일반 방화벽 인터페이스

이 장에는 EtherChannel, VLAN 하위 인터페이스, IP 주소 등 일반 방화벽 threat defense 인터페이스 설정을 포함합니다.

참고 Firepower 4100/9300의 초기 인터페이스 설정에 대해서는 인터페이스 구성를 참조합니다.

정규 방화벽 인터페이스 요구 사항 및 사전 요건

모델 지원

Threat Defense

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

Firepower 1010 스위치 포트 구성

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 스위치 포트에 할당하는 작업 등을 비롯한, 스위치 포트의 구성을 시작하기 위한 작업이 포함되어 있습니다. 이 섹션에서는 지원되는 인터페이스에서 PoE(Power over Ethernet)를 맞춤화하는 방법에 대해서도 설명합니다.

Firepower 1010 스위치 포트 관련 정보

이 섹션에서는 Firepower 1010의 스위치 포트를 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. 투명 모드에서 이러한 인터페이스는 구성된 보안 정책을 사용해 방화벽 서비스를 적용하여 레이어 2에서 동일한 네트워크에 있는 인터페이스 간에 트래픽을 전달하는 브리지 그룹 멤버입니다. 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(인라인 집합 및 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. 진단 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 정

책이 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.

Auto-MDI/MDIX 기능

Firepower 1010 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. 속도와 양방향을 1000 및 최대로 설정하면 인터페이스에서 항상 자동 협상이 실행되므로 Auto-MDI/MDIX 기능도 항상 사용 설정된 상태이고 이를 사용 해제할 수 없습니다.

Firepower 1010 스위치 포트에 대한 지침 및 제한 사항

고가용성 및 클러스터링

- 클러스터는 지원되지 않습니다.
- 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:
  - 라우팅 방화벽 모드 - 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. MAC 주소 구성, 72 페이지의 내용을 참조하십시오.

- 투명 방화벽 모드 - 각 VLAN 인터페이스에는 고유한 MAC 주소가 있습니다. 원하는 경우 MAC 주소를 수동으로 할당하여 생성된 MAC 주소를 재정의할 수 있습니다. MAC 주소 구성, 72 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
- 인라인 집합 또는 패시브 인터페이스
- EtherChannel
- 장애 조치 및 상태 링크
- SGT(Security Group Tagging)

기타 지침 및 제한 사항

- Firepower 1010에서 명명된 인터페이스를 최대 60개 구성할 수 있습니다.
- 진단 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.

스위치 포트 및 PoE(Power over Ethernet) 구성

스위치 포트 및 PoE를 구성하려면 다음 작업을 완료합니다.

스위치 포트 모드 활성화 또는 비활성화

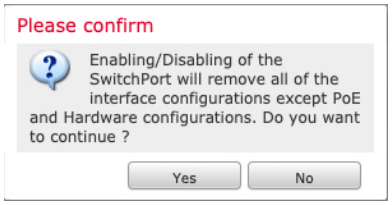
각 인터페이스를 방화벽 인터페이스나 스위치 포트 중 하나에 독립적으로 설정할 수 있습니다. 기본적으로 이더넷 1/1은 방화벽 인터페이스이며, 남은 이더넷 인터페이스는 스위치 포트로 구성됩니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 **SwitchPort** 열에서 슬라이더를 클릭해서 스위치 포트 모드를 설정해서 **Slider enabled(**슬라이더 활성화됨**)** ( ) 또는 **Slider disabled(**슬라이더 비활성화됨**)** ( )으로 표시되도록 합니다.

기본적으로 스위치 포트는 VLAN 1에서 액세스 모드로 설정됩니다. 논리적 VLAN 1 인터페이스(또는 이러한 스위치 포트에 설정한 모든 VLAN)를 수동으로 추가해 트래픽이 라우팅되고 FTD 보안 정책에 참여하게 합니다(자세한 내용은 VLAN 인터페이스 구성, 5 페이지의 내용을 참조하십시오). 관리 인터페이스는 스위치 포트 모드로 설정할 수 없습니다. 스위치 포트 모드를 변경하면 지원되지 않는 구성은 모두 제거됩니다.



VLAN 인터페이스 구성

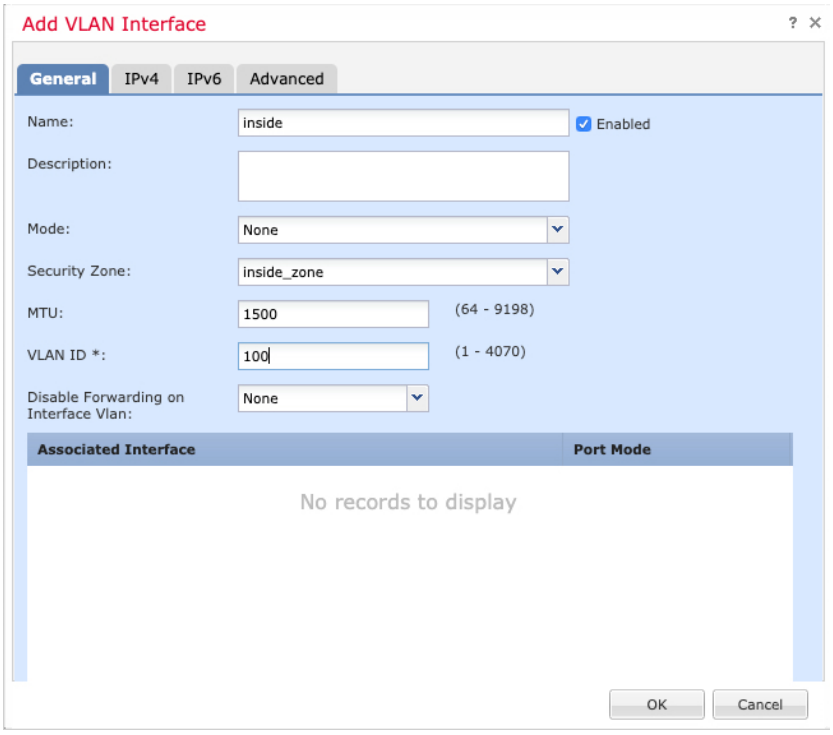
이 섹션에서는 연결된 스위치 포트에 사용할 VLAN 인터페이스를 구성하는 방법에 대해 설명합니다. 기본적으로 스위치 포트는 VLAN1에 할당됩니다. 하지만 논리적 VLAN1 인터페이스(또는 이러한 스위치 포트에 설정한 모든 VLAN)를 수동으로 추가해 트래픽이 라우팅되고 FTD 보안 정책에 참여하게 해야 합니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 **Add Interfaces(**인터페이스 추가**)** > **VLAN Interface(VLAN** 인터페이스**)**를 클릭합니다.

단계 3 **General(**일반**)**에서 다음 VLAN 전용 매개변수를 설정합니다.



기존 VLAN 인터페이스를 편집한다면, **Associated Interface(**연결된 인터페이스**)** 테이블에는 이 VLAN의 스위치 포트가 표시됩니다.

a) 내부 사용을 위해 예약된 3968~4047 범위의 ID를 제외하고 1~4070의 **VLAN ID**를 설정합니다.

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

b) (선택 사항) **Disable Forwarding on Interface VLAN(Interface VLAN**에서의 포워딩 비활성화**)**의 VLAN ID를 클릭해 다른 VLAN에 대한 포워딩을 비활성화합니다.

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 포워딩을 비활성화할 수 있습니다. 비즈니스 네트워크에서는 홈 네트워크에 액세스할 수 있지만 홈 네트워크에서는 비즈니스 네트워크에 액세스할 수 없습니다.

단계 **4** 인터페이스 구성을 완료하려면 다음 절차 중 하나를 참조하십시오.

- 라우팅 모드 인터페이스 구성, 44 페이지
- 일반 브리지 그룹 멤버 인터페이스 파라미터 구성, 50 페이지

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(구축)** > **Deployment(구축)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

스위치 포트를 액세스 포트로 구성

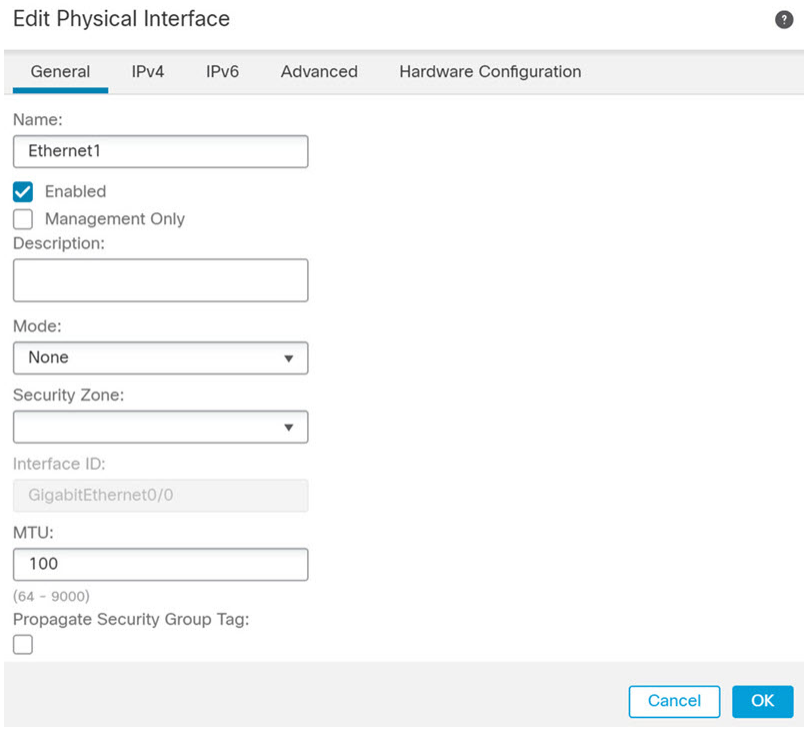
단일 VLAN에 스위치 포트를 할당하려면 해당 포트를 액세스 포트로 구성합니다. 액세스 포트에서는 태그 없는 트래픽만 허용됩니다. 기본적으로 이더넷 1/2~이더넷 1/8 스위치 포트는 VLAN 1에 할당됩니다.

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

프로시저

단계 **1** **Devices(디바이스)** > **Device Management(디바이스 관리)**를 선택하고 threat defense 디바이스에 대한 **Edit(수정)** ()를 클릭합니다. 기본적으로는 **Interfaces(인터페이스)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(수정)** ()을 클릭합니다.



단계 **3** **Enabled(활성화됨)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **4** (선택 사항) **Description(설명)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **5** **Port Mode(**포트 모드**)**를 **Access(**액세스**)**로 설정합니다.

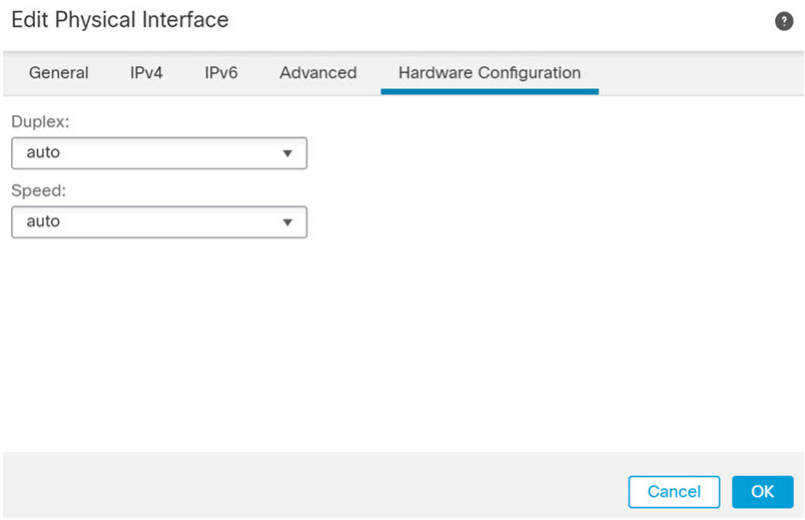
단계 **6** **VLAN ID** 필드에서 이 스위치 포트의 VLAN을 1~4070으로 설정합니다.

기본 VLAN ID는 1입니다.

단계 **7** (선택 사항) **Protected(**보호됨**)** 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, 각 스위치 포트에 **Protected(**보호됨**)**을 활성화하면 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.

단계 **8** (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.



Auto-negotiation(자동 협상**)** 확인란(기본값)을 선택해 속도와 듀플렉스를 자동으로 탐지합니다. 이 확인란 선택 취소하면 속도와 듀플렉스를 수동으로 설정할 수 있습니다.

- **Duplex(**듀플렉스**) - Full(**풀**)** 또는 **Half(**하프**)**를 선택합니다.
- **Speed(**속도**) - 10mbps**, **100mbps** 또는 **1gbps**를 선택합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

스위치 포트를 트렁크 포트로 구성

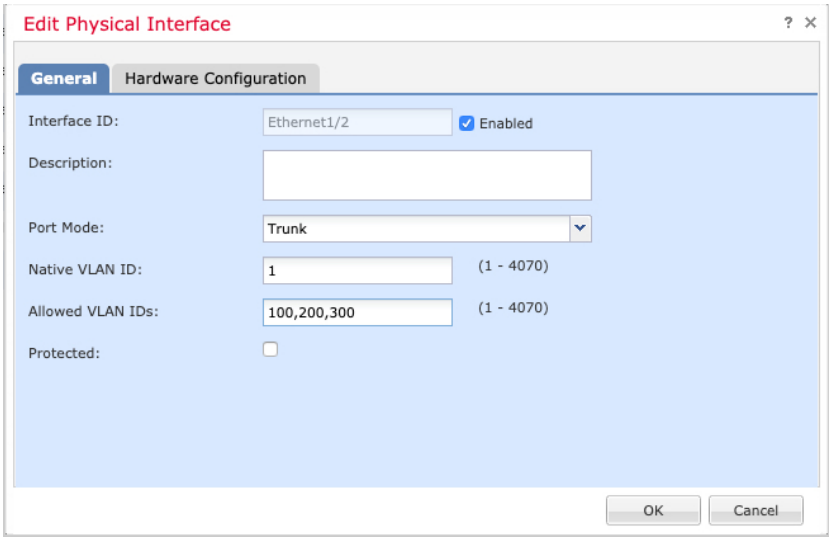
이 절차에서는 802.1Q 태깅을 사용하여 여러 VLAN을 전송할 수 있는 트렁크 포트를 생성하는 방법에 대해 설명합니다. 트렁크 포트의 경우 태그 없는 트래픽과 태그 있는 트래픽이 허용됩니다. 허용된 VLAN의 트래픽에서는 트렁크 포트가 변경되지 않은 상태로 전달됩니다.

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.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.



단계 **3** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **4** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **5** **Port Mode(**포트 모드**)**를 **Trunk(**트렁크**)**로 설정합니다.

단계 **6** **Native VLAN ID(**네이티브 **VLAN ID)** 필드에 이 스위치 포트의 네이티브 VLAN을 1~4070으로 설정합니다.

기본 네이티브 VLAN ID는 1입니다.

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

단계 **7** **Allowed VLAN IDs(**허용되는 **VLAN ID)** 필드에 이 트렁크 포트의 VLAN을 1~4070으로 입력합니다.

다음 방법 중 하나를 통해 최대 20개의 ID를 식별할 수 있습니다.

- 단일 번호(n)
- 범위(n-x)
- 쉼표로 구분된 번호와 범위는 다음 예와 같습니다.

  5,7-10,13,45-100

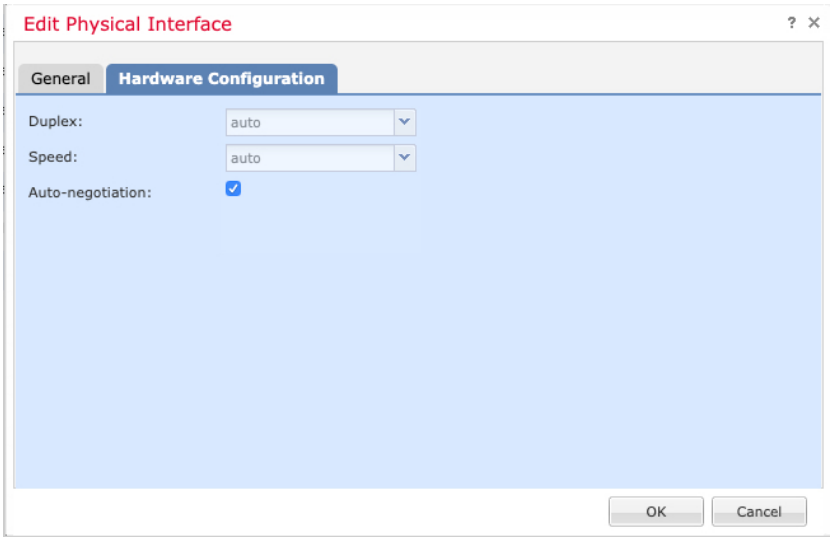
  쉼표 대신 공백을 입력해도 됩니다.

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.

단계 **8** (선택 사항) **Protected(**보호됨**)** 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, 각 스위치 포트에 **Protected(**보호됨**)**을 활성화하면 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.

단계 **9** (선택 사항) **Hardware Configuration(**하드웨어 컨피그레이션**)**을 클릭하여 듀플렉스 및 속도를 설정합니다.



Auto-negotiation(자동 협상**)** 확인란(기본값)을 선택해 속도와 듀플렉스를 자동으로 탐지합니다. 이 확인란 선택 취소하면 속도와 듀플렉스를 수동으로 설정할 수 있습니다.

- **Duplex(**듀플렉스**) - Full(**풀**)** 또는 **Half(**하프**)**를 선택합니다.

- **Speed(속도) - 10mbps**, **100mbps** 또는 **1gbps**를 선택합니다.

단계 **10** **OK(확인)**를 클릭합니다.

단계 **11** **Save(저장)**를 클릭합니다.

이제 **Deploy(구축)** > **Deployment(구축)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

PoE(Power over Ethernet) 구성

이더넷 1/7 및 이더넷 1/8에서는 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.

스위치 포트를 종료하거나 포트를 방화벽 인터페이스로 구성한다면, 디바이스의 전원을 비활성화해야 합니다.

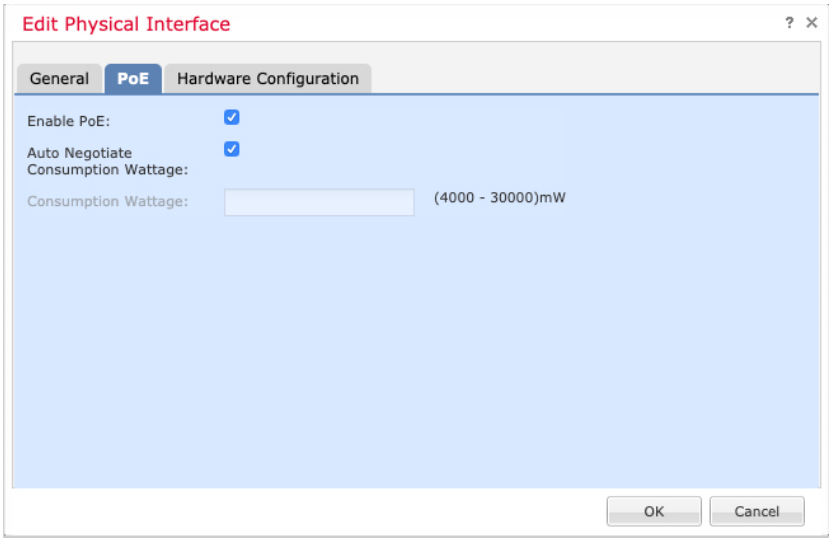
PoE는 이더넷 1/7 및 이더넷 1/8에서 기본적으로 활성화되어 있습니다. 이 절차에서는 PoE를 비활성화하는 방법과 활성화하는 방법, 파라미터(선택 사항)를 설정하는 방법을 설명합니다.

프로시저

단계 **1** **Devices(디바이스)** > **Device Management(디바이스 관리)**를 선택하고 threat defense 디바이스에 대한 **Edit(수정)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(인터페이스)** 페이지가 선택됩니다.

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

단계 **3** **PoE**를 클릭합니다.



단계 **4** **Enable PoE(PoE 활성화)** 확인란을 선택합니다.

PoE는 기본적으로 활성화되어 있습니다.

단계 **5** (선택 사항) 필요한 전력량을 정확하게 알고 있다면 **Auto Negotiate Consumption Wattage(**소비 전력량 자동 협상**)** 확인란을 선택 해제하고 **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 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

EtherChannel 인터페이스 구성

이 섹션에서는 EtherChannel 인터페이스를 구성하는 방법을 알려줍니다.

참고 Firepower 4100/9300의 경우 FXOS에 EtherChannel을 구성합니다. 자세한 내용은 EtherChannel(포트 채널) 추가를 참조하십시오.

EtherChannel

이 섹션에서는 EtherChannel를 설명합니다.

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 16개의 액티브 인터페이스를 포함할 수 있습니다. 단, 8개의 액티브 인터페이스를 지원하는Firepower 1000, 2100, Secure Firewall 3100 모델은 제외됩니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다. 16개의 액티브 인터페이스를 사용하려는 경우 스위치에서

해당 기능을 지원하는지 확인하십시오(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000).

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

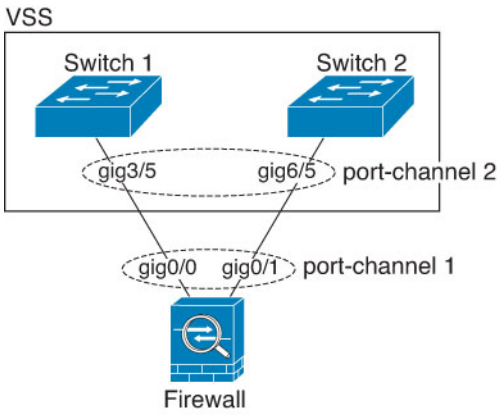
EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 소스 또는 목적지 MAC 주소, IP 주소, TCP 및 UDP 포트 번호, VLAN 번호를 기준으로 전용 해시 알고리즘을 사용하여 인터페이스를 선택합니다.

다른 디바이스에서 **EtherChannel**에 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 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다.

그림 ***1: VSS/vPC***에 연결

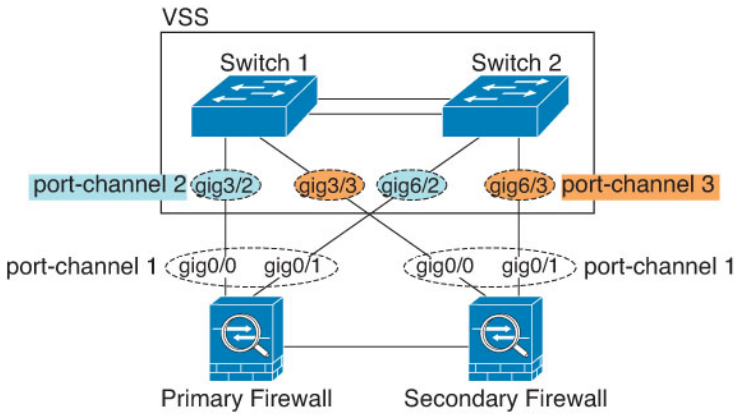


참고 threat defense 디바이스의 모드가 투명 방화벽 모드이고, 두 VSS/vPC 스위치 세트 사이에 threat defense 디바이스의 배치가 이루어지는 경우, EtherChannel을 사용하여 threat defense 디바이스에 연결된 모든 스위치 포트에서 UDLD(Unidirectional Link Detection)를 비활성화해야 합니다. UDLD를 활성화하면 스위치 포트가 다른 VSS/vPC 쌍의 두 스위치에서 제공되는 UDLD 패킷을 수신할 수 있습니다. 수신 스위치는 "UDLD 인접한 라우터 불일치"라는 이유와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

로 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.
- 패시브 — LACP 업데이트를 받습니다. 패시브 EtherChannel은 오로지 액티브 EtherChannel과 연결을 설정할 수 있습니다. 하드웨어 모델에서는 지원되지 않습니다.
- 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.

Firepower 및 Secure Firewall 하드웨어

포트 채널 인터페이스는 내부 인터페이스 Internal-Data 0/1의 MAC 주소를 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 직접 구성할 수도 있습니다. 섀시의 모든 EtherChannel 인터페이스는 동일한 MAC 주소를 사용하므로, 예를 들어 SNMP 폴링을 사용하는 경우 여러 인터페이스의 MAC 주소가 동일하다는 점에 유의하십시오.

참고 멤버 인터페이스는 재부팅 후 Internal-Data 0/1 MAC 주소만 사용합니다. 재부팅하기 전에 멤버 인터페이스는 자체 MAC 주소. 재부팅 후 새 멤버 인터페이스를 추가하는 경우 MAC 주소를 업데이트하려면 다시 재부팅해야 합니다.

EtherChannel용 가이드라인

브리지 그룹

라우팅 모드에서 Management Center정의 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(EtherChannel 인터페이스의 경우 장애 발생이 허용되는 멤버 인터페이스 수를 구성할 수 있음).

- 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

- Firepower 4100/9300용 management center 또는 threat defense virtual에서는 EtherChannel을 추가할 수 없습니다. Firepower 4100/9300에서는 EtherChannel을 지원하지만 사용자는 섀시의 FXOS에서 EtherChannel의 모든 하드웨어 구성을 수행해야 합니다.
- 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 16개의 액티브 인터페이스를 포함할 수 있습니다. 단, 8개의 액티브 인터페이스를 지원하는 Firepower 1000, 2100, Secure Firewall 3100 모델은 제외됩니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 수 있습니다. 16개의 액티브 인터페이스를 사용하려는 경우 스위치에서 해당 기능을 지원하는지 확인하십시오(예: F2-Series 10기가비트 이더넷 모듈이 포함된 Cisco Nexus 7000).
- 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. 이 경우 최저 공통 속도가 사용됩니다.
- 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.
- 다음 디바이스 모델은 LACP 빠른 속도를 지원하지 않습니다. LACP는 항상 일반 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.
  - Firepower 1000
  - Firepower 2100

  - Secure Firewall 3100

- 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 구성

이 섹션에서는 EtherChannel 포트 채널 인터페이스를 생성하고, EtherChannel에 인터페이스를 할당하며, EtherChannel을 맞춤화하는 방법에 대해 알아봅니다.

