FPR1010의 L2 스위치, 아키텍처, 검증 및 문제 해결

목차

소개

이 문서에서는 FP1010 디바이스의 L2 스위치에 대해 설명합니다.특히, 구현 과정에서 주로 SSP(Security Services Platform)/FXOS(Firepower eXtensive Operation System)를 다룹니다.6.5 릴리스에서는 Firepower 1010(데스크탑 모델)이 내장 L2 하드웨어 스위치에서 스위칭 기능을 활성화했습니다.이를 통해 추가 하드웨어 스위치를 피할 수 있으며 비용이 절감됩니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

- FP1010은 ASA5505 및 ASA5506-X 플랫폼을 대체하는 데스크탑 모델 SOHO(Small-Office Home-Office)입니다.
- FMC(Firepower Management Center), FDM(Firepower Device Manager) 또는 CDO(Cloud Defense Orchestrator)에서 관리하는 FTD 이미지(6.4 이상)에 대한 소프트웨어 지원
- CSM, ASDM 또는 CLI에서 관리하는 ASA 이미지(9.13+)에 대한 소프트웨어 지원
- 운영 체제(OS), ASA 또는 FTD는 FXOS 번들(FP21xx와 유사)입니다.
- 10/100/1000Mbps 데이터 포트 8개
- 포트 E1/7, E1/8은 PoE+를 지원합니다.
- 하드웨어 스위치는 포트 간 회선 속도 통신을 허용합니다(예:로컬 서버에 카메라 피드).

Firepower 6.5 추가

- SVI(Switched Virtual Interface)라는 새로운 유형의 인터페이스 소개
- 혼합 모드:인터페이스는 스위치드(L2) 또는 비스위치드(L3) 모드에서 구성할 수 있습니다.
- L3 모드 인터페이스는 모든 패킷을 보안 애플리케이션으로 전달합니다.
- L2 모드 포트는 두 포트가 동일한 VLAN에 속할 경우 하드웨어에서 전환할 수 있으며, 이는 처리량과 레이턴시를 개선합니다.라우팅하거나 브리지해야 하는 패킷은 보안 애플리케이션에 연결됩니다(예:(인터넷에서 새 펌웨어를 다운로드하는 카메라) 및 구성에 따라 보안 검사를 받습니다.
- L2 물리적 인터페이스는 하나 이상의 SVI 인터페이스와 연결할 수 있습니다.
- L2 모드 인터페이스는 액세스 또는 트렁크 모드일 수 있습니다.
- 액세스 모드 L2 인터페이스는 태그 없는 트래픽만 허용합니다.
- 트렁크 모드 L2 인터페이스는 태그 처리된 트래픽을 허용합니다.
- 트렁크 모드 L2 인터페이스에 대한 네이티브 VLAN 지원.
- ASA CLI, ASDM, CSM, FDM, FMC는 새로운 기능을 지원하도록 향상되었습니다.

FMC 추가

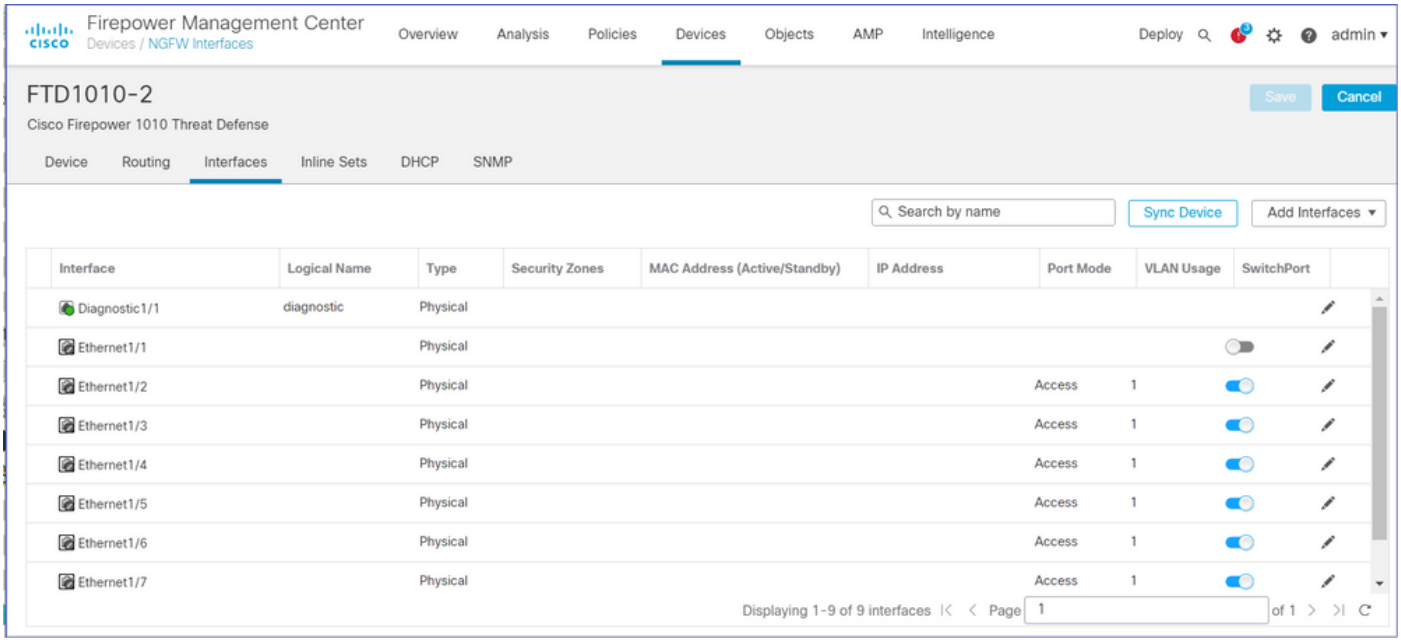
- 물리적 인터페이스가 L3 또는 L2 인터페이스인지 식별하는 데 사용되는 물리적 인터페이스에

switchport라는 새로운 인터페이스 모드가 도입되었습니다.

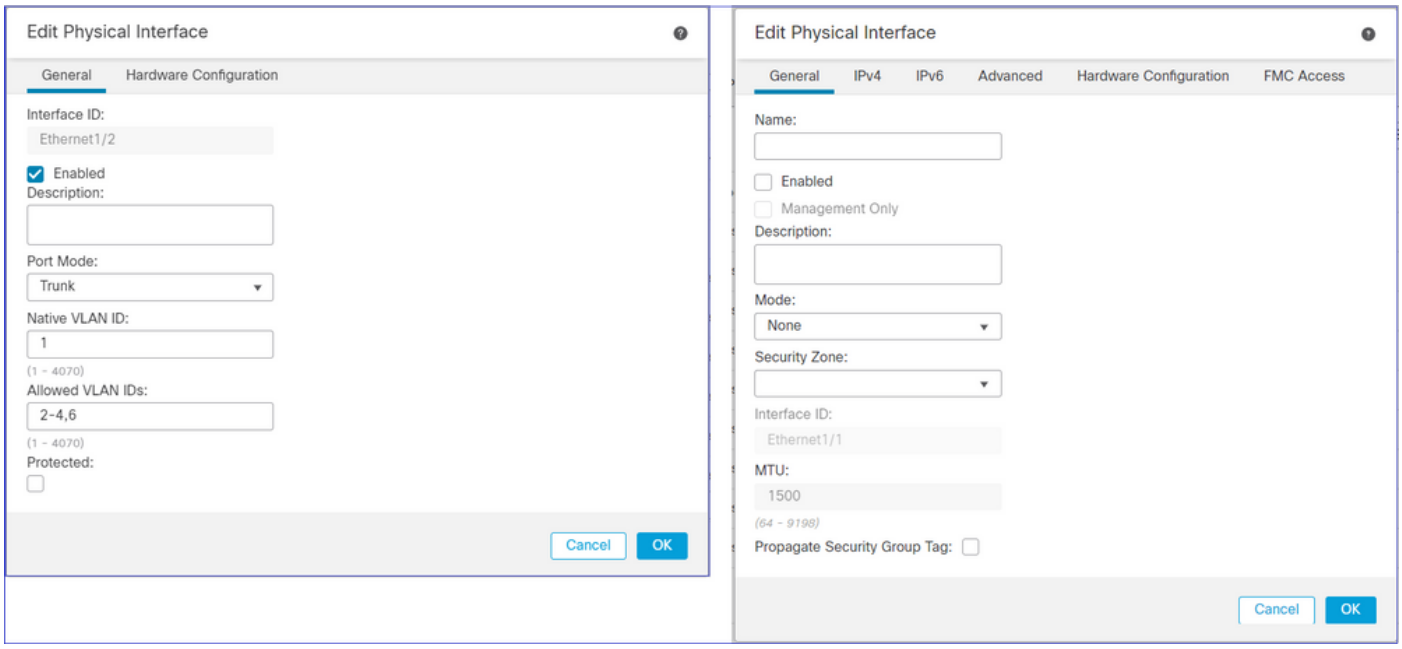
- L2 물리적 인터페이스는 액세스 또는 트렁크 모드에 따라 하나 이상의 VLAN 인터페이스와 연결할 수 있습니다.
- Firepower 1010은 마지막 2개의 데이터 인터페이스(예: Ethernet1/7 및 Ethernet1/8)에서 PoE(Power Over Ethernet) 컨피그레이션을 지원합니다.
- 스위치드 컨피그레이션과 비스위치드 간 인터페이스 변경은 PoE 및 하드웨어 컨피그레이션을 제외한 모든 컨피그레이션을 지웁니다.

작동 방식

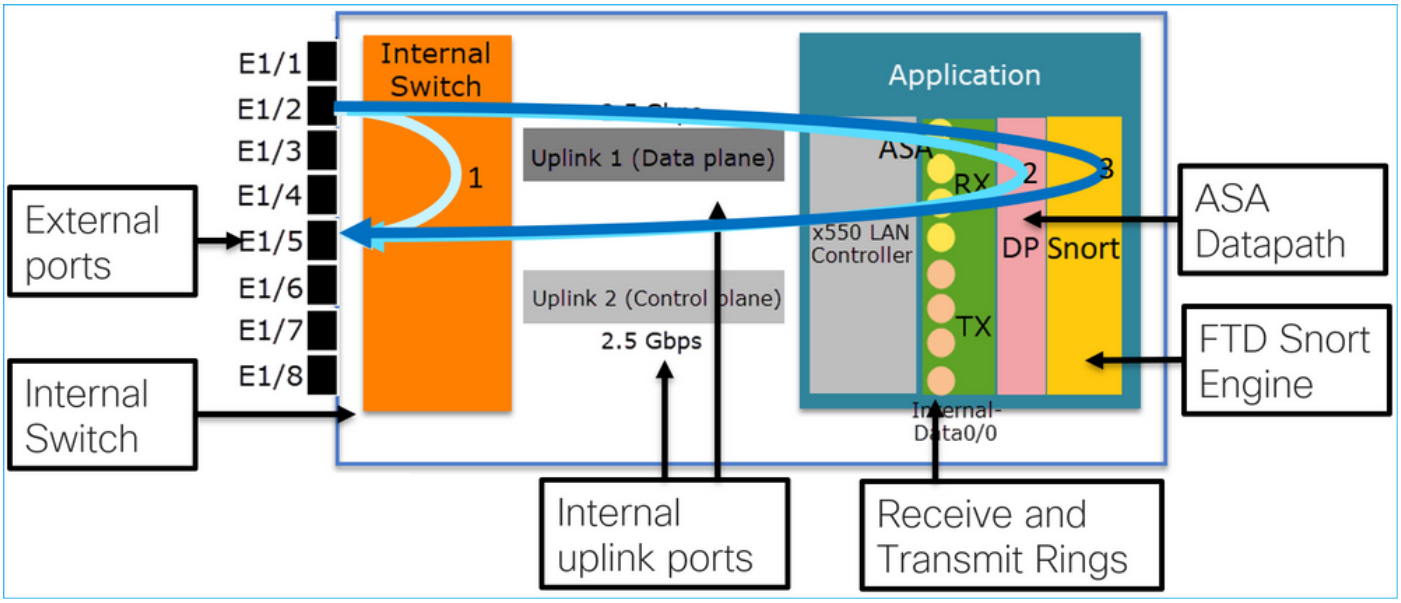
이 기능은 FMC(Device **Management**(디바이스 **관리) > Interface Page(인터페이스 페이지)**에서 기존 인터페이스 지원**을 개선한** 것입니다.



