인터페이스

다음 주제에서는 threat defense 디바이스에서 인터페이스를 컨피그레이션하는 방법을 설명합니다.

- Threat Defense 인터페이스에 대한 정보, 1 페이지
- 인터페이스에 대한 지침 및 제한 사항, 5 페이지
- 실제 인터페이스 구성, 6 페이지
- 브리지 그룹 구성, 11 페이지
- EtherChannel 구성, 16 페이지
- VLAN 인터페이스 및 스위치 포트 구성(Firepower 1010), 26 페이지
- VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성, 37 페이지
- 패시브 인터페이스 구성, 43 페이지
- 고급 인터페이스 옵션 구성, 47 페이지
- 인터페이스 변경 사항 스캔 및 인터페이스 마이그레이션, 51 페이지
- Secure Firewall 3100용 네트워크 모듈 관리, 57 페이지
- 정전(ISA 3000)에 대한 하드웨어 우회 구성, 66 페이지
- 모니터링 인터페이스, 68 페이지
- 인터페이스의 예시, 69 페이지

Threat Defense 인터페이스에 대한 정보

Threat Defense에는 데이터 인터페이스와 관리/진단 인터페이스가 포함되어 있습니다.

물리적 또는 가상 인터페이스 연결에 케이블을 연결하려면 인터페이스를 구성해야 합니다. 최소한 인터페이스 이름을 지정하고 트래픽을 전달하도록 인터페이스를 활성화해야 합니다. 인터페이스가 브리지 그룹의 멤버인 경우에는 이 작업만 수행하면 됩니다. 비브리지 그룹 멤버의 경우에는 인터페이스에 IP 주소도 지정해야 합니다. 지정된 포트의 단일 실제 인터페이스가 아닌 VLAN 하위 인터페이스를 생성하려는 경우에는 일반적으로 실제 인터페이스가 아닌 하위 인터페이스에 IP 주소를 구성합니다. VLAN 하위 인터페이스를 사용하면 물리적 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다. 이는 스위치의 트렁크 포트에 연결할 때 유용합니다. 패시브 인터페이스에서는 IP 주소를 구성하지 않습니다.

Interfaces(인터페이스**)** 페이지에는 인터페이스 유형의 하위 페이지인 **Interfaces(**인터페이스**)**(물리적 인터페이스용), **Bridge Groups(**브리지 그룹**)**, **Virtual Tunnel Interfaces**, **EtherChannels** 및 **VLAN**(for

the Firepower 1010)이 포함되어 있습니다. device manager이 아니라 FXOS에서만 EtherChannel 파라미터를 수정할 수 있기 때문에 Firepower 4100/9300 EtherChannel은 **Interfaces(**인터페이스**)** 페이지에 나열되며 **EtherChannel** 페이지에는 나열되지 않습니다. 각 페이지에는 사용 가능한 인터페이스, 해당 이름, 주소, 모드 및 상태가 표시됩니다. 인터페이스 목록에서 바로 인터페이스의 상태를 켜기 또는 끄기로 변경할 수 있습니다. 목록에는 컨피그레이션을 기준으로 인터페이스 특성이 표시됩니다. 브리지 그룹, EtherChannel 또는 VLAN 인터페이스의 열기/닫기 화살표를 사용하여 멤버 인터페이스를 확인하십시오. 이러한 인터페이스는 해당 목록에서 단독으로도 표시됩니다. 지원되는 상위 인터페이스의 하위 인터페이스도 확인할 수 있습니다. 이러한 인터페이스가 가상 인터페이스 및 네트워크 어댑터에 매핑되는 방식에 대한 자세한 정보는 VMware 네트워크 어댑터 및 인터페이스가 Threat Defense 물리적 인터페이스에 매핑되는 방식의 내용을 참조하십시오.

다음 항목에서는 device manager를 통해 인터페이스를 구성할 때의 제한사항과 기타 인터페이스 관리 개념에 관해 설명합니다.

인터페이스 모드

각 인터페이스에 대해 다음과 같은 모드 중 하나를 구성할 수 있습니다.

라우팅 모드

각 Layer 3 라우팅 인터페이스에는 고유한 서브넷의 IP 주소가 필요합니다. 이러한 인터페이스는 보통 스위치, 다른 라우터의 포트 또는 ISP/WAN 게이트웨이에 연결합니다.

수동

패시브 인터페이스는 스위치 SPAN(Switched Port Analyzer) 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다.

스위치 포트**(Firepower 1010)**

스위치 포트에서는 하드웨어에서 스위칭 기능을 사용하여 레이어 2에서 트래픽을 전달합니다. 동일한 VLAN의 스위치 포트는 하드웨어 스위칭을 사용하여 서로 통신할 수 있으며 트래픽에는 threat defense 보안 정책이 적용되지 않습니다. 액세스 포트의 경우 태그 없는 트래픽만 허용되며 이러한 포트는 단일 VLAN에 할당할 수 있습니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용되며 둘 이상의 VLAN에 속할 수 있습니다. 관리 인터페이스는 스위치 포트로 구성할 수 없습니다.

BridgeGroupMember

브리지 그룹은 threat defense 디바이스에서 경로 대신 브리징하는 인터페이스 그룹입니다. 모든 인터페이스는 동일한 네트워크에 있습니다. 브리지 그룹은 브리지 네트워크에 IP 주소가 있는 BVI(브리지 가상 인터페이스)로 표시됩니다.

BVI의 이름을 지정하면 라우팅 인터페이스와 BVI를 라우팅할 수 있습니다. 이 경우 BVI는 멤버 인터페이스와 라우팅 인터페이스 간의 게이트웨이 역할을 합니다. BVI의 이름을 지정하지 않으면 브리지 그룹 멤버 인터페이스의 트래픽은 브리지 그룹을 벗어날 수 없습니다. 일반적으로는 인터넷에 멤버 인터페이스를 라우팅할 수 있도록 인터페이스 이름을 지정합니다.

라우팅 모드에서 브리지 그룹을 사용하는 방식 중 하나는 외부 스위치 대신 threat defense 디바이스에서 추가 인터페이스를 사용하는 것입니다. 브리지 그룹 멤버 인터페이스에 엔드포인트를 직접 연결할 수 있습니다. 또한 스위치를 연결하여 BVI와 같은 네트워크에 엔드포인트를 더 추가할 수도 있습니다.

관리/진단 인터페이스

레이블이 관리(threat defense virtual의 경우 Management0/0 가상 인터페이스)인 물리적 포트에는 실제로 두 개의 별도 인터페이스가 연결되어 있습니다.

- 관리 가상 인터페이스 - 시스템 통신에 사용되는 IP 주소입니다. 이 주소는 시스템이 데이터베이스 업데이트를 검색할 때와 스마트 라이선싱에 사용하는 주소입니다. 이 주소에 대해 관리 세션(device manager 및 CLI)을 열 수 있습니다. **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 정의되는 관리 주소를 설정해야 합니다.
- 진단 가상 인터페이스 — 이 인터페이스를 사용하여 외부 시스템 로그 서버로 시스템 로그 메시지를 전송할 수 있습니다. 진단 인터페이스에 대한 IP 주소는 필요한 경우에만 구성하면 됩니다. 즉, 시스템 로그 메시지에 사용하려는 경우 인터페이스를 구성합니다. 이 인터페이스는 **Device(**디바이스**)** > **Interfaces(**인터페이스**)** 페이지에 표시되며 해당 페이지에서 구성할 수 있습니다. 진단 인터페이스는 관리 트래픽만 허용하며 통과 트래픽은 허용하지 않습니다.

(하드웨어 디바이스.) 관리/진단을 구성하는 한 가지 방법은 물리적 포트를 네트워크에 유선으로 연결하지 않는 것입니다. 대신 관리 IP 주소만 구성하고 인터넷에서 업데이트를 가져오는 게이트웨이로 데이터 인터페이스를 사용하도록 해당 주소를 구성합니다. 그런 다음 HTTPS/SSH 트래픽으로 연결되는 내부 인터페이스를 열고(기본값으로 HTTPS는 활성화되어 있음) 내부 IP 주소를 사용하여 device manager를 엽니다(관리 액세스 목록 구성 참조).

threat defense virtual의 경우 권장되는 컨피그레이션은 Management0/0을 내부 인터페이스와 같은 네트워크에 연결하고 내부 인터페이스를 게이트웨이로 사용하는 것입니다. 진단에 대해 별도의 주소를 구성하지는 마십시오.

별도의 관리 네트워크 구성에 대한 권장 사항

(하드웨어 디바이스.) 별도의 관리 네트워크를 사용하려는 경우 스위치 또는 라우터에 물리적 관리 인터페이스를 유선으로 연결합니다.

threat defense virtual의 경우, 임의의 데이터 인터페이스에서 별도의 네트워크에 Management0/0을 연결합니다. 기본 IP 주소를 계속 사용 중인 경우에는 동일한 서브넷에 있는 관리 IP 주소 또는 내부 인터페이스 IP 주소를 변경해야 합니다.

그런 후에 다음 항목을 구성합니다.

- **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택하고 연결된 네트워크에서 IPv4 또는 IPv6 주소, 또는 두 가지를 모두 설정합니다. 원하는 경우 네트워크의 다른 엔드포인트에 IPv4 주소를 제공하도록 DHCP 서버를 구성할 수 있습니다. 관리 네트워크에 인터넷으로의 경로가 포함된 라우터가 있으면 해당 라우터를 게이트웨이로 사용합니다. 그렇지 않은 경우에는 데이터 인터페이스를 게이트웨이로 사용합니다.

- 인터페이스를 통해 syslog 메시지를 시스템 로그 서버로 보내려는 경우에만 **Device(**디바이스**)** > **Interfaces(**인터페이스**)**에서 진단 인터페이스의 주소를 설정합니다. 그렇지 않은 경우에는 진단용 주소가 필요하지 않으므로 구성하지 마십시오. 구성하는 모든 IP 주소는 관리 IP 주소와 같은 서브넷에 있어야 하며 DHCP 서버 풀에 있을 수는 없습니다. 예를 들어, 관리 주소로 192.168.45.45를 사용하고 DHCP 풀로 192.168.45.46-192.168.45.254를 사용할 경우 192.168.45.1-192.168.45.44 범위에 포함되는 임의의 주소를 사용하여 진단을 구성할 수 있습니다.

보안 영역

각 인터페이스는 단일 보안 영역에 할당할 수 있습니다. 그런 후에 영역을 기준으로 하여 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 예를 들어, 트래픽이 내부에서 외부로는 이동하되 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다.

각 영역은 라우팅 또는 패시브 모드가 됩니다. 이 모드는 인터페이스 모드와 직접 관련이 있습니다. 라우팅 및 패시브 인터페이스는 같은 모드의 보안 영역에만 추가할 수 있습니다.

브리지 그룹의 경우 영역에 멤버 인터페이스를 추가할 수는 있지만 BVI(브리지 가상 인터페이스)는 추가할 수 없습니다.

영역에는 관리/진단 인터페이스를 포함하지 않습니다. 영역은 데이터 인터페이스에만 적용됩니다.

개체 페이지에서 보안 영역을 생성할 수 있습니다.

IPv6 주소 지정

IPv6를 위해 2가지 유형의 유니캐스트 주소를 구성할 수 있습니다.

- 전역—전역 주소는 공용 네트워크에서 사용할 수 있는 공용 주소입니다. 브리지 그룹의 경우 각 멤버 인터페이스가 아닌 BVI(브리지 가상 인터페이스)에 대해 글로벌 주소를 구성합니다. 다음 항목은 글로벌 주소로 지정할 수 없습니다.
  - 내부에서 예약된 IPv6 주소: fd00::/56(from=fd00:: to= fd00:0000:0000:00ff:ffff:ffff:ffff:ffff)
  - ::/128 등의 지정되지 않은 주소
  - 루프백 주소(::1/128)
  - 멀티캐스트 주소(ff00::/8)
  - 링크-로컬 주소(fe80::/10)
- 링크-로컬—링크-로컬 주소는 직접 연결된 네트워크에서만 사용할 수 있는 사설 주소입니다. 라우터에서 링크-로컬 주소를 사용하여 패킷을 전달하지 않습니다. 이는 특정 물리적 네트워크 세그먼트에서의 통신에만 사용됩니다. 이러한 주소는 주소 확인 및 네이버 검색과 같은 네트워크 검색 기능이나 주소 컨피그레이션에만 사용할 수 있습니다. 브리지 그룹에서 BVI에 대해 IPv6를 활성화하면 각 브리지 그룹 멤버 인터페이스에 대해 링크-로컬 주소가 자동으로 구성됩니다. 각 인터페이스에는 자체 주소가 있어야 합니다. 링크-로컬 주소는 세그먼트에서만 사용 가능하며 인터페이스 MAC 주소와 연결되기 때문입니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 링크-로컬 주소가 인터페이스에서 자동으로 구성되므로 링크-로컬 주소를 특별히 구성하지 않아도 됩니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

Auto-MDI/MDIX 기능

RJ-45 인터페이스의 경우 기본 자동 협상 설정에는 Auto-MDI/MDIX 기능도 포함됩니다. Auto-MDI/MDIX는 자동 협상 단계에서 직선 케이블이 감지된 경우 내부 크로스오버를 수행하므로 크로스오버 케이블이 필요 없습니다. 인터페이스에서 Auto-MDI/MDIX를 활성화하려면 속도 또는 양방향을 자동 협상하도록 설정해야 합니다. 속도와 양방향 둘 다 명시적으로 고정 값으로 설정한 경우 두 설정 모두에 대해 자동 협상을 사용 해제하면 Auto-MDI/MDIX도 사용 해제됩니다. 기가비트 인터넷의 경우 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 사용 설정된 상태이고 이를 사용 해제할 수 없습니다.

인터페이스에 대한 지침 및 제한 사항

다음 주제에서는 인터페이스의 몇 가지 제한 사항에 대해 다룹니다.

인터페이스 컨피그레이션에 대한 제한 사항

device manager를 사용하여 디바이스를 구성할 때는 인터페이스 구성에 여러 가지 제한이 적용됩니다. 다음 기능 중 어느 것이든 필요한 경우, management center를 사용하여 디바이스를 구성해야 합니다.

- 라우팅 방화벽 모드만 지원됩니다. 투명 방화벽 모드 인터페이스는 구성할 수 없습니다.
- 패시브 인터페이스는 구성할 수 있지만 ERSPAN 인터페이스는 구성할 수 없습니다.
- 인터페이스를 IPS 전용 처리를 위해 인라인(인라인 집합 내) 또는 인라인 탭으로 구성할 수는 없습니다. IPS 전용 모드 인터페이스는 여러 방화벽 검사를 건너뛰며 IPS 보안 정책만 지원합니다. 그에 비해 방화벽 모드 인터페이스는 흐름 유지, IP 및 TCP 레이어 둘 다에서 흐름 상태 추적, IP 조각 모음 및 TCP 표준화와 같은 방화벽 기능에 트래픽을 적용합니다. 보안 정책에 따라 이 방화벽 모드 트래픽에 대해 IPS 기능을 선택 사항으로 구성할 수도 있습니다.
- 이중 인터페이스는 구성할 수 없습니다.
- Firepower 1000, Firepower 2100, Secure Firewall 3100, ISA 3000 모델에 대해 device manager에서 EtherChannel을 구성할 수 있습니다. Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager **Interfaces(**인터페이스**)** 페이지에 표시됩니다.
- 브리지 그룹은 하나만 추가할 수 있습니다.
- Threat Defense는 라우팅 인터페이스에서만 IPv4 PPPoE를 지원합니다. 고가용성 장치에서는 PPPoE가 지원되지 않습니다.

디바이스 모델별 VLAN 하위 인터페이스의 최대 수

디바이스 모델은 구성할 수 있는 VLAN 하위 인터페이스의 최대 수를 제한합니다. 하위 인터페이스는 데이터 인터페이스에서만 구성할 수 있으며 관리 인터페이스에서는 구성할 수 없습니다.

다음 표에서는 각 디바이스 모델의 제한 사항에 대해 설명합니다.

모델	**VLAN** 하위 인터페이스의 최대 수
Firepower 1010	60
Firepower 1120	512
Firepower 1140, 1150	1024
Firepower 2100	1024
Secure Firewall 3100	1024
Firepower 4100	1024
Firepower 9300	1024
Threat Defense Virtual	50
ISA 3000	100

실제 인터페이스 구성

실제 인터페이스를 사용하려면 최소한 인터페이스를 활성화해야 합니다. 일반적으로는 실제 인터페이스의 이름을 지정하고 IP 주소를 구성합니다. VLAN 하위 인터페이스를 생성하려는 경우, 패시브 모드 인터페이스를 구성하는 경우 또는 인터페이스를 브리지 그룹에 추가하려는 경우에는 IP 주소를 구성하지 않습니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager **Interfaces(**인터페이스**)** 페이지에 표시되며, 이 절차는 그러한 EtherChannel에도 적용됩니다. 사용자는 섀시의 FXOS에서 Firepower 4100/9300 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다.

참고 물리적 인터페이스를 Firepower 1010 스위치 포트로 구성하려면 VLAN 인터페이스 및 스위치 포트 구성(Firepower 1010), 26 페이지의 내용을 참조하십시오.

물리적 인터페이스를 패시브 인터페이스로 구성하려면 패시브 모드로 물리적 인터페이스 구성, 46 페이지의 내용을 참조하십시오.

인터페이스를 비활성화하여 연결된 네트워크에서 전송을 일시적으로 차단할 수 있습니다. 인터페이스 컨피그레이션을 제거할 필요는 없습니다.

프로시저

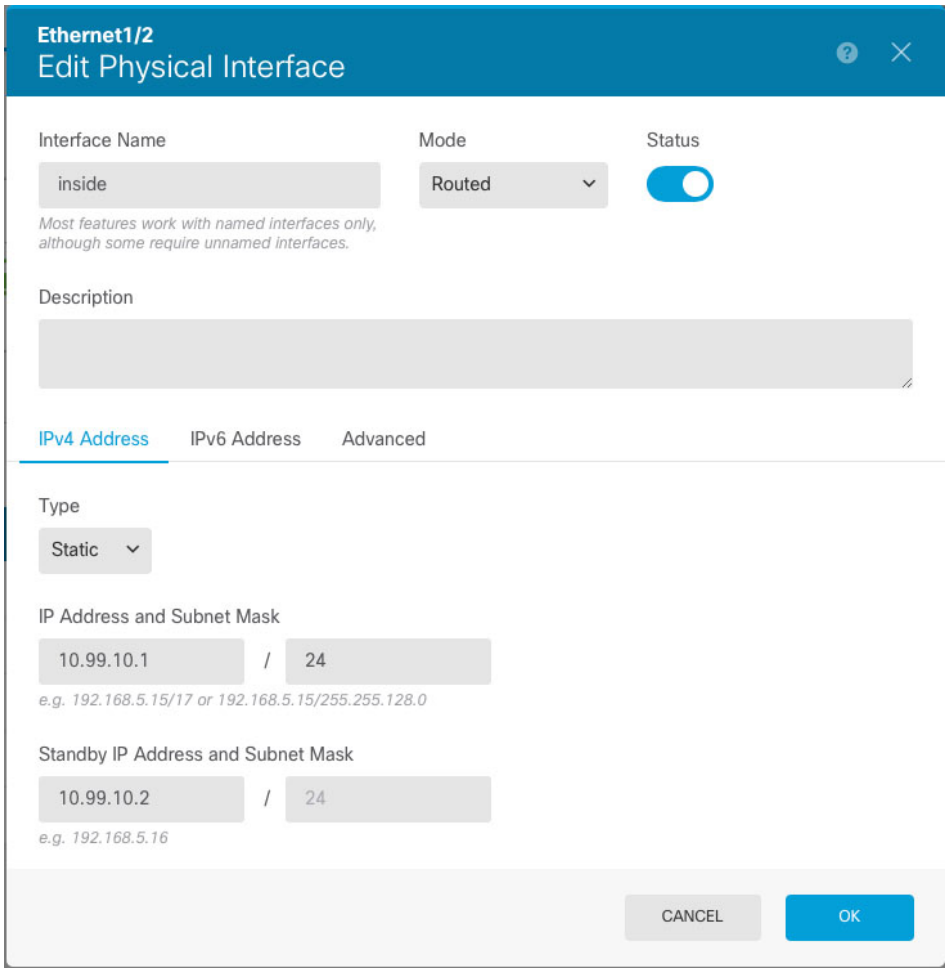
단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 수정할 실제 인터페이스의 수정 아이콘( )을 클릭합니다.

고가용성 컨피그레이션에서 페일오버 또는 스테이트풀 페일오버 링크로 사용 중인 인터페이스는 수정할 수 없습니다.

단계 **3** 다음을 설정합니다.



a) **Interface Name(**인터페이스 이름**)**을 설정합니다.

인터페이스의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이름을 입력하지 않으면 나머지 인터페이스 컨피그레이션이 무시됩니다. 하위 인터페이스를 구성하는 경우가 아니면 인터페이스에는 이름이 있어야 합니다. 참고**:** EtherChannel에 추가할 인터페이스의 이름을 구성하지 마십시오.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

b) **Mode(**모드**)**를 선택합니다.

- **Routed(**라우팅**)** - 라우팅 모드 인터페이스는 플로우 유지, IP 및 TCP 레이어 모두에서 플로우 상태 추적, IP 조각 모음, TCP 정규화 등의 모든 방화벽 기능과 방화벽 정책에 트래픽을 적용합니다. 이 모드가 기본 인터페이스 모드입니다.
- **Passive(**패시브**)** - 패시브 인터페이스는 스위치 SPAN 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 이 모드를 선택하는 경우 이 절차의 나머지 단계를 수행하지 마십시오. 대신 패시브 모드로 물리적 인터페이스 구성, 46 페이지 섹션을 참조하십시오. 패시브 인터페이스에서는 IP 주소를 구성할 수 없습니다.
- **Switch Port(**스위치 포트**)** - (Firepower 1010) 스위치 포트를 사용하면 동일한 VLAN에 있는 포트 간에 하드웨어 스위칭이 가능합니다. 스위칭된 트래픽에는 보안 정책이 적용되지 않습니다. 이 모드를 선택하는 경우 이 절차의 나머지 단계를 수행하지 마십시오. 대신, 다음을 참조하십시오. VLAN 인터페이스 및 스위치 포트 구성(Firepower 1010), 26 페이지

나중에 이 인터페이스를 브리지 그룹에 추가하면 모드가 자동으로 **BridgeGroupMember**로 변경됩니다. 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정()으로 지정합니다.

