라우팅 모드에서 Firepower Threat Defense 인터페이스 구성

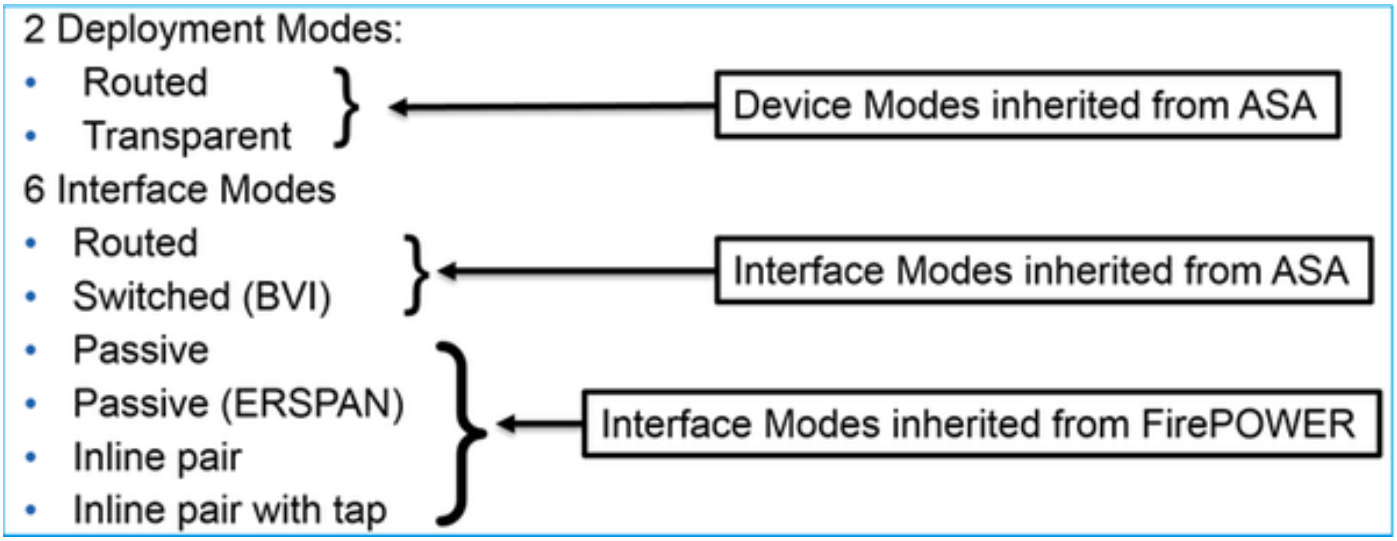
목차

소개

FTD(Firepower Threat Defense)는 다음 플랫폼에 설치할 수 있는 통합 소프트웨어 이미지입니다.

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR4100, FPR9300
- VMware(ESXi)
- AWS(Amazon Web Services)
- KVM
- ISR 라우터 모듈

FTD는 2개의 구축 모드와 6개의 인터페이스 모드를 제공합니다.



참고: 단일 FTD 어플라이언스에서 여러 인터페이스 모드를 함께 사용할 수 있습니다.

다음 표에는 다양한 FTD 구축 및 인터페이스 모드가 간략하게 요약되어 있습니다.

FTD 인터페이스 모드	FTD 구축 모드	설명	트래픽 삭제 가능 여부
라우팅 모드	라우팅 모드	전체 ASA 엔진 및 Snort 엔진 검사	예
전환됨	투명 모드	전체 ASA 엔진 및 Snort 엔진 검사	예
인라인 페어	라우팅 또는 투명 모드	부분 ASA 엔진 및 전체 Snort 엔진 검사	예
인라인 페어(탭 포함)	라우팅 또는 투명 모드	부분 ASA 엔진 및 전체 Snort 엔진 검사	아니요
수동	라우팅 또는 투명 모드	부분 ASA 엔진 및 전체 Snort 엔진 검사	아니요
수동(ERSPAN)	라우팅 모드	부분 ASA 엔진 및 전체 Snort 엔진 검사	아니요

목표

이 문서의 목표는 다음과 같습니다.

- FTD 라우팅 인터페이스 및 하위 인터페이스를 구성하는 방법 제시
- 라우팅 인터페이스 모드 작업 설명

사용되는 구성 요소

- FTD 코드 6.1.0.x를 실행하는 ASA5512-X
- 6.1.0.x를 실행하는 FMC(Firepower Management Center)

라우팅 인터페이스 및 하위 인터페이스 추가

다음 요건에 따라 하위 인터페이스 G0/0.201 및 인터페이스 G0/1을 구성합니다.