물리적 인터페이스 보기(L2 및 L3)



FP1010 아키텍처



- 8개의 외부 데이터 포트.
- 1 내부 스위치
- 3 업링크 포트(그림에 표시된 포트 2개), 데이터 플레인, 컨트롤 플레인, 구성 포트 1개
- x550 LAN 컨트롤러(애플리케이션과 업링크 간의 인터페이스)
- 4 수신(RX) 및 4 전송(TX) 링
- 데이터 경로 프로세스(ASA 및 FTD).
- Snort 프로세스(FTD에서)

패킷 처리

두 가지 주요 요인은 패킷 처리에 영향을 미칠 수 있습니다.

1. 인터페이스/포트 모드

2. 적용된 정책

패킷은 다음과 같은 세 가지 방법으로 FP1010을 통과할 수 있습니다.

1. 내부 스위치에서만 처리

2. 애플리케이션(ASA/FTD)까지 전달되어 데이터 경로 프로세스에서만 처리

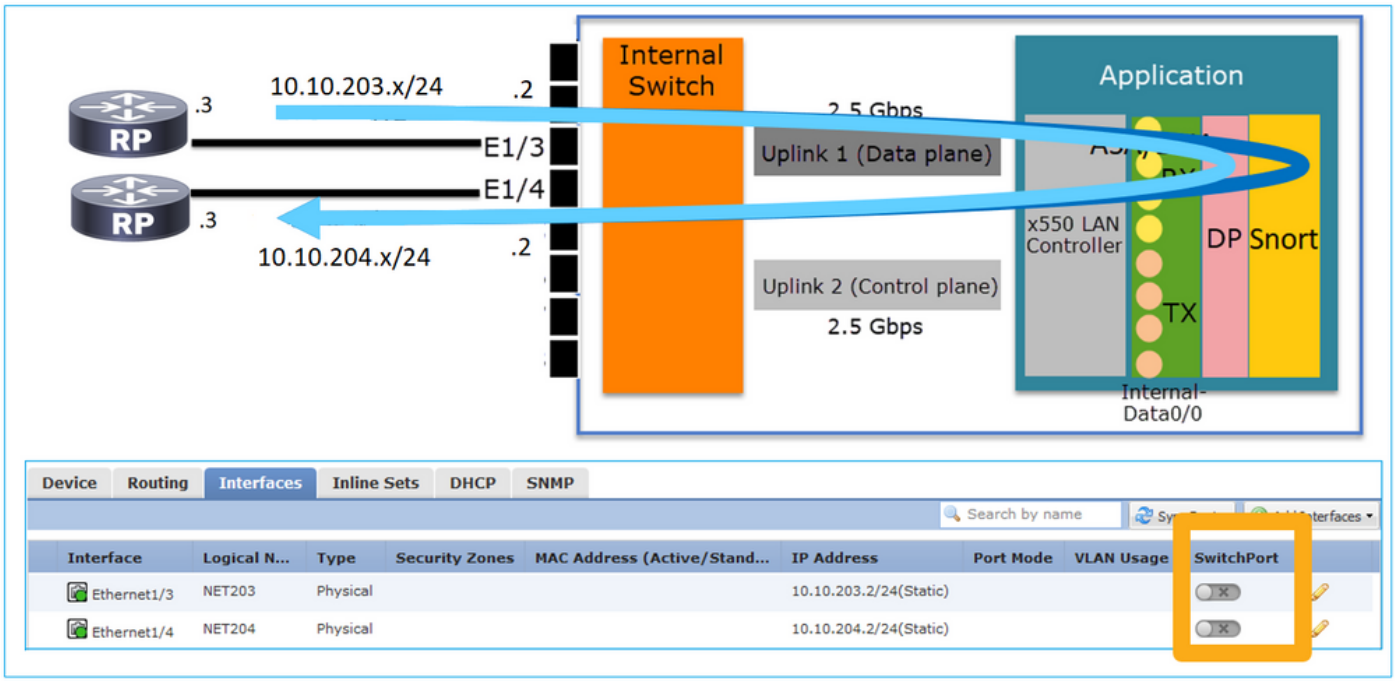
3. 애플리케이션(FTD)까지 포워딩되어 데이터 경로 및 Snort 엔진에서 처리

FP1010 포트 모드

UI 예제는 FMC이고 CLI 예제는 FTD입니다.대부분의 개념은 ASA에도 완전히 적용됩니다.

FP1010 케이스 1. 라우팅 포트(IP 라우팅)

구성 및 운영



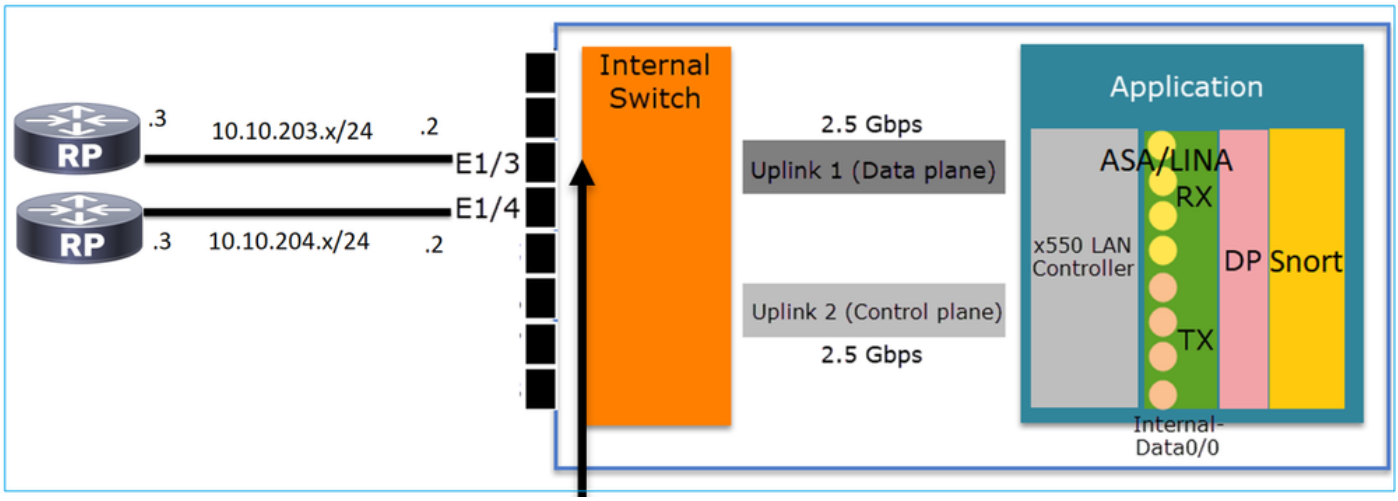
주요 내용

- 설계 관점에서 2개의 포트는 2개의 서로 다른 L2 서브넷에 속합니다.
- 포트가 라우팅 모드에서 구성되면 패킷이 애플리케이션(ASA 또는 FTD)에 의해 처리됩니다.
- FTD의 경우 규칙 작업(예: ALLOW)을 기반으로 Snort 엔진에서도 패킷을 검사할 수 있습니다.

FTD 인터페이스 컨피그레이션

```
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 라우티드 포트 확인



FXOS CLI에서 물리적 인터페이스 카운터를 확인할 수 있습니다.다음 예에서는 E1/3 포트의 인그레스 유니캐스트 및 이그레스 유니캐스트 카운터를 보여줍니다.

```
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 데이터 경로 캡처를 적용하고 패킷을 추적할 수 있습니다.

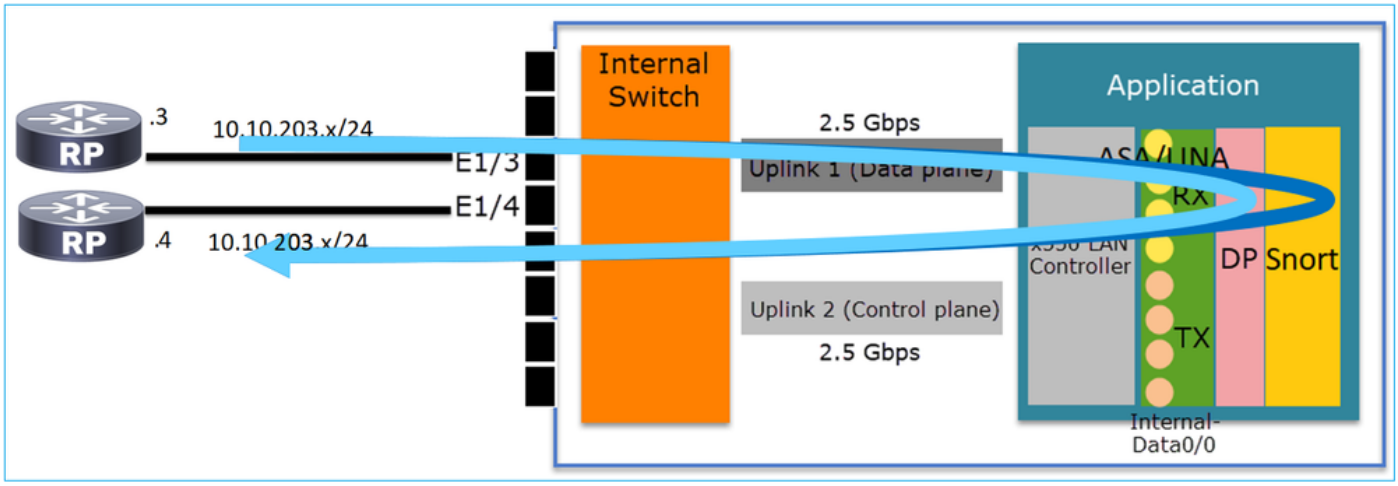
```
FP1010# show capture
capture CAP203 type raw-data trace interface NET203 [Capturing - 185654 bytes]
```

