Firepower Threat Defense의 고가용성

다음 주제에서는 Cisco Firepower Threat Defense의 고가용성을 달성하기 위해 액티브/스탠바이 장애 조치를 구성하는 방법을 설명합니다.

Firepower Threat Defense 고가용성 정보

고가용성 또는 장애 조치를 구성하려면 두 개의 동일한 Firepower Threat Defense디바이스가 장애 조치 전용 링크 또는 경우에 따라 상태 링크와 각각 연결되어야 합니다. Firepower Threat Defense는 한 개의 유닛이 액티브 유닛으로 트래픽을 통과하는 Active/Standby(액티브/스탠바이) 장애 조치를 지원합니다. 스탠바이 유닛은 능동적으로 트래픽을 전달하지 않지만, 액티브 유닛에서 컨피그레이션 및 기타 상태 정보를 동기화합니다. 장애 조치가 일어나면 액티브 유닛은 스탠바이 유닛으로 장애 조치를 시작하며, 이때 스탠바이 유닛이 액티브 유닛이 됩니다.

액티브 유닛의 상태(하드웨어, 인터페이스, 소프트웨어 및 환경 상태)를 모니터링하여 특정 페일오버 조건이 충족되는지 확인합니다. 이러한 조건이 충족되면 장애 조치가 이루어집니다.

참고 고가용성은 퍼블릭 클라우드에서 실행되는 Firepower Threat Defense Virtual에서 지원되지 않습니다.

고가용성 시스템 요구 사항

이 섹션에서는 고가용성 구성에서 ASA의 하드웨어, 소프트웨어 및 라이선스 요구 사항에 대해 설명합니다.

하드웨어 요구 사항

고가용성 구성의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 모델이어야 합니다. 또한 컨테이너 인스턴스에 동일한 리소스 프로파일 속성을 사용해야 합니다.

  Firepower 9300의 경우 고가용성은 동일한 유형의 모듈 간에만 지원되지만, 두 섀시는 혼합된 모듈을 포함할 수 있습니다. 각 섀시에 SM-36 및 SM-44가 있는 경우를 예로 들 수 있습니다. SM-36 모듈 간 SM-44 모듈 간에 고가용성 쌍을 생성할 수 있습니다.

  고가용성 쌍을 FMC에 추가한 후 리소스 프로파일을 변경하는 경우 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **System(**시스템**)** > **Inventory(**인벤토리**)** 대화 상자에서 각 유닛의 인벤토리를 업데이트합니다.

- 인터페이스 개수와 유형이 같아야 합니다.

  의 Firepower 4100/9300 섀시의 경우, 고가용성 기능을 활성화하기 전에 FXOS에서 동일하게 모든 인터페이스를 사전에 구성해야 합니다. 고가용성 기능을 활성화한 후에 인터페이스를 변경하는 경우, 스탠바이 유닛의 FXOS에서 인터페이스를 변경하고 나서 활성 유닛에서 동일하게 변경을 수행합니다.

- 같은 모듈을 설치해야 합니다(있을 경우).

- 같은 RAM을 설치해야 합니다.

고가용성 구성에서 플래시 메모리 크기가 다른 유닛을 사용 중인 경우, 플래시 메모리 용량이 작은 유닛에 소프트웨어 이미지 파일 및 구성 파일을 수용할 수 있는 충분한 공간이 있는지 확인해야 합니다. 그렇지 않을 경우 플래시 메모리 용량이 큰 유닛에서 플래시 메모리 용량이 작은 유닛으로 컨피그레이션을 동기화할 수 없습니다.

소프트웨어 요구 사항

고가용성 구성의 유닛 2개에서 충족해야 하는 조건은 다음과 같습니다.

- 같은 상황 모드에 있어야 합니다(단일 또는 다중).

- 같은 방화벽 모드에 있어야 합니다(라우팅 또는 투명).

- 주(첫 번째 번호) 및 부(두 번째 번호) 소프트웨어 버전이 같아야 합니다. 그러나 업그레이드 과정에서 일시적으로 여러 소프트웨어 버전을 사용할 수 있습니다. 예를 들어, 버전 8.3(1)에서 버전 8.3(2)으로 업그레이드하고 장애 조치를 활성 상태로 유지할 수 있습니다. 장기적으로 호환성을 보장하려면 두 유닛을 모두 같은 버전으로 업그레이드하는 것이 좋습니다.

- 같은 AnyConnect 이미지가 있어야 합니다. 무중단 업그레이드를 수행할 때 장애 조치 쌍에 불일치하는 이미지가 있을 경우, 업그레이드 프로세스의 마지막 재부팅 단계에서 클라이언트리스 SSL VPN 연결이 종료되고 데이터베이스에 Orphan 세션이 표시되며 IP 풀에는 클라이언트에 할당된 IP 주소가 "사용 중"인 것으로 표시됩니다.

- (Firepower 4100/9300) 같은 플로우 오프로드 모드가 있으며, 둘 다 활성화하거나 비활성화해야 합니다.

고가용성 쌍의 FTD 디바이스에 대한 라이선스 요구 사항

Firepower Threat Defense 고가용성이 설정된 디바이스에는 동일한 라이선스가 있어야 합니다.

고가용성 컨피그레이션에서는 디바이스 쌍의 각 디바이스에 대해 하나씩, 두 개의 Smart License 자격이 필요합니다.

고가용성을 설정하기 전에는 보조/스탠바이 디바이스에 어떤 라이선스가 할당되든 상관이 없습니다. 고가용성 설정 중에 Firepower Management Center은 스탠바이 디바이스에 할당된 불필요한 라이선스를 해제하고 기본/액티브 디바이스에 할당된 것과 동일한 라이선스로 교체합니다. 예를 들어 액티브 디바이스에 Base 라이선스와 Threat 라이선스가 있고 스탠바이 디바이스에는 Base 라이선스만 있는 경우, Firepower Management Center은 Cisco Smart Software Manager와 통신하여 스탠바이 디바이스의 계정에서 사용 가능한 Threat 라이선스를 가져옵니다. Smart License에 포함되어 있는 구매한 엔타이틀먼트가 충분하지 않으면 정확한 수의 라이선스를 구매할 때까지 어카운트는 컴플라이언스 위반 상태가 됩니다.

가상 고 가용성 구성에서 등록 할 각 FTD에는 추가 Firepower MCv 디바이스 라이선스가 필요합니다.Firepower Management Center

페일오버 및 스테이트풀 페일오버 링크

장애 조치 링크 및 스테이트풀 장애 조치 링크(선택 사항)는 2개 유닛 간의 전용 연결입니다. Cisco에서는 페일오버 링크 또는 스테이트 풀 페일오버 링크의 두 디바이스 간에 같은 인터페이스 사용을 권장합니다. 예를 들어 페일오버 링크에서 device 1에 eth0를 사용한다면, device 2에서도 같은 인터페이스(eth0)를 사용해야 합니다.

⚠

주의 IPsec 터널이나 장애 조치 키로 통신 보안을 설정하지 않는 한 장애 조치 및 상태 링크를 통해 전송되는 모든 정보는 일반 텍스트로 전송됩니다. ASA를 사용하여 VPN 터널을 종료할 경우, 이 정보에는 터널 설정에 사용된 모든 사용자 이름, 비밀번호, PSK(사전 공유 키)가 포함됩니다. 이러한 민감한 데이터를 일반 텍스트로 전송할 경우 중대한 보안 위험을 초래할 수 있습니다. ASA를 사용하여 VPN 터널을 종료할 경우 IPsec 터널이나 장애 조치 키로 장애 조치 통신의 보안을 설정하는 것이 좋습니다.

페일오버 링크

장애 조치 쌍의 유닛 2개에서는 장애 조치 링크를 통해 지속적으로 통신을 수행하여 각 유닛의 작동 상태를 확인합니다.

장애 조치 링크 데이터

다음 정보는 페일오버 링크를 통해 전달됩니다.

- 유닛 상태(액티브 또는 스탠바이)
- Hello 메시지(keep-alives)
- 네트워크 링크 상태

- MAC 주소 교환
- 컨피그레이션 복제 및 동기화

장애 조치 링크에 대한 인터페이스

사용되지 않는 데이터 인터페이스(물리적, 이중화 또는 EtherChannel)는 모두 장애 조치 링크로 사용할 수 있습니다. 그러나 현재 이름이 구성된 인터페이스는 지정할 수 없습니다. Firepower 4100/9300 섀시에 정의되어 있는 하위 인터페이스를 제외하고 하위 인터페이스를 사용할 수 없습니다 장애 조치 링크 인터페이스는 일반적인 네트워킹 인터페이스로 구성되지 않으며, 장애 조치 통신용으로만 존재합니다. 이 인터페이스는 장애 조치 링크용으로만 사용할 수 있습니다(또한 상태 링크용으로도 사용 가능).