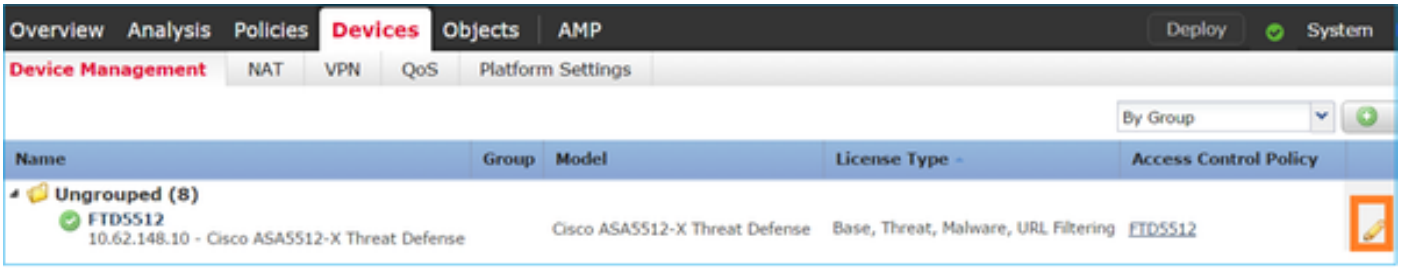
인터페이스	G0/0.201	G0/1
이름	내부	외부
Security Zone	INSIDE_ZONE	OUTSIDE_ZONE
설명	내부	EXTERNAL
하위 인터페이스 ID	201	-
VLAN ID	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
듀플렉스/속도	Auto	Auto