지침

- 모델용 인터페이스의 수에 따라 최대 48개의 EtherChannel을 구성할 수 있습니다.
- 각 채널 그룹에는 최대 8개의 액티브 인터페이스를 포함할 수 있습니다. 단, 16개의 액티브 인터페이스를 지원하는 ISA 3000은 제외됩니다. 액티브 인터페이스를 8개만 지원하는 스위치의 경우, 채널 그룹 하나에 최대 16개의 인터페이스를 할당할 수 있습니다. 이 중 8개만 액티브 인터페이스가 될 수 있으며, 나머지 인터페이스는 인터페이스 오류에 대비하여 스탠바이 링크 역할을 수행할 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. 이 경우 최저 공통 속도가 사용됩니다.

참고 Firepower 4100/9300의 경우 FXOS에 EtherChannel을 구성합니다. 자세한 내용은 EtherChannel(포트 채널) 추가를 참조하십시오.

시작하기 전에

- 해당 이름을 구성하지 않은 경우 물리적 인터페이스를 채널 그룹에 추가할 수 없습니다. 먼저 이름을 제거해야 합니다.

참고 컨피그레이션에서 물리적 인터페이스를 이미 사용 중인 경우, 이름을 제거하면 인터페이스에서 참조하는 모든 컨피그레이션이 지워집니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 2 물리적 인터페이스 활성화 및 이더넷 설정 구성에 따라 멤버 인터페이스를 활성화합니다.

단계 3 인터페이스 추가 > **EtherChannel** 인터페이스를 클릭합니다.

단계 4 **General(**일반**)** 탭에서 **Ether Channel ID**를 1에서 48까지의 숫자로(Firepower 1010에서는 1에서 8까지의 숫자로) 설정합니다.

단계 5 사용 가능한 인터페이스 영역에서 인터페이스를 클릭하고 추가를 클릭하여 선택된 인터페이스 영역으로 이동합니다. 멤버로 추가하려면 모든 인터페이스에 대해 반복합니다.

모든 인터페이스의 유형과 속도가 같은지 확인합니다.

단계 6 (선택 사항) EtherChannel을 사용자 정의하려면 고급 탭을 클릭합니다. 정보 하위 탭에서 다음 파라미터를 설정합니다.

- (ISA 3000만 해당) 로드 밸런싱 - 그룹 채널 인터페이스 전반에서 패킷 로드 밸런싱에 사용되는 기준을 선택합니다. 기본적으로 threat defense 디바이스는 패킷의 소스 및 대상 IP 주소에 따라 인터페이스에서 패킷 로드 밸런싱을 수행합니다. 패킷이 분류되는 속성을 변경하려면 다른 기준 집합을 선택합니다. 예를 들어 동일한 소스와 목적지 IP 주소에 트래픽이 심하게 편중된 경우 EtherChannel의 인터페이스에 트래픽 할당이 불균형해질 수 있습니다. 다른 알고리즘으로 변경할 경우 트래픽이 보다 고르게 분산될 수 있습니다. 로드 밸런싱에 대한 자세한 내용은 부하 균형, 14 페이지을 참조하십시오.
- **LACP** 모드 - 액티브, 패시브, 켜기를 선택합니다. 액티브 모드(기본값)를 사용하는 것이 좋습니다.
- (ISA 3000만 해당) 액티브 물리적 인터페이스: 범위 - 왼쪽의 드롭다운 목록에서 EtherChannel 시 액티브 상태여야 할 액티브 인터페이스의 최소 개수를 1~16 사이에서 선택합니다. 기본값은 1입니다. 오른쪽의 드롭다운 목록에서 EtherChannel에 허용되는 액티브 인터페이스의 최대 개수를 1~16 사이에서 선택합니다. 기본값은 16입니다. 스위치에서 16개의 액티브 인터페이스를 지원하지 않을 경우, 이 명령을 8 이하로 설정합니다.
- 액티브 **Mac** 주소 - 필요한 경우 수동 MAC 주소를 설정합니다. mac_address는 H.H.H 형식이며, 여기서 H는 16비트 16진수입니다. 예를 들어 MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력됩니다.

단계 7 하드웨어 구성 탭을 클릭하고 모든 멤버 인터페이스에 듀플렉스 및 속도를 설정합니다.

단계 8 **OK(**확인**)**를 클릭합니다.

단계 9 **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

단계 10 (선택 사항) VLAN 하위 인터페이스 추가 하위 인터페이스 추가, 26 페이지의 내용을 참조하십시오.

단계 **11** 라우팅 및 투명 모드 인터페이스 파라미터 구성 라우팅 모드 인터페이스 구성, 44 페이지 또는 브리지 그룹 인터페이스 구성, 50 페이지를 참조하십시오.

루프백 인터페이스 구성

이 섹션에서는 루프백 인터페이스를 구성하는 방법을 알려줍니다.

루프백 인터페이스 정보

루프백 인터페이스는 물리적 인터페이스를 에뮬레이트하는 소프트웨어 전용 인터페이스입니다. 이 인터페이스는 여러 물리적 인터페이스를 통해 IPv4 및 IPv6에서 연결할 수 있습니다. 루프백 인터페이스는 경로 장애를 극복 하는 데 도움이 됩니다. 모든 물리적 인터페이스에서 액세스할 수 있으므로 하나가 다운되 면 다른 인터페이스에서 루프백 인터페이스에 액세스할 수 있습니다.

루프백 인터페이스는 다음에 사용할 수 있습니다.

- 정적 및 동적 VTI 터널

threat defense는 동적 라우팅 프로토콜을 사용하여 루프백 주소를 배포할 수 있습니다. 또는 threat defense의 물리적 인터페이스 중 하나를 통해 루프백 IP 주소에 도달하도록 피어 디바이스에서 정적 경로를 구성할 수 있습니다. 루프백 인터페이스를 지정하는 threat defense에서는 정적 경로를 구성할 수 없습니다.

관련 항목

루프백 인터페이스에 대한 지침 및 제한 사항, 19 페이지
루프백 인터페이스 구성, 20 페이지

루프백 인터페이스에 대한 지침 및 제한 사항

방화벽 모드

- 라우팅 모드에서만 지원됩니다.

고가용성 및 클러스터링

- 클러스터링은 지원되지 않습니다.

추가 지침 및 제한

- TCP 시퀀스 임의 설정은 물리적 인터페이스에서 루프백 인터페이스로의 트래픽에 대해 항상 비활성화됩니다.

루프백 인터페이스 구성

디바이스의 루프백 인터페이스를 추가하려면:

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** **Add Interfaces(**인터페이스 추가**)** 드롭다운 목록에서 **Loopback Interface(**루프백 인터페이스**)**를 선택합니다.

단계 **3** **General(**일반**)** 탭에서 다음 매개변수를 구성합니다.

a) **Name(**이름**)**—루프백 인터페이스의 이름을 입력합니다.

b) **Enabled(**활성화됨**)**—루프백 인터페이스를 활성화하려면 이 확인란을 선택합니다.

c) **Loopback ID(**루프백 **ID)** — 1에서 1024 사이의 루프백 ID를 입력합니다.

d) **Description(**설명**)** - 루프백 인터페이스에 대한 설명을 입력합니다.

단계 **4** 라우팅 모드 인터페이스 매개변수를 구성합니다. 라우팅 모드 인터페이스 구성, 44 페이지의 내용을 참조하십시오.

루프백 인터페이스에 대한 트래픽 속도 제한

시작하기 전에

시스템의 과부하를 방지하기 위해 루프백 인터페이스 IP 주소로 이동하는 트래픽의 속도를 제한해야 합니다. 전역 서비스 정책에 연결 제한 규칙을 추가할 수 있습니다.

프로시저

단계 **1** 루프백 인터페이스 IP 주소의 트래픽을 식별하는 확장 액세스 목록을 생성합니다.

a) **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하고 목차에서 **Access Control Lists(**액세스 제어 목록**)** > **Extended(**확장**)**를 선택합니다.

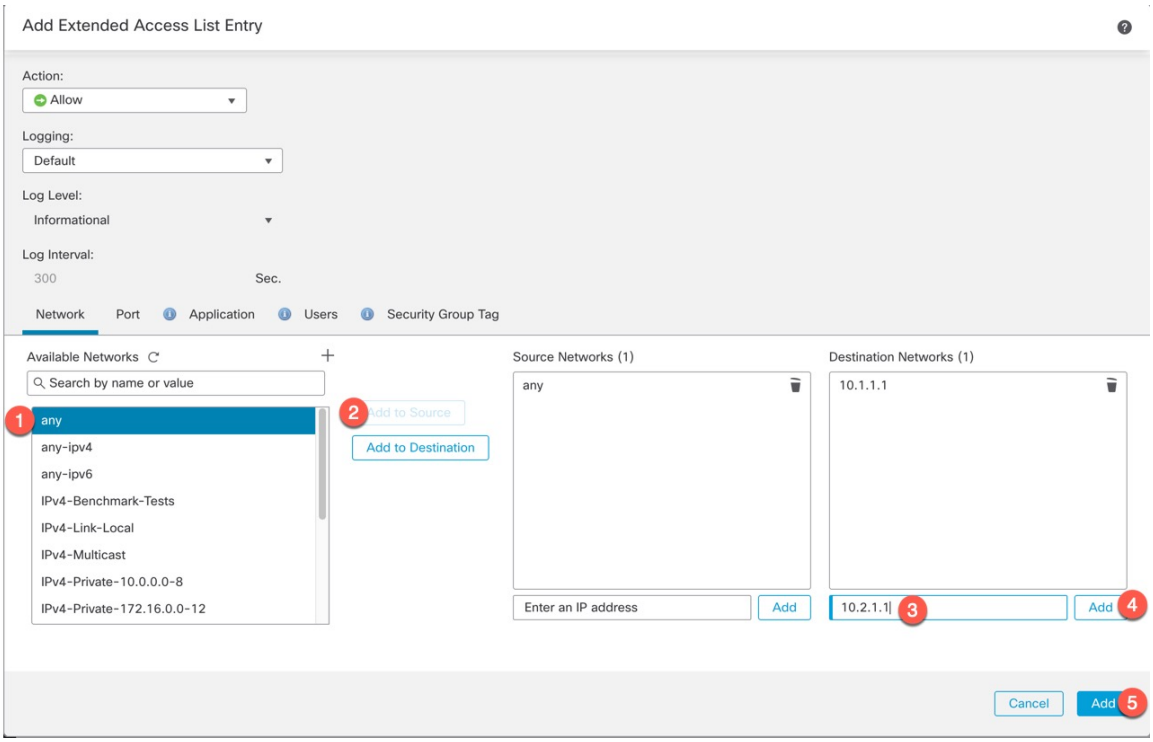
b) **Add Extended Access List(**확장된 액세스 목록 추가**)**를 클릭하여 새 ACL을 생성합니다.

c) **New Extended Access List Object(**새 확장 액세스 목록 개체**)** 대화 상자에서 ACL의 이름을 입력하고(공백은 허용되지 않음) **Add(**추가**)**를 클릭하여 새 항목을 생성합니다.

그림 ***3: ACL*** 이름 지정 및 항목 추가

d) **Network(**네트워크**)** 탭에서 소스(임의) 및 수신 주소(루프백 IP 주소)를 구성합니다.

그림 ***4:*** 소스 및 대상 네트워크



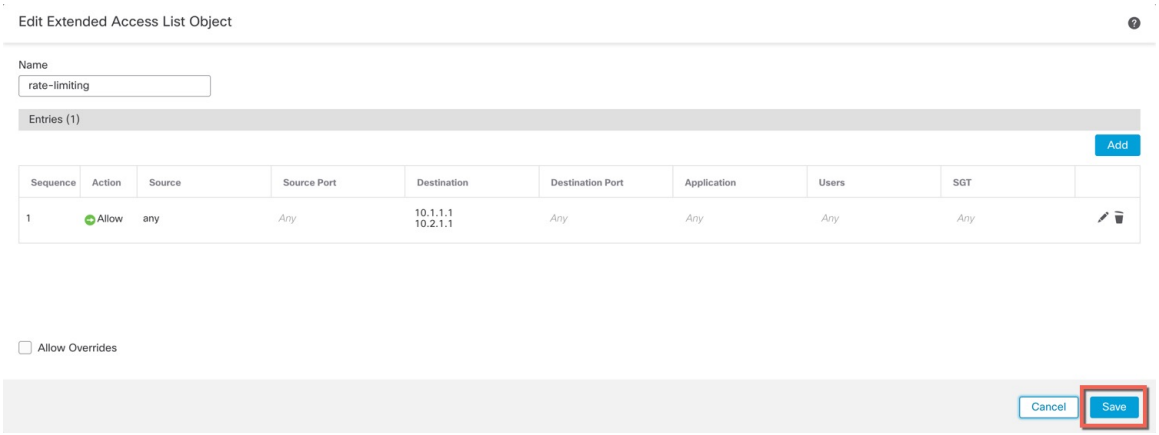
참고 기본 **Action(**작업**)**을 **Allow(**허용**)**(일치)로 유지하고 기타 설정을 있는 그대로 유지합니다.

- Source(소스) - **Available Networks(**사용 가능한 네트워크**)** 목록에서 **any(**임의**)**를 선택하고 **Add to Source(**소스에 추가**)**를 클릭합니다. **any(**임의**)** 대신 소스 IP 주소를 지정하여 이 액세스 목록의 범위를 좁힐 수도 있습니다.
- Destination(대상) - **Destination Networks(**대상 네트워크**)** 목록 아래의 편집 상자에 주소를 입력하고 **Add(**추가**)**를 클릭합니다. 각 루프백 인터페이스에 대해 이 작업을 반복합니다.

e) **Add(**추가**)**를 클릭하여 ACL에 항목을 추가합니다.

f) **Save(**저장**)**를 클릭하여 ACL을 저장합니다.

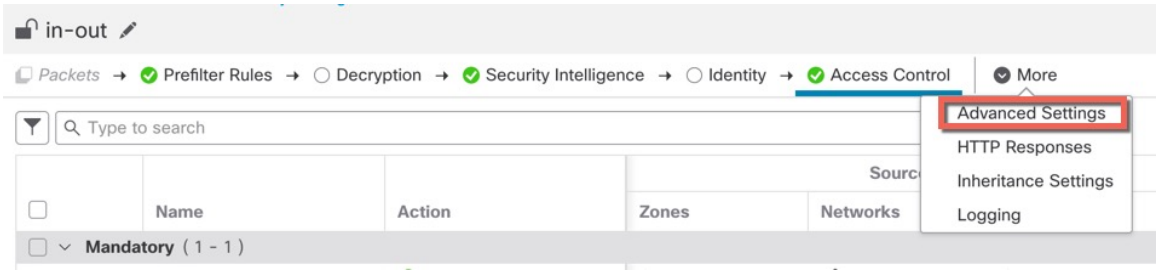
그림 ***5: ACL*** 저장



단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)**을 선택하고 디바이스에 할당된 액세스 제어 정책에 대해 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운에서 **Advanced Settings(**고급 설정**)**를 클릭합니다.

그림 ***6: Advanced Settings(***고급 설정***)***

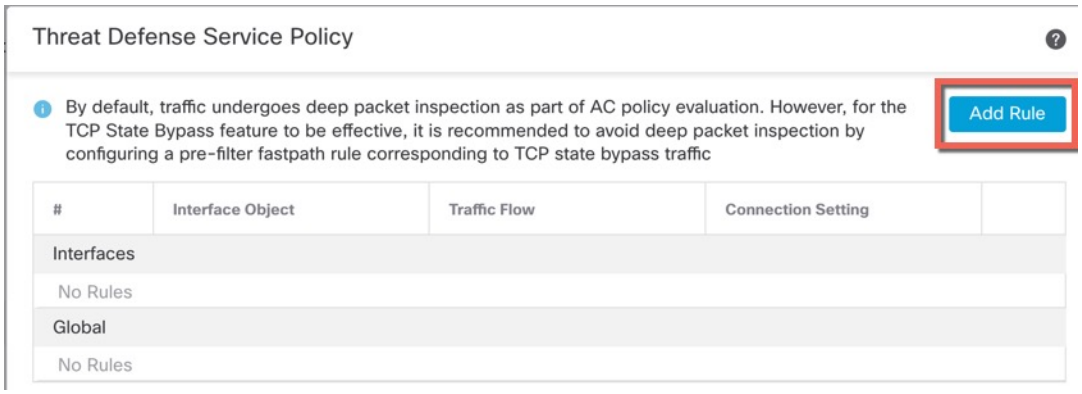


단계 **4** **Threat Defense Service Policy(Threat Defense Service** 정책**)** 그룹에서 **Edit(**수정**)** (✎)을 클릭합니다.

그림 ***7:*** 위협 방어 서비스 정책

단계 **5** **Add Rule(**규칙 추가**)**을 클릭하여 새로운 규칙을 추가합니다.

그림 *8:* 규칙 추가



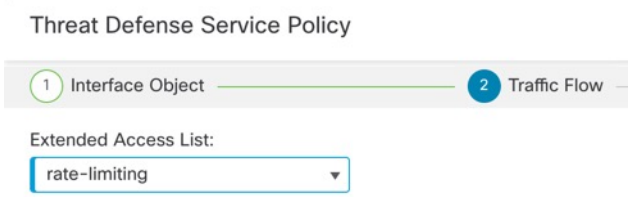
서비스 정책 규칙 마법사가 열리고 규칙을 구성하는 과정을 단계별로 안내합니다.

단계 **6** **Interface Object(**인터페이스 개체**)** 단계에서 **Global(**전역**)**을 클릭하여 모든 인터페이스에 적용되는 전역 규칙을 생성하고 **Next(**다음**)**를 클릭합니다.

그림 *9:* 전역 정책

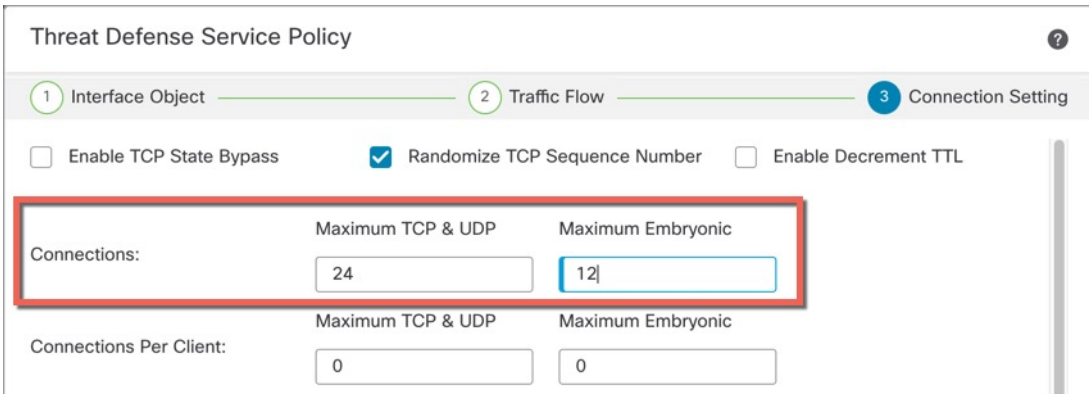
단계 **7** **Traffic Flow(**트래픽 플로우**)** 단계에서는 단계 1, 20 페이지단계에서 생성한 확장 액세스 목록 개체를 선택하고 **Next(**다음**)**를 클릭합니다.

그림 *10:* 확장 액세스 목록 선택



단계 **8** **Connection Setting(**연결 설정**)** 단계에서 **Connections(**연결**)** 제한을 설정합니다.

그림 *11:* 연결 제한 설정



Maximum TCP & UDP(최대 **TCP** 및 **UDP)** 연결 수를 루프백 인터페이스에 대한 예상 연결 수로 설정하고 **Maximum Embryonic**(최대 원시) 연결 수를 더 낮은 수로 설정합니다. 예를 들어, 필요한 예상 루프백 인터페이스 세션에 따라 5/2, 10/5 또는 1024/512로 설정할 수 있습니다.

원시 연결 수 제한을 설정하면 TCP 인터셉트를 통해 TCP SYN 패킷을 인터페이스에 플러딩하는 수법의 DoS 공격으로부터 시스템을 보호할 수 있습니다.

단계 **9** 변경 사항을 저장하려면 **Finish(**마침**)**를 클릭합니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Advanced Settings(**고급 설정**)** 창에서 **Save(**저장**)**를 클릭합니다.

단계 **12** 이제 영향을 받는 디바이스에 변경 사항을 구축할 수 있습니다.

VLAN 하위 인터페이스 및 802.1Q 트렁킹 구성

VLAN 하위 인터페이스를 사용하면 물리적, 이중 또는 EtherChannel 인터페이스를 다른 VLAN ID가 태그 처리된 여러 논리적 인터페이스로 분할할 수 있습니다. 하나 이상의 VLAN 하위 인터페이스가 포함된 인터페이스는 자동으로 802.1Q 트렁크로 구성됩니다. VLAN을 사용하면 주어진 물리적 인터페이스에서 트래픽을 분리할 수 있으므로 추가로 물리적 인터페이스 또는 디바이스를 추가하지 않고도 네트워크에 사용 가능한 인터페이스 수를 늘릴 수 있습니다.

VLAN 하위 인터페이스에 대한 가이드라인 및 제한 사항

모델 지원

- Firepower 1010 - VLAN 하위 인터페이스는 스위치 포트 또는 VLAN 인터페이스에서 지원되지 않습니다.

높은 가용성 및 클러스터링

페일오버 또는 상태 링크용 또는 클러스터 제어 링크용 하위 인터페이스를 사용할 수 없습니다. 다중 인스턴스 모드의 경우는 예외입니다. 이러한 링크에 대해 섀시 정의 하위 인터페이스를 사용할 수 있습니다.

추가 지침

- 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. 이러한 속성은 이중 인터페이스 쌍의 물리적 인터페이스 및 EtherChannel 링크에서도 마찬가지입니다. 하위 인터페이스에서 트래픽을 전달하려면 물리적, 이중화 또는 EtherChannel 인터페이스를 활성화해야 하므로, 인터페이스 이름을 설정하지 않음으로써 물리적, 이중화 또는 EtherChannel 인터페이스가 트래픽을 전달하지 않도록 합니다. 물리적, 이중화 또는 EtherChannel 인터페이스에서 태그되지 않은 패킷을 전달하려면 평소와 같이 이름을 구성합니다.
- 관리 인터페이스에서는 하위 인터페이스를 구성할 수 없습니다.
- 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 defense에 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 defense의 특정 인스턴스에서 트래픽이 중단되는 것을 방지할 수 있습니다.

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

모델	**VLAN** 하위 인터페이스의 최대 수
Firepower 4100	1024
Firepower 9300	1024
Threat Defense Virtual	50
ISA 3000	100

하위 인터페이스 추가

물리적, 이중 또는 포트 채널 인터페이스에 하나 이상의 하위 인터페이스를 추가합니다.

Firepower 4100/9300의 경우 컨테이너 인스턴스와 함께 사용하기 위해 FXOS에서 하위 인터페이스를 구성할 수 있습니다. 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가를 참조하십시오. 이러한 하위 인터페이스는 management center 인터페이스 목록에 표시됩니다. management center에 하위 인터페이스를 추가할 수도 있습니다. 그러나 FXOS에서 정의된 하위 인터페이스가 아직 없는 상위 인터페이스에서만 가능합니다.

참고 상위 물리적 인터페이스는 태그가 지정되지 않은 패킷을 전달합니다. 태그가 지정되지 않은 패킷을 전달하고 싶지 않은 경우 보안 정책에 상위 인터페이스를 포함하지 않아야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 물리적 인터페이스 활성화 및 이더넷 설정 구성에 따라 상위 인터페이스를 활성화합니다.

단계 **3** 인터페이스 추가 > 하위 인터페이스를 클릭합니다.

단계 **4** 일반에서 다음 파라미터를 설정합니다.

a) 인터페이스 - 하위 인터페이스에 추가할 물리적, 이중화 또는 포트 채널 인터페이스를 선택합니다.

b) 하위 인터페이스 **ID** - 하위 인터페이스 ID를 1~4294967295 사이의 정수로 입력합니다. 허용되는 하위 인터페이스의 개수는 플랫폼에 따라 다릅니다. 다음을 설정한 후에는 ID를 변경할 수 없습니다.

c) **VLAN ID** - 이 하위 인터페이스에서 패킷에 태그를 지정하는 데 사용할 1~4094 사이의 VLAN ID를 입력합니다.

이 VLAN ID에는 상위 인터페이스에 대해 고유한 에서는 이 VLAN을 재사용할 수 있습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(구축)** > **Deployment(구축)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

단계 **7** 라우팅 및 투명 모드 인터페이스 파라미터 구성 라우팅 모드 인터페이스 구성, 44 페이지 또는 브리지 그룹 인터페이스 구성, 50 페이지를 참조하십시오.

VXLAN 인터페이스 구성

이 장에서는 VXLAN(확장 가능 가상 LAN) 인터페이스를 구성하는 방법을 알려 줍니다. VXLAN 인터페이스는 Layer 2 네트워크를 확장하기 위해 Layer 3 물리적 네트워크에서 Layer 2 가상 네트워크 역할을 합니다.

VXLAN 인터페이스 정보

VXLAN은 VLAN과 동일한 이더넷 Layer 2 네트워크 서비스를 제공하지만 확장성과 유연성이 우수합니다. VLAN에 비해 VXLAN은 다음과 같은 이점을 제공합니다.

- 데이터 센터 전체에서 다중 테넌시 세그먼트를 유연하게 배치합니다.
- 더 많은 Layer 2 세그먼트를 해결하기 위한 우수한 확장성: 최대 1600만 개의 VXLAN 세그먼트.

이 섹션에서는 VXLAN의 작동 방식을 설명합니다. VXLAN에 대한 자세한 정보는 RFC 7348을 참조하십시오. Geneve에 대한 자세한 내용은 RFC 8926을 참조하십시오.