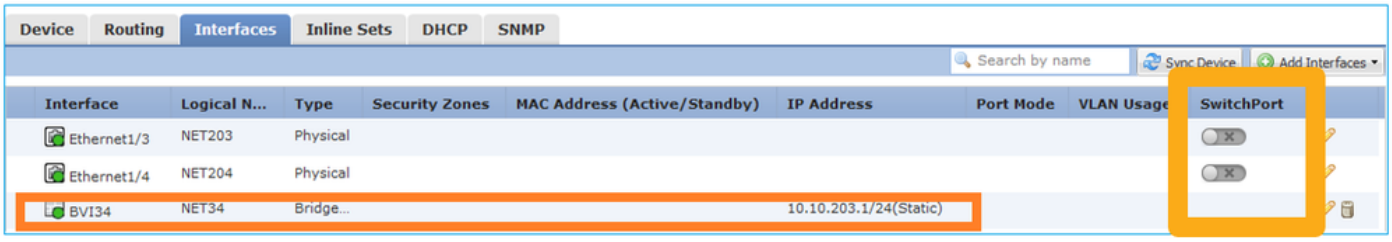
캡처 조각입니다.예상대로 패킷은 ROUTE LOOKUP에 따라 전달됩니다.

```
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 사례 2. 브리지 그룹 모드(브리징)

구성 및 운영





주요 내용

- 설계 관점에서 2개의 포트는 동일한 L3 서브넷(투명 방화벽과 유사)에 연결되지만 다른

VLAN에 연결됩니다.

- 포트가 브리징 모드에서 구성되면 패킷은 애플리케이션(ASA 또는 FTD)에서 처리됩니다.
- FTD의 경우 규칙 작업(예: ALLOW)을 기반으로 Snort 엔진에서도 패킷을 검사할 수 있습니다.

FTD 인터페이스 컨피그레이션

```
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 브리지-그룹 포트 확인

이 명령은 BVI 34의 인터페이스 멤버를 보여줍니다.

```
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
```

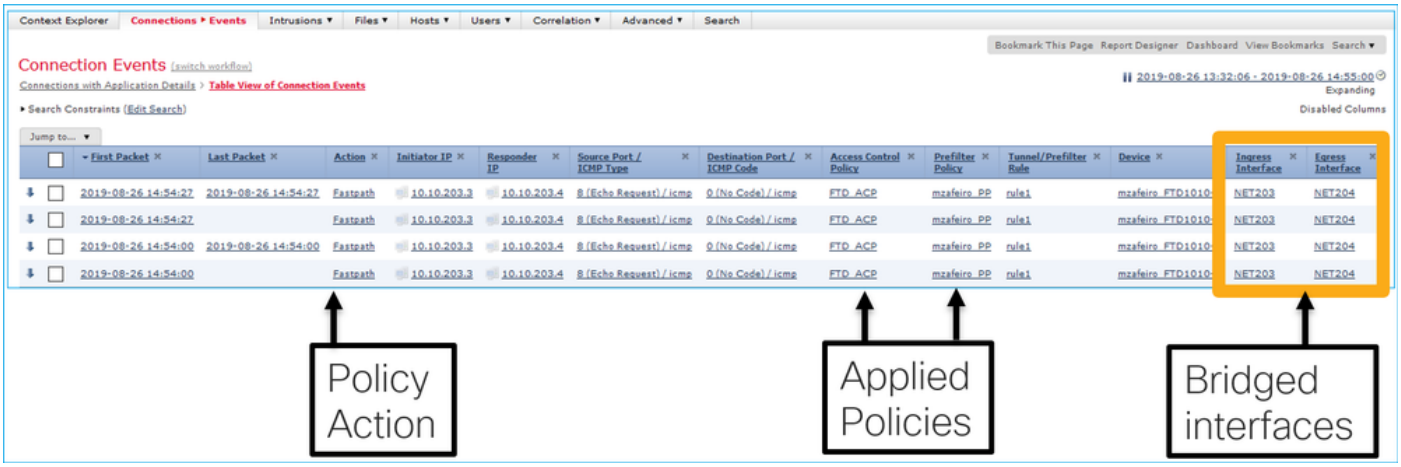
이 명령은 ASA/FTD 데이터 경로 CAM(Content Addressable Memory) 테이블을 표시합니다.

```
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
```

패킷 추적 코드 조각은 패킷이 대상 MAC L2 조회를 기반으로 포워딩됨을 보여줍니다.

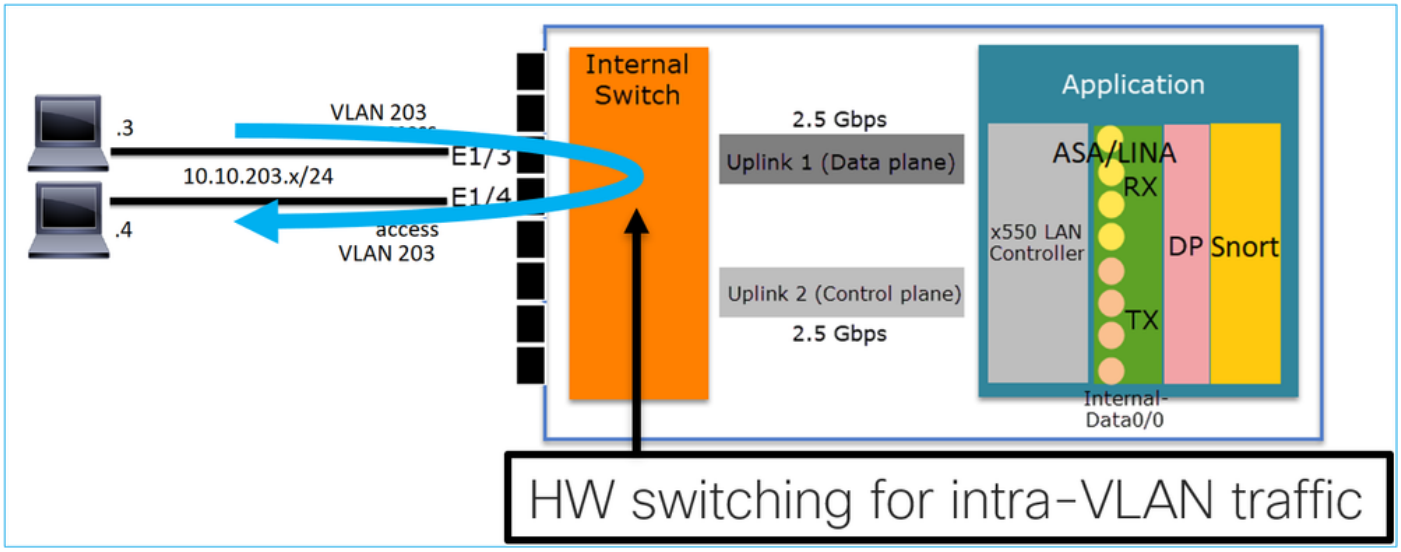
```
FP1010# show cap CAP203 packet-number 1 trace

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
```

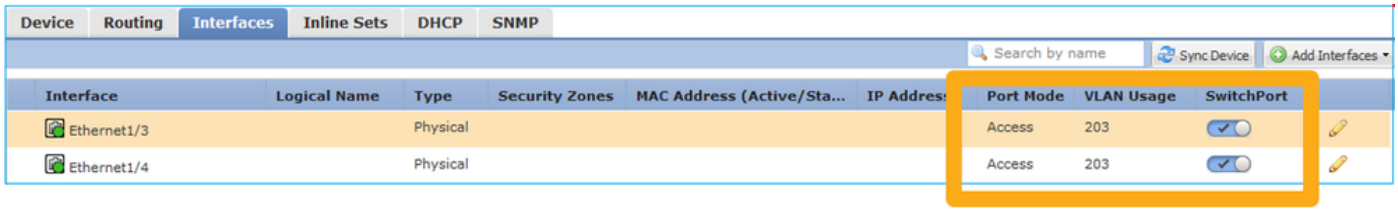
FTD의 경우 FMC Connection Events는 흐름 검사 및 트랜짓 브리지 그룹 인터페이스에 대한 정보도 제공할 수 있습니다.



액세스 모드의 FP1010 사례 3. 스위치 포트(HW 스위칭)

구성 및 운영





주요 내용

- HW 스위칭은 FTD **6.5+** 및 ASA **9.13+** 기능입니다.
- 설계 관점에서 2개의 포트는 동일한 L3 서브넷과 동일한 VLAN에 연결됩니다.
- 이 시나리오의 포트는 액세스 모드에서 작동 중입니다(태그 없는 트래픽만 해당).
- SwitchPort 모드로 구성된 방화벽 포트에 논리적 이름(nameif)이 구성되지 않았습니다.
- 포트가 스위칭 모드에서 구성되고 동일한 VLAN(intra-VLAN 트래픽)에 속하는 경우 패킷은 FP1010 내부 스위치에서만 처리됩니다.

FTD 인터페이스 컨피그레이션

CLI 관점에서 컨피그레이션은 L2 스위치와 매우 유사합니다.

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

```
switchport access vlan 203
```

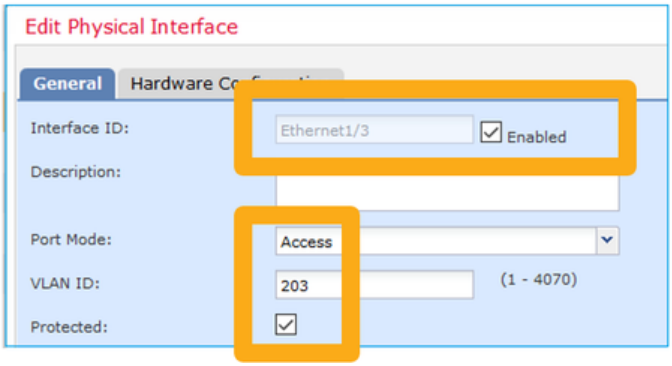
Intra-VLAN 트래픽 필터링

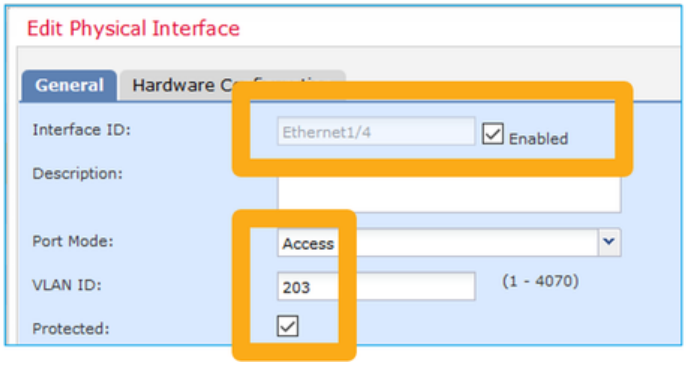
당면 과제:**ACL은 intra-VLAN 트래픽을 필터링할 수 없습니다!**

해결 방법:**보호된** 포트

그 원리는 매우 간단하다.보호됨으로 구성된 포트 2개는 서로 통신할 수 없습니다.

