VLANs chega ao aplicativo.



configuração de interface FTD

A configuração é semelhante a uma SVI (Switch Virtual Interface, Interface virtual do switch):

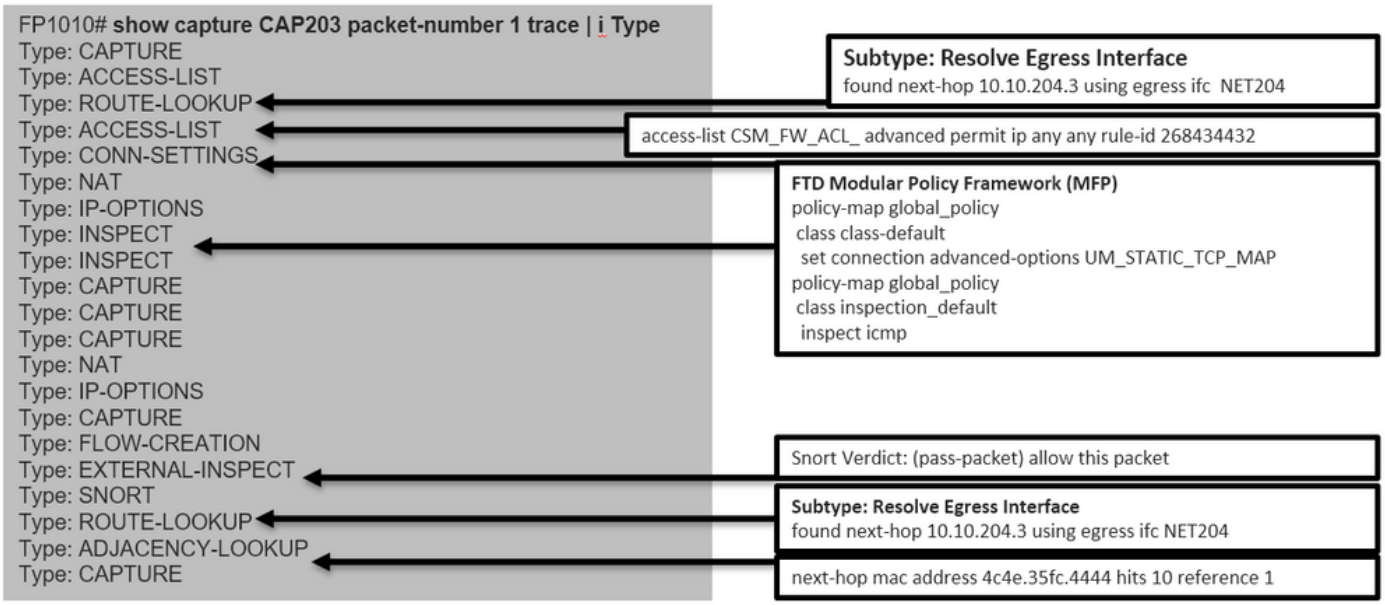
```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

Processamento de pacotes para tráfego entre VLANs

Este é um rastreamento de um pacote que atravessa 2 VLANs diferentes:

```
FP1010# show capture CAP203 packet-number 1 trace | include Type
Type: CAPTURE
Type: ACCESS-LIST
Type: ROUTE-LOOKUP
Type: ACCESS-LIST
Type: CONN-SETTINGS
Type: NAT
Type: IP-OPTIONS
Type: INSPECT
Type: INSPECT
Type: CAPTURE
Type: CAPTURE
Type: CAPTURE
Type: NAT
Type: IP-OPTIONS
Type: CAPTURE
Type: FLOW-CREATION
Type: EXTERNAL-INSPECT
Type: SNORT
Type: ROUTE-LOOKUP
Type: ADJACENCY-LOOKUP
Type: CAPTURE
```

As principais fases do processo do pacote:



FP1010 Caso 6. Filtro entre VLANs

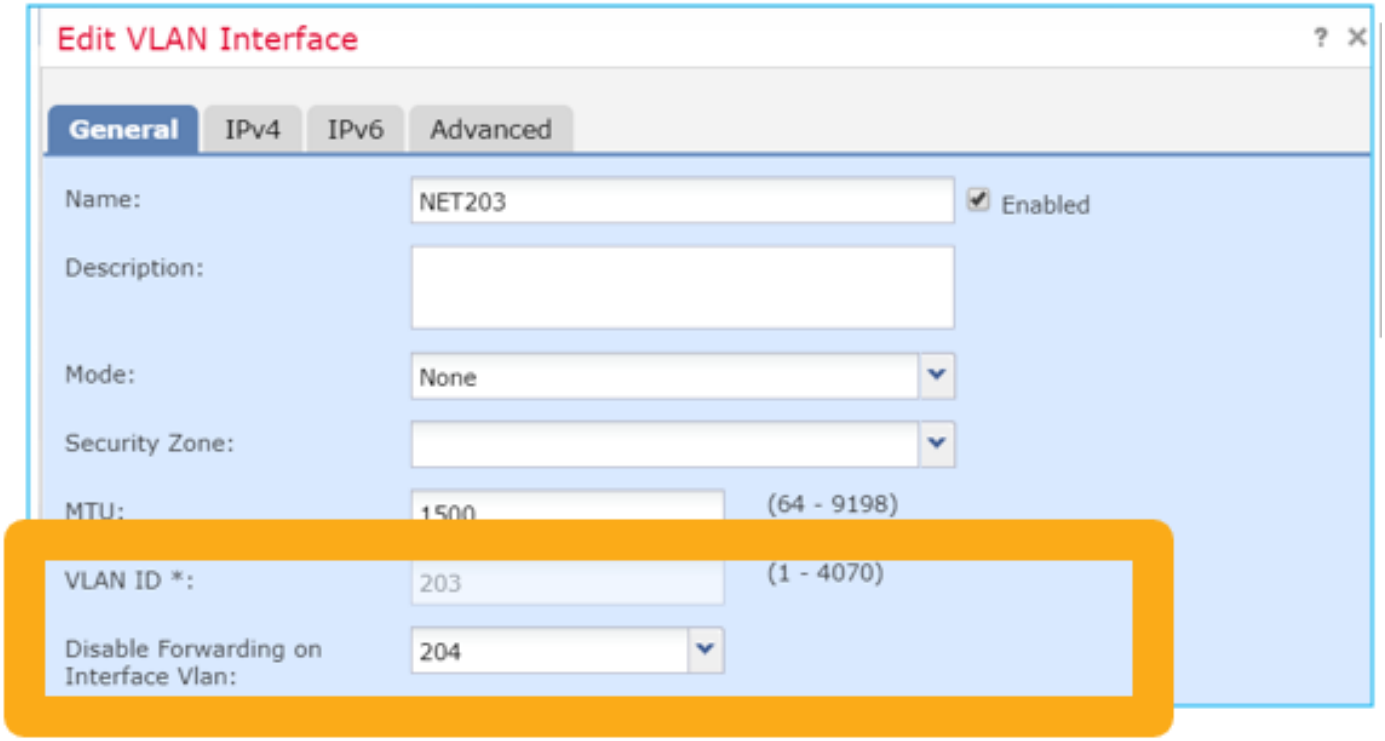
Configuração e operação

Há duas opções principais para filtrar o tráfego entre VLANs:

1. Política de controle de acesso
2. "no forward"

Filtrar o tráfego entre VLANs com o uso do comando 'no forward'

Configuração da IU da FMC:



Principais pontos

- A queda para frente é unidirecional.
- Ele não pode ser aplicado às duas interfaces VLAN.
- A verificação no forward é feita antes da verificação da ACL.

configuração de interface FTD

A configuração da CLI neste caso é:

