Firepower 4100/9300에서 ASA용 클러스터 구축

최종 변경: 2026년 5월 20일

Firepower 4100/9300에서 ASA용 클러스터 구축

클러스터링을 사용하면 여러 개의 ASA 유닛을 하나의 논리적 디바이스로 그룹화할 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다. 클러스터링은 ASA 하드웨어 모델에서도 지원되지만, Firepower 4100/9300에서는 FXOS에서 별도의 구성을 필요로 하기 때문에 이 문서에서는 FXOS 및 ASA의 전체 구성에 중점을 둡니다.

참고 클러스터링을 사용할 경우 일부 기능이 지원되지 않습니다. 클러스터링으로 지원되지 않는 기능, 68 페이지의 내용을 참조하십시오.

참고 이 문서에서는 최신 ASA 버전의 기능에 대해 설명합니다. 기능 변경에 대한 자세한 내용은 ASA 클러스터링에 대한 기록 - Firepower 4100/9300, 84 페이지를 참조하십시오. 이전 버전의 소프트웨어를 사용할 경우에는 해당 버전에 대한 FXOS 컨피규레이션 가이드 및 ASA 컨피규레이션 가이드의 절차를 참조하십시오.

이 통합의 혜택

FXOS 플랫폼을 사용하면 ASA를 비롯한 여러 논리적 디바이스를 실행할 수 있습니다. 섀시 내 클러스터(Firepower 9300 용) 및 섀시 간 클러스터 모두에서 독립형 및 클러스터형 논리적 디바이스를 구축하는 것은 쉽습니다. FXOS에서 클러스터를 구축할 때는 ASA 부트 스트랩 구성을 사전 구성하므로 ASA 애플리케이션 내에서 사용자 맞춤화가 거의 필요하지 않습니다. FXOS에서 클러스터 구성을 내보내 클러스터 멤버를 추가할 수도 있습니다.

통합 제품

이 표에는 이 통합에 필요한 제품이 나와 있습니다.

표 *1:* 클러스터링용 통합 제품

제품	기능	최소 버전	필수 여부
Firepower 4100 또는 9300	ASA를 실행하기 위한 하드웨어 플랫폼	FXOS 1.1.2	필수

제품	기능	최소 버전	필수 여부
Firepower Chassis Manager	FXOS GUI 디바이스 관리자	Firepower Chassis Manager 1.1.2	선택 사항. CLI를 사용할 수도 있음
ASA	방화벽 애플리케이션	ASA 9.4(1.152)	필수
ASDM	ASA GUI 디바이스 관리자	ASDM 7.4(3)	선택 사항. CLI를 사용할 수도 있음

워크플로

이 워크플로우에서는 FXOS에서는 Firepower Chassis Manager, ASA에서는 ASDM을 사용하여 클러스터링 구축을 완료합니다.

프로시저

단계 **1** FXOS 사전 요건:

- 스마트 라이선싱 구성. 스마트 라이선싱을 사용하려면 NTP 서버(또는 최소한 정확한 수동 시간) 및 DNS를 구성해야 합니다.

단계 **2** FXOS 작업:

a) FXOS: 인터페이스 구성, 19 페이지. ASA에 할당할 하나의 관리 및 모든 데이터 인터페이스를 구성합니다. 클러스터 인터페이스는 기본적으로 포트 채널 48로 정의되지만 섀시 간 클러스터링의 경우에는 멤버 인터페이스를 추가해야 합니다.

b) ASA 클러스터 생성, 23 페이지.

c) 클러스터 멤버 더 추가, 29 페이지.

단계 **3** ASA 작업. 마스터 유닛에서만 다음 작업을 수행합니다.

a) (선택 사항) 통신 사업자 및 상황 기능에 대한 라이선스를 구성합니다. ASA의 일반적인 작업 구성 가이드를 참조하십시오.

b) (선택 사항) ASA: 방화벽 모드 및 상황 모드 변경, 31 페이지. 기본적으로 FXOS 섀시에서는 라우팅 방화벽 모드와 단일 상황 모드에서 클러스터를 구축합니다.

c) ASA: 데이터 인터페이스 구성, 31 페이지. 관리 인터페이스는 클러스터를 구축할 때 사전 구성되어 있습니다.

d) (선택 사항) ASA: 클러스터 구성 맞춤화, 34 페이지. 사이트 간 기능 및 분산 사이트 간 VPN을 비롯한 다양한 클러스터링 기능을 사용자 지정하거나 활성화합니다.

Firepower 4100/9300 섀시 클러스터링 정보

Firepower 4100/9300 섀시에서 클러스터를 구축할 때는 다음 작업이 수행됩니다.

- 노드 간 통신에 사용되는 클러스터 제어 링크(기본값: port-channel 48)를 생성합니다.

  단일 Firepower 9300 섀시 내에서 보안 모듈로 격리된 클러스터의 경우 이 링크는 클러스터 통신에 Firepower 9300 백플레인을 활용합니다.

  다중 섀시 클러스터링의 경우, 섀시 간의 통신을 위해 물리적 인터페이스를 이 EtherChannel에 수동으로 할당해야 합니다.

- 애플리케이션 내부에 클러스터 부트스트랩 구성을 생성합니다.

  클러스터를 구축할 때, 섀시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다. 클러스터링 환경을 사용자 정의하려는 경우, 사용자가 일부 부트스트랩 구성을 애플리케이션 내부에 구성할 수 있습니다.

- 데이터 인터페이스를 *Spanned* 인터페이스로 클러스터에 할당합니다.

  단일 Firepower 9300 섀시 내에서 보안 모듈로 격리된 클러스터의 경우, 다중 섀시 클러스터링과 마찬가지로 Spanned 인터페이스는 EtherChannel로 제한되지 않습니다. Firepower 9300 수퍼바이저는 EtherChannel 기술을 내부에 사용하여 트래픽을 공유 인터페이스의 다중 모듈에 로드 밸런싱하므로 모든 데이터 인터페이스 유형이 Spanned(스팬) 모드에서 작동합니다. 다중 섀시 클러스터링의 경우, 모든 데이터 인터페이스에 Spanned EtherChannel을 사용해야 합니다.

참고 개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

- 관리 인터페이스를 클러스터의 모든 유닛에 할당합니다.

클러스터링에 대한 자세한 내용은 다음 섹션을 참고하십시오.

부트스트랩 구성

클러스터를 구축할 때, Firepower 4100/9300 섀시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 구성을 푸시합니다. 클러스터링 환경을 사용자 정의하려는 경우, 일부 부트스트랩 설정은 사용자가 구성할 수 있습니다.

클러스터 멤버

클러스터 멤버는 보안 정책 및 트래픽 흐름을 공유하기 위해 서로 연동됩니다.

클러스터의 멤버 중 하나는 제어 유닛입니다. 제어 유닛은 자동으로 결정됩니다. 다른 모든 멤버는 데이터 유닛입니다.

모든 설정은 제어 유닛에서만 수행되어야 하며, 이후 설정이 데이터 유닛에 복제됩니다.

일부 기능은 클러스터로 확장되지 않으며, 제어 유닛에서 이러한 기능에 대한 모든 트래픽을 처리합니다. 클러스터링을 위한 중앙 집중식 기능, 69 페이지를 참고하십시오.

클러스터 제어 링크

유닛 간 통신에 사용되는 클러스터 제어 링크는 EtherChannel(port-channel 48)입니다. 섀시 내 클러스터링을 위해 이 링크에서는 클러스터 통신에 Firepower 9300 백플레인을 활용합니다. 섀시 간 클러스터링의 경우 섀시 간의 통신을 위해 물리적 인터페이스를 Firepower 4100/9300 섀시의 이 EtherChannel에 수동으로 할당해야 합니다.

2-섀시의 섀시 간 클러스터의 경우 클러스터 제어 링크를 한 섀시에서 다른 섀시로 직접 연결하지 마십시오. 인터페이스에 직접 연결할 경우, 유닛 하나에 오류가 발생하면 클러스터 제어 링크에도 오류가 발생하므로 나머지 정상 유닛에도 오류가 발생합니다. 스위치를 통해 클러스터 제어 링크를 연결할 경우 클러스터 제어 링크는 가동 상태를 유지하여 정상 유닛을 지원합니다.

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

제어 트래픽에는 다음 사항이 해당됩니다.

- 제어 노드 선택.
- 구성 복제
- 상태 모니터링

데이터 트래픽에는 다음 사항이 해당됩니다.

- 상태 복제
- 연결 소유권 쿼리 및 데이터 패킷 전송

클러스터 제어 링크에 대한 자세한 내용은 다음 섹션을 참조하십시오.

클러스터 제어 링크 크기 조정

가능한 경우, 각 섀시의 예상 처리량에 맞게 클러스터 제어 링크의 크기를 조정하여 클러스터 제어 링크가 최악의 시나리오를 처리할 수 있게 해야 합니다.

클러스터 제어 링크 트래픽은 주로 상태 업데이트 및 전달된 패킷으로 구성되어 있습니다. 클러스터 제어 링크의 트래픽 양은 언제든지 달라질 수 있습니다. 전달된 트래픽의 양은 로드 밸런싱 효율성 또는 중앙 집중식 기능에 많은 트래픽이 있는지에 따라 좌우됩니다. 예를 들면 다음과 같습니다.

- NAT의 경우 연결의 로드 밸런싱이 저하되며, 모든 반환 트래픽을 올바른 유닛으로 다시 밸런싱해야 합니다.
- 네트워크 액세스용 AAA는 중앙 집중식 기능이므로 모든 트래픽이 제어 유닛으로 전달됩니다.
- 멤버가 변경된 경우, 클러스터에서는 다량의 연결을 다시 밸런싱해야 하므로 일시적으로 많은 양의 클러스터 제어 링크 대역폭을 사용합니다.

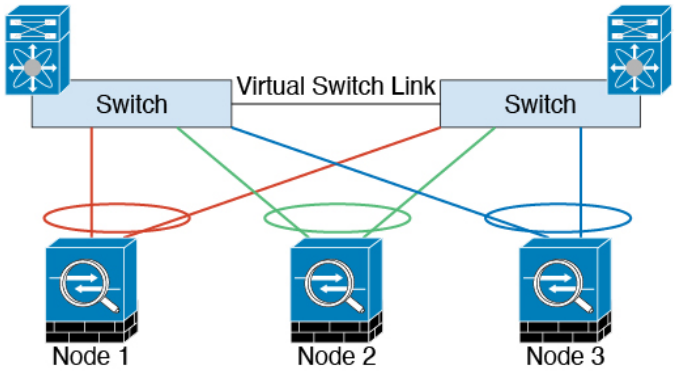
대역폭이 높은 클러스터 제어 링크를 사용하면 멤버가 변경될 경우 클러스터를 더 빠르게 통합할 수 있고 처리량 병목 현상을 방지할 수 있습니다.

참고 클러스터에 비대칭(다시 밸런싱된) 트래픽이 많은 경우 클러스터 제어 링크 크기를 늘려야 합니다.

클러스터 제어 링크 이중화

클러스터 제어 링크에는 EtherChannel을 사용하는 편이 바람직하며, 이렇게 할 경우 EtherChannel 내의 여러 링크에 트래픽을 전달하는 동시에 이중화를 실현할 수 있습니다.

다음 다이어그램은 EtherChannel을 VSS(Virtual Switching System), vPC(Virtual Port Channel), StackWise 또는 StackWise 가상 환경에서 클러스터 제어 링크로 사용하는 방법을 보여줍니다. EtherChannel의 모든 링크가 활성화되어 있습니다. 스위치가 중복 시스템의 일부인 경우 동일한 EtherChannel 내의 방화벽 인터페이스를 중복 시스템의 개별 스위치에 연결할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 디바이스 로컬이 아닌 스팬 EtherChannel입니다.