캡슐화

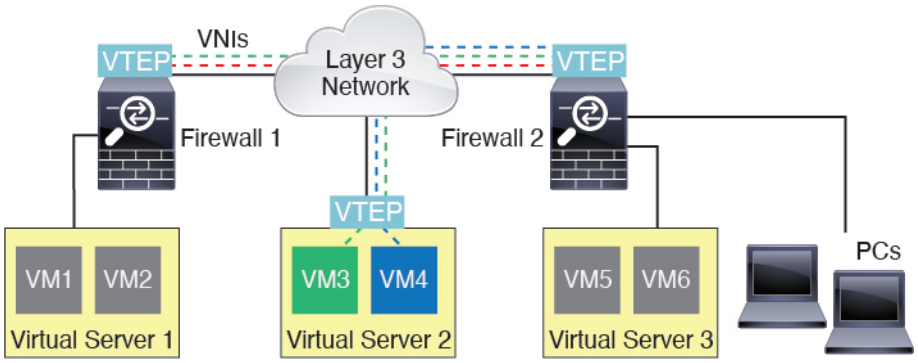
threat defense는 두 가지 유형의 VXLAN 캡슐화를 지원합니다.

- VXLAN(모든 모델)—VXLAN은 MAC-in-UDP(사용자 데이터그램 프로토콜의 MAC 주소) 캡슐화를 사용합니다. 원래의 Layer 2 프레임에는 VXLAN 헤더가 추가됩니다. 그런 다음 UDP-IP 패킷에 배치됩니다.
- Geneve(threat defense virtual만 해당) - Geneve에는 MAC 주소로 제한되지 않는 유연한 내부 헤더가 있습니다. Geneve 캡슐화는 AWS(Amazon Web Services) 게이트웨이 로드 밸런서와 어플라이언스 간에 패킷을 투명하게 라우팅하고 추가 정보를 전송하는 데 필요합니다.

VXLAN 터널 엔드포인트

VXLAN 터널 엔드포인트(VTEP) 디바이스는 VXLAN 캡슐화 및 역캡슐화를 수행합니다. 각 VTEP에는 2개의 인터페이스 유형이 있습니다. VNI(VXLAN 네트워크 식별자) 인터페이스라고 하는 하나 이상의 가상 인터페이스에는 보안 정책이 적용되며 VTEP 소스 인터페이스라고 하는 일반 인터페이스는 VTEP 사이에서 VNI 인터페이스를 터널링합니다. VTEP 소스 인터페이스는 VTEP대 VTEP 통신을 위해 전송 IP 네트워크에 연결됩니다.

다음 그림은 여러 사이트 사이에서 VNI 1, 2, 3 네트워크를 확장하여 Layer 3 네트워크 전체에서 VTEP 역할을 수행하는 2개의 threat defense 및 가상 서버 2를 보여 줍니다. threat defense는 VXLAN 및 VXLAN 이외 네트워크 간의 브리지 또는 게이트웨이 역할을 수행합니다.



VTEP 간의 기반 IP 네트워크는 VXLAN 오버레이와 상관이 없습니다. 캡슐화된 패킷은 소스 IP 주소로 시작 VTEP 및 대상 IP 주소로 종료 VTEP가 있는 외부 IP 주소 헤더에 기반하여 라우팅됩니다. VXLAN 캡슐화의 경우: 대상 IP 주소는 원격 VTEP가 알려지지 않은 경우 멀티캐스트 그룹일 수 있습니다. Geneve에서는 threat defense만 고정 피어를 지원합니다. VXLAN의 대상 포트는 기본적으로 UDP 포트 4789입니다(사용자가 구성 가능). Geneve의 대상 포트는 6081입니다.

VTEP 소스 인터페이스

VTEP 소스 인터페이스는 모든 VNI 인터페이스를 연결할 일반 인터페이스(물리적, EtherChannel 또는 VLAN)입니다. threat defense virtual별로 1개의 VTEP 소스 인터페이스를 구성할 수 있습니다. 하나의 VTEP 소스 인터페이스만 구성할 수 있으므로 동일한 디바이스에서 VXLAN 및 Geneve 인터페이스를 모두 구성할 수는 없습니다. AWS 또는 Azure에서의 threat defense virtual 클러스터링에는 예외가 있습니다. 여기서 2개의 VTEP 소스 인터페이스를 사용할 수 있습니다. VXLAN 인터페이스는 클러스터 제어 링크에 사용되고 Geneve(AWS) 또는 VXLAN(Azure) 인터페이스는 게이트웨이 로드 밸런서에 사용할 수 있습니다.

VTEP 소스 인터페이스는 VXLAN 트래픽에 사용하도록 제한되지 않는 경우에도 VXLAN 트래픽에 모두 사용될 수 있습니다. 필요 시, 일반 트래픽에 이 인터페이스를 사용하고 해당 트래픽에 대한 인터페이스에 보안 정책을 적용할 수 있습니다. 단, VXLAN 트래픽의 경우 모든 보안 정책을 VNI 인터페이스에 적용해야 합니다. VTEP 인터페이스는 물리적 포트로만 사용됩니다.

투명한 방화벽 모드에서, VTEP 소스 인터페이스는 BVI의 일부가 아니며 관리 인터페이스가 처리되는 방식과 유사하게 이 인터페이스에 대해 IP 주소를 구성합니다.

VNI 인터페이스

VNI 인터페이스는 VLAN 인터페이스와 유사합니다. 이 인터페이스는 네트워크 트래픽을 태그 지정을 사용하여 지정된 물리적 인터페이스에서 분리되게 유지하는 가상 인터페이스입니다. 각 VNI 인터페이스에 보안 정책을 직접 적용하십시오.

VTEP 인터페이스는 하나만 추가할 수 있으며 모든 VNI 인터페이스는 동일한 VTEP 인터페이스와 연결되어 있습니다.AWS 또는 Azure에서의 threat defense virtual 클러스터링에 대한 예외가 있습니다. AWS 클러스터링의 경우 VXLAN 인터페이스가 클러스터 제어 링크에 사용되고 Generve 인터페이스가 AWS 게이트웨이 로드 밸런서에 사용될 수 있다는 두 가지 VTEP 소스 인터페이스를 사용할 수 있

습니다.Azure 클러스터링의 경우 VXLAN 인터페이스가 클러스터 제어 링크에 사용되고 두 번째 VXLAN 인터페이스가 Azure 게이트웨이 로드 밸런서에 사용될 수 있다는 두 가지 VTEP 소스 인터페이스를 사용할 수 있습니다.

VXLAN 패킷 처리

VXLAN

VTEP 소스 인터페이스를 드나드는 트래픽은 VXLAN 처리, 특히 캡슐화 또는 역캡슐화 과정을 거칩니다.

캡슐화 처리에는 다음 작업이 포함됩니다.

- VTEP 소스 인터페이스는 VXLAN 헤더가 있는 내부 MAC 프레임을 캡슐화합니다.
- UDP 체크섬 필드가 0으로 설정됩니다.
- 외부 프레임 소스 IP가 VTEP 인터페이스 IP로 설정됩니다.
- 외부 프레임 대상 IP는 원격 VTEP IP 조회에 따라 결정됩니다.

역캡슐화: threat defense는 다음 경우에 VXLAN 패킷에 역캡슐화만 수행합니다.

- 대상 포트가 4789로 설정된 UDP 패킷인 경우(이 값은 사용자가 구성 가능함).
- 인그레스 인터페이스가 VTEP 소스 인터페이스입니다.
- 인그레스 인터페이스 IP 주소가 대상 IP 주소와 동일합니다.
- VXLAN 패킷 형식은 표준을 준수합니다.

Geneve

VTEP 소스 인터페이스를 드나드는 트래픽은 Geneve 처리, 특히 캡슐화 또는 역캡슐화 과정을 거칩니다.

캡슐화 처리에는 다음 작업이 포함됩니다.

- VTEP 소스 인터페이스는 Geneve 헤더가 있는 내부 MAC 프레임을 캡슐화합니다.
- UDP 체크섬 필드가 0으로 설정됩니다.
- 외부 프레임 소스 IP가 VTEP 인터페이스 IP로 설정됩니다.
- 외부 프레임 대상 IP는 구성한 피어 IP 주소로 설정됩니다.

역캡슐화: ASA에서는 다음과 같은 경우 Geneve 패킷에 역캡슐화만 수행합니다.

- 대상 포트가 6081로 설정된 UDP 패킷인 경우(이 값은 사용자가 구성 가능함).
- 인그레스 인터페이스가 VTEP 소스 인터페이스입니다.
- 인그레스 인터페이스 IP 주소가 대상 IP 주소와 동일합니다.
- Geneve 패킷 형식은 표준을 준수합니다.

피어 VTEP

threat defense에서 피어 VTEP 뒤쪽의 디바이스에 패킷을 보낼 경우 threat defense에서는 2가지 중요한 정보가 필요합니다.

- 원격 디바이스의 대상 MAC 주소
- 피어 VTEP의 대상 IP 주소

threat defense는 VNI 인터페이스에 대한 원격 VTEP IP 주소로의 대상 MAC 주소 매핑을 유지합니다.

VXLAN 피어

threat defense가 이 정보를 찾을 수 있는 방법은 다음의 2가지 방법이 있습니다.

- 단일 피어 VTEP IP 주소를 threat defense에서 정적으로 구성할 수 있습니다.

  그런 다음 threat defense는 엔드 노드 MAC 주소를 확인하기 위해 VTEP에 VXLAN 캡슐화 ARP 브로드캐스트를 전송합니다.

- threat defense에서 피어 VTEP IP 주소 그룹을 정적으로 구성할 수 있습니다.

  그런 다음 threat defense는 엔드 노드 MAC 주소를 확인하기 위해 VTEP에 VXLAN 캡슐화 ARP 브로드캐스트를 전송합니다.

- 멀티캐스트 그룹은 각각의 VNI 인터페이스에서 구성될 수 있습니다(또는 VTEP에서 전체로 구성 가능).

  threat defense는 VTEP 소스 인터페이스를 통해 IP 멀티캐스트 패킷 내에서 VXLAN 캡슐화 ARP 브로드캐스트 패킷을 전송합니다. 이 ARP 요청에 대한 응답을 통해 threat defense는 원격 엔드 노드의 대상 MAC 주소와 함께 원격 VTEP IP 주소를 확인할 수 있습니다.

  이 옵션은 Geneve에서는 지원되지 않습니다.

Geneve 피어

threat defense virtual는 정적으로 정의된 피어만 지원합니다. AWS 게이트웨이 로드 밸런서에서 threat defense virtual 피어 IP 주소를 정의할 수 있습니다. threat defense virtual는 게이트웨이 로드 밸런서에 대한 트래픽을 시작하지 않으므로 threat defense virtual에서 게이트웨이 로드 밸런서 IP 주소를 지정할 필요가 없습니다. Geneve 트래픽을 수신할 때 피어 IP 주소를 학습합니다. 멀티캐스트 그룹은 Geneve에서 지원되지 않습니다.

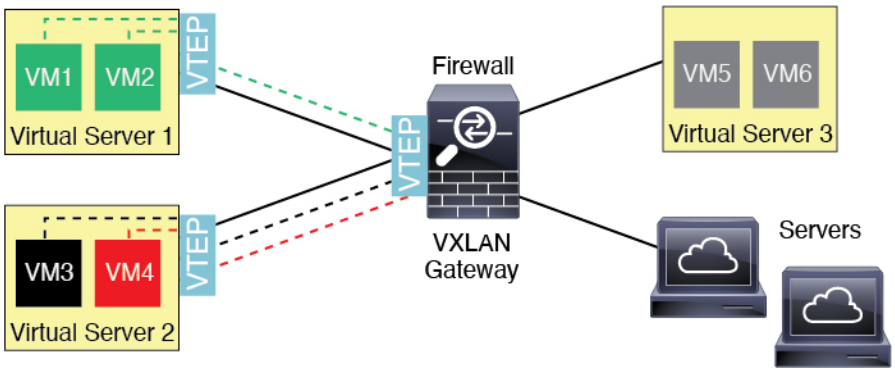
VXLAN 사용 사례

이 섹션에서는 threat defense에서의 VXLAN 구현에 대한 사용 사례를 설명합니다.

VXLAN 브리지 또는 게이트웨이 개요

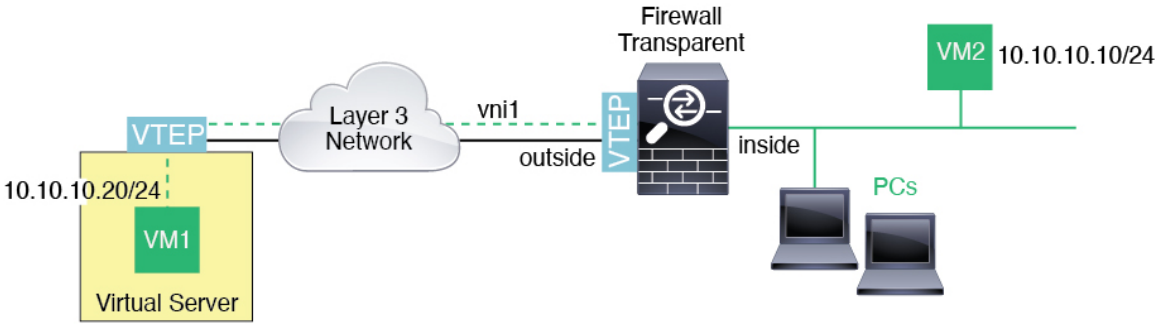
각 threat defense VTEP는 VM, 서버, PC 및 VXLAN 오버레이 네트워크 등의 엔드 노드 사이에서 브리지 또는 게이트웨이 역할을 합니다. VTEP 소스 인터페이스에서 VXLAN 캡슐화를 통해 받은 수신 프레임의 경우 threat defense는 VXLAN 헤더를 제거하여 이 헤더를 내부 이더넷 프레임의 대상 MAC 주소에 기반하는 VXLAN 이외 네트워크에 연결되어 있는 물리적 인터페이스에 전달합니다.

threat defense는 항상 VXLAN 패킷을 처리하며 2개의 다른 VTEP 사이에서 원래 상태로 있는 VXLAN 패킷은 전달하지 않습니다.



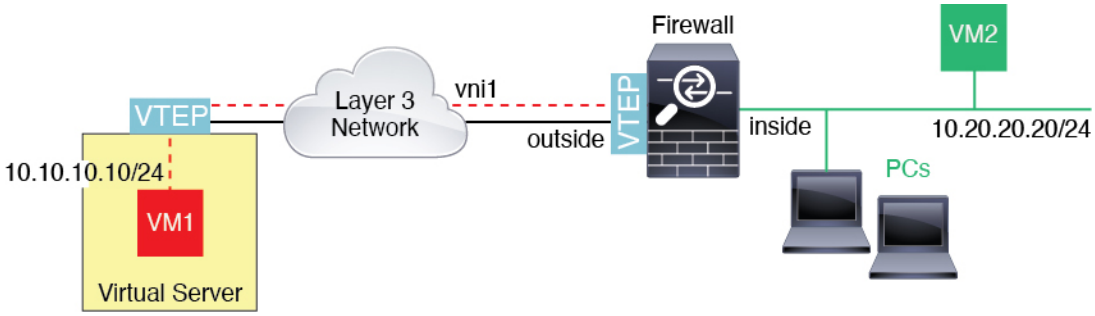
VXLAN 브리지

투명한 방화벽 모드 또는 라우팅 모드(선택 사항)에서 브리지 그룹을 사용할 경우, threat defense에서는 동일한 네트워크에 있는 원격 VXLAN 세그먼트와 로컬 세그먼트 사이에서 VXLAN 브리지 역할을 수행할 수 있습니다. 이 경우, 브리지 그룹의 한 멤버는 일반 인터페이스이며 이때 다른 멤버는 VNI 인터페이스입니다.



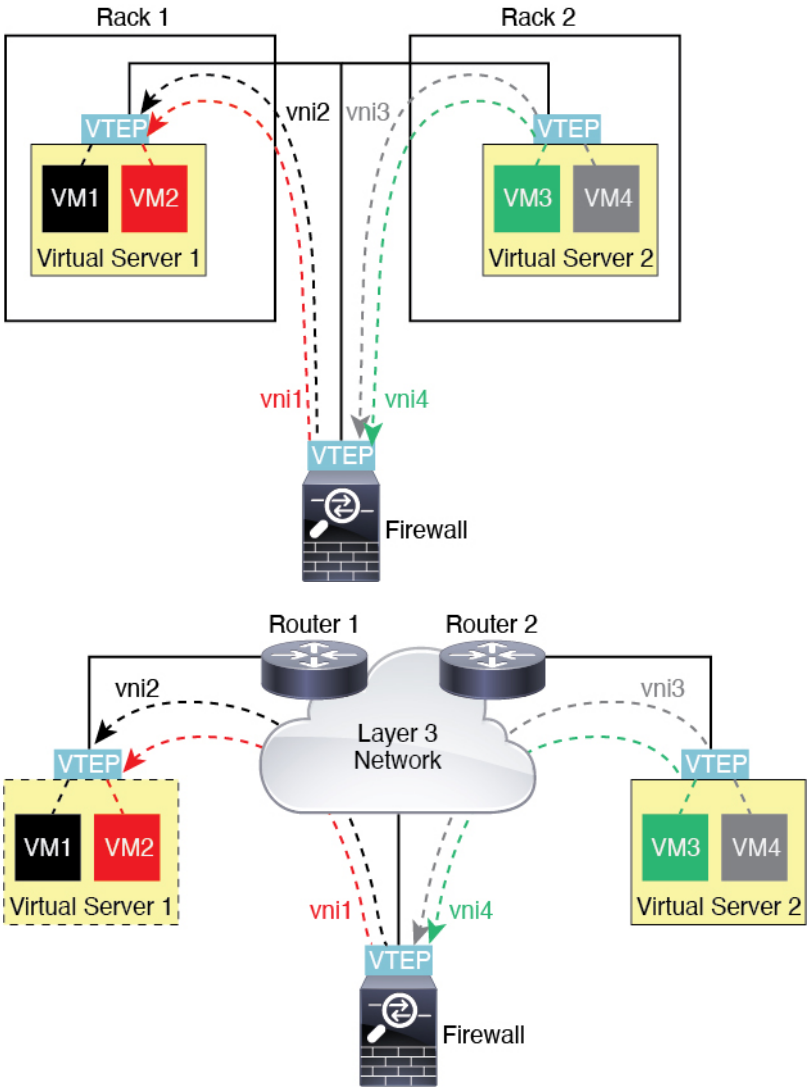
VXLAN 게이트웨이(라우팅 모드)

threat defense는 다른 네트워크에 있는 디바이스를 연결하여 VXLAN과 VXLAN 이외 도메인 사이에서 라우터 역할을 수행할 수 있습니다.



VXLAN 도메인 사이의 라우터

VXLAN 확장 Layer 2 도메인에서 VM은 threat defense가 동일한 랙에 있지 않은 경우 또는 threat defense가 Layer 3 네트워크 상에서 멀리 있는 경우에도 게이트웨이로 threat defense를 가리킬 수 있습니다.



이 시나리오에 대한 다음 주의사항을 참조하십시오.

1. VM3~VM1 패킷의 경우, threat defense가 기본 게이트웨이이므로 대상 MAC 주소는 threat defense MAC 주소입니다.
2. 가상 서버 2의 VTEP 소스 인터페이스에서 VM3로부터 패킷을 수신하고 VNI 3의 VXLAN 태그로 패킷을 캡슐화한 다음 threat defense에 전송합니다.
3. threat defense가 이 패킷을 수신하면 내부 프레임을 얻기 위해 패킷을 역캡슐화합니다.
4. threat defense는 경로 조회를 위해 내부 프레임을 사용한 다음 해당 대상이 VNI 2에 있는지 찾습니다. VM1에 대한 매핑이 없는 경우, threat defense는 VNI 2에서 멀티캐스트 그룹 IP에 대해 캡슐화 ARP 브로드캐스트를 전송합니다.

참고 이 시나리오에서 threat defense는 여러 VTEP 피어를 지니므로 동적 VTEP 피어 검색을 사용해야 합니다.

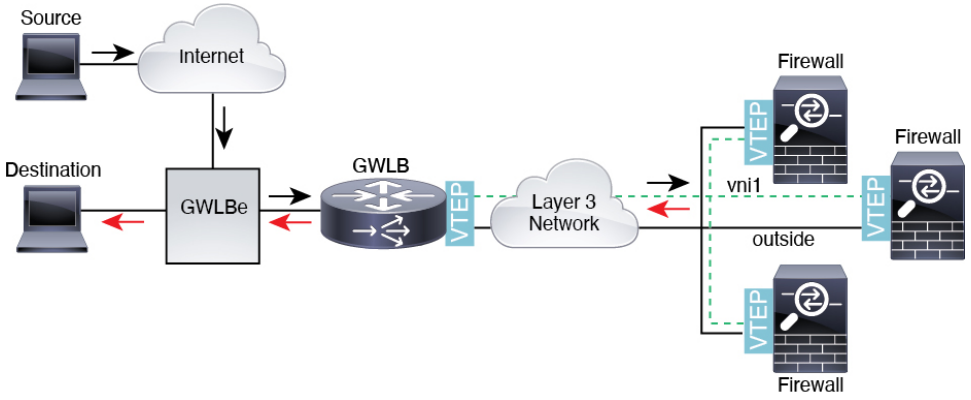
5. threat defense는 VNI 2에 대한 VXLAN 태그를 사용하여 패킷을 다시 캡슐화한 다음 이 패킷을 가상 서버 1에 전송합니다. 캡슐화하기 전에 threat defense는 내부 프레임 대상 MAC 주소를 VM1의 MAC로 변경합니다(threat defense가 VM1 MAC 주소를 파악하는 데 멀티캐스트 캡슐화 ARP가 필요할 수 있음).
6. 가상 서버 1에서 VXLAN 패킷을 수신하는 경우 패킷을 역캡슐화하고 내부 프레임을 VM1에 제공합니다.

Geneve 단일 암 프록시

참고 이 사용 사례는 Geneve 인터페이스에 대해 현재 지원되는 유일한 사용 사례입니다.

AWS 게이트웨이 로드 밸런서는 트래픽을 분산하고 온디맨드 방식으로 가상 어플라이언스를 확장하는 로드 밸런서와 투명 네트워크 게이트웨이를 결합합니다. 위협 대응 가상는 분산형 데이터 플레인(게이트웨이 로드 밸런서 엔드포인트)이 있는 게이트웨이 로드 밸런서 중앙 집중식 제어 평면을 지원합니다. 다음 그림에는 게이트웨이 로드 밸런서 엔드포인트에서 게이트웨이 로드 밸런서로 전달되는 트래픽이 나와 있습니다. 게이트웨이 로드 밸런서는 여러 위협 대응 가상 간에 트래픽을 밸런싱하며, 이를 삭제하거나 게이트웨이 로드 밸런서로 다시 전송하기 전에 트래픽을 검사합니다(U-turn 트래픽). 그런 다음 게이트웨이 로드 밸런서는 게이트웨이 로드 밸런서 엔드포인트 및 대상으로 트래픽을 다시 전송합니다.

그림 ***12: Geneve*** 단일 암 프록시

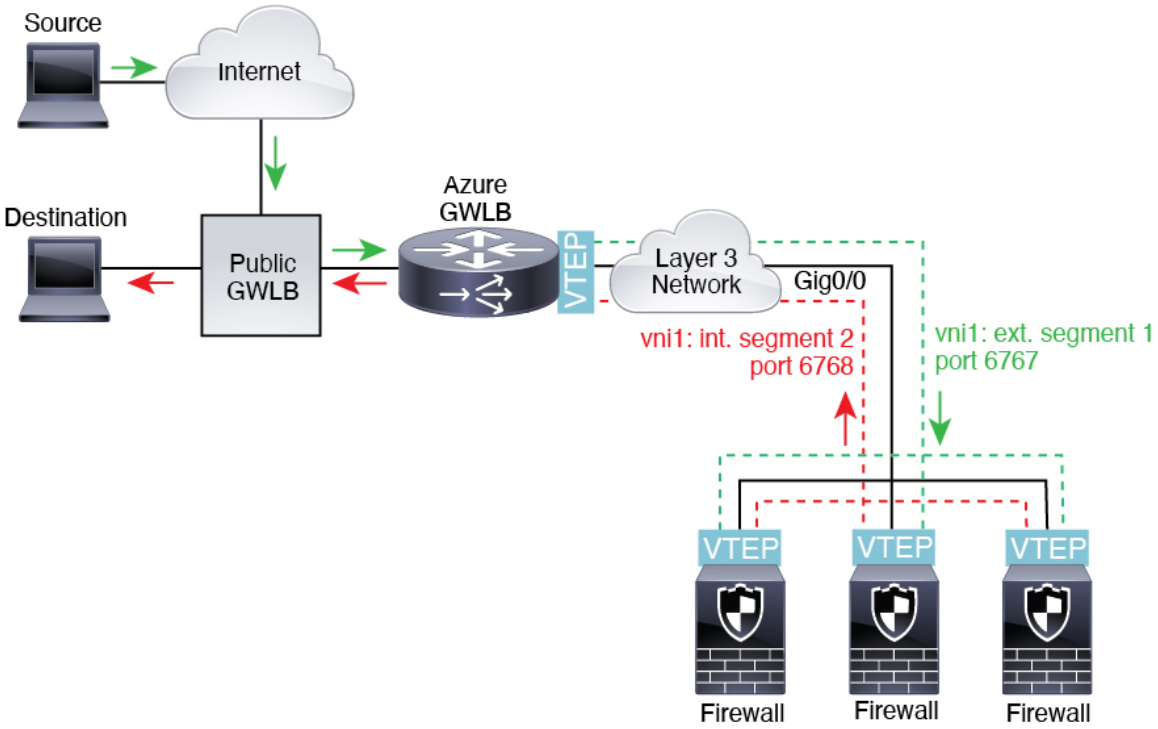


Azure 게이트웨이 로드 밸런서 및 페어링된 프록시

Azure 서비스 체인에서 위협 대응 가상는 인터넷과 고객 서비스 간의 패킷을 인터셉트할 수 있는 투명 게이트웨이 역할을 합니다. 위협 대응 가상는 페어링된 프록시에서 VXLAN 세그먼트를 활용하여 단일 NIC에서 외부 인터페이스 및 내부 인터페이스를 정의합니다.