Firepower 4100/9300 디바이스에 있는 인터페이스의 경우 FXOS에서 인터페이스도 활성화해야 합니다.

이 실제 인터페이스에 대해 하위 인터페이스를 구성하려는 경우에는 이러한 작업만 수행하면 될 가능성이 높습니다. **Save(**저장**)**를 클릭하고 VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성, 37 페이지를 계속 진행합니다. 그렇지 않으면 아래 작업을 계속합니다.

참고 하위 인터페이스를 구성할 때도 인터페이스 이름을 지정하고 IP 주소를 제공할 수 있습니다. 이러한 방식은 일반적인 설정은 아니지만, 필요한 경우에는 해당 설정을 구성할 수 있습니다.

d) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **4** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- **DHCP** — 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(**경로 메트릭**)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(**기본 경로 얻기**)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).
- **Static(**고정**)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

  참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정의 내용을 참조하십시오.

- **PPPoE** — PPPoE(Point-to-Point Protocol over Ethernet)를 사용하여 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 다음 값을 설정합니다.
  - **Group Name(**그룹 이름**)** — 이 연결을 나타내는 그룹 이름을 원하는 대로 지정합니다.
  - **PPPoE Username(PPPoE** 사용자 이름**)** — ISP에서 제공한 사용자 이름을 지정합니다.
  - **PPPoE Password(PPPoE** 비밀번호**)** — ISP에서 제공한 비밀번호를 지정합니다.
  - **PPP Authentication(PPP** 인증**) - PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

    PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
  - **PPPoE Learned Route Metric(PPPoE** 학습된 경로 메트릭**)** — 학습된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
  - **Obtain Default Route from PPPoE(PPPoE**에서 기본 경로 가져오기**)** — PPPoE 서버에서 기본 경로를 가져오려면 이 확인란을 선택합니다.

- **IP Address Type(IP** 주소 유형**)** — PPPoE 서버에서 IP 주소를 가져오려면 **Dynamic(**동적**)**을 선택합니다. 또는 ISP에서 정적 IP 주소를 할당한 경우 **Static(**정적**)**을 선택할 수 있습니다.

단계 **5** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**)** - 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(**주소 자동 컨피그레이션**)** - 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

  RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Static Address/Prefix(**고정 주소/접두사**)** - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 4 페이지를 참조하십시오.

  주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

  참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. threat defense는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **6** (선택 사항). 고급 옵션 구성, 49 페이지에 전달하는 고성능 고속 어플라이언스입니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 보안 영역에 인터페이스를 추가합니다. 보안 영역 구성의 내용을 참조하십시오.
- 동적 DNS 서비스 제공자에 FQDN(Fully Qualified Domain Name)을 등록하고 DNS 서버가 IPv4 및 IPv6 인터페이스 주소로 업데이트되도록 DDNS를 설정합니다. 동적 DNS 구성의 내용을 참조하십시오.

브리지 그룹 구성

브리지 그룹은 하나 이상의 인터페이스를 그룹화하는 가상 인터페이스입니다. 인터페이스를 그룹화하는 주요 이유는 스위치 인터페이스 그룹을 생성하기 위해서입니다. 따라서 브리지 그룹에 포함된 인터페이스에 워크스테이션 또는 기타 엔드포인트 디바이스를 직접 연결할 수 있습니다. 이러한 워크스테이션이나 디바이스는 별도의 물리적 스위치를 통해 연결할 필요는 없지만, 브리지 그룹 멤버에 스위치를 연결할 수도 있습니다.

그룹 멤버에는 IP 주소가 없습니다. 대신 모든 멤버 인터페이스는 BVI(브리지 가상 인터페이스)의 IP 주소를 공유합니다. BVI에서 IPv6를 활성화하는 경우 멤버 인터페이스에는 고유한 링크-로컬 주소가 자동으로 할당됩니다.

멤버 인터페이스는 개별적으로 활성화 및 비활성화합니다. 그러므로 사용하지 않는 인터페이스는 브리지 그룹에서 제거할 필요 없이 비활성화할 수 있습니다. 브리지 그룹 자체는 항상 활성화됩니다.

일반적으로는 BVI(브리지 그룹 인터페이스)에서 DHCP 서버를 구성합니다. 이 서버는 멤버 인터페이스를 통해 연결된 모든 엔드포인트에 대해 IP 주소를 제공합니다. 그러나 원하는 경우에는 멤버 인터페이스에 연결된 엔드포인트에서 고정 주소를 구성할 수 있습니다. 브리지 그룹 내의 모든 엔드포인트에는 브리지 그룹 IP 주소와 같은 서브넷의 IP 주소가 있어야 합니다.

지침 및 제한 사항

- 브리지 그룹을 한 개 추가할 수 있습니다.
- Device Manager 정의 EtherChannel은 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.

- Firepower 2100 Series 또는 threat defense virtual 디바이스에서는 브리지 그룹을 구성할 수 없습니다.
- Firepower 1010의 경우, 동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수 없습니다.
- ISA 3000는 브리지 그룹 BVI1으로 사전 구성된 상태로 제공됩니다(이름은 지정되어 있지 않으며, 이는 라우팅에 참여하지 않음을 의미). BVI1에는 모든 데이터 인터페이스(GigabitEthernet1/1(outside1), GigabitEthernet1/2(inside1), GigabitEthernet1/3(outside2), GigabitEthernet1/4(inside2))가 포함되어 있습니다. 네트워크와 일치하도록 BVI1 IP 주소를 설정해야 합니다.

시작하기 전에

브리지 그룹의 멤버로 추가할 인터페이스를 구성합니다. 구체적으로 각 멤버 인터페이스는 다음 요건을 충족해야 합니다.

- 인터페이스에 이름이 있어야 합니다.
- 인터페이스에 대해 IPv4 또는 IPv6 주소(고정 주소 또는 DHCP를 통해 제공된 주소)가 정의되어 있으면 안 됩니다. 현재 사용 중인 인터페이스에서 주소를 제거해야 하는 경우에는 주소가 있는 인터페이스를 사용하는 인터페이스의 다른 컨피그레이션(예: 정적 경로, DHCP 서버 또는 NAT 규칙)도 제거해야 할 수 있습니다.
- 인터페이스가 보안 영역에 있는 경우 보안 영역에서 인터페이스를 제거하고 인터페이스에 대한 NAT 규칙을 삭제해야 브리지 그룹에 인터페이스를 추가할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **Bridge Groups(**브리지 그룹**)**를 클릭합니다.

브리지 그룹 목록에는 기존 브리지 그룹이 표시됩니다. 각 브리지 그룹의 멤버 인터페이스를 보려면 열기/닫기 화살표를 클릭합니다. 멤버 인터페이스는 **Interfaces(**인터페이스**)** 또는 **VLAN** 페이지에 개별적으로도 표시됩니다.

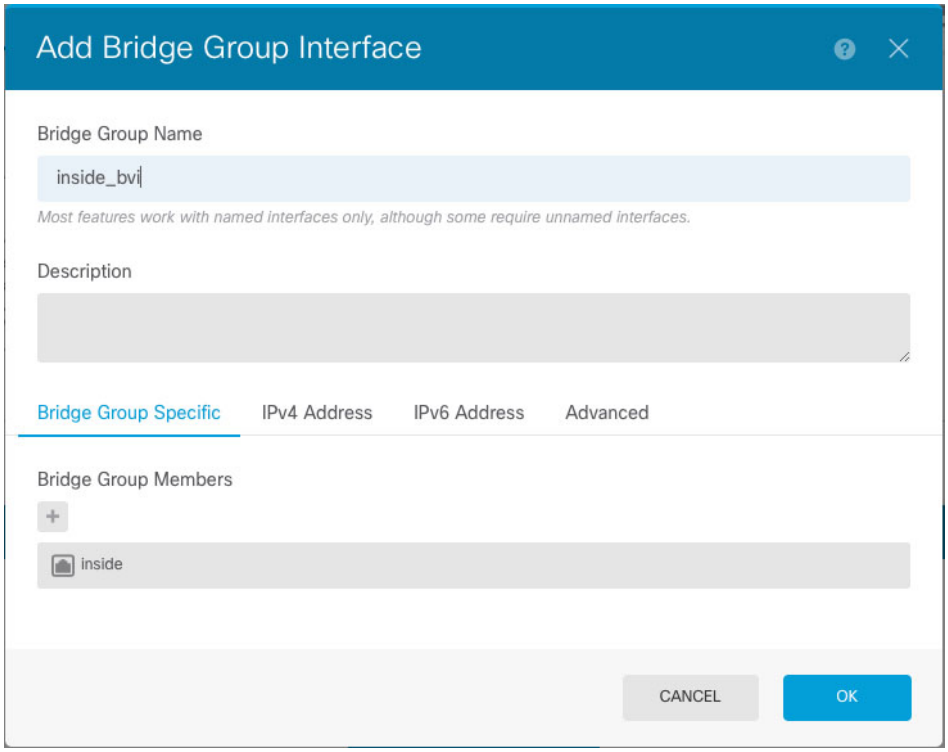
단계 **2** 다음 중 하나를 수행합니다.

- BVI1 브리지 그룹의 수정 아이콘( )을 클릭합니다.
- **Create Bridge Group(**브리지 그룹 생성**)** 또는 더하기 아이콘( )을 클릭하여 새 그룹을 생성합니다.

  참고 단일 브리지 그룹을 생성할 수 있습니다. 브리지 그룹을 이미 정의한 경우에는 새 그룹을 생성하는 대신 해당 그룹을 수정해야 합니다. 새 브리지 그룹을 생성해야 하는 경우 먼저 기존 브리지 그룹을 삭제해야 합니다.

- 더 이상 필요하지 않은 브리지 그룹의 삭제 아이콘( )을 클릭합니다. 브리지 그룹을 삭제하면 해당 멤버는 표준 라우팅 인터페이스가 되며 모든 NAT 규칙 또는 보안 영역 멤버십은 유지됩니다. 인터페이스를 수정하여 IP 주소를 지정할 수 있습니다. 새 브리지 그룹에 인터페이스를 추가하려는 경우에는 먼저 NAT 규칙을 제거하고 인터페이스를 해당 보안 영역에서 제거해야 합니다.

단계 **3** 다음을 구성합니다.



a) (선택 사항) **Interface Name(**인터페이스 이름**)**을 설정합니다.

브리지 그룹의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이 BVI가 해당 인터페이스와 다른 명명된 인터페이스 간의 라우팅에 참여하게 만들려면 이름을 설정합니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

b) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

c) **Bridge Group Members(**브리지 그룹 멤버**)** 목록을 수정합니다.

단일 브리지 그룹에는 인터페이스 또는 하위 인터페이스를 64개까지 추가할 수 있습니다.

- 인터페이스 추가 — 더하기 아이콘(+)을 클릭하고 하나 이상의 인터페이스를 클릭한 다음, **OK(**확인**)**를 클릭합니다.
- 인터페이스 제거 — 인터페이스 위에 마우스를 올려놓고 오른쪽의 **x**를 클릭합니다.

단계 **4** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- **Static(**고정**)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 브리지 그룹의 IP 주소와 서브넷 마스크를 입력합니다. 연결되는 모든 엔드포인트는 이 네트워크에 포함됩니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

  참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정의 내용을 참조하십시오.

- **Dynamic(**동적**)**(DHCP) - 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 이 옵션은 브리지 그룹에 대해 일반적으로 구성하는 항목은 아니지만 필요한 경우 구성할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다.필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(**경로 메트릭**)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(**기본 경로 얻기**)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

단계 **5** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**)** - 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Static Address/Prefix(**고정 주소/접두사**)** - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 4 페이지를 참조하십시오.

주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. 위협 방지 디바이스는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **6** (선택 사항). 고급 옵션 구성, 49 페이지에 전달하는 고성능 고속 어플라이언스입니다.

대부분의 고급 옵션은 브리지 그룹 멤버 인터페이스에 대해 구성하지만 브리지 그룹 인터페이스에 대해 사용할 수 있는 옵션도 있습니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 사용하려는 모든 멤버 인터페이스가 활성화되어 있는지 확인합니다.
- 브리지 그룹에 대해 DHCP 서버를 구성합니다. DHCP 서버 설정를 참조하십시오.
- 적절한 보안 영역에 멤버 인터페이스를 추가합니다. 보안 영역 구성를 참조하십시오.
- ID, NAT, 액세스 등의 정책이 브리지 그룹 및 멤버 인터페이스에 필요한 서비스를 제공하는지 확인합니다.

EtherChannel 구성

이 섹션에서는 EtherChannel 및 이를 구성하는 방법에 대해 설명합니다.

참고 device manager의 EtherChannels을 다음 모델에 추가할 수 있습니다.

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- ISA 3000

Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager 인터페이스 페이지에 표시됩니다. 또한 threat defense virtual와 같은 다른 모델에서는 device manager에서 EtherChannel을 설정할 수 없습니다.

EtherChannel 정보

802.3ad EtherChannel은 개별 이더넷 링크(채널 그룹)의 번들로 구성된 논리적 인터페이스(일명 포트 채널 인터페이스)이므로, 단일 네트워크의 대역폭을 늘리게 됩니다. 포트 채널 인터페이스는 인터페이스 관련 기능을 구성할 경우 물리적 인터페이스와 동일한 방식으로 사용됩니다.

모델에서 지원하는 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.

채널 그룹 인터페이스

각 채널 그룹에는 최대 8개의 액티브 인터페이스를 포함할 수 있습니다.

채널 그룹의 모든 인터페이스는 유형과 속도가 같아야 합니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다.

EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 소스 또는 목적지 MAC 주소, IP 주소, TCP 및 UDP 포트 번호, VLAN 번호를 기준으로 전용 해시 알고리즘을 사용하여 인터페이스를 선택합니다.

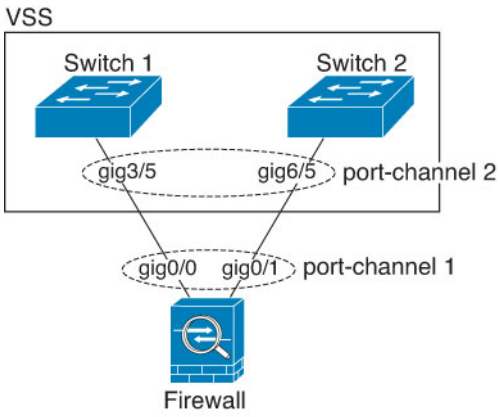
다른 디바이스에서 EtherChannel에 연결

threat defense EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다. 예를 들어 Catalyst 6500 스위치 또는 Cisco Nexus 7000에 연결할 수 있어야 합니다.

스위치가 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel)의 일부인 경우, 동일한 EtherChannel 내에서 threat defense 인터페이스를 연결하여 VSS/vPC에서 스위치를 분리할 수 있습니

다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다.

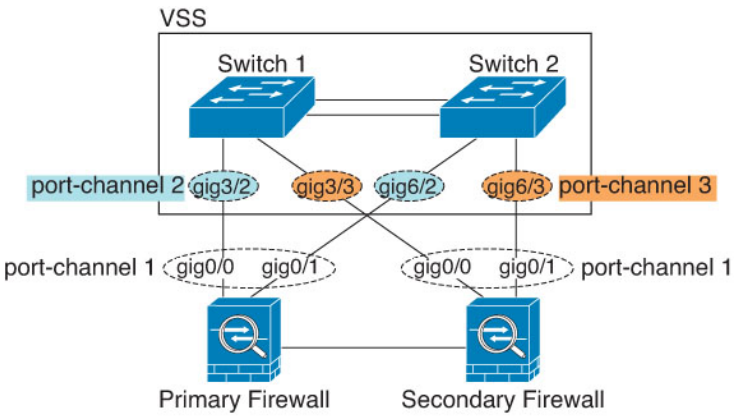
그림 ***1: VSS/vPC***에 연결



참고 threat defense 디바이스의 모드가 투명 방화벽 모드이고, 두 VSS/vPC 스위치 세트 사이에 threat defense 디바이스의 배치가 이루어지는 경우, EtherChannel을 사용하여 threat defense 디바이스에 연결된 모든 스위치 포트에서 UDLD(Unidirectional Link Detection)를 비활성화해야 합니다. UDLD를 활성화하면 스위치 포트가 다른 VSS/vPC 쌍의 두 스위치에서 제공되는 UDLD 패킷을 수신할 수 있습니다. 수신 스위치는 "UDLD 인접한 라우터 불일치"라는 이유와 함께 수신 인터페이스를 중단 상태로 설정합니다.

활성/대기 장애 조치 구축 시 threat defense 디바이스를 사용할 경우 VSS/vPC의 스위치에 각 threat defense 디바이스에 별도의 EtherChannel을 생성해야 합니다. 각 threat defense 디바이스에서 하나의 EtherChannel이 두 스위치 모두에 연결됩니다. 모든 스위치 인터페이스를 threat defense 디바이스에 연결된 단일 EtherChannel으로 그룹화하는 것은 가능하지만(이 경우 별도의 threat defense 시스템 ID로 인해 EtherChannel이 설정되지 않음), 스탠바이 threat defense 디바이스로 트래픽이 전송되는 것은 바람직하지 않으므로 단일 EtherChannel은 권장되지 않습니다.

그림 ***2:*** 액티브/스탠바이 장애 조치 및 ***VSS/vPC***



LACP(Link Aggregation Control Protocol)

LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 인터페이스를 다음과 같이 구성할 수 있습니다.

- Active(활성화) — LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- On(켜짐) — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

LACP에서는 사용자의 작업 없이 EtherChannel에 링크를 자동으로 추가 및 삭제하는 작업을 조율합니다. 또한 구성 오류를 처리하고 멤버 인터페이스의 양끝이 모두 올바른 채널 그룹에 연결되어 있는지 확인합니다. "On" 모드에서는 인터페이스가 중단될 경우 채널 그룹의 스탠바이 인터페이스를 사용할 수 없으며, 연결 및 컨피그레이션이 확인되지 않습니다.

부하 균형

threat defense 디바이스에서는 패킷의 소스 및 대상 IP 주소를 해싱하여 EtherChannel의 인터페이스에 패킷을 분산시킵니다(이 조건은 구성 가능함). 결과의 나머지 부분에 따라 흐름을 보유하는 인터페이스가 결정되는 모듈로 작업의 액티브 링크 수를 기준으로 결과 해시가 분할됩니다. *hash_value* **mod** *active_links*의 결과가 0인 모든 패킷은 EtherChannel의 첫 번째 인터페이스로 이동하고, 결과가 1인 패킷은 두 번째 인터페이스, 결과가 2인 패킷은 세 번째 인터페이스로 이동하는 방식이 이어집니다. 예를 들어 액티브 링크가 15개 있는 경우 모듈로 작업에서는 0에서 14까지의 값을 제공합니다. 액티브 링크가 6개인 경우 해당 값은 0 ~ 5가 되며, 이런 식으로 계속 적용할 수 있습니다.

액티브 인터페이스가 중단되고 스탠바이 인터페이스로 대체되지 않을 경우, 나머지 링크 간의 트래픽이 다시 밸런싱됩니다. 오류는 Layer 2의 스패닝 트리와 Layer 3의 라우팅 테이블에서 모두 마스킹되므로, 전환 작업은 다른 네트워크 디바이스에 투명하게 이루어집니다.

EtherChannel MAC 주소

채널 그룹의 일부인 모든 인터페이스에서는 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다.

포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우에 대비하여 직접 고유한 MAC 주소를 구성하는 것이 좋습니다. 포트-채널 MAC 주소를 제공하던 인터페이스를 삭제한 경우, 포트-채널 MAC 주소가 그다음으로 낮은 번호의 인터페이스로 바뀌면서 트래픽 중단이 일어납니다.

EtherChannel용 가이드라인

브리지 그룹

Device Manager정의 EtherChannel은 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.

고가용성

- 이중 또는 EtherChannel 인터페이스를 고가용성 링크로 사용할 경우, 고가용성 쌍의 두 유닛에 모두 이를 사전 구성해야 합니다. 복제를 위해서는 고가용성링크 자체가 필요하므로 이러한 인터페이스를 기본 유닛에 구성한 다음 이를 보조 유닛에 복제할 수 없습니다.
- 상태 링크에 EtherChannel 인터페이스를 사용할 경우, 특별한 컨피그레이션이 필요하지 않으며 컨피그레이션을 기본 유닛에서 정상적으로 복제할 수 있습니다. Firepower 4100/9300 섀시의 경우, EtherChannel을 비롯한 모든 인터페이스를 두 유닛에서 모두 사전 구성해야 합니다.
- **monitor-interface**명령을 사용하여 고가용성를 위한 EtherChannel 인터페이스를 모니터링. 액티브 멤버 인터페이스에서 스탠바이 인터페이스로 장애 조치를 시작할 경우, 디바이스 수준의 고가용성가 모니터링되고 있으면 이 작업을 수행해도 EtherChannel 인터페이스에 장애를 발생시키지 않습니다. 모든 물리적 인터페이스에 장애가 발생하는 경우에만 EtherChannel 인터페이스에 장애가 발생하는 것으로 나타납니다.
- 고가용성 또는 상태 링크에 EtherChannel 인터페이스를 사용할 경우, 패킷의 장애를 방지하기 위해 EtherChannel에서 하나의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 고가용성 링크로 사용 중인 경우 EtherChannel 구성을 변경할 수 없습니다. 구성을 변경하려면 고가용성을 일시적으로 비활성화해야 합니다. 이렇게 하면 지속 시간 동안 고가용성이 발생하지 않습니다.

모델 지원

- device manager의 EtherChannels을 다음 모델에 추가할 수 있습니다.
  - Firepower 1000
  - Firepower 2100
  - Secure Firewall 3100
  - ISA 3000

  Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager 인터페이스 페이지에 표시됩니다. 또한 ASA 5500-X 시리즈와 같은 다른 모델에서는 device manager에서 EtherChannel을 설정할 수 없습니다.
- EtherChannel에서는 Firepower 1010 스위치 포트 또는 VLAN 인터페이스를 사용할 수 없습니다.