토폴로지

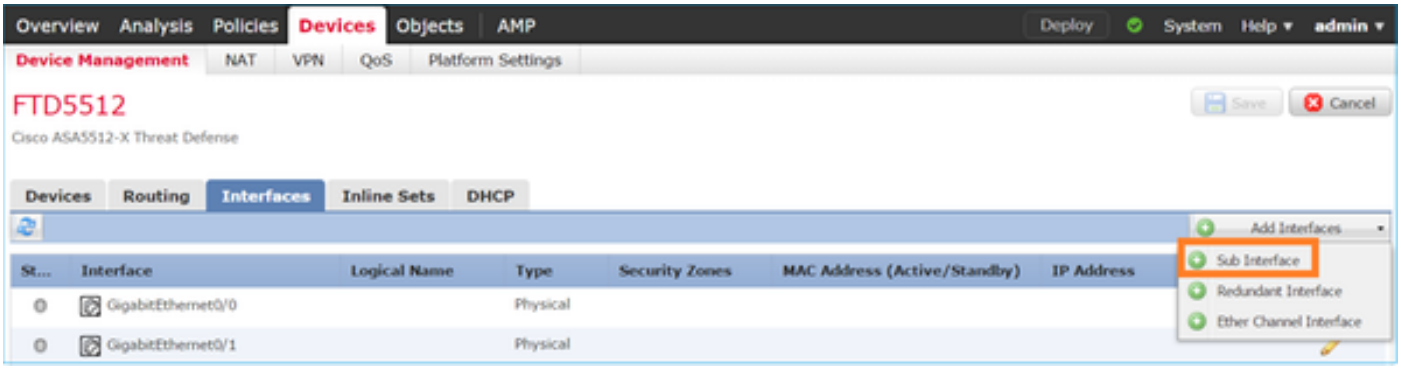
해결책

1단계 - 논리적 인터페이스(하위 인터페이스) 구성

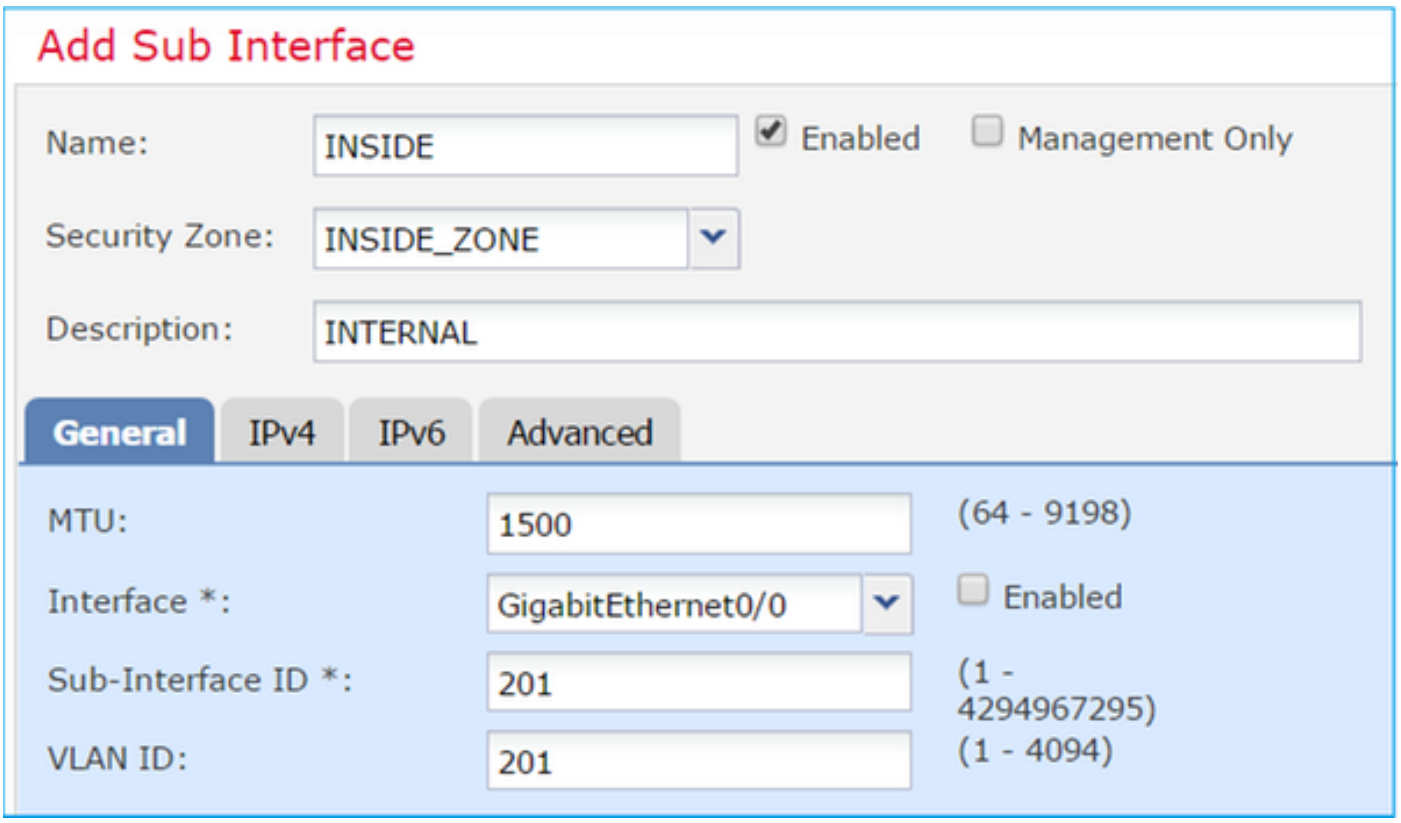
Devices(디바이스) > Device Management(디바이스 관리)로 이동하여 적절한 디바이스를 선택하고 **Edit(수정)** 아이콘을 클릭합니다.



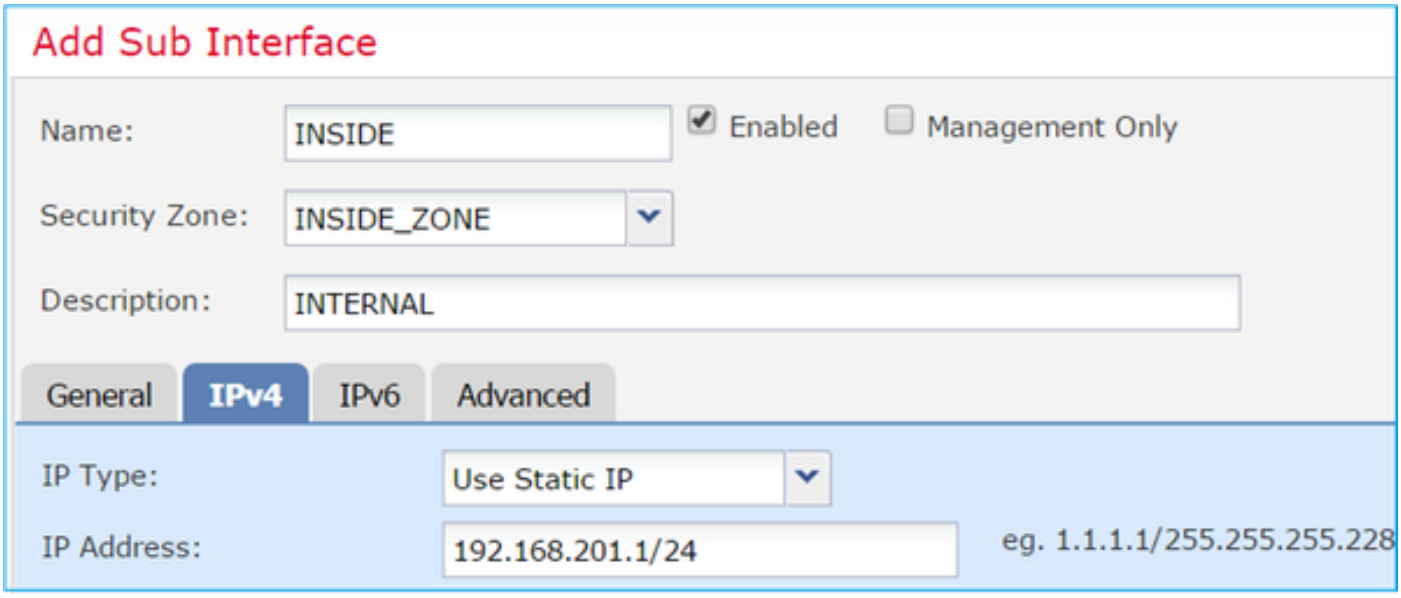
Add Interfaces(인터페이스 추가) > Sub Interface(하위 인터페이스)를 클릭합니다.