다음 그림에서는 외부 VXLAN 세그먼트의 공용 게이트웨이 로드 밸런서에서 Azure 게이트웨이 로드 밸런서로 전달되는 트래픽을 보여줍니다. 게이트웨이 로드 밸런서는 여러 위협 대응 가상 간에 트래픽을 밸런싱하며, 이를 삭제하거나 내부 VXLAN 세그먼트에서 게이트웨이 로드 밸런서로 다시 전송하기 전에 트래픽을 검사합니다. 그런 다음 Azure 게이트웨이 로드 밸런서는 퍼블릭 게이트웨이 로드 밸런서 및 대상으로 트래픽을 다시 전송합니다.

그림 ***13:*** 페어링된 프록시가 있는 ***Azure*** 게이트웨이 로드 밸런서



VXLAN 인터페이스 요구 사항 및 사전 요건

모델 요구 사항

- Firepower 1010 스위치 포트 또는 VLAN 인터페이스는 VTEP 인터페이스로 지원되지 않습니다.
- Geneve 캡슐화는 다음 모델에서 지원됩니다.
  - AWS(Amazon Web Services)의 Threat Defense Virtual
- 페어링된 프록시 모드의 VXLAN은 다음 모델에서 지원됩니다.
  - Azure의 Threat Defense Virtual

VXLAN 인터페이스에 대한 지침

방화벽 모드

- Geneve 인터페이스는 라우팅된 방화벽 모드에서만 지원됩니다.
- 쌍으로 구성된 프록시 VXLAN 인터페이스는 라우팅된 방화벽 모드에서만 지원됩니다.

IPv6

- VNI 인터페이스는 IPv4 및 IPv6 트래픽을 모두 지원합니다.
- VTEP 소스 인터페이스 IP 주소는 IPv4만 지원합니다.

클러스터링

- 클러스터링은 클러스터 제어 링크를 제외하고 개별 인터페이스 모드에서 VXLAN을 지원하지 않습니다(threat defense virtual 전용). 스팬 EtherChannel 모드만 VXLAN을 지원합니다.

  GWLB와 함께 사용하기 위해 추가 Geneve 인터페이스를 사용할 수 있는 AWS 및 Azure의 경우에는 예외입니다. GWLB와 함께 사용하기 위해 추가 페어링된 프록시 VXLAN 인터페이스를 사용할 수 있습니다.

라우팅

- 고정 라우팅 또는 정책 기반 라우팅만 VNI 인터페이스에서 지원되며 동적 라우팅 프로토콜은 지원되지 않습니다.

MTU

- VXLAN 캡슐화—소스 인터페이스 MTU가 IPv4의 경우 1554바이트보다 작은 경우 threat defense에서는 MTU를 자동으로 1554바이트로 늘립니다. 이 경우 전체 이더넷 데이터그램이 캡슐화되고 있으므로 새 패킷이 더 크고 더 대량의 MTU가 필요합니다. 다른 디바이스에서 사용된 MTU가 더 큰 경우 소스 인터페이스 MTU를 로 설정해야 합니다. threat defense virtual의 경우 점보 프레임 예약을 활성화하려면 이 MTU를 다시 시작해야 합니다.
- Geneve 캡슐화— 소스 인터페이스 MTU가 1806바이트보다 작은 경우, threat defense에서는 자동으로 MTU를 1806바이트로 늘립니다. 이 경우 전체 이더넷 데이터그램이 캡슐화되고 있으므로 새 패킷이 더 크고 더 대량의 MTU가 필요합니다. 다른 디바이스에서 사용된 MTU가 더 큰 경우, 소스 인터페이스 MTU를 네트워크 MTU + 306바이트로 설정해야 합니다. 점보 프레임 예약을 활성화하려면 이 MTU를 다시 시작해야 합니다.

VXLAN 인터페이스 구성

VXLAN을 구성하려면 다음 단계를 수행하십시오.

참고 VXLAN 또는 Geneve(threat defense virtual만 해당)를 구성할 수 있습니다. Geneve 인터페이스에 대해서는 Geneve 인터페이스 구성, 38 페이지의 내용을 참조하십시오.

참고 Azure GWLB의 경우 ARM 템플릿을 사용하여 VM을 구축할 때 VXLAN 인터페이스가 구성됩니다. 이 섹션을 사용하여 구성을 변경할 수 있습니다.

1. VTEP 소스 인터페이스 구성, 36 페이지.
2. VNI 인터페이스 구성, 37 페이지.
3. (Azure GWLB).게이트웨이 로드 밸런서 상태 확인 허용, 40 페이지

VTEP 소스 인터페이스 구성

threat defense 디바이스별로 1개의 VTEP 소스 인터페이스를 구성할 수 있습니다. VTEP는 NVE(네트워크 가상화 엔드포인트)로 정의됩니다. VXLAN은 기본 캡슐화 유형입니다. Azure의 threat defense virtual에서 클러스터링하는 경우는 예외입니다. 여기서 클러스터 제어 링크에 하나의 VTEP 소스 인터페이스를 사용하고 Azure GWLB에 연결된 데이터 인터페이스에 두 번째 인터페이스를 사용할 수 있습니다.

프로시저

단계 **1** 피어 VTEP 그룹을 지정하려면 피어 IP 주소를 사용하여 네트워크 개체를 추가합니다. 네트워크 개체 생성의 내용을 참조하십시오.

단계 **2** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **3** VXLAN을 구성할 디바이스 옆에 있는 **Edit(**편집**)** ( )를 클릭합니다.

단계 **4** (선택 사항) 소스 인터페이스를 NVE 전용으로 지정합니다.

이 설정은 라우팅 모드에서 선택사항이며 이때 이 설정에서 트래픽을 이 인터페이스의 VXLAN과 일반 관리 트래픽으로 제한합니다. 이 설정은 투명 방화벽 모드에 대해 자동으로 활성화됩니다.

a) **Interfaces(**인터페이스**)**를 클릭합니다.
b) VTEP 소스 인터페이스에 대해 **Edit(**편집**)**( )를 클릭합니다.
c) **General(**일반**)** 페이지에서 **NVE Only(NVE** 전용**)** 확인란을 선택합니다.

단계 **5** 아직 표시되지 않은 경우 **VTEP**를 클릭합니다.

단계 **6** **Enable NVE(NVE** 활성화**)**를 선택합니다.

단계 **7** **Add VTEP(VTEP** 추가**)**를 클릭합니다.

단계 **8** **Encapsulation Type(**캡슐화 유형**)**에서 **VxLAN**을 선택합니다.

AWS의 경우 **VxLAN**과 **Geneve** 중에서 선택할 수 있습니다. 다른 플랫폼에서는 **VxLAN**이 자동으로 선택됩니다.

단계 **9** 지정된 범위 내에서 캡슐화 포트의 값을 입력합니다.

기본값은 4789입니다.

단계 **10** **VTEP Source Interface(VTEP** 소스 인터페이스**)**를 선택합니다.

디바이스에 있는 사용 가능한 물리적 인터페이스 목록에서 선택합니다. 소스 인터페이스 MTU가 IPv4의 경우 1554바이트보다 작은 경우 management center에서는 MTU를 자동으로 1554바이트로 늘립니다.

단계 **11** **Neighbor Address(**인접한 라우터 주소**)**를 선택합니다. 사용 가능한 옵션은 다음과 같습니다.

- **None(**없음**)** — 인접한 라우터 주소가 지정되지 않았습니다.
- **Peer VTEP(**피어 **VTEP)** — 피어 VTP 주소를 지정합니다.
- **Peer Group(**피어 그룹**)** - 피어 IP 주소를 사용하여 네트워크 개체를 지정합니다.
- **Default Multicast(**기본 멀티캐스트**)**—연결된 모든 VNI 인터페이스에 대한 기본 멀티캐스트 그룹을 지정합니다. VNI 인터페이스별로 멀티캐스트 그룹을 구성하지 않은 경우, 이 그룹이 사용됩니다. VNI 인터페이스 수준에서 그룹을 구성하는 경우 이 그룹은 다음 설정을 재정의합니다.

단계 **12** **OK(**확인**)**를 클릭합니다.

단계 **13** **Save(**저장**)**를 클릭합니다.

단계 **14** 라우팅 인터페이스 매개변수를 구성합니다. 라우팅 모드 인터페이스 구성을 참조하십시오.

VNI 인터페이스 구성

VNI 인터페이스를 추가하고 VTEP 소스 인터페이스에 연결하며 기본 인터페이스 파라미터를 구성합니다.

Azure에서 threat defense virtual의 경우 일반 VXLAN 인터페이스를 구성하거나 Azure GWLB와 함께 사용할 페어링된 프록시 모드 VXLAN 인터페이스를 구성할 수 있습니다. 페어링된 프록시 모드는 클러스터링에서 유일하게 지원되는 모드입니다.

Threat Defense 기능 기록**:**

- 7.3 - Azure 게이트웨이 로드 밸런서용 threat defense virtual에 대해 페어링된 프록시 VXLAN

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** VXLAN을 구성할 디바이스 옆에 있는 **Edit(**편집**)** ( )를 클릭합니다.

단계 **3** **Interfaces(**인터페이스**)**를 클릭합니다.

단계 **4** **Add Interfaces(**인터페이스 추가**)**를 클릭한 다음 **VNI Interface(VNI** 인터페이스**)**를 선택합니다.

단계 **5** 인터페이스 **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 **6** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

단계 **7** 지정된 범위 내에서 **Priority(**우선순위**)** 필드의 값을 입력합니다. 기본적으로 0이 선택됩니다.

단계 **8** 1에서 10000 사이에서 **VNI ID**의 값을 입력합니다.

이 ID는 유일한 내부 인터페이스 식별자입니다.

단계 **9** (Azure GWLB용 페어링된 프록시 VXLAN) 프록시 페어링 모드를 활성화하고 필수 매개변수를 설정합니다.

a) **Proxy Paired(**프록시 페어링됨**)**를 선택합니다.
b) **Internal Port(**내부 포트**)**를 1024~65535로 설정합니다.
c) **Internal Segment ID(**내부 세그먼트 **ID)**를 1~16777215로 설정합니다.
d) **External Port(**외부 포트**)**를 1024~65535로 설정합니다.
e) **External Segment ID(**외부 세그먼트 **ID)**를 1~16777215로 설정합니다.

단계 **10** (일반 VXLAN) **VNI Segment ID(VNI** 세그먼트 **ID)** 값을 1~16777215로 입력합니다.

세그먼트 ID는 VXLAN 태그 지정에 사용됩니다.

단계 **11** 멀티캐스트 그룹 **IP** 주소를 입력합니다.

VNI 인터페이스에 대해 멀티캐스트 그룹을 설정하지 않은 경우, VTEP 소스 인터페이스 구성의 기본 그룹이 사용됩니다(사용 가능한 경우). VTEP 소스 인터페이스에 대해 VTEP 피어 IP를 직접 설정하는 경우, VNI 인터페이스에 대해 멀티캐스트 그룹을 지정할 수 없습니다.

단계 **12** **VTEP** 인터페이스에 매핑된 **NVE**를 선택합니다.

이 옵션은 VTEP 소스 인터페이스와 이 인터페이스를 연결합니다.

단계 **13** **OK(**확인**)**를 클릭합니다.

단계 **14** **Save(**저장**)**를 클릭하여 인터페이스 구성을 저장합니다.

단계 **15** 라우팅 또는 투명 인터페이스 매개변수를 구성합니다. 라우팅 및 투명 모드 인터페이스 구성, 41 페이지의 내용을 참조하십시오.

Geneve 인터페이스 구성

threat defense virtual에 대한 Geneve 인터페이스를 구성하려면 다음 단계를 수행하십시오.

참고 VXLAN 또는 Geneve를 구성할 수 있습니다. VXLAN 인터페이스에 대해서는 VXLAN 인터페이스 구성, 35 페이지의 내용을 참조하십시오.

1. VTEP 소스 인터페이스 구성, 39 페이지.
2. VNI 인터페이스 구성, 39 페이지.
3. 게이트웨이 로드 밸런서 상태 확인 허용, 40 페이지.

VTEP 소스 인터페이스 구성

threat defense virtual 디바이스별로 1개의 VTEP 소스 인터페이스를 구성할 수 있습니다. VTEP는 NVE(네트워크 가상화 엔드포인트)로 정의되며.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 2 Geneve를 구성하려는 디바이스 옆에 있는 **Edit(**편집**)**( )를 클릭합니다.

단계 3 **VTEP**를 클릭합니다.

단계 4 **Enable NVE(NVE** 활성화**)**를 선택합니다.

단계 5 **Add VTEP(VTEP** 추가**)**를 클릭합니다.

단계 6 **Encapsulation Type(**캡슐화 유형**)**에서 **Geneve**를 선택합니다.

단계 7 지정된 범위 내에서 캡슐화 포트의 값을 입력합니다.

Geneve 포트는 변경하지 않는 것이 좋습니다. AWS에는 포트 6081이 필요합니다.

단계 8 **VTEP Source Interface(VTEP** 소스 인터페이스**)**를 선택합니다.

디바이스에 있는 사용 가능한 물리적 인터페이스 목록에서 선택할 수 있습니다. 소스 인터페이스 MTU가 1806바이트보다 작은 경우, management center에서는 자동으로 MTU를 1806바이트로 늘립니다.

단계 9 **OK(**확인**)**를 클릭합니다.

단계 10 **Save(**저장**)**를 클릭합니다.

단계 11 라우팅 인터페이스 매개변수를 구성합니다. 라우팅 모드 인터페이스 구성을 참조하십시오.

VNI 인터페이스 구성

VNI 인터페이스를 추가하고 VTEP 소스 인터페이스에 연결하며 기본 인터페이스 파라미터를 구성합니다.

프로시저

단계 1 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 2 Geneve를 구성하려는 디바이스 옆에 있는 **Edit(**편집**)**( )를 클릭합니다.

단계 3 **Interfaces(**인터페이스**)**를 클릭합니다.

단계 4 **Add Interfaces(**인터페이스 추가**)**를 클릭한 다음 **VNI Interface(VNI** 인터페이스**)**를 선택합니다.

단계 5 인터페이스 **Name(**이름**)** 및 **Description(**설명**)**을 입력합니다.

단계 6 1에서 10000 사이에서 **VNI ID**의 값을 입력합니다.

이 ID는 유일한 내부 인터페이스 식별자입니다.

단계 **7** **Enable Proxy(**프록시 활성화**)**를 선택합니다.

이 옵션은 단일 암 프록시를 활성화하고, 트래픽이 입력한 것과 동일한 인터페이스를 종료하도록 허용합니다(U-turn 트래픽). 나중에 인터페이스를 편집하는 경우 단일 연결 프록시를 비활성화할 수 없습니다. 이렇게 하려면 기존 인터페이스를 삭제하고 새 VNI 인터페이스를 생성해야 합니다.

이 옵션은 Geneve VTEP에만 사용할 수 있습니다.

단계 **8** **NVE Mapped to VTEP Interface(VTEP** 인터페이스에 매핑된 **NVE)**를 선택합니다.

이 옵션은 VTEP 소스 인터페이스와 이 인터페이스를 연결합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭하여 인터페이스 구성을 저장합니다.

단계 **11** 라우팅 인터페이스 매개변수를 구성합니다. 라우팅 모드 인터페이스 구성을 참조하십시오.

게이트웨이 로드 밸런서 상태 확인 허용

AWS 또는 Azure GWLB를 사용하려면 어플라이언스가 상태 점검에 올바르게 응답해야 합니다. GWLB는 정상으로 간주되는 어플라이언스에만 트래픽을 전송합니다. SSH, HTTP 또는 HTTPS 상태 확인에 응답하도록 threat defense virtual를 구성해야 합니다.

다음 방법 중 하나를 사용합니다.

프로시저

단계 **1** SSH를 구성합니다. 보안 셸 구성을 참조하십시오.

GWLB IP 주소에서 SSH를 허용합니다. GWLB는 threat defense virtual에 대한 연결을 설정하려고 시도하며 threat defense virtual의 로그인 프롬프트가 상태 증명으로 간주됩니다. SSH 로그인 시도는 1분 후에 시간 초과됩니다. 이 시간 초과를 수용하려면 GWLB에서 더 긴 상태 확인 간격을 구성해야 합니다.

단계 **2** 포트 변환 고정 인터페이스 NAT를 사용하여 HTTP(S) 리디렉션을 구성합니다.

상태 확인을 메타데이터 HTTP(S) 서버로 리디렉션하도록 threat defense virtual를 구성할 수 있습니다. HTTP(S) 상태 확인의 경우 HTTP(S) 서버는 200~399 범위의 상태 코드를 사용하여 GWLB에 응답해야 합니다. threat defense virtual에서는 동시 관리 연결 수에 제한이 있으므로 상태 확인을 외부 서버로 오프로드하도록 선택할 수 있습니다.

포트 변환 고정 인터페이스 NAT를 사용하면 포트(예: 포트 80)에 대한 연결을 다른 IP 주소로 리디렉션할 수 있습니다. 예를 들어 GWLB의 HTTP 패킷을 threat defense virtual 외부 인터페이스의 대상으로 변환하여 HTTP 서버의 대상을 사용하는 threat defense virtual 외부 인터페이스에서 온 것처럼 보이도록 변환합니다. 그런 다음 threat defense virtual는 패킷을 매핑된 대상 주소로 전달합니다. HTTP 서버는 threat defense virtual 외부 인터페이스에 응답한 다음 threat defense virtual는 응답을 GWLB로 다시 전달합니다. GWLB에서 HTTP 서버로의 트래픽을 허용하는 액세스 규칙이 필요합니다.

a) 액세스 규칙에서 GWLB 네트워크의 외부 인터페이스에서 HTTP(S) 트래픽을 허용합니다. 액세스 컨트롤 규칙을 참조하십시오.
b) HTTP(S)의 경우 소스 GWLB IP 주소를 threat defense virtual 외부 인터페이스 IP 주소로 변환합니다. 그런 다음 외부 인터페이스 IP 주소의 대상을 HTTP(S) 서버 IP 주소로 변환합니다. 고정 수동 NAT 구성의 내용을 참조하십시오.

라우팅 및 투명 모드 인터페이스 구성

이 섹션은 라우팅 또는 투명 방화벽 모드에서 모든 모델의 일반 인터페이스 구성을 완료하는 작업이 포함되어 있습니다.

라우팅 및 투명 모드 인터페이스 정보

방화벽 모드 인터페이스는 IP 및 TCP 레이어, IP 조각 모음, TCP 표준화에서 플로우 유지, 플로우 상태 추적 등의 방화벽 기능에 트래픽을 적용합니다. 필요한 경우 보안 정책에 따라 해당 트래픽에 대한 IPS 기능을 구성할 수도 있습니다.

구성할 수 있는 방화벽 인터페이스의 유형은 디바이스의 방화벽 모드 집합이 라우팅인지 투명 모드인지에 따라 달라집니다. 자세한 내용은 투명한 또는 라우팅된 방화벽 모드를 참조하십시오.

- 라우팅 모드 인터페이스(라우팅된 방화벽 모드 전용) - 서로 라우팅하려는 각 인터페이스가 다른 서브넷에 있습니다.
- 브리지 그룹 인터페이스(라우팅 및 투명 방화벽 모드 - 네트워크의 여러 인터페이스를 그룹화할 수 있고 Firepower Threat Defense 디바이스는 브리지 기술을 사용해 인터페이스 간 트래픽을 전달합니다. 각 브리지 그룹은 네트워크에서 IP 주소를 할당할 BVI(Bridge Virtual Interface)를 포함합니다. 라우팅 모드에서 Firepower Threat Defense 디바이스는 BVI 및 일반 라우팅 인터페이스를 라우팅합니다. 투명 모드에서 의 각 브리지 그룹은 구분되며 서로 통신할 수 없습니다.

이중 IP 스택(IPv4 및 IPv6)

위협 방지 디바이스은 하나의 인터페이스에서 IPv6 및 IPv4 주소를 모두 지원합니다. IPv4 및 IPv6 모두에 대한 기본 경로를 구성해야 합니다.

31비트 서브넷 마스크

라우팅 인터페이스의 경우, 지점 간 연결을 위해 31비트 서브넷에서 IP 주소를 구성할 수 있습니다. 31비트 서브넷 주소는 주소를 2개만 포함합니다. 일반적으로 서브넷의 첫 번째 주소 및 마지막 주소는 네트워크 및 브로드캐스트용으로 예약되어 있으므로 2개의 주소 서브넷은 사용할 수 없습니다. 그러나 지점 간 연결이 있으며 네트워크 또는 브로드캐스트 주소가 필요하지 않은 경우, 31비트 서브넷은 IPv4에서 주소를 보존하는 유용한 방법입니다. 예를 들어, 2개의 threat defense 간의 페일오버 링크에는 주소가 2개만 필요합니다. 링크의 한 쪽 끝에서 전송되는 모든 패킷은 항상 다른 쪽에서 수신되며 브로드캐스팅이 필요하지 않습니다. SNMP 또는 Syslog를 실행하는 직접 연결된 관리 스테이션을 사용할 수도 있습니다.

31비트 서브넷 및 클러스터링

관리 인터페이스 및 클러스터 제어 링크를 제외하고 에서 클러스터 인터페이스에 대해 31비트 서브넷 마스크를 사용할 수 있습니다.

31비트 서브넷 및 장애 조치

장애 조치를 위해 threat defense 인터페이스 IP 주소에 대해 31비트 서브넷을 사용하는 경우, 주소가 충분하지 않으므로 인터페이스에 대해 스탠바이 IP 주소를 구성할 수 없습니다. 일반적으로, 스탠바이 인터페이스 상태를 확인하기 위해 액티브 유닛에서 인터페이스 테스트를 수행할 수 있도록 장애 조치를 위한 인터페이스에는 스탠바이 IP 주소가 있어야 합니다. 스탠바이 IP 주소가 없으면 threat defense에서는 모든 네트워크 테스트를 수행할 수 없으며 링크 상태만 추적할 수 있습니다.

포인트 투 포인트 연결인 장애 조치 및 별도의 상태 링크(선택 사항)에서 31비트 서브넷도 사용할 수 있습니다.

31비트 서브넷 및 관리

직접 연결된 관리 스테이션을 사용하는 경우 threat defense의 SSH 또는 HTTP에 대해 또는 관리 스테이션의 SNMP 또는 시스템 로그에 대해 포인트 투 포인트 연결을 사용할 수 있습니다.

31비트 서브넷의 지원되지 않는 기능

다음 기능은 31비트 서브넷을 지원하지 않습니다.

- 브리지 그룹에 대한 BVI 인터페이스 — 브리지 그룹에는 최소 3개의 호스트 주소가 필요합니다. 즉, 두 개의 브리지 그룹 멤버 인터페이스에 연결된 BVI 및 2개의 호스트가 필요합니다. /29 서브넷 또는 더 작은 서브넷을 사용해야 합니다.
- 멀티캐스트 라우팅

라우팅 모드 및 투명 모드 인터페이스에 대한 지침 및 제한 사항

고가용성, 클러스터링 및 다중 인스턴스

- 이 장의 절차를 사용하여 장애 조치 링크를 구성해서는 안 됩니다. 자세한 내용은 고가용성 장을 참조하십시오.
- 클러스터 인터페이스의 경우 클러스터링 장에서 요구 사항을 참조하십시오.
- 다중 인스턴스 모드의 경우 공유 인터페이스는 브리지 그룹 멤버 인터페이스(투명 모드 또는 라우팅 모드)에서 지원되지 않습니다.
- 고가용성를 사용하는 경우 데이터 인터페이스에 대해 IP 주소 및 스탠바이 주소를 수동으로 설정해야 하며, DHCP 및 PPPoE는 지원되지 않습니다. 모니터링되는 인터페이스 영역의 디바이스 > 디바이스 관리 > 고가용성 탭에서 스탠바이 IP 주소를 설정합니다. 자세한 내용은 고가용성 장을 참조하십시오.

IPv6

- 모든 인터페이스에서 IPv6가 지원됩니다.
- 투명 모드에서 IPv6 주소만 수동으로 구성할 수 있습니다.
- 위협 방지 디바이스는 IPv6 애니캐스트 주소를 지원하지 않습니다.
- DHCPv6 및 접두사 위임 옵션은 다중 상황 모드, 투명 클러스터링 또는 고가용성에서 지원되지 않습니다.

모델 지침

- 브리지 ixgbevf 인터페이스를 사용하는 VMware의 threat defense virtual의 경우 브리지 그룹이 지원되지 않습니다.
- Firepower 2100 Series의 경우, 브리지 그룹은 라우팅 모드에서 지원되지 않습니다.

투명 모드 및 브리지 그룹 지침

- 브리지 그룹당 64개의 인터페이스가 있는 최대 250개의 브리지 그룹을 생성할 수 있습니다.
- 직접 연결된 각 네트워크는 같은 서브넷에 있어야 합니다.
- 위협 방지 디바이스는 보조 네트워크의 트래픽을 지원하지 않습니다. BVI IP 주소와 동일한 네트워크의 트래픽만 지원됩니다.
- 디바이스 간 및 디바이스에서 관리 트래픽과 위협 방지 디바이스를 통과하는 데이터 트래픽의 경우 각 브리지 그룹에 대해 BBI의 IP 주소가 필요합니다. IPv4 트래픽의 경우 IPv4 주소를 지정합니다. IPv6 트래픽의 경우 IPv6 주소를 지정합니다.
- IPv6 주소만 수동으로 구성할 수 있습니다.
- BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. 서브넷을 호스트 서브넷(255.255.255.255)으로 설정할 수 없습니다.
- 관리 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- 다중 인스턴스 모드의 경우 공유 인터페이스는 브리지 그룹 멤버 인터페이스(투명 모드 또는 라우팅 모드)에서 지원되지 않습니다.
- 브리지 ixgbevf 인터페이스를 사용하는 VMware의 threat defense virtual의 경우 투명 방화벽 모드 브리지 그룹이 지원되지 않으며 브리지 그룹은 라우팅 모드에서 지원되지 않습니다.
- Firepower 2100 Series의 경우, 브리지 그룹은 라우팅 모드에서 지원되지 않습니다.
- Firepower 1010의 경우, 동일한 브리지 그룹에서 논리적 VLAN 인터페이스와 물리적 방화벽 인터페이스를 혼합할 수 없습니다.
- Firepower 4100/9300의 경우, 데이터 공유 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다.
- 투명 모드에서는 1개 이상의 브리지 그룹을 사용해야 합니다. 데이터 인터페이스는 브리지 그룹에 속해야 합니다.