EtherChannel 일반 지침

- 모델에서 사용할 수 있는 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.
- 각 채널 그룹에는 최대 8개의 액티브 인터페이스를 포함할 수 있습니다.
- 채널 그룹의 모든 인터페이스는 미디어 유형 및 속도 용량 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 속도가 Detect SFP(SFP 탐지)로 설정되어 있는 한 다른 인터페이스 용량을 지원하는 Secure Firewall 3100의 경우를 제외하고, 대용량 인터페이스에서는 속도를 더 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합할 수 없습니다. .
- threat defense EtherChannel을 연결하는 디바이스에서는 802.3ad EtherChannel도 지원해야 합니다.
- threat defense 디바이스에서는 VLAN 태그 처리된 LACPDU를 지원하지 않습니다. Cisco IOS **vlan dot1Q tag native** 명령을 사용하여 인접한 스위치에서 네이티브 VLAN 태깅을 활성화할 경우, threat defense 디바이스에서는 태그 처리된 LACPDU를 제거합니다. 인접한 스위치에서 네이티브 VLAN 태깅을 비활성화해야 합니다.
- Firepower 1000 및 Firepower 2100, Secure Firewall 3100은 LACP 속도, fast(빠르게)를 지원하지 않습니다. LACP는 항상 정상 속도를 사용합니다. 이 설정은 구성 가능하지 않습니다. FXOS에서 EtherChannel을 구성하는 Firepower 4100/9300의 LACP 속도는 기본적으로 fast(빠르게)로 설정되어 있습니다. 이러한 플랫폼에서는 속도를 구성할 수 있습니다.
- 15.1(1)S2 이전 Cisco IOS 소프트웨어 버전에서는 threat defense가 EtherChannel과 스위치 스택 간의 연결을 지원하지 않았습니다. 기본 스위치 설정으로 threat defense EtherChannel이 교차 스택에 연결되어 있는 상태에서 기본 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 가동되지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 다시 로드 시간을 고려하여 충분히 큰 값으로 설정합니다(예: 8분 또는 무한인 경우 0). 또는 15.1(1)S2 같은 더 안정적인 스위치 소프트웨어 버전으로 업그레이드할 수 있습니다.
- 모든 threat defense 컨피그레이션에서는 멤버 물리적 인터페이스 대신 논리적 EtherChannel 인터페이스를 참조합니다.

EtherChannel 추가

EtherChannel을 추가하고 멤버 인터페이스를 할당합니다.

참고 device manager의 EtherChannels을 다음 모델에 추가할 수 있습니다.

- Firepower 1000
- Firepower 2100
- Secure Firewall 3100
- ISA 3000

Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다. Firepower 4100/9300 EtherChannel은 단일한 물리적 인터페이스와 함께 device manager 인터페이스 페이지에 표시됩니다. 또한 ASA 5500-X 시리즈와 같은 다른 모델에서는 device manager에서 EtherChannel을 설정할 수 없습니다.

시작하기 전에

- 채널 그룹의 모든 인터페이스는 미디어 유형 및 속도 용량 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 속도가 Detect SFP(SFP 탐지)로 설정되어 있는 한 다른 인터페이스 용량을 지원하는 Secure Firewall 3100의 경우를 제외하고, 대용량 인터페이스에서는 속도를 더 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합할 수 없습니다. .
- 멤버 인터페이스의 이름을 지정할 수 없습니다.

주의 구성에서 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 구성이 지워집니다.

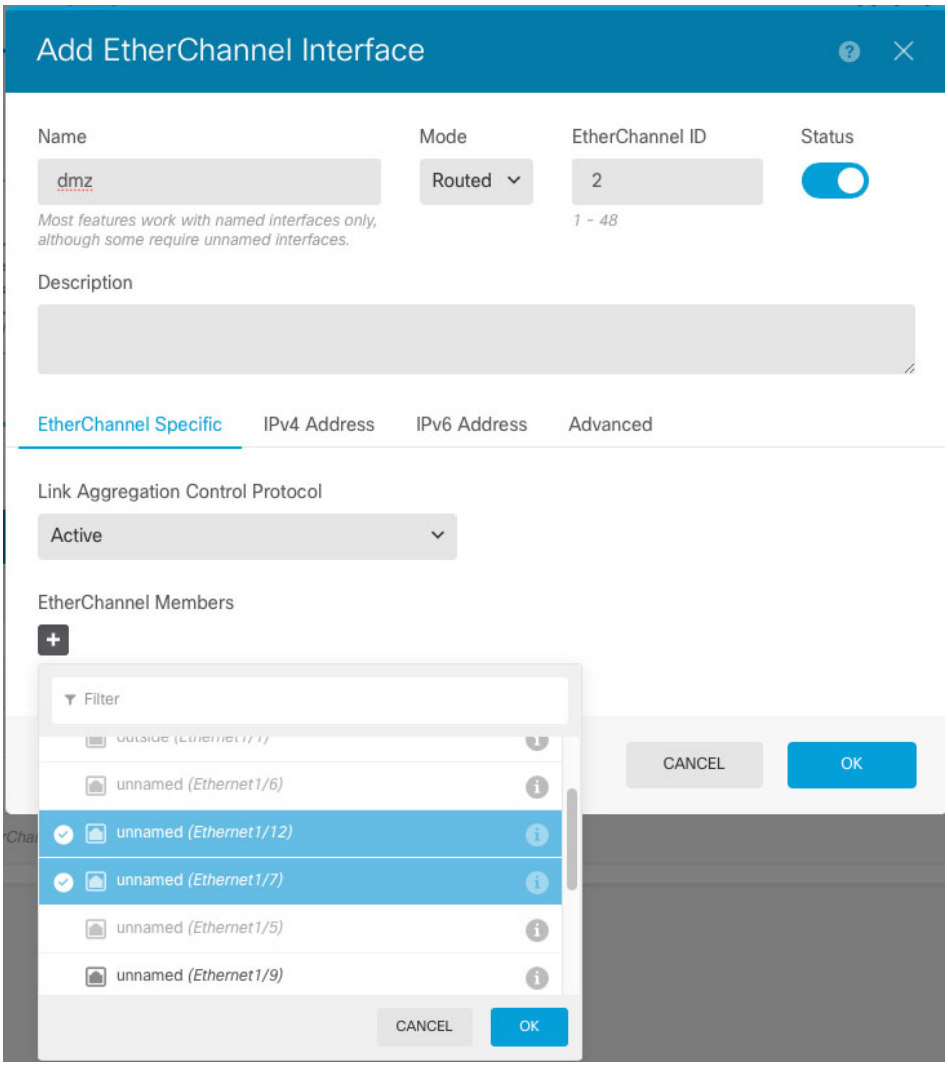
프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **EtherChannel**을 클릭합니다.

EtherChannel 목록에는 기존 EtherChannel, 해당 이름, 주소 및 상태가 표시됩니다. 각 EtherChannel의 멤버 인터페이스를 보려면 열기/닫기 화살표를 클릭합니다. 멤버 인터페이스는 **Interfaces(**인터페이스**)** 페이지에 개별적으로도 표시됩니다.

단계 **2** **Create EtherChannel(EtherChannel** 생성**)**(현재 EtherChannel이 없는 경우) 또는 더하기 아이콘(+ ˅)을 클릭한 다음, **EtherChannel**을 클릭하여 새 EtherChannel을 생성합니다.

단계 **3** 다음을 구성합니다.



a) **Interface Name(**인터페이스 이름**)**을 설정합니다.

EtherChannel의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

b) **Mode(**모드**)**를 설정합니다.

- **Routed(**라우팅**)** — 라우팅 모드 인터페이스는 플로우 유지, IP 및 TCP 레이어 모두에서 플로우 상태 추적, IP 조각 모음, TCP 정규화 등의 모든 방화벽 기능과 방화벽 정책에 트래픽을 적용합니다. 트래픽이 인터페이스를 통과하도록 하려는 경우 이 모드를 사용합니다. 이 모드가 기본 인터페이스 모드입니다.

- **Passive(패시브)** - 패시브 인터페이스는 스위치 SPAN 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다. 수동 구축으로 구성된 시스템에서는 트래픽 차단 또는 형성과 같은 특정 작업을 할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다. 이 모드를 선택하는 경우 이 절차의 나머지 단계를 수행하지 마십시오. 대신 패시브 모드로 물리적 인터페이스 구성, 46 페이지 섹션을 참조하십시오.

c) **EtherChannel ID**를 1~48(Firepower 1010의 경우 1~8)로 설정합니다.

d) **Status(상태)** 슬라이더를 활성화된 설정()으로 지정합니다.

e) (선택 사항) **Description(설명)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

f) **EtherChannel Mode(EtherChannel 모드)**를 선택합니다.

- **Active(액티브)** — (권장) LACP 업데이트를 보내고 받습니다. 액티브 EtherChannel은 액티브 또는 패시브 EtherChannel과의 연결을 설정할 수 있습니다. LACP 트래픽 양을 최소화할 필요가 없는 한 액티브 모드를 사용해야 합니다.
- **On(켜짐)** — EtherChannel은 항상 켜져 있으며 LACP는 사용되지 않습니다. "on"으로 된 EtherChannel은 오로지 또 다른 "on" 상태의 EtherChannel과 연결을 설정할 수 있습니다.

g) **EtherChannel Members(EtherChannel 멤버)**를 추가합니다.

EtherChannel에는 최대 8개(이름 미지정)의 인터페이스를 추가할 수 있습니다.

- 인터페이스 추가 — 더하기 아이콘()을 클릭하고 하나 이상의 인터페이스를 클릭한 다음, **OK(확인)**를 클릭합니다.
- 인터페이스 제거 — 인터페이스 위에 마우스를 올려놓고 오른쪽의 **x**를 클릭합니다.

단계 **4** **IPv4 Address(IPv4 주소)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형) 필드에서 다음 옵션 중 하나를 선택합니다.

- **DHCP** — 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(경로 메트릭)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(기본 경로 얻기)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).
- **Static(고정)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정의 내용을 참조하십시오.

- **PPPoE** — PPPoE(Point-to-Point Protocol over Ethernet)를 사용하여 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 다음 값을 설정합니다.
  - **Group Name(**그룹 이름**)** — 이 연결을 나타내는 그룹 이름을 원하는 대로 지정합니다.
  - **PPPoE Username(PPPoE** 사용자 이름**)** — ISP에서 제공한 사용자 이름을 지정합니다.
  - **PPPoE Password(PPPoE** 비밀번호**)** — ISP에서 제공한 비밀번호를 지정합니다.
  - **PPP Authentication(PPP** 인증**) - PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

    PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
  - **PPPoE Learned Route Metric(PPPoE** 학습된 경로 메트릭**)** — 학습된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
  - **Obtain Default Route from PPPoE(PPPoE**에서 기본 경로 가져오기**)** — PPPoE 서버에서 기본 경로를 가져오려면 이 확인란을 선택합니다.
  - **IP Address Type(IP** 주소 유형**)** — PPPoE 서버에서 IP 주소를 가져오려면 **Dynamic(**동적**)**을 선택합니다. 또는 ISP에서 정적 IP 주소를 할당한 경우 **Static(**정적**)**을 선택할 수 있습니다.

단계 **5** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**) -** 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(**주소 자동 컨피그레이션**) -** 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스

를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Static Address/Prefix(**고정 주소/접두사**)** - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 4 페이지를 참조하십시오.

  주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

  참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. threat defense는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **6** **Advanced(**고급**)**를 클릭하고 속도를 설정하여 멤버 인터페이스의 속도를 설정합니다.

다른 고급 옵션을 구성할 수도 있습니다. 고급 옵션 구성, 49 페이지의 내용을 참조하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 보안 영역에 EtherChannel을 추가합니다. 보안 영역 구성의 내용을 참조하십시오.

VLAN 인터페이스 및 스위치 포트 구성(Firepower 1010)

각 Firepower 1010 인터페이스가 일반 방화벽 인터페이스 또는 레이어 2 하드웨어 스위치 포트로 실행되도록 구성할 수 있습니다. 이 섹션에는 스위치 모드의 활성화 또는 비활성화, VLAN 인터페이스 생성 및 VLAN에 스위치 포트 할당 등을 비롯하여 스위치 포트의 구성을 시작하기 위한 작업이 포함되어 있습니다. 이 섹션에서는 지원되는 인터페이스에서 PoE(Power over Ethernet)를 맞춤화하는 방법에 대해서도 설명합니다.

Firepower 1010 포트 및 인터페이스 이해

포트 및 인터페이스

각 물리적 Firepower 1010 인터페이스의 경우, 해당 작업을 방화벽 인터페이스 또는 스위치 포트로 설정할 수 있습니다. 물리적 인터페이스, 포트 유형 및 스위치 포트를 할당할 논리적 VLAN 인터페이스에 대한 다음과 같은 정보를 참조하십시오.

- 물리적 방화벽 인터페이스 - 라우팅 모드에서 이러한 인터페이스는 구성된 보안 정책을 사용해 방화벽과 VPN 서비스를 적용하여 레이어 3에서 네트워크 간에 트래픽을 전달합니다. 라우팅 모드에서는 일부 인터페이스와의 통합 라우팅 및 브리징을 브리지 그룹 멤버로 사용하고 기타 인터페이스를 레이어 3 인터페이스로 사용할 수도 있습니다. 기본적으로 Ethernet 1/1 인터페이스는 방화벽 인터페이스로 구성됩니다.이러한 인터페이스를 IPS 전용(패시브 인터페이스)으로 구성할 수도 있습니다.
- 물리적 스위치 포트 - 스위치 포트에서는 하드웨어에서 스위칭 기능을 사용하여 레이어 2에서 트래픽을 전달합니다. 동일한 VLAN의 스위치 포트는 하드웨어 스위칭을 사용하여 서로 통신할 수 있으며 트래픽에는 threat defense 보안 정책이 적용되지 않습니다. 액세스 포트의 경우 태그 없는 트래픽만 허용되며 이러한 포트는 단일 VLAN에 할당할 수 있습니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용되며 둘 이상의 VLAN에 속할 수 있습니다. 기본적으로, Ethernet 1/2~1/8은 VLAN 1에서 액세스 스위치 포트로 설정됩니다. 관리 인터페이스는 스위치 포트로 구성할 수 없습니다.
- 논리적 VLAN 인터페이스 - 이러한 인터페이스는 물리적 방화벽 인터페이스와 동일하게 작동합니다. 단, 하위 인터페이스IPS 전용 인터페이스(인라인 집합 및 패시브 인터페이스) 또는 EtherChannel 인터페이스는 생성할 수 없습니다. 스위치 포트가 다른 네트워크와 통신해야 하는 경우, threat defense 디바이스에서 VLAN 인터페이스에 보안 정책을 적용하고 다른 논리적 VLAN 인터페이스 또는 방화벽 인터페이스로 라우팅됩니다. VLAN 인터페이스와의 통합 라우팅 및 브리징을 브리지 그룹 멤버로 사용할 수도 있습니다. 동일한 VLAN의 스위치 포트 간 트래픽에는 threat defense 보안 정책이 적용되지 않지만, 브리지 그룹에 있는 VLAN 간의 트래픽에는 보안 정책이 적용됩니다. 따라서 특정 세그먼트 간에 보안 정책을 적용하려면 레이어 브리지 그룹 및 스위치 포트를 계층화하도록 선택할 수 있습니다.

PoE(Power over Ethernet)

Ethernet 1/7 및 Ethernet 1/8에서는 PoE+(Power over Ethernet+)를 지원합니다.

Firepower 1010 스위치 포트에 대한 지침 및 제한 사항

고가용성

- 고가용성 사용 시 스위치 포트 기능을 사용해서는 안 됩니다. 스위치 포트는 하드웨어에서 작동하므로 액티브 및 스탠바이 유닛에서 계속 트래픽을 전달합니다. 고가용성은 트래픽이 스탠바이 유닛을 통과하는 것을 방지하기 위해 고안되었지만 스위치 포트로 확장되지는 않습니다. 일반 고가용성 네트워크 설정에서 두 유닛의 액티브 스위치 포트는 네트워크 루프로 이어집니다. 모든 스위칭 기능에는 외부 스위치를 사용하는 것이 좋습니다. VLAN 인터페이스는 장애 조치를 통해 모니터링될 수 있지만 스위치 포트는 그럴 수 없습니다. 이론적으로는 VLAN에 단일 스위치 포트를 배치하고 고가용성을 정상적으로 사용할 수 있지만, 물리적 방화벽 인터페이스를 대신 사용하면 더 간단하게 설정할 수 있습니다.
- 방화벽 인터페이스만 장애 조치 링크로 사용할 수 있습니다.

논리적 **VLAN** 인터페이스

- 최대 60개의 VLAN 인터페이스를 생성할 수 있습니다.
- 방화벽 인터페이스에서 VLAN 하위 인터페이스도 사용하는 경우에는 논리적 VLAN 인터페이스에 동일한 VLAN ID를 사용할 수 없습니다.
- MAC 주소:
  - 모든 VLAN 인터페이스에서는 MAC 주소를 공유합니다. 연결된 스위치가 이 시나리오에 도움이 될 수 있을지 확인하십시오. 연결된 스위치에 고유한 MAC 주소가 필요한 경우, MAC 주소를 수동으로 할당할 수 있습니다. 고급 옵션 구성, 49 페이지의 내용을 참조하십시오.

브리지 그룹

동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수는 없습니다.

VLAN 인터페이스 및 스위치 포트에서 지원되지 않는 기능

VLAN 인터페이스 및 스위치 포트에서는 다음을 지원하지 않습니다.

- 동적 라우팅
- 멀티캐스트 라우팅
- ECMP(Equal-Cost Multi-Path) 라우팅
- 패시브 인터페이스
- EtherChannel

- 장애 조치 및 상태 링크

기타 지침 및 제한 사항

- Firepower 1010에서 명명된 인터페이스를 최대 60개 구성할 수 있습니다.
- 관리 인터페이스는 스위치 포트로 구성할 수 없습니다.

기본 설정

- Ethernet 1/1은 방화벽 인터페이스입니다.
- Ethernet 1/2~Ethernet 1/8은 VLAN 1에 할당된 스위치 포트입니다.
- 기본 속도 및 듀플렉스 - 기본적으로 속도 및 듀플렉스는 자동 협상으로 설정됩니다.

VLAN 인터페이스 구성

이 섹션에서는 연결된 스위치 포트에 사용할 VLAN 인터페이스를 구성하는 방법에 대해 설명합니다. 먼저 스위치 포트에 할당할 각 VLAN에 대해 VLAN 인터페이스를 구성해야 합니다.

참고 특정 VLAN의 스위치 포트 간에만 스위칭을 활성화하고 VLAN과 기타 VLAN 또는 방화벽 인터페이스 간에는 라우팅하지 않으려는 경우에는 VLAN 인터페이스 이름을 비워 둡니다. 이 경우에도 IP 주소를 구성할 필요가 없습니다. 즉, 모든 IP 구성은 무시됩니다.

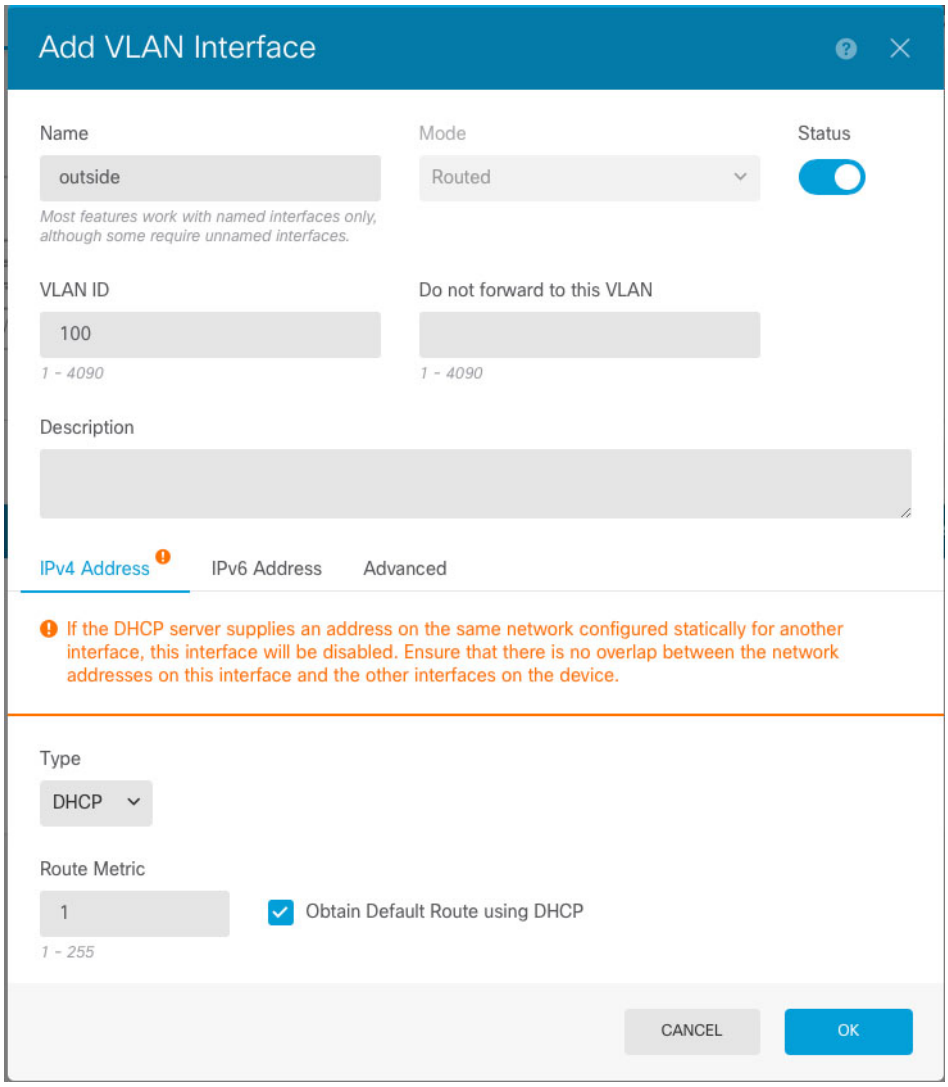
프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **VLAN**을 클릭합니다.