을 위한 클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(round-trip time)가 20ms 이하여야 합니다. 이러한 최대 레이턴시는 서로 다른 지리적 사이트에 설치된 클러스터 멤버와의 호환성을 개선하는 역할을 합니다. 레이턴시를 확인하려면 유닛 간의 클러스터 제어 링크에서 Ping을 수행합니다.

클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 사이트 간 구축의 경우 전용 링크를 사용해야 합니다.

클러스터 제어 링크 네트워크

Firepower 4100/9300 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id.slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다.클러스터를 구축할 때 이 IP 주소를 맞춤 설정할 수 있습니다. 클러스터 제어 링크 네트워크는 유닛 간에 라우터를 포함할 수 없으며 레이어 2 스위칭만 허용됩니다. 사이트 간 트래픽의 경우에는 OTV(Overlay Transport Virtualization)를 사용하는 것이 좋습니다.

클러스터 제어 링크 MTU ping 테스트

제어 노드 ping 테스트

노드가 클러스터에 조인하면 제어 노드는 MTU의 두 배인 페이로드 크기로 ping을 전송합니다. 기본 IP 계층은 MTU 제한을 초과하는 패킷을 프래그먼트하기 때문에 이 프로세스는 패킷 프래그먼트를 처리하는 네트워크의 기능을 테스트합니다.

ping에 성공하면 네트워크 경로가 적절한 프래그먼트를 지원하며 클러스터 제어 링크가 설정된 MTU 크기에서 트래픽을 안정적으로 처리할 수 있음을 확인합니다.

ping이 실패하면 다음 메시지를 확인합니다.

- **show cluster history**—이벤트: 유닛 이름에 대한 CCL MTU 테스트 실패
- 콘솔 경고- 경고: CCL 점보 프레임 ICMP 테스트에서 유닛 이름에 연결할 수 없습니다. 클러스터 인터페이스 및 스위치의 MTU 설정을 확인해 주십시오.

ping이 실패하더라도 노드는 클러스터에 조인할 수 있습니다. 이 경우 최대한 빨리 MTU 불일치를 해결해야 합니다.

데이터 노드 ping 테스트

노드가 클러스터에 조인하면 조인하는 노드가 클러스터 제어 링크 MTU와 일치하는 패킷 크기로 제어 노드에 ping을 전송하여 MTU 호환성을 확인합니다. 초기 ping이 실패하면 노드 ping이 성공할 때까지 더 작은 패킷 크기(MTU를 2로 나눈 다음 4로 나눈 다음 8로 나눈 값)를 사용하여 ping을 시도합니다.

ping이 실패하면 다음 메시지를 확인합니다.

- **show cluster info trace**—경고: CCL MTU가 *cfg_mtu_size*로 구성되었습니다. 그러나 유닛 이름에 대한 CCL MTU 테스트는 *larger_test_size* 크기로 실패했습니다(*small_test_size* 크기로 전달됨). 스위치 MTU 구성을 확인하십시오.

  이 경고를 쉽게 확인하려면 **show cluster info trace | incl MTU**를 사용하여 **show** 출력을 필터링합니다.

- **show cluster history**—경고: CCL 인터페이스에서 MTU 불일치가 감지되었습니다. 연결된 스위치의 MTU 설정이 방화벽에 구성된 MTU(*cfg_mtu_size*)와 일치하는지 확인하십시오.
- 콘솔 경고- 경고: CCL 점보 프레임 ICMP 테스트에서 유닛 이름에 연결할 수 없습니다. 클러스터 인터페이스 및 스위치의 MTU 설정을 확인해 주십시오.

ping이 실패하더라도 노드는 클러스터에 조인할 수 있습니다. 이 경우 최대한 빨리 MTU 불일치를 해결해야 합니다.

클러스터 인터페이스

단일 Firepower 섀시 내의 보안 모듈에 격리된 클러스터의 경우, 클러스터에 물리적 인터페이스 또는 Etherchannel(포트 채널)을 할당할 수 있습니다. 클러스터에 할당된 인터페이스는 클러스터의 모든 멤버에 대해 트래픽의 로드 밸런싱을 수행하는 Spanned 인터페이스입니다.

다중 섀시 클러스터링의 경우 클러스터에 데이터 Etherchannel만 할당할 수 있습니다. Spanned EtherChannel은 각 섀시에 동일한 멤버 인터페이스를 포함합니다. 업스트림 스위치에서 모든 인터페이스는 단일 EtherChannel에 포함되므로 스위치는 인터페이스가 여러 디바이스와 연결되었는지 알지 못합니다.

개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

이중화 스위치 시스템에 연결

VSS, vPC, StackWise 또는 StackWise Virtual 시스템과 같은 이중화 스위치 시스템에 EtherChannel을 연결하여 인터페이스에 이중화를 제공하는 것이 좋습니다.

구성 복제

클러스터의 모든 노드에서는 단일 구성을 공유합니다. 제어 노드에서는 구성만 변경할 수 있으며(부트스트랩 구성 예외), 변경 사항은 클러스터의 모든 다른 노드에 자동으로 동기화됩니다.

Secure Firewall ASA클러스터 관리

ASA 클러스터링을 사용하는 데 따른 여러 장점 중 하나는 관리하기가 쉽다는 점입니다. 이 섹션에서는 클러스터를 관리하는 방법에 대해 설명합니다.

관리 네트워크

모든 유닛을 단일한 관리 네트워크에 연결할 것을 권장합니다. 이 네트워크는 클러스터 제어 링크와 분리되어 있습니다.

관리 인터페이스

클러스터에 관리 유형 인터페이스를 할당해야 합니다. 이 인터페이스는 Spanned 인터페이스와는 다른 특수 개별 인터페이스입니다. 관리 인터페이스를 사용하면 각 유닛에 직접 연결할 수 있습니다.

기본 클러스터 IP 주소는 현재 제어 유닛에 항상 속해 있는 클러스터의 고정 주소입니다. 주소의 범위를 설정하여 현재 제어 유닛을 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 합니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 제어 유닛이 변경될 경우 기본 클러스터 IP 주소는 새 제어 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다.

예를 들어, 현재 제어 유닛에 항상 연결되어 있는 기본 클러스터 IP 주소에 연결하여 클러스터를 관리할 수 있습니다. 로컬 IP 주소에 연결하여 개별 멤버를 관리할 수 있습니다.

참고 To-the-box 트래픽은 노드의 관리 IP 주소로 전달되어야 합니다. To-the-box 트래픽은 클러스터 제어 링크를 통해 다른 노드로 전달되지 않습니다.

TFTP 또는 시스템 로그 같은 아웃바운드 관리 트래픽의 경우, 제어 유닛을 비롯한 각 유닛에서는 로컬 IP 주소를 사용하여 서버에 연결합니다.

제어 유닛 관리 대 데이터 유닛 관리

모든 관리 및 모니터링은 제어 노드에서 수행할 수 있습니다. 제어 노드에서 런타임 통계, 리소스 사용량 또는 모든 노드의 기타 모니터링 정보를 확인할 수 있습니다. 또한 클러스터 내의 모든 노드에 명령을 구축하고, 데이터 노드의 콘솔 메시지를 제어 노드로 복제할 수 있습니다.

필요한 경우 데이터 노드를 직접 모니터링할 수 있습니다. 제어 노드에서도 사용 가능하지만 데이터 노드에서 파일 관리를 수행할 수 있습니다(구성 백업 및 이미지 업데이트 포함). 제어 노드에서는 다음 기능을 사용할 수 없습니다.

- 노드당 클러스터별 통계 모니터링.
- 노드당 Syslog 모니터링(콘솔 복제가 활성화된 경우 콘솔로 전송되는 syslog 제외).
- SNMP
- NetFlow

암호화 키 복제

제어 노드에서 암호화 키를 생성할 경우, 해당 키는 모든 데이터 노드에 복제됩니다. 기본 클러스터 IP 주소에 대한 SSH 세션이 있는 경우 제어 노드에 오류가 발생하면 연결이 끊어집니다. 새 제어 노드에서는 SSH 연결에 동일한 키를 사용하므로, 새 제어 노드에 다시 연결할 때 캐시된 SSH 호스트 키를 업데이트하지 않아도 됩니다.

ASDM 연결 인증서 **IP** 주소 불일치

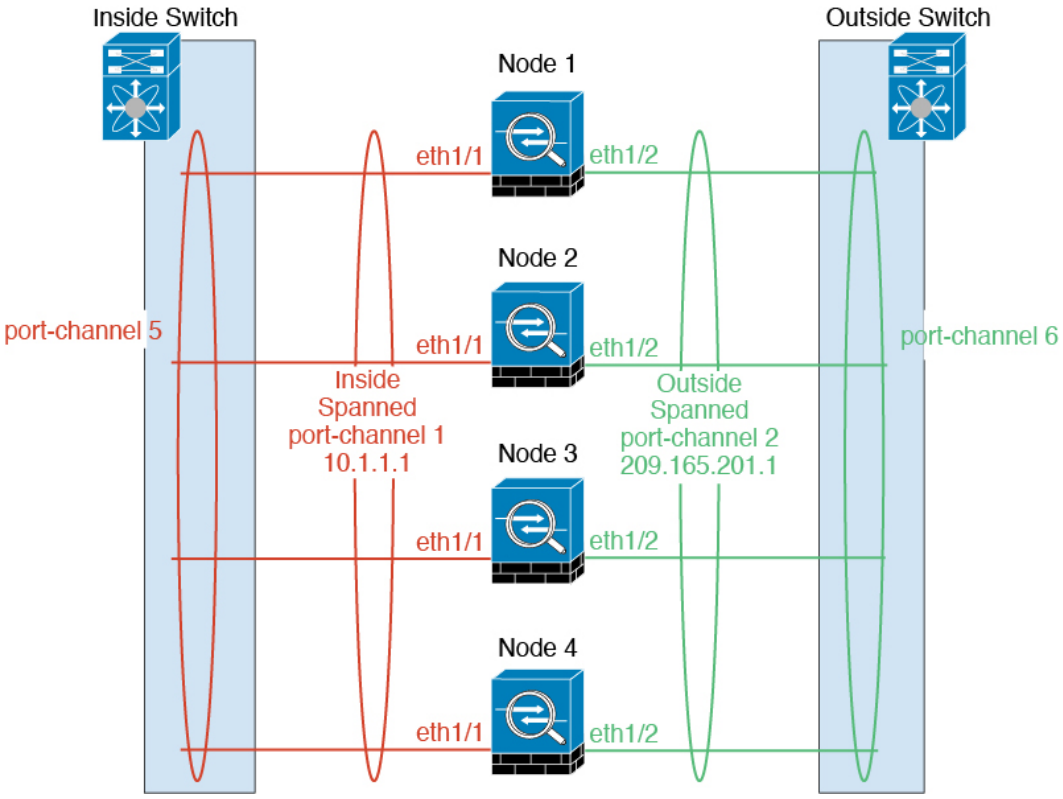
기본적으로, 자체 서명된 인증서는 로컬 IP 주소를 기준으로 ASDM 연결에 사용됩니다. ASDM을 사용하여 기본 클러스터 IP 주소를 연결할 경우, 인증서에서는 기본 클러스터 IP 주소가 아닌 로컬 IP 주소를 사용하므로 IP 주소가 일치하지 않는다는 경고 메시지가 표시됩니다. 이 메시지를 무시하고 ASDM 연결을 설정할 수 있습니다. 그러나 이러한 유형의 경고를 방지하려면 기본 클러스터 IP 주소 및 IP 주소 풀의 모든 로컬 IP 주소가 포함된 인증서를 등록하면 됩니다. 그런 다음 이 인증서를 각 클러스터 멤버에 사용할 수 있습니다. 자세한 내용은 https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html를 참조하십시오.