FTD에서는 사용자 데이터와 장애 조치 링크 간에 인터페이스 공유를 지원하지 않습니다.또한 데이터와 장애 조치 링크에 대해 동일한 상위에서 별도의 하위 인터페이스를 사용할 수 없습니다(Firepower 4100/9300 섀시 하위 인터페이스만 해당). 장애 조치 링크용으로 Firepower 4100/9300 하위 인터페이스를 사용하는 경우에는 해당 상위 인터페이스의 모든 하위 인터페이스와 상위 인터페이스 자체가 장애 조치 링크로 사용되도록 제한됩니다.

참고 EtherChannel 또는 이중 인터페이스를 장애 조치 또는 상태 링크로 사용하는 경우, 고가용성을 설정하기 전에 동일한 멤버 인터페이스를 사용하는 동일한 EtherChannel 또는 이중 인터페이스가 두 디바이스에 있는지 확인해야 합니다.

장애 조치 링크에 대한 다음 지침을 참조하십시오.

- Firepower 4100/9300 - 페일오버 및 상태 링크를 통합하려면 10GB 데이터 인터페이스를 사용하는 것이 좋습니다.
- 기타 모델 — 1GB 인터페이스는 통합된 장애 조치 및 상태 링크에 충분한 크기입니다.

장애 조치 링크로 사용된 이중 인터페이스의 경우, 추가된 이중성에 대한 다음 이점을 참조하십시오.

- 장애 조치 유닛이 부팅될 때, 활성 유닛을 검색하기 위해 멤버 인터페이스 간에 교체를 수행합니다.
- 장애 조치 유닛이 멤버 인터페이스 중 하나에서 피어로부터 keepalive 메시지 수신을 중지하는 경우, 다른 멤버 인터페이스로 전환합니다.

장애 조치 링크로 사용된 EtherChannel의 경우, EtherChannel의 인터페이스만 사용됩니다. 해당 인터페이스에 오류가 발생할 경우 EtherChannel의 다음 인터페이스가 사용됩니다. 장애 조치 링크로 사용 중인 경우 EtherChannel 컨피그레이션을 변경할 수 없습니다.

장애 조치 링크 연결

다음 2가지 방법 중 하나를 사용하여 장애 조치 링크를 연결합니다.

- 같은 네트워크 세그먼트(브로드캐스트 도메인 또는 VLAN)에 다른 디바이스가 없는 상태에서 스위치를 의 장애 조치 인터페이스로 사용합니다.

- 외부 스위치를 사용할 필요 없이 이더넷 케이블을 사용하여 유닛을 직접 연결합니다.

유닛 간에 스위치를 사용하지 않으려는 경우 인터페이스에 오류가 발생하면 두 피어에서 링크가 중단됩니다. 이 경우 인터페이스에 오류가 발생하고 링크가 중단된 결과를 초래한 유닛이 어떤 것인지 쉽게 확인할 수 없으므로 문제 해결에 방해될 수 있습니다.

ASA에서는 구리 이더넷 포트의 Auto-MDI/MDIX를 지원하므로 crossover 케이블 또는 straight-through 케이블을 사용할 수 있습니다. 다이렉트 케이블을 사용할 경우 인터페이스에서는 케이블을 자동으로 감지하고 송/수신 쌍 중 하나를 MDIX로 교체합니다.

스테이트풀 페일오버 링크

스테이트풀 장애 조치를 사용하려면 연결 상태 정보를 전달할 스테이트풀 장애 조치 링크(상태 링크라고도 함)를 구성해야 합니다.

장애 조치 링크 공유

장애 조치 링크를 공유하는 방법은 인터페이스를 보호하는 가장 좋은 방법입니다. 그러나 컨피그레이션 규모가 크고 네트워크의 트래픽이 많은 경우에는 상태 링크와 페일오버 링크에 대해 전용 인터페이스를 사용하는 것을 고려해야 합니다.

전용 인터페이스

상태 링크에 전용 데이터 인터페이스(물리적, 이중 또는 EtherChannel)를 사용할 수 있습니다. 전용 상태 링크의 요구 사항은 장애 조치 링크에 대한 인터페이스, 4 페이지의 내용, 그리고 상태 링크 연결에 대한 정보는 장애 조치 링크 연결, 4 페이지의 내용을 참조하십시오.

장거리 페일오버를 사용할 경우 최적의 성능을 보장하려면 페일오버 링크의 레이턴시는 10밀리초 미만이어야 하고 250밀리초를 초과해서는 안 됩니다. 레이턴시가 10밀리초를 초과하는 경우 페일오버 메시지의 재전송으로 인해 성능이 다소 저하됩니다.

페일오버 및 데이터 링크 중단 방지

페일오버 링크 및 데이터 인터페이스가 다른 경로를 통해 이동하도록 설정하여 모든 인터페이스에 동시 다발적으로 오류가 발생하는 가능성을 줄이는 것이 좋습니다. 페일오버 링크가 중단될 경우 Firepower Threat Defense 디바이스는 데이터 인터페이스를 사용하여 페일오버가 필요한지 여부를 확인할 수 있습니다. 그런 다음 페일오버 링크 상태가 복원될 때까지는 페일오버 작업이 보류됩니다.

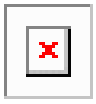
복원력이 뛰어난 페일오버 네트워크를 설계하려면 다음 연결 시나리오를 참조하십시오.

시나리오 **1** — 권장하지 않음

단일 스위치 또는 스위치 집합을 사용하여 두 Firepower Threat Defense 디바이스 간의 페일오버 및 데이터 인터페이스를 모두 연결한 상태에서 스위치 또는 스위치 간 링크가 중단될 경우 두 Firepower Threat Defense 디바이스 모두 액티브 상태가 됩니다. 따라서 아래의 그림에 있는 다음 2가지 연결 방법은 권장하지 않습니다.

그림 *1:* 단일 스위치로 연결 - 권장하지 않음

그림 *2:* 이중 스위치로 연결 - 권장하지 않음



시나리오 **2** - 권장함

페일오버 링크에서는 데이터 인터페이스와 같은 스위치를 사용하지 않는 것이 좋습니다. 대신 다음 그림에 나와 있는 것처럼 다른 스위치를 사용하거나 다이렉트 케이블을 사용하여 페일오버 링크에 연결합니다.

그림 *3:* 다른 스위치로 연결

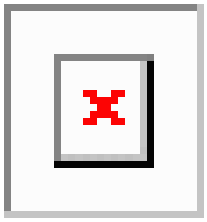
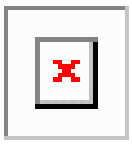


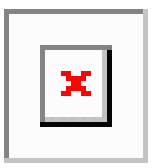
그림 *4:* 케이블로 연결



시나리오 **3** — 권장

Firepower Threat Defense 데이터 인터페이스가 여러 개의 스위치 집합에 연결되어 있는 경우, 페일오버 링크는 이러한 스위치 중 하나에 연결될 수 있으며 다음 그림에 나온 것처럼 주로 네트워크의 보안(내부) 측에 있는 스위치일 가능성이 높습니다.

그림 *5:* 보안 스위치로 연결



시나리오 **4** — 권장

가장 안정적인 페일오버 컨피그레이션에서는 다음 그림에 나와 있는 것처럼 페일오버 링크에서 이중 인터페이스를 사용합니다.

그림 *6:* 이중 인터페이스로 연결

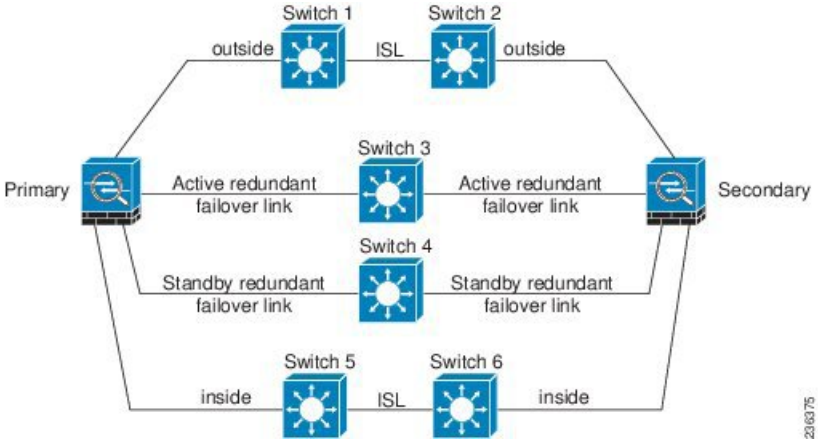
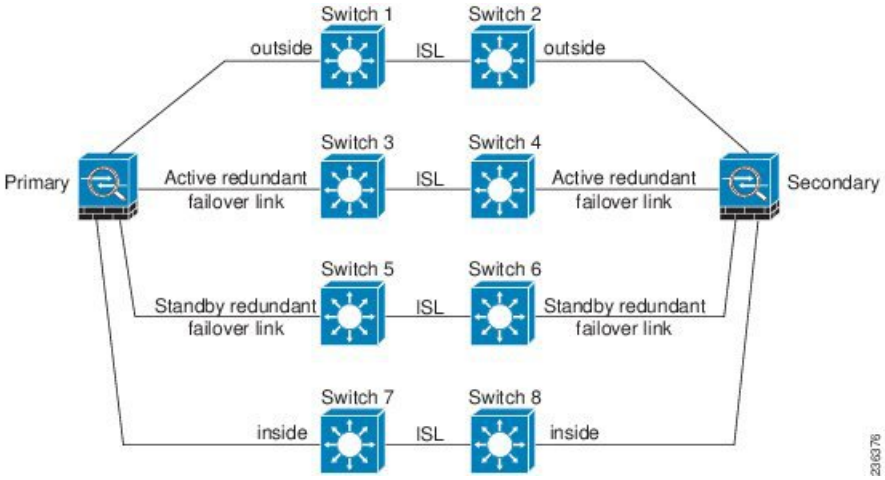