VLAN 목록에는 기존 VLAN 인터페이스가 표시됩니다. 각 VLAN과 연결된 스위치 포트를 보려면 열기/닫기 화살표를 클릭합니다. 스위치 포트는 **Interfaces(**인터페이스**)** 페이지에 개별적으로도 표시됩니다.

단계 **2** **Create VLAN Interface(VLAN** 인터페이스 생성**)** (현재 VLAN이 없는 경우) 또는 더하기 아이콘(+)을 클릭하여 새 VLAN 인터페이스를 생성합니다.

단계 **3** 다음을 구성합니다.



a) **Interface Name(**인터페이스 이름**)**을 설정합니다.

VLAN의 이름을 최대 48자로 설정합니다. 영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다.

VLAN과 기타 VLAN 또는 방화벽 인터페이스 간에 라우팅하지 않으려는 경우에는 VLAN 인터페이스 이름을 비워 둡니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

b) 이 **Mode(**모드**)**를 **Routed(**라우팅**)**인 상태로 둡니다.

나중에 이 VLAN 인터페이스를 브리지 그룹에 추가하면 모드가 자동으로 **BridgeGroupMember**로 변경됩니다. 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정()으로 지정합니다.

d) 1~4070의 **VLAN ID**를 설정합니다.

인터페이스를 저장한 후에는 VLAN ID를 변경할 수 없습니다. VLAN ID는 사용된 VLAN 태그이자 구성의 인터페이스 ID입니다.

e) (선택 사항) **Do not forward to this VLAN(**이 **VLAN**으로 전달하지 않음**)** 필드에 이 VLAN 인터페이스에서 트래픽을 시작할 수 없는 VLAN ID를 입력합니다.

예를 들어, 인터넷 액세스를 위해 외부에 VLAN 1개를, 내부 비즈니스용 네트워크에 또 다른 VLAN 1개를 그리고 홈 네트워크에 3번째 VLAN을 할당합니다. 홈 네트워크에서는 비즈니스 네트워크에 액세스할 필요가 없으므로 홈 VLAN에서 Block Traffic From this Interface to(이 인터페이스에서 다음 위치로 가는 트래픽 차단) 옵션을 사용할 수 있습니다. 비즈니스 네트워크에서는 홈 네트워크에 액세스할 수 있지만 홈 네트워크에서는 비즈니스 네트워크에 액세스할 수 없습니다.

f) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **4** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- **DHCP** — 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(**경로 메트릭**)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(**기본 경로 얻기**)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).

- **Static(**고정**)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

  참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정의 내용을 참조하십시오.

- **PPPoE** — PPPoE(Point-to-Point Protocol over Ethernet)를 사용하여 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 다음 값을 설정합니다.

- **Group Name(**그룹 이름**)** — 이 연결을 나타내는 그룹 이름을 원하는 대로 지정합니다.
- **PPPoE Username(PPPoE** 사용자 이름**)** — ISP에서 제공한 사용자 이름을 지정합니다.
- **PPPoE Password(PPPoE** 비밀번호**)** — ISP에서 제공한 비밀번호를 지정합니다.
- **PPP Authentication(PPP** 인증**) - PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

  PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
- **PPPoE Learned Route Metric(PPPoE** 학습된 경로 메트릭**)** — 학습된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
- **Obtain Default Route from PPPoE(PPPoE**에서 기본 경로 가져오기**)** — PPPoE 서버에서 기본 경로를 가져오려면 이 확인란을 선택합니다.
- **IP Address Type(IP** 주소 유형**)** — PPPoE 서버에서 IP 주소를 가져오려면 **Dynamic(**동적**)**을 선택합니다. 또는 ISP에서 정적 IP 주소를 할당한 경우 **Static(**정적**)**을 선택할 수 있습니다.

단계 **5** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**) -** 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(**주소 자동 컨피그레이션**) -** 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

  RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Static Address/Prefix(**고정 주소/접두사**) -** 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 4 페이지를 참조하십시오.

주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. threat defense는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **6** (선택 사항). 고급 옵션 구성, 49 페이지에 전달하는 고성능 고속 어플라이언스입니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **7** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 보안 영역에 VLAN을 추가합니다. 보안 영역 구성의 내용을 참조하십시오.

스위치 포트를 액세스 포트로 구성

단일 VLAN에 스위치 포트를 할당하려면 해당 포트를 액세스 포트로 구성합니다. 기본적으로, Ethernet 1/2~Ethernet 1/8 스위치 포트는 활성화되며 VLAN 1에 할당됩니다.

참고 Firepower 1010에서는 네트워크에서의 루프 탐지를 위해 Spanning Tree Protocol을 지원하지 않습니다. 따라서 threat defense와의 연결이 네트워크 루프에서 종료되지 않도록 해야 합니다.

시작하기 전에

액세스 포트를 할당할 VLAN ID에 대한 VLAN 인터페이스를 추가합니다. 액세스 포트에서는 태그 없는 트래픽만 허용됩니다. VLAN 인터페이스 구성, 28 페이지의 내용을 참조하십시오.

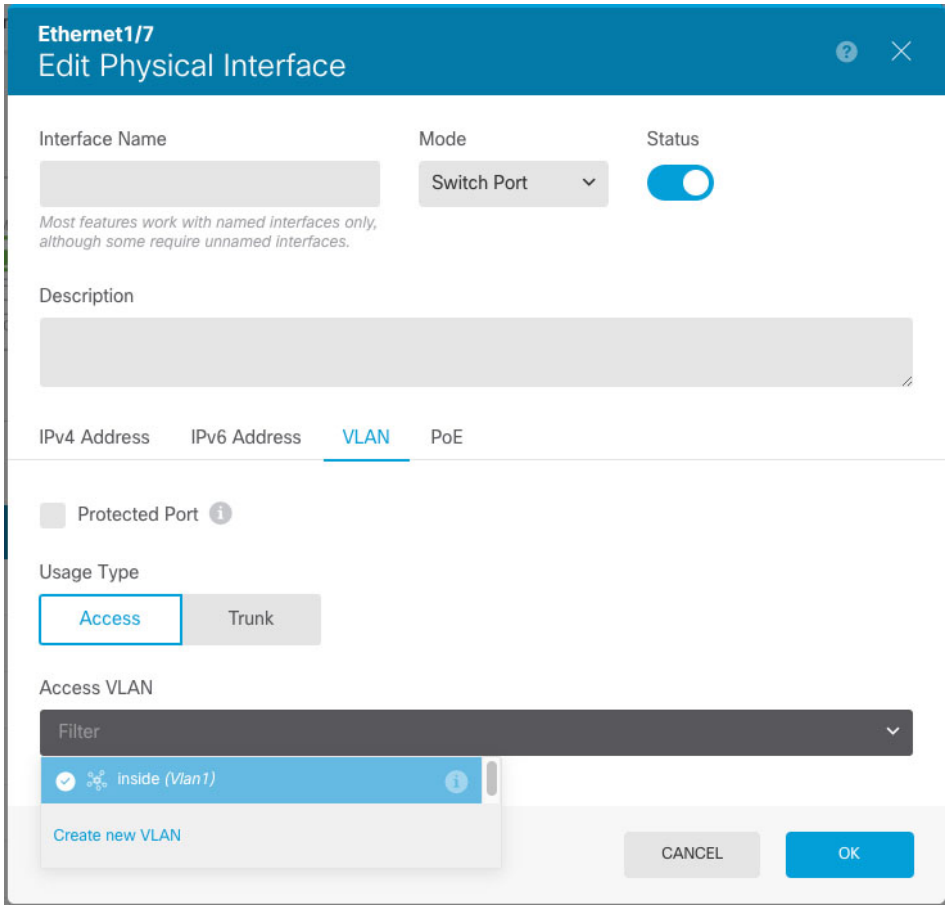
프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 수정할 실제 인터페이스의 수정 아이콘( )을 클릭합니다.

단계 **3** 다음을 설정합니다.



a) 스위치 포트에 대한 **Interface Name(**인터페이스 이름**)**은 설정하지 마십시오. 연결된 VLAN 인터페이스만 명명된 인터페이스입니다.

b) **Mode(**모드**)**를 **Switch Port(**스위치 포트**)**로 설정합니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정( )으로 지정합니다.

d) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **4** **VLAN**을 클릭하여 다음을 설정합니다.

a) (선택 사항) **Protected Port(**보호된 포트**)** 확인란을 선택하여 이 스위치 포트를 보호된 상태로 설정합니다. 그러면 스위치 포트가 동일한 VLAN에서 보호되는 다른 스위치 포트와 통신하는 것을 방지할 수 있습니다.

스위치 포트의 디바이스가 주로 다른 VLAN에서 액세스되어 VLAN 간 액세스를 허용할 필요가 없으며 감염 또는 기타 보안 침입 시 디바이스를 서로 분리하려는 경우 스위치 포트가 서로 통신하지 못하도록 할 수 있습니다. 예를 들어 세 개의 웹 서버를 호스팅하는 DMZ가 있는 경우, 이 옵션을 각 스위치 포트에 적용하면 웹 서버를 서로 분리할 수 있습니다. 내부 및 외부 네트워크 둘 다 세 개의 웹 서버와 통신할 수 있지만 웹 서버 간에 서로 통신할 수는 없습니다.

b) **Usage Type(**사용 유형**)**에서 **Access(**액세스**)**를 클릭합니다.

c) **Access VLAN(**액세스 **VLAN)**의 경우, 아래쪽 화살표를 클릭하여 기존의 VLAN 인터페이스 중 하나를 선택합니다.

Create new VLAN(새 **VLAN** 생성**)**을 클릭하여 새 VLAN 인터페이스를 추가할 수 있습니다. VLAN 인터페이스 구성, 28 페이지의 내용을 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭합니다.

스위치 포트를 트렁크 포트로 구성

이 절차에서는 802.1Q 태깅을 사용하여 여러 VLAN을 전송할 수 있는 트렁크 포트를 생성하는 방법에 대해 설명합니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용됩니다. 허용된 VLAN의 트래픽에서는 트렁크 포트가 변경되지 않은 상태로 전달됩니다.

트렁크에서는 태그 없는 트래픽을 수신하는 경우 ASA에서 해당 트래픽을 올바른 스위치 포트로 전달하거나 다른 방화벽 인터페이스로 라우팅할 수 있도록 해당 트래픽을 네이티브 VLAN ID에 대해 태그 지정합니다. ASA에서는 트렁크 포트 외부로 네이티브 VLAN ID 트래픽을 전송하는 경우 VLAN 태그를 제거합니다. 태그 없는 트래픽이 동일한 VLAN에 대해 태그 지정될 수 있도록 다른 스위치의 트렁크 포트에서 동일한 네이티브 VLAN을 설정해야 합니다.

시작하기 전에

트렁크 포트를 할당할 각 VLAN ID에 대한 VLAN 인터페이스를 추가합니다. VLAN 인터페이스 구성, 28 페이지의 내용을 참조하십시오.

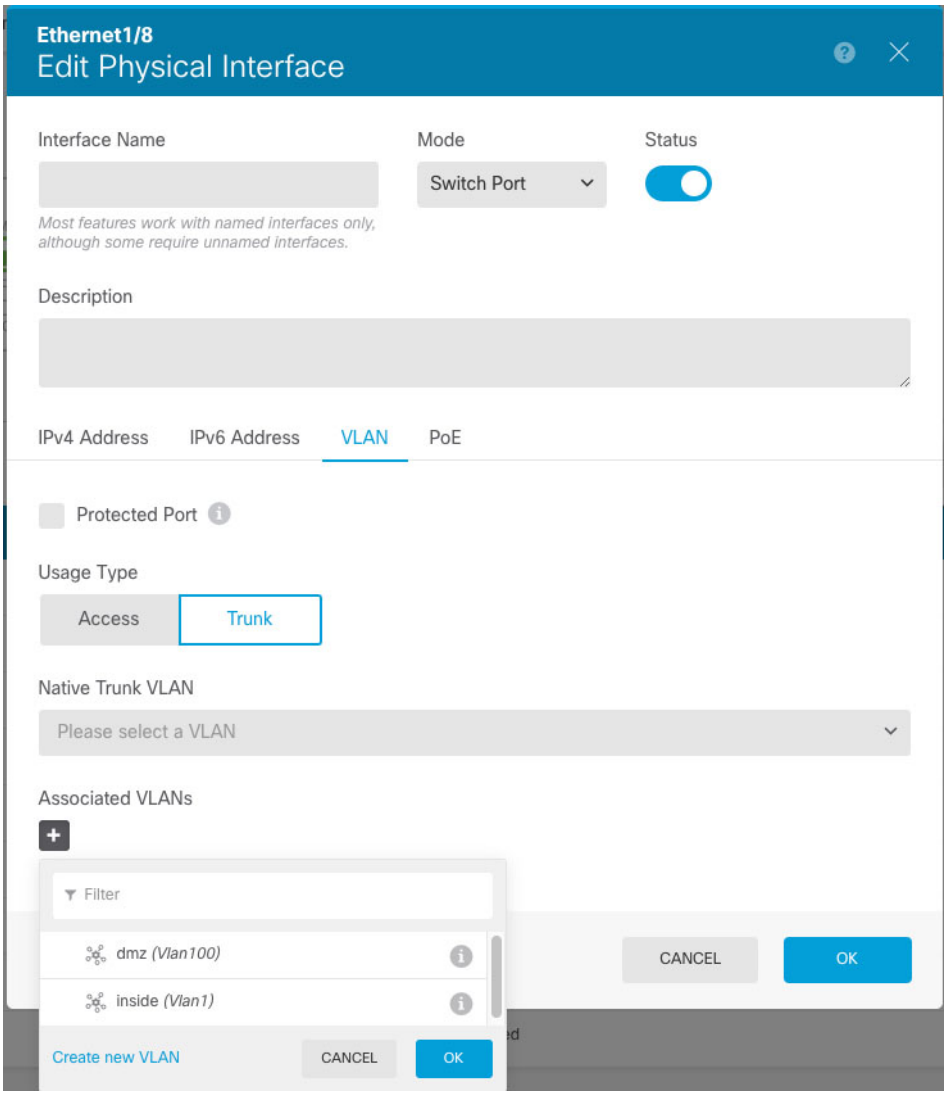
프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 수정할 실제 인터페이스의 수정 아이콘( )을 클릭합니다.

단계 **3** 다음을 설정합니다.



a) 스위치 포트에 대한 **Interface Name(**인터페이스 이름**)**은 설정하지 마십시오. 연결된 VLAN 인터페이스만 명명된 인터페이스입니다.

b) **Mode(**모드**)**를 **Switch Port(**스위치 포트**)**로 설정합니다.

c) **Status(**상태**)** 슬라이더를 활성화된 설정( )으로 지정합니다.

d) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **4** **VLAN**을 클릭하여 다음을 설정합니다.

a) (선택 사항) **Protected Port(**보호된 포트**)** 확인란을 선택하여 이 스위치 포트를 보호된 상태로 설정합니다. 그러면 스위치 포트가 동일한 VLAN에서 보호되는 다른 스위치 포트와 통신하는 것을 방지할 수 있습니다.

스위치 포트의 디바이스가 주로 다른 VLAN에서 액세스되어 VLAN 간 액세스를 허용할 필요가 없으며 감염 또는 기타 보안 침입 시 디바이스를 서로 분리하려는 경우 스위치 포트가 서로 통신하지 못하도록 할 수 있습니다. 예를 들어 세 개의 웹 서버를 호스팅하는 DMZ가 있는 경우, 이 옵션을 각 스위치 포트에 적용하면 웹 서버를 서로 분리할 수 있습니다. 내부 및 외부 네트워크 둘 다 세 개의 웹 서버와 통신할 수 있지만 웹 서버 간에 서로 통신할 수는 없습니다.

b) **Usage Type(**사용 유형**)**에서 **Trunk(**트렁크**)**를 클릭합니다.

c) (선택 사항) **Native Trunk VLAN(**기본 트렁크 **VLAN)**의 경우, 아래쪽 화살표를 클릭하여 네이티브 VLAN에 대해 기존의 VLAN 인터페이스 중 하나를 선택합니다.

기본 네이티브 VLAN ID는 1입니다.

각 포트에는 하나의 네이티브 VLAN만 있을 수 있지만, 모든 포트의 네이티브 VLAN은 같거나 다를 수 있습니다.

Create new VLAN(새 **VLAN** 생성**)**을 클릭하여 새 VLAN 인터페이스를 추가할 수 있습니다. VLAN 인터페이스 구성, 28 페이지의 내용을 참조하십시오.

d) **Associated VLAN(**연결된 **VLAN)**의 경우, 더하기 아이콘(+)을 클릭하여 기존의 VLAN 인터페이스를 하나 이상 선택합니다.

이 필드에 네이티브 VLAN을 포함하는 경우 해당 VLAN은 무시됩니다. 트렁크 포트에서는 포트 외부로 네이티브 VLAN 트래픽을 전송할 때 항상 VLAN 태깅을 제거합니다. 뿐만 아니라, 이렇게 한 후에도 네이티브 VLAN 태깅이 있는 트래픽은 수신하지 않습니다.

Create new VLAN(새 **VLAN** 생성**)**을 클릭하여 새 VLAN 인터페이스를 추가할 수 있습니다. VLAN 인터페이스 구성, 28 페이지의 내용을 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭합니다.

PoE(Power over Ethernet) 구성

Ethernet1/7 및 Ethernet1/8에서는 IP 전화기 또는 무선 액세스 포인트와 같은 디바이스에 대해 PoE(Power over Ethernet)를 지원합니다. Firepower 1010에서는 IEEE 802.3af(PoE) 및 802.3at(PoE+)을 모두 지원합니다. PoE+에서는 LLDP(Link Layer Discovery Protocol)를 사용하여 전력 레벨을 협상합니다. PoE+에서는 전력 디바이스에 최대 30와트를 제공할 수 있습니다. 전원은 필요한 경우에만 제공됩니다.

인터페이스를 종료한 경우 디바이스의 전원을 비활성화합니다.

PoE는 Ethernet1/7 및 Ethernet1/8에서 기본적으로 활성화되어 있습니다. 이 절차에서는 PoE를 비활성화하는 방법과 활성화하는 방법, 파라미터(선택 사항)를 설정하는 방법을 설명합니다.

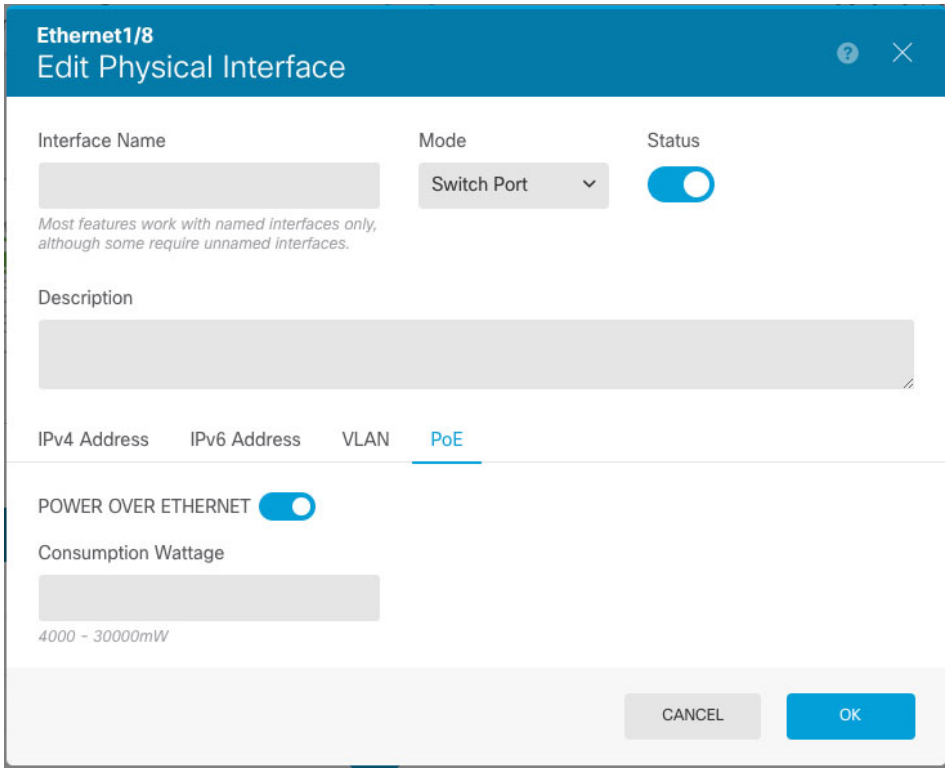
프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** Ethernet1/7 또는 1/8에 대해 수정 아이콘( )을 클릭합니다.

단계 **3** **PoE**를 클릭하고 다음을 설정합니다.



a) **PoE(Power over Ethernet)**를 활성화하려면 슬라이더( )를 클릭하여 활성화합니다.

PoE는 기본적으로 활성화되어 있습니다.

b) (선택 사항) 필요한 전력량을 정확히 알고 있는 경우 **Consumption Wattage(**소비 전력량**)**를 입력합니다.

기본적으로 PoE에서는 전력 디바이스의 클래스에 적절한 전력량을 사용하여 전력 디바이스에 전원을 자동으로 제공합니다. Firepower 1010에서는 LLDP를 사용하여 정확한 전력량을 추가로 협상합니다. 특정 전력량을 알고 있으며 LLDP 협상을 비활성화하려는 경우 4,000~30,000 밀리와트의 값을 입력합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성

VLAN 하위 인터페이스를 사용하면 실제 인터페이스를 각기 다른 VLAN ID로 태그가 지정된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 정해진 실제 인터페이스에서 트래픽

을 따로 유지할 수 있으므로, 실제 인터페이스 또는 디바이스를 더 추가하지 않고 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

스위치의 트렁크 포트에 물리적 인터페이스를 연결하는 경우 하위 인터페이스를 생성합니다. 스위치 트렁크 포트에 표시될 수 있는 각 VLAN에 대해 하위 인터페이스를 생성합니다. 스위치의 액세스 포트에 물리적 인터페이스를 연결하는 경우 하위 인터페이스를 생성할 필요가 없습니다.