스팬 **EtherChannels**(권장)

섀시당 하나 이상의 인터페이스를 클러스터 내의 모든 섀시를 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다.

스팬 EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 브리지 그룹 멤버 인터페이스가 아닌 BVI에 IP 주소가 할당됩니다.

EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.



사이트 간 클러스터링

사이트 간 설치 시 다음 권장 지침을 준수하면 ASA 클러스터링을 활용할 수 있습니다.

각 클러스터 섀시를 별도의 사이트 ID에 속하도록 구성할 수 있습니다.

사이트 ID는 사이트별 MAC 주소 및 IP 주소와 작동합니다. 클러스터에서 이그레스되는 패킷은 사이트별 MAC 주소 및 IP 주소를 사용하는 반면, 클러스터가 수신한 패킷은 전역 MAC 주소 및 IP 주소를 사용합니다. 이 기능은 스위치가 서로 다른 두 포트의 두 사이트로부터 동일한 전역 MAC 주소를 학습하지 못하게 하는 한편, MAC 플래핑(flapping)을 일으킵니다. 대신 스위치는 사이트 MAC 주소만 학습합니다. 사이트별 MAC 주소 및 IP 주소는 Spanned EtherChannel만을 사용하는 라우팅 모드에서 지원됩니다.

사이트 ID는 LISP 검사를 사용한 플로우 모빌리티 활성화, 데이터 센터의 사이트 간 클러스터링에 대해 왕복 시간 레이턴시를 줄이고 성능을 개선하기 위한 관리자 지역화, 그리고 트래픽 플로우의 백업 소유자가 항상 소유자와 다른 사이트에 있는 연결에 대한 사이트 이중화에도 사용됩니다.

사이트 간 클러스터링에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 데이터 센터 인터커넥트 크기 조정 -클러스터링의 요구 사항 및 사전 요구 사항 - Firepower 4100/9300 섀시, 10 페이지
- 사이트 간 지침 -클러스터링 지침 및 제한 사항, 13 페이지
- 클러스터 플로우 모빌리티 구성 —클러스터 플로우 모빌리티 구성, 40 페이지

- 관리자 현지화 활성화 —기본 ASA 클러스터 파라미터 구성, 34 페이지
- 사이트 이중화 활성화 —기본 ASA 클러스터 파라미터 구성, 34 페이지

클러스터링의 요구 사항 및 사전 요구 사항 - Firepower 4100/9300 섀시

모델별 최대 클러스터링 유닛 수

- Firepower 4100 — 16개 섀시
- Firepower 9300 — 16개 모듈 예를 들어 섀시 16개에 모듈 1개, 섀시 8개에 모듈 2개, 또는 모듈을 16개까지 제공하는 어떤 조합도 사용할 수 있습니다.

섀시 간 클러스터링을 위한 하드웨어 및 소프트웨어 요구 사항

클러스터의 모든 섀시:

- Firepower 4100의 경우 모든 섀시가 동일한 모델이어야 합니다. Firepower 9300의 경우: 모든 보안 모듈이 동일한 유형이어야 합니다. 예를 들어 클러스터링을 사용하는 경우 Firepower 9300의 모든 모듈은 SM-40이어야 합니다. 빈 슬롯을 포함하여 섀시에 있는 모든 모듈은 클러스터에 속해야 하지만 각 섀시에 설치된 보안 모듈의 수는 다를 수 있습니다.
- 이미지 업그레이드 시 동일한 FXOS 및 애플리케이션 소프트웨어 예외를 실행해야 합니다. 소프트웨어 버전이 일치하지 않으면 성능이 저하될 수 있으므로 동일한 유지 관리 기간에 모든 노드를 업그레이드해야 합니다.
- 클러스터에 할당하는 인터페이스에 대한 것과 동일한 인터페이스 구성을 포함해야 합니다(예: EtherChannel, 활성 인터페이스, 속도 및 이중 등). 동일한 인터페이스 ID에 대해 용량이 일치하고 동일한 Spanned EtherChannel에서 성공적인 인터넷 번들링이 가능한 한 섀시에서 서로 다른 네트워크 모듈 유형을 사용할 수 있습니다. 모든 데이터 인터페이스는 섀시가 여러 개인 클러스터의 EtherChannel이어야 합니다. 인터페이스 모듈을 추가 또는 제거하거나 EtherChannel을 구성하는 등의 방법을 통해 클러스터링을 활성화한 후 FXOS에서 인터페이스를 변경하는 경우에는 각 섀시에서 데이터 노드부터 시작하여 마지막으로 제어 노드까지 같은 변경을 수행합니다. FXOS에서 인터페이스를 제거하는 경우 ASA 구성에서는 관련 명령을 유지하므로 필요한 조정을 수행할 수 있습니다. 구성에서 인터페이스를 제거하는 경우에는 구성 전반에 걸쳐 영향을 줄 수 있습니다. 이전 인터페이스 구성을 수동으로 제거할 수 있습니다.
- 동일한 NTP 서버를 사용해야 합니다. 시간을 수동으로 설정해서는 안 됩니다.
- ASA: 각 FXOS 섀시를 License Authority 또는 Satellite Server에 등록해야 합니다. 데이터 노드에 대한 추가 비용은 없습니다. 영구 라이선스를 예약하려면 각 섀시용으로 별도의 라이선스를 구매해야 합니다. Firewall Threat Defense의 경우 모든 라이선싱이 Firewall Management Center에서 처리됩니다.

스위치 요구 사항

- Firepower 4100/9300 섀시에서 클러스터링을 구성하기 전에 스위치 구성을 완료하고 섀시의 모든 EtherChannel을 스위치에 성공적으로 연결하십시오.
- 지원되는 스위치 특성은 Cisco FXOS 호환성을 참조하십시오.

사이트 간 클러스터링을 위한 **Data Center Interconnect** 크기 조정

클러스터 제어 링크 트래픽을 처리하기 위한 DCI(data center interconnect) 대역폭을 다음 계산과 같이 예약해야 합니다.

$$\frac{\#\text{ of cluster members per site}}{2} \times \text{cluster control link size per member}$$

각 사이트의 멤버 수가 다를 경우, 더 큰 숫자를 계산에 사용합니다. DCI의 최소 대역폭은 한 멤버에 대한 클러스터 제어 링크의 크기보다 작으면 안 됩니다.

예를 들면 다음과 같습니다.

- 2개 사이트에 멤버가 4개인 경우:
  - 총 클러스터 멤버 4개
  - 각 사이트당 멤버 2개
  - 멤버당 5Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 5Gbps(2/2 x 5Gbps)
- 3개 사이트에 멤버가 6개인 경우 크기가 다음과 같이 증가함:
  - 총 클러스터 멤버 6개
  - 사이트 1에 멤버 3개, 사이트 2에 멤버 2개, 사이트 3에 멤버 1개
  - 멤버당 10Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 15Gbps(3/2 x 10Gbps)
- 2개 사이트에 멤버가 2개인 경우:
  - 총 클러스터 멤버 2개
  - 사이트당 멤버 1개
  - 멤버당 10Gbps 클러스터 제어 링크

  예약된 DCI 대역폭 = 10Gbps(1/2 x 10Gbps = 5Gbps). 그러나 최소 대역폭은 클러스터 제어 링크의 크기(10Gbps)보다 작으면 안 됩니다.

클러스터링에 대한 라이선스 - Firepower 4100/9300 섀시

Smart Software Manager 일반 및 온프레미스

클러스터링 기능 자체에는 라이선스가 필요하지 않습니다. 강력한 암호화 및 기타 선택적 라이선스를 사용하려면 각 Firepower 4100/9300 섀시 라이선스가 License Authority 또는 Smart Software Manager 일반 및 온프레미스 서버에 등록되어야 합니다. 데이터 유닛에 대한 추가 비용은 없습니다.

사용자가 등록 토큰을 적용하면 적격 고객을 대상으로 강력한 암호화 라이선스가 자동으로 활성화됩니다. 토큰을 사용하는 경우 각 섀시에 동일한 암호화 라이선스가 있어야 합니다. ASA 구성에서 활성화된 선택적 강력한 암호화(3DES/AES) 기능 라이선스에 대해서는 아래를 참조하십시오.

ASA 라이선스 구성에서는 제어 유닛에서만 스마트 라이선싱을 구성할 수 있습니다. 구성은 데이터 유닛에 복제됩니다. 하지만 일부 라이선스의 경우 구성을 사용하지 않고 캐시된 상태로 남으며, 제어 유닛만 라이선스를 요청합니다. 라이선스는 클러스터 유닛에서 공유된 단일 클러스터 라이선스로 집계되고, 이 집계된 라이선스는 데이터 유닛 중 하나가 나중에 제어 유닛이 되면 사용할 제어 유닛에서도 캐시됩니다. 각 라이선스 유형은 다음과 같이 관리됩니다.

- Essentials - 이제 제어 유닛에서만 서버에서 Essentials 라이선스를 요청할 수 있으며, 라이선스 집계 덕분에 두 유닛 모두 이 라이선스를 사용할 수 있습니다.
- Context — 제어 유닛만 서버에서 Context 라이선스를 요청합니다. Essentials 라이선스는 기본적으로 10개의 상황을 포함하며 모든 클러스터 멤버에 있습니다. 각 유닛의 Essentials 라이선스 값과 제어 유닛의 Context 라이선스 값은 집계된 클러스터 라이선스에서 플랫폼 한도에 도달할 때까지 통합됩니다. 예를 들면 다음과 같습니다.
  - 클러스터에 6개의 Firepower 9300 모듈을 갖고 있습니다. Essentials 라이선스는 10개의 상황을 포함하고 이러한 라이선스는 6개 유닛에 최대 60개의 상황을 추가합니다. 제어 유닛에서 20개의 추가 Context 라이선스를 구성합니다. 따라서 집계된 클러스터 라이선스에서는 80개의 상황을 포함합니다. 모듈 1개에 대한 플랫폼 한도가 250개이므로 통합된 라이선스에서는 최대 250개의 상황을 허용합니다. 80개의 상황은 제한을 초과하지 않습니다. 따라서 제어 유닛에서 최대 80개의 상황을 구성할 수 있습니다. 각 데이터 유닛에서도 구성 복제를 통해 80개의 상황을 포함할 수 있습니다.
  - 클러스터에 3개의 Firepower 4112 유닛을 갖고 있습니다. Essentials 라이선스는 10개의 상황을 포함하고 이러한 라이선스는 3개 유닛에 최대 30개의 상황을 추가합니다. 제어 유닛에서 250개의 추가 Context 라이선스를 구성합니다. 따라서 집계된 클러스터 라이선스에서는 280개의 상황을 포함합니다. 유닛 1개에 대한 플랫폼 한도가 250개이므로 통합된 라이선스에서는 최대 250개의 상황을 허용합니다. 280개의 상황은 제한을 초과합니다. 따라서 제어 유닛에서는 최대 250개의 상황만 구성할 수 있습니다. 각 데이터 유닛에서도 구성 복제를 통해 250개의 상황을 포함할 수 있습니다. 이 경우 제어 유닛 Context 라이선스만 220개의 상황으로 구성해야 합니다.
- 통신 사업자 — 분산 S2S VPN에 필요합니다. 이 라이선스는 유닛당 엔타이틀먼트이며 각 유닛은 서버에서 고유한 라이선스를 요청합니다.
- 강력한 암호화(3DES) - 2.3.0 이전의 Cisco Smart Software Manager 온프레미스 구축의 경우 또는 스마트 어카운트가 강력한 암호화에 대해 인증되지 않았지만 Cisco에서 강력한 암호화를 사용

할 수 있다고 결정한 경우, 수동으로 어카운트에 강력한 암호화 라이선스를 추가할 수 있습니다. 이 라이선스는 유닛당 엔타이틀먼트이며 각 유닛은 서버에서 고유한 라이선스를 요청합니다.