그림 *7:* 스위치 간 링크로 연결



MAC 주소와 IP 주소 - 고가용성

인터페이스를 구성할 때는 동일한 네트워크에서 액티브 IP 주소 및 스탠바이 IP 주소를 지정할 수 있습니다. 일반적으로 페일오버가 발생할 때는 활성 IP 주소와 MAC 주소가 새 액티브 유닛에 승계됩니다. 네트워크 디바이스에서는 MAC-IP 주소 쌍의 변화가 감지되지 않으므로, 네트워크 어디에서도 ARP 항목의 변경이나 시간 초과가 발생하지 않습니다.

참고 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다. 관리 목적으로 해당 인터페이스에서 스탠바이 유닛에 연결할 수도 없습니다.

상태 링크의 IP 주소와 MAC 주소는 장애 조치 시 변경되지 않습니다.

액티브/스탠바이 **IP** 주소와 **MAC** 주소

액티브/스탠바이 고가용성의 경우 페일오버 이벤트가 발생하는 동안의 IP 주소 및 MAC 주소 사용법은 다음 설명을 참조하십시오.

1. 액티브 유닛은 항상 기본 유닛의 IP 주소와 MAC 주소를 사용합니다.
2. 액티브 유닛에서 장애 조치가 수행될 때 스탠바이 유닛에서는 장애 발생 유닛의 IP 주소와 MAC 주소를 사용해 트래픽 전달을 시작합니다.
3. 장애 발생 유닛은 다시 온라인으로 설정되면 스탠바이 상태가 되며 스탠바이 IP 주소와 MAC 주소를 승계합니다.

하지만 기본 유닛을 감지하지 않고 부팅되는 보조 유닛은 액티브 유닛이 되며 기본 유닛의 MAC 주소를 알지 못하므로 고유한 MAC 주소를 사용합니다. 기본 유닛이 사용 가능해지면 보조(액티브) 유닛이 MAC 주소를 기본 유닛의 주소로 변경하므로 네트워크 트래픽이 중단될 수 있습니다. 마찬가지로, 기본 유닛을 새 하드웨어로 교체하면 새 MAC 주소가 사용됩니다.

시작 시 보조 유닛에 액티브 MAC 주소가 알려지므로 가상 MAC 주소에서는 이러한 중단을 방지하며, 새 기본 유닛 하드웨어가 사용될 경우에도 가상 MAC 주소는 그대로 유지됩니다. 가상 MAC 주소를 구성하지 않을 경우, 연결된 라우터에서 ARP 테이블을 지워 트래픽 흐름을 복원해야 할 수 있습니다. MAC 주소가 변경될 경우 Firepower Threat Defense 디바이스에서는 고정 NAT 주소에 불필요한 ARP를 전송하지 않으므로, 연결된 라우터에서는 이러한 주소의 MAC 주소 변경을 알지 못합니다.

가상 **MAC** 주소

Firepower Threat Defense 디바이스에서는 여러 가지 방법으로 가상 MAC 주소를 구성할 수 있습니다. 한 가지 방법만 사용하는 것이 좋습니다. 여러 방법을 사용하여 MAC 주소를 설정할 경우, 사용되는 MAC 주소는 다양한 변수에 따라 달라지며 예측하기 어려워질 수 있습니다.

다중 인스턴스 기능의 경우 FXOS 섀시에서는 모든 인터페이스에 대해 기본 MAC 주소만 자동 생성합니다. 생성된 MAC 주소를 기본 및 보조 MAC 주소가 모두 포함된 가상 MAC 주소로 덮어쓸 수 있습니다. 보조 MAC 주소를 반드시 사전 정의해야 하는 것은 아니지만, 보조 MAC 주소를 설정하면 새 보조 유닛 하드웨어 사용 시 to-the-box 관리 트래픽이 중단되지 않도록 보장할 수 있습니다.

스테이트풀 페일오버

스테이트풀 장애 조치를 스테이트풀 장애 조치 동안액티브 유닛에서는 연결당 상태 정보를 스탠바이 유닛으로 전달하거나 액티브/액티브 장애 조치에서 액티브 및 스탠바이 장애 조치 그룹 간에 지속적으로 전달합니다. 장애 조치가 일어난 후에는 새 액티브 유닛에서 동일한 연결 정보를 사용할 수 있습니다. 지원되는 최종 사용자 애플리케이션이 없어도 다시 연결하여 동일한 통신 세션을 그대로 유지할 수 있습니다.

지원 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 Firepower Threat Defense 디바이스로 전달됩니다.

- NAT 변환 테이블.

- TCP 및 UDP 연결과 상태(HTTP 연결 상태 포함). 다른 유형의 IP 프로토콜과 ICMP는 새 패킷이 도착하면 새 액티브 유닛에서 설정되므로 액티브 유닛에서 구문 분석되지 않습니다.
- SCTP 연결 상태. 그러나 SCTP 검사 스테이트풀 페일오버가 최상의 결과입니다. 페일오버 중에 SACK 패킷이 손실되면 새 액티브 유닛은 누락된 패킷이 수신될 때까지 대기열에서 문제가 있는 기타 모든 패킷을 삭제합니다.
- Snort 연결 상태, 검사 결과 및 핀홀 정보(엄격한 TCP 적용 포함).
- ARP 테이블
- 레이어 2 브리지 테이블(브리지 그룹용)
- ISAKMP 및 IPsec SA 테이블
- GTP PDP 연결 데이터베이스
- SIP 시그널링 세션 및 핀홀.
- 정적 및 동적 라우팅 테이블 - 스테이트풀 페일오버는 OSPF 및 EIGRP 같은 동적 라우팅 프로토콜에 참여하므로, 액티브 유닛에서 동적 라우팅 프로토콜을 통해 확인한 경로는 스탠바이 유닛의 RIB(Routing Information Base) 테이블에 유지됩니다. 페일오버 이벤트 발생 시 액티브 보조 유닛에서는 초기 규칙에 따라 기본 유닛을 미러링하므로 트래픽 중단을 최소화면서도 패킷이 정상적으로 이동됩니다. 페일오버가 끝난 직후에는 새 액티브 유닛에서 재통합 타이머가 시작됩니다. 그러면 RIB 테이블의 시간대 숫자가 늘어납니다. 재통합을 수행하는 동안 OSPF 및 EIGRP 경로는 새 시간대 숫자로 업데이트됩니다. 타이머가 만료되면 오래된 경로 항목(시간대 숫자에 의해 결정됨)이 테이블에서 제거됩니다. 그런 다음 RIB에 새 액티브 유닛에 대한 최신 라우팅 프로토콜 전달 정보가 포함됩니다.

  참고 경로는 액티브 유닛의 링크 작동 또는 링크 중단 이벤트가 있을 경우에만 동기화됩니다. 스탠바이 유닛에서 링크가 작동하거나 중단될 경우, 액티브 유닛에서 전송된 동적 경로가 손실될 수 있습니다. 이는 일반적이고 정상적인 동작입니다.

- DHCP 서버 - DHCP 주소 임대는 복제되지 않습니다. 그러나 인터페이스에 구성된 DHCP 서버는 ping을 전송하여 특정 주소가 사용 중이지 않음을 확인한 후에 DHCP 클라이언트에 해당 주소를 부여하므로 서비스에는 영향이 없습니다. 상태 정보는 DHCP 릴레이 또는 DDNS와 관련이 없습니다.
- 액세스 제어 정책 결정 - 트래픽 일치(URL, URL 카테고리, 지리위치 등), 침입 탐지, 악성코드 및 파일 유형과 관련된 결정은 페일오버 중에 그대로 유지됩니다. 그러나 페일오버 시점에서 평가 중인 연결의 경우 다음 경고가 적용됩니다.
  - AVC - 앱-ID 판정은 복제되지만 탐지 상태는 복제되지 않습니다. 페일오버가 수행되기 전에 앱-ID 판정이 완료 및 동기화되면 적절한 동기화가 수행됩니다.
  - 침입 탐지 상태 - 페일오버 시 중간 플로우 픽업이 발생하면 새 검사는 완료되지만 이전 상태는 손실됩니다.