지침 및 제한 사항

- 물리적 인터페이스의 태그 지정되지 않은 패킷 방지 — 하위 인터페이스를 사용할 경우, 일반적으로 물리적 인터페이스에서 트래픽을 전달하지 않도록 하고자 합니다. 물리적 인터페이스에서는 태그 지정되지 않은 패킷을 전달하기 때문입니다. 하위 인터페이스에서 트래픽을 전달하려면 실제 인터페이스를 활성화해야 하므로, 인터페이스의 이름을 지정하지 않는 방법을 통해 실제 인터페이스가 트래픽을 전달하지 않도록 해야 합니다. 실제 인터페이스에서 태그가 지정되지 않은 패킷을 전달할 수 있도록 하려면 일반적인 방식으로 인터페이스 이름을 지정하면 됩니다.
- Firepower 1010 - 하위 인터페이스는 스위치 포트 또는 VLAN 인터페이스에서 지원되지 않습니다.
- 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다. 그러나 필요에 따라 고급 설정을 수정할 수는 있습니다.
- 동일한 상위 인터페이스에 있는 모든 하위 인터페이스는 브리지 그룹 멤버 또는 라우팅 인터페이스 중 하나여야 하며 이를 혼합하고 일치시킬 수 없습니다.
- Threat Defense에서는 DTP(Dynamic Trunking Protocol)를 지원하지 않으므로 조건 없이 트렁킹을 수행할 연결된 스위치 포트를 구성해야 합니다.
- threat defense 디바이스에 정의된 하위 인터페이스에서 상위 인터페이스의 번인된(burned-in) MAC 주소와 동일한 주소를 사용하므로 이 하위 인터페이스에 고유한 MAC 주소를 할당해야 할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 threat defense 디바이스의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. EtherChannel에 하위 인터페이스를 추가하려면 **EtherChannel**을 클릭합니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 다음 중 하나를 수행합니다.

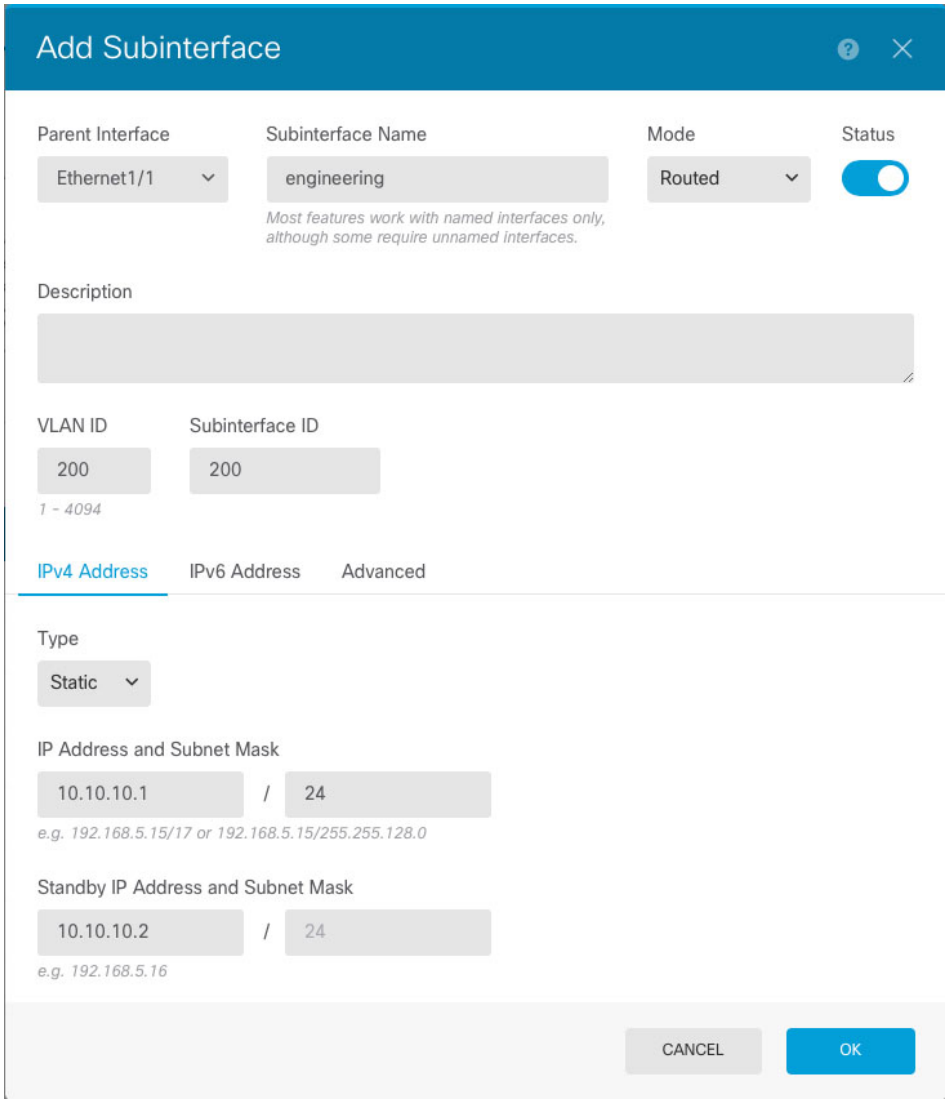
- **Interfaces(**인터페이스**)** 페이지에서 더하기 아이콘(+)을 클릭하여 새 하위 인터페이스를 생성합니다.

- **EtherChannel** 페이지에서 더하기 및 아래쪽 화살표 아이콘(+)을 클릭하고 **Subinterface(**하위 인터페이스**)**를 선택합니다.
- 수정할 하위 인터페이스의 수정 아이콘()을 클릭합니다.

하위 인터페이스가 더 이상 필요하지 않은 경우, 해당 하위 인터페이스의 삭제 아이콘()을 클릭하여 삭제합니다.

단계 **3** **Status(**상태**)** 슬라이더를 활성화된 설정()으로 지정합니다.

단계 **4** 상위 인터페이스, 이름 및 설명을 구성합니다.



a) **Parent Interface(**상위 인터페이스**)**를 선택합니다.

상위 인터페이스는 하위 인터페이스를 추가할 물리적 인터페이스입니다. 하위 인터페이스를 생성한 후에는 상위 인터페이스를 변경할 수 없습니다.

b) **Subinterface Name(**하위 인터페이스 이름**)**이름을 최대 48자로 설정합니다.

영문자는 소문자로 입력해야 합니다. 예를 들면 **inside** 또는 **outside**와 같이 입력합니다. 이름을 입력하지 않으면 나머지 인터페이스 컨피그레이션이 무시됩니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

c) **Mode(**모드**)**를 **Routed(**라우팅**)**로 설정합니다.

나중에 이 인터페이스를 브리지 그룹에 추가하면 모드가 자동으로 **BridgeGroupMember**로 변경됩니다. 브리지 그룹 멤버 인터페이스에서는 IP 주소를 구성할 수 없습니다.

d) (선택 사항) **Description(**설명**)**을 설정합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

e) **VLAN ID**를 설정합니다.

이 하위 인터페이스에서 패킷에 태그를 지정하는 데 사용할 1~4094의 VLAN ID를 입력합니다.

f) **Subinterface ID(**하위 인터페이스 **ID)**를 설정합니다.

하위 인터페이스 ID를 1~4294967295의 정수로 입력합니다. 이 ID는 인터페이스 ID에 추가됩니다(예: Ethernet1/1.100). 편의를 위해 VLAN ID를 일치시킬 수 있으나 꼭 그렇게 해야 하는 것은 아닙니다. 하위 인터페이스를 생성한 후에는 ID를 변경할 수 없습니다.

단계 **5** **IPv4 Address(IPv4** 주소**)** 탭을 클릭하고 IPv4 주소를 구성합니다.

Type(유형**)** 필드에서 다음 옵션 중 하나를 선택합니다.

- **DHCP** — 네트워크의 DHCP 서버에서 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 필요에 따라 다음 옵션을 변경합니다.
  - **Route Metric(**경로 메트릭**)** - DHCP 서버에서 기본 경로를 가져오는 경우 확인된 경로까지의 관리 거리(1~255)입니다. 기본값은 1입니다.
  - **Obtain Default Route(**기본 경로 얻기**)** - DHCP 서버에서 기본 경로를 가져올지 여부를 선택합니다. 일반적으로는 이 옵션을 선택합니다(기본값).
- **Static(**고정**)** - 변경되면 안 되는 주소를 할당하려면 이 옵션을 선택합니다. 인터페이스에 연결된 네트워크에 대해 인터페이스의 IP 주소와 서브넷 마스크를 입력합니다. 예를 들어 10.100.10.0/24 네트워크를 연결하는 경우 10.100.10.1/24를 입력할 수 있습니다. 주소가 네트워크에서 이미 사용되고 있지 않은지 확인합니다.

  고가용성을 구성했으며 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IP 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

참고 인터페이스에 대해 구성된 DHCP 서버가 있을 경우, 해당 컨피그레이션이 표시됩니다. DHCP 주소 풀을 수정하거나 삭제할 수 있습니다. 인터페이스 IP 주소를 다른 서브넷으로 변경할 경우, 인터페이스 변경 사항을 저장하려면 우선 DHCP 서버를 삭제하거나, 새 서브넷에서 주소 풀을 구성해야 합니다. DHCP 서버 설정의 내용을 참조하십시오.

- **PPPoE** — PPPoE(Point-to-Point Protocol over Ethernet)를 사용하여 주소를 가져와야 하는 경우 이 옵션을 선택합니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 고가용성을 구성하는 경우 이 옵션을 사용할 수 없습니다. 다음 값을 설정합니다.
  - **Group Name(**그룹 이름**)** — 이 연결을 나타내는 그룹 이름을 원하는 대로 지정합니다.
  - **PPPoE Username(PPPoE** 사용자 이름**)** — ISP에서 제공한 사용자 이름을 지정합니다.
  - **PPPoE Password(PPPoE** 비밀번호**)** — ISP에서 제공한 비밀번호를 지정합니다.
  - **PPP Authentication(PPP** 인증**) - PAP**, **CHAP**, 또는**MSCHAP**를 선택합니다.

    PAP에서는 인증이 진행되는 동안 일반 텍스트 사용자 이름 및 비밀번호를 전달하므로 안전하지 않습니다. CHAP를 사용하면 클라이언트에서는 서버 챌린지에 대한 응답으로 암호화된 [challenge plus password]와 함께 일반 텍스트로 된 사용자 이름을 반환합니다. CHAP는 PAP보다 안전하지만 데이터가 암호화되지 않습니다. MSCHAP는 CHAP와 유사하지만, CHAP의 일반 텍스트로 비밀번호와 달리 서버에서 암호화된 비밀번호만 저장하고 비교하므로 훨씬 안전합니다. MSCHAP에서도 MPPE를 통해 데이터 암호화용 키를 생성합니다.
  - **PPPoE Learned Route Metric(PPPoE** 학습된 경로 메트릭**)** — 학습된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
  - **Obtain Default Route from PPPoE(PPPoE**에서 기본 경로 가져오기**)** — PPPoE 서버에서 기본 경로를 가져오려면 이 확인란을 선택합니다.
  - **IP Address Type(IP** 주소 유형**)** — PPPoE 서버에서 IP 주소를 가져오려면 **Dynamic(**동적**)**을 선택합니다. 또는 ISP에서 정적 IP 주소를 할당한 경우 **Static(**정적**)**을 선택할 수 있습니다.

단계 **6** (선택 사항). **IPv6 Address(IPv6** 주소**)** 탭을 클릭하고 IPv6 주소를 구성합니다.

- **Sate(**상태**) -** 글로벌 어드레스를 구성하지 않는 경우 IPv6 처리를 활성화하고 링크-로컬 주소를 자동으로 구성하려면 **Enabled(**활성화됨**)**를 선택합니다. 링크 로컬 주소는 인터페이스 MAC 주소(수정된 EUI-64 형식)를 기반으로 생성됩니다.

  참고 IPv6를 비활성화해도 명시적 IPv6 주소로 구성되었거나 자동 컨피그레이션용으로 활성화된 인터페이스에서 IPv6 처리가 비활성화되지는 않습니다.

- **Address Auto Configuration(**주소 자동 컨피그레이션**) -** 주소를 자동으로 구성하려면 이 옵션을 선택합니다. IPv6 스테이트리스 자동 컨피그레이션에서는 디바이스가 있는 링크에 IPv6 서비스를 제공하도록 구성된 라우터가 있는 경우에만 글로벌 IPv6 주소를 생성합니다. 이러한 서비스에는 링크에서 사용할 IPv6 글로벌 접두사 알림이 포함됩니다. 링크에서 IPv6 라우팅 서비스를 사용할 수 없는 경우에는 링크-로컬 IPv6 주소만 제공됩니다. 디바이스의 직접 네트워크 링크 외

부에서는 이 주소에 액세스할 수 없습니다. 링크 로컬 주소는 수정된 EUI-64 인터페이스 ID를 기반으로 합니다.

RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지를 표시하지 않고 RFC를 준수하려면 **RA** 표시 안 함을 선택합니다.

- **Static Address/Prefix(**고정 주소/접두사**)** - 스테이트리스 자동 컨피그레이션을 사용하지 않는 경우 전체 고정 글로벌 IPv6 주소와 네트워크 접두사를 입력합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48와 같이 입력합니다. IPv6 주소 지정에 대한 자세한 내용은 IPv6 주소 지정, 4 페이지를 참조하십시오.

  주소를 링크 로컬 전용으로 사용하려는 경우 링크-로컬 옵션을 선택합니다. 로컬 네트워크 외부에서는 링크 로컬 주소에 액세스할 수 없습니다. 브리지 그룹 인터페이스에서는 링크-로컬 주소를 구성할 수 없습니다.

  참고 링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). Modified EUI-64 형식으로 링크-로컬 주소를 자동으로 지정하는 것이 좋습니다. 만약 다른 디바이스에서 Modified EUI-64 형식을 강제 적용하는 경우 수동으로 지정된 링크-로컬 주소 때문에 패킷이 폐기될 수 있습니다.

- **Standby IP Address(**스탠바이 **IP** 주소**)** - 고가용성을 구성하는 경우 이 인터페이스에서 HA를 모니터링하는 중이라면 같은 서브넷에 스탠바이 IPv6 주소도 구성합니다. 스탠바이 디바이스의 이 인터페이스에서 스탠바이 주소를 사용합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

- **Suppress RA(RA** 표시 안 함**)** - 라우터 알림을 표시하지 않을지를 선택합니다. threat defense는 인접 디바이스가 기본 라우터 주소를 동적으로 학습할 수 있도록 라우터 알림에 참여할 수 있습니다. 기본적으로 라우터 알림 메시지(ICMPv6 유형 134)는 IPv6가 구성된 각 인터페이스에 주기적으로 전송됩니다.

  라우터 광고는 라우터 요청 메시지에 대한 응답으로도 보내집니다(ICMPv6 Type 133). 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

  threat defense 디바이스에서 IPv6 접두사를 제공하지 않도록 하려는 인터페이스(예: 외부 인터페이스)에서는 이러한 메시지를 표시하지 않을 수 있습니다.

단계 **7** (선택 사항). 고급 옵션 구성, 49 페이지에 전달하는 고성능 고속 어플라이언스입니다.

고급 설정에는 대부분의 네트워크에 적합한 기본값이 있습니다. 네트워크 문제를 해결하는 경우에만 이러한 기본값을 수정하십시오.

단계 **8** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

- 적절한 보안 영역에 하위 인터페이스를 추가합니다. 보안 영역 구성의 내용을 참조하십시오.

- 동적 DNS 서비스 제공자에 FQDN(Fully Qualified Domain Name)을 등록하고 DNS 서버가 IPv4 및 IPv6 인터페이스 주소로 업데이트되도록 DDNS를 설정합니다. 동적 DNS 구성의 내용을 참조하십시오.

패시브 인터페이스 구성

패시브 인터페이스는 스위치 SPAN(Switched Port Analyzer) 또는 미러 포트를 사용하여 네트워크를 통과하는 트래픽을 모니터링합니다. SPAN 또는 미러 포트를 사용하면 스위치의 다른 포트에서 트래픽을 복사할 수 있습니다. 이 기능을 사용하면 네트워크 트래픽의 플로우 내에 있지 않더라도 시스템 가시성이 확보됩니다.

패시브 구축으로 구성된 시스템은 트래픽 차단 등의 특정 작업을 수행할 수 없습니다. 패시브 인터페이스는 모든 트래픽을 조건 없이 수신하며 이러한 인터페이스에서 수신된 트래픽은 재전송되지 않습니다.

패시브 인터페이스를 사용하여 네트워크의 트래픽을 모니터링해 트래픽에 대한 정보를 수집합니다. 예를 들어 침입 정책을 적용해 네트워크에 피해를 주는 위협 유형을 파악하거나 사용자가 보내는 웹 요청의 URL 카테고리를 확인할 수 있습니다. 다양한 보안 정책과 규칙을 구현하여 시스템이 능동적으로 구축될 때 어떤 작업을 수행할지 확인할 수 있습니다. 그러면 시스템이 액세스 제어 규칙과 기타 규칙에 따라 트래픽을 삭제할 수 있습니다.

그러나 패시브 인터페이스는 트래픽에 영향을 줄 수 없으므로 여러 가지 컨피그레이션 제한이 적용됩니다. 이러한 인터페이스를 사용하는 시스템은 트래픽을 확인할 수만 있으며, 패시브 인터페이스로 들어가는 패킷은 디바이스에서 나가지 않습니다.

다음 주제에서는 패시브 인터페이스 및 패시브 인터페이스 구성 방법을 더 자세히 설명합니다.

패시브 인터페이스를 사용하는 이유

패시브 인터페이스를 사용하는 주요 목적은 단순 데모 모드를 제공하기 위해서입니다. 단일 소스 포트를 모니터링하도록 스위치를 설정한 다음 워크스테이션을 사용하여 패시브 인터페이스가 모니터링하는 테스트 트래픽을 전송할 수 있습니다. 그러므로 threat defense 시스템에서 어떻게 연결을 평가하고 위협을 식별하는지 등을 확인할 수 있습니다. 시스템의 작업 수행 방식에 만족하는 경우 네트워크에서 해당 컨피그레이션을 능동적으로 구축하고 패시브 인터페이스 컨피그레이션은 제거할 수 있습니다.

하지만 다음 서비스를 제공 하기 위해 프로덕션 환경에서 패시브 인터페이스를 사용할 수도 있습니다.

- 순수 IDS 구축 - 시스템을 방화벽이나 IPS(Intrusion Detection System)로 사용하지 않으려는 경우 패시브 방식을 통해 IDS(Intrusion Detection System)로 구축할 수 있습니다. 이 구축 방법에서는 액세스 제어 규칙을 사용하여 모든 트래픽에 침입 정책을 적용합니다. 시스템이 스위치의 여러 소스 포트를 모니터링하도록 지정할 수도 있습니다. 그리고 나면 대시보드를 사용하여 네트워크에서 확인되는 위협을 모니터링할 수 있습니다. 그러나 이 모드에서는 이러한 위협을 방지하기 위해 시스템이 어떤 작업도 수행할 수 없습니다.

- 혼합 구축 - 액티브 라우팅 인터페이스와 패시브 인터페이스를 같은 시스템에서 함께 사용할 수 있습니다. 즉 일부 네트워크에서는 threat defense 디바이스를 방화벽으로 구축하고 다른 네트워크에서는 트래픽을 모니터링하도록 하나 이상의 수동 인터페이스를 컨피그레이션할 수 있습니다.

패시브 인터페이스에 대한 제한 사항

패시브 모드 인터페이스로 정의하는 모든 물리적 인터페이스에는 다음 제한이 적용됩니다.

- 패시브 인터페이스에서는 하위 인터페이스를 구성할 수 없습니다.
- 브리지 그룹에는 패시브 인터페이스를 포함할 수 없습니다.
- 패시브 인터페이스에서는 IPv4 또는 IPv6 주소를 구성할 수 없습니다.
- 패시브 인터페이스에서는 Management Only(관리 전용) 옵션을 선택할 수 없습니다.
- 패시브 인터페이스는 패시브 모드 보안 영역에만 포함할 수 있으며 라우팅 보안 영역에는 포함할 수 없습니다.
- 액세스 제어 또는 ID 규칙의 소스 기준에 패시브 보안 영역을 포함할 수 있습니다. 대상 기준에는 패시브 영역을 사용할 수 없습니다. 동일한 규칙에서 패시브 영역과 라우팅 영역을 함께 사용할 수 없습니다.
- 패시브 인터페이스에서는 관리 액세스 규칙(HTTPS 또는 SSH)을 구성할 수 없습니다.
- NAT 규칙에 패시브 인터페이스를 사용할 수 없습니다.
- 패시브 인터페이스에서는 정적 경로를 구성할 수 없습니다. 라우팅 프로토콜 컨피그레이션에서는 패시브 인터페이스를 사용할 수 없습니다.
- 패시브 인터페이스에서는 DHCP 서버를 구성할 수 없습니다. 패시브 인터페이스를 사용하여 자동 컨피그레이션을 통해 DHCP 설정을 획득할 수 없습니다.
- syslog 서버 컨피그레이션에 패시브 인터페이스를 사용할 수 없습니다.
- 패시브 인터페이스에서는 어떤 유형의 VPN도 구성할 수 없습니다.

하드웨어 **Threat Defense** 패시브 인터페이스용 스위치 구성

하드웨어 threat defense 디바이스의 수동 인터페이스는 네트워크 스위치를 정확하게 컨피그레이션해야만 작동합니다. 다음 절차는 Cisco Nexus 5000 Series 스위치를 기준으로 합니다. 다른 유형의 스위치를 사용하는 경우에는 명령이 달라질 수 있습니다.

기본적으로는 SPAN(Switched Port Analyzer) 또는 미러 포트를 구성하고, 해당 포트에 패시브 인터페이스를 연결하고, 하나 이상의 소스 포트에서 SPAN 또는 미러 포트로 트래픽 복사본을 전송하도록 스위치에서 모니터링 세션을 구성합니다.

프로시저

단계 **1** 스위치의 포트를 모니터(SPAN 또는 미러) 포트로 구성합니다.

```
switch(config)# interface Ethernet1/48
switch(config-if)# switchport monitor
switch(config-if)#
```

단계 **2** 모니터링할 포트를 식별하는 모니터링 세션을 정의합니다.