새 제어 유닛이 선택되면 새 제어 유닛은 집계된 라이선스를 계속해서 사용합니다. 또한 제어 유닛 라이선스를 다시 요청하기 위해 캐시된 라이선스 구성을 사용합니다. 이전 제어 유닛이 클러스터를 데이터 유닛으로 다시 조인하는 경우, 제어 유닛 라이선스 엔타이틀먼트를 릴리스합니다. 데이터 유닛이 라이선스를 릴리스하기 전에 어카운트에서 사용 가능한 라이선스가 없는 경우 제어 유닛의 라이선스는 비준수 상태일 수 있습니다. 유지된 라이선스는 30일 동안 유효하지만 유예 기간이 지난 후에도 계속해서 비준수 상태인 경우 특별 라이선스가 필요한 기능의 구성을 변경할 수 없습니다. 이를 제외하면 작동에 영향을 미치지 않습니다. 새 액티브 유닛은 라이선스 준수 상태가 될 때까지 12시간마다 엔타이틀먼트 권한 부여 갱신 요청을 보냅니다. 라이선스 요청이 완전히 처리될 때까지 구성을 변경하지 않아야 합니다. 유닛이 클러스터를 떠나는 경우, 캐시된 제어 구성은 제거되는 반면, 유닛당 엔타이틀먼트는 유지됩니다. 특히, 비클러스터 유닛에서 Context 라이선스를 다시 요청해야 합니다.

영구 라이선스 예약

영구 라이선스를 예약하려면, 각 섀시에 대해 별도의 라이선스를 구매하고 클러스터링을 구성하기 전에 해당 라이선스를 활성화해야 합니다.

클러스터링 지침 및 제한 사항

섀시 간 클러스터링을 위한 스위치

- 연결된 스위치가 클러스터 데이터 인터페이스 및 클러스터 제어 링크 인터페이스 모두의 MTU와 일치해야 합니다. 클러스터 제어 링크 인터페이스 MTU를 데이터 인터페이스 MTU보다 100바이트 이상 높게 설정해야 하므로 스위치를 연결하는 클러스터 제어 링크를 적절하게 설정해야 합니다. 클러스터 제어 링크 트래픽에는 데이터 패킷 전달이 포함되므로 클러스터 제어 링크는 데이터 패킷의 전체 크기와 클러스터 트래픽 오버헤드를 모두 수용해야 합니다. 또한 Cisco에서는 클러스터 제어 링크 MTU를 2561과 8362 사이로 설정하지 않는 것을 권장합니다. 블록 풀 처리로 인해 이 MTU 크기는 시스템 작동에 최적이 아닙니다.
- Cisco IOS XR 시스템의 경우 기본이 아닌 MTU를 설정하려면 IOS 인터페이스 MTU를 클러스터 디바이스 MTU보다 14바이트 높게 설정합니다. 그렇지 않으면, **mtu-ignore** 옵션을 사용하지 않는 경우 OSPF 인접 피어링 시도에 실패할 수 있습니다. 클러스터 디바이스 MTU는 IOS XR *IPv4* MTU와 일치해야 합니다. Cisco Catalyst 및 Cisco Nexus 스위치에는 이 조정이 필요하지 않습니다.
- 클러스터 제어 링크 인터페이스용 스위치의 경우, 클러스터 유닛에 연결된 스위치 포트에서 Spanning Tree PortFast를 사용하도록 선택하여 새 유닛에 대한 참가 프로세스 속도를 높일 수 있습니다.
- 스위치에서는 **source-dest-ip**또는 **src-dst-mixed-ip-port** EtherChannel 로드 밸런싱 알고리즘 중 하나를 사용하는 것이 좋습니다(Cisco Nexus OS 및 Cisco IOS **port-channel load-balance** 명령 참조). 로드 밸런싱 알고리즘에서는 **vlan** 키워드를 사용하지 마십시오. 이렇게 할 경우 클러스터의 디바이스에 트래픽이 균일하지 않게 분산될 수 있습니다. 클러스터 디바이스에서 로드 밸런싱 알고리즘의 기본값을 변경하지 마십시오.

- 스위치에서 EtherChannel의 로드 밸런싱 알고리즘을 변경할 경우, 스위치의 EtherChannel 인터페이스에서 트래픽 전달이 일시적으로 중단되며 Spanning Tree Protocol이 재시작됩니다. 트래픽에서 흐름을 다시 시작하기 전까지 지연이 발생하게 됩니다.
- 클러스터 제어 링크 경로의 스위치에서는 L4 체크섬을 확인하지 않습니다. 클러스터 제어 링크를 통해 리디렉션된 트래픽에는 올바른 L4 체크섬이 없습니다. L4 체크섬을 확인하는 스위치의 경우 트래픽이 감소하는 결과를 초래할 수 있습니다.
- 포트 채널 번들링 다운타임은 구성된 keepalive 기간을 초과하면 안 됩니다.
- Supervisor 2T EtherChannel에서 기본 해시 분산 알고리즘은 적응형입니다. VSS 설계에서 비대칭 트래픽을 방지하려면 클러스터 디바이스에 연결된 포트 채널의 해시 알고리즘을 다음과 같이 변경하여 수정합니다.

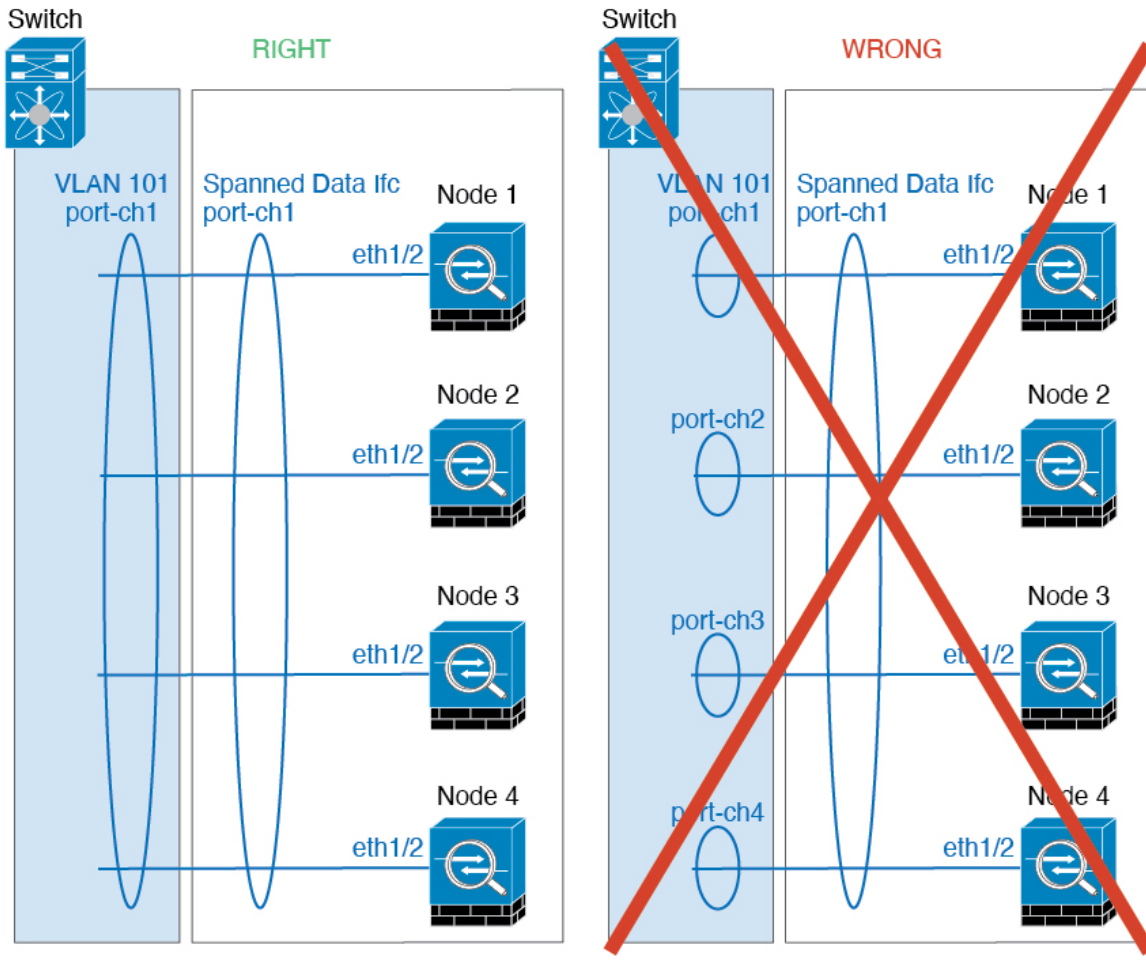
  router(config) # **port-channel** *id* **hash-distribution fixed**

  VSS 피어 링크의 적응형 알고리즘을 활용할 때가 있을 수 있으므로 알고리즘을 전역으로 변경하지 마십시오.

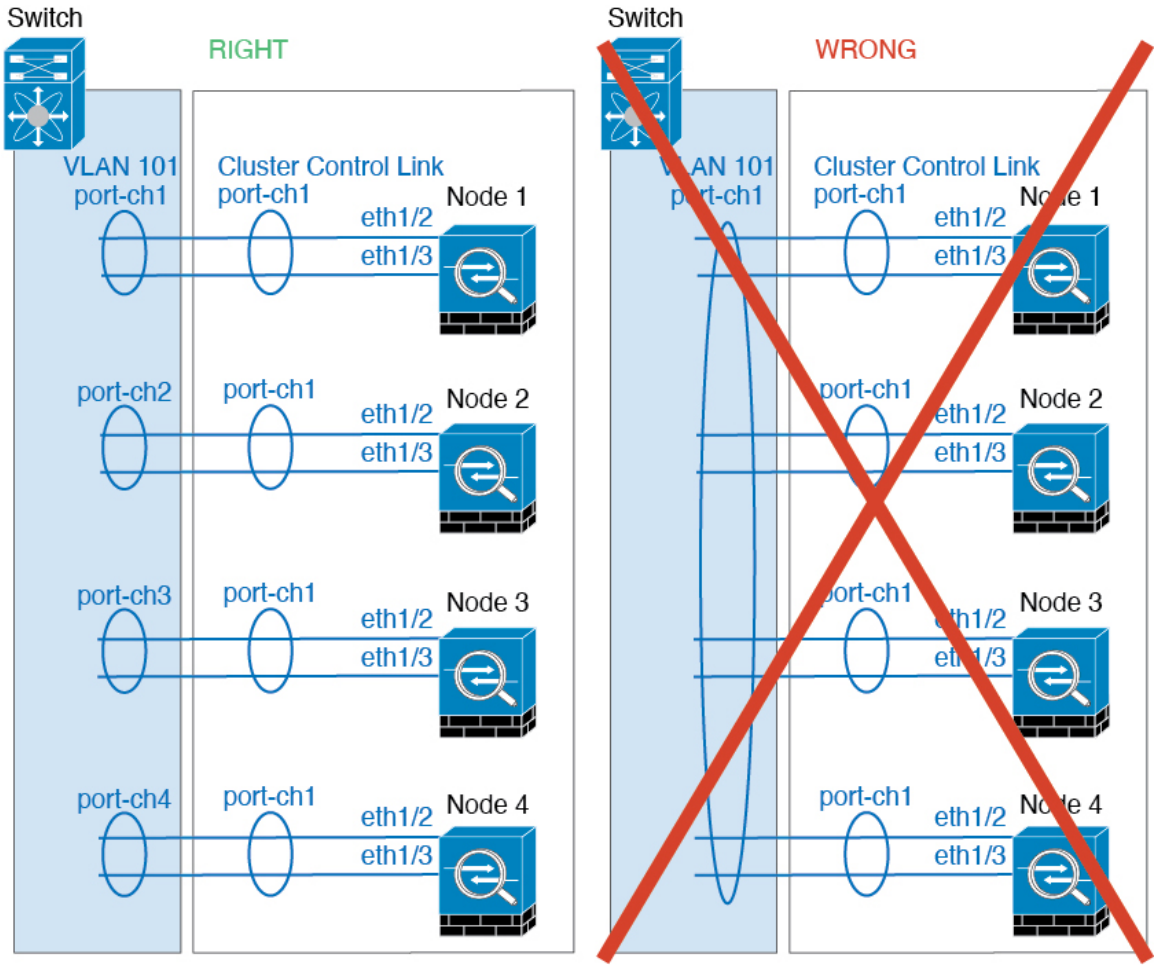
- ASA 하드웨어 클러스터와 달리, Firepower 4100/9300 클러스터는 LACP 단계적 통합을 지원합니다. 따라서 플랫폼의 경우, 연결된 Cisco Nexus 스위치에서 LACP 단계적 통합을 활성화된 상태로 둘 수 있습니다.
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대한 LACP 속도를 빠르게 설정할 수 있습니다. FXOS EtherChannel에서는 기본적으로 LACP 속도가 fast(고속)로 설정됩니다. Nexus Series와 같은 일부 스위치는 ISSU(In-Service Software Upgrade) 수행 시 고속 LACP를 지원하지 않으므로 클러스터링에서는 ISSU를 사용하지 않는 것이 좋습니다.