```
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 um pacote for descartado pelo recurso no forward, uma mensagem de syslog de dados ASA/FTD será gerada:

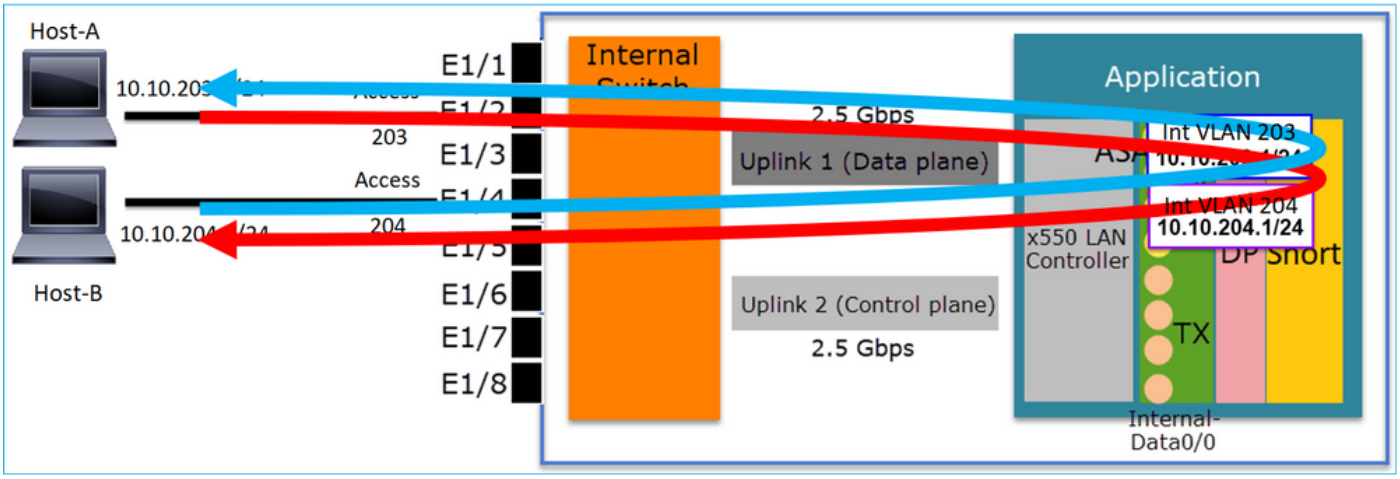
```
FP1010# show log
Sep 10 2019 07:44:54: %FTD-5-509001: Connection attempt was prevented by "no forward" command:
icmp src NET203:10.10.203.3 dst NET204:10.10.204.3 (type 8, code 0)
```

Do ponto de vista do Accelerated Security Path (ASP), ele é considerado uma queda da ACL:

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

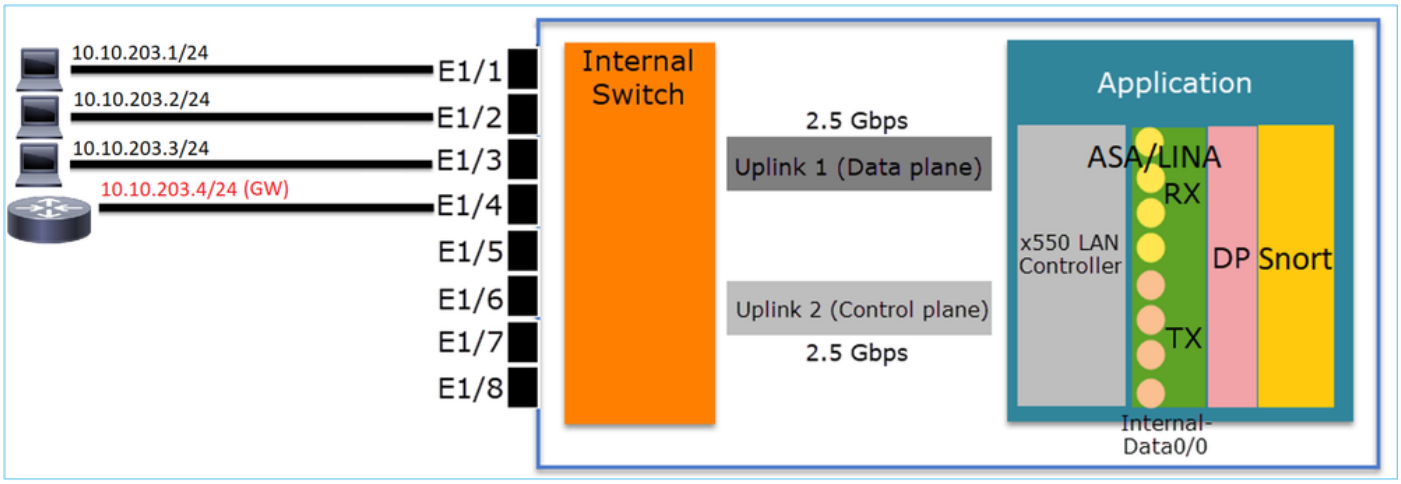
Como a queda é unidirecional, o Host-A (VLAN 203) não pode iniciar o tráfego para o Host-B

(VLAN 204), mas o oposto é permitido:



Estudo de caso - FP1010. Bridging vs HW Switching + Bridging

Considere a seguinte topologia:



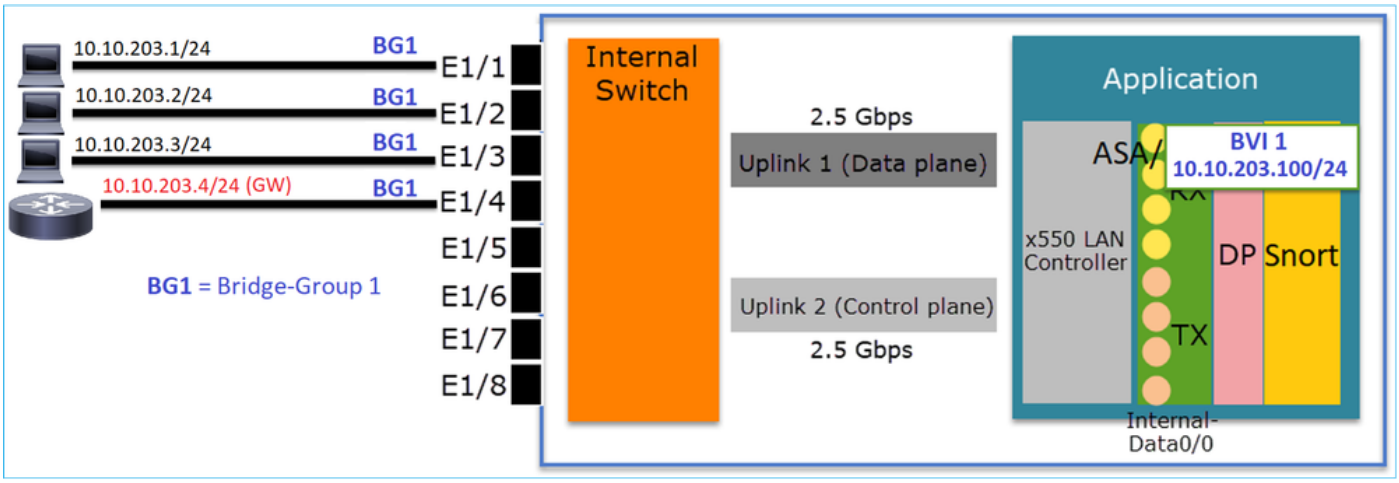
Nesta topologia:

- Três hosts finais pertencem à mesma sub-rede L3 (10.10.203.x/24).
- O roteador (10.10.203.4) atua como um GW na sub-rede.

Nesta topologia, há duas opções principais de projeto:

1. Bridging
2. Comutação de HW + Bridging

Opção de design 1. Bridging

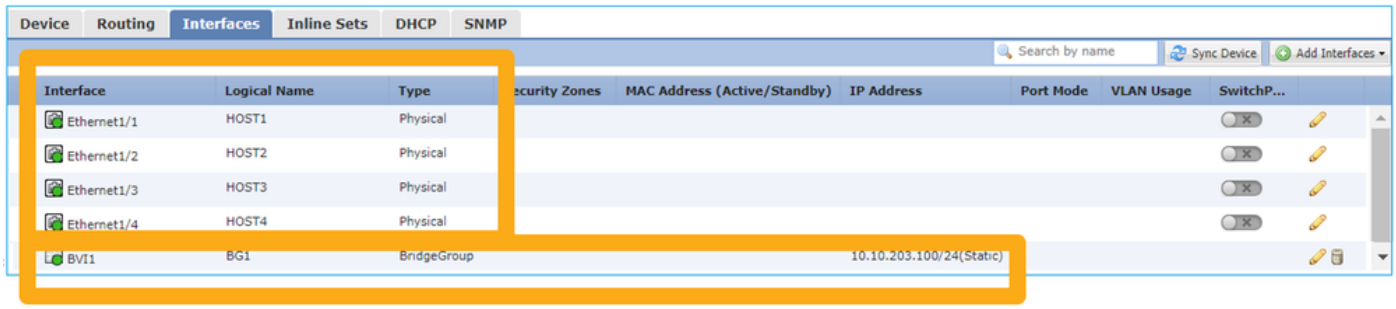


Principais pontos

Os principais pontos deste projeto são:

- Há a BVI 1 criada com um IP na mesma sub-rede (10.10.203.x/24) dos 4 dispositivos conectados.
- Todas as quatro portas pertencem ao mesmo grupo de bridge (grupo 1 nesse caso).
- Cada uma das quatro portas tem um nome configurado.
- A comunicação host-a-host e host-a-GW passa pelo aplicativo (por exemplo, FTD).

Do ponto de vista da IU da FMC, a configuração é:

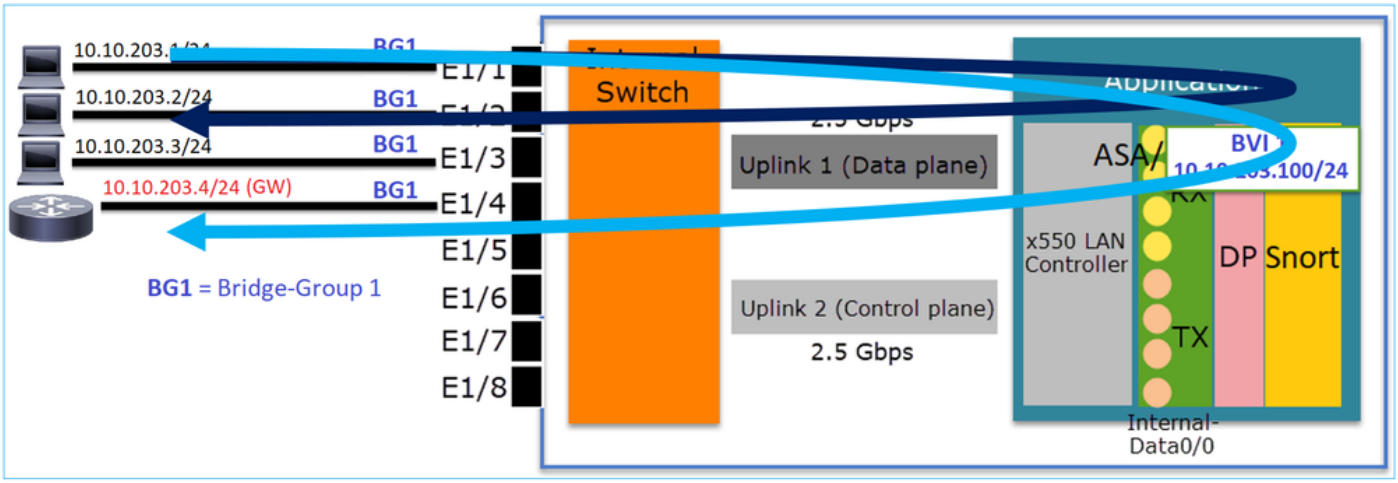


configuração de interface FTD

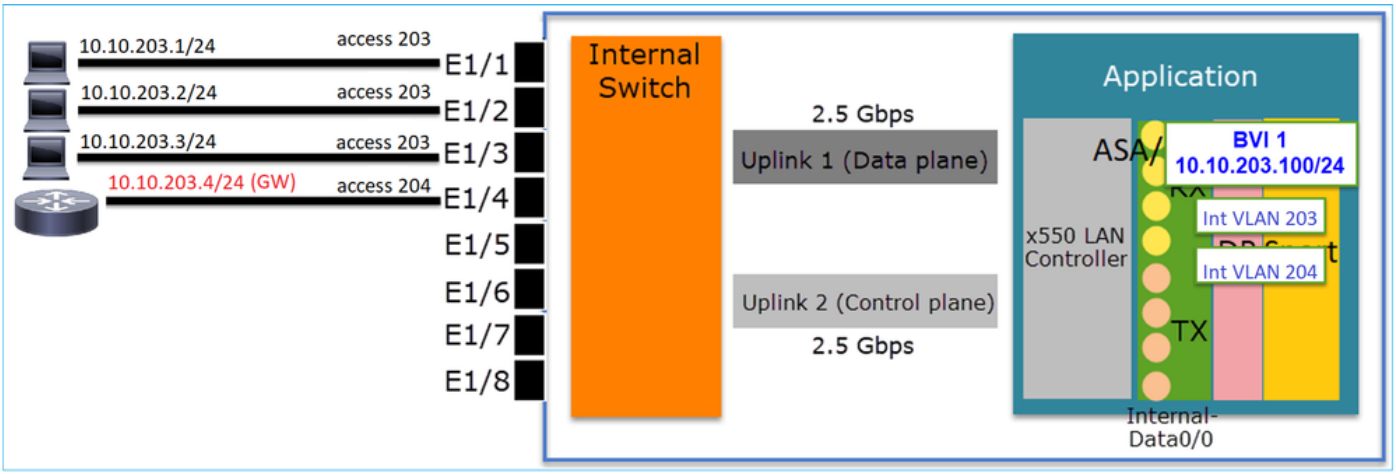
A configuração neste caso é:

```
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
```