보호된 포트의 경우 FMC UI:





FTD 인터페이스 컨피그레이션

보호되는 명령 **switchport는** 인터페이스 아래에 구성됩니다.

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

FP1010 스위치 포트 확인

이 예에서는 특정 크기(1100바이트)로 전송되는 유니캐스트 패킷(ICMP)이 1000개 있습니다.

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

트랜짓 인터페이스의 인그레스 및 이그레스 유니캐스트 카운터를 확인하려면 다음 명령을 사용합니다.

```
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
```

이 명령은 내부 스위치 VLAN 상태를 표시합니다.

```
FP1010# show switch vlan
VLAN Name            Status    Ports
---- --------------- --------- ---------------------
1     -              down
203 - up Ethernet1/3, Ethernet1/4
```

하나 이상의 포트가 VLAN에 할당된 경우 VLAN의 상태가 UP입니다.

관리 목적으로 포트가 다운되었거나 연결된 스위치 포트가 다운/케이블 연결이 끊어진 상태에서 VLAN에 할당된 유일한 포트인 경우 VLAN 상태도 다운됩니다.

```
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
```

이 명령은 내부 스위치의 CAM 테이블을 보여줍니다.

```
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
```

내부 스위치 CAM 테이블의 기본 에이징 시간은 5분 30초입니다.

FP1010에는 2개의 CAM 테이블이 있습니다.

1. **내부 스위치 CAM 테이블**:HW 스위칭의 경우 사용
2. **ASA/FTD 데이터 경로 CAM 테이블**:브리징의 경우 사용

FP1010을 통과하는 각 패킷/프레임은 포트 모드를 기반으로 단일 CAM 테이블(내부 스위치 또는 FTD 데이터 경로)에 의해 처리됩니다.

> **주의:**SwitchPort 모드에서 사용되는 **show switch mac-address-table** 내부 스위치 CAM 테이블과 bridged 모드에서 사용되는 **show mac-address-table** FTD 데이터 경로 CAM 테이블을 혼동하지 마십시오.

HW 스위칭:알아야 할 추가 사항

ASA/FTD 데이터 경로 로그는 HW 스위치 흐름에 대한 정보를 표시하지 않습니다.

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

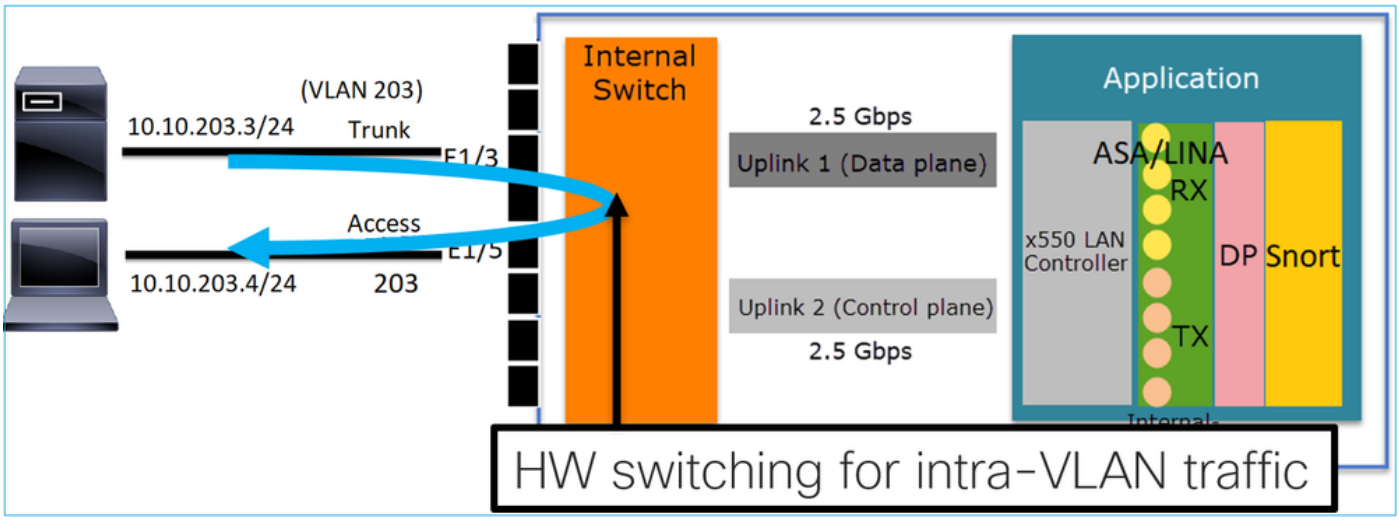
ASA/FTD 데이터 경로 연결 테이블에는 HW 스위치 플로우가 표시되지 않습니다.

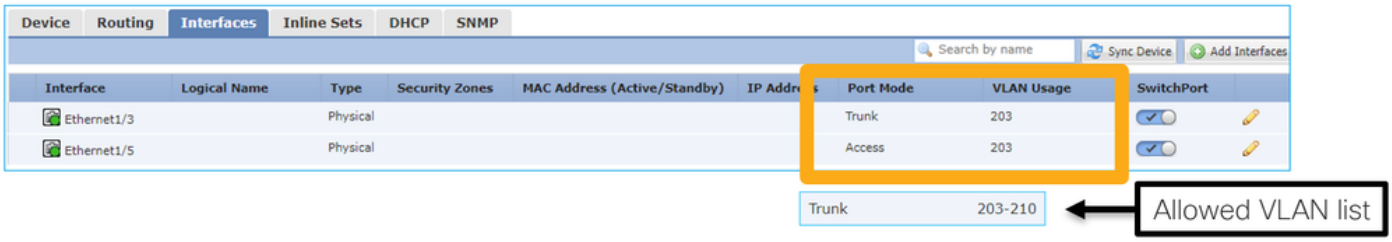
```
FP1010# show conn
0 in use, 3 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect
```

또한 FMC 연결 이벤트에는 HW 스위치 플로우가 표시되지 않습니다.

FP1010 케이스 4. 스위치 포트(트렁킹)

구성 및 운영





주요 내용

- HW 스위칭은 FTD **6.5+** 및 ASA **9.13+** 기능입니다.
- 설계 관점에서 2개의 포트는 동일한 L3 서브넷과 동일한 VLAN에 연결됩니다.
- 트렁크 포트는 태그가 지정된 프레임과 태그가 지정되지 않은(네이티브 VLAN의 경우)를 허용합니다.
- 포트가 스위칭 모드에서 구성되고 동일한 VLAN(intra-VLAN 트래픽)에 속하는 경우 패킷은 내부 스위치에서만 처리됩니다.

FTD 인터페이스 컨피그레이션

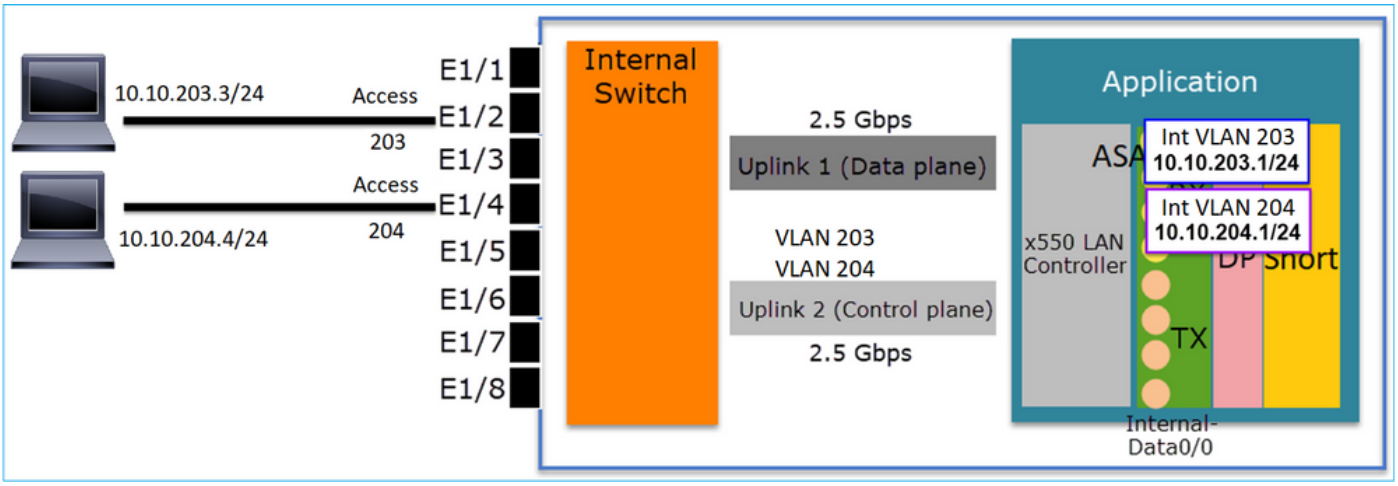
구성은 레이어 2 스위치 포트와 유사합니다.

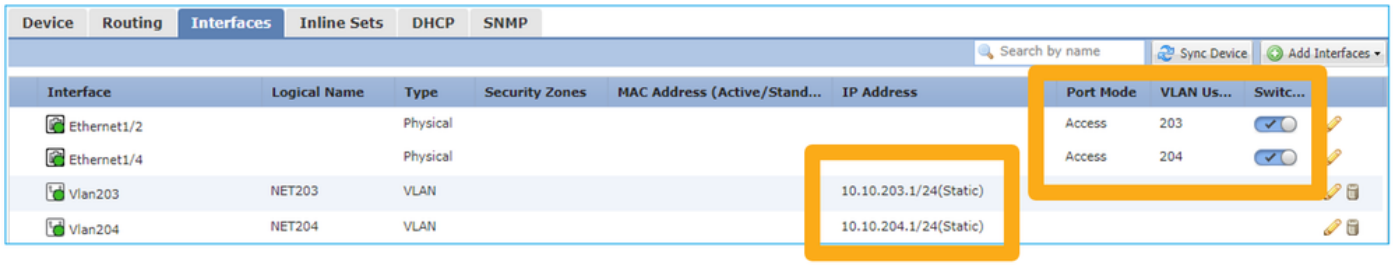
```
interface Ethernet1/3 switchport switchport trunk allowed vlan 203 switchport trunk native vlan
```

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

FP1010 케이스 5. 스위치 포트(VLAN 간)