- 투명 모드에서는 BVI IP 주소를 연결된 디바이스의 기본 게이트웨이로 지정하지 마십시오. 디바이스의 경우 threat defense의 다른 쪽에 있는 라우터를 기본 게이트웨이로 지정해야 합니다.
- 투명 모드에서는 관리 트래픽의 반환 경로를 제공하는 데 필요한 기본 경로가 하나의 브리지 그룹 네트워크에서 발생하는 관리 트래픽에만 적용됩니다. 그 이유는 기본 경로에서 브리지 그룹의 인터페이스 및 브리지 그룹 네트워크의 라우터 IP 주소를 지정하기 때문이며, 하나의 기본 경로만 정의할 수 있습니다. 관리 트래픽이 여러 개의 브리지 그룹 네트워크에서 발생할 경우, 관리 트래픽이 발생할 것으로 예상되는 네트워크를 식별하는 일반 고정 경로를 지정해야 합니다.
- 투명 모드에서 PPPoE는 진단 인터페이스에 대해 지원되지 않습니다.
- 투명 모드는 Amazon Web Services, Microsoft Azure, Google Cloud Platform 및 Oracle Cloud Infrastructure에 구축된 위협 방어 가상 인스턴스에서 지원되지 않습니다.
- 라우팅 모드에서 브리지 그룹 및 기타 라우팅 인터페이스 간을 라우팅하려면 BVI의 이름을 지정해야 합니다.
- 라우팅 모드에서 threat defense 정의된 EtherChannel 인터페이스는 브리지 그룹 멤버로 지원되지 않습니다. Firepower 4100/9300의 EtherChannel은 브리지 그룹 멤버가 될 수 있습니다.
- BFD(Bidirectional Forwarding Detection) 에코 패킷은 브리지 그룹 멤버를 사용할 때 threat defense를 통과하는 것이 허용되지 않습니다. BFD를 실행하는 threat defense의 양쪽 측면에 두 개의 네이버가 있는 경우, threat defense는 두 개의 네이버가 동일한 소스 및 대상 IP 주소를 지니고 있으며 LAND 공격의 일부로 표시되므로 BFD 에코 패킷을 삭제합니다.

추가 지침 및 요건

- threat defense는 패킷에서 하나의 802.1Q 헤더만 지원하며 방화벽 인터페이스에 대해 여러 헤더(Q-in-Q 지원이라고 하는)를 지원하지 않습니다.참고: 인라인 집합 및 패시브 인터페이스의 경우 FTD는 하나의 802.1Q 헤더만 지원하는 Firepower 4100/9300을 제외하고 패킷에서 최대 2개의 802.1Q 헤더를 지원합니다.

라우팅 모드 인터페이스 구성

이 절차에서는 이름, 보안 영역, IPv4 주소를 설정하는 방법에 대해 설명합니다.

참고 모든 인터페이스 유형에 대해 모든 필드가 지원되는 것은 아닙니다.

시작하기 전에

- **Firepower 4100/9300**
  1. 실제 인터페이스 구성
  2. (선택 사항) 특수 인터페이스를 구성합니다.
     - EtherChannel(포트 채널) 추가

- 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가 FXOS에서
- 루프백 인터페이스 구성, 20 페이지
- 하위 인터페이스 추가, 26 페이지 in management center
- VXLAN 인터페이스 구성, 35 페이지

- (선택 사항) 기타 모든 모델:
  - EtherChannel 구성, 17 페이지
  - 루프백 인터페이스 구성, 20 페이지
  - 하위 인터페이스 추가, 26 페이지
  - VXLAN 인터페이스 구성, 35 페이지
  - Threat Defense Virtual AWS에서: Geneve 인터페이스 구성, 38 페이지
  - Firepower 1010: VLAN 인터페이스 구성, 5 페이지

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

이름은 "cluster"로 시작할 수 없습니다. 이는 내부용으로 사용하기 위해 예약되어 있습니다.

단계 **4** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **5** (선택 사항) 관리 트래픽으로 트래픽을 제한하려면 이 인터페이스를 관리 전용으로 설정합니다. through-the-box 트래픽은 허용되지 않습니다.

단계 **6** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **7** **Mode(**모드**)** 드롭다운 목록에서 **None(**없음**)**을 선택합니다.

일반 방화벽 인터페이스는 None(없음) 모드로 설정됩니다. 다른 모드는 IPS 전용 인터페이스 유형입니다.

단계 **8** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

라우팅된 인터페이스는 라우팅 유형 인터페이스이며 라우팅 유형 영역에만 속할 수 있습니다.

단계 **9** **MTU**에 대한 자세한 내용은 MTU 구성, 71 페이지를 참조하십시오.

단계 **10** **Priority(**우선순위**)** 필드에 0~65535 범위의 숫자를 입력합니다.

이 값은 정책 기반 라우팅 구성에서 사용됩니다. 우선순위는 여러 이그레스 인터페이스에서 트래픽을 라우팅하는 방법을 결정하는 데 사용됩니다. 자세한 내용은 정책 기반 라우팅 정책 구성를 참고하십시오.

단계 **11** **IPv4** 탭을 클릭합니다. IP 주소를 설정하려면 **IP** 유형 드롭다운 목록에서 다음 중 하나를 사용합니다.

고가용성 및 클러스터링 및 루프백인터페이스는 고정 IP 주소 설정만 지원합니다. DHCP 및 PPPoE는 지원되지 않습니다.

- 고정 **IP** 사용 - IP 주소 및 서브넷 마스크를 입력합니다. 포인트 투 포인트 연결을 위해 31비트 서브넷 마스크(255.255.255.254)를 지정할 수 있습니다. 이 경우 IP 주소가 네트워크 또는 브로드캐스트 주소에 대해 예약되어 있습니다. 이 경우 스탠바이 IP 주소를 설정할 수 없습니다. 고가용성의 경우 고정 IP 주소만 사용할 수 있습니다. **Monitored Interfaces(**모니터링되는 인터페이스**)** 영역의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **High Availability(**고가용성**)** 탭에서 스탠바이 IP 주소를 설정합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **DHCP** 사용 - 다음 선택 파라미터를 구성합니다.
  - **DHCP**에서 기본 경로 가져오기 - DHCP 서버에서 기본 경로를 가져옵니다.
  - **DHCP** 경로 메트릭 - 파악된 경로에 대해 1과 255 사이의 관리 거리를 할당합니다. 파악된 경로의 기본 관리 거리는 1입니다.
- **PPPoE** 사용 - 인터페이스가 DSL, 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하며 ISP가 PPPoE를 사용해 IP 주소를 제공하는 경우 다음 파라미터를 구성합니다.
  - **VPDN** 그룹 이름 - 이 연결을 대표하는 그룹 이름을 원하는 대로 지정합니다.
  - **PPPoE** 사용자 이름 - ISP에서 제공한 사용자 이름을 지정합니다.
  - **PPPoE** 암호/암호 확인 - ISP에서 제공한 비밀번호를 지정하고 확인합니다.
  - **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** 경로 메트릭 - 파악된 경로에 관리 거리를 할당합니다. 유효한 값은 1 ~ 255입니다. 파악된 경로의 기본 관리 거리는 1입니다.
  - 경로 설정 사용 - PPPoE IP 주소를 수동으로 구성하려면 이 체크 박스를 선택하고 **IP** 주소를 입력합니다.

Enable Route Settings(경로 설정 활성화**)** 확인란을 선택하고 **IP Address(IP** 주소**)**를 입력하지 않으면, 이 예시에서처럼 **ip address pppoe setroute** 명령이 적용됩니다.

```
interface GigabitEthernet0/2
nameif inside2_pppoe
cts manual
  propagate sgt preserve-untag
  policy static sgt disabled trusted
security-level 0
pppoe client vpdn group test
pppoe client route distance 10
ip address pppoe setroute
```

- 플래시에 사용자 이름 및 비밀번호 저장 - 플래시 메모리에 사용자 이름 및 비밀번호를 저장합니다.

  threat defense에서는 NVRAM의 특수 위치에 사용자 이름 및 비밀번호를 저장합니다.

단계 **12** (선택 사항) **IPv6** 탭에서 IPv6 주소 지정을 구성하려면 IPv6 주소 지정 구성, 54 페이지를 참조하십시오.

단계 **13** (선택 사항) 고급 탭에서 MAC 주소를 수동으로 구성하려면 MAC 주소 구성, 72 페이지를 참조하십시오.

단계 **14** (선택 사항) **Hardware Configuration(**하드웨어 구성**)** > **Speed(**속도**)**를 클릭하여 듀플렉스 및 속도를 설정합니다.

- **Duplex(**듀플렉스**)** - **Full(**풀**)** 또는 **Half(**하프**)**를 선택합니다. SFP 인터페이스는 전이중만 지원합니다.
- **Speed(**속도**)** — 속도를 선택합니다(모델에 따라 다름). (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.
- 전달 오류 수정 모드 - (Secure Firewall 3100만 해당) 25Gbps 이상의 인터페이스에서는 전달 오류 수정(FEC)을 활성화합니다. EtherChannel 멤버 인터페이스의 경우, 이를 EtherChannel에 추가하기 전에 전달 오류 수정을 구성해야 합니다. **Auto(**자동**)**를 사용할 때 선택하는 설정은 트렌시버 유형 및 인터페이스가 고정(내장) 또는 네트워크 모듈에 있는지 여부에 따라 달라집니다.

표 ***1:*** 자동 설정을 위한 기본 ***FEC***

트랜시버 유형	고정 포트 기본 **FEC(Ethernet 1/9~1/16)**	네트워크 모듈 기본 **FEC**
25G-SR	조항 108 RS-FEC	조항 108 RS-FEC
25G-LR	조항 108 RS-FEC	조항 108 RS-FEC
10/25G-CSR	조항 108 RS-FEC	조항 74 FC-FEC(25/50G)

트랜시버 유형	고정 포트 기본 **FEC(Ethernet 1/9~1/16)**	네트워크 모듈 기본 **FEC**
25G-AOC*x*M	조항 74 FC-FEC	조항 74 FC-FEC
25G-CU2.5/3M	자동 협상	자동 협상
25G-CU4/5M	자동 협상	자동 협상

단계 **15** (선택 사항) management center은(는) **Manager Access(**관리자 액세스**)** 페이지에서 데이터 인터페이스에 대한 액세스를 관리합니다.

threat defense를 처음 설정할 때 데이터 인터페이스에서 관리자 액세스를 활성화할 수 있습니다. management center에 threat defense를 추가한 후 관리자 액세스를 활성화하거나 비활성화하려면 다음을 참조하십시오.

- 관리자 액세스를 활성화합니다. 관리에서 데이터로 Manager 액세스 인터페이스 변경

  참고 관리에서 데이터 인터페이스로의 관리자 인터페이스 마이그레이션을 먼저 시작하지 않으면 관리자 액세스를 활성화할 수 없습니다. 마이그레이션을 시작한 후 관리자 액세스 페이지에서 관리자 액세스를 활성화하고 구성을 성공적으로 저장할 수 있습니다.

- 관리자 액세스를 비활성화합니다. 데이터에서 관리로 Manager 액세스 인터페이스 변경

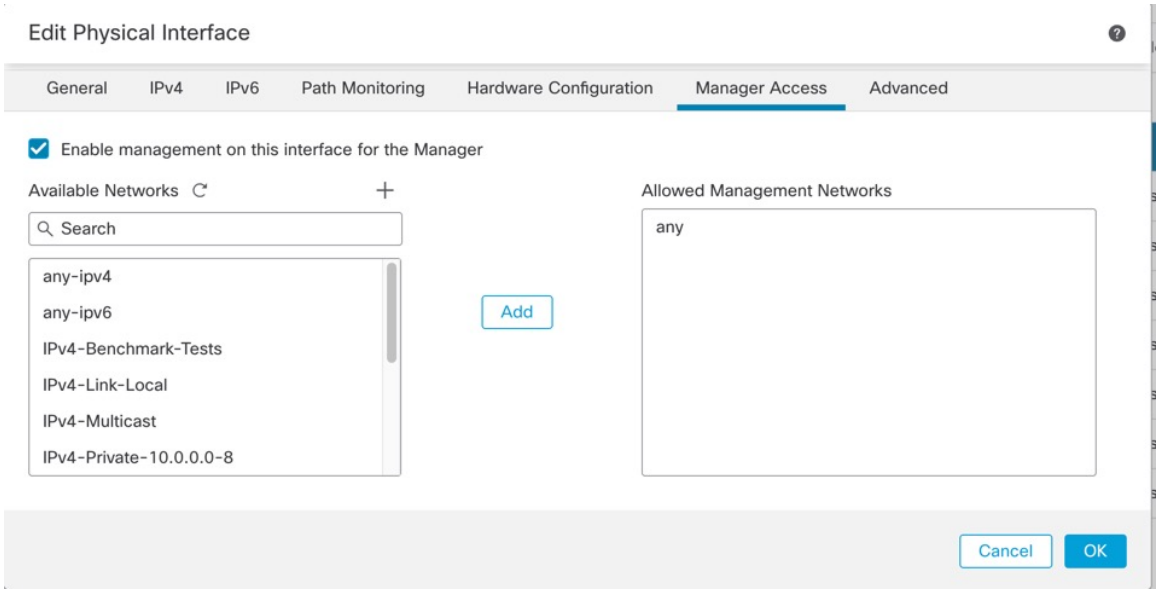
관리자 액세스 인터페이스를 한 데이터 인터페이스에서 다른 데이터 인터페이스로 변경하려면 원래 데이터 인터페이스에서 관리자 액세스를 비활성화해야 하지만 인터페이스 자체는 아직 비활성화하지 않아야 합니다. 원본 데이터 인터페이스를 사용하여 구축을 수행해야 합니다. 새 관리자 액세스 인터페이스에서 동일한 IP 주소를 사용하려는 경우 원래 인터페이스에서 IP 구성을 삭제하거나 변경할 수 있습니다. 이 변경 사항은 구축에 영향을 미치지 않습니다. 새 인터페이스에 다른 IP 주소를 사용하는 경우 management center에 표시된 디바이스 IP 주소도 변경합니다. Management Center에서 호스트 이름 또는 IP 주소 업데이트의 내용을 참조하십시오. 정적 경로, DDNS 및 DNS 설정과 같은 새 인터페이스를 사용하려면 관련 구성도 업데이트해야 합니다.

데이터 인터페이스에서의 관리자 액세스에는 다음과 같은 제한이 있습니다.

- 물리적 데이터 인터페이스에서만 관리자 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.또한 management center를 사용하여 리던던시(redundancy)를 위해 단일 보조 인터페이스에서 관리자 액세스를 활성화할 수 있습니다.
- 이 인터페이스는 관리 전용일 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 threat defense와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.

- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 management center를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다. Amazon Web Services의 threat defense virtual에서는 콘솔 포트를 사용할 수 없으므로 구성을 계속하기 전에 관리 인터페이스에 대한 SSH 액세스를 유지해야 합니다. 또는 관리자 액세스를 위해 데이터 인터페이스를 설정하고 연결을 끊기 전에 모든 CLI 구성(**configure manager add** 명령 포함)을 완료해야 합니다.
- 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.
- 클러스터링은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.
- 고가용성은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.

그림 ***14:*** 관리자 액세스



- Firepower Management Center가 전용 관리 인터페이스 대신 이 데이터 인터페이스를 관리용으로 사용하려면 **Enable interface on this interface for this interface(**이 인터페이스에서 관리 활성화**)**를 선택합니다.
- (선택 사항) **Allowed Management Networks(**허용되는 관리 네트워크**)** 상자에 관리자 액세스를 허용할 네트워크를 추가합니다. 기본적으로 모든 네트워크가 허용됩니다.

단계 **16** **OK(**확인**)**를 클릭합니다.

단계 **17** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

브리지 그룹 인터페이스 구성

브리지 그룹은 Secure Firewall Threat Defense 디바이스에서 경로 대신 브리징하는 인터페이스 그룹입니다. 브리지 그룹은 투명 방화벽 모드와 라우팅 방화벽 모드에서 지원됩니다. 브릿지 그룹에 대한 자세한 내용은 브리지 그룹 정보를 참조하십시오.

브리지 그룹 및 연결된 인터페이스를 구성하려면, 다음 단계를 수행하십시오.

일반 브리지 그룹 멤버 인터페이스 파라미터 구성

이 절차에서는 각 브리지 그룹 멤버 인터페이스의 이름 및 보안 영역을 설정하는 방법을 설명합니다. 동일한 브리지 그룹은 다양한 유형의 인터페이스를 포함할 수 있습니다. 예를 들어, 물리적 인터페이스, VLAN 하위 인터페이스, Firepower 1010 VLAN 인터페이스, EtherChannel 및 이중 인터페이스가 있습니다. 관리 인터페이스는 지원되지 않습니다. 라우팅된 모드에서 Etherchannel은 지원되지 않습니다. Firepower 4100/9300의 경우 데이터 공유 유형 인터페이스는 지원되지 않습니다.

시작하기 전에

- **Firepower 4100/9300**
  1. 실제 인터페이스 구성
  2. (선택 사항) 특수 인터페이스를 구성합니다.
     - EtherChannel(포트 채널) 추가
     - 컨테이너 인스턴스에 VLAN 하위 인터페이스 추가 FXOS에서
     - 하위 인터페이스 추가, 26 페이지 in management center
- (선택 사항) 기타 모든 모델**:**
  - EtherChannel 구성, 17 페이지
  - 하위 인터페이스 추가, 26 페이지
  - Firepower 1010: VLAN 인터페이스 구성, 5 페이지

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

이름은 "cluster"로 시작할 수 없습니다. 이는 내부용으로 사용하기 위해 예약되어 있습니다.

단계 **4** **Enabled(**활성화됨**)** 체크 박스를 선택하여 인터페이스를 활성화합니다.

단계 **5** (선택 사항) 관리 트래픽으로 트래픽을 제한하려면 이 인터페이스를 관리 전용으로 설정합니다. through-the-box 트래픽은 허용되지 않습니다.

단계 **6** (선택 사항) **Description(**설명**)** 필드에 설명을 추가합니다.

설명은 줄 바꿈 없이 1줄, 최대 200자로 작성할 수 있습니다.

단계 **7** **Mode(**모드**)** 드롭다운 목록에서 **None(**없음**)**을 선택합니다.

일반 방화벽 인터페이스는 None(없음) 모드로 설정됩니다. 다른 모드는 IPS 전용 인터페이스 유형입니다. 이 인터페이스를 브리지 그룹으로 할당하면 모드는 스위치라고 표시됩니다.

단계 **8** **Security Zone(**보안 영역**)** 드롭다운 목록에서 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

브리지 그룹 멤버 인터페이스는 스위치 유형 인터페이스이며 스위치 유형 영역에만 속할 수 있습니다. 이 인터페이스에는 IP 주소 설정을 구성하지 마십시오. 브리지 가상 인터페이스(BVI)에만 IP 주소를 구성할 수 있습니다. BVI는 영역에 속하지 않으므로 BVI에 액세스 제어 정책을 적용할 수 없습니다.

단계 **9** **MTU**에 대한 자세한 내용은 MTU 구성, 71 페이지를 참조하십시오.

단계 **10** (선택 사항) **Hardware Configuration(**하드웨어 구성**)** > **Speed(**속도**)**를 클릭하여 듀플렉스 및 속도를 설정합니다.

- **Duplex(**듀플렉스**)** - **Full(**풀**)** 또는 **Half(**하프**)**를 선택합니다. SFP 인터페이스는 전이중만 지원합니다.
- **Speed(**속도**)** — 속도를 선택합니다(모델에 따라 다름). (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.
- 전달 오류 수정 모드 - (Secure Firewall 3100만 해당) 25Gbps 이상의 인터페이스에서는 전달 오류 수정(FEC)을 활성화합니다. EtherChannel 멤버 인터페이스의 경우, 이를 EtherChannel에 추가하기 전에 전달 오류 수정을 구성해야 합니다. **Auto(**자동**)**를 사용할 때 선택하는 설정은 트렌시버 유형 및 인터페이스가 고정(내장) 또는 네트워크 모듈에 있는지 여부에 따라 달라집니다.

표 ***2:*** 자동 설정을 위한 기본 ***FEC***

트랜시버 유형	고정 포트 기본 **FEC(Ethernet 1/9~1/16)**	네트워크 모듈 기본 **FEC**
25G-SR	조항 108 RS-FEC	조항 108 RS-FEC
25G-LR	조항 108 RS-FEC	조항 108 RS-FEC
10/25G-CSR	조항 108 RS-FEC	조항 74 FC-FEC(25/50G)
25G-AOC*x*M	조항 74 FC-FEC	조항 74 FC-FEC

트랜시버 유형	고정 포트 기본 **FEC(Ethernet 1/9~1/16)**	네트워크 모듈 기본 **FEC**
25G-CU2.5/3M	자동 협상	자동 협상
25G-CU4/5M	자동 협상	자동 협상

단계 **11** (선택 사항) **IPv6** 탭에서 IPv6 주소 지정을 구성하려면 IPv6 주소 지정 구성, 54 페이지를 참조하십시오.

단계 **12** (선택 사항) 고급 탭에서 MAC 주소를 수동으로 구성하려면 MAC 주소 구성, 72 페이지를 참조하십시오.

단계 **13** **OK(**확인**)**를 클릭합니다.

단계 **14** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

BVI(Bridge Virtual Interface) 구성

각 브리지 그룹에는 IP 주소를 구성하는 BVI가 필요합니다. threat defense에서는 브리지 그룹에서 시작하는 패킷의 소스 주소로 이 IP 주소를 사용합니다. BVI IP 주소는 연결된 네트워크와 동일한 서브넷에 있어야 합니다. IPv4 트래픽의 경우 트래픽을 전달하려면 BVI IP 주소가 필요합니다. IPv6 트래픽에서는 적어도 트래픽을 전달하기 위해서는 링크-로컬 주소를 구성해야 합니다. 그러나 원격 관리, 기타 관리 작업을 포함한 전체 기능에 하나의 전역 관리 주소를 사용하는 것이 좋습니다.

라우팅 모드에서 BVI의 이름을 제공하는 경우 BVI는 라우팅에 참여합니다. 이름이 없는 경우 브리지 그룹은 투명 방화벽 모드에서와 같이 격리된 상태로 남아 있습니다.

참고 별도의 진단 인터페이스의 경우 구성 불가한 브리지 그룹(ID 301)이 자동으로 설정에 추가됩니다. 이 브리지 그룹은 브리지 그룹 한도의 대상이 아닙니다.

시작하기 전에

BVI를 보안 영역에 추가할 수 없습니다. 따라서 BVI에 액세스 제어 정책을 적용할 수 없습니다. 영역에 따라 브리지 그룹 멤버 인터페이스에 정책을 적용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 인터페이스 추가 > 브리지 그룹 인터페이스를 선택합니다.

단계 **3** (라우팅 모드 이름 필드에서 최대 48자의 이름을 입력합니다.

브리지 그룹 외부 멤버에게 트래픽을 라우팅하려는 경우 BVI의 이름을 지정해야 합니다. 예를 들어, 외부 인터페이스 또는 기타 브리지 그룹의 멤버에게 트래픽을 라우팅하는 경우입니다. 이름은 대소문자를 구분하지 않습니다.

단계 **4** 브리지 그룹 **ID** 필드에는 1~250 범위로 브리지 그룹 ID를 입력합니다.

단계 **5** 설명 필드에는 브리지 그룹에 대한 설명을 입력합니다.

단계 **6** 인터페이스 탭에서 인터페이스를 클릭하고 추가를 클릭하여 선택된 인터페이스 영역으로 이동합니다. 멤버로 추가하려면 모든 인터페이스에 대해 반복합니다.

단계 **7** (투명 모드) **IPv4** 탭을 클릭합니다. **IP** 주소 필드에 IPv4 주소 및 서브넷 마스크를 입력합니다.

BVI에 호스트 주소(/32 또는 255.255.255.255)를 할당하지 마십시오. 또한 /30 서브넷(255.255.255.252)과 같이 3개 미만의 호스트 주소(업스트림 라우터, 다운스트림 라우터, 투명 방화벽 각각 하나씩)를 포함한 다른 서브넷은 사용하지 마십시오. threat defense 디바이스는 서브넷의 첫 주소 및 마지막 주소와 주고받는 모든 ARP 패킷을 삭제합니다. 만약 /30 서브넷을 사용하고 그 서브넷에서 업스트림 라우터에 예약된 주소를 지정할 경우 threat defense 디바이스는 다운스트림 라우터에서 업스트림 라우터로 ARP 요청을 폐기합니다.

고가용성을 위해서는 모니터링되는 인터페이스 영역의 디바이스 > 디바이스 관리 > 고가용성 탭에서 스탠바이 IP 주소를 설정합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

단계 **8** (라우팅 모드) **IPv4** 탭을 클릭합니다. IP 주소를 설정하려면 **IP** 유형 드롭다운 목록에서 다음 중 하나를 사용합니다.

고가용성 및 클러스터링 인터페이스는 고정 IP 주소 설정만 지원합니다. DHCP는 지원되지 않습니다.

- 고정 **IP** 사용 - IP 주소 및 서브넷 마스크를 입력합니다. 고가용성의 경우 고정 IP 주소만 사용할 수 있습니다. 모니터링되는 인터페이스 영역의 디바이스 > 디바이스 관리 > 고가용성 탭에서 스탠바이 IP 주소를 설정합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.
- **DHCP** 사용 - 다음 선택 파라미터를 구성합니다.
  - **DHCP**에서 기본 경로 가져오기 - DHCP 서버에서 기본 경로를 가져옵니다.
  - **DHCP** 경로 메트릭 - 파악된 경로에 대해 1과 255 사이의 관리 거리를 할당합니다. 파악된 경로의 기본 관리 거리는 1입니다.