  - 파일 악성코드 차단 - 페일오버 전에 파일 상태를 확인할 수 있어야 합니다.
  - 파일 유형 탐지 및 차단 - 페일오버 전에 파일 유형이 식별되어야 합니다. 원래 액티브 디바이스가 파일을 식별하는 중에 페일오버가 수행되면 파일 유형이 동기화되지 않습니다. 따라서 파일 정책에서 해당 파일 유형을 차단하더라도 새 액티브 디바이스는 파일을 다운로드합니다.

- 보안 인텔리전스 결정. 그러나 페일오버 시점에서 처리 중인 DNS 기반 결정은 완료되지 않습니다.
- RA VPN - 원격 액세스 VPN 최종 사용자는 페일오버 후 VPN 세션을 다시 인증하거나 다시 연결하지 않아도 됩니다. 그러나 VPN 연결을 통해 작동하는 애플리케이션의 경우 페일오버 프로세스 도중 패킷이 손실될 수 있으며 패킷이 손실되면 복구되지 않습니다.

지원되지 않는 기능

스테이트풀 페일오버에서는 다음 상태 정보가 스탠바이 Firepower Threat Defense 디바이스로 전달되지 않습니다.

- GRE 또는 IP-in-IP와 같은 일반 텍스트 터널 내의 세션. 터널 내의 세션은 복제되지 않으며, 새 액티브 노드는 기존 검사 판정을 재사용하여 정확한 정책 규칙 일치 여부를 확인할 수 없습니다.
- 암호 해독된 TLS/SSL 연결 - 암호 해독 상태가 동기화되지 않고 만약 액티브 유닛에 장애가 발생하면 암호 해독된 연결이 재설정됩니다. 새 활성 유닛에 새 연결을 설정해야 합니다. 암호 해독되지 않은 연결(암호 해독 안 함 규칙과 일치하는 연결)은 영향을 받지 않으며, 올바르게 복제됩니다.
- TCP 상태 우회 연결
- 멀티캐스트 라우팅.

고가용성에 대한 브리지 그룹 요구 사항

브리지 그룹 사용 시 고가용성에 대해 특별히 고려해야 할 사항이 있습니다.

액티브 유닛이 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 스위치 포트가 토폴로지 변경을 인지하는 경우 30초~50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 브리지 그룹 멤버 인터페이스에서 트래픽 손실을 방지하려면 다음 해결 방법 중 하나를 구성할 수 있습니다.

- 스위치 포트는 액세스 모드입니다 - 스위치에서 STP PortFast 기능을 활성화합니다.

```
interface interface_id
  spanning-tree portfast
```

  PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 스위치 포트가 트렁크 모드 상태이거나 STP PortFast를 활성화할 수 없는 경우 페일오버 기능 또는 STP 안정성에 영향을 줄 수 있는 다음 해결 방법을 선택할 수 있습니다.
  - 브리지 그룹 및 멤버 인터페이스에 인터페이스 모니터링을 비활성화합니다.
  - 페일오버 기준에서 인터페이스 대기 시간을 큰 값으로 늘려 유닛 페일오버 전 STP를 통합시킵니다.
  - 스위치가 STP를 인터페이스 대기 시간보다 빠르게 통합하도록 STP 타이머를 감소시킵니다.

장애 조치 상태 모니터링

ASA에서는 각 유닛의 전체 상태 및 인터페이스 상태를 모니터링합니다. 이 섹션에는 ASA에서 각 유닛의 상태를 확인하기 위해 테스트를 수행하는 방법에 대한 정보가 포함되어 있습니다.

유닛 상태 모니터링

ASA에서는 hello 메시지가 있는 장애 조치 링크를 모니터링하여 다른 유닛의 상태를 확인합니다. 장애 조치 링크에서 hello 메시지가 유닛에 3번 연속으로 수신되지 않는 경우, 유닛에서는 장애 조치 링크를 비롯한 각 데이터 인터페이스에 LANTEST 메시지를 전송하여 피어의 응답 여부를 확인합니다. ASA에서 취하는 조치는 다른 유닛의 응답에 따라 달라집니다. 아래의 가능한 조치를 참조하십시오.

- ASA에서 장애 조치 링크에 대한 응답을 수신하지 못할 경우 장애 조치가 이루어지지 않습니다.
- ASA에서 장애 조치 링크에 대한 응답은 수신하지 못했으나 데이터 인터페이스에 대한 응답은 수신한 경우, 유닛에서 장애 조치를 수행하지 않습니다. 페일오버 링크가 실패한 것으로 표시됩니다. 페일오버 링크가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버할 수 없으므로 최대한 빨리 페일오버 링크를 복원해야 합니다.
- ASA에서 인터페이스에 대한 응답을 받지 못한 경우 스탠바이 유닛은 액티브 모드로 전환되고 다른 유닛을 실패한 것으로 분류합니다.

인터페이스 모니터링

최대 1025개의 인터페이스를 모니터링할 수 있습니다(다중 상황 모드에서 해당되며 모든 상황 간에 분할됨). 중요한 인터페이스를 모니터링해야 합니다. 예를 들어 다중 상황 모드에서 하나의 공유 인터페이스를 모니터링하기 위해 단일 상황을 구성할 수 있습니다. 인터페이스가 공유되므로, 모든 상황은 모니터링을 활용합니다.

15초(기본값) 동안 모니터링된 인터페이스에 대한 hello 메시지가 유닛에 수신되지 않을 경우 인터페이스 테스트가 실행됩니다. (기간을 변경하려면 **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **Failover(**페일오버**)** > **Criteria(**기준**)** > **Failover Poll Times(**페일오버 폴링 시간**)**를 참조하십시오.) 인터페이스에 대한 단일 인터페이스 테스트가 실패하였으나 다른 유닛에 있는 이 동일한 인터페이스에서는 지속적으로 트래픽을 전달할 수 있다면, 해당 인터페이스는 오류가 발생한 것으로 간주되며 ASA는 테스트를 중단합니다.

오류가 발생한 인터페이스 수에 정의한 임계값이 충족된다면를 참조하십시오. 액티브 유닛이 대기 유닛보다 오류가 발생한 인터페이스가 많으면 페일오버가 발생합니다. 두 유닛의 인터페이스가 모두 실패하면, 두 인터페이스 모두 'Unknown(알 수 없음)' 상태가 되며 페일오버 인터페이스 정책에서 정의하는 페일오버 한도에 합산되지 않습니다.

트래픽이 수신될 경우 인터페이스는 다시 작동을 시작합니다. 인터페이스 장애 임계값이 더 이상 충족되지 않을 경우 장애가 발생한 ASA는 스탠바이 모드로 돌아갑니다.

ASA FirePOWER 모듈이 있다면, ASA에서는 백플레인 인터페이스에서 모듈의 상태를 모니터링합니다. 모듈의 오류를 유닛 오류로 간주하고 장애 조치를 시작합니다. 이 설정은 구성 가능합니다.

인터페이스에 구성된 IPv4 및 IPv6 주소가 없는 경우 ASA에서는 IPv4 주소를 사용하여 상태 모니터링을 수행합니다. 인터페이스에 IPv6 주소만 구성되어 있으면 ASA에서는 ARP 대신 IPv6 네이버 검색을 사용하여 상태 모니터링 테스트를 수행합니다. 브로드캐스트 ping 테스트의 경우 ASA에서는 IPv6 모든 노드 주소를 사용합니다(FE02::1).

참고 오류가 발생한 유닛에서 복구가 이루어지지 않고 오류가 발생해서는 안 되는 유닛일 경우 **failover reset** 명령을 입력하여 상태를 재설정할 수 있습니다. 그러나 장애 조치 상태가 지속되면 유닛에 다시 오류가 발생합니다.

인터페이스 테스트

ASA에서는 다음과 같은 인터페이스 테스트를 사용합니다. 각 테스트 시간은 기본적으로 1.5초이며, 페일오버 인터페이스 대기 시간의 경우에는 1/16초입니다(**Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **Failover(**페일오버**)** > **Criteria(**기준**)** > **Failover Poll Times(**페일오버 폴링 시간**)**참조).