SPAN 또는 미러 포트를 대상 포트로 정의해야 합니다. 다음 예시에서는 소스 포트 2개를 모니터링합니다.

```
switch(config)# monitor session 1
switch(config-monitor)# source interface ethernet 1/7
switch(config-monitor)# source interface ethernet 1/8
switch(config-monitor)# destination interface ethernet 1/48
switch(config-monitor)# no shut
```

단계 **3** (선택 사항). **show monitor session** 명령을 사용하여 컨피그레이션을 확인합니다.

다음 예시에서는 세션 1의 간략한 출력이 나와 있습니다.

```
switch# show monitor session 1 brief
   session 1
---------------
type              : local
state             : up
source intf       :
    rx            : Eth1/7        Eth1/8
    tx            : Eth1/7        Eth1/8
    both          : Eth1/7        Eth1/8
source VSANs      :
destination ports : Eth1/48

Legend: f = forwarding enabled, l = learning enabled
```

단계 **4** threat defense 수동 인터페이스에서 스위치의 목적지 포트에 케이블을 물리적으로 연결합니다.

물리적 연결 전이나 후에 인터페이스를 패시브 모드로 구성할 수 있습니다. 패시브 모드로 물리적 인터페이스 구성, 46 페이지의 내용을 참조하십시오.

Threat Defense Virtual 패시브 인터페이스의 VLAN 구성

threat defense virtual 디바이스의 수동 인터페이스는 가상 네트워크의 VLAN을 정확하게 컨피그레이션해야만 작동합니다. 이를 위해 다음 작업을 수행해야 합니다.

- 무차별 모드에서 컨피그레이션한 VLAN에 threat defense virtual 인터페이스를 연결합니다. 그런 다음 패시브 모드로 물리적 인터페이스 구성, 46 페이지에서 설명한 대로 인터페이스를 구성합니다. 패시브 인터페이스에는 프로미스큐어스 VLAN의 모든 트래픽 복사본이 표시됩니다.
- 동일한 VLAN에 가상 Windows 시스템 등의 엔드포인트 디바이스를 하나 이상 연결합니다. VLAN에서 인터넷으로의 연결이 있는 경우 단일 디바이스를 사용할 수 있습니다. 그렇지 않은 경우에는 트래픽을 전달할 수 있는 둘 이상의 디바이스가 필요합니다. URL 카테고리에 대한 데이터를 가져오려면 인터넷 연결이 필요합니다.

패시브 모드로 물리적 인터페이스 구성

인터페이스를 패시브 모드로 구성할 수 있습니다. 인터페이스는 패시브 방식으로 작동할 때 스위치 자체(하드웨어 디바이스의 경우) 또는 프로미스큐어스 VLAN(threat defense virtual의 경우)에 구성된 모니터링 세션에서 소스 포트의 트래픽만 모니터링합니다. 스위치 또는 가상 네트워크에서 구성해야 하는 항목에 대한 세부 정보는 다음 주제를 참조하십시오.

- 하드웨어 Threat Defense 패시브 인터페이스용 스위치 구성, 44 페이지
- Threat Defense Virtual 패시브 인터페이스의 VLAN 구성, 45 페이지

트래픽에 영향을 주지 않고 모니터링되는 스위치 포트를 통해 들어오는 트래픽을 분석하려는 경우 패시브 모드를 사용합니다. 패시브 모드를 사용하는 전체 예시는 네트워크에서 트래픽을 능동적으로 모니터링하는 방법의 내용을 참조하십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, **Interfaces** 또는 **EtherChannel**을 클릭합니다.

단계 **2** 수정할 물리적 인터페이스 또는 EtherChannel의 수정 아이콘( )을 클릭합니다.

현재 사용되지 않는 인터페이스를 선택합니다. 사용 중인 인터페이스를 패시브 인터페이스로 변환하려는 경우 먼저 모든 보안 영역에서 인터페이스를 제거하고 해당 인터페이스를 사용하는 다른 모든 컨피그레이션을 제거해야 합니다.

단계 **3** **Status(**상태**)** 슬라이더를 활성화된 설정( )으로 지정합니다.

단계 **4** 다음을 구성합니다.

- **Interface Name(**인터페이스 이름**)** - 인터페이스의 이름(최대 48자)입니다. 영문자는 소문자로 입력해야 합니다. 예를 들어 monitor를 입력합니다.
- **Mode(**모드**)** - **Passive(**패시브**)**를 선택합니다.
- (선택 사항). **Description(**설명**)** - 설명은 줄바꿈 없이 1줄, 최대 200자로 작성합니다.

참고 IPv4 또는 IPv6 주소는 구성할 수 없습니다. Advanced(고급) 탭에서는 MTU, 이중 및 속도 설정만 변경할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

다음에 수행할 작업

인터페이스에 표시되는 트래픽에 대한 정보를 대시보드에 채워 넣으려면 패시브 인터페이스를 생성하는 것만으로는 부족합니다. 다음 작업도 수행해야 합니다. 사용 사례에서 이러한 단계를 살펴봅니다. 네트워크에서 트래픽을 능동적으로 모니터링하는 방법의 내용을 참조하십시오.

- 패시브 보안 영역을 생성하고 인터페이스를 해당 영역에 추가합니다. 보안 영역 구성의 내용을 참조하십시오.
- 패시브 보안 영역을 소스 영역으로 사용하는 액세스 제어 규칙을 생성합니다. 일반적으로는 이러한 규칙에 침입 정책을 적용하여 IDS(Intrusion Detection System) 모니터링을 구현합니다. 액세스 제어 정책 구성의 내용을 참조하십시오.
- 선택적으로 패시브 보안 영역용 SSL 암호 해독 및 ID 규칙을 생성하고 보안 인텔리전스 정책을 활성화합니다.

고급 인터페이스 옵션 구성

고급 옵션으로는 MTU, 하드웨어 설정, 관리 전용, MAC 주소 및 기타 설정이 있습니다.

MAC 주소 정보

MAC(Media Access Control) 주소를 수동으로 구성하여 기본값을 재정의할 수 있습니다.

고가용성 컨피그레이션의 경우, 인터페이스에 대해 액티브 및 스탠바이 MAC 주소를 모두 구성할 수 있습니다. 액티브 유닛이 페일오버하고 스탠바이 유닛이 활성화되면 새 액티브 유닛은 액티브 MAC 주소를 사용하기 시작하므로 네트워크 중단이 최소화됩니다.

기본 MAC 주소

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- VLAN 인터페이스(Firepower 1010) - 모든 VLAN 인터페이스에서 MAC 주소를 공유합니다. 연결된 스위치가 이 시나리오에 도움이 될 수 있을지 확인하십시오. 연결된 스위치에 고유한 MAC 주소가 필요한 경우, MAC 주소를 수동으로 할당할 수 있습니다. 고급 옵션 구성, 49 페이지의 내용을 참조하십시오.
- EtherChannel - EtherChannel의 경우 채널 그룹에 속한 모든 인터페이스가 동일한 MAC 주소를 공유합니다. 이 기능은 EtherChannel을 네트워크 애플리케이션 및 사용자에게 투명하게 만듭니다. 이들은 논리적 연결만 볼 수 있으며, 개별 링크에 대해서는 모르기 때문입니다. 포트 채널 인터페이스는 풀의 고유 MAC 주소를 사용하며 인터페이스 멤버십은 MAC 주소에 영향을 주지 않습니다.

- 하위 인터페이스 - 물리적 인터페이스의 모든 하위 인터페이스에서도 동일한 번인된(burned-in) MAC 주소를 사용합니다. 하위 인터페이스에 고유한 MAC 주소를 할당할 수 있습니다. 이를테면 서비스 공급자가 MAC 주소를 기준으로 액세스 제어를 수행하려 합니다. 또한 IPv6 링크 로컬 주소는 MAC 주소에 근거하여 생성되므로 하위 인터페이스에 고유한 MAC 주소를 할당하면 고유한 IPv6 링크 로컬 주소를 사용할 수 있습니다. 이에 따라 threat defense의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

MTU 정보

MTU에서는 위협 방지 디바이스가 지정된 이더넷 인터페이스에서 전송할 수 있는 최대 프레임 페이로드 크기를 지정합니다. MTU 값은 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 없는 프레임 크기입니다. 예를 들어, MTU를 1500으로 설정할 경우 예상 프레임 크기는 헤더 포함 시 1518바이트이고 VLAN 사용 시에는 1522입니다. 이러한 헤더를 수용하기 위해 MTU 값을 이보다 더 높게 설정하지 마십시오.

경로 MTU 검색

위협 방지 디바이스에서는 경로 MTU 검색을 지원하며(RFC 1191에 규정), 이 기능을 사용하면 두 호스트 간의 네트워크 경로에 있는 모든 디바이스에서 MTU를 조율할 수 있으므로, 경로의 최저 MTU에 대한 표준을 설정할 수 있습니다.

MTU 및 단편화

IPv4의 경우 지정된 MTU보다 큰 발신 IP 패킷은 2개 이상의 프레임으로 단편화됩니다. 분할된 패킷은 목적지(또는 일부 경우 중간 홉에서)에서 다시 합쳐지며, 분할이 일어날 경우 성능이 저하될 수 있습니다. IPv6의 경우에는 일반적으로 패킷의 단편화가 전혀 허용되지 않습니다. 따라서 분할을 방지하려면 IP 패킷이 MTU 크기 내에 맞아야 합니다.

UDP 또는 ICMP의 경우 애플리케이션은 단편화 방지를 위해 MTU를 고려해야 합니다.

참고 위협 방지 디바이스에서는 메모리에 공간이 있는 한 구성된 MTU보다 큰 프레임을 수신할 수 있습니다.

MTU와 점보 프레임

큰 MTU를 사용하는 경우 더 큰 패킷을 전송할 수 있습니다. 큰 패킷은 네트워크에서 더욱 효율적으로 사용할 수 있습니다. 다음 지침을 참조하십시오.

- 트래픽 경로의 MTU 일치 — 모든 threat defense 인터페이스 및 기타 디바이스 인터페이스의 MTU를 트래픽 경로와 동일하게 설정하는 것이 좋습니다. MTU를 일치시키면 패킷 분할 시 디바이스가 중간에 끼어드는 현상을 방지할 수 있습니다.
- 점보 프레임 수용 - 점보 프레임은 최대 표준 1522바이트(레이어 2 헤더 및 VLAN 헤더 포함)보다 큰 이더넷 패킷이며, 최대 9216바이트에 이릅니다. 점보 프레임을 수용하기 위해 MTU를 9000바이트 이상으로 설정할 수 있습니다. 최대값은 모델에 따라 다릅니다.

참고 MTU를 늘리면 점보 프레임에 더 많은 메모리가 할당되므로 액세스 규칙 등 다른 기능의 최대 사용량이 제한될 수 있습니다. threat defense virtual에서 MTU를 기본값인 1500 이상으로 늘리는 경우에는 시스템을 재부팅해야 합니다. 고가용성을 위해 디바이스를 컨피그레이션한 경우, 스탠바이 디바이스도 재부팅해야 합니다. 점보 프레임 지원이 항상 활성화되어 있는 다른 모델은 재부팅하지 않아도 됩니다.

고급 옵션 구성

고급 인터페이스 옵션에는 대부분의 네트워크에 적합한 기본 설정이 있습니다. 네트워킹 문제를 해결하는 경우 또는 고가용성을 구성하는 경우에만 이러한 설정을 구성하십시오.

다음 절차에서는 인터페이스가 이미 정의되어 있다고 가정합니다. 인터페이스를 처음 수정하거나 생성할 때 이러한 설정을 수정할 수도 있습니다.

제한 사항

- 브리지 그룹의 경우에는 멤버 인터페이스에서 이러한 옵션 중 대부분을 구성합니다. DAD 시도 및 Enable for HA Monitoring(HA 모니터링에 대해 활성화)를 제외하고 이러한 옵션을 BVI(Bridge Virtual Interface)에 사용할 수 없습니다.
- 에서는 관리 인터페이스의 MTU, 듀플렉스 또는 속도를 설정할 수 없습니다.
- Firepower 1010 스위치 포트에는 고급 옵션을 사용할 수 없습니다.
- Firepower 4100/9300에서는 인터페이스의 듀플렉스 또는 속도를 설정할 수 없습니다. FXOS를 사용하여 인터페이스에 대해 이러한 기능을 설정합니다.
- 패시브 인터페이스의 경우 MTU, 이중 및 속도만 설정할 수 있으며 인터페이스 관리만 수행할 수는 없습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭하고 **Interfaces(**인터페이스**)** 요약의 링크를 클릭한 다음, 인터페이스 유형을 클릭하여 인터페이스 목록을 확인합니다.

단계 **2** 수정할 인터페이스의 수정 아이콘( )을 클릭합니다.

단계 **3** **Advanced Options(**고급 옵션**)**를 클릭합니다.

단계 **4** 시스템에서 고가용성 컨피그레이션의 피어 유닛으로 페일오버를 수행할지 여부를 결정할 때 인터페이스 상태를 고려하려면 **Enable for HA Monitoring(HA** 모니터링에 대해 활성화**)**을 선택합니다.

이 옵션은 고가용성을 구성하지 않는 경우 무시되며 인터페이스의 이름을 구성하지 않는 경우에도 무시됩니다.

단계 **5** 데이터 인터페이스 관리만 수행하려면 **Management Only(**관리만**)**를 선택합니다.

관리 전용 인터페이스에서는 통과 트래픽을 허용하지 않으므로 데이터 인터페이스를 관리 전용으로 설정할 때 사용할 수 있는 값은 거의 없습니다. 관리/진단 인터페이스(항상 관리 전용)의 경우에는 이 설정을 변경할 수 없습니다.

단계 **6** Cisco Trustsec을 활성화하려면 **Propagate Security Group Tag(**보안 그룹 태그 전파**)**를 선택합니다.

물리적, 하위 인터페이스, EtherChannel, VLAN, 관리 또는 BVI 인터페이스(명명 여부에 관계없이)에서 Cisco Trustsec을 활성화하거나 비활성화할 수 있습니다. 기본적으로 Cisco Trustsec은 인터페이스의 이름을 지정할 때 자동으로 활성화됩니다.

단계 **7** **MTU**(Maximum Transmission Unit)를 원하는 값으로 변경합니다.

기본 MTU는 1500바이트입니다. 최소값과 최대값은 플랫폼에 따라 다릅니다. 네트워크에서 대개 점보 프레임이 표시되면 높은 값을 설정합니다.

참고 ISA 3000 Series 디바이스 또는 threat defense virtual에서 MTU를 1500보다 큰 값으로 늘리는 경우에는 디바이스를 재부팅해야 합니다. 고가용성을 위해 디바이스를 컨피그레이션한 경우, 스탠바이 디바이스도 재부팅해야 합니다. 점보 프레임 지원이 항상 활성화되어 있는 다른 모델은 재부팅하지 않아도 됩니다.

단계 **8** (실제 인터페이스만 해당됨) 속도 및 이중 설정을 수정합니다.

기본적으로 인터페이스는 연결 반대쪽의 인터페이스와 최적의 이중 및 속도를 협상하지만, 필요한 경우 특정 이중이나 속도를 강제 적용할 수 있습니다. 나열된 옵션은 인터페이스에서 지원하는 유일한 옵션입니다. 네트워크 모듈의 인터페이스에 이러한 옵션을 설정하기 전에 인터페이스 컨피그레이션에 대한 제한 사항, 5 페이지의 내용을 읽어보십시오.

- **Duplex(**듀플렉스**)** — **Half(**하프**)** 또는 **Full(**풀**)**을 선택합니다. SFP 인터페이스는 풀 듀플렉스만 지원합니다.
- **Speed(**속도**)** - 속도(모델에 따라 다름)를 선택합니다. (Secure Firewall 3100만 해당) 설치된 SFP 모듈의 속도를 탐지하고 적절한 속도를 사용하려면 **Detect SFP(SFP** 탐지**)**를 선택합니다. Duplex(듀플렉스)는 항상 Full(풀)이며 자동 협상은 항상 활성화되어 있습니다. 이 옵션은 나중에 네트워크 모듈을 다른 모델로 변경하고 속도를 자동으로 업데이트하려는 경우에 유용합니다.
- **Auto Negotiation(**자동 협상**)** - 속도, 링크 상태 및 흐름 제어를 협상하도록 인터페이스를 설정합니다. 1000Mbps 미만의 속도에서는 이 설정을 수정할 수 없습니다. SFP 인터페이스의 경우 속도가 1000Mbps로 설정된 경우에만 자동 협상을 비활성화할 수 있습니다.
- 전달 오류 수정 모드 - (Secure Firewall 3100만 해당) 25Gbps 이상의 인터페이스에서는 전달 오류 수정을 활성화합니다. EtherChannel 멤버 인터페이스의 경우, 이를 EtherChannel에 추가하기 전에 전달 오류 수정을 구성해야 합니다.

단계 **9** **IPv6** 컨피그레이션 설정을 수정합니다.

- **IPv6** 주소 컨피그레이션에 **DHCP** 활성화 - IPv6 라우터 알림 패킷에서 관리 주소 컨피그레이션 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 파생된 스테이트리스 자동 컨피그레이션 주소 이외의 주소도 얻도록 안내합니다.

- **IPv6** 비주소 컨피그레이션에 **DHCP** 활성화 - IPv6 라우터 알림 패킷에서 기타 주소 컨피그레이션 플래그를 설정할지 여부를 선택합니다. 이 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다.
- **DAD** 시도 - 인터페이스가 DAD(Duplicate Address Detection)를 수행하는 빈도를 0~600 사이의 값으로 설정합니다. 기본값은 1입니다. 스테이트리스 자동 컨피그레이션 프로세스에서 DAD는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다. 중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다. 인터페이스에서는 네이버 요청 메시지를 사용하여 DAD를 수행합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.

단계 **10** (선택 사항, 하위 인터페이스 및 고가용성 유닛의 경우 권장함.) MAC 주소를 구성합니다.

시스템은 기본적으로 인터페이스에 대해 NIC(Network Interface Card)에 버닝된 MAC 주소를 사용합니다. 따라서 인터페이스의 모든 하위 인터페이스는 같은 MAC 주소를 사용하므로 하위 인터페이스별로 고유한 주소를 생성할 수 있습니다. 고가용성을 구성하는 경우에는 액티브/스탠바이 MAC 주소도 수동으로 구성하는 것이 좋습니다. MAC 주소를 정의하면 페일오버 시 네트워크에서 일관성을 유지할 수 있습니다.

- **MAC Address(MAC** 주소**)** - H.H.H. 형식의 MAC(Media Access Control) 주소입니다. 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력합니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다(즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없음).
- **Standby MAC Address(**스탠바이 **MAC** 주소**)** - 고가용성에 사용할 주소입니다. 액티브 유닛이 페일오버되고 스탠바이 유닛이 액티브 상태가 되면, 네트워크 중단을 최소화하기 위해 새 액티브 유닛에서 액티브 MAC 주소를 사용하기 시작하고 기존 액티브 유닛은 스탠바이 주소를 사용합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

인터페이스 변경 사항 스캔 및 인터페이스 마이그레이션

디바이스에서 인터페이스를 변경하면 디바이스에서 변경 사항이 발생했음을 device manager에 알립니다. 인터페이스 스캔을 수행할 때까지 구성을 구축할 수 없습니다. device manager에서는 보안 정책의 인터페이스를 다른 인터페이스로 마이그레이션할 수 있도록 지원하므로 인터페이스는 거의 완벽하게 제거될 수 있습니다.

인터페이스 스캐닝 및 마이그레이션 정보

스캔

디바이스에서 인터페이스를 변경하면 디바이스에서 변경 사항이 발생했음을 device manager에 알립니다. 인터페이스 스캔을 수행할 때까지는 구성을 구축할 수 없습니다. 추가, 제거 또는 복원된 인터

페이스를 탐지하는 스캔을 수행한 후에 구성을 구축할 수 있습니다. 그러나 제거된 인터페이스를 참조하는 구성 부분은 구축되지 않습니다.

스캔해야 할 인터페이스 변경 사항에는 인터페이스 추가 또는 제거 작업이 포함됩니다. 네트워크 모듈 변경, Firepower 4100/9300 섀시의 할당된 인터페이스 변경, threat defense virtual의 인터페이스 변경을 예로 들 수 있습니다.

다음과 같은 항목은 변경해도 스캔 후 구축이 차단되지 않습니다.

- 보안 영역 멤버십
- EtherChannel 인터페이스 멤버십
- Firepower 1010 VLAN 인터페이스 스위치 포트 멤버십
- BVI를 참조하는 정책에 대한 브리지 그룹 인터페이스 멤버십

참고 Syslog 서버 이그레스 인터페이스를 변경하면 구축이 차단되지는 않지만, 수동으로 또는 인터페이스 교체 기능을 사용하여 syslog 서버 구성을 수정해야 합니다.

마이그레이션

새 인터페이스를 추가하거나 사용하지 않는 인터페이스를 제거하는 경우 threat defense 구성에 미치는 영향은 아주 적습니다. 그러나 보안 정책에 사용되는 인터페이스를 제거하면 구성에 영향이 미칩니다. 보안 영역, NAT, VPN, 라우팅, DHCP 서버 등 threat defense 구성의 여러 위치에서 인터페이스를 직접 참조할 수 있습니다.

Device Manager 에서는 보안 정책의 인터페이스를 다른 인터페이스로 마이그레이션할 수 있도록 지원하므로 인터페이스는 거의 완벽하게 제거될 수 있습니다.

참고 마이그레이션 기능을 사용하는 경우에는 이름, IP 주소 및 기타 구성이 한 인터페이스에서 다른 인터페이스로 복사되지 않으며, 기존 인터페이스 대신 새 인터페이스를 참조하도록 보안 정책이 변경됩니다. 마이그레이션하기 전에 새 인터페이스 설정을 수동으로 구성해야 합니다.

인터페이스를 제거해야 하는 경우, 제거하기 전에 새 인터페이스를 추가하고 기존 인터페이스를 마이그레이션하는 것이 좋습니다. 동시에 인터페이스를 추가하고 제거하는 경우에도 마이그레이션 프로세스는 계속 진행됩니다. 그러나 이를 참조하는 제거된 인터페이스 또는 정책을 수동으로 수정할 수는 없으므로 마이그레이션을 단계별로 수행하는 것이 더 쉬울 수 있습니다.