단계 **9** (선택 사항) IPv6 주소를 설정하려면 IPv6 주소 지정 구성, 54 페이지을 참조하십시오.

단계 **10** (선택 사항) (투명 모드에 한해) **ARP**와 **MAC** 설정을 구성하려면 고정 ARP 항목 추가, 73 페이지및 고정 MAC 주소를 추가하고 브리지 그룹에 대한 MAC 학습을 비활성화, 74 페이지를 참조하십시오.

단계 **11** **OK(**확인**)**를 클릭합니다.

단계 **12** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

IPv6 주소 지정 구성

이 섹션에서는 라우팅 및 투명 모드에서 IPv6 주소 지정을 구성하는 방법에 대해 설명합니다.

IPv6 정보

이 섹션에서는 IPv6에 대한 정보를 다룹니다.

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 이 주소는 멤버 인터페이스가 아닌 BVI에 대해 구성되어야 합니다. 투명 모드에서는 관리 인터페이스에 대해 전역 IPv6 주소를 구성할 수도 있습니다.
- 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. 주소 구성 또는 주소 확인과 같은 네이버 검색 기능에 사용할 수 있습니다. 브리지 그룹에서 멤버 인터페이스에만 링크 로컬 주소가 있습니다. BVI에는 링크 로컬 주소가 없습니다.

적어도 IPv6가 작동하려면 링크-로컬 주소를 구성해야 합니다. 전역 주소를 설정하면 링크-로컬 주소가 인터페이스에서 자동으로 구성되므로 링크-로컬 주소를 특별히 구성하지 않아도 됩니다. 브리지 그룹 멤버 인터페이스에서 BVI에 전역 주소를 구성하는 경우, 위협 방지 디바이스에서는 멤버 인터페이스에 대한 링크 로컬 주소를 자동으로 생성합니다. 전역 주소를 구성하지 않은 경우 자동으로 또는 수동으로 링크-로컬 주소를 구성해야 합니다.

수정된 EUI-64 인터페이스 ID

RFC 3513: IPv6(Internet Protocol Version 6) Addressing Architecture에 따르면, 모든 유니캐스트 IPv6 주소(이진 값 000으로 시작하는 것 제외)의 인터페이스 식별자 부분은 길이가 64비트이고 Modified EUI-64 형식이어야 합니다. 위협 방지 디바이스는 로컬 링크에 연결된 호스트에 이 요구 사항을 적용할 수 있습니다.

이 기능이 인터페이스에서 활성화된 경우, 그 인터페이스에서 수신한 IPv6 패킷의 소스 주소를 소스 MAC 주소와 비교하여 검증함으로써 인터페이스 식별자가 Modified EUI-64 형식을 사용하는지 확인합니다. IPv6 패킷에서 인터페이스 식별자에 Modified EUI-64 형식을 사용하지 않을 경우 패킷은 폐기되고 다음 시스템 로그 메시지가 생성됩니다.

```
325003: EUI-64 source address check failed.
```

주소 형식 검증은 흐름이 생성되는 경우에만 수행됩니다. 기존 흐름의 패킷은 검사하지 않습니다. 또한 이 주소 검증은 로컬 링크의 호스트에 대해서만 수행할 수 있습니다.

IPv6 접두사 위임 클라이언트 구성

threat defense는 클라이언트 인터페이스(예: 케이블 모뎀에 연결된 외부 인터페이스)가 하나 이상의 IPv6 접두사를 수신할 수 있도록 DHPCv6 접두사 위임 클라이언트 역할을 수행할 수 있습니다. 그런 다음 threat defense는 내부 인터페이스에 서브넷을 지정하고 할당할 수 있습니다.

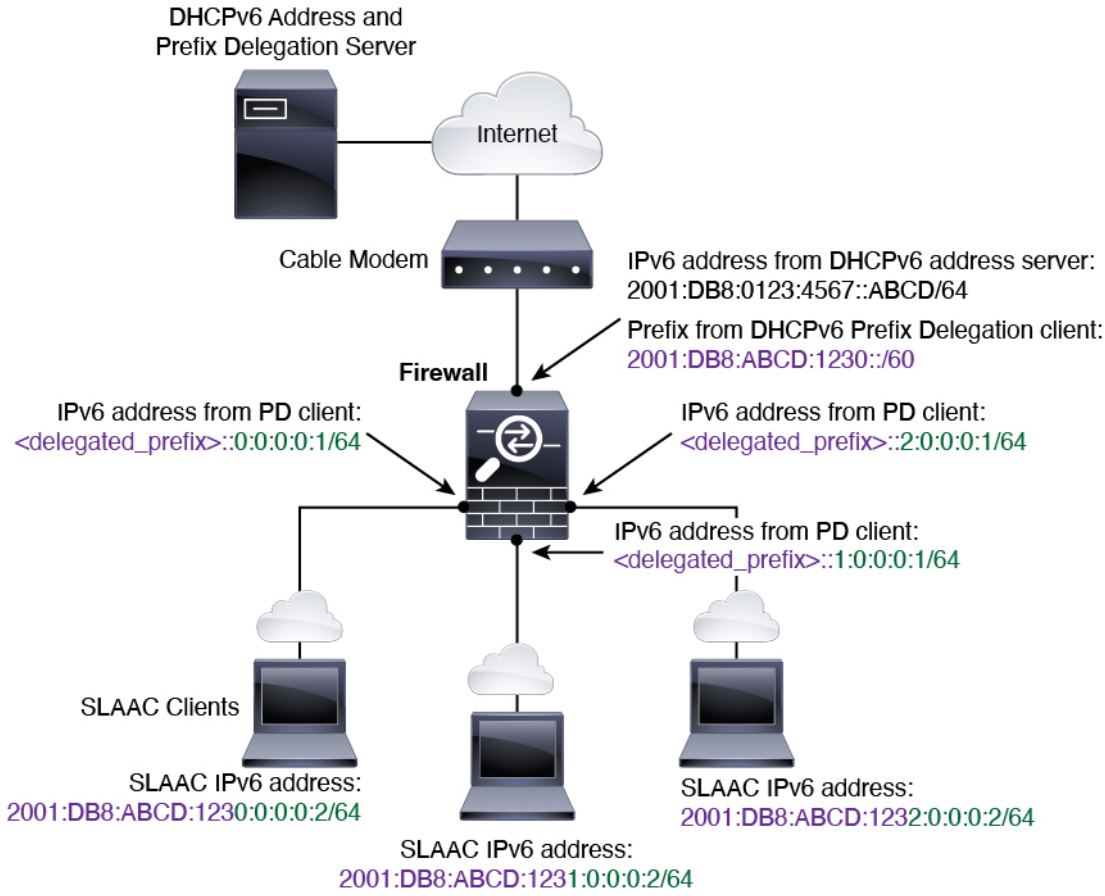
IPv6 접두사 위임 정보

threat defense는 클라이언트 인터페이스(예: 케이블 모뎀에 연결된 외부 인터페이스)가 하나 이상의 IPv6 접두사를 수신할 수 있도록 DHPCv6 접두사 위임 클라이언트 역할을 수행할 수 있습니다. 그런 다음 threat defense는 내부 인터페이스에 서브넷을 지정하고 할당할 수 있습니다. 그러면 내부 인터페이스에 연결된 호스트는 SLAAC(StateLess Address Auto Configuration)를 사용하여 전역 IPv6 주소를 획득할 수 있습니다. 내부 threat defense 인터페이스는 결과적으로 접두사 위임 서버 역할을 수행하지 않습니다. threat defense에서는 SLAAC 클라이언트에 전역 IP 주소만 제공할 수 있습니다. 예를 들어, 라우터가 threat defense에 연결된 경우, 라우터는 IP 주소를 획득하기 위해 SLAAC 클라이언트 역할을 수행할 수 있습니다. 그러나, 라우터 뒤에 있는 네트워크에 대해 위임된 접두사의 서브넷을 사용하려는 경우, 라우터의 내부 인터페이스에서 이러한 주소를 수동으로 구성해야 합니다.

threat defense에는 경량 DHCPv6 서버가 포함되어 있으므로 threat defense에서는 SLAAC 클라이언트가 threat defense에 IR(정보 요청) 패킷을 보낼 때 SLAAC 클라이언트에 DNS 서버 및 도메인 이름 등의 정보를 제공할 수 있습니다. threat defense는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다. 클라이언트에서 IPv6 자동 구성을 활성화하여 자체 IPv6 주소를 생성하도록 클라이언트를 구성합니다. 클라이언트에서 스테이트리스 자동 구성을 사용하도록 설정하면 라우터 광고 메시지에서 수신된 접두사, 즉 threat defense가 접두사 위임을 사용하여 수신한 접두사를 기준으로 IPv6 주소를 구성합니다.

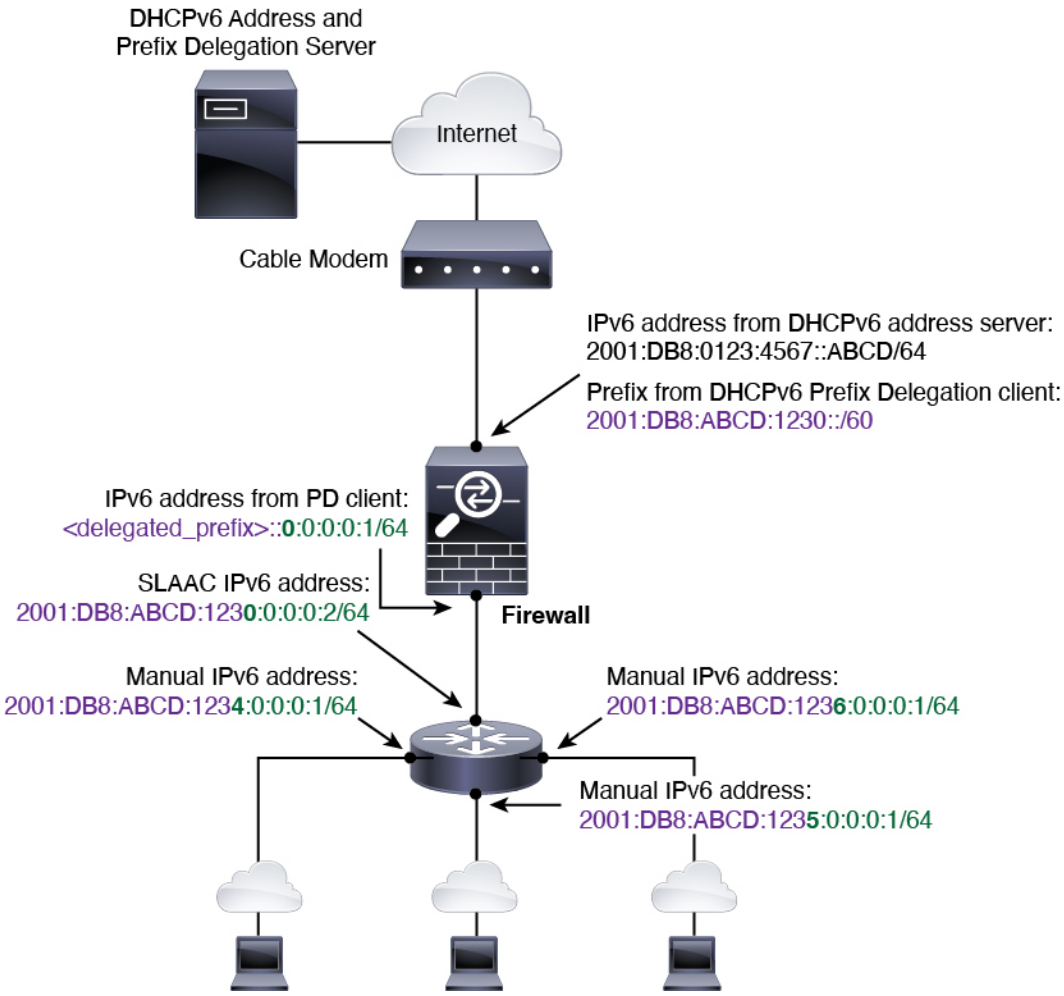
IPv6 접두사 위임 */64* 서브넷의 예

다음 예에는 DHCPv6 주소 클라이언트를 사용하여 외부 인터페이스의 IP 주소를 수신하는 threat defense가 나와 있습니다. 또한 DHCPv6 접두사 위임 클라이언트를 사용하여 위임된 접두사를 가져옵니다. threat defense에서는 위임된 접두사를 /64 네트워크에 대해 서브넷을 지정하고 전역 IPv6 주소를 위임된 접두사를 사용하여 내부 인터페이스에 동적으로 할당하고 인터페이스별로 구성된 서브넷(::0, ::1 또는 ::2)과 IPv6 주소(0:0:0:1)를 수동으로 구성합니다. 이러한 내부 인터페이스에 연결된 SLAAC 클라이언트는 각 /64 서브넷에서 IPv6 주소를 획득합니다.



IPv6 접두사 위임 */62* 서브넷의 예

다음 예에는 접두사를 4 /62 서브넷으로 서브넷 지정하는 threat defense가 나와 있습니다. 2001:DB8:ABCD:123**0**::/62, 2001:DB8:ABCD:123**4**::/62, 2001:DB8:ABCD:123**8**::/62, and 2001:DB8:ABCD:123**C**::/62. threat defense에서는 내부 네트워크(::0)에 대해 2001:DB8:ABCD:1230::/62에서 4개의 사용 가능한 /64 서브넷 중 하나를 사용합니다. 그런 다음 다운스트림 라우터에 대해 추가 /62 서브넷을 수동으로 사용할 수 있습니다. 표시된 라우터는 내부 인터페이스(::4, ::5 및 ::6)에 대해 2001:DB8:ABCD:1234::/62에서 4개의 사용 가능한 /64 서브넷 중 3개를 사용합니다. 이 경우, 내부 라우터 인터페이스는 위임된 접두사를 동적으로 획득할 수 없으므로 threat defense에서 위임된 접두사를 확인한 다음 해당 접두사를 라우터 구성에 사용해야 합니다. 일반적으로 리스가 만료되면 ISP에서는 지정된 클라이언트에 동일한 접두사를 위임하지만 threat defense에서 새 접두사를 수신하는 경우, 새 접두사를 사용하도록 라우터 구성을 수정해야 합니다. DHCP 고유 식별자(DUID)는 재부팅 시에도 유지됩니다.



IPv6 접두사 위임 클라이언트 활성화

하나 이상의 인터페이스에서 DHCPv6 접두사 위임 클라이언트를 활성화합니다. threat defense에서는 서브넷을 지정하고 내부 네트워크에 할당할 수 있는 하나 이상의 IPv6 접두사를 획득합니다. 일반적으로 접두사 위임 클라이언트를 활성화하는 인터페이스는 DHCPv6 주소 클라이언트를 사용하여 IP 주소를 획득합니다. 다른 threat defense 인터페이스만 위임된 접두사에서 파생된 주소를 사용합니다.

이 기능은 라우팅 모드에서만 지원됩니다. 이 기능은 클러스터링 또는 고가용성에서 지원되지 않습니다.

시작하기 전에

접두사 위임을 사용하는 경우, IPv6 트래픽 중단을 방지하기 위해 DHCPv6 서버에서 할당한 접두사에 기본적으로 설정된 수명보다 훨씬 낮게 threat defense IPv6 네이버 검색 라우터 알림 간격을 설정해야 합니다. 예를 들어, DHCPv6 서버에서 기본 설정 접두사 위임 수명을 300초로 설정하는 경우, threat defense RA 간격을 150초로 설정해야 합니다. 기본 설정 수명을 설정하려면 **show ipv6 general-prefix** 명령을 사용합니다. threat defense RA 간격을 설정하려면 IPv6 네이버 검색 구성, 63 페이지의 내용을 참조하십시오. 기본값은 200초입니다.

프로시저

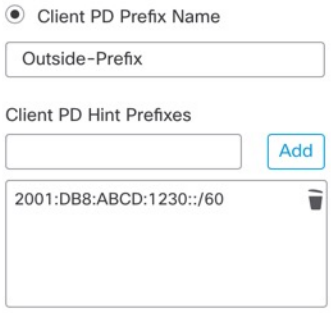
단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **IPv6** 페이지를 클릭한 다음 **DHCP**를 클릭합니다.

단계 **4** **Client PD Prefix Name(**클라이언트 **PD** 접두사 이름**)**을 클릭하고 이 접두사의 이름을 입력합니다.

그림 ***15:*** 접두사 위임 클라이언트 활성화



name은 최대 200자입니다.

단계 **5** (선택 사항) **Client PD Hint Prefixes(**클라이언트 **PD** 힌트 접두사**)** 필드에 접두사 및 접두사 길이를 입력하여 수신하려는 위임된 접두사에 대한 하나 이상의 힌트를 DHCP 서버에 제공한 다음 **Add(**추가**)**를 클릭합니다.

일반적으로 ::/60과 같은 특정한 접두사 길이를 요청하거나 이전에 특정한 접두사를 받은 적이 있으며 리스가 만료될 때 이 접두사를 다시 획득하고 싶은 경우, 전체 접두사를 힌트로 입력할 수 있습니다. 여러 힌트(다양한 접두사 또는 길이)를 입력하는 경우, 어떤 힌트를 준수할 것인지 또는 힌트를 모두 준수할 것인지 여부는 DHCP 서버에 달려 있습니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

전역 **IPv6** 주소 구성

모든 라우팅 모드 인터페이스와 투명 또는 라우팅 모드 BVI에 전역 IPv6 주소를 구성하려면, 다음 단계를 수행하십시오.

참고 전역 주소를 자동으로 구성하면 링크-로컬 주소가 구성됩니다. 즉 따로 구성할 필요 없습니다. 브리지 그룹에서 BVI에 전역 주소를 구성하면 모든 멤버 인터페이스에서 링크 로컬 주소가 자동으로 구성됩니다.

threat defense에서 정의된 하위 인터페이스는 상위 인터페이스에 동일하게 번인된 MAC 주소를 사용하기 때문에 MAC 주소의 수동 설정을 권장합니다. 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. MAC 주소 구성, 72 페이지의 내용을 참조하십시오.

Threat Defense 기능 기록**:**

- 7.3—DHCPv6 주소 클라이언트
- 7.3—DHCPv6 접두사 위임 클라이언트
- 7.3—DHCPv6 스테이트리스 서버

시작하기 전에

브리지 그룹에 대한 IPv6 네이버 검색의 경우, 양방향 액세스 규칙을 사용하여 threat defense 브리지 그룹 멤버 인터페이스를 통해 네이버 요청(ICMPv6 유형 135) 및 네이버 알림(ICMPv6 유형 136) 패킷을 명시적으로 허용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** **IPv6** 페이지를 클릭합니다.

라우팅 모드에서는 기본적으로 **Basic(**기본**)** 페이지가 선택되어 있습니다. 투명 모드에서는 기본적으로 **Address(**주소**)** 페이지가 선택되어 있습니다.

단계 **4** (선택 사항) **Basic(**기본**)** 페이지에서 **Enable IPv6(IPv6** 활성화**)**를 선택합니다.

링크-로컬 주소만 구성하려면 이 옵션을 사용합니다. 그렇지 않은 경우 IPv6 주소를 구성하면 IPv6 처리가 자동으로 활성화됩니다.

단계 **5** 다음 방법 중 하나를 사용하여 전역 IPv6 주소를 구성합니다.

루프백 인터페이스는 수동 구성만 지원합니다.

- (라우팅 인터페이스) 상태 비저장 자동 구성 - 자동 구성 확인란을 선택합니다.

  인터페이스에서 스테이트리스 자동 컨피그레이션을 활성화하면 라우터 광고 메시지에서 수신된 접두사를 기반으로 IPv6 주소가 구성됩니다. 스테이트리스 자동 컨피그레이션이 활성화될 경

우, Modified EUI-64 인터페이스 ID를 기반으로 하는 Link-Local 주소가 인터페이스에 대해 자동으로 생성됩니다.

RFC 4862에서는 스테이트리스 자동 컨피그레이션에 대해 구성한 호스트에서 라우터 알림 메시지를 전송하지 않도록 지정하지만, 이 경우에는 threat defense 디바이스에서 라우터 알림 메시지를 전송합니다. 메시지가 표시되지 않도록 하려면 **IPv6** > 설정 > **RA** 활성화 체크 박스의 선택을 취소합니다.

- 수동 컨피그레이션 — 전역 IPv6 주소를 수동으로 컨피그레이션하려면

  1. **Address(**주소**)** 페이지를 클릭하고 (+)**Add Address(**주소 추가**)**를 클릭합니다.

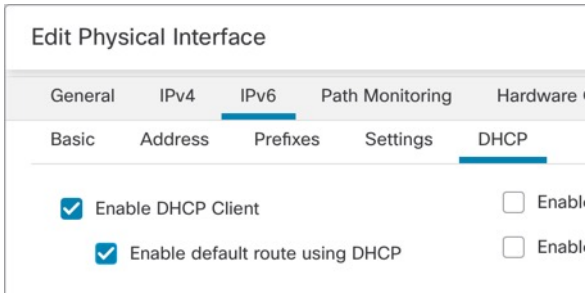
     주소 추가 대화 상자가 나타납니다.

  2. 주소 필드에 인터페이스 ID를 포함한 전체 전역 IPv6 주소를 입력하거나 IPv6 접두사 길이를 포함한 IPv6 접두사를 입력합니다. (라우팅 모드) 접두사만 입력하려면 **EUI 64** 강제 체크 박스를 선택하여 수정된 EUI-64 형식을 사용한 인터페이스 ID를 생성해야 합니다. 예를 들어, 2001:0DB8::BA98:0:3210/48(전체 주소) 또는 2001:0DB8::/48(접두사, EUI 64 선택됨) 같은 형태입니다.

     (**EUI 64** 강제를 선택하지 않은 경우) 고가용성의 경우, **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **High Availability(**고가용성**)** 페이지의 **Monitored Interfaces(**모니터링되는 인터페이스**)**에서 스탠바이 IP 주소를 설정합니다. 스탠바이 IP 주소를 설정하지 않으면 액티브 유닛이 네트워크 테스트를 사용하여 스탠바이 인터페이스를 모니터링할 수 없으며 링크 상태만 추적할 수 있습니다.

- (라우팅된 인터페이스) DHCPv6을 사용하여 주소 가져오기 - DHCPv6을 사용하려면 다음을 수행합니다.

  그림 ***16: DHCPv6*** 클라이언트 활성화

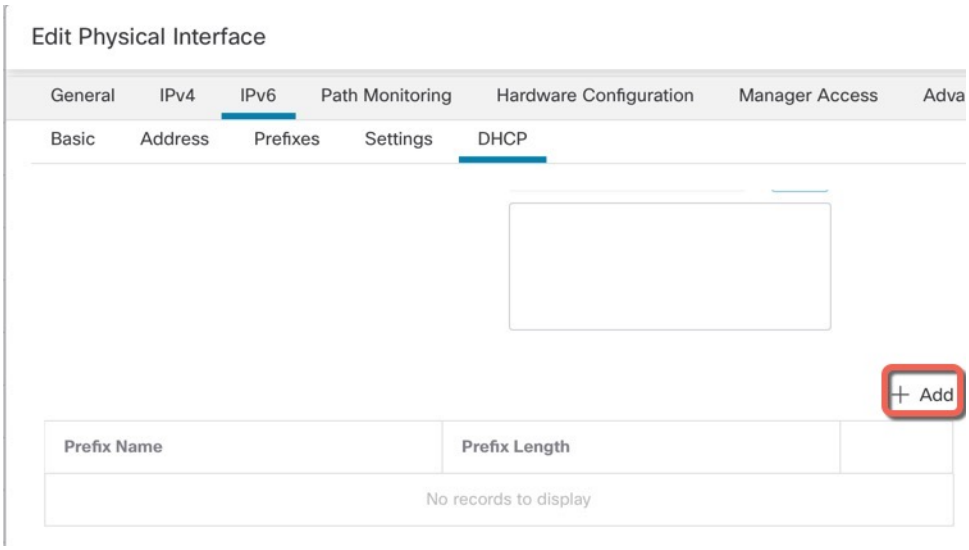
  1. **DHCP** 페이지를 클릭합니다.
  2. **Enable DHCP Client(DHCP** 클라이언트 활성화**)** 체크 박스를 선택합니다.
  3. (선택 사항) **Enable default route using DHCP(DHCP**를 사용하여 기본 경로 활성화**)** 체크 박스를 선택하여 라우터 알림에서 기본 경로를 가져옵니다.

- (라우팅된 인터페이스) 위임된 접두사 사용 - 위임된 접두사를 사용하여 IPv6 주소를 할당하려면 다음을 수행합니다.

이 기능을 사용하려면 threat defense에서 DHCPv6 접두사 위임 클라이언트를 다른 인터페이스에서 활성화해야 합니다. IPv6 접두사 위임 클라이언트 활성화, 57 페이지을 참조하십시오.

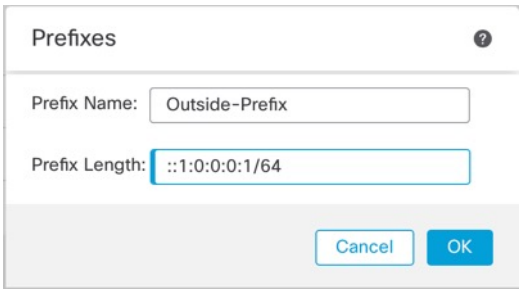
1. **DHCP** 페이지를 클릭합니다.
2. **Add(**추가**)** (+) 버튼을 클릭합니다.

   그림 ***17:*** 위임된 접두사 사용



3. 다른 인터페이스에서 접두사 위임 클라이언트(IPv6 접두사 위임 클라이언트 활성화, 57 페이지 참조)에 대해 지정한 **Prefix Name(**접두사 이름**)**을 입력합니다.

   그림 ***18:*** 접두사 이름 및 주소 지정



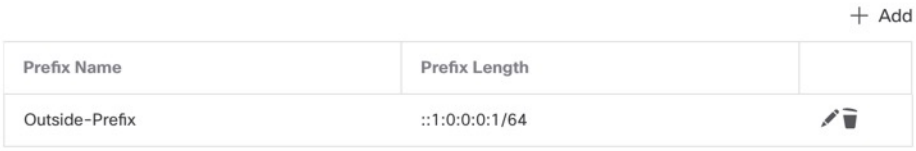
4. IPv6 주소와 접두사 길이를 입력합니다.