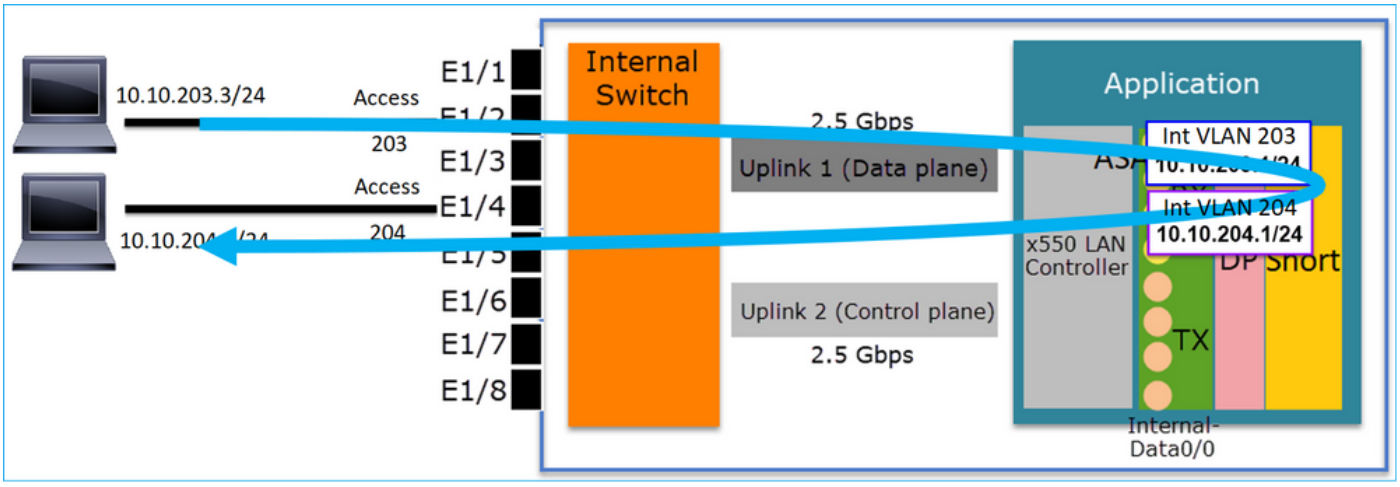
구성 및 운영





주요 내용

- 설계 관점에서 2개의 포트는 2개의 서로 다른 L3 서브넷 및 2개의 서로 다른 VLAN에 연결됩니다.
- VLAN 간 트래픽은 VLAN 인터페이스(SVI와 유사)를 거칩니다.
- 트래픽 흐름 관점에서 VLAN 간 트래픽은 애플리케이션에 도달합니다.



FTD 인터페이스 컨피그레이션

구성은 SVI(Switch Virtual Interface)와 유사합니다.

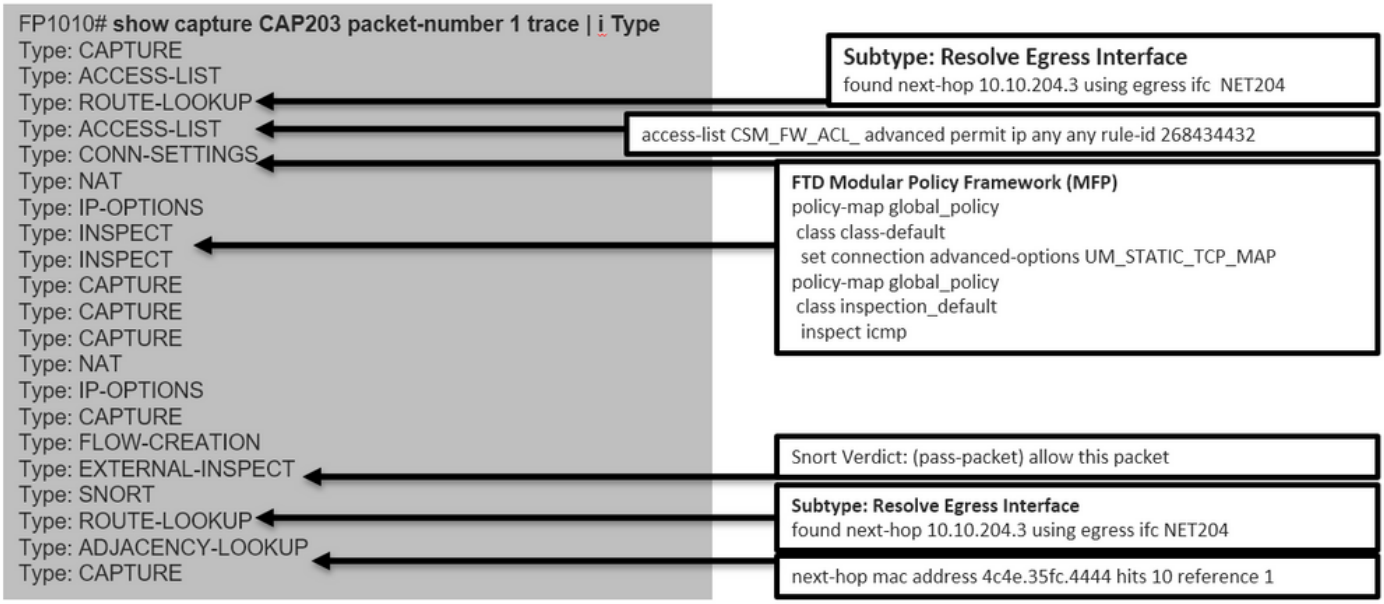
```
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203 nameif NET203 security-level 0 ip address 10.10.203.1 255.255.255.0
interface Vlan204 nameif NET204 security-level 0 ip address 10.10.204.1 255.255.255.0
```

VLAN 간 트래픽에 대한 패킷 처리

다음은 2개의 서로 다른 VLAN을 통과하는 패킷의 추적입니다.

```
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
```

패킷 프로세스의 주요 단계는 다음과 같습니다.



FP1010 케이스 6. VLAN 간 필터

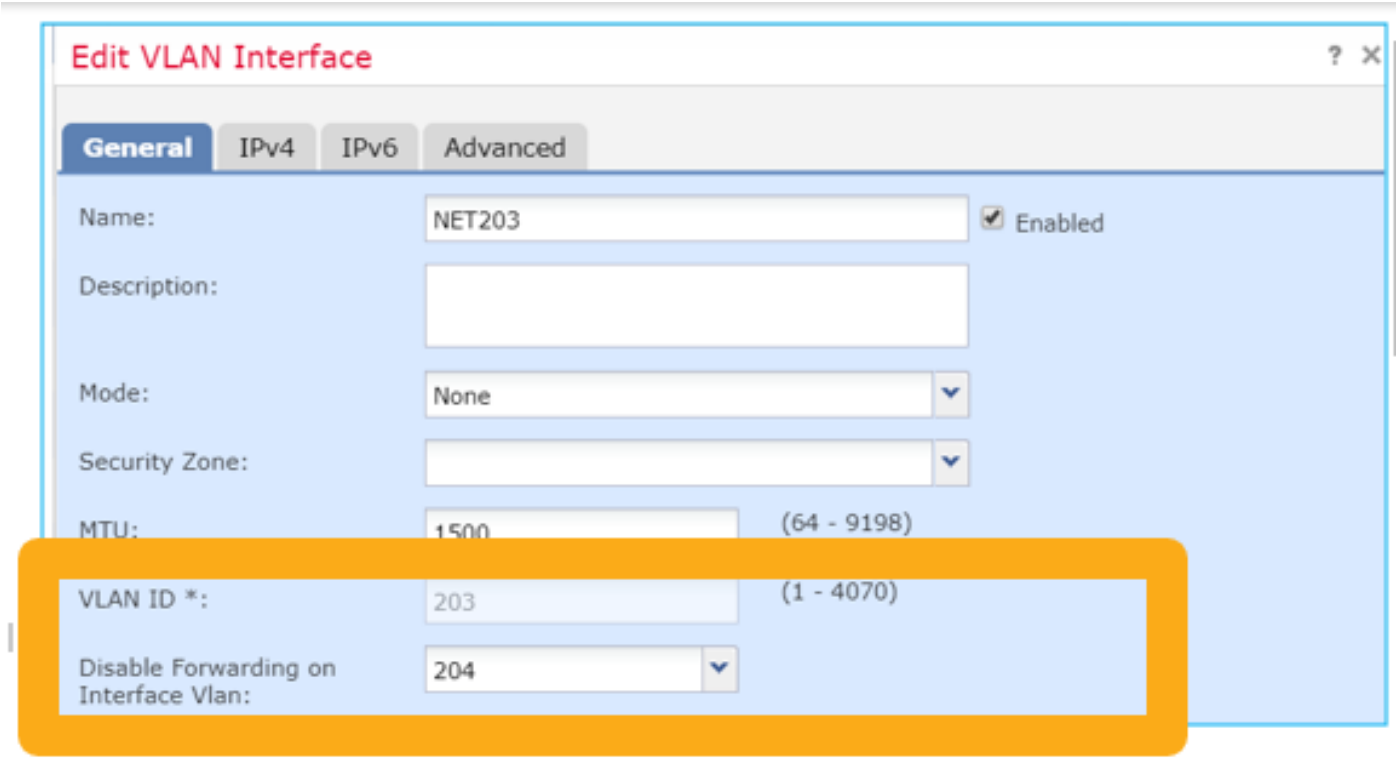
구성 및 운영

VLAN 간 트래픽을 필터링하는 두 가지 기본 옵션이 있습니다.

1. 액세스 제어 정책
2. 'no forward' 명령

'no forward' 명령을 사용하여 VLAN 간 트래픽 필터링

FMC UI 구성:



주요 내용

- no forward drop은 단방향입니다.
- 두 VLAN 인터페이스에 모두 적용할 수 없습니다.
- ACL 확인 전에 no forward check가 수행됩니다.

FTD 인터페이스 컨피그레이션

이 경우 CLI 컨피그레이션은 다음과 같습니다.

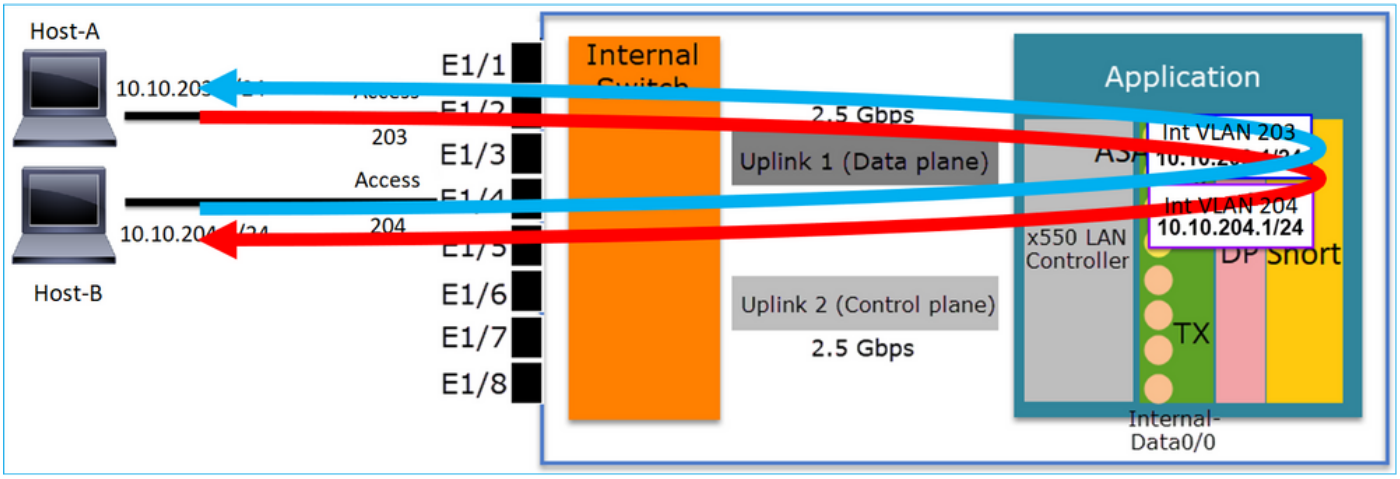
```
interface Vlan203
no forward interface Vlan204
 nameif NET203
 security-level 0
 ip address 10.10.203.1 255.255.255.0
!
interface Vlan204
 nameif NET204
 security-level 0
 ip address 10.10.204.1 255.255.255.0
```