인터페이스를 동일한 유형으로 대체하는 경우(예: 네트워크 모듈을 RMA해야 하는 경우)에는 다음 작업을 수행할 수 있습니다. 1. 섀시에서 이전 모듈을 제거합니다. 2. 스캔을 수행합니다. 3. 제거된 인터페이스와 관련이 없는 변경 사항을 구축합니다. 4. 모듈을 교체합니다. 5. 새 스캔을 수행합니다. 6. 인터페이스와 관련된 모든 변경 사항을 비롯하여 구성을 구축합니다. 새 인터페이스에의 인터페이스 ID와 특성이 이전 인터페이스와 동일한 경우에는 마이그레이션을 수행할 필요가 없습니다.

인터페이스 스캐닝 및 마이그레이션에 대한 지침 및 제한 사항

지원되지 않는 인터페이스 마이그레이션

- BVI에 대한 물리적 인터페이스
- 방화벽 인터페이스에 대한 패시브 인터페이스
- 브리지 그룹 멤버
- EtherChannel 인터페이스 멤버
- ISA 3000 하드웨어 우회 멤버
- Firepower 1010 VLAN 인터페이스 또는 스위치 포트
- 진단 인터페이스
- HA 장애 조치 및 상태 링크
- 다른 유형의 인터페이스 마이그레이션(예: 브리지 그룹 인터페이스를 물리적 인터페이스가 필요한 기능으로 마이그레이션)

추가 지침

- 인터페이스를 제거해야 하는 경우, 제거하기 전에 새 인터페이스를 추가하고 기존 인터페이스를 마이그레이션하는 것이 좋습니다.
- threat defense virtual의 경우 인터페이스 목록 끝에 인터페이스만 추가하고 제거합니다. 다른 곳에서 인터페이스를 추가하거나 제거하는 경우, 하이퍼바이저에서는 인터페이스의 번호를 다시 매깁니다. 그 결과 구성에서 인터페이스 ID가 잘못된 인터페이스에 맞춰 정렬됩니다.
- 스캔/마이그레이션이 잘못된 경우, 섀시에서 원래 인터페이스를 복원한 후 다시 스캔하여 원래 상태로 돌아갑니다.
- 백업의 경우 새 인터페이스를 사용하여 새 백업을 생성하십시오. 이전 구성으로 복원하면 이전 인터페이스 정보가 복원되며 스캔/교체를 다시 수행해야 합니다.
- HA의 경우, 액티브 유닛에서 인터페이스 스캔을 수행하기 전에 두 유닛에서 인터페이스를 동일하게 변경합니다. 액티브 유닛에서 스캔/마이그레이션만 수행하면 됩니다. 구성 변경 사항은 스탠바이 유닛에 복제됩니다.

인터페이스 스캔 및 마이그레이션

device manager에서 인터페이스 변경 사항을 스캔하고 제거된 인터페이스에서 인터페이스 구성을 마이그레이션합니다. 인터페이스 구성만 마이그레이션하려는 경우(및 스캔이 필요하지 않은 경우), 스캐닝과 관련된 다음 절차의 단계를 무시합니다.

참고 마이그레이션 기능을 사용하는 경우에는 이름, IP 주소 및 기타 구성이 한 인터페이스에서 다른 인터페이스로 복사되지 않으며, 기존 인터페이스 대신 새 인터페이스를 참조하도록 보안 정책이 변경됩니다. 마이그레이션하기 전에 새 인터페이스 설정을 수동으로 구성해야 합니다.

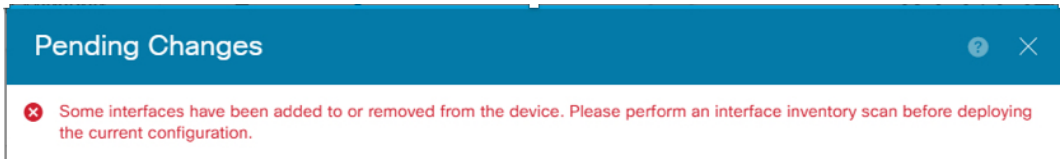
프로시저

단계 **1** 섀시에서 인터페이스를 추가하거나 제거합니다.

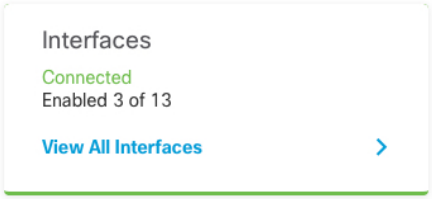
인터페이스를 제거해야 하는 경우, 제거하기 전에 새 인터페이스를 추가하고 기존 인터페이스를 교체하는 것이 좋습니다.

단계 **2** 인터페이스 변경 사항을 스캔합니다.

인터페이스 스캔을 수행할 때까지는 구성을 구축할 수 없습니다. 스캔 전에 구축을 시도하는 경우 다음 오류가 표시됩니다.

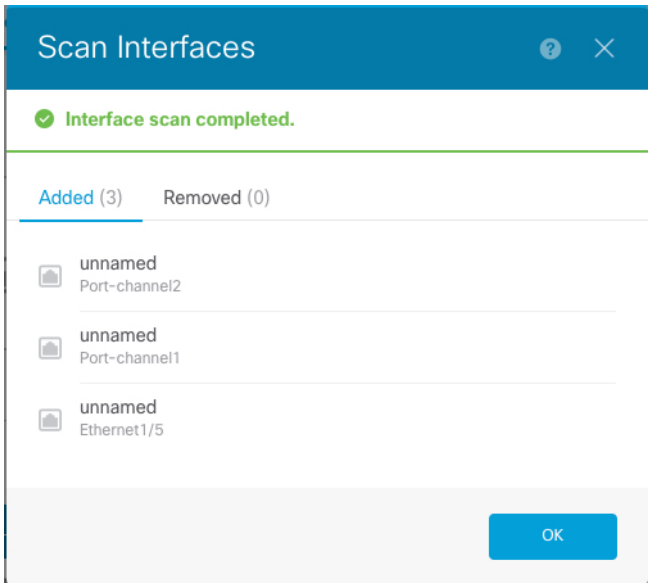


a) **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다.

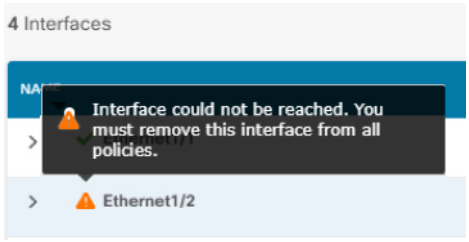


b) Scan Interfaces(인터페이스 스캔) 아이콘( )을 클릭합니다.

c) 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.



스캔 후에는 제거된 인터페이스가 다음과 같이 주의 기호와 함께 Interfaces(인터페이스) 페이지에 표시됩니다.

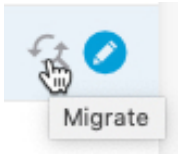


단계 **3** 기존 인터페이스를 새 인터페이스로 마이그레이션하려면 다음을 수행합니다.

a) 이름, IP 주소 등을 사용하여 새 인터페이스를 구성합니다.

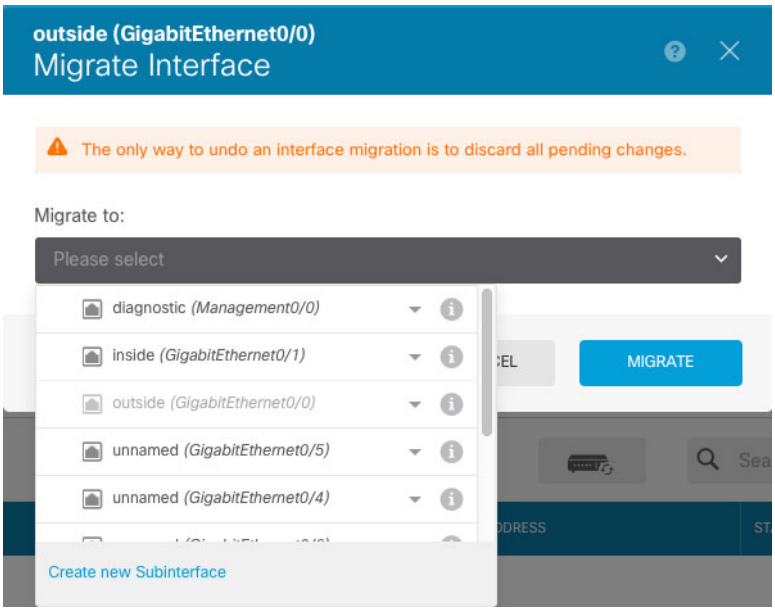
제거할 인터페이스의 기존 IP 주소 및 이름을 사용하려는 경우에는 먼저 새 인터페이스에서 해당 설정을 사용할 수 있도록 기존 인터페이스를 더미 이름 및 IP 주소로 다시 구성해야 합니다.

b) 기존 인터페이스의 Migrate(마이그레이션) 아이콘을 클릭합니다.

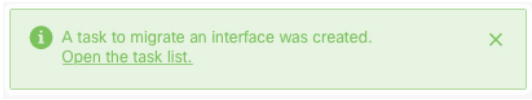


이 프로세스를 수행하면 인터페이스를 참조하는 모든 구성 설정에서 기존 인터페이스가 새 인터페이스로 마이그레이션됩니다.

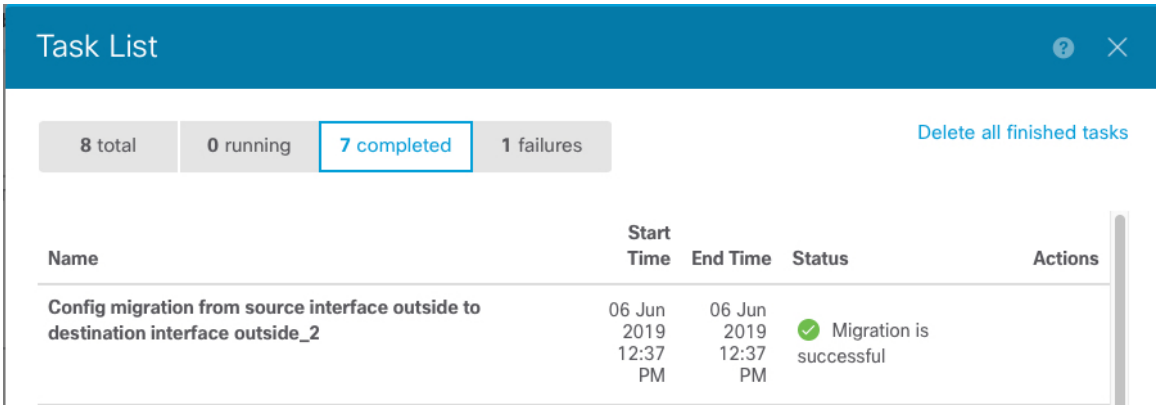
c) **Migrate to:(**마이그레이션 대상**:)** 드롭다운 목록에서 새 인터페이스를 선택합니다.



d) **Interfaces(**인터페이스**)** 페이지에 메시지가 나타납니다. 메시지에서 링크를 클릭합니다.



e) **Task List(**작업 목록**)**를 확인하여 마이그레이션에 성공했는지 확인합니다.

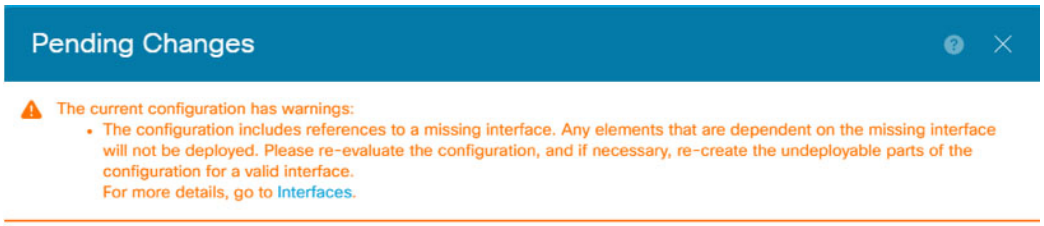


f) 마이그레이션에 실패하면 API Explorer에서 원인을 확인할 수 있습니다.

API Explorer를 열려면 More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다. **Interface(**인터페이스**)** > **GET /jobs/interfacemigrations**를 선택한 다음, **Try it Out!(**시도**)**을 클릭합니다.

단계 **4** 구성을 구축합니다.

제거된 인터페이스를 참조하는 구성의 일부가 구축되지 않습니다. 이 경우 다음 메시지가 표시됩니다.



단계 **5** 섀시에서 이전 인터페이스를 제거하고 다른 스캔 작업을 수행합니다.

정책에서 더 이상 사용되지 않으며 제거된 인터페이스가 **Interfaces(**인터페이스**)** 페이지에서 제거됩니다.

단계 **6** 구성을 다시 구축하여 사용되지 않는 인터페이스를 구성에서 제거합니다.

Secure Firewall 3100용 네트워크 모듈 관리

방화벽의 전원을 켜기 전에 네트워크 모듈을 설치하는 경우에는 별도의 작업이 필요하지 않습니다. 네트워크 모듈이 활성화되었으며 사용할 준비가 되었습니다.

초기 부팅 후 네트워크 모듈 설치를 변경해야 하는 경우 다음 절차를 참조하십시오.

브레이크아웃 포트 구성

각 40GB 이상의 인터페이스에 대해 10GB 분할 포트를 구성할 수 있습니다. 이 절차에서는 포트를 분리하고 다시 조인하는 방법을 설명합니다. 브레이크아웃 포트는 EtherChannel에 추가되는 것을 포함하여 다른 물리적 이더넷 포트와 마찬가지로 사용할 수 있습니다.

고가용성을 위해 액티브 유닛에서 이 절차를 수행합니다. 인터페이스 변경 사항은 다른 유닛에 복제됩니다.

시작하기 전에

- 지원되는 브레이크아웃 케이블을 사용해야 합니다. 자세한 내용은 하드웨어 설치 가이드를 참조하십시오.
- 인터페이스는 컨피그레이션에서 사용할 수 없습니다. 하위 인터페이스를 포함하거나 EtherChannel의 일부일 수 없습니다.
- 고가용성을 위해 인터페이스의 이름을 지정하거나, 활성화하거나, 고가용성을 모니터링할 수 없습니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다. 인터페이스 목록에는 물리적 인터페이스, 해당 이름, 주소 및 상태가 표시됩니다.

단계 **2** 40GB 이상의 인터페이스에서 10GB 포트를 브레이크아웃하려면 인터페이스 오른쪽에 있는 브레이크아웃 아이콘( )을 클릭합니다.

확인 대화 상자에서 **OK(**확인**)**를 클릭합니다. 인터페이스가 사용 중인 경우 오류 메시지가 표시됩니다. 모든 사용 사례를 해결해야 브레이크아웃을 다시 시도할 수 있습니다. 예를 들어 다른 인터페이스를 사용하도록 구성을 마이그레이션할 수 있습니다.

예를 들어 Ethernet2/1 40GB 인터페이스를 분리하기 위해 결과 하위 인터페이스는 Ethernet2/1/1, Ethernet2/1/2, Ethernet2/1/3 및 Ethernet2/1/4로 식별됩니다.

인터페이스 그래픽에서 분리된 포트의 모양은 다음과 같습니다. 왼쪽 및 오른쪽 화살표를 클릭하여 브레이크아웃 포트 상태를 자세히 설명하는 페이지를 스크롤할 수 있습니다.

단계 **3** 브레이크아웃 포트에 다시 조인하려면 인터페이스 오른쪽에 있는 조인 아이콘( )을 클릭합니다.

확인 대화 상자에서 **OK(**확인**)**를 클릭합니다. 하위 포트가 사용 중인 경우 오류 메시지가 표시됩니다. 모든 사용 사례를 해결해야 다시 조인할 수 있습니다. 예를 들어 다른 인터페이스를 사용하도록 구성을 마이그레이션할 수 있습니다.

인터페이스의 모든 하위 포트에 다시 조인해야 합니다.

단계 **4** 구성을 구축합니다.

네트워크 모듈 추가

초기 부팅 후 방화벽에 네트워크 모듈을 추가하려면 다음 단계를 수행합니다. 새 모듈을 추가하려면 재부팅해야 합니다.

프로시저

단계 **1** 하드웨어 설치 가이드에 따라 네트워크 모듈을 설치합니다.

고가용성을 위해 두 유닛에 네트워크 모듈을 설치합니다.

단계 **2** 방화벽을 재부팅합니다. 시스템 리부팅 또는 종료의 내용을 참조하십시오. 고가용성을 위해 스탠바이 유닛을 재부팅한 다음 스탠바이 유닛에서 이 절차의 나머지를 수행합니다.

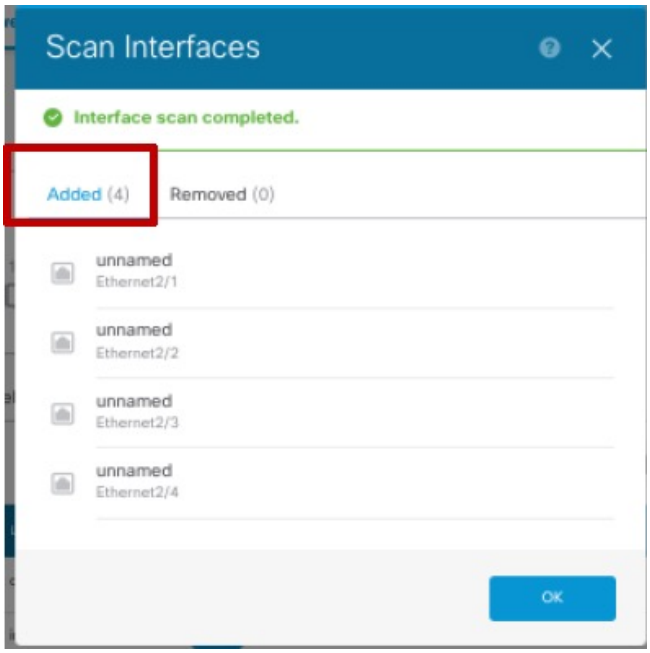
단계 **3** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다.

그래픽은 인터페이스 스캔이 필요함을 보여줍니다.

그림 *3:* 인터페이스 스캔 필요

단계 **4** 새 네트워크 모듈 상세 정보로 페이지를 업데이트하려면 인터페이스 스캔을 클릭합니다. 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.

그림 *4:* 인터페이스 스캔

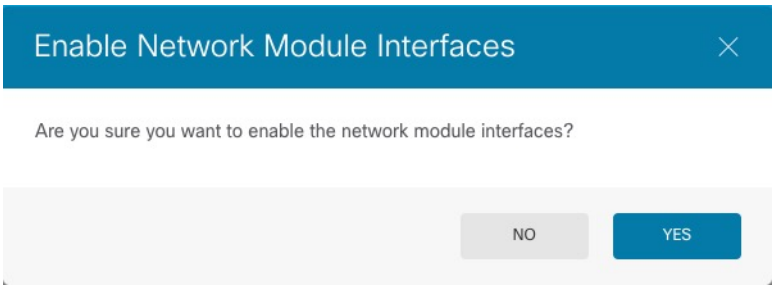


단계 **5** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 활성화합니다.

그림 *5:* 네트워크 모듈 활성화

단계 **6** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 *6:* 사용 확인



단계 **7** 고가용성을 위해 액티브 유닛을 변경한 다음(액티브 및 스탠바이 피어 전환(강제 페일오버) 참조) 새 스탠바이 유닛에 대해 위의 단계를 수행합니다.

네트워크 모듈 핫 스왑

재부팅할 필요 없이 네트워크 모듈을 동일한 유형의 새 모듈로 핫 스왑할 수 있습니다. 그러나 안전하게 제거하려면 현재 모듈을 종료해야 합니다. 이 절차에서는 기존 모듈을 종료하고 새 모듈을 설치하고 활성화하는 방법을 설명합니다.

시작하기 전에

고가용성의 경우 페일오버 링크가 모듈에 있는 경우 네트워크 모듈을 비활성화할 수 없습니다. 고가용성을 해제해야 합니다(고가용성 해제 참조). 모듈을 핫 스왑한 후 고가용성을 재편성할 수 있습니다.

프로시저

단계 **1** 고가용성을 위해 핫 스왑을 수행할 유닛이 대기 노드인지 확인합니다. 액티브 및 스탠바이 피어 전환(강제 페일오버)를 참조하십시오.

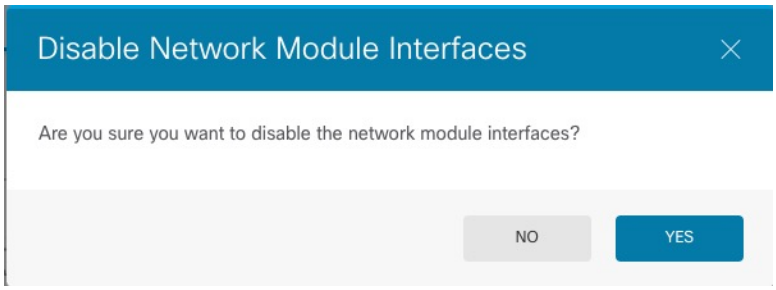
단계 **2** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다.

단계 **3** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 비활성화합니다.

그림 *7:* 네트워크 모듈 비활성화

단계 **4** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 *8:* 사용 안 함 확인



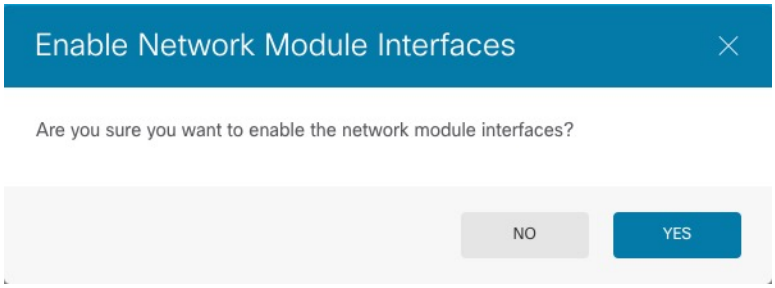
단계 **5** 하드웨어 설치 가이드에 따라 네트워크 모듈을 설치합니다.