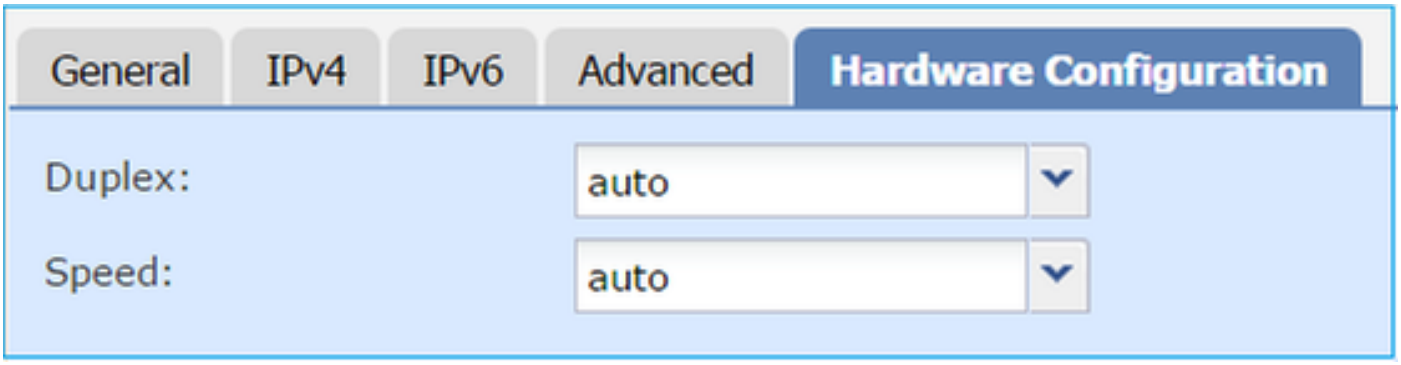
요건에 따라 하위 인터페이스 설정을 구성합니다.



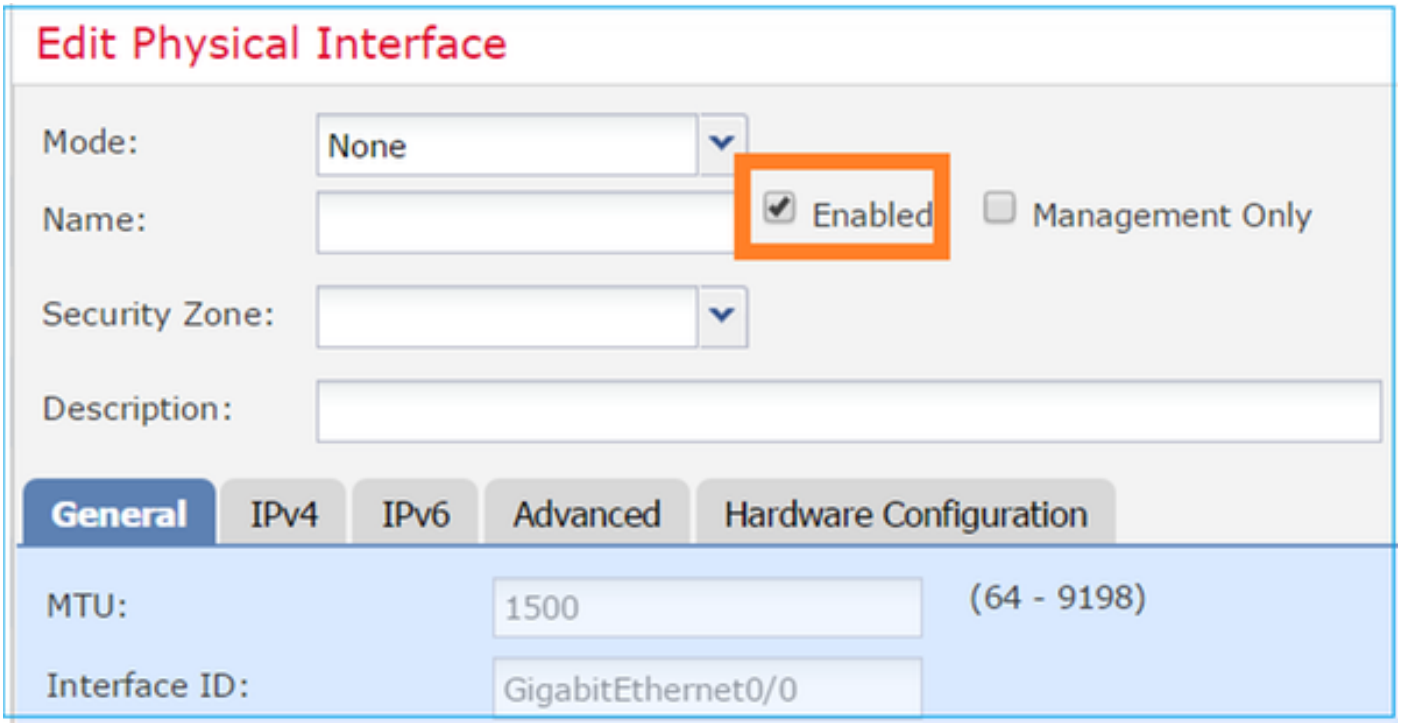
인터페이스 IP 설정:



물리적 인터페이스(GigabitEthernet0/0) 아래에서 Duplex(듀플렉스) 및 Speed(속도) 설정을 지정합니다.

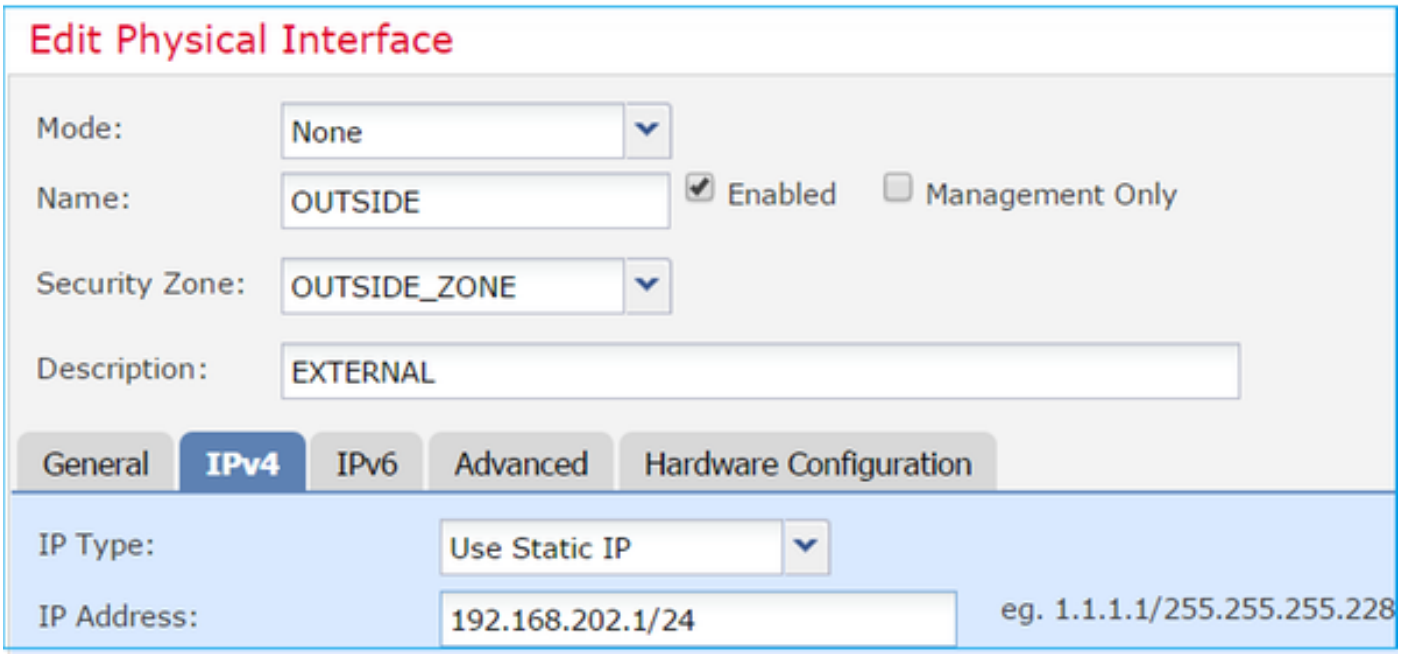


물리적 인터페이스(여기서는 G0/0)를 활성화합니다.



2단계 - 물리적 인터페이스 구성

요건에 따라 GigabitEthernet0/1 물리적 인터페이스를 수정합니다.