1. 링크 작동/중단 테스트 - 인터페이스 상태에 대한 테스트입니다. 링크 작동/중단 테스트는 인터페이스가 중단되었는지 여부를 나타내며, ASA에서는 이 상태를 실패로 간주하고 테스트를 중단합니다. 작동 상태일 경우 ASA에서는 네트워크 활동 테스트를 수행합니다.
2. 네트워크 활동 테스트 - 수신된 네트워크 활동 테스트입니다. 테스트를 시작할 때마다 각 유닛에서는 해당 인터페이스에 대한 수신된 패킷 수를 지웁니다. 유닛에서 테스트 도중 적합한 패킷을 수신하는 즉시, 인터페이스는 작동 중으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛에서도 트래픽을 수신하지 못하면, ASA에서는 ARP 테스트를 시작합니다.
3. ARP 테스트 - 성공적인 ARP 응답에 대한 테스트입니다. 각 유닛은 ARP 테이블의 가장 최근 항목에 있는 IP 주소에 대한 단일 ARP 요청을 전송합니다. 유닛이 테스트 중에 ARP 응답이나 기타 네트워크 트래픽을 수신한다면, 인터페이스는 작동하는 것으로 간주됩니다. 유닛이 ARP 회신을 수신하지 못한다면, ASA는 ARP 테이블의 다음 항목에 있는 IP 주소에 대한 단일 ARP 요청을 전송합니다. 유닛이 테스트 중에 ARP 응답이나 기타 네트워크 트래픽을 수신한다면, 인터페이스는 작동하는 것으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛에서도 트래픽을 수신하지 못하면, ASA에서는 Broadcast Ping(브로드캐스트 핑) 테스트를 시작합니다.

4. Broadcast Ping(브로드캐스트 핑) 테스트 - 성공적인 핑 회신에 대한 테스트입니다. 각 유닛은 브로드캐스트 핑을 보낸 다음 수신된 모든 패킷을 계산합니다. 유닛이 테스트 도중 패킷을 수신하면, 인터페이스는 작동 중으로 간주됩니다. 두 유닛 모두가 트래픽을 수신하면 테스트가 중단됩니다. 한 유닛에는 트래픽이 수신되고 다른 유닛에는 수신되지 않는다면, 트래픽이 수신되지 않은 유닛의 인터페이스는 오류가 발생한 것으로 간주되고 테스트가 중단됩니다. 어떤 유닛도 트래픽을 수신하지 않으면, 테스트는 ARP 테스트와 함께 다시 시작됩니다. 두 유닛 모두 ARP 및 Broadcast Ping(브로드캐스트 핑) 테스트에서 트래픽을 계속 수신하지 못하면, 테스트는 영구적으로 계속 실행됩니다.

인터페이스 상태

모니터링한 인터페이스에는 다음과 같은 상태가 표시될 수 있습니다.

- Unknown - 초기 상태입니다. 이 상태는 상태를 확인할 수 없음을 의미할 수도 있습니다.
- Normal - 인터페이스를 트래픽을 받는 중입니다.
- Testing - 다섯 번의 폴링 시간 동안 인터페이스에 Hello 메시지가 수신되지 않았습니다.
- Link Down - 관리자가 인터페이스 또는 VLAN을 중단했습니다.
- No Link - 인터페이스에 대한 물리적 링크가 중단되었습니다.
- Failed - 인터페이스에 수신된 트래픽이 없지만 피어 인터페이스에는 트래픽이 수신되었습니다.

장애 조치 시간

다음 이벤트는 Firepower 고가용성 쌍에서 페일오버를 트리거합니다.

- 활성 유닛의 Snort 인스턴스 중 50 % 이상이 다운되었습니다.
- 활성 유닛의 디스크 공간이 90 % 이상 찼습니다.
- **no failover active(**활성 페일오버 없음**)** 명령이 활성 유닛에서 실행되거나 **failover active(**활성 페일오버**)** 명령이 대기 유닛에서 실행됩니다.
- 대기 유닛보다 활성 유닛에 더 많은 실패 인스턴스가 있습니다.
- 활성 디바이스의 인터페이스 오류가 구성된 임계 값을 초과합니다.

  기본적으로 하나의 인터페이스에 오류가 발생하면 페일오버가 실행됩니다. 인터페이스 수에 대한 임계값 또는 페일오버가 발생하기 위해 실패해야 하는 모니터링되는 인터페이스의 백분율을 구성하여 기본값을 변경할 수 있습니다. 활성 디바이스에서 임계값이 위반되면 페일오버가 발생합니다. 대기 디바이스에서 임계값 위반이 발생하면 유닛은 **Fail(**실패**)** 상태로 전환됩니다.

  기본 페일오버 기준을 변경하려면 전역 구성 모드에서 다음 명령을 입력합니다.

표 *1:*

명령어	목적
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	기본 페일오버 기준을 변경합니다. 인터페이스의 특정 개수를 지정할 경우, *num* 인수의 지원되는 범위는 1에서 250까지입니다. 인터페이스의 백분율을 지정할 경우 *num* 인수의 지원되는 범위는 1에서 100까지입니다.

표 *2: ASA*

장애 조치 조건	최소	기본	최대
활성 유닛의 전원이 끊기거나, 하드웨어가 다운되거나, 소프트웨어가 다시 로드되거나 충돌합니다. 이러한 상황이 발생하면 모니터링되는 인터페이스 또는 페일오버 링크에서 hello 메시지를 수신하지 않습니다.	800밀리초	15초	45초
액티브 유닛 메인 보드 인터페이스 의 연결이 해제됩니다.	500밀리초	5초	15초
액티브 유닛 4GE 모듈 인터페이스 링크가 중단됩니다.	2초	5초	15초
액티브 유닛 FirePOWER 모듈에 장애가 발생합니다.	2초	2초	2초
액티브 유닛 인터페이스가 작동하지만 연결 문제로 인해 인터페이스 테스트가 실행됩니다.	5초	25초	75초

액티브/스탠바이 페일오버 정보

액티브/스탠바이 페일오버에서는 스탠바이 Firepower Threat Defense 디바이스를 사용해 장애가 발생한 유닛의 기능을 인수할 수 있습니다. 액티브 유닛에 장애가 발생하는 경우 스탠바이 유닛이 액티브 유닛이 됩니다.

기본/보조 역할 및 액티브/스탠바이 상태

페일오버 쌍의 두 유닛의 주된 차이점은 어느 유닛이 액티브 유닛이고 어느 유닛이 스탠바이 유닛인지와 관련 있습니다. 즉, 어떤 IP 주소를 사용하고 어떤 유닛이 트래픽을 능동적으로 전달하는지에 달려 있습니다.

그러나 유닛 간의 몇몇 차이점은 어느 유닛이 기본(컨피그레이션에 지정된 사항에 따라) 유닛이고 어느 유닛이 보조 유닛인지에 따라서도 결정됩니다.

- 두 유닛이 동시에 시작되고 둘 다 정상적인 상태로 작동될 경우 기본 유닛은 항상 액티브 유닛이 됩니다.
- 기본 유닛의 MAC 주소는 액티브 IP 주소와 항상 연계됩니다. 보조 유닛이 액티브 유닛이 되고 페일오버 링크를 통해 기본 유닛의 MAC 주소를 획득할 수 없는 경우에는 이러한 규칙에 예외가 발생합니다. 이 경우 보조 유닛의 MAC 주소가 사용됩니다.

시작 시 액티브 유닛 결정

액티브 유닛은 다음에 따라 결정됩니다.

- 유닛이 부팅되고 이미 액티브로 실행 중인 피어가 감지된 경우, 해당 유닛은 스탠바이 유닛이 됩니다.
- 유닛이 부팅되고 피어가 감지되지 않은 경우 해당 유닛은 액티브 유닛이 됩니다.
- 두 유닛이 동시에 부팅될 경우 기본 유닛이 액티브 유닛이 되고 보조 유닛은 스탠바이 유닛이 됩니다.

페일오버 이벤트

액티브/스탠바이 페일오버 시 페일오버는 유닛을 기준으로 실행됩니다.

다음 표에서는 각 페일오버 이벤트에 대한 페일오버 작업을 보여줍니다. 이 표에는 각 페일오버 이벤트에 적용되는 페일오버 정책(페일오버 실행 또는 페일오버 없음), 액티브 유닛에서 시행한 조치, 스탠바이 유닛에서 시행한 조치, 페일오버 조건 및 각 조치에 대한 특별 참고 사항이 나와 있습니다.