클러스터링을 위한 **EtherChannel**

- 15.1(1)S2 이전 Catalyst 3750-X Cisco IOS 소프트웨어 버전에서는 클러스터 유닛에서 EtherChannel과 스위치 스택 간 연결을 지원하지 않았습니다. 기본 스위치 설정으로 클러스터 유닛 EtherChannel이 교차 스택에 연결되어 있는 상태에서 제어 유닛 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.
- Spanned EtherChannel 구성과 디바이스-로컬 EtherChannel 구성 — Spanned EtherChannel과 디바이스-로컬 EtherChannel에서 각각 알맞게 스위치를 구성해야 합니다.
  - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 클러스터 유닛 스팬 EtherChannels의 경우, 인터페이스가 스위치의 단일 EtherChannel에 통합됩니다. 각 인터페이스가 스위치의 동일한 채널 그룹에 있는지 확인하십시오.



- 디바이스-로컬 EtherChannel - 클러스터 제어 링크에 대해 구성된 모든 EtherChannel을 비롯한 클러스터 유닛 디바이스-로컬 EtherChannel의 경우 스위치에서 별도의 EtherChannel을 구성해야 합니다. 여러 클러스터 유닛 EtherChannel을 스위치에서 하나의 EtherChannel에 통합하지 마십시오.



사이트 간 클러스터링

사이트 간 클러스터링에 대한 다음 지침을 참조하십시오.

- 클러스터 제어 링크 레이턴시는 RTT(왕복 시간)가 20ms 이하여야 합니다.
- 클러스터 제어 링크는 오류가 나거나 폐기된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 전용 링크를 사용해야 합니다.
- 연결 리밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 연결이 리밸런싱됩니다.
- ASA는 DCCI(Data Center Interconnect)에서 사용되는 경우에도 전용 링크이므로 클러스터 제어 링크에서 전달된 데이터 트래픽을 암호화하지 않습니다. OTV(Overlay Transport Virtualization)를 사용하거나 로컬 제어 도메인 외부에서 클러스터 제어 링크를 확장하는 경우 OTV를 통한 802.1AE MacSec과 같은 보더 라우터에서 암호화를 구성할 수 있습니다.
- 클러스터를 구현할 경우 들어오는 연결에 대한 여러 사이트에 있는 멤버가 구분되지 않습니다. 따라서 하나의 특정한 연결의 연결 역할은 사이트 전체를 포괄하게 될 수 있습니다. 이는 정상적

인 동작입니다. 그러나 관리자 지역화를 활성화하는 경우 항상 연결 소유자와 동일한 사이트에서 로컬 관리자 역할이 선택됩니다(사이트 ID에 따라). 원래 소유자가 실패하면 로컬 관리자는 동일한 사이트에서 새 소유자를 선택합니다.(참고: 트래픽이 사이트 간에 비동기 상태이고 원래 소유자가 실패한 후 원격 사이트로부터 계속 트래픽이 발생하면, 원격 사이트의 노드가 재호스팅 기간 내에 데이터 패킷을 수신하는 경우 새로운 소유자가 될 수 있습니다.)

- 관리자 지역화의 경우 NAT 또는 PAT 트래픽, SCTP에서 검사된 트래픽, 단편화 소유자 쿼리 등의 트래픽 유형은 지역화를 지원하지 않습니다.
- North-South 구축 환경에서 UDP 장기 유동의 경우, 원본 유동 소유자 사이트의 노드가 장애 발생 후 복구되면 라우팅 루프가 발생할 수 있습니다. 이후 유동은 다시 원본 사이트로 재지정됩니다. 다른 사이트의 새 소유자가 목적지까지의 경로를 가지고 있지 않으면, 해당 플로우를 인터넷으로 되돌려 보내게 되어 루프 현상이 발생합니다. 이 경우 새 소유자에서 **clear conn** 명령을 사용하여 플로우를 강제로 재설정합니다.
- 투명 모드에서, 클러스터가 내부 및 외부 라우터(north-south 삽입이라고도 함) 쌍 사이에 위치하면 내부 라우터 모두에서 MAC 주소를 공유해야 하며 외부 라우터 모두에서도 MAC 주소를 공유해야 합니다. 사이트 1의 클러스터 멤버가 사이트 2의 멤버에 연결을 전달할 경우, 목적지 MAC 주소가 유지됩니다. MAC 주소가 사이트 1의 라우터와 동일할 경우 패킷은 사이트 2의 라우터에만 도달합니다.
- 투명 모드에서 클러스터가 내부 네트워크(East-West 삽입이라고 함) 사이에서 방화벽을 위해 각 사이트에서 데이터 네트워크 및 게이트웨이 라우터 사이에 위치하면 각 게이트웨이 라우터는 HSRP와 같은 첫 번째 홉 이중화 프로토콜(FHRP)을 사용하여 각 사이트에서 동일한 가상 IP 및 MAC 주소 대상을 제공해야 합니다. 데이터 VLAN은 OTV(오버레이 전송 가상화) 또는 유사한 기능을 사용하는 사이트 전체로 확장됩니다. DCI를 통해 다른 사이트로 전송 중인 로컬 게이트웨이 라우터에 예약된 트래픽을 방지하려면 필터를 생성해야 합니다. 게이트웨이 라우터가 1개의 사이트에 연결할 수 없게 되면, 모든 필터를 제거해야 트래픽이 성공적으로 다른 사이트의 게이트웨이에 연결할 수 있습니다.
- 투명 모드의 경우, 클러스터가 HSRP 라우터에 연결된 경우 라우터 HSRP MAC 주소를 ASA. 인접 라우터가 HSRP를 사용하는 경우, HSRP IP 주소로 향하는 트래픽은 HSRP MAC 주소로 전송되지만, 반환 트래픽은 HSRP 쌍에 있는 특정 라우터 인터페이스의 MAC 주소에서 제공됩니다. 따라서 ASA MAC 주소 테이블은 일반적으로 HSRP IP 주소에 대한 ASA ARP 테이블 항목이 만료되고 ASA가 ARP 요청을 보내고 응답을 수신하는 경우에만 업데이트됩니다. ASA의 ARP 테이블 항목은 기본적으로 14,400초 후에 만료되지만 MAC 주소 테이블 항목은 기본적으로 300초 후에 만료되므로 MAC 주소 테이블 만료 트래픽 삭제를 방지하려면 고정 MAC 주소 항목이 필요합니다.
- Spanned EtherChannel을 사용하는 라우팅 모드의 경우 사이트별 MAC 주소를 구성하십시오. OTV 또는 유사한 것을 사용하여 사이트 전체로 데이터 VLAN을 확장하십시오. 전역 MAC 주소로 향하는 트래픽이 DCI를 통해 다른 사이트에 가지 않도록 필터를 생성해야 합니다. 어떤 사이트에서 클러스터가 연결할 수 없게 되면 트래픽이 다른 사이트의 클러스터 노드에 성공적으로 도달할 수 있도록 모든 필터를 제거해야 합니다. 사이트 간 클러스터가 확장 세그먼트의 FHR(First Hop Router)로 작동하는 경우에는 동적 라우팅이 지원되지 않습니다.

추가 지침

- 중요한 토폴로지 변경 사항(예: EtherChannel 인터페이스 추가 또는 제거, Firepower 4100/9300 섀시 또는 스위치의 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS, vPC, StackWise 또는 StackWise Virtual 구성)이 발생할 경우, 상태 검사 기능을 비활성화하고 비활성화된 인터페이스에 대해 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.
- 기존 클러스터에 유닛을 추가하거나 유닛을 다시 로드할 경우, 일시적이고 제한적으로 패킷/연결이 감소하며 이는 정상적인 동작입니다. 경우에 따라 감소된 패킷으로 인해 연결이 끊어질 수 있습니다. 예를 들어, FTP 연결의 FIN/ACK 패킷이 감소할 경우 FTP 클라이언트가 끊어집니다. 이 경우 FTP 연결을 다시 설정해야 합니다.
- Spanned EtherChannel 인터페이스에 연결된 Windows 2003 서버를 사용할 경우 syslog 서버 포트가 중지되면 서버에서 ICMP 오류 메시지를 제한하지 않아 대량의 ICMP 메시지가 클러스터에 다시 전송됩니다. 이러한 메시지로 인해 클러스터의 일부 유닛에서 CPU 점유율이 높아져 성능에 영향을 미칠 수 있습니다. 이러한 문제를 방지하려면 ICMP 오류 메시지를 제한하는 것이 좋습니다.
- 이중화를 위해 EtherChannel을 VSS, vPC, StackWise 또는 StackWise Virtual에 연결하는 것이 좋습니다.
- 섀시 내에서 일부 보안 모듈을 클러스터하여 독립형 모드에서 다른 보안 모듈을 실행할 수 없습니다. 클러스터에 모든 보안 모듈을 포함해야 합니다.

기본값

- 클러스터 상태 검사 기능은 기본적으로 활성화되어 있으며 3초간의 대기 시간이 있습니다. 인터페이스 상태 모니터링은 모든 인터페이스에서 기본적으로 활성화됩니다.
- 연결 리밸런싱은 기본적으로 비활성화되어 있습니다. 연결 리밸런싱을 활성화할 경우 로드 정보를 교환하는 데 걸리는 기본 시간은 5초입니다.
- 실패한 클러스터 제어 링크에 대한 클러스터 자동 다시 참가 기능은 5분마다 무제한으로 시도하도록 설정됩니다.
- 실패한 데이터 인터페이스에 대한 클러스터 자동 다시 참가 기능은 간격이 2로 늘어 5분마다 3번 시도하도록 설정됩니다.
- 5초 연결 복제 지연은 HTTP 트래픽에 대해 기본적으로 활성화되어 있습니다.