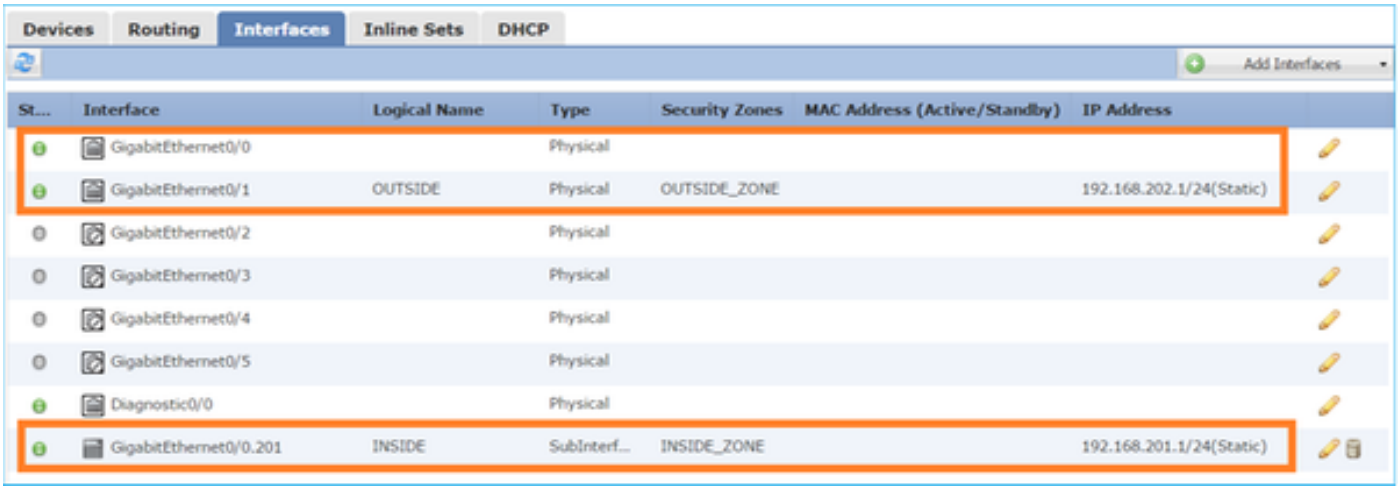


- 라우팅 인터페이스의 경우 모드는 **None(없음)**입니다.
- 이름은 ASA 인터페이스 **nameif**와 동일합니다.
- FTD에서 모든 인터페이스의 보안 레벨은 0입니다.

마지막으로 **Save(저장)**하고 **Deploy(구축)**합니다.

확인

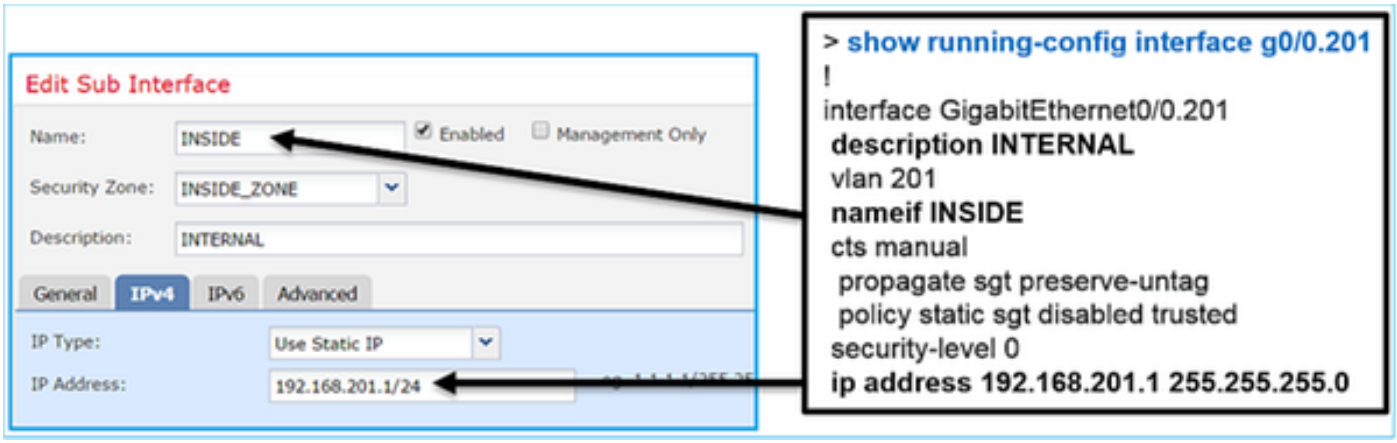
FMC GUI의 경우:



FTD CLI의 경우:

> **show interface ip brief** Interface IP-Address OK? Method Status Protocol GigabitEthernet0/0 unassigned YES unset up up **GigabitEthernet0/0.201 192.168.201.1 YES manual up up GigabitEthernet0/1 192.168.202.1 YES manual up up** GigabitEthernet0/2 unassigned YES unset administratively down down GigabitEthernet0/3 unassigned YES unset administratively down down GigabitEthernet0/4 unassigned YES unset administratively down down GigabitEthernet0/5 unassigned YES unset administratively down down Internal-Control0/0 127.0.1.1 YES unset up up Internal-Data0/0 unassigned YES unset up up Internal-Data0/1 unassigned YES unset up up Internal-Data0/2 169.254.1.1 YES unset up up Management0/0 unassigned YES unset up up > **show ip** System IP Addresses: Interface Name IP address Subnet mask Method GigabitEthernet0/0.201 INSIDE 192.168.201.1 255.255.255.0 manual GigabitEthernet0/1 OUTSIDE 192.168.202.1 255.255.255.0 manual Current IP Addresses: Interface Name IP address Subnet mask Method **GigabitEthernet0/0.201 INSIDE 192.168.201.1 255.255.255.0 manual GigabitEthernet0/1 OUTSIDE 192.168.202.1 255.255.255.0 manual**