O fluxo de tráfego neste cenário:



Opção de design 2. Comutação de HW + Bridging

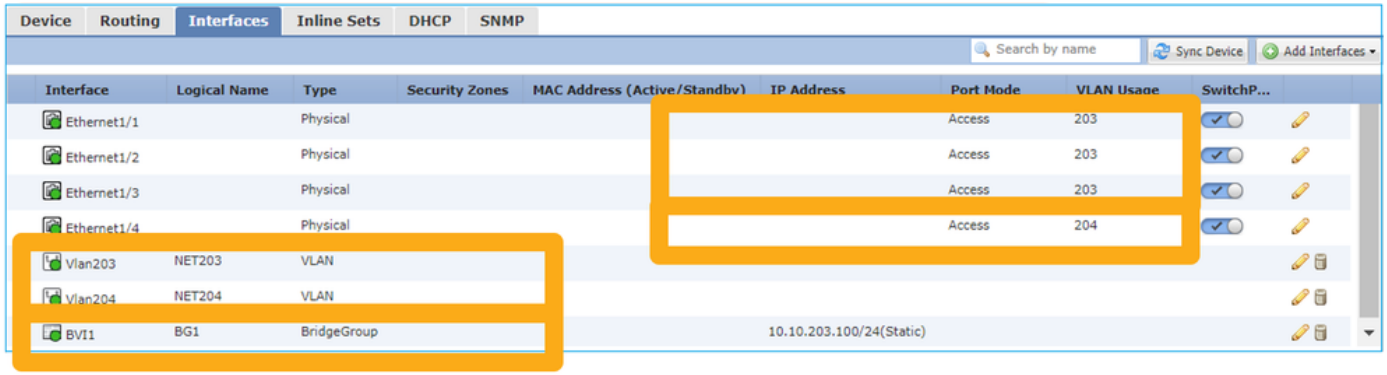


Principais pontos

Os principais pontos deste projeto são:

- Há a BVI 1 criada com um IP na mesma sub-rede (10.10.203.x/24) dos 4 dispositivos conectados.
- As portas conectadas aos hosts finais são configuradas no modo SwitchPort e pertencem à mesma VLAN (203).
- A porta conectada ao GW é configurada no modo SwitchPort e pertence a uma VLAN diferente (204).
- Há 2 interfaces de VLAN (203, 204). As 2 interfaces de VLAN não têm um IP atribuído e pertencem ao Grupo de Bridge 1.
- A comunicação host-a-host passa somente pelo switch interno.
- A comunicação de host para GW passa pelo aplicativo (por exemplo, FTD).

Configuração da IU da FMC:

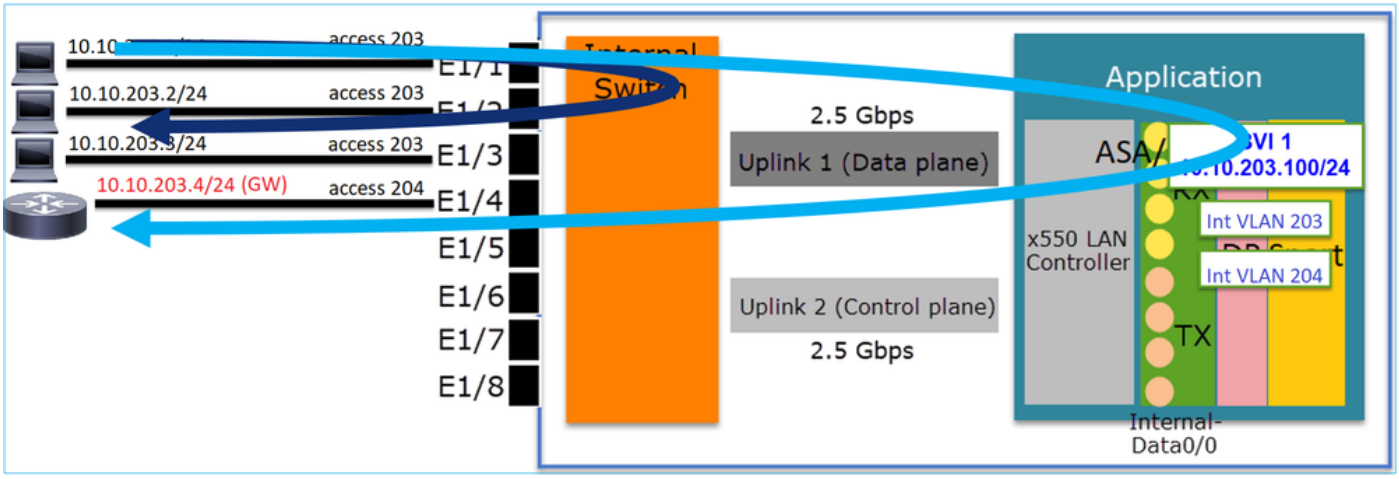


configuração de interface FTD

A configuração neste caso é:

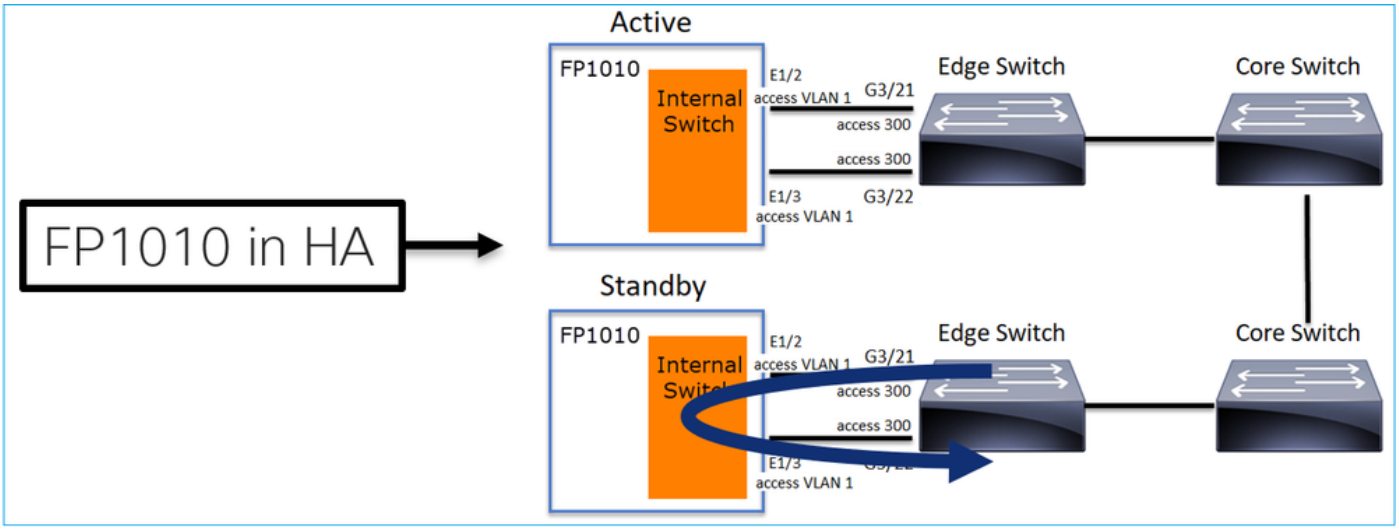
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1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

Comunicação host a host versus comunicação host a GW:



Considerações sobre o design do FP1010

Switching e alta disponibilidade (HA)

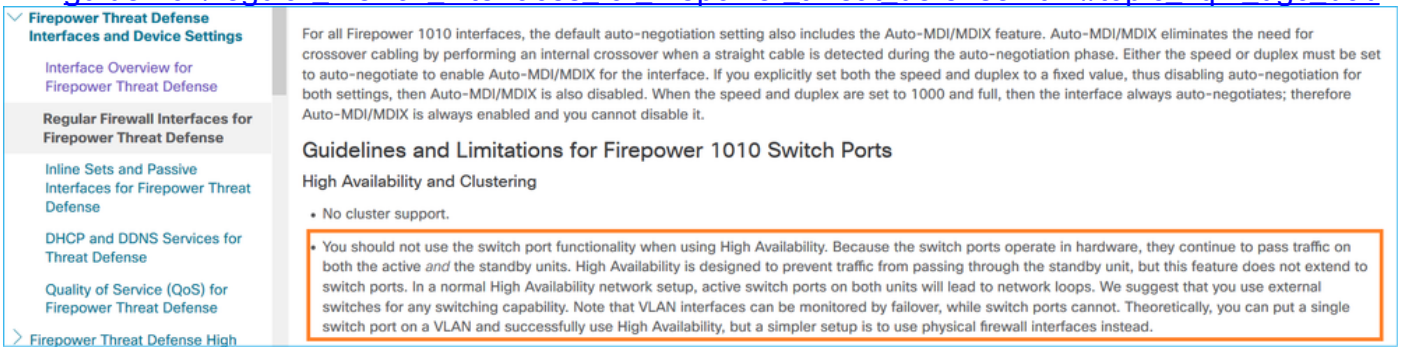


Há dois problemas principais quando a comutação HW é configurada em um ambiente HA:

1. A comutação de HW na unidade de standby encaminha pacotes através do dispositivo. Isso pode causar loops de tráfego.
2. SwitchPorts não são monitorados por HA

Requisito de design

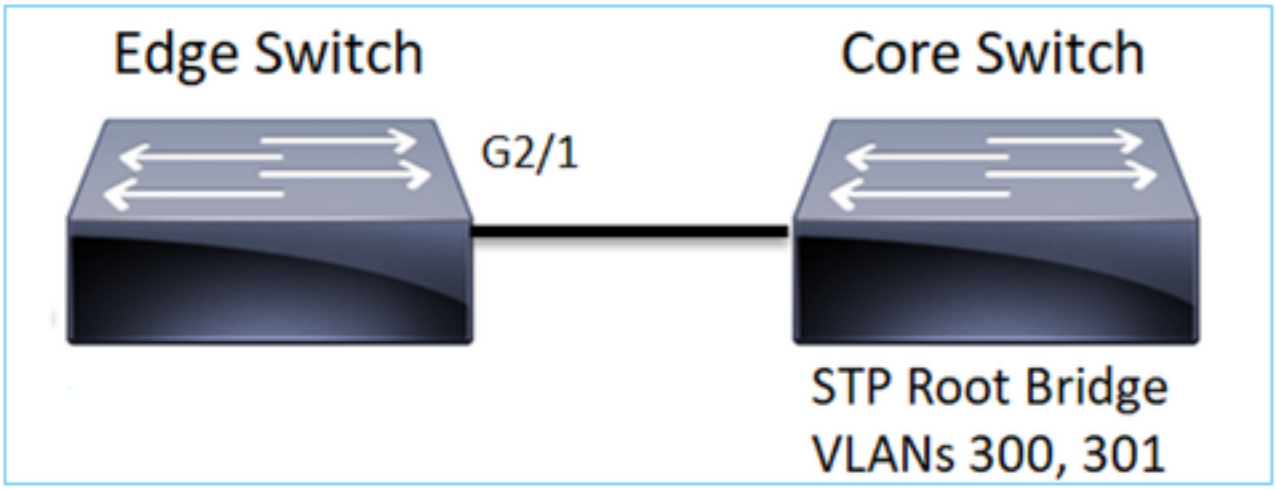
- Você não deve usar a funcionalidade SwitchPort com a alta disponibilidade do ASA/FTD. Isso está documentado no guia de configuração do FMC: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b