단계 **6** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 활성화합니다.

그림 *9:* 네트워크 모듈 활성화

단계 **7** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 *10:* 사용 확인



네트워크 모듈을 다른 유형으로 교체

네트워크 모듈을 다른 유형으로 교체하는 경우 재부팅해야 합니다. 새 모듈에 이전 모듈보다 인터페이스가 더 적은 경우 더 이상 존재하지 않을 인터페이스와 관련된 모든 구성을 수동으로 제거해야 합니다.

시작하기 전에

고가용성의 경우 페일오버 링크가 모듈에 있는 경우 네트워크 모듈을 비활성화할 수 없습니다. 고가용성을 해제해야 합니다(고가용성 해제 참조). 즉, 액티브 유닛을 재부팅하면 다운타임이 발생합니다. 유닛 리부팅이 완료되면 고가용성을 재구성할 수 있습니다.

프로시저

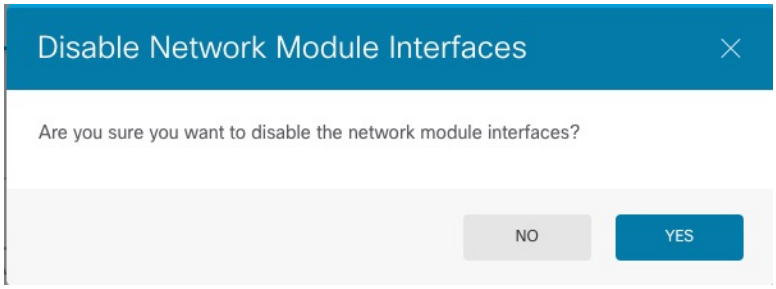
단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다. 고가용성을 위해 스탠바이 유닛에서 이 절차를 먼저 수행합니다.

단계 **2** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 비활성화합니다.

그림 ***11:*** 네트워크 모듈 비활성화

단계 **3** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***12:*** 사용 안 함 확인

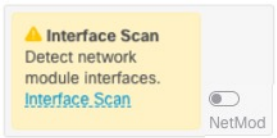


단계 **4** 디바이스에서 하드웨어 설치 가이드에 따라 기존 네트워크 모듈을 제거하고 새 네트워크 모듈로 교체합니다.

단계 **5** 방화벽을 재부팅합니다. 시스템 리부팅 또는 종료의 내용을 참조하십시오.

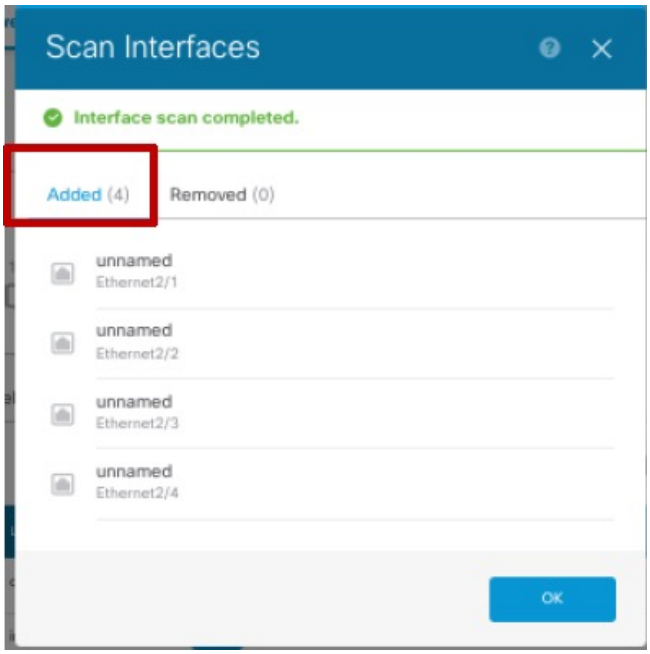
단계 **6** 인터페이스 페이지의 그래픽은 인터페이스 스캔이 필요함을 나타냅니다. 새 네트워크 모듈 상세 정보로 페이지를 업데이트하려면 인터페이스 스캔을 클릭합니다.

그림 ***13:*** 인터페이스 스캔 필요



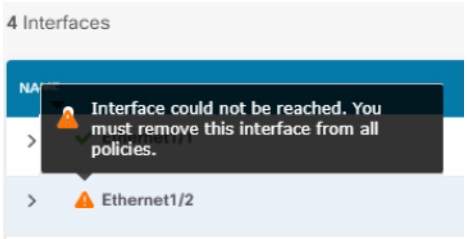
단계 **7** 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.

그림 ***14:*** 인터페이스 스캔



스캔 후에는 제거된 인터페이스가 다음과 같이 주의 기호와 함께 **Interfaces(**인터페이스**)** 페이지에 표시됩니다.

그림 ***15:*** 제거된 인터페이스



단계 **8** 네트워크 모듈의 인터페이스 수가 더 적은 경우 제거된 인터페이스를 직접 참조하는 모든 구성을 제거해야 합니다.

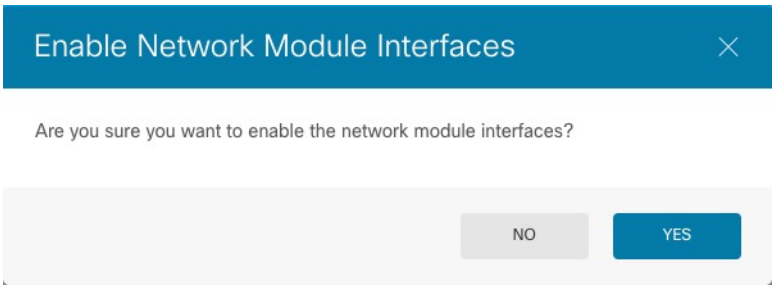
보안 영역을 참조하는 정책은 영향을 받지 않습니다. 선택적으로 구성을 다른 인터페이스로 마이그레이션할 수 있습니다. 인터페이스 스캔 및 마이그레이션, 53 페이지를 참조하십시오.

단계 **9** 인터페이스 그래픽에서 슬라이더( )를 클릭하여 네트워크 모듈을 활성화합니다.

그림 ***16:*** 네트워크 모듈 활성화

단계 **10** 네트워크 모듈을 켤지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***17:*** 사용 확인



단계 **11** 인터페이스 속도를 변경하려면 고급 옵션 구성, 49 페이지의 내용을 참조하십시오.

기본 속도는 설치된 SFP에서 올바른 속도를 탐지하는 Detect SFP(SFP 탐지)로 설정됩니다. 수동으로 속도를 특정 값으로 설정하고 이제 새 속도가 필요한 경우에만 속도를 수정해야 합니다.

단계 **12** 구성을 변경해야 하는 경우 구축 아이콘을 클릭합니다.

네트워크 모듈 변경 사항을 저장하기 위해 구축할 필요는 없습니다.

단계 **13** 고가용성을 위해 액티브 유닛을 변경한 다음(액티브 및 스탠바이 피어 전환(강제 페일오버) 참조) 새 스탠바이 유닛에 대해 위의 단계를 수행합니다.

네트워크 모듈 분리

네트워크 모듈을 영구적으로 제거하려면 다음 단계를 수행합니다. 네트워크 모듈을 제거하려면 재부팅해야 합니다.

시작하기 전에

고가용성의 경우 네트워크 모듈에 페일오버 링크가 없는지 확인하십시오.

프로시저

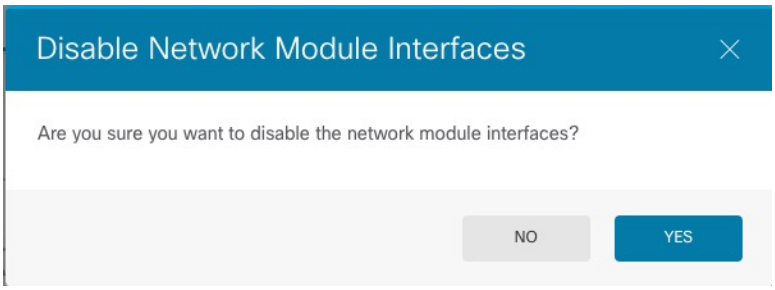
단계 **1** **Device(**디바이스**)**를 클릭한 다음, **Interfaces(**인터페이스**)** 요약에서 **View All Interfaces(**모든 인터페이스 보기**)** 링크를 클릭합니다. 고가용성을 위해 스탠바이 유닛에서 이 절차를 먼저 수행합니다.

단계 **2** 인터페이스 그래픽에서 슬라이더()를 클릭하여 네트워크 모듈을 비활성화합니다.

그림 ***18:*** 네트워크 모듈 비활성화

단계 **3** 네트워크 모듈을 끌지 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

그림 ***19:*** 사용 안 함 확인



단계 **4** 방화벽에서 네트워크 모듈을 분리합니다.

단계 **5** 방화벽을 재부팅합니다. 시스템 리부팅 또는 종료의 내용을 참조하십시오.

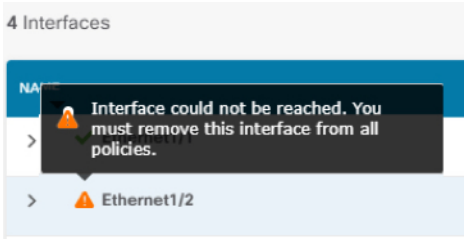
단계 **6** 인터페이스 페이지의 그래픽은 인터페이스 스캔이 필요함을 나타냅니다. 올바른 네트워크 모듈 상세 정보로 페이지를 업데이트하려면 인터페이스 스캔을 클릭합니다.

그림 ***20:*** 인터페이스 스캔 필요

단계 **7** 인터페이스가 스캔될 때까지 기다린 다음, **OK(**확인**)**를 클릭합니다.

스캔 후에는 제거된 인터페이스가 다음과 같이 주의 기호와 함께 **Interfaces(**인터페이스**)** 페이지에 표시됩니다.

그림 ***21:*** 제거된 인터페이스



단계 **8** 제거된 인터페이스를 직접 참조하는 모든 구성을 제거해야 합니다.

보안 영역을 참조하는 정책은 영향을 받지 않습니다. 선택적으로 구성을 다른 인터페이스로 마이그레이션할 수 있습니다. 인터페이스 스캔 및 마이그레이션, 53 페이지를 참조하십시오.

단계 **9** 구성을 변경해야 하는 경우 구축 아이콘을 클릭합니다.

네트워크 모듈 변경 사항을 저장하기 위해 구축할 필요는 없습니다.

단계 **10** 고가용성을 위해 액티브 유닛을 변경한 다음(액티브 및 스탠바이 피어 전환(강제 페일오버) 참조) 새 스탠바이 유닛에 대해 위의 단계를 수행합니다.

정전(ISA 3000)에 대한 하드웨어 우회 구성

정전 상태에서도 인터페이스 쌍 간에 트래픽 플로우가 계속되도록 하드웨어 바이패스를 활성화할 수 있습니다. 지원되는 인터페이스 쌍은 구리 인터페이스 GigabitEthernet 1/1과 1/2 및 GigabitEthernet 1/3과 1/4입니다. 파이버 이더넷 모델을 사용하는 경우에는 구리 이더넷 쌍(GigabitEthernet 1/1 및 1/2)만 하드웨어 바이패스를 지원합니다. 기본적으로 하드웨어 우회는 지원되는 경우 두 인터페이스 쌍 모두에 대해 활성화됩니다.

하드웨어 바이패스가 활성 상태이면 트래픽이 계층 1에서 이러한 인터페이스 쌍 간을 통과합니다. device manager 및 threat defense CLI는 인터페이스가 중단되는 것으로 간주합니다. 방화벽 기능은 없으므로 트래픽의 디바이스 통과를 허용하는 경우의 위험을 파악해야 합니다.

이 절차에서 설명하는 대로 TCP 시퀀스 번호 임의 설정을 비활성화하는 것이 좋습니다. 기본적으로 ISA 3000을 통과하는 TCP 연결의 ISN(초기 시퀀스 번호)는 임의의 숫자로 재작성됩니다. 하드웨어 바이패스를 활성화하면 ISA 3000은 더 이상 데이터 경로에 없으며 시퀀스 번호를 변환하지 않습니다. 수신 클라이언트는 예상치 않은 시퀀스 번호를 수신하므로 연결을 삭제합니다. 따라서 TCP 세션을 다시 설정해야 합니다. TCP 시퀀스 번호 임의 설정을 비활성화하더라도 전환 중에 일시적으로 중단되는 링크 때문에 일부 TCP 연결은 다시 설정해야 합니다.

CLI 콘솔 또는 SSH 세션에서 **show hardware-bypass** 명령을 사용하여 운영 상태를 모니터링합니다.

시작하기 전에

다음 조건을 충족해야 하드웨어 바이패스가 작동합니다.

- 같은 브리지 그룹에 인터페이스 쌍을 배치해야 합니다.
- 스위치의 액세스 포트에 인터페이스를 연결해야 합니다. 트렁크 포트에는 인터페이스를 연결하지 마십시오.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 Interfaces(인터페이스) 요약의 링크를 클릭합니다.

페이지 상단에 있는 **Hardware Bypass(**하드웨어 우회**)** 섹션에서는 이 디바이스에 허용된 인터페이스 쌍의 현재 컨피그레이션을 표시합니다.

그러나 쌍이 동일한 브리지 그룹에 컨피그레이션되어 있는지 먼저 확인한 후에야 하드웨어 우회를 활성화할 수 있습니다.

단계 **2** **Edit(**수정**)**를 클릭하여 하드웨어 우회를 구성합니다.

Hardware Bypass Configuration(하드웨어 우회 컨피그레이션**)** 대화 상자가 나타납니다.

단계 **3** 자동 하드웨어 우회 동작을 구성하려면 각 인터페이스 쌍에 대해 **Hardware Bypass during Power Down(**정전 시 하드웨어 우회**)** 영역에서 다음 옵션 중 하나를 선택합니다.

- **Disable(**비활성화**)** — 하드웨어 우회를 비활성화합니다. 정전 시에는 트래픽이 디바이스를 통과하지 않습니다.
- **Enable(**활성화**)** — 정전 시 하드웨어 우회를 활성화합니다. 하드웨어 우회를 사용하면 정전 시에도 트래픽이 중단되지 않습니다. 우회된 트래픽은 검사되지 않으며 보안 정책이 적용되지 않습니다. 전원이 복구되면 하드웨어 우회가 자동으로 비활성화되므로 트래픽이 검사를 통해 정상적으로 통과할 수 있습니다. 하드웨어 우회가 비활성화되면 트래픽이 잠시 중단될 수 있습니다.
- **Enable with Persistence(**영구 활성화**)** — 정전 시 하드웨어 우회를 활성화하고 전력 복구 후에도 활성화 상태를 유지합니다. 전력이 복구되면 **Manual Hardware Bypass(**수동 하드웨어 우회**)** 슬라이더를 사용하여 하드웨어 우회를 비활성화해야 합니다. 이 옵션을 통해 트래픽이 일시 중단되는 시점을 제어할 수 있습니다.

단계 **4** (선택 사항) 하드웨어 우회를 수동으로 활성화하거나 또는 비활성화하려면 **Manual Hardware Bypass(**수동 하드웨어 우회**)** 슬라이더를 클릭합니다.

예를 들어 어떤 이유로 시스템을 테스트하거나 일시적으로 디바이스를 우회해야 할 경우가 있을 수 있습니다. 하드웨어 우회의 상태를 변경하려면 컨피그레이션을 구축해야 한다는 점에 유의하십시오. 설정을 변경하는 것만으로는 충분하지 않습니다.

하드웨어 바이패스를 수동으로 활성화/비활성화하면 다음 메시지가 표시됩니다. 여기서 *pair*는 1/1-1/2 또는 1/3-1/4입니다.

- %FTD-6-803002: GigabitEthernet 쌍을 통해 전송되는 트래픽은 시스템에서 보호하지 않습니다.
- %FTD-6-803003: 사용자가 GigabitEthernet 쌍에서 우회를 수동으로 비활성화했습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

변경 사항은 즉시 적용되지 않습니다. 컨피그레이션을 구축해야만 적용됩니다.

단계 **6** (선택 사항). TCP 시퀀스 번호 임의 설정을 비활성화하는 데 필요한 FlexConfig 개체 및 정책을 생성합니다.

a) **Device(**디바이스**)** > **Advanced Configuration(**고급 컨피그레이션**)**에서 **View Configuration(**컨피그레이션 보기**)**을 클릭합니다.
b) Advanced Configuration(고급 컨피그레이션) 목차에서 **FlexConfig** > **FlexConfig Objects(FlexConfig** 개체**)**를 클릭합니다.
c) + 버튼을 클릭하여 새 개체를 생성합니다.
d) 개체의 이름을 입력합니다. **Disable_TCP_Randomization**을 예로 들 수 있습니다.
e) **Template(**템플릿**)** 편집기에서 TCP 시퀀스 번호 임의 설정을 비활성화하는 명령을 입력합니다.

해당 명령은 **set connection random-sequence-number disable**이지만 정책 맵 내의 특정 클래스에 맞게 명령을 컨피그레이션해야 합니다. 현재까지 확인된 가장 쉬운 방식은 임의 시퀀스 번호를 전역적으로 비활성화하는 것입니다. 이렇게 하려면 다음 명령을 사용해야 합니다.

```
policy-map global_policy
 class default_class
  set connection random-sequence-number disable
```

f) **Negate Template(**무효화 템플릿**)** 편집기에 이 컨피그레이션을 실행 취소하는 데 필요한 행을 입력합니다.

예를 들어 TCP 시퀀스 번호 임의 설정을 전역적으로 비활성화하는 경우, 무효화 템플릿은 다음과 같습니다.

```
policy-map global_policy
 class default_class
  set connection random-sequence-number enable
```

g) **OK(**확인**)**를 클릭하여 개체를 저장합니다.

이제 개체를 FlexConfig 정책에 추가해야 합니다. 개체를 만드는 것으로는 충분하지 않습니다.

h) 목차에서 **FlexConfig Policy(FlexConfig** 정책**)**를 클릭합니다.

i) Group List(그룹 목록)에서 **+**를 클릭합니다.

j) Disable_TCP_Randomization 개체를 선택하고 **OK(**확인**)**를 클릭합니다.

템플릿의 명령으로 미리보기가 업데이트됩니다. 올바른 명령이 표시되는지 확인합니다.

k) **Save(**저장**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다.

모니터링 인터페이스

다음 영역에서 인터페이스에 대한 몇 가지 기본 정보를 확인할 수 있습니다.

- **Device(**디바이스**)**. 포트 그래픽을 사용하여 인터페이스의 현재 상태를 모니터링합니다. 포트 위에 마우스를 올려놓으면 해당 IP 주소, EtherChannel 멤버십, 및 활성화 상태 및 링크 상태가 표시됩니다. IP 주소는 정적으로 할당할 수도 있고 DHCP를 사용하여 가져올 수도 있습니다.

  인터페이스 포트는 다음 색 코드를 사용합니다.

  - 녹색 — 인터페이스가 구성되어 있고 활성화된 상태이며 링크가 작동합니다.
  - 회색 — 인터페이스를 활성화하지 않습니다.
  - 주황색/빨간색 — 인터페이스가 구성되어 있고 활성화된 상태이지만 링크가 작동하지 않습니다. 유선 인터페이스의 경우 이 색은 수정해야 하는 오류 상태를 나타냅니다. 유선 인터페이스가 아닌 경우에는 이 색이 표시되는 것이 정상입니다.

- **Monitoring(**모니터링**)** > **System(**시스템**)**. 처리량 대시보드에는 시스템을 통과하는 트래픽에 대한 정보가 표시됩니다. 모든 인터페이스에서 정보를 확인할 수도 있고 검사할 특정 인터페이스를 선택할 수도 있습니다.
- **Monitoring(**모니터링**)** > **Zones(**영역**)**. 이 대시보드에는 인터페이스로 구성된 보안 영역을 기반으로 한 통계가 표시됩니다. 이 정보를 자세히 확인하여 추가 세부사항을 파악할 수 있습니다.

CLI에서 인터페이스 모니터링

CLI 콘솔을 열거나 디바이스 CLI에 로그인한 후에 다음 명령을 사용하여 인터페이스 관련 행동 및 통계에 대한 상세 정보를 가져올 수도 있습니다.

- **show interface** 인터페이스 통계 및 컨피그레이션 정보를 표시합니다. 이 명령에는 필요한 정보를 가져오는 데 사용할 수 있는 여러 키워드가 있습니다. 사용 가능한 옵션을 확인하려면 키워드로 ?를 사용합니다.
- **show ipv6 interface** 인터페이스에 대한 IPv6 컨피그레이션 정보를 표시합니다.
- **show bridge-group** 멤버 정보와 IP 주소를 비롯하여 BVI(브리지 가상 인터페이스)에 대한 정보를 표시합니다.
- **show conn** 인터페이스를 통해 현재 설정되어 있는 연결에 대한 정보를 표시합니다.
- **show traffic** 각 인터페이스를 통과하는 트래픽에 대한 통계를 표시합니다.
- **show ipv6 traffic** 디바이스를 통과하는 IPv6 트래픽에 대한 통계를 표시합니다.
- **show dhcpd** 인터페이스의 DHCP 사용량에 대한 통계와 기타 정보(특히 인터페이스에 구성된 DHCP 서버 관련)를 표시합니다.
- **show switch vlan** VLAN-스위치 포트 연결을 표시합니다.
- **show switch mac-address-table** 정적 및 동적 MAC 주소 항목을 표시합니다.
- **show arp** 동적, 정적 및 프록시 ARP 항목을 표시합니다.
- **show power inline** PoE 상태를 표시합니다.
- **show vpdn group** PPPoE 그룹 및 구성된 사용자 이름 및 인증을 표시합니다.
- **show vpdn username** PPPoE 사용자 이름 및 비밀번호를 표시합니다.
- **show vpdn session pppoe state** PPPoE 세션 상태를 표시합니다.

인터페이스의 예시

사용 사례 장에는 다음과 같은 인터페이스 관련 예시가 포함되어 있습니다.

- Device Manager에서 디바이스 구성 방법
- 서브넷을 추가하는 방법

- 네트워크에서 트래픽을 능동적으로 모니터링하는 방법