   일반적으로 위임된 접두사는 /60보다 작으므로 여러 개의 /64 네트워크에 서브넷을 지정할 수 있습니다. 연결된 클라이언트에 대해 SLAAC를 지원하려는 경우 /64는 지원되는 서브넷 길이입니다. /60 서브넷을 완성하는 주소를 지정해야 합니다. 예를 들어, ::1:0:0:0:1입니다. 접두사가 /60보다 작은 경우, 주소 앞에 ::를 입력합니다. 예를 들어, 위임된 접두사가 2001:DB8:1234:5670::/60인 경우, 이 인터페이스에 할당된 전역 IP 주소는 2001:DB8:1234:5671::1/64입니다. 라우터 알림에서 알려진 접두사는 2001:DB8:1234:5671::/64입니다. 이 예에서는 접두사가 /60보다 작은 경우, 접두사의 나머지 비트는 앞에 ::를 사용하

여 표시한 것처럼 0이 됩니다. 예를 들어, 접두사가 2001:DB8:1234::/48이면 IPv6 주소는 2001:DB8:1234::1:0:0:0:1/64가 됩니다.

5. **OK(**확인**)**를 클릭합니다.

그림 ***19:*** 접두사 위임 테이블



6. 선택적으로 이 인터페이스에서 DHCPv6 스테이트리스 서버를 활성화합니다(DHCPv6 스테이트리스 서버 활성화 참조). 이 경우 **Enable DHCP for non-address config(**주소 이외의 구성에 대해 **DHCP** 활성화**)** 옵션도 선택하는 것이 좋습니다.

단계 **6** 라우팅 인터페이스의 경우, **Basic(**기본**)** 페이지에서 필요에 따라 다음 값을 설정할 수 있습니다.

- 로컬 링크의 IPv6 주소에서 수정된 EUI-64 형식 인터페이스 식별자 사용을 강제하려면 **EUI-64** 체크 상자를 확인하십시오.
- 링크-로컬 주소를 수동으로 설정하려면 링크-로컬 주소 필드에 주소를 입력합니다.

  링크-로컬 주소는 FE8, FE9, FEA 또는 FEB로 시작해야 합니다(예: fe80::20d:88ff:feee:6a82). 전역 주소를 구성하지 않고 링크-로컬 주소만 구성해야 할 경우, 링크-로컬 주소를 수동으로 정의하는 옵션을 선택할 수 있습니다. 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.

단계 **7** 라우팅 인터페이스의 경우, **DHCP** 페이지에서 필요에 따라 다음 값을 설정할 수 있습니다.

- 주소 구성에 **DHCP** 사용 체크 상자를 선택하면 IPv6 라우터 알림 패킷에서 기타 주소 구성 플래그를 설정합니다.

  IPv6 라우터 알림의 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 파생된 스테이트리스 자동 컨피그레이션 주소 이외의 주소도 얻도록 안내합니다.
- 주소 외 구성에 **DHCP** 사용 체크 상자를 선택하면 IPv6 라우터 알림 패킷에서 기타 주소 구성 플래그를 설정합니다.

  IPv6 라우터 알림의 플래그는 IPv6 자동 컨피그레이션 클라이언트에게 DHCPv6를 사용하여 DHCPv6로부터 추가 정보(예: DNS 서버 주소)를 얻도록 안내합니다. DHCPv6 접두사 위임과 함께 DHCPv6 스테이트리스 서버를 사용하는 경우 이 옵션을 사용합니다.

단계 **8** 라우팅 인터페이스의 **Prefixes(**접두사**)** 및 **Settings(**설정**)** 페이지에서 설정을 구성하려면 IPv6 네이버 검색 구성, 63 페이지의 내용을 참조하십시오. BVI 인터페이스의 경우, **Settings(**설정**)** 페이지에 있는 다음의 매개변수를 확인하십시오.

- **DAD** 시도 - 최대 DAD 시도 수로 1에서 600사이의 값을 지정합니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다. 이 설정은 IPv6 주소에 대한 DAD를 수행하는 동안 인터페이스에서 전송되는 연속 네이버 요청 메시지의 개수를 구성합니다. 기본값은 1입니다.
- **NS** 간격 - 인터페이스에서 IPv6 네이버 요청 재전송 간격이며 1000~3600000밀리초 사이의 범위입니다. 기본값은 1000밀리초입니다.
- 연결 가능 확인 - 연결 가능 확인 이벤트가 일어나고 원격 IPv6 노드가 연결 가능한 것으로 간주되는 시간이며 0~3600000밀리초 사이의 범위입니다. 기본값은 0밀리초입니다. 값이 0이면 연결 가능 시간은 undetermined로 전송됩니다. 연결 가능 시간의 값을 설정하고 추적하는 일은 수신 디바이스에서 담당합니다. 네이버 연결 가능 시간으로 사용 불가 네이버를 감지할 수 있습니다. 시간을 짧게 구성하면 사용할 수 없는 네이버를 보다 빠르게 감지할 수 있지만 IPv6 네트워크 대역폭과 모든 IPv6 네트워크 디바이스의 처리 리소스를 더 많이 소비합니다. 일반적인 IPv6 운영에서는 시간을 너무 짧게 구성하지 않는 것이 좋습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

IPv6 네이버 검색 구성

IPv6 네이버 검색 프로세스는 ICMPv6 메시지와 solicited-node 멀티캐스트 주소를 사용하여 동일 네트워크(로컬 링크)에 있는 네이버의 링크 계층 주소를 확인하고 네이버의 가독성을 확인하며 주변 라우터를 추적합니다.

노드(호스트)는 네이버 검색을 사용하여 연결된 링크에 상주하는 것으로 알려진 네이버에 대한 링크 계층 주소를 확인하고 무효화되는 충돌 값을 빠르게 삭제합니다. 호스트는 또한 네이버 검색을 사용하여 대신 패킷을 전달할 의사가 있는 주변 라우터를 찾기도 합니다. 또한 노드는 프로토콜을 이용하여 네이버의 연결 가능 여부를 능동적으로 추적하고 변경된 링크 계층 주소를 감지합니다. 라우터 또는 라우터 경로가 실패할 경우 호스트가 정상 작동하는 대안을 능동적으로 검색합니다.

시작하기 전에

라우팅 모드에서만 지원됩니다. 투명 모드에서 지원되는 IPv6 네이버 설정에 대해서는 전역 IPv6 주소 구성, 58 페이지의 내용을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **IPv6**를 클릭한 다음 접두사를 클릭합니다.

단계 **4** (선택 사항) IPv6 라우터 알림에 어떤 IPv6 접두사를 포함할지 구성하려면 다음 단계를 수행합니다.

a) (+)**Add Prefix(**접두사 추가**)**를 클릭합니다.

b) 주소 필드에 접두사 길이를 포함한 IPv6 주소를 입력하거나 기본 접두사를 사용하려면 기본 확인란을 선택합니다.

c) (선택 사항) 알림의 체크 박스의 선택을 해제하면 IPv6 접두사가 알려지지 않음을 나타냅니다.

d) 오프 링크 체크 박스를 선택하면 지정된 접두사가 링크에 할당됨을 나타냅니다. 지정된 접두사를 포함한 주소로 트래픽을 보내는 노드는 링크에서 목적지와의 로컬 연결이 가능한 것으로 간주합니다. 이 접두사는 온 링크 결정에 사용할 수 없습니다.

e) 자동 설정에 지정된 접두사를 사용하려는 경우 자동 설정 확인란을 선택합니다.

f) 접두사 수명을 선택하려면 기간 또는 만료 날짜를 클릭합니다.

- 기간 - 접두사에 대한 선호 수명을 초 단위로 입력합니다. 이 설정은 지정된 IPv6 접두사가 유효 수명으로 광고되는 기간입니다. 최대값은 무한대를 나타냅니다. 유효한 값은 0~4294967295입니다. 기본값은 2592000(30일)입니다. 접두사에 대한 유효 수명을 초 단위로 입력합니다. 이 설정은 지정된 IPv6 접두사가 기본 수명으로 광고되는 기간입니다. 최대값은 무한대를 나타냅니다. 유효한 값은 0 ~ 4294967295입니다. 기본 설정은 604800(7일)입니다. 무제한 기간을 설정하려면 **Infinite(**무한**)** 체크 박스를 선택합니다.
- 만료 날짜 - 유효하고 선호되는 날짜 및 시간을 선택합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **5** 설정을 클릭합니다.

단계 **6** (선택 사항) 1~600 사이로 **DAD** 시도 최대 수를 설정합니다. 기본값은 1입니다. DAD(Duplicate Address Detection) 처리를 비활성화하려면 값을 0으로 설정합니다.

이 설정은 IPv6 주소에 대한 DAD를 수행하는 동안 인터페이스에서 전송되는 연속 네이버 요청 메시지의 개수를 구성합니다.

스테이트리스 자동 컨피그레이션 프로세스에서 DAD(Duplicate Address Detection)는 새로운 유니캐스트 IPv6 주소가 고유한지 확인한 다음 주소를 인터페이스에 할당합니다.

중복 주소가 확인되면 주소 상태가 DUPLICATE로 설정되고 주소가 사용되지 않으며 다음 오류 메시지가 생성됩니다.

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

중복 주소가 인터페이스의 링크-로컬 주소인 경우 인터페이스의 IPv6 패킷 처리가 사용 해제됩니다. 중복 주소가 전역 주소인 경우 주소가 사용되지 않습니다.

단계 **7** (선택 사항) **NS** 간격 필드에서 1000~3600000밀리초 사이로 IPv6 네이버 요청 재전송 간격을 설정합니다.

기본값은 1000밀리초입니다.

네이버 요청 메시지(ICMPv6 Type 135)는 로컬 링크에 있는 다른 노드의 링크 계층 주소를 발견하려는 노드가 로컬 링크에서 전송합니다. 네이버 요청 메시지를 수신한 후 목적지 노드는 로컬 링크에서 네이버 광고 메시지(ICPMv6 Type 136)를 전송함으로써 응답합니다.

소스 노드가 네이버 광고를 수신한 후 소스 노드와 목적지 노드가 통신할 수 있습니다. 네이버 요청 메시지는 네이버의 링크 계층 주소를 식별한 후 네이버의 연결 가능성을 확인하는 데 사용됩니다. 노드가 네이버의 연결 가능성을 확인하고자 하는 경우 네이버 요청 메시지의 목적지 주소는 네이버의 유니캐스트 주소입니다.

네이버 광고 메시지는 로컬 링크에 있는 노드의 링크 계층 주소가 변경될 경우에도 전송됩니다.

단계 **8** (선택 사항) 연결 가능 확인 이벤트가 일어나고 원격 IPv6 노드가 연결 가능한 것으로 간주되는 시간을 연결 가능 확인 필드에 0~3600000밀리초 사이의 범위로 입력합니다.

기본값은 0밀리초입니다. 값이 0이면 연결 가능 시간은 undetermined로 전송됩니다. 연결 가능 시간의 값을 설정하고 추적하는 일은 수신 디바이스에서 담당합니다.

네이버 연결 가능 시간으로 사용 불가 네이버를 감지할 수 있습니다. 시간을 짧게 구성하면 사용할 수 없는 네이버를 보다 빠르게 감지할 수 있지만 IPv6 네트워크 대역폭과 모든 IPv6 네트워크 디바이스의 처리 리소스를 더 많이 소비합니다. 일반적인 IPv6 운영에서는 시간을 너무 짧게 구성하지 않는 것이 좋습니다.

단계 **9** (선택 사항) 라우터 알림 전송을 원하지 않을 경우 **RA** 활성화 체크 박스의 선택을 취소합니다. 라우터 알림 전송을 활성화하는 경우 RA 수명 및 간격을 설정할 수 있습니다.

라우터 알림 메시지(ICMPv6 Type 134)는 라우터 요청 메시지(ICMPv6 Type 133)에 대한 응답으로 자동 전송됩니다. 예정된 다음 라우터 광고 메시지를 기다릴 필요 없이 호스트가 즉시 자동 구성을 할 수 있도록 시스템 시동 시 라우터 요청 메시지가 전송됩니다.

threat defense가 IPv6 접두사를 전송하길 원치 않는 인터페이스에서 이 메시지를 비활성화할 수 있습니다(예: 인터페이스 외부).

- **RA** 수명 - 0~9000초 사이로 IPv6 라우터 알림에서 라우터 수명 값을 구성합니다.

  기본값은 1800초입니다.

- **RA** 간격 - 3~1800초 사이로 IPv6 라우터 알림 전송 간격을 구성합니다.

  기본값은 200초입니다.

단계 **10** **OK(**확인**)**를 클릭합니다.

단계 **11** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

고급 인터페이스 설정 구성

이 섹션에서는 일반 방화벽 모드 인터페이스에 대한 MAC 주소를 구성하는 방법, 최대 전송 단위(MTU)를 설정하는 방법, 기타 고급 파라미터를 설정하는 방법을 설명합니다.

고급 인터페이스 구성 정보

이 섹션에서는 고급 인터페이스 설정을 설명합니다.

MAC 주소 정보

MAC 주소를 수동으로 할당하여 기본값을 재정의할 수 있습니다. . 컨테이너 인스턴스의 경우 FXOS 섀시는 모든 인터페이스에 대해 고유 MAC 주소를 자동으로 생성합니다.

참고 threat defense에 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.

참고 컨테이너 인스턴스의 경우에는 하위 인터페이스를 공유하지 않더라도 MAC 주소를 수동으로 구성하는 경우에는 패킷이 적절하게 분류되도록 같은 상위 인터페이스의 모든 하위 인터페이스에 대해 고유 MAC 주소를 사용해야 합니다.

기본 MAC 주소

기본 인스턴스의 경우:

기본 MAC 주소 할당은 인터페이스의 유형에 따라 다릅니다.

- 물리적 인터페이스 - 물리적 인터페이스는 버닝된 MAC 주소를 사용합니다.
- VLAN 인터페이스(Firepower 1010) - 라우팅된 방화벽 모드: 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. MAC 주소 구성, 72 페이지의 내용을 참조하십시오.

  투명 방화벽 모드: 각 VLAN 인터페이스에는 고유한 MAC 주소가 있습니다. 원하는 경우 MAC 주소를 수동으로 할당하여 생성된 MAC 주소를 재정의할 수 있습니다. MAC 주소 구성, 72 페이지를 참조하십시오.

- EtherChannel(Firepower 모델) - 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.
- EtherChannel(ASA 모델) - 포트-채널 인터페이스는 가장 낮은 번호의 채널 그룹 인터페이스 MAC 주소를 포트-채널 MAC 주소로 사용합니다. 또는 포트-채널 인터페이스의 MAC 주소를 구성할 수도 있습니다. 그룹 채널 인터페이스 멤버십이 변경될 경우 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.
- 하위 인터페이스(threat defense에서 정의) - 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.

컨테이너 인스턴스의 경우:

- 모든 인터페이스의 MAC 주소를 MAC 주소 풀에서 가져옵니다. 하위 인터페이스의 경우에는 MAC 주소를 수동으로 구성할 때 적절한 분류를 위해 동일한 상위 인터페이스의 모든 하위 인터페이스에 대해 고유한 MAC 주소를 사용해야 합니다. 컨테이너 인스턴스 인터페이스용 자동 MAC 주소의 내용을 참조하십시오.

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.

Geneve의 경우 전체 이더넷 데이터그램이 캡슐화되므로 새 IP 패킷이 더 크기 때문에 더 큰 MTU가 필요합니다. 따라서 ASA VTEP 소스 인터페이스 MTU를 네트워크 MTU + 306바이트로 설정해야 합니다.

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.

기본 MTU

위협 방지 디바이스의 기본 MTU는 1500바이트입니다. 이 값에는 18~22바이트의 이더넷 헤더, VLAN 태깅 또는 기타 오버헤드가 포함되지 않습니다.

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.

TCP 패킷의 경우 엔드포인트는 일반적으로 해당 MTU를 사용해 TCP 최대 세그먼트 크기(예: MTU - 40)를 결정합니다. 중간에 사이트 대 사이트 VPN 터널 등에 사용하기 위해 TCP 헤더가 더 추가된 경우에는 터널링 엔티티를 통해 TCP MSS를 하향 조정해야 할 수 있습니다. TCP MSS 정보, 68 페이지를 참조하십시오.

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 프레임을 활성화할 때 MTU를 9000바이트 이상으로 설정할 수 있습니다. 최대값은 모델에 따라 다릅니다.

TCP MSS 정보

TCP MSS(최대 세그먼트 크기)는 TCP 및 IP 헤더가 추가되기 전의 TCP 페이로드 크기입니다. UDP 패킷은 영향을 받지 않습니다. 연결을 설정할 경우 클라이언트와 서버에서는 3방향 핸드셰이크 동안 TCP MSS 값을 교환합니다.

위협 방지 디바이스에서 통과 트래픽에 대해 FlexConfig 참조) TCP MSS를 설정할 수 있습니다(#unique_142 참조). 기본적으로 최대 TCP MSS는 1380바이트로 설정됩니다. 이 설정은 위협 방지 디바이스에서 IPsec VPN 캡슐화를 할 때 패킷 크기를 추가해야 하는 경우 유용합니다. 그러나 IPsec 이외의 엔드포인트에 대해서는 위협 방지 디바이스에서 최대 TCP MSS를 비활성화해야 합니다.

최대 TCP MSS를 설정하는 경우, 연결의 엔드포인트에서 위협 방지 디바이스에 설정된 값보다 큰 TCP MSS를 요청하면 위협 방지 디바이스에서는 요청 패킷의 TCP MSS를 위협 방지 디바이스 최대 값으로 덮어씁니다. 호스트 또는 서버에서 TCP MSS를 요청하지 않을 경우, 위협 방지 디바이스에서는 RFC 793 기본값을 536바이트(IPv4) 또는 1220바이트(IPv6)로 가정하며 패킷을 수정하지 않습니다. 기본 MTU를 1500바이트로 유지하는 경우를 예로 들어보겠습니다. 이 경우 호스트는 1500바이트에서 TCP 및 IP 헤더 길이를 뺀 MSS를 요청하므로 MSS는 1460으로 설정됩니다. 위협 방지 디바이스 최대 TCP MSS가 1380(기본값)이면 위협 방지 디바이스에서는 TCP 요청 패킷의 MSS 값을 1380으로

변경합니다. 그러면 서버에서는 1380바이트 페이로드가 포함된 패킷을 전송합니다. 이 경우 위협 방지 디바이스이(가) 최대 120바이트의 헤더를 패킷에 추가해도 MTU 크기인 1500을 맞출 수 있습니다.

또한 최소 TCP MSS를 구성할 수 있습니다. 호스트 또는 서버에서 요청한 TCP MSS가 매우 작을 경우, 위협 방지 디바이스에서는 값을 조정하여 올릴 수 있습니다. 기본적으로 최소 TCP MSS는 활성화되어 있지 않습니다.

SSL VPN 연결 트래픽을 포함한 to-the-box 트래픽에는 이 설정이 적용되지 않습니다. 이 경우 위협 방지 디바이스에서는 MTU를 사용하여 TCP MSS: MTU - 40(IPv4) 또는 MTU - 60(IPv6)을 파생합니다.

기본 **TCP MSS**

기본적으로 위협 방지 디바이스의 최대 TCP MSS는 1380바이트입니다. 이 기본값을 사용하면 헤더가 120바이트와 동일한 값까지 가능한 경우 IPv4 IPsec VPN 연결을 수용하는 것이 가능합니다. 이 값은 기본값이 1500바이트인 MTU에 적합합니다.

최대 **TCP MSS** 설정 제안

기본 TCP MSS는 위협 방지 디바이스가 IPv4 IPsec VPN 엔드포인트 역할을 수행하고 1500바이트의 MTU를 갖는다고 가정합니다. 위협 방지 디바이스가 IPv4 IPsec VPN 엔드포인트 역할을 수행하는 경우, TCP 및 IP 헤더용으로 최대 120바이트까지 수용해야 합니다.

MTU 값을 변경하고 IPv6를 사용하거나 위협 방지 디바이스를 IPsec VPN 엔드포인트로 사용하지 않는 경우, FlexConfig에서 Sysopt_Basic 개체를 사용하여의 내용을 참조하십시오.

참고 MSS를 명시적으로 설정하더라도 TLS/SSL 암호 해독 또는 서버 검색과 같은 구성 요소에 특정 MSS가 필요한 경우, 인터페이스 MTU를 기반으로 해당 MSS를 설정하고 MSS 설정을 무시합니다.

다음 지침을 참조하십시오.

- 정상 트래픽 — TCP MSS 제한을 비활성화하고 연결 엔드포인트 간에 설정한 값을 허용합니다. 연결 엔드포인트의 경우 대개 MTU에서 TCP MSS가 파생되므로 비 IPsec 패킷은 일반적으로 이러한 TCP MSS에 적합합니다.
- IPv4 IPsec 엔드포인트 트래픽 — MTU에 대한 최대 TCP MSS를 120으로 설정합니다. 예를 들어, 점보 프레임을 사용하고 MTU를 9000으로 설정할 경우 새로운 MTU를 활용하기 위해 TCP MSS를 8880으로 설정해야 합니다.
- IPv6 IPsec 엔드포인트 트래픽 — MTU에 대한 최대 TCP MSS를 140으로 설정합니다.

브리지 그룹 트래픽에 대한 **ARP** 검사

기본적으로 모든 ARP 패킷은 브리지 그룹 멤버 간에 허용됩니다. ARP 감시를 활성화하여 ARP 패킷의 흐름을 제어할 수 있습니다.

ARP 감시 기능은 악의적인 사용자가 다른 호스트 또는 라우터로 위장(ARP 스푸핑이라고도 함)하는 것을 방지합니다. ARP 스푸핑은 "끼어들기" 공격을 활성화할 수 있습니다. 예를 들어, 호스트에서 ARP 요청을 게이트웨이 라우터에 전송할 경우 해당 게이트웨이 라우터는 게이트웨이 라우터 MAC 주소에 응답합니다. 그러나 공격자는 라우터 MAC 주소가 아닌 공격자 MAC 주소가 포함된 다른 ARP

응답을 호스트에 전송합니다. 이제 공격자는 라우터에 트래픽이 전달되기 전에 모든 호스트 트래픽을 가로챌 수 있게 됩니다.

ARP 감시 기능은 고정 ARP 테이블에 올바른 MAC 주소와 관련 IP 주소를 입력하기만 하면 공격자가 공격자 MAC 주소가 포함된 ARP 응답을 보낼 수 없도록 합니다.

ARP 감시를 활성화할 경우 위협 방지 디바이스에서는 MAC 주소, IP 주소, 모든 ARP 패킷의 소스 인터페이스를 ARP 테이블의 고정 항목과 비교하고 다음과 같은 조치를 취합니다.

- IP 주소, MAC 주소, 소스 인터페이스가 ARP 항목과 일치하면 패킷이 통과됩니다.
- MAC 주소와 IP 주소 또는 인터페이스 간에 불일치하는 항목이 있을 경우 위협 방지 디바이스에서는 패킷을 누락시킵니다.
- ARP 패킷이 고정 ARP 테이블의 어느 항목과도 일치하지 않으면 위협 방지 디바이스를 설정하여 패킷을 모든 인터페이스로 전달(플러딩)하거나 패킷이 누락되도록 합니다.

참고 전용 진단 인터페이스는 이 파라미터가 플러딩을 실행하도록 설정된 경우에도 패킷을 플러딩하지 않습니다.

MAC 주소 테이블

브리지 그룹을 사용할 때 threat defense에서는 일반적인 브리지 또는 스위치와 유사한 방식으로 MAC 주소 테이블을 학습하고 구축합니다. 디바이스에서 브리지 그룹을 통해 패킷을 전송하면 threat defense에서는 MAC 주소를 해당 테이블에 추가합니다. 테이블에서는 MAC 주소와 소스 인터페이스를 연결하므로 threat defense에서는 디바이스에 대해 주소가 지정된 모든 패킷을 올바른 인터페이스로 전송할 수 있다는 사실을 파악합니다. 브리지 그룹 멤버는 threat defense 보안 정책의 적용을 받으므로, 패킷의 목적지 MAC 주소가 테이블에 없다면 일반적인 브리지에서는 원래 패킷을 모든 인터페이스에 플러딩하지만 threat defense의 경우에는 이러한 작업을 수행하지 않습니다. 그 대신 ASA에서는 직접 연결된 디바이스 또는 원격 디바이스에 다음 패킷을 생성합니다.

- 직접 연결된 디바이스에 대한 패킷 - threat defense에서 대상 IP 주소에 대한 ARP 요청을 생성하므로 어떤 인터페이스에서 ARP 응답을 수신하는지 알 수 있습니다.
- 원격 디바이스에 대한 패킷 — threat defense에서 대상 IP 주소에 대한 Ping을 생성하므로 어떤 인터페이스에서 Ping 응답을 수신하는지 알 수 있습니다.

원래 패킷은 손실됩니다.

기본 설정

- ARP 감시를 활성화할 경우 기본 설정은 불일치 패킷을 플러딩하는 것입니다.
- 동적 MAC 주소 테이블 항목의 기본 시간 초과 값은 5분입니다.
- 기본적으로 각 인터페이스에서는 들어오는 트래픽의 MAC 주소를 자동으로 알게 되며, 위협 방지 디바이스에서는 해당 항목을 MAC 주소 테이블에 추가합니다.

참고 Secure Firewall Threat Defense 디바이스 상태 기반 검사 엔진에 의해 거부된 연결을 재설정하기 위한 재설정 패킷을 생성합니다. 여기서 패킷의 대상 MAC 주소는 ARP 테이블 조회를 기반으로 결정되지 않지만 거부되는 패킷(연결)에서 직접 가져옵니다.

ARP 검사 및 MAC 주소 테이블에 대한 지침

- ARP 검사는 브리지 그룹에만 지원됩니다.
- MAC 주소 테이블 구성은 브리지 그룹에만 지원됩니다.

MTU 구성

점보 프레임을 허용하려면 인터페이스에서 MTU를 사용자 정의해야 합니다.