Interação com o Spanning Tree Protocol (STP)

O switch interno FP1010 não executa o STP.

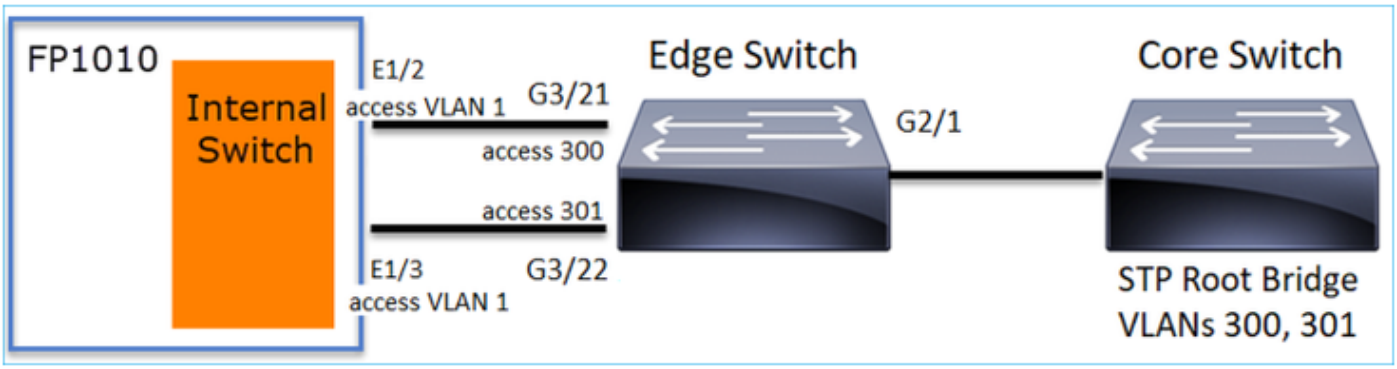
Considere este cenário:



No switch de borda, a porta raiz para ambas as VLANs é G2/1:

```
Edge-Switch# show spanning-tree root | i 300|301
VLAN0300         33068 0017.dfd6.ec00         4    2   20  15  Gi2/1
VLAN0301  33069 0017.dfd6.ec00         4    2   20  15  Gi2/1
```

Conecte um FP1010 ao switch de borda e configure ambas as portas na mesma VLAN (HW Switching):



O problema

- Devido ao **vazamento de VLAN** BPDUs superiores para a VLAN 301 recebida em 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
```

aviso: Se você conectar um switch L2 ao FP1010, poderá afetar o domínio STP

Isso também está documentado no guia de configuração do 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.

APIs REST FXOS

APIs REST do FMC

Estas são as APIs REST para este suporte de recursos:

- Interface física L2 [PUT/GET suportado]

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

- Interface VLAN [POST/PUT/GET/DELETE suportado]

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

Solução de problemas/diagnóstico

Visão geral do diagnóstico

- Os arquivos de log são capturados em uma solução de problemas FTD/NGIPS ou na saída show tech. Estes são os itens que precisam ser procurados para obter mais detalhes em caso de solução de problemas:
- /opt/cisco/platform/logs/portmgr.out
- /var/sysmgr/sam_logs/svc_sam_dme.log
- /var/sysmgr/sam_logs/svc_sam_portAG.log
- /var/sysmgr/sam_logs/svc_sam_appAG.log
- Asa running-config
- /mnt/disk0/log/asa-appagent.log

Coletar dados do FXOS (dispositivo) - CLI

No caso do DTF (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)#
```