패킷이 no forward 기능에 의해 삭제되는 경우 ASA/FTD 데이터 경로 Syslog 메시지가 생성됩니다.

```
FP1010# show log
Sep 10 2019 07:44:54: %FTD-5-509001: Connection attempt was prevented by "no forward" command:
```

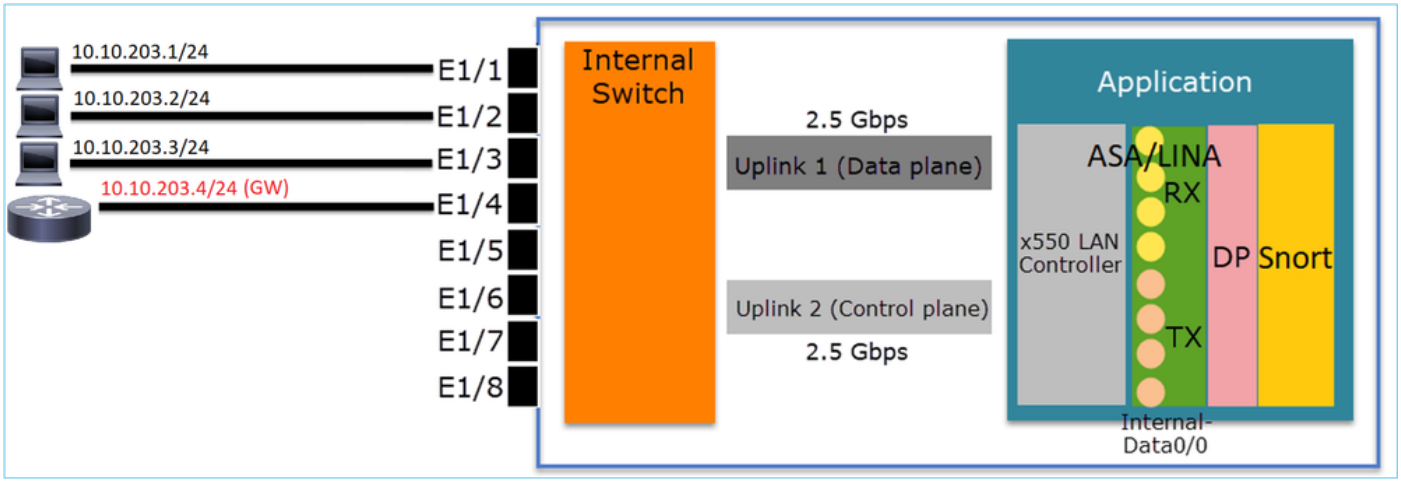
```
icmp src NET203:10.10.203.3 dst NET204:10.10.204.3 (type 8, code 0)
```
ASP(Accelerated Security Path) 드롭다운 보기에서 ACL 삭제로 간주됩니다.

```
FP1010-2# show asp drop
Frame drop:
Flow is denied by configured rule (acl-drop) 1
```
드롭이 단방향이므로 Host-A(VLAN 203)는 Host-B(VLAN 204)에 대한 트래픽을 시작할 수 없지만 그 반대는 허용됩니다.



사례 연구 - FP1010. 브리징 vs HW 스위칭 + 브리징

다음 토폴로지를 고려하십시오.



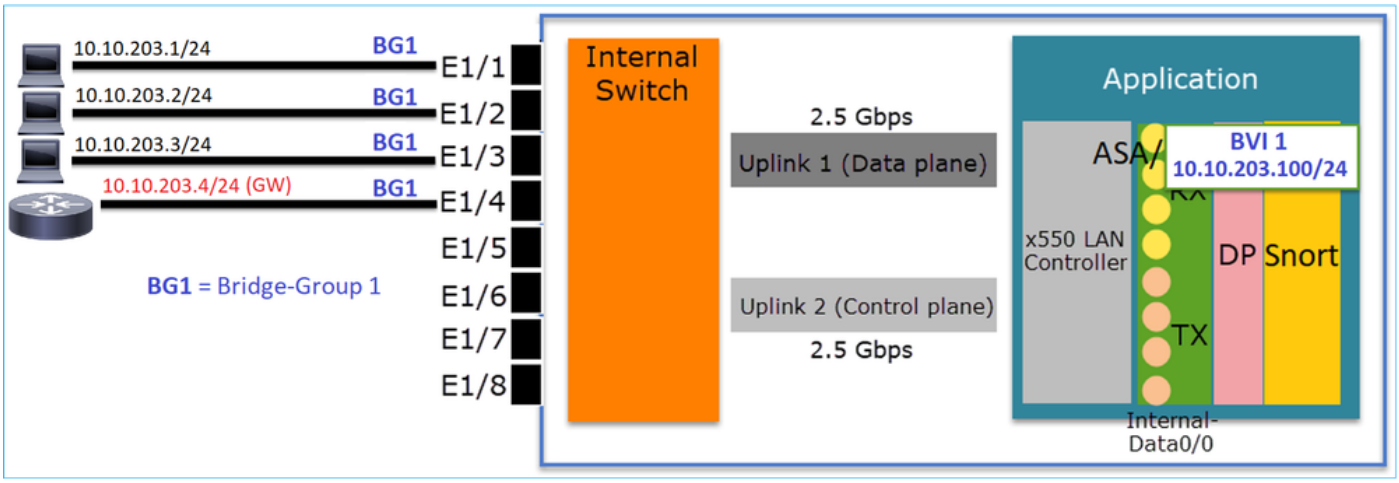
이 토폴로지에서는 다음과 같이 합니다.

- 세 개의 엔드-호스트가 동일한 L3 서브넷(10.10.203.x/24)에 속합니다.
- 라우터(10.10.203.4)은 서브넷에서 GW 역할을 합니다.

이 토폴로지에서는 다음 두 가지 기본 설계 옵션이 있습니다.

1. 브리징
2. HW 스위칭 + 브리징

설계 옵션 1. 브리징

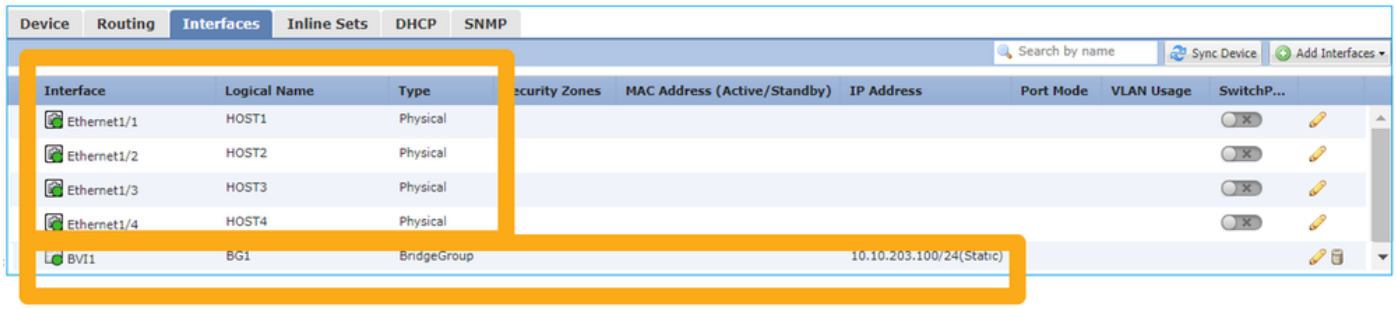


주요 내용

이 설계의 핵심은 다음과 같습니다.

- 연결된 4개의 디바이스와 동일한 서브넷(10.10.203.x/24)에 IP를 사용하여 BVI 1이 생성됩니다 .
- 네 포트 모두 동일한 Bridge-Group(이 경우 그룹 1)에 속합니다.
- 4개 포트 각각에는 구성된 이름이 있습니다.
- 호스트 대 호스트 및 호스트 대 GW 통신은 애플리케이션(예: FTD)을 거칩니다.

FMC UI 관점에서 컨피그레이션은 다음과 같습니다.