클러스터링 구성 - Firepower 4100/9300 섀시

Firepower 4100/9300 섀시 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다. 이 섹션에서는 ASA에서 수행할 수 있는 기본 부트스트랩 구성 및 맞춤화(선택 사항)에 대해 설명합니다. 이 섹션에서는 ASA 내에서 클러스터 멤버를 관리하는 방법에 대해서도 설명합니다. Firepower 4100/9300 섀시에서 클러스터 멤버십을 관리할 수도 있습니다. 자세한 내용은 Firepower 4100/9300 섀시 설명서를 참조하십시오.

프로시저

단계 1 FXOS: ASA 클러스터 추가, 23 페이지
단계 2 ASA: 방화벽 모드 및 상황 모드 변경, 31 페이지
단계 3 ASA: 데이터 인터페이스 구성, 31 페이지
단계 4 ASA: 클러스터 구성 맞춤화, 34 페이지
단계 5 ASA: 클러스터 멤버 관리, 52 페이지

FXOS: 인터페이스 구성

클러스터의 경우 다음 유형의 인터페이스를 구성해야 합니다.

- 클러스터를 구축하기 전에 데이터 유형 인터페이스 또는 EtherChannel(port-channel이라고도 함)을 최소 1개 추가합니다. EtherChannel(포트 채널) 추가, 21 페이지 또는 실제 인터페이스 구성, 20 페이지를 참조하십시오.

  섀시 간 클러스터링의 경우, 모든 데이터 인터페이스는 멤버 인터페이스가 최소 1개 있는 Spanned EtherChannel이어야 합니다. 각 섀시에 동일한 EtherChannel을 추가합니다. 스위치의 단일 EtherChannel에 모든 클러스터 유닛의 멤버 인터페이스를 결합합니다. 섀시 간 클러스터링을 위한 EtherChannel에 대한 자세한 내용은 클러스터링 지침 및 제한 사항, 13 페이지을 참조하십시오.

- 관리 유형 인터페이스 또는 EtherChannel을 추가합니다. EtherChannel(포트 채널) 추가, 21 페이지 또는 실제 인터페이스 구성, 20 페이지를 참조하십시오.

  관리 인터페이스는 필수 항목입니다. 이 관리 인터페이스는 섀시 관리용으로만 사용되는 섀시 관리 인터페이스(FXOS에서 MGMT, management0 또는 기타 유사한 이름으로 표시되는 섀시 관리 인터페이스 확인 가능)와는 다릅니다.

  섀시 간 클러스터링의 경우 각 섀시에 동일한 Management(관리) 인터페이스를 추가합니다.

- 섀시간 클러스터링의 경우, 멤버 인터페이스를 클러스터 제어 링크 EtherChannel에 추가합니다(기본: 포트 채널 48). EtherChannel(포트 채널) 추가, 21 페이지의 내용을 참조하십시오.

  인트라 섀시 클러스터링(intra-chassis clustering)용으로 멤버 인터페이스를 추가하지 마십시오. 멤버를 추가하면 섀시에서는 이 클러스터를 섀시 간 클러스터로 가정하며, 예를 들어 Spanned EtherChannel만 사용하도록 허용합니다.

  멤버 인터페이스가 포함되지 않은 경우, **Interfaces(**인터페이스**)** 탭에서 port-channel 48 클러스터 유형 인터페이스에 **Operation State(**운영 상태**)**가 **failed(**실패**)**로 표시됩니다. 인트라 섀시 클러스터링(intra-chassis clustering)의 경우 이 EtherChannel에는 멤버 인터페이스가 필요하지 않으므로 이 Operation State(운영 상태)를 무시할 수 있습니다.

  각 섀시에 동일한 멤버 인터페이스를 추가합니다. 클러스터 제어 링크는 각 섀시의 디바이스-로컬 EtherChannel입니다. 디바이스별 스위치에서 별도의 EtherChannel을 사용합니다. 섀시 간 클

러스터링을 위한 EtherChannel에 대한 자세한 내용은 클러스터링 지침 및 제한 사항, 13 페이지을 참조하십시오.

실제 인터페이스 구성

인터페이스를 물리적으로 활성화 및 비활성화할 뿐만 아니라 인터페이스 속도 및 듀플렉스를 설정할 수 있습니다. 인터페이스를 사용하려면 FXOS에서 인터페이스를 물리적으로 활성화하고 애플리케이션에서 논리적으로 활성화해야 합니다.

참고

- QSFPH40G-CUxM의 경우, 자동 협상은 기본값으로 항상 활성화되어 있으며 비활성화할 수 없습니다.
- SFP를 다른 SFP 모듈로 교체하는 경우 인터페이스의 속도, 듀플렉스 및 자동 협상이 자동으로 업데이트되지 않습니다. 인터페이스를 수동으로 다시 구성해야 합니다.

시작하기 전에

- 이미 EtherChannel의 멤버인 인터페이스는 개별적으로 편집할 수 없습니다. EtherChannel에 인터페이스를 추가하기 전에 설정을 구성하십시오.

프로시저

단계 **1** **Interfaces(**인터페이스**)**를 선택하여 Interfaces(인터페이스) 페이지를 엽니다.

All Interfaces(모든 인터페이스**)** 페이지 상단에는 현재 설치되어 있는 인터페이스가 시각적으로 표시되며, 아래 표에는 설치되어 있는 인터페이스의 목록이 나와 있습니다.

단계 **2** 편집하려는 인터페이스 행에서 **Edit(**편집**)**를 클릭하여 **Edit Interface(**인터페이스 편집**)** 대화 상자를 엽니다.

단계 **3** 인터페이스를 활성화하려면 **Enable(**활성화**)** 확인란을 선택합니다. 인터페이스를 비활성화하려면 **Enable(**활성화**)** 확인란의 선택을 취소합니다.

단계 **4** 인터페이스 유형을 선택합니다.

- 데이터
- 관리
- 클러스터 - 클러스터 유형은 선택하지 마십시오. 기본적으로 클러스터 제어 링크는 Port-channel 48에서 자동으로 생성됩니다.

단계 **5** (선택 사항) **Speed(**속도**)** 드롭다운 목록에서 인터페이스의 속도를 선택합니다.

단계 **6** (선택 사항) 인터페이스가 **Auto Negotiation(**자동 협상**)**을 지원하는 경우 **Yes(**예**)** 또는 **No(**아니요**)** 라디오 버튼을 클릭합니다.

50G 케이블을 통해 포트에 연결하는 피어 스위치가 자동 협상을 지원하지 않는 경우 스위치 및 플랫폼 인터페이스에서도 자동 협상을 비활성화해야 합니다. 예를 들어 N9K-C93400LD-H1은 50G 케이블에서 자동 협상을 지원하지 않습니다. 연결할 포트에 대해 플랫폼 및 스위치에서 기본 자동 협상을 비활성화해야 합니다.

단계 **7** (선택 사항) **Duplex(**듀플렉스**)** 드롭다운 목록에서 인터페이스의 듀플렉스를 선택합니다.

단계 **8** (선택 사항) 명시적으로 디바운스 시간**(ms)**을 구성합니다. 0~15000밀리초 사이의 값을 입력합니다.

참고
디바운스 시간 구성은 1G 인터페이스에서는 지원되지 않습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

EtherChannel(포트 채널) 추가

EtherChannel(포트 채널로 알려짐)은 동일한 미디어 유형 및 용량의 멤버 인터페이스를 최대 16개까지 포함할 수 있으며 동일한 속도 및 듀플렉스로 설정해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다. LACP(Link Aggregation Control Protocol)에서는 두 네트워크 디바이스 간의 LACPDU(Link Aggregation Control Protocol Data Units)를 교환하여 인터페이스를 취합합니다.

EtherChannel의 각 물리적 데이터 인터페이스를 다음과 같이 구성할 수 있습니다.

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

참고 On에서 활성화, 또는 활성화에서 On으로 모드를 변경하는 경우 EtherChannel가 작동하는 데 최대 3분이 걸립니다.

비 데이터 인터페이스는 액티브 모드만 지원합니다.

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 구성이 확인되지 않습니다.

Firepower 4100/9300에서 EtherChannel을 생성하면 물리적 링크가 가동 중이더라도 EtherChannel은 논리적 디바이스에 할당될 때까지 Active LACP(액티브 LACP) 모드인 경우 **Suspended(**일시 중단**)** 상태로, On LACP(LACP 켜짐) 모드인 경우 **Down(**중단**)** 상태로 유지됩니다. 다음의 상황에서는 EtherChannel의 **Suspended(**일시 중단**)** 상태가 해제됩니다.

- EtherChannel이 독립형 논리적 디바이스에 대한 데이터 인터페이스 또는 관리 인터페이스로 추가됩니다.
- EtherChannel이 클러스터의 일부인 논리적 디바이스에 대한 관리 인터페이스 또는 클러스터 제어 링크로 추가됩니다.
- EtherChannel이 클러스터의 일부이며 유닛 하나 이상이 클러스터에 조인된 논리적 디바이스에 대한 데이터 인터페이스로 추가됩니다.

EtherChannel은 논리적 디바이스에 할당될 때까지 나타나지 않습니다. EtherChannel을 논리적 디바이스에서 제거하거나 논리적 디바이스가 삭제된 경우, EtherChannel은 **Suspended(**일시 중단**)** 또는 **Down(**중단**)** 상태로 전환됩니다.

프로시저

단계 **1** **Interfaces(**인터페이스**)**를 선택하여 Interfaces(인터페이스) 페이지를 엽니다.

All Interfaces(모든 인터페이스**)** 페이지 상단에는 현재 설치되어 있는 인터페이스가 시각적으로 표시되며, 아래 표에는 설치되어 있는 인터페이스의 목록이 나와 있습니다.

단계 **2** 인터페이스 테이블 위에 있는 **Add Port Channel(**포트 채널 추가**)**을 클릭하여 **Add Port Channel(**포트 채널 추가**)** 대화 상자를 엽니다.

단계 **3** **Port Channel ID(**포트 채널 **ID)** 필드에 포트 채널의 ID를 입력합니다. 유효한 값은 1~47입니다.

Port-channel 48은 클러스터된 논리적 디바이스를 구축할 때 클러스터 제어 링크로 예약됩니다. 클러스터 제어 링크에 포트 채널 48을 사용하지 않으려면 포트 채널 48을 삭제한 다음 다른 ID로 클러스터 유형 EtherChannel을 구성하면 됩니다.여러 클러스터 유형 EtherChannel과 멀티 인스턴스 클러스터링에 사용할 VLAN 하위 인터페이스를 추가할 수 있습니다. 인트라 섀시 클러스터링(intra-chassis clustering)의 경우, 클러스터 EtherChannel에 인터페이스를 할당하지 마십시오.

단계 **4** 포트 채널을 활성화하려면 **Enable(**활성화**)** 확인란을 선택합니다. 포트 채널을 비활성화하려면 **Enable(**활성화**)** 확인란의 선택을 취소합니다.

단계 **5** 인터페이스 유형을 선택합니다.

- 데이터
- 관리
- 클러스터

단계 **6** 드롭다운 목록에서 멤버 인터페이스의 필요한 **Admin Speed(**관리 속도**)**를 설정합니다.

지정된 속도가 아닌 멤버 인터페이스를 추가하면 포트 채널에 성공적으로 조인되지 않습니다.

단계 **7** 데이터 인터페이스의 경우 LACP 포트 채널 모드를 **Active(**액티브**)** 또는 **On(**켜짐**)** 중에서 선택합니다.

비 데이터 인터페이스의 경우 모드는 항상 액티브입니다.