표 ***3:*** 페일오버 이벤트

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
액티브 유닛 오류(전력 또는 하드웨어)	페일오버	해당 없음	액티브 상태가 됨 액티브가 실패한 것으로 표시됨	모니터링된 인터페이스 또는 페일오버 링크에 대한 hello 메시지가 수신되지 않음
이전 액티브 유닛 복구	페일오버 없음	스탠바이 상태가 됨	작업 없음	없음

오류 이벤트	정책	액티브 유닛 조치	스탠바이 유닛 조치	참고
스탠바이 유닛 오류(전력 또는 하드웨어)	페일오버 없음	스탠바이가 실패한 것으로 표시됨	해당 없음	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.
작동 중 페일오버 링크에 오류 발생	페일오버 없음	페일오버 링크가 실패한 것으로 표시됨	페일오버 링크가 실패한 것으로 표시됨	페일오버가 중단된 동안에는 유닛에서 스탠바이 유닛으로 페일오버를 시작하지 못하므로 최대한 빨리 페일오버 링크를 복구해야 합니다.
시작 시 페일오버 링크에 오류 발생	페일오버 없음	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	액티브 상태가 됨 페일오버 링크가 실패한 것으로 표시됨	시작 시 페일오버 링크가 중단되면 두 유닛 모두 액티브 상태가 됩니다.
상태 링크 오류 발생	페일오버 없음	작업 없음	작업 없음	페일오버가 실행될 경우 상태 정보가 최신이 아닌 것으로 변경되며 세션이 종료됩니다.
임계값을 넘은 액티브 유닛에서 인터페이스 오류 발생	페일오버	액티브가 실패한 것으로 표시됨	액티브 상태가 됨	없음
임계값을 넘은 스탠바이 유닛에서 인터페이스 오류 발생	페일오버 없음	작업 없음	스탠바이가 실패한 것으로 표시됨	스탠바이 유닛이 실패한 것으로 표시될 경우, 액티브 유닛에서는 페일오버를 시도하지 않으며 인터페이스 오류 임계값을 넘은 경우에도 마찬가지입니다.

고가용성 요구 사항 및 전제 조건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

Network Admin(네트워크 관리자)

고가용성 지침

모델 지원

- Firepower 1010:
  - 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.

  참고 버전 6.5 이상이 Firepower Management Center 버전 6.5 이상에서 새로 설치하고 관리하는 Firepower 1010 디바이스에서 기본 인터페이스는 스위치 포트 유형이 됩니다. 스위치 포트 기능은 페일오버에 지원되지 않으므로 해당 인터페이스에서 스위치 포트를 끄고 구축을 수행한 다음 페일오버를 생성합니다. 6.5 이전 버전에서 업그레이드된 Firepower 1010 시스템의 경우, 기본 인터페이스는 이전 버전과 동일합니다.

- Microsoft Azure 및 Amazon Web Services와 같은 퍼블릭 클라우드 네트워크에 있는 Firepower Threat Defense Virtual에서는 Layer 2 연결이 필요하기 때문에 고가용성를 통해 지원되지 않습니다.

추가 지침

- 액티브 유닛에서 스탠바이 유닛으로 페일오버를 시작할 경우, STP(Spanning Tree Protocol)를 실행 중인 연결된 스위치 포트에서는 토폴로지 변경을 인지하는 경우 30초 ~ 50초 동안 차단 상태가 될 수 있습니다. 포트가 차단 상태일 때 트래픽 손실을 방지하기 위해 스위치에서 STP PortFast 기능을 활성화할 수 있습니다.

interface *interface_id* **spanning-tree portfast**

이 해결 방법은 라우팅 모드 및 브리지 그룹 인터페이스에 모두 연결된 스위치에 적용됩니다. PortFast 기능을 사용하면 링크 작동 시 포트가 STP 전달 모드로 즉시 전환됩니다. 포트는 STP에 계속 참여합니다. 따라서 포트가 루프의 일부인 경우 포트가 STP 차단 모드로 전환됩니다.

- 로컬 CA 서버가 구성된 경우 장애 조치를 활성화할 수 없습니다. **no crypto ca server** 명령을 사용하여 CA 구성을 제거합니다.
- Firepower Threat Defense 장애 조치 쌍에 연결된 스위치에서 포트 보안을 구성할 경우 장애 조치 이벤트가 발생할 때 통신에 문제가 생길 수 있습니다. 이러한 문제는 한 보안 포트에서 구성하거나 확보한 보안 MAC 주소가 다른 보안 포트로 이동될 경우 발생하며, 스위치 포트 보안 기능에 의해 위반 여부가 플래그로 표시됩니다.
- 액티브/스탠바이 고가용성 및 VPN IPsec 터널의 경우, VPN 터널을 통해 SNMP를 사용하여 액티브 유닛과 스탠바이 유닛을 모두 모니터링할 수는 없습니다. 스탠바이 유닛에는 활성 VPN 터널이 없으며 NMS로 전송되는 트래픽은 삭제됩니다. 암호화 기능이 있는 SNMPv3을 대신 사용하면 IPsec 터널을 사용하지 않아도 됩니다.

Firepower Threat Defense 고가용성 쌍 추가

액티브/스탠 바이 고가용성 쌍을 설정하는 경우 하나를 기본 디바이스로 지정하고 다른 하나를 보조 디바이스로 지정합니다. 시스템은 페어링된 디바이스에 병합된 설정을 적용합니다. 충돌이 있는 경우 기본으로 지정한 디바이스의 설정이 적용됩니다.

다중 도메인 구축의 고가용성 쌍의 디바이스는 동일한 도메인에 속해야 합니다.

참고 스테이트풀 페일오버 링크는 피어 간 애플리케이션 콘텐츠 동기화에 사용되며 시스템은 페일오버 링크로 구성을 동기화합니다. 페일오버 링크와 스테이트풀 페일오버 링크는 사설 IP 공간에 있으며 고가용성 쌍의 피어 간 통신에만 사용됩니다. 고가용성이 설정되면 선택된 인터페이스 링크와 암호화 설정은 고가용성 쌍을 해제하고 재구성하기 전까지 수정할 수 없습니다.

주의 Firepower Threat Defense 고가용성 상태를 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작을 참고하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

시작하기 전에

두 디바이스에 대해 다음을 확인합니다.

- 같은 모델이어야 합니다.
- 인터페이스의 개수와 유형이 동일해야 합니다.
- 동일한 도메인 및 그룹에 포함되어야 합니다.
- 정상 상태이고 동일한 소프트웨어를 실행해야 합니다.
- 라우팅 또는 투명 모드가 필요합니다.
- NTP 구성이 같아야 합니다. Threat Defense를 위한 NTP 시간 동기화 구성의 내용을 참조하십시오.
- 커밋되지 않은 변경 사항 없이 완전히 구축되어야 합니다.
- DHCP 또는 PPPoE가 인터페이스에 구성되어 있지 않아야 합니다.

참고 원격 액세스 VPN에 고가용성 기능을 설정할 때 주 디바이스가 CertEnrollment 개체를 사용해 등록한 ID 인증서로 RAVPN 설정을 한 경우 보조 디바이스의 ID 인증서는 동일한 CertEnrollment 개체를 사용해 등록해야 합니다. CertEnrollment 개체는 디바이스별 오버라이드로 인해 주 디바이스 및 보조 디바이스에 다른 값을 가질 수 있습니다. HA를 형성하기 전 두 개의 디바이스에 대해 동일한 CertEnrollment 개체를 보유해야 한다는 제약이 있습니다.

프로시저

단계 **1** FMC에 디바이스 추가에 따라 Firepower Management Center에 두 디바이스를 추가합니다.

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

단계 **3** **Add(**추가**)** 드롭다운 메뉴에서 **High Availability(**고가용성**)**을 선택합니다.

단계 **4** 고가용성 쌍에 대한 표시 이름을 입력합니다.

단계 **5** 장치 유형에서 **Firepower Threat Defense**를 선택합니다.

단계 **6** 고가용성 쌍에 기본 피어 디바이스를 선택합니다.

단계 **7** 고가용성 쌍에 보조 피어 디바이스를 선택합니다.

단계 **8** **Continue(**계속**)**를 클릭합니다.

단계 **9** LAN 페일오버 링크에서 페일오버 통신이 충분히 가능한 대역폭이 있는 인터페이스를 선택합니다.

참고 논리적 이름을 갖지 않고 보안 영역에 속하지 않은 인터페이스만 고가용성 쌍 추가 대화상자의 인터페이스 드롭다운 메뉴에 표시됩니다.

단계 **10** 식별된 논리적 이름을 입력합니다.

단계 **11** 액티브 유닛에서 페일오버 링크에 대한 기본 **IP** 주소를 입력합니다. 이 주소는 사용되지 않는 서브넷에 있어야 합니다.

참고 169.254.0.0/16 및 fd00:0:0:*::/64는 내부적으로 사용되는 서브넷이며 페일오버 또는 상태 링크에 사용할 수 없습니다.

단계 **12** 필요에 따라 **IPv6** 주소 사용을선택합니다.

단계 **13** 스탠바이 유닛에서 페일오버 링크에 대한 보조 **IP** 주소를 입력합니다. 이 IP 주소는 기본 IP 주소와 동일한 서브넷에 있어야 합니다.

단계 **14** IPv4 주소를 사용하는 경우 기본 및 보조 IP 주소에 적용되는 서브넷 마스크 를 입력합니다.