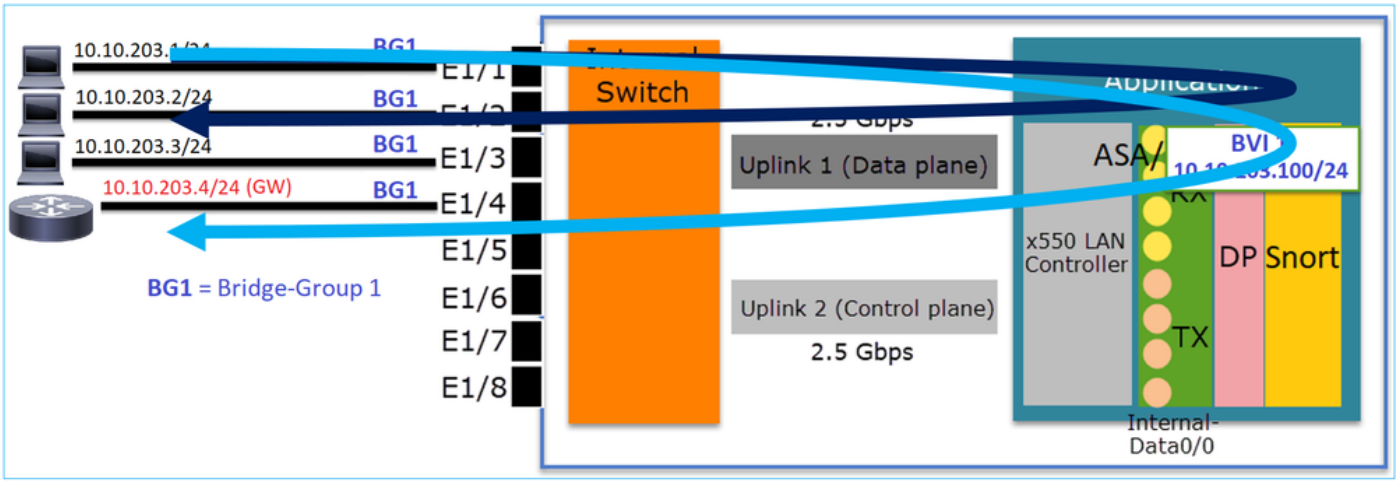


FTD 인터페이스 컨피그레이션

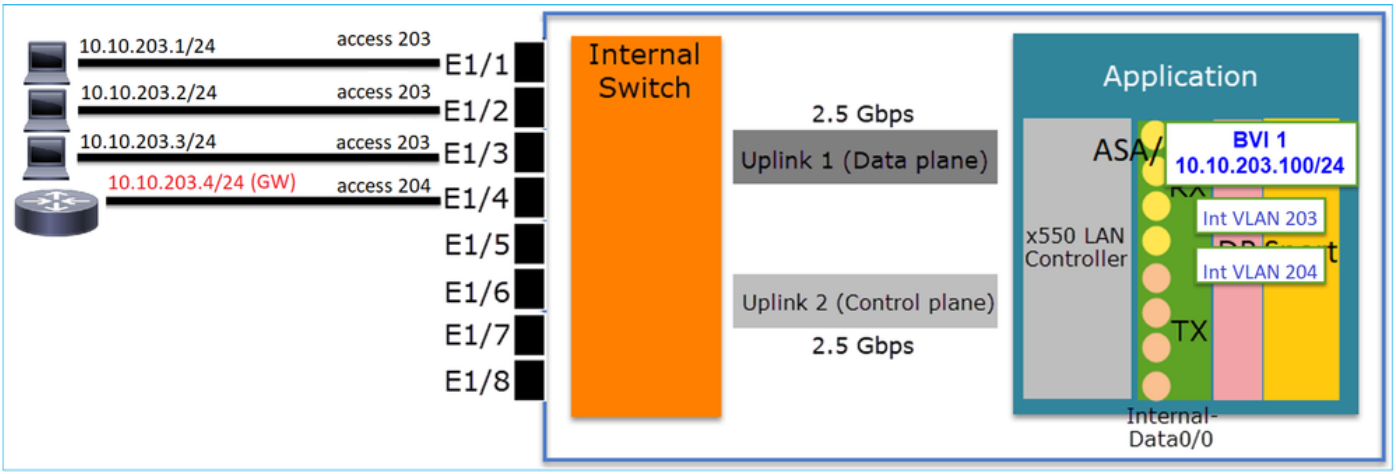
이 경우 컨피그레이션은 다음과 같습니다.

```
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
```

이 시나리오의 트래픽 흐름:



설계 옵션 2. HW 스위칭 + 브리징

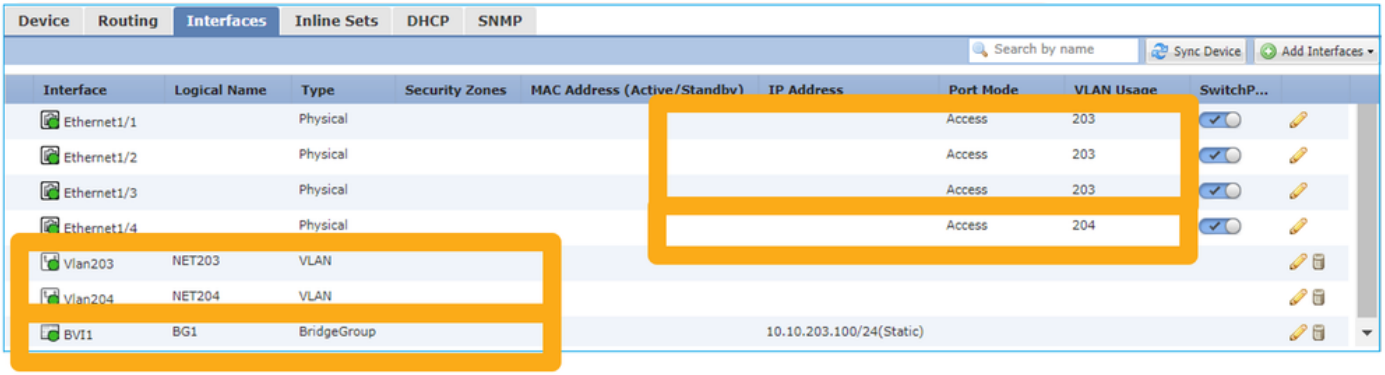


주요 내용

이 설계의 핵심은 다음과 같습니다.

- 연결된 4개의 디바이스와 동일한 서브넷(10.10.203.x/24)에 IP를 사용하여 BVI 1이 생성됩니다 .
- 엔드 호스트에 연결된 포트는 SwitchPort 모드에서 구성되며 동일한 VLAN(203)에 속합니다.
- GW에 연결된 포트는 SwitchPort 모드에서 구성되며 다른 VLAN에 속합니다(204).
- 2개의 VLAN 인터페이스(203, 204)가 있습니다. 2개의 VLAN 인터페이스에는 IP가 할당되지 않았으며 Bridge-Group 1에 속합니다.
- 호스트 간 통신은 내부 스위치만 거칩니다.
- 호스트 대 GW 통신은 애플리케이션(예: FTD)을 거칩니다.

FMC UI 구성:

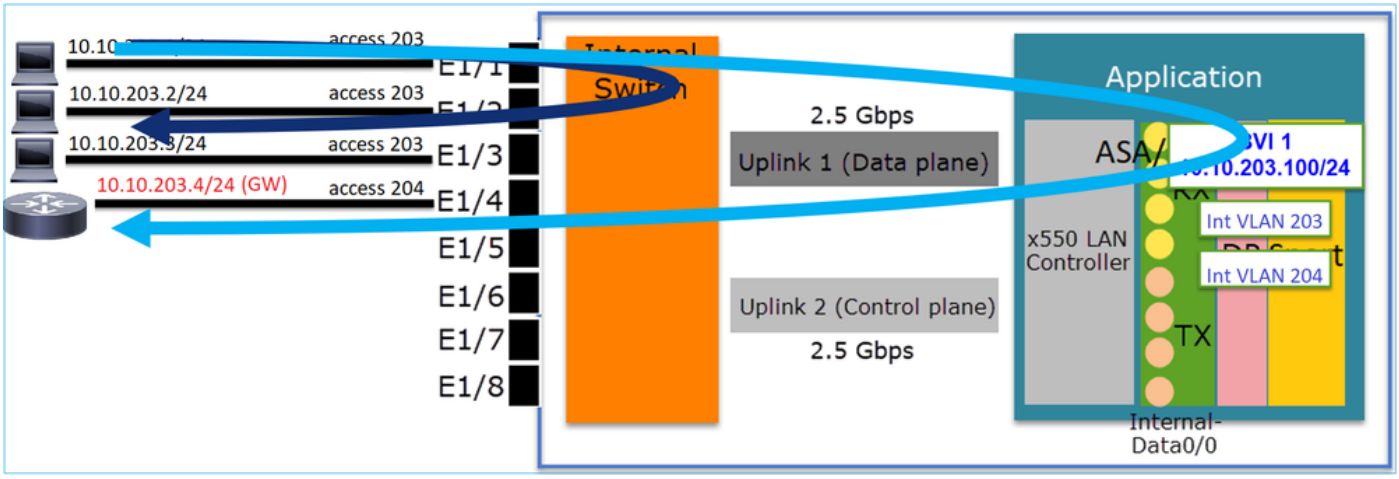


FTD 인터페이스 컨피그레이션

이 경우 컨피그레이션은 다음과 같습니다.