단계 **8** 멤버 인터페이스에 대해 필요한 **Admin Duplex(**관리 듀플렉스**)**, **Full Duplex(**풀 듀플렉스**)** 또는 **Half Duplex(**하프 듀플렉스**)**를 설정합니다

지정된 듀플렉스로 설정된 멤버 인터페이스를 추가하면 포트 채널에 성공적으로 조인되지 않습니다.

단계 **9** 인터페이스를 포트 채널에 추가하려면 **Available Interface(**사용 가능한 인터페이스**)** 목록에서 인터페이스를 선택하고 **Add Interface(**인터페이스 추가**)**를 클릭하여 Member ID(멤버 ID) 목록으로 해당 인터페이스를 이동시킵니다.

미디어 유형과 용량이 동일한 멤버 인터페이스는 최대 16개까지 추가할 수 있습니다. 멤버 인터페이스는 동일한 속도 및 듀플렉스로 설정되어야 하며, 이 포트 채널에 대해 설정한 속도 및 듀플렉스와 일치해야 합니다. 미디어 유형은 RJ-45 또는 SFP일 수 있으며 서로 다른 유형(구리 및 광섬유)의 SFP를 혼합할 수 있습니다. 더 큰 용량의 인터페이스에서는 속도를 낮게 설정하여 인터페이스 용량(예: 1GB 및 10GB 인터페이스)을 혼합하여 사용할 수 없습니다.

팁
한 번에 여러 인터페이스를 추가할 수 있습니다. 여러 개별 인터페이스를 선택하려면 **Ctrl** 키를 누른 상태에서 필요한 인터페이스를 클릭합니다. 인터페이스 범위를 선택하려면 범위에서 첫 번째 인터페이스를 선택한 다음 **Shift** 키를 누른 상태에서 범위에 있는 마지막 인터페이스를 선택합니다.

단계 **10** 포트 채널에서 인터페이스를 제거하려면 Member ID(멤버 ID) 목록의 인터페이스 오른쪽에 있는 **Delete(**삭제**)** 버튼을 클릭합니다.

단계 **11** **OK(**확인**)**를 클릭합니다.

FXOS: ASA 클러스터 추가

단일 Firepower 9300 섀시를 섀시 내 클러스터로 추가하거나 섀시 간 클러스터링용으로 여러 섀시를 추가할 수 있습니다. 섀시 간 클러스터링의 경우, 각 섀시를 개별적으로 구성해야 합니다. 섀시 하나에 클러스터를 추가한 다음 쉽게 구축하기 위해 첫 번째 섀시의 부트스트랩 구성을 다음 섀시에 복사합니다.

ASA 클러스터 생성

이미지 버전의 범위를 설정합니다.

Firepower 4100/9300 섀시 수퍼바이저에서 클러스터를 손쉽게 구축할 수 있습니다. 모든 초기 구성은 유닛마다 자동으로 생성됩니다.

다중 섀시 클러스터의 경우 각 섀시를 개별적으로 구성해야 합니다. 섀시 하나에 클러스터를 구축한 다음 쉽게 구축하기 위해 첫 번째 섀시의 부트스트랩 컨피그레이션을 다음 섀시에 복사합니다.

모듈을 설치하지 않은 경우에도 Firepower 9300 섀시의 3개 모듈 슬롯 모두에 대해 클러스터링을 활성화해야 합니다. 3개 모듈을 모두 구성하지 않은 경우 클러스터가 나타나지 않습니다.

다중 컨텍스트 모드의 경우 먼저 논리적 디바이스를 구축한 다음 ASA 애플리케이션에서 다중 컨텍스트 모드를 활성화해야 합니다.

클러스터를 구축할 때 Firepower 4100/9300 섀시 수퍼바이저는 다음 부트스트랩 구성을 사용하여 각 ASA 애플리케이션을 구성합니다. 필요한 경우 나중에 ASA에서 일부 부트스트랩 구성을 수정할 수 있습니다(굵은 텍스트로 표시됨).

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```

참고 **local-unit** 이름은 클러스터링을 비활성화하는 경우에만 변경할 수 있습니다.

시작하기 전에

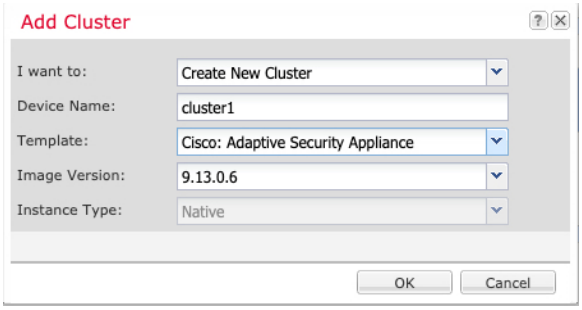
- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드한 다음, 해당 이미지를 Firepower 4100/9300 섀시에 업로드합니다.
- 다음 정보를 수집합니다.
  - 관리 인터페이스 ID, IP 주소, 네트워크 마스크
  - 게이트웨이 IP 주소

프로시저

단계 **1** 인터페이스를 구성합니다. FXOS: 인터페이스 구성, 19 페이지 섹션을 참조하십시오.

단계 **2** **Logical Devices(**논리적 디바이스**)**를 선택합니다.

단계 **3** **Add(**추가**)** > **Cluster(**클러스터**)**를 클릭하고 다음 파라미터를 설정합니다.



a) **I want to:(**수행할 작업**:)** > **Create New Cluster(**새 클러스터 생성**)**를 선택합니다.
b) **Device Name(**디바이스 이름**)**을 입력합니다.

   이 이름은 내부적으로 섀시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 애플리케이션 구성에 사용되는 디바이스 이름이 아닙니다.

c) **Template(**템플릿**)**은 **Cisco Adaptive Security Appliance**를 선택합니다.
d) **Image Version(**이미지 버전**)**을 선택합니다.
e) **Instance Type(**인스턴스 유형**)**의 경우, **Native(**네이티브**)** 유형만 지원됩니다.
f) **OK(**확인**)**를 클릭합니다.

   Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

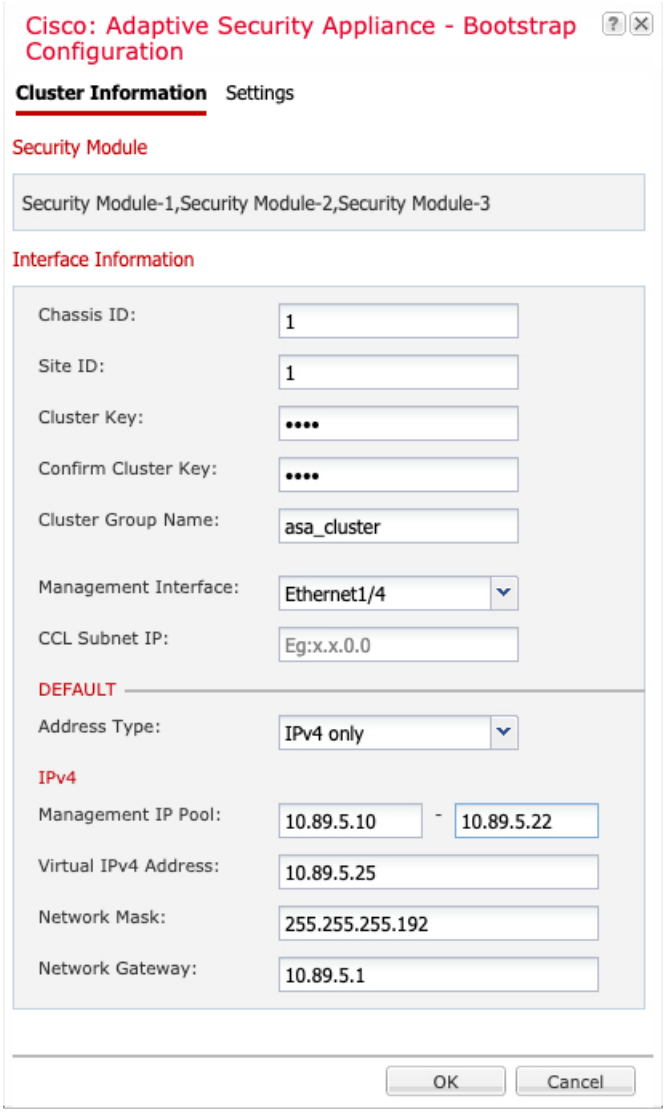
단계 **4** 이 클러스터에 할당할 인터페이스를 선택합니다.

유효한 모든 인터페이스가 기본적으로 할당되어 있습니다. 여러 클러스터 유형의 인터페이스를 지정했다면 하나를 제외하고 모두 선택 해제합니다.

단계 **5** 화면 중앙의 디바이스 아이콘을 클릭합니다.

초기 부트스트랩 설정을 구성할 수 있는 대화 상자가 표시됩니다. 이러한 설정은 초기 구축 전용 또는 재해 복구용입니다. 일반 작업 시에는 애플리케이션 CLI 구성에서 대부분의 값을 나중에 변경할 수 있습니다.

단계 **6** **Cluster Information(**클러스터 정보**)** 페이지에서 다음 작업을 수행합니다.



a) 다중 섀시 클러스터링의 경우, **Chassis ID(**섀시 **ID)** 필드에 섀시 ID를 입력합니다. 클러스터의 각 섀시는 고유 ID를 사용해야 합니다.

   이 필드는 클러스터 제어 링크 Port-Channel 48에 멤버 인터페이스를 추가한 경우에만 나타납니다.

b) 사이트 간 클러스터링의 경우 이 섀시에 대해 **Site ID(**사이트 **ID)** 필드에 1~8의 사이트 ID를 입력합니다.

c) **Cluster Key(**클러스터 키**)** 필드에서 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 구성합니다.

   공유 비밀은 1자 ~ 63자로 된 ASCII 문자열입니다. 공유 비밀은 키를 생성하는 데 사용됩니다. 이 옵션은 연결 상태 업데이트 및 전달된 패킷을 비롯한 데이터 경로 트래픽에 영향을 미치지 않으며, 항상 일반 텍스트로 전송됩니다.

d) **Cluster Group Name(**클러스터 그룹 이름**)**(논리적 디바이스 구성의 클러스터 그룹 이름)을 설정합니다.

이름은 1자 ~ 38자로 된 ASCII 문자열이어야 합니다.

중요
2.4.1부터는 클러스터 그룹 이름의 공백이 특수 문자로 간주되므로 논리적 디바이스를 구축하는 동안 오류가 발생할 수 있습니다. 이 문제를 방지하려면 공백 없이 클러스터 그룹 이름을 바꿔야 합니다.

e) **Management Interface(**관리 인터페이스**)**를 선택합니다.

이 인터페이스는 논리적 디바이스를 관리하는 데 사용됩니다. 이 인터페이스는 섀시 관리 포트와 별개입니다.

f) 관리 인터페이스의 **Address Type(**주소 유형**)**을 선택합니다.

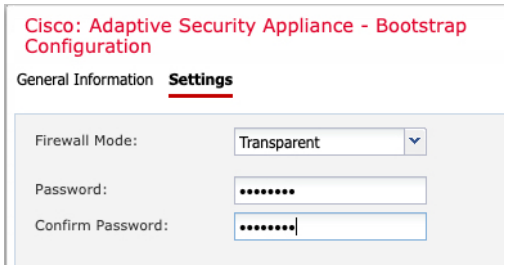
이 정보는 ASA 구성에서 관리 인터페이스를 구성하는 데 사용됩니다. 다음 정보를 설정합니다.