ASA 모델의 경우 ISA 3000 및 threat defense virtual에서 MTU를 1500바이트 이상으로 변경하면 점보 프레임 예약이 자동으로 활성화됩니다. 점보 프레임을 사용하려면 먼저 시스템을 재시작해야 합니다. 클러스터링을 지원하는 threat defense virtual의 경우 Day0 구성에서 점보 프레임 예약을 활성화할 수 있으므로 이 경우 재시작할 필요가 없습니다. 재시작한 후에는 점보 프레임 예약을 비활성화할 수 없습니다. threat defense virtual의 경우는 예외입니다. Day0 구성에서 점보 프레임 예약을 비활성화할 수 있습니다(지원되는 경우). 인라인 집합의 인터페이스를 사용하는 경우 MTU 설정이 사용되지 않습니다. 그러나 점보 프레임 예약 설정은 인라인 집합과 관련이 있으며 점보 프레임은 최대 9000바이트까지 패킷을 수신하도록 인라인 인터페이스를 활성화합니다. 점보 프레임 예약을 활성화하려면 모든 인터페이스의 MTU를 1500바이트 이상으로 설정해야 합니다.

점보 프레임은 다른 플랫폼에서 기본적으로 활성화됩니다.

주의 데이터 인터페이스에 대해 디바이스의 최고 MTU 값을 변경하면 구성 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 수정한 인터페이스만이 아니라 모든 데이터 인터페이스에서 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 또는 추가 검사 없이 통과되는지 여부는 매니지드 디바이스의 모델 및 인터페이스 유형에 따라 달라집니다. 이 주의 사항은 진단 인터페이스 또는 관리 전용 인터페이스에는 적용되지 않습니다. 자세한 내용은 Snort 재시작 트래픽 동작를 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **General(**일반**)** 탭에서 **MTU**를 설정합니다. 최소값과 최대값은 플랫폼에 따라 다릅니다.

기본값은 1500바이트입니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

단계 **6** 의 경우 ISA 3000 및 threat defense virtual에서 MTU를 1500바이트 이상으로 변경하면 시스템이 재시작되어 점보 프레임 예약이 활성화됩니다. 디바이스 종료 또는 재시작의 내용을 참조하십시오.

MAC 주소 구성

MAC 주소를 수동으로 할당해야 할 수 있습니다. 또한 디바이스 > 기기 관리 > 고가용성 탭에서 액티브 및 스탠바이 MAC 주소를 설정할 수 있습니다. 두 화면의 인터페이스에 대한 MAC 주소를 설정하는 경우 인터페이스 > 고급 탭의 주소가 우선 적용됩니다.

참고 컨테이너 인스턴스의 경우에는 하위 인터페이스를 공유하지 않더라도 MAC 주소를 수동으로 구성하는 경우에는 패킷이 적절하게 분류되도록 같은 상위 인터페이스의 모든 하위 인터페이스에 대해 고유 MAC 주소를 사용해야 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **Advanced(**고급**)** 탭을 클릭합니다.
정보 탭을 선택합니다.

단계 **4** 액티브 **MAC** 주소 필드에 H.H.H. 형식으로 MAC 주소를 입력하고, 여기서 H는 16비트 16진수입니다.

예를 들어, MAC 주소 00-0C-F1-42-4C-DE는 000C.F142.4CDE로 입력됩니다. MAC 주소에는 멀티캐스트 비트를 설정해서는 안 됩니다. 즉, 왼쪽에서 두 번째 16진수는 홀수일 수 없습니다.

단계 **5** 스탠바이 **MAC** 주소에 고가용성에 사용할 MAC 주소를 입력합니다.

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 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

고정 **ARP** 항목 추가

기본적으로 모든 ARP 패킷은 브리지 그룹 멤버 간에 허용됩니다. ARP 검사를 활성화하여 ARP 패킷 플로우를 제어할 수 있습니다.(ARP 감시 참조) ARP 검사에서는 ARP 패킷을 ARP 테이블의 고정 ARP 항목과 비교합니다.

라우팅 인터페이스의 경우 고정 ARP 항목을 입력할 수 있지만 일반적으로 동적 항목이면 충분합니다. 라우팅 인터페이스의 경우 직접 연결된 호스트에 패킷을 전달하는 데 ARP 테이블이 사용됩니다. 발신자가 IP 주소로 패킷 대상을 식별하긴 하지만, 이더넷에서 패킷이 실제 전달되는 것은 이더넷 MAC 주소에 달려 있습니다. 라우터 또는 호스트에서 패킷을 직접 연결된 디바이스에 전달하려는 경우, IP 주소와 연관된 MAC 주소를 묻는 ARP 요청이 전송되며 그 후 ARP 응답에 따라 패킷이 MAC 주소로 전달됩니다. 호스트 또는 라우터에서는 ARP 테이블을 보관하므로, 모든 패킷을 전달할 때마다 ARP 요청을 보내지 않아도 됩니다. ARP 테이블은 ARP 응답이 네트워크로 전송될 때마다 동적으로 업데이트되며, 일정 기간 동안 사용되지 않는 항목이 있으면 해당 항목은 시간 초과로 만료됩니다. 항목이 잘못된 경우(예: 제공된 IP 주소의 MAC 주소가 변경된 경우), 해당 항목은 새 정보로 업데이트되기 전에 시간 제한에 도달해야 합니다.

투명 모드의 경우 threat defense은 관리 트래픽 등 threat defense 디바이스와 주고받는 ARP 테이블의 다이내믹 ARP 항목만 사용합니다.

시작하기 전에

이 화면은 명명된 인터페이스에서만 사용 가능합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** ( )를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **Advanced(**고급**)** 탭을 클릭하고 **ARP** 탭(투명 모드의 경우 **ARP and MAC(ARP** 및 **MAC)**)을 클릭합니다.

단계 **4** ( )**Add ARP Config(ARP** 구성 추가**)**를 클릭합니다.
Add ARP Config(ARP 구성 추가**)** 대화 상자가 나타납니다.

단계 **5** **IP Address(IP** 주소**)** 필드에 호스트의 IP 주소를 입력합니다.

단계 **6** **MAC Address(MAC** 주소**)** 필드에 호스트의 MAC 주소를 00e0.1e4e.3d8b과 같은 형식으로 입력합니다.

단계 **7** 이 주소에 대해 프록시 ARP를 수행하려면 **Enable Alias(**별칭 활성화**)** 체크 박스를 선택합니다.

지정된 IP 주소의 ARP 요청이 threat defense 디바이스에 수신되면 ASA에서는 지정된 MAC 주소에 응답합니다.

단계 **8** **OK(**확인**)**를 클릭하고 고급 설정에서 나가려면 다시 **OK(**확인**)**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

고정 MAC 주소를 추가하고 브리지 그룹에 대한 MAC 학습을 비활성화

일반적으로 MAC 주소는 특정 MAC 주소의 트래픽이 인터페이스에 들어올 때 MAC 주소 테이블에 동적으로 추가됩니다. MAC 주소 학습을 비활성화할 수 있으나, 테이블에 MAC 주소를 고정으로 추가하지 않으면 트래픽이 threat defense를 통과하여 전달될 수 없습니다. 고정 MAC 주소를 MAC 주소 테이블에 추가할 수 있습니다. 고정 항목을 추가함으로써 얻을 수 있는 한 가지 혜택은 MAC 스푸핑을 차단할 수 있다는 점입니다. 동일한 MAC 주소를 고정 항목으로 보유한 클라이언트에서 고정 항목이 일치하지 않는 인터페이스에 트래픽을 전송하려고 시도할 경우, threat defense 디바이스에서는 해당 트래픽을 누락하며 시스템 메시지가 생성됩니다. 고정 ARP 항목을 추가할 경우(고정 ARP 항목 추가, 73 페이지 참조), 고정 MAC 주소가 MAC 주소 테이블에 자동으로 추가됩니다.

시작하기 전에

이 화면은 명명된 인터페이스에서만 사용 가능합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** **Advanced(**고급**)** 탭을 클릭하고 **ARP and MAC(ARP** 및 **MAC)** 탭을 클릭합니다.

단계 **4** (선택 사항) **Enable MAC Learning(MAC** 학습 활성화**)** 체크 박스 선택을 취소하여 MAC 학습을 비활성화합니다.

단계 **5** 고정 MAC 주소를 추가하려면 **Add MAC Config(MAC** 구성 추가**)**를 클릭합니다.
Add MAC Config(MAC 구성 추가**)** 대화 상자가 나타납니다.

단계 **6** **MAC Address(MAC** 주소**)** 필드에 호스트의 MAC 주소를 00e0.1e4e.3d8b과 같은 형식으로 입력합니다. **OK(**확인**)**를 클릭합니다.

단계 **7** 고급 설정에서 나가려면 **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

보안 구성 파라미터 설정

이 섹션에서는 IP 스푸핑을 방지하여 전체 프래그먼트 리어셈블리를 허용하고 플랫폼 설정의 디바이스 수준에서 기본 프래그먼트 설정 집합을 오버라이드하는 방법을 설명합니다.

스푸핑 차단

이 섹션에서는 인터페이스의 유니캐스트 역방향 경로 전달을 활성화합니다. 유니캐스트 RPF는 모든 패킷이 라우팅 테이블에 따라 올바른 소스 인터페이스와 일치하는 소스 IP 주소를 갖도록 보장함으로써 IP 스푸핑(실제 소스를 알아볼 수 없도록 패킷이 잘못된 소스 IP 주소를 사용함)을 방지합니다.

일반적으로 threat defense 디바이스는 패킷을 어디로 전달할지를 결정할 때 수신 주소만 확인합니다. 유니캐스트 RPF는 디바이스에 소스 주소도 확인하도록 지시합니다. 따라서 이것을 RPF(Reverse Path Forwarding)라고 부릅니다. threat defense 디바이스의 통과를 허용할 모든 트래픽에 대해 디바이스 라우팅 테이블은 소스 주소로 돌아가는 경로를 포함해야 합니다. 자세한 내용은 RFC 2267을 참조하십시오.

예를 들어 외부 트래픽의 경우 threat defense 디바이스는 유니캐스트 RPF 보호를 충족하기 위해 기본 경로를 사용할 수 있습니다. 트래픽이 외부 인터페이스에서 들어오고 소스 주소가 라우팅 테이블에 알려지지 않은 경우, 디바이스는 기본 경로를 사용하여 외부 인터페이스를 소스 인터페이스로서 정확히 식별합니다.

트래픽이 라우팅 테이블에 알려진 주소에서 외부 인터페이스로 이동하는 경우 threat defense 디바이스는 패킷을 삭제합니다. 마찬가지로, 트래픽이 알려지지 않은 소스 주소로부터 내부 인터페이스로 이동하는 경우 일치하는 경로(기본 경로)가 외부 인터페이스임을 나타내기 때문에 디바이스는 패킷을 삭제합니다.

유니캐스트 RPF는 다음과 같이 구현됩니다.

- ICMP 패킷에는 세션이 없으므로 각 패킷이 점검됩니다.
- UDP 및 TCP에는 세션이 있으므로 초기 패킷에서 역방향 경로 조회를 요구합니다. 세션 중에 도착하는 후속 패킷은 세션의 일부로서 유지 관리되는 기존 상태를 사용하여 점검됩니다. 초기 패킷 이외의 패킷에서는 초기 패킷에 사용된 것과 동일한 인터페이스에 도착했는지를 확인합니다.

패킷당 프래그먼트

기본적으로 threat defense 디바이스는 IP 패킷당 최대 24 프래그먼트를 허용하고 리어셈블리 대기열에 최대 200개의 프래그먼트를 허용합니다. UDP를 통한 NFS와 같이 일상적으로 패킷을 프래그먼트하는 애플리케이션이 있는 경우 네트워크에 프래그먼트가 필요할 수도 있습니다. 그러나 트래픽을 프래그먼트하는 애플리케이션이 없으면 threat defense 디바이스로 프래그먼트를 허용하지 않는 것이 좋습니다. 프래그먼트 패킷은 종종 서비스 거부(DoS) 공격으로 사용됩니다.

프래그먼트 리어셈블리

threat defense 디바이스는 다음 프래그먼트 리어셈블리 프로세스를 수행합니다.

- IP 프래그먼트는 프래그먼트 집합이 구성되거나 시간 초과 간격이 경과할 때까지 수집됩니다.
- 어떤 프래그먼트 집합이 구성되면 그 집합에 대해 무결성 검사가 실시됩니다. 이 검사에서는 중복, 테일 오버플로우, 체인 오버플로우가 없는지도 검사합니다.
- threat defense 디바이스에서 종료하는 IP 프래그먼트는 항상 완전히 재결합됩니다.
- 전체 프래그먼트 리어셈블리가 비활성화된 경우(기본), 프래그먼트 집합은 추가 처리를 위해 전송 레이어에 전달됩니다.
- 전체 프래그먼트 리어셈블리를 활성화하는 경우 프래그먼트 집합은 단일 IP 패킷에 먼저 결합됩니다. 이 단일 IP 패킷이 추가 처리를 위해 전송 계층으로 전달됩니다.

시작하기 전에

이 화면은 명명된 인터페이스에서만 사용 가능합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 threat defense 디바이스에 대한 **Edit(**수정**)** (✎)를 클릭합니다. 기본적으로는 **Interfaces(**인터페이스**)** 페이지가 선택됩니다.

단계 **2** 수정할 인터페이스의 **Edit(**수정**)** (✎)을 클릭합니다.

단계 **3** 고급 탭을 클릭하고 보안 설정 탭을 클릭합니다.

단계 **4** 유니캐스트 역방향 경로 전송을 활성화하려면 **Enable Anti Spoofing(**스푸핑 차단 활성화**)** 체크 박스를 선택합니다.

단계 **5** 전체 프래그먼트 리어셈블리를 활성화하려면 **Allow Full Fragment Reassembly(**전체 프래그먼트 리어셈블리 허용**)** 체크 박스를 선택합니다.

단계 **6** 패킷당 허용되는 프래그먼트의 수를 변경하려면 기본 프래그먼트 설정 오버라이드 체크 박스를 선택하고 다음 값을 설정합니다.

- 크기 - 리어셈블리를 위해 대기하는 IP 리어셈블리 데이터베이스에 포함될 수 있는 최대 패킷 수를 설정합니다. 기본값은 200입니다. 비활성화 프래그먼트는 1로 설정합니다.
- 체인 - 프래그먼트가 가능한 전체 IP 패킷의 최대 패킷 수입니다. 기본값은 24패킷입니다.
- 시간 초과 - 프래그먼트된 전체 패킷이 도착할 때까지 대기하는 최대 시간(초)입니다. 패킷의 첫 번째 프래그먼트가 도착하면 타이머가 시작됩니다. 패킷의 모든 프래그먼트가 지정된 시간(초)에 도착하지 않을 경우 이미 수신된 패킷의 프래그먼트는 모두 폐기됩니다. 기본값은 5일입니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

Secure Firewall Threat Defense의 일반 방화벽 인터페이스 기록

기능	버전	세부 사항
VTI에 대한 루프백 인터페이스 지원	7.3	이제 루프백 인터페이스를 추가할 수 있습니다. 루프백 인터페이스는 경로 장애를 극복하는 데 도움이 됩니다. 인터페이스가 다운되면 루프백 인터페이스에 할당된 IP 주소를 통해 모든 인터페이스에 액세스할 수 있습니다. VTI의 경우 루프백 인터페이스를 소스 인터페이스로 설정하는 것 외에도 고정으로 구성된 IP 주소 대신 루프백 인터페이스에서 IP 주소를 상속받는 지원이 추가되었습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interface(**인터페이스**)** > **Add Interface(**인터페이스 추가**)** > **Add Loopback Interface(**루프백 인터페이스 추가**)**
IPv6 DHCP	7.3	이제 threat defense에서 IPv6 주소 지정에 대해 다음 기능을 지원합니다. • DHCPv6 주소 클라이언트 — threat defense는 DHCPv6 서버에서 IPv6 전역 주소 및 선택 사항인 기본 경로를 가져옵니다. • DHCPv6 접두사 위임 클라이언트 — threat defense는 DHCPv6 서버에서 위임된 접두사를 가져옵니다. 그런 다음 threat defense는 이러한 접두사를 사용하여 SLAAC(Stateless Address Auto Configuration) 클라이언트가 동일한 네트워크에서 IPv6 주소를 자동으로 구성할 수 있도록 다른 threat defense 인터페이스 주소를 구성할 수 있습니다. • 위임된 접두사에 대한 BGP 라우터 알림 • DHCPv6 스테이트리스 서버 — threat defense는 SLAAC 클라이언트가 threat defense에 IR(정보 요청) 패킷을 보낼 때 SLAAC 클라이언트에 도메인 이름 등의 기타 정보를 제공합니다. threat defense는 IR 패킷만 수락하고 클라이언트에 주소를 할당하지는 않습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Add/Edit Interfaces(**인터페이스 추가/편집**)** > **IPv6** > **DHCP** • **Objects(**개체**)** > **Object Management(**개체 관리**)** > **DHCP IPv6 Pool(DHCP IPv6** 풀**)** 신규/수정된 명령: **show bgp ipv6 unicast, show ipv6 dhcp, show ipv6 general-prefix**

기능	버전	세부 사항
Azure 게이트웨이 로드 밸런서에 대한 threat defense virtual의 페어링된 프록시 VXLAN	7.3	Azure 게이트웨이 로드 밸런서(GWLB)와 함께 사용하기 위해 Azure에서 threat defense virtual에 대해 페어링된 프록시 모드 VXLAN 인터페이스를 구성할 수 있습니다. threat defense virtual는 페어링된 프록시에서 VXLAN 세그먼트를 활용하여 단일 NIC에서 외부 인터페이스 및 내부 인터페이스를 정의합니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Interface(**인터페이스**)** > **Add Interface(**인터페이스 추가**)** > **VNI Interface(VNI** 인터페이스**)** 지원되는 플랫폼: Azure의 Threat Defense Virtual
VXLAN 지원	7.2	VXLAN 캡슐화 지원이 추가되었습니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **VTEP** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Interface(**인터페이스**)** > **Add Interface(**인터페이스 추가**)** > **VNI Interface(VNI** 인터페이스**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Interfaces(**인터페이스**)**edit physical interface(물리적 인터페이스 편집) > **General(**일반**)** 지원되는 플랫폼: 전체.
Threat Defense Virtual에 대한 Geneve 지원	7.1	AWS(Amazon Web Services) 게이트웨이 로드 밸런서에 대한 단일 암 프록시를 지원하기 위해 threat defense virtual에 대한 Geneve 캡슐화 지원이 추가되었습니다. AWS 게이트웨이 로드 밸런서는 투명 네트워크 게이트웨이(모든 트래픽에 대한 단일 진입점 및 종료 지점 포함)와 트래픽을 분산하고 트래픽 수요에 맞게 threat defense virtual를 확장하는 로드 밸런서를 결합합니다. 이 기능을 사용하려면 Snort 3이 필요합니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **VTEP** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Interface(**인터페이스**)** > **Add Interface(**인터페이스 추가**)** > **VNI Interface(VNI** 인터페이스**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Interfaces(**인터페이스**)**edit physical interface(물리적 인터페이스 편집) > **General(**일반**)** 지원되는 플랫폼: AWS의 Threat Defense Virtual

기능	버전	세부 사항
31비트 서브넷 마스크	7.0	라우팅 인터페이스의 경우, 지점 간 연결을 위해 31비트 서브넷에서 IP 주소를 구성할 수 있습니다. 31비트 서브넷 주소는 주소를 2개만 포함합니다. 일반적으로 서브넷의 첫 번째 주소 및 마지막 주소는 네트워크 및 브로드캐스트용으로 예약되어 있으므로 2개의 주소 서브넷은 사용할 수 없습니다. 그러나 지점 간 연결이 있으며 네트워크 또는 브로드캐스트 주소가 필요하지 않은 경우, 31비트 서브넷은 IPv4에서 주소를 보존하는 유용한 방법입니다. 예를 들어, 2개의 FTD 간의 페일오버 링크에는 주소가 2개만 필요합니다. 링크의 한 쪽 끝에서 전송되는 모든 패킷은 항상 다른 쪽에서 수신되며 브로드캐스팅이 필요하지 않습니다. SNMP 또는 Syslog를 실행하는 직접 연결된 관리 스테이션을 사용할 수도 있습니다. 이 기능은 브리지 그룹 또는 멀티캐스트 라우팅을 위한 BVI에서는 지원되지 않습니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)**
threat defense 작동 링크 상태와 Firepower 4100/9300의 물리적 링크 상태 간 동기화	6.7	이제 Firepower 4100/9300 섀시는 threat defense 작동 링크 상태를 데이터 인터페이스의 물리적 링크 상태와 동기화할 수 있습니다. 현재로서는, FXOS 관리 상태가 작동 중이고 물리적 링크 상태가 작동 중이면 인터페이스는 작동 상태가 됩니다. threat defense 애플리케이션 인터페이스 관리 상태는 고려되지 않습니다. 예를 들어 threat defense에서 동기화하지 않으면 threat defense 애플리케이션이 완전히 온라인 상태가 되기 전에 데이터 인터페이스가 물리적으로 작동 상태가 되거나 threat defense 종료를 시작한 후 일정 기간 동안 작동 상태를 유지할 수 있습니다. 인라인 집합의 경우 threat defense에서 트래픽을 처리하기 전에 외부 라우터가 threat defense로 트래픽 전송을 시작할 수 있으므로 이러한 상태 불일치로 인해 패킷이 삭제될 수 있습니다. 이 기능은 기본적으로 비활성화되어 있으며 FXOS에서 논리적 디바이스별로 활성화할 수 있습니다. 참고 이 기능은 클러스터링, 컨테이너 인스턴스 또는 Radware vDP 데코레이터가 포함된 threat defense에는 지원되지 않습니다. ASA에서도 지원되지 않습니다. 신규/수정된 Firepower Chassis Manager 화면: **Logical Devices(**논리적 디바이스**) > Enable Link State(**링크 상태 활성화**)** 신규/수정된 FXOS 명령: **set link-state-sync enabled**, **show interface expand detail** 지원되는 플랫폼: Firepower 4100/9300

기능	버전	세부 사항
Firepower 1010 하드웨어 스위치 지원	6.5	Firepower 1010에서는 각 이더넷 인터페이스를 스위치 포트 또는 방화벽 인터페이스로 설정하는 것을 지원합니다. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Add VLAN Interface(VLAN** 인터페이스 추가**)**
이더넷 1/7 및 이더넷 1/8에서의 Firepower 1010 PoE+ 지원	6.5	Firepower 1010에서는 스위치 포트로 구성된 이더넷 1/7 및 이더넷 1/8의 PoE+(Power over Ethernet+)를 지원합니다. 신규/수정된 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** > **PoE**
컨테이너 인스턴스에 사용할 VLAN 하위 인터페이스	6.3.0	물리적 인터페이스를 유연하게 사용할 수 있도록 FXOS에서 VLAN 하위 인터페이스를 생성하는 동시에 여러 인스턴스 간에 인터페이스를 공유할 수 있습니다. 신규/수정된 Secure Firewall Management Center 화면: **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Edit(**수정**)** 아이콘 > **Interfaces(**인터페이스**)** 탭 신규/수정된 Secure Firewall 섀시 관리자 화면: **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Add New(**새로 추가**)** 드롭다운 메뉴 > **Subinterface(**하위 인터페이스**)** 신규/수정된 명령: **create subinterface, set vlan, show interface,show subinterface** 지원되는 플랫폼: Firepower 4100/9300
컨테이너 인스턴스용 데이터 공유 인터페이스	6.3.0	물리적 인터페이스를 유연하게 사용할 수 있도록 여러 인스턴스 간에 인터페이스를 공유할 수 있습니다. 신규/수정된 Secure Firewall 섀시 관리자 화면: **Interfaces(**인터페이스**)** > **All Interfaces(**모든 인터페이스**)** > **Type(**유형**)** 신규/수정된 명령: **set port-type data-sharing, show interface** 지원되는 플랫폼: Firepower 4100/9300

기능	버전	세부 사항
통합 라우팅 및 브리징	6.2.0	통합 라우팅 및 브리징은 브리지 그룹과 라우팅 인터페이스 간을 라우팅하는 기능을 제공합니다. 브리지 그룹은 threat defense에서 경로 대신 브리징하는 인터페이스 그룹입니다. threat defense는 실제 브리지가 아닙니다. threat defense는 계속해서 방화벽으로 작동하며, 이를 통해 인터페이스 간의 액세스 제어가 제어되고 모든 일반 방화벽 검사가 올바르게 수행됩니다. 이전에는 브리지 그룹 간에 라우팅할 수 없는 투명 방화벽 모드에서만 브리지 그룹을 구성할 수 있었습니다. 이 기능을 사용하면 라우팅 방화벽 모드에서 브리지 그룹을 구성하고 브리지 그룹 간, 그리고 브리지 그룹과 라우팅 인터페이스 간을 라우팅할 수 있습니다. 브리지 그룹은 BVI(브리지 가상 인터페이스)를 사용하여 라우팅에 참여함으로써 브리지 그룹의 게이트웨이로 작동합니다. 브리지 그룹에 할당할 추가 인터페이스가 threat defense에 있는 경우에는 외부 Layer 2 스위치를 사용하는 대신 통합형 라우팅 및 브리징을 사용할 수 있습니다. 라우팅 모드에서 BVI는 명명된 인터페이스가 될 수 있으며 액세스 규칙 및 DHCP 서버 같은 일부 기능에서 멤버 인터페이스와 별도로 참여할 수 있습니다. 투명 모드에서 지원되는 클러스터링은 라우팅 모드에서는 지원되지 않습니다. 다음 기능은 BVI에서도 지원되지 않습니다. 동적 라우팅 및 멀티캐스트 라우팅. 신규/수정된 화면: • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Edit Physical Interface(**물리적 인터페이스 수정**)** • **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Interfaces(**인터페이스**)** > **Add Interfaces(**인터페이스 추가**)** > **Bridge Group Interface(**브릿지 그룹 인터페이스**)** 지원되는 플랫폼: Firepower 2100 및 threat defense virtual을 제외한 모든 플랫폼