FMC GUI 및 FTD CLI의 상관관계:



> **show interface g0/0.201 Interface GigabitEthernet0/0.201 "INSIDE", is up, line protocol is up** Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec **VLAN identifier 201 Description: INTERNAL** MAC address a89d.21ce.fdea, MTU 1500 **IP address 192.168.201.1, subnet mask 255.255.255.0** Traffic Statistics for "INSIDE": 1 packets input, 28 bytes 1 packets output, 28 bytes 0 packets dropped > **show interface g0/1 Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up** Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec **Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)** Input flow control is unsupported, output flow control is off **Description: EXTERNAL** MAC address a89d.21ce.fde7, MTU 1500 **IP address 192.168.202.1, subnet mask 255.255.255.0** 0 packets input, 0 bytes, 0 no buffer Received 0 broadcasts, 0 runts, 0 giants 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort 0 pause input, 0 resume input 0 L2 decode drops 1 packets output, 64 bytes, 0 underruns 0 pause output, 0 resume output 0 output errors, 0 collisions, 12 interface resets 0 late collisions, 0 deferred 0 input reset drops, 0 output reset drops input queue (blocks free curr/low): hardware (511/511) output queue (blocks free curr/low): hardware (511/511) Traffic Statistics for "OUTSIDE": 0 packets input, 0 bytes 0 packets output, 0 bytes 0 packets dropped 1 minute input rate 0 pkts/sec, 0 bytes/sec 1 minute output rate 0 pkts/sec, 0 bytes/sec 1 minute drop rate, 0 pkts/sec 5 minute input rate 0 pkts/sec, 0 bytes/sec 5 minute output rate 0 pkts/sec, 0 bytes/sec 5 minute drop rate, 0 pkts/sec >

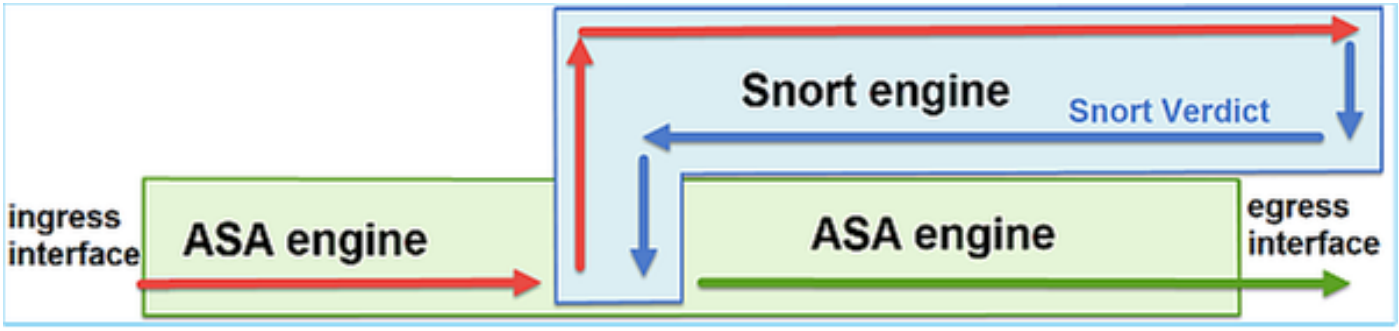
FTD 라우팅 인터페이스 작업

라우팅 인터페이스를 사용 중일 때 FTD 패킷 처리를 확인합니다.

해결책

FTD 아키텍처 개요

아래 그림에는 FTD 데이터 플레인이 대략적으로 나와 있습니다.



다음 그림에서는 각 엔진 내에서 수행되는 일부 검사를 보여줍니다.