No caso do DTF (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)#
```

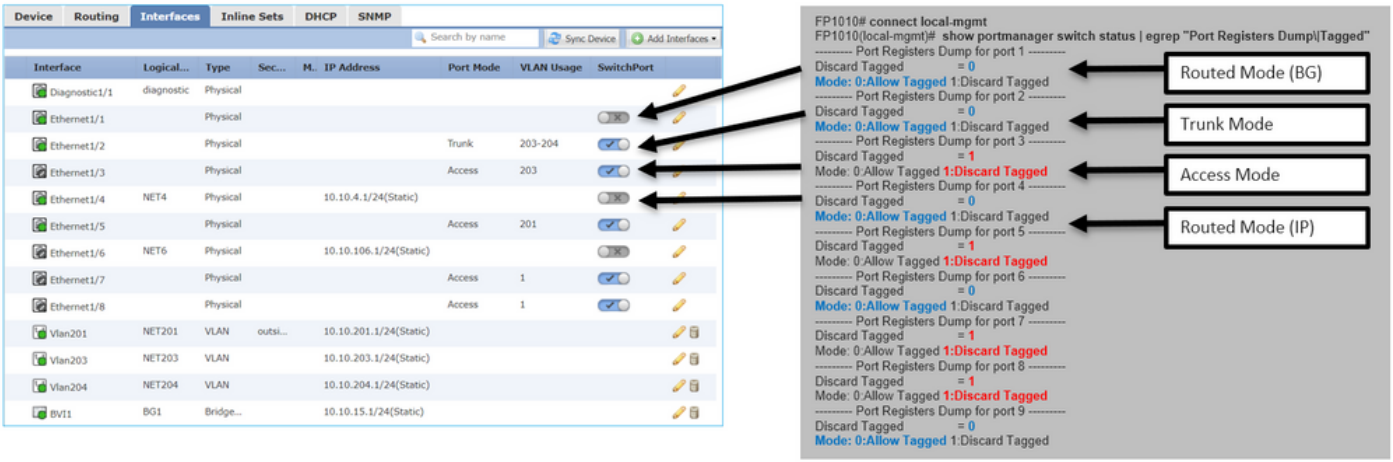
Back-end FP1010

Os registros de porta definem todas as funções internas do switch e da porta.

Nesta captura de tela, é mostrada a seção 'Controle de porta' dos registros de porta e especificamente o registro que determina se o tráfego marcado recebido na interface deve ser descartado (1) ou permitido (0). Esta é a seção de registro completo para uma 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
```

Nesta captura de tela, você pode ver os vários valores de registro Discard Tagged para os vários modos de porta:

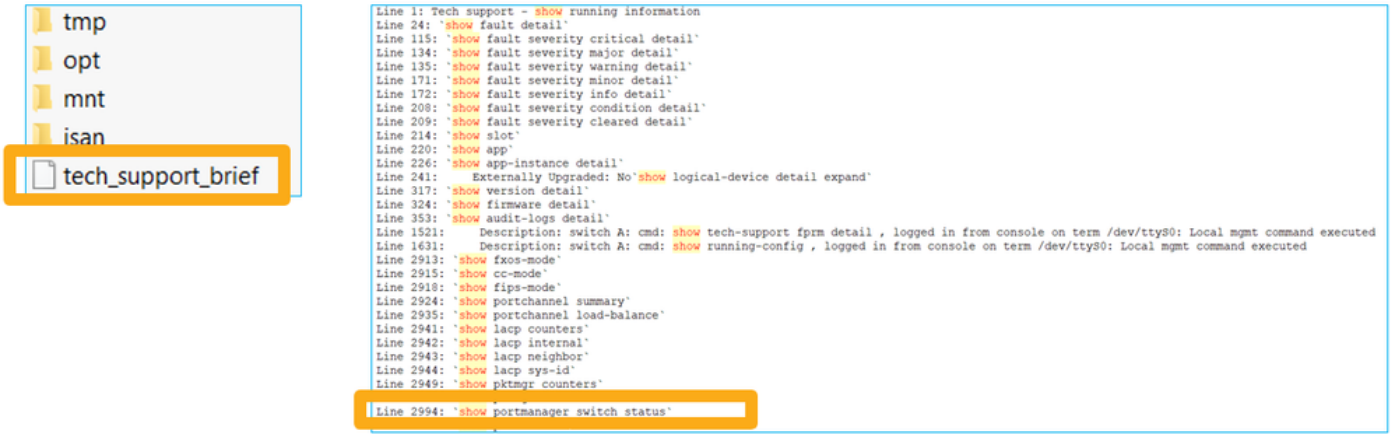


Coletar o show tech do FPRM no FP1010

Para gerar um pacote FPRM e carregá-lo em um servidor FTP:

```
FP1010(local-mgmt)# show tech-support fprm detail
FP1010(local-mgmt)# copy workspace:///techsupport/20190913063603_FP1010-2_FPRM.tar.gz
ftp://ftp@10.229.20.96
```

O pacote FPRM contém um arquivo chamado tech_support_brief. O arquivo tech_support_brief contém uma série de comandos show. Um deles é o **show portmanager switch status**:



Detalhes de limitações, problemas comuns e soluções alternativas

Limitações da implementação da versão 6.5

- Os protocolos de roteamento dinâmico não são suportados para interfaces SVI.
- Multi-contexto não suportado em 1010.
- Intervalo de ID da VLAN SVI limitado a 1-4070.
- O canal de porta para L2 não é suportado.
- A porta L2 como um link de failover não é suportada.

Limites relacionados aos recursos do switch

Recurso	Descrição	Limite
Número de interfaces VLAN	Número total de interfaces VLAN que podem ser criadas	60
VLAN de modo de tronco	Número máximo de VLANs permitidas em uma porta no modo de tronco	20
VLAN nativo	Mapeia todos os pacotes não marcados alcançando uma porta para a VLAN nativa configurada na porta	1
Interfaces nomeadas	Inclui todas as interfaces nomeadas (interface VLAN, subinterface, canal de porta, interface física etc)	60

Outras limitações

- As subinterfaces e a interface VLAN não podem usar a mesma VLAN.
- Todas as interfaces que participam do BVI devem pertencer à mesma classe de interface.
- Uma BVI pode ser criada com uma combinação de portas de modo L3 e subinterfaces de porta de modo L3.
- Uma BVI pode ser criada com uma combinação de VLANs de interface.
- Não é possível criar um BVI misturando portas de modo L3 e VLANs de interface.

Informações Relacionadas

- Dispositivo de segurança Cisco Firepower 1010
- Guias de configuração