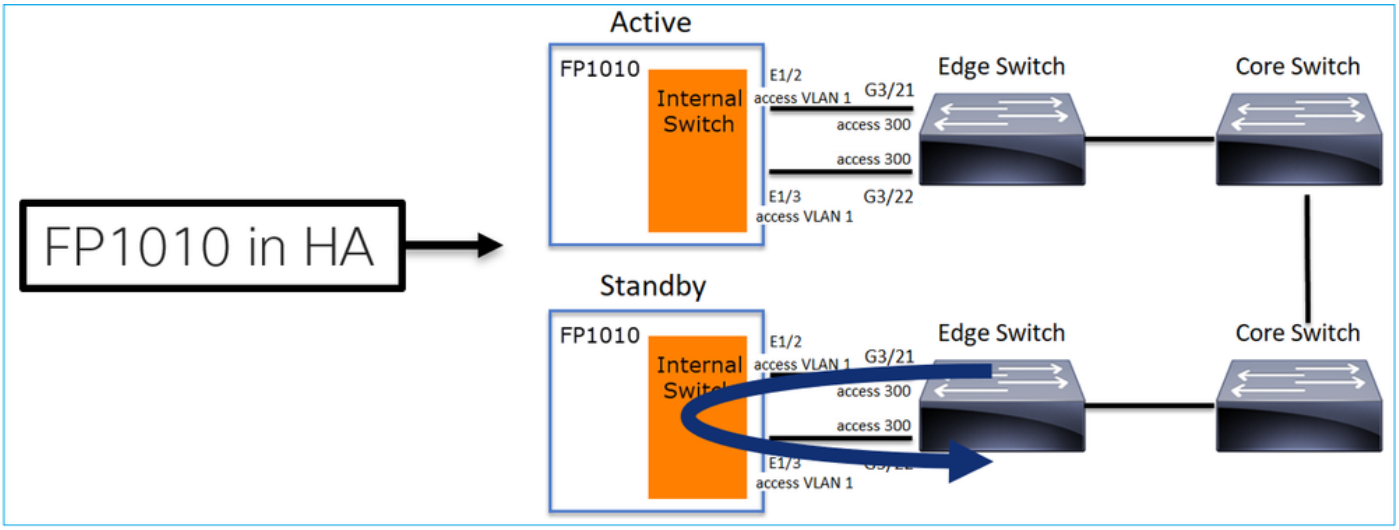
```
interface Ethernet1/1
 switchport switchport access vlan 203
interface Ethernet1/2
 switchport switchport access vlan 203
interface Ethernet1/4
 switchport switchport access vlan 204
!
interface Vlan203
 bridge-group 1 nameif NET203
interface Vlan204
 bridge-group 1 nameif NET204
!
interface BVI1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

호스트 간 통신과 호스트 대 GW 통신 비교:



FP1010 설계 고려 사항

스위칭 및 고가용성(HA)

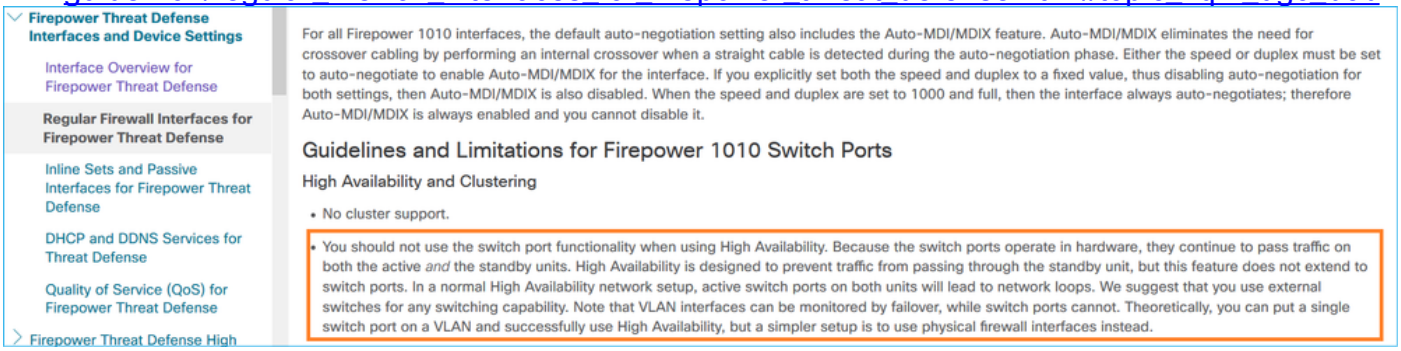


HA 환경에서 HW 스위칭이 구성된 경우 2가지 주요 문제가 있습니다.

1. 스탠바이 유닛의 HW 스위칭은 디바이스를 통해 패킷을 전달합니다.이로 인해 트래픽 루프가 발생할 수 있습니다.
2. 스위치 포트는 HA에서 모니터링되지 않음

설계 요구 사항

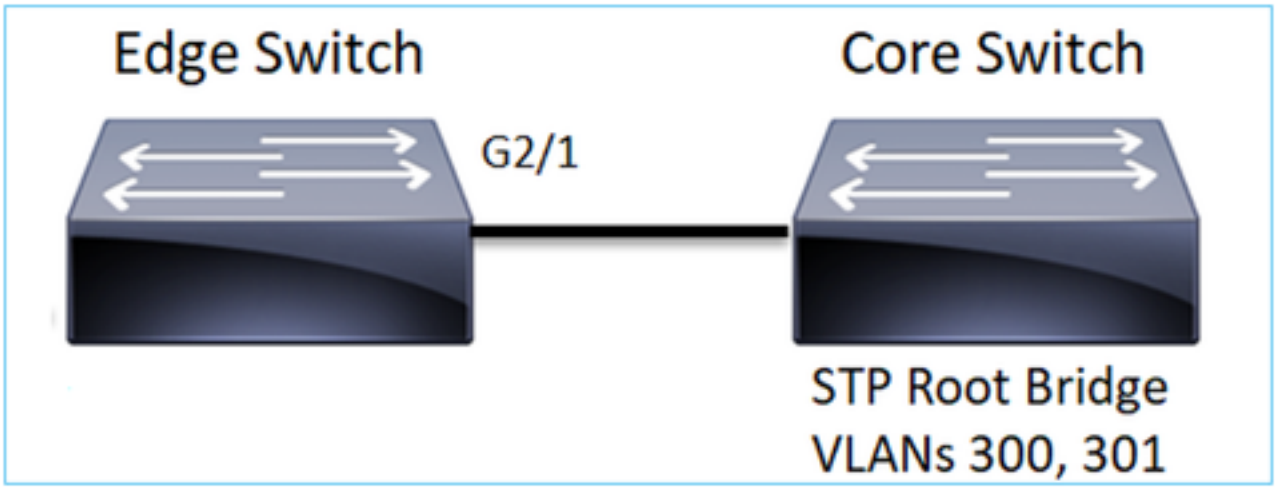
- ASA/FTD High Availability에는 SwitchPort 기능을 사용할 수 없습니다.이 내용은 FMC 컨피그레이션 가이드에 설명되어 있습니다. https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/regular_firewall_interfaces_for_firepower_threat_defense.html#topic_kqm_dgc_b3b



STP(Spanning Tree Protocol)와의 상호 작용

FP1010 내부 스위치는 STP를 실행하지 않습니다.

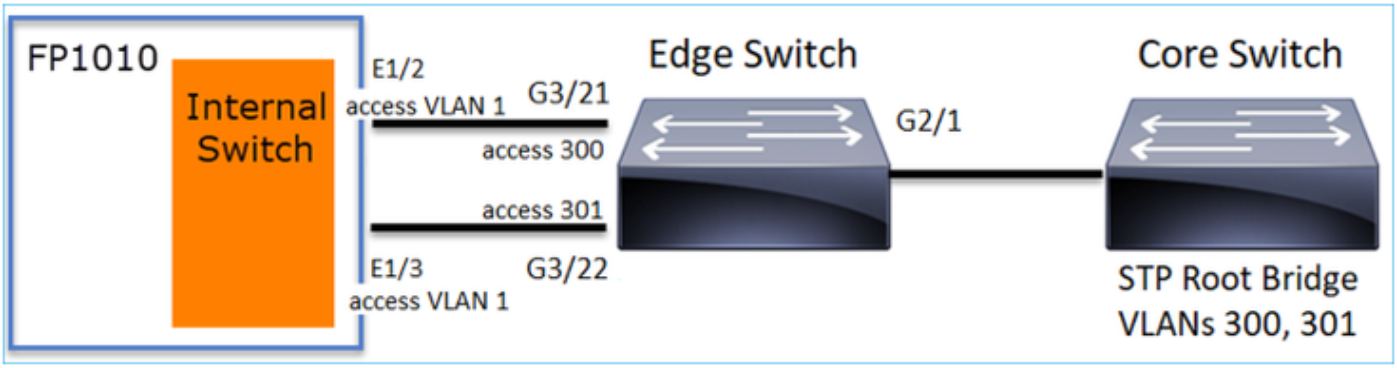
다음 시나리오를 고려해 보십시오.



에지 스위치에서 두 VLAN의 루트 포트는 G2/1입니다.

```
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
```

에지 스위치에 FP1010을 연결하고 동일한 VLAN(HW 스위칭)에서 두 포트를 모두 구성합니다.



문제

- G3/22에서 **수신된 VLAN** 301에 대한 우수한 BPDU가 VLAN에서 유출되기 때문

```
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
```

경고:L2 스위치를 FP1010에 연결할 경우 STP 도메인에 영향을 줄 수 있습니다

이 내용은 FMC 컨피그레이션 가이드에도 설명되어 있습니다.

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

다음은 이 기능 지원을 위한 REST API입니다.

- L2 물리적 인터페이스 [지원되는 PUT/GET]

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

- VLAN 인터페이스 [지원되는 POST/PUT/GET/DELETE]

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

문제 해결/진단

진단 개요

- 로그 파일은 FTD/NGIPS 트러블슈팅 또는 show tech 출력에 캡처됩니다.다음은 트러블슈팅 시 더 자세한 내용을 확인해야 하는 항목입니다.
- /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

FXOS에서 데이터 수집(디바이스) - CLI

FTD(SSH)의 경우:

```
> 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)#
```

FTD의 경우(콘솔):

```
> 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 백엔드

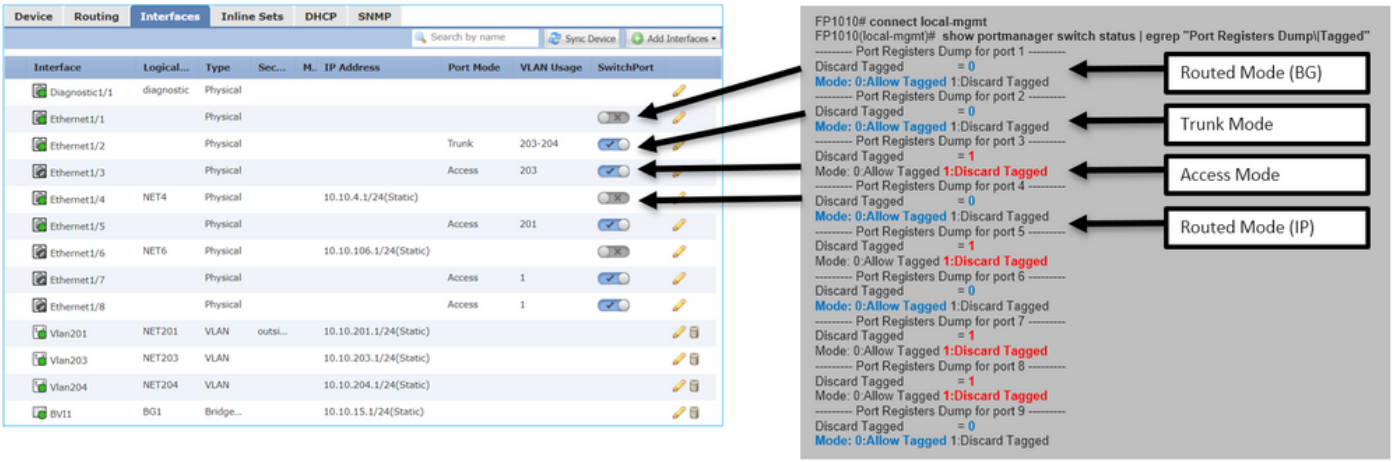
포트 레지스터는 모든 내부 스위치 및 포트 기능을 정의합니다.

이 스크린샷에서는 포트 레지스터의 'Port Control' 섹션이 표시되고, 특히 인터페이스에서 수신된

태그 처리된 트래픽을 폐기해야 하는지(1) 또는 허용해야 하는지(0)를 지시하는 레지스터가 표시됩니다. 한 포트에 대한 전체 등록 섹션은 다음과 같습니다.

```
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
```

이 스크린샷에서는 다양한 포트 모드에 대한 다양한 Discard Tagged 레지스터 값을 볼 수 있습니다.

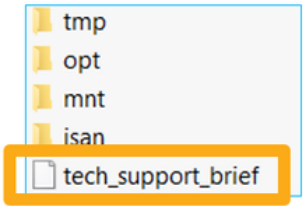


FP1010에서 FPRM 쇼 기술 수집

FPRM 번들을 생성하여 FTP 서버에 업로드하려면

```
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 번들에는 tech_support_brief라는 파일이 포함되어 있습니다.tech_support_brief 파일에는 일련의 show 명령이 포함되어 있습니다.그 중 하나는 **show portmanager 스위치 상태입니다**.



제한 사항 세부 사항, 일반적인 문제 및 해결 방법

6.5 릴리스의 구현 제한 사항

- 동적 라우팅 프로토콜은 SVI 인터페이스에 대해 지원되지 않습니다.
- 다중 컨텍스트는 1010에서 지원되지 않습니다.
- SVI VLAN ID 범위는 1~4070으로 제한됩니다.
- L2용 포트 채널이 지원되지 않습니다.
- 장애 조치 링크로 L2 포트는 지원되지 않습니다.

스위치 기능과 관련된 제한

기능	설명	제한
VLAN 인터페이스 수	생성할 수 있는 총 VLAN 인터페이스 수	60
트렁크 모드 VLAN	트렁크 모드의 포트에서 허용되는 최대 VLAN 수	20
네이티브 VLAN	태그가 지정되지 않은 모든 패킷 매핑 포트에서 포트에 구성된 네이티브 VLAN에 연결	1
명명된 인터페이스	명명된 모든 인터페이스 포함 (인터페이스 VLAN, 하위 인터페이스, 포트 채널, 물리적 인터페이스 등)	60

기타 제한 사항

- 하위 인터페이스와 인터페이스 VLAN은 동일한 VLAN을 사용할 수 없습니다.
- BVI에 참여하는 모든 인터페이스는 동일한 인터페이스 클래스에 속해야 합니다.
- L3 모드 포트와 L3 모드 포트 하위 인터페이스의 조합으로 BVI를 생성할 수 있습니다.
- 인터페이스 VLAN의 조합으로 BVI를 생성할 수 있습니다.
- L3 모드 포트와 인터페이스 VLAN을 혼합하여 BVI를 생성할 수 없습니다.

관련 정보

- Cisco Firepower 1010 Security Appliance

- 구성 가이드