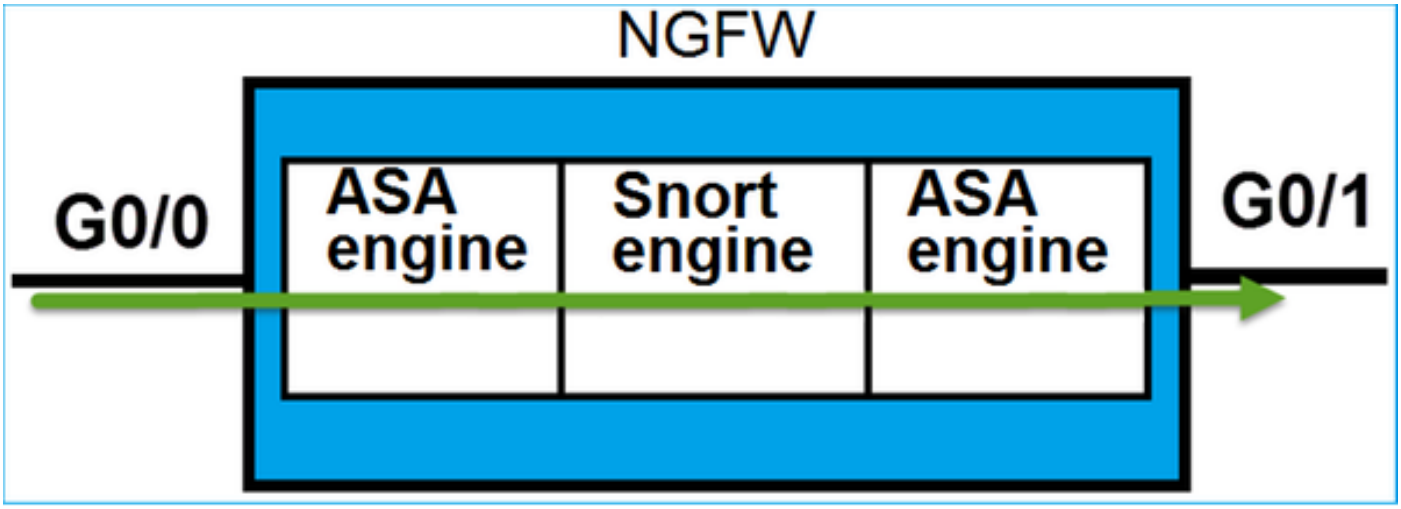
키포인트

- 맨 아래 검사는 FTD ASA 엔진 데이터 경로에 해당합니다.
- 파란색 상자 안의 검사는 FTD Snort 엔진 인스턴스에 해당합니다.

FTD 라우팅 인터페이스 개요

- **라우팅** 구축에서만 사용 가능
- 기존 **L3 방화벽 구축**
- 하나 이상의 물리적 또는 논리적(VLAN) 라우팅 가능 인터페이스
- NAT 또는 동적 라우팅 프로토콜과 같은 기능을 구성할 수 있음
- 패킷은 **경로 조회**를 기준으로 전달되며
  다음 홉은 **ARP 조회**를 기준으로 해결됨
- 실제 트래픽을 **삭제할 수 있음**
- **전체 ASA 엔진** 검사가 **전체 Snort 엔진** 검사와 함께 적용됨

마지막 항목은 다음 그림과 같이 표시할 수 있습니다.



FTD 라우팅 인터페이스에서 패킷 추적

토폴로지

적용된 정책을 확인하려면 다음 파라미터를 포함하여 패킷 트레이서를 사용합니다.

입력 인터페이스	내부
프로토콜/서비스	TCP 포트 80
Source IP(소스 IP)	192.168.201.100
Destination IP(목적지 IP)	192.168.202.100

해결책

아래에 나와 있는 것처럼 라우팅 인터페이스를 사용할 때는 패킷이 클래식 ASA 라우팅 인터페이스와 비슷한 방식으로 처리됩니다. 경로 조회, MPF(Modular Policy Framework), NAT, ARP 조회 등의 검사는 ASA 엔진 데이터 경로에서 수행됩니다. 또한, 액세스 제어 정책에 그렇게 하도록 지정된 경우에는 Snort 엔진(Snort 인스턴스 중 하나)이 패킷을 검사하여 판정(블랙리스트, 화이트리스트)합니다.

> **packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80**

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 192.168.202.100 using egress ifc OUTSIDE

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268437505
access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 -
Defau

lt/1
access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE
Additional Information:
This packet will be sent to snort for additional processing where a verdict
wil

l be reached

Phase: 3
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Config:
class-map class-default
match any
policy-map global_policy
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
service-policy global_policy global
Additional Information:

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS

```
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 11336, packet dispatched to next module

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: allow

>
```

참고 - 4단계에서는 UM_STATIC_TCP_MAP이라는 TCP 맵을 기준으로 하여 패킷을 검사합니다. 이 맵은 FTD의 기본 TCP 맵입니다.

```
firepower# show run all tcp-map ! tcp-map UM_STATIC_TCP_MAP
 no check-retransmission
 no checksum-verification
 exceed-mss allow
 queue-limit 0 timeout 4
 reserved-bits allow
 syn-data allow
 synack-data drop
 invalid-ack drop
 seq-past-window drop
 tcp-options range 6 7 allow
 tcp-options range 9 18 allow
 tcp-options range 20 255 allow
 tcp-options selective-ack allow
 tcp-options timestamp allow
 tcp-options window-scale allow
 tcp-options mss allow
 tcp-options md5 clear
 ttl-evasion-protection
 urgent-flag allow
 window-variation allow-connection
!
>
```

관련 문서

Firepower Device Manager, 버전 6.1용 Cisco Firepower Threat Defense 컨피그레이션 가이드

ASA 55xx-X 디바이스에서 Firepower Threat Defense 설치 및 업그레이드

FTD(Firepower Threat Defense) 캡처 및 패킷 트레이서 사용