단계 **15** 필요에 따라 스테이트풀 페일오버 링크에서 동일한 인터페이스를 선택하거나 다른 인터페이스를 선택하고 고가용성 설정 정보를 입력합니다.

참고 169.254.0.0/16 및 fd00:0:0:*::/64는 내부적으로 사용되는 서브넷이며 페일오버 또는 상태 링크에 사용할 수 없습니다.

단계 **16** 필요에 따라 활성화를 선택하고 페일오버 링크 간 IPsec 암호화 용 키 생성 방법을 선택합니다.

단계 **17** **OK(**확인**)**를 클릭합니다. 이때 시스템에서 데이터를 동기화하는 데 몇 분 정도 걸립니다.

다음에 수행할 작업

디바이스를 백업하는지 확인합니다. 백업을 이용하면 장애가 발생한 디바이스를 빠르게 교체하고, Firepower Management Center와의 연결을 해제하지 않고도 고가용성 서비스를 복원할 수 있습니다. 자세한 내용은 백업 및 복원를 참고하십시오.

선택적 고가용성 파라미터 구성

Firepower Management Center에서 초기 고가용성 설정을 볼 수 있습니다. 고가용성 쌍을 해제하고 다시 설정하지 않으면 이러한 설정을 편집할 수 없습니다.

페일오버 결과를 개선하기 위해 페일오버 트리거 기준을 편집할 수 있습니다. 인터페이스 모니터링은 페일오버에 가장 적합한 인터페이스를 결정하도록 합니다.

스탠바이 **IP** 주소 및 인터페이스 모니터링 구성

각 인터페이스에 대한 스탠바이 IP 주소를 설정합니다. 스탠바이 주소는 지정하는 것이 좋지만 필수 항목은 아닙니다. 스탠바이 IP 주소가 없으면 액티브 유닛이 네트워크 테스트를 수행하여 스탠바이 인터페이스 상태를 확인할 수 없으며 링크 상태만 추적할 수 있습니다.

기본적으로 모니터링은 모든 물리적 인터페이스에서 활성화되며, Firepower 1010에서는 논리적 이름이 구성된 모든 VLAN 인터페이스에서 활성화됩니다. 중요도가 낮은 네트워크에 연결된 인터페이스를 제외하여 페일오버 정책에 영향을 미치지 않도록 하고자 할 수 있습니다. Firepower 1010 스위치 포트는 인터페이스 모니터링에 적용되지 않습니다.

프로시저

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

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** **High Availability(**고가용성**)** 탭을 클릭합니다.

단계 **4** 모니터링되는 인터페이스 영역에서 편집하려는 인터페이스 옆의 수정( )를 클릭합니다.

단계 **5** 오류에 대해 이 인터페이스 모니터링 확인란을 선택합니다.

단계 **6** **IPv4** 탭에서 스탠바이 **IP** 주소를 입력합니다.

이 주소는 액티브 IP 주소와 같은 네트워크에 있는 여유 주소여야 합니다.

단계 **7** **IPv6** 탭에서 수동으로 IPv6 주소를 구성하는 경우 액티브 IP 주소 옆의 수정( )를 클릭하고 스탠바이 **IP** 주소를 입력한 뒤 **OK**를 클릭합니다.

이 주소는 액티브 IP 주소와 같은 네트워크에 있는 여유 주소여야 합니다. 자동으로 생성되거나 **EUI 64** 강제 적용된 주소의 경우 스탠바이 주소가 자동으로 생성됩니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

고가용성 페일오버 기준 수정

네트워크 구축에 따라 페일오버 기준을 사용자 정의할 수 있습니다.

프로시저

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

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** **Failover Trigger Criteria(**페일오버 트리거 기준**)** 옆의 수정( )을(를) 클릭합니다.

단계 **5** **Interface Failure Threshold(**인터페이스 페일오버 임계값**)**에서 디바이스 페일오버 이전에 오류가 발생해야 하는 인터페이스의 수 또는 비율을 선택합니다.

단계 **6** **Hello** 패킷 간격**(Hello** 패킷 간격**)**에서 페일오버 링크에 보낼 Hello 패킷 수를 선택합니다.

참고 Firepower 2100에서 원격 액세스 VPN을 사용한다면, 기본 Hello 패킷 간격을 사용합니다. 그렇지 않으면 높은 CPU 사용량 때문에 페일오버가 발생할 수 있습니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

가상 MAC 주소 구성

Firepower Management Center의 두 위치에서 페일오버에 대해 액티브 및 스탠바이 MAC 주소를 구성할 수 있습니다.

- 인터페이스 구성 중 인터페이스 편집 내 고급 탭에 대한 설명은 MAC 주소 구성의 내용을 참조하십시오.
- 고가용성 페이지에서 액세스한 인터페이스 MAC 주소 추가는 참조합니다.

액티브 및 스탠바이 MAC 주소가 두 위치에 구성되면 페일오버 시 인터페이스 구성 중 설정한 주소가 우선됩니다.

물리적 인터페이스에 액티브 및 스탠바이 MAC 주소를 지정하여 페일오버 중 트래픽 손실을 최소화할 수 있습니다. 이 기능은 페일오버에 대한 IP 주소 매핑의 이중화를 제공합니다.

프로시저

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

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** 인터페이스 MAC 주소 옆의 추가( )을 선택합니다.

단계 **5** 물리적 인터페이스를 선택합니다.

단계 **6** 액티브 인터페이스 **MAC** 주소를 입력합니다.

단계 **7** 스탠바이 인터페이스 **MAC** 주소를 입력합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

Manage(관리) 고가용성

이 섹션에서는 고가용성를 활성화한 다음, 고가용성 유닛을 관리하는 방법을 설명합니다. 고가용성 설정을 변경하고 한 유닛에서 다른 유닛으로의 장애 조치를 강제로 수행하는 방법도 알아봅니다.

Firepower Threat Defense 고가용성 쌍의 활성 피어 전환

Firepower Threat Defense 고가용성 쌍을 설정하면 액티브 및 스탠바이 유닛을 수동으로 전환할 수 있으며 현재 액티브 유닛의 영구 오류 또는 상태 이벤트 시 페일오버를 효과적으로 강제할 수 있습니다. 이 절차를 완료하기 전 두 유닛이 모두 완전히 구축되어야 합니다.

프로시저

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

단계 **2** 액티브 피어를 변경할 고가용성 쌍 옆에 있는 **Switch Active Peer(**액티브 피어 전환**)**를 클릭합니다.

단계 **3** 다음 작업을 수행할 수 있습니다.

- **Yes(**예**)**를 클릭하여 스탠바이 디바이스를 고가용성 쌍의 액티브 디바이스로 즉시 설정합니다.
- 취소하고 디바이스 관리 페이지로 돌아가려면 아니오를 클릭합니다.

고가용성 일시 중단 또는 재개

고가용성 쌍의 유닛을 일시 중단할 수 있습니다. 이렇게 하면 다음과 같은 경우에 유용합니다.

- 두 유닛이 모두 액티브-액티브인 상태에서 페일오버 링크의 통신을 수정해도 문제가 해결되지 않는 경우.
- 액티브 또는 스탠바이 유닛을 트러블슈팅하고 트러블슈팅 중에는 유닛을 페일오버하지 않으려는 경우.

고가용성을 일시 중단하면 디바이스 쌍이 더 이상 페일오버 유닛으로 동작하지 않게 됩니다. 현재 액티브 디바이스는 액티브 상태로 유지되어 모든 사용자 연결을 처리합니다. 그러나 페일오버 기준은 더 이상 모니터링되지 않으며 시스템은 현재 의사 스탠바이 디바이스로 페일오버되지 않습니다. 스탠바이 디바이스의 컨피그레이션은 보존되지만 해당 디바이스는 비활성 상태로 유지됩니다.

HA 일시 중단과 해제의 주요 차이점은 일시 중단된 HA 디바이스에서는 고가용성 컨피그레이션이 보존된다는 것입니다. 반면 HA를 해제하면 컨피그레이션이 지워집니다. 따라서 일시 중단된 시스템에서 HA를 다시 시작하는 옵션이 제공됩니다. 그러면 기존 컨피그레이션이 활성화되며 두 디바이스가 다시 페일오버 쌍으로 작동합니다.

HA를 일시 중단하려면 **configure high-availability suspend** 명령을 사용합니다.

```
> configure high-availability suspend
Please ensure that no deployment operation is in progress before suspending
high-availability.
Please enter 'YES' to continue if there is no deployment operation in
progress and 'NO' if you wish to abort: YES
Successfully suspended high-availability.
```

액티브 유닛에서 고가용성을 일시 중단하면 액티브 유닛과 스탠바이 유닛 둘 다에서 컨피그레이션이 일시 중단됩니다. 스탠바이 유닛에서 고가용성을 일시 중단하는 경우에는 스탠바이 유닛에서만 고가용성이 일시 중단되며 액티브 유닛은 일시 중단된 유닛으로의 페일오버를 시도하지 않습니다.

페일오버를 재시작하려면 **configure high-availability resume** 명령을 사용합니다.

```
> configure high-availability resume
```

```
Successfully resumed high-availablity.
```

Suspended(일시 중단됨) 상태인 유닛만 다시 시작할 수 있습니다. 이 유닛은 피어 유닛과 액티브/스탠바이 상태를 협상합니다.

참고 고가용성 일시 중단은 임시 상태입니다. 유닛을 다시 불러오면 고가용성 구성을 자동으로 재시작하고 피어와 액티브/스탠바이 상태 협상을 시작합니다.

FTD 고가용성 쌍의 유닛 교체

백업 파일을 사용하여 Firepower Threat Defense 고가용성 쌍에서 장애가 발생한 유닛을 교체하려면 Firepower 어플라이언스 복구의 내용을 참조하십시오.

장애가 발생한 디바이스의 백업이 없는 경우 고가용성을 해제해야 합니다. 그런 다음 Firepower Management Center에 교체 디바이스를 등록하고 고가용성을 다시 설정합니다. 이 프로세스는 디바이스가 기본 디바이스인지 보조 디바이스인지에 따라 달라집니다.

- 기본 FTD HA 유닛을 백업 없이 교체, 24 페이지
- 보조 FTD HA 유닛을 백업 없이 교체, 25 페이지

기본 FTD HA 유닛을 백업 없이 교체

Firepower Threat Defense 고가용성 쌍에서 장애가 발생한 기본 유닛을 교체하려면 다음 단계를 수행합니다. 다음 단계를 수행하지 않으면 기존 고가용성 설정을 오버라이트할 수 있습니다.

주의 Firepower Threat Defense 고가용성 상태를 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작을 참고하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

프로시저

단계 **1** 고가용성 쌍을 분리하기 위해 강제 해제를 선택합니다. 고가용성 쌍의 유닛 분리, 26 페이지를 참조하십시오.

참고 중단 작업은 Firepower Threat Defense 및 Firepower Management Center에서 HA와 관련된 모든 구성을 제거하며, 나중에 수동으로 다시 생성해야 합니다. 동일한 HA 쌍을 설정하려면 HA 중단 작업을 실행하기 전에 모든 인터페이스/하위 인터페이스의 IP, MAC 주소, 모니터링 설정을 저장해야 합니다.

단계 2 Firepower Management Center에서 오류가 발생한 기본 Firepower Threat Defense 유닛의 등록을 해제하려면 FMC에서 디바이스 삭제을 참조하십시오.

단계 3 Firepower Management Center에 Firepower Threat Defense을 교체 등록하려는 경우 FMC에 디바이스 추가을 참조하십시오.

단계 4 등록 시 기존 보조/액티브 유닛을 기본 디바이스로 사용하고 교체 디바이스를 보조/스탠바이 디바이스로 하여 고가용성을 구성하려면 Firepower Threat Defense 고가용성 쌍 추가, 18 페이지을 참조하십시오.

보조 FTD HA 유닛을 백업 없이 교체

Firepower Threat Defense 고가용성 쌍에서 장애가 발생한 보조 유닛을 교체하려면 다음 단계를 수행합니다.

⚠

주의 Firepower Threat Defense 고가용성 상태를 생성하거나 해제하면 기본 및 보조 디바이스에서 Snort 프로세스가 즉시 재시작되므로 일시적으로 두 디바이스의 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 트래픽 동작을 참고하십시오. 고가용성 쌍을 생성할 때 시스템은 기본 및 보조 디바이스에서 Snort 프로세스가 재시작된다는 경고 메시지를 표시하며 사용자가 작업을 취소할 수 있습니다.

프로시저

단계 1 고가용성 쌍을 분리하기 위해 강제 해제를 선택합니다. 고가용성 쌍의 유닛 분리, 26 페이지를 참조하십시오.

참고 중단 작업은 Firepower Threat Defense 및 Firepower Management Center에서 HA와 관련된 모든 구성을 제거하며, 나중에 수동으로 다시 생성해야 합니다. 동일한 HA 쌍을 설정하려면 HA 중단 작업을 실행하기 전에 모든 인터페이스/하위 인터페이스의 IP, MAC 주소, 모니터링 설정을 저장해야 합니다.

단계 2 Firepower Management Center에서 Firepower Threat Defense 보조 디바이스의 등록을 해제합니다. FMC에서 디바이스 삭제을 참조하십시오.

단계 3 Firepower Management Center에 Firepower Threat Defense의 교체 디바이스를 등록합니다. FMC에 디바이스 추가을 참조하십시오.

단계 4 등록 시 기존 기본/액티브 유닛을 기본 디바이스로 사용하고 교체 디바이스를 보조/스탠바이 디바이스로 하여 고가용성을 구성하려면 Firepower Threat Defense 고가용성 쌍 추가, 18 페이지을 참조하십시오.

고가용성 쌍의 유닛 분리

고가용성 쌍을 해제하는 경우 액티브 디바이스는 전체 구축된 기능을 유지합니다. 스탠바이 디바이스는 페일오버 및 인터페이스 구성을 잃고 독립형 디바이스가 됩니다. Firepower Management Center는 고가용성 라이선스를 내보내고 독립형 디바이스의 개별 라이선스로 교체합니다. 고가용성 쌍을 해제하기 전 해제 작업 이전에 액티브 디바이스에 구축된 정책은 해제 작업이 완료되면 자동으로 구축됩니다.

팁 FlexConfig 정책은 예외입니다. 액티브 디바이스에 구축된 FlexConfig 정책은 HA 해제 작업 완료 후 구축 실패를 표시할 수 있습니다. FlexConfig 정책을 변경하고 액티브 디바이스에 다시 구축해야 합니다.

참고 Firepower Management Center을 사용해 고가용성 쌍에 연결할 수 없는 경우 **configure high-availability disable** CLI 명령을 사용하여 두 디바이스에서 페일오버 설정을 제거해야 합니다.

프로시저

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

단계 **2** 해제하려는 고가용성 쌍 옆의 **Break HA(HA** 해제**)**를 클릭합니다.

단계 **3** 스탠바이 피어가 응답하지 않고 필요한 경우 강제 해제 확인란을 선택합니다.

단계 **4** **Yes(**예**)**를 클릭합니다. 디바이스 고가용성 쌍이 분리됩니다.

해제 작업은 액티브 및 스탠바이 디바이스에서 페일오버 설정을 제거합니다.

다음에 수행할 작업

(선택 사항) 액티브 디바이스에서 flex-config 정책을 사용하는 경우 구축 오류를 제거하기 위해 flex-config 정책을 변경하고 다시 구축합니다.

고가용성 쌍 등록 해제

Firepower Management Center에서 쌍을 삭제하고 CLI를 사용해 각 유닛에서 고가용성을 비활성화할 수 있습니다.

시작하기 전에

이 절차에서는 CLI 액세스가 필요합니다.

프로시저

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

단계 **2** 등록을 취소하려는 고가용성 쌍 옆의 삭제( )을 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭합니다. 디바이스 고가용성 쌍이 삭제됩니다.

단계 **4** 각 유닛에서 Firepower Threat Defense CLI에 액세스하고 다음 명령을 입력합니다.

configure high-availability disable

이 명령을 입력하지 않으면 유닛을 다시 등록하고 새로운 HA 쌍을 형성할 수 없습니다.

참고 방화벽 모드를 변경하기 전에 이 명령을 입력하십시오. 모드를 변경하면 유닛은 **configure high-availability disable** 명령의 입력을 거부할 것이며 Firepower Management Center은 이 명령을 사용하지 않으면 HA 쌍으로 재구성되지 않습니다.

모니터링 고가용성

이 섹션에서는 고가용성 상태를 모니터링할 수 있습니다.

페일오버 기록 보기

두 개의 고가용성 디바이스의 페일오버를 단일 보기에서 볼 수 있습니다. 시간 순으로 표시되며 페일오버의 이유를 표시합니다.

프로시저

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

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 요약을 선택합니다.

단계 **4** General(일반)에서 보기 ( )을 클릭합니다.

스테이트풀 페일오버 통계 보기

고가용성 쌍의 기본 및 보조 디바이스에 대한 스테이트풀 고가용성 링크 통계를 볼 수 있습니다.

프로시저

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

단계 **2** 편집하려는 디바이스 고가용성 쌍 옆의 수정( )을 클릭합니다.

다중 도메인 구축에서 현재 위치가 리프 도메인이 아니면 도메인을 전환하라는 메시지가 표시됩니다.

단계 **3** 고가용성을 선택합니다.

단계 **4** Stateful Failover Link(스테이트풀 페일오버 링크)에서 보기 ( )를 클릭합니다.

단계 **5** 통계를 보려는 디바이스를 선택합니다.