- **Management IP Pool(**관리 **IP** 풀**)** - 시작 및 종료 주소를 하이픈으로 구분하여 입력해 로컬 IP 주소의 풀을 구성합니다. 이 중 하나는 인터페이스의 각 클러스터 유닛에 할당됩니다.

  최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. Firepower 9300에서는 모든 모듈 슬롯을 채우지 않은 경우에도 섀시당 3개 주소를 포함해야 합니다. 클러스터를 확장하려는 경우, 추가 주소를 포함하십시오. 현재 제어 유닛에 속하는 가상 IP 주소(기본 클러스터 IP 주소)는 이러한 풀에 속하지 않습니다. 따라서 동일한 네트워크에서 기본 클러스터 IP 주소에 대한 IP 주소를 예약해 두어야 합니다. IPv4 및/또는 IPv6 주소를 사용할 수 있습니다.

- **Network Mask(**네트워크 마스크**)** 또는 **Prefix Length(**접두사 길이**)**
- 네트워크 게이트웨이
- **Virtual IP address(**가상 **IP** 주소**)** — 현재 제어 유닛의 관리 IP 주소를 설정합니다. 이 IP 주소는 같은 네트워크의 클러스터 풀 주소로 있어야 하지만 풀의 일부는 아닙니다.

단계 **7** **Settings(**설정**)** 페이지에서 다음 작업을 완료합니다.



a) **Firewall Mode(**방화벽 모드**)** 드롭다운 목록에서 **Transparent(**투명**)** 또는 **Routed(**라우팅됨**)**를 선택합니다.

라우팅 모드에서 Firewall Threat Defense는 네트워크의 라우터 홉으로 간주됩니다. 라우팅할 각 인터페이스가 다른 서브넷에 있습니다. 이와 반대로 투명 방화벽은 "비활성 엔드포인트(bump in

the wire)" 또는 "은폐형 방화벽(stealth firewall)" 같은 역할을 수행하는 레이어 2 방화벽이며, 연결된 디바이스에 대한 라우터 홉으로 표시되지 않습니다.

방화벽 모드는 초기 구축 시에만 설정됩니다. 부트스트랩 설정을 다시 적용하는 경우에는 이 설정이 사용되지 않습니다.

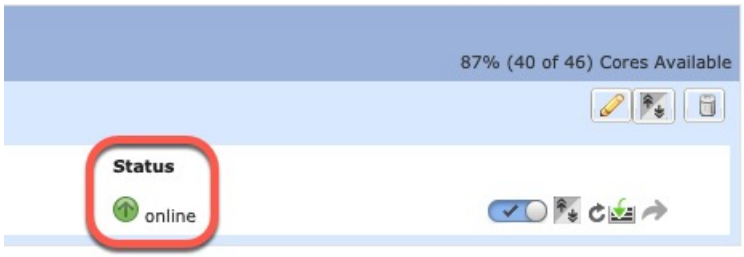
b) 관리자 및 비밀번호 활성화에 대해 **Password(**비밀번호**)**를 입력하고 확인합니다.

비밀번호를 복구할 때는 사전 구성된 ASA 관리자가 있으면 유용합니다. FXOS 액세스 권한이 있다면 관리자 비밀번호를 잊어버린 경우 재설정할 수 있습니다.

단계 **8** **OK(**확인**)**를 클릭하여 구성 대화 상자를 닫습니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 새 논리적 디바이스의 상태를 확인합니다. 논리적 디바이스의 **Status(**상태**)**가 **online(**온라인**)**으로 표시되면 나머지 클러스터 섀시를 추가할 수도 있고, 단일 Firepower 9300 섀시 내의 보안 모듈에 격리된 클러스터의 경우 애플리케이션 내에서 클러스터 구성을 시작할 수도 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 **10** 다중 섀시 클러스터링의 경우, 다음 섀시를 클러스터에 추가합니다.

a) Firewall Chassis Manager의 첫 번째 섀시에서 오른쪽 상단에 있는 **Show Configuration(**구성 표시**)** 아이콘을 클릭하여 표시된 클러스터 구성을 복사합니다.

b) 다음 섀시에 있는 Firewall Chassis Manager에 연결하고 이 절차에 따라 논리적 디바이스를 추가합니다.

c) **I want to:(**수행할 작업**:) > Join an Existing Cluster(**기존 클러스터에 조인**)**를 선택합니다.

d) **OK(**확인**)**를 클릭합니다.

e) **Copy Cluster Details(**클러스터 세부사항 복사**)** 상자에서 첫 번째 섀시의 클러스터 구성에 붙여 넣고 **OK(**확인**)**를 클릭합니다.

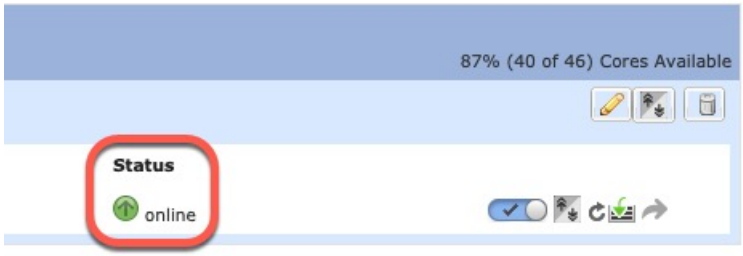
f) 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

- **Chassis ID(**섀시 **ID)** - 고유한 섀시 ID를 입력합니다.
- **Site ID(**사이트 **ID)** - 올바른 사이트 ID를 입력합니다.
- **Cluster Key(**클러스터 키**)** - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.

OK(확인**)**를 클릭합니다.

g) **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status(**상태**)**가 **online(**온라인**)**으로 표시되면 애플리케이션 내에서 클러스터 구성을 시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



단계 **11** 제어 유닛 ASA에 연결하여 클러스터링 컨피그레이션을 맞춤화합니다.

클러스터 멤버 더 추가

ASA 클러스터 멤버를 추가하거나 교체합니다.

참고 이 절차는 섀시 추가 또는 교체 시에만 적용됩니다. 클러스터링이 이미 활성화된 Firepower 9300에 모듈을 추가하거나 교체하는 경우에는 모듈이 자동으로 추가됩니다.

시작하기 전에

- 기존 클러스터에서 이 새 멤버의 관리 IP 주소 풀에 충분한 IP 주소가 있는지 확인하십시오. IP 주소가 충분하지 않은 경우, 이 새 멤버를 추가하기 전에 각 섀시에서 기존 클러스터 부트스트랩 구성을 수정해야 합니다. 이러한 변경으로 인해 논리적 디바이스가 재시작됩니다.

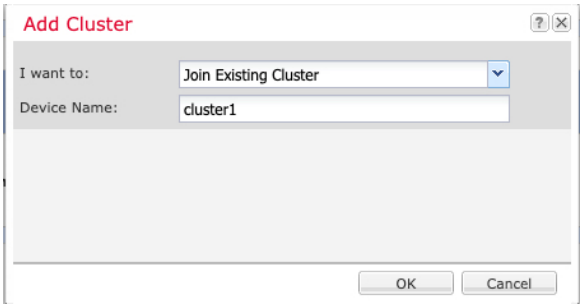
- 인터페이스 구성은 새 섀시에서 동일해야 합니다. FXOS 섀시 구성 내보내기와 가져오기를 통해 이 프로세스를 더 쉽게 수행할 수 있습니다.
- 다중 컨텍스트 모드의 경우 첫 번째 클러스터 멤버의 ASA 애플리케이션에서 다중 컨텍스트 모드를 활성화합니다. 그러면 추가 클러스터 멤버가 다중 컨텍스트 모드 구성을 자동으로 상속합니다.

프로시저

단계 **1** 기존 클러스터 Firewall Chassis Manager에서 **Logical Devices(**논리적 디바이스**)**를 선택하여 **Logical Devices(**논리적 디바이스**)** 페이지를 엽니다.

단계 **2** 오른쪽 상단의 구성 표시 아이콘( )를 클릭하여 표시되는 클러스터 구성을 복사합니다.

단계 **3** 새 섀시에서 Firewall Chassis Manager에 연결한 다음 **Add(**추가**)** > **Cluster(**클러스터**)**를 클릭합니다.



단계 **4** **I want to:(**수행할 작업**:)** > **Join an Existing Cluster(**기존 클러스터에 조인**)**를 선택합니다.

단계 **5** **Device Name(**디바이스 이름**)**에 논리적 디바이스의 이름을 입력합니다.

단계 **6** **OK(**확인**)**를 클릭합니다.

단계 **7** **Copy Cluster Details(**클러스터 세부사항 복사**)** 상자에서 첫 번째 섀시의 클러스터 구성에 붙여 넣고 **OK(**확인**)**를 클릭합니다.

단계 **8** 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보는 대부분 미리 채워지지만 다음 설정은 변경해야 합니다.

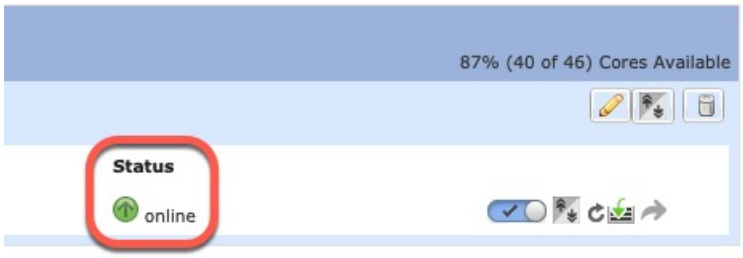
- **Chassis ID(**섀시 **ID)** - 고유한 섀시 ID를 입력합니다.
- **Site ID(**사이트 **ID)** - 올바른 사이트 ID를 입력합니다.
- **Cluster Key(**클러스터 키**)** - (미리 채워지지 않음) 동일한 클러스터 키를 입력합니다.

OK(확인**)**를 클릭합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

섀시에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 구성 및 관리 인터페이스 설정을 애플리케이션 인스턴스에 푸시하여 논리적 디바이스를 구축합니다. **Logical Devices(**논리적 디바이스**)** 페이지에서 각 클러스터 멤버의 새 논리적 디바이스의 상태를 확인합니다. 각 클러스터 멤버의 논리적 디바이스의 **Status(**상태**)**가 **online(**온라인**)**으로 표시되면 애플리케이션 내에서 클러스터 구성을

시작할 수 있습니다. 프로세스의 일부로 "보안 모듈이 응답하지 않음" 상태가 표시될 수 있습니다. 이 상태는 정상이며 일시적입니다.



ASA: 방화벽 모드 및 상황 모드 변경

기본적으로 FXOS 섀시에서는 라우팅 방화벽 모드와 단일 상황 모드에서 클러스터를 구축합니다.

- 방화벽 모드 변경 — 구축한 후에 모드를 변경하려면 제어 유닛에서 모드를 변경합니다. 모드는 일치시킬 모든 데이터 유닛에서 자동으로 변경됩니다.의 내용을 참조하십시오. 다중 상황 모드에서는 상황별로 방화벽 모드를 설정합니다.ASA의 일반적인 작업 구성 가이드를 참조하십시오.
- 여러 상황 모드로 변경 — 구축한 후에 여러 상황 모드로 변경하려면 제어 유닛에서 모드를 변경합니다. 모드는 일치시킬 모든 데이터 유닛에서 자동으로 변경됩니다. ASA의 일반적인 작업 구성 가이드를 참조하십시오.

ASA: 데이터 인터페이스 구성

이 절차에서는 FXOS에서 클러스터를 구축할 때 클러스터에 할당한 각 데이터 인터페이스의 기본 파라미터를 구성합니다. 다중 섀시 클러스터링의 경우, 데이터 인터페이스는 항상 Spanned EtherChannel 인터페이스입니다.

참고 관리 인터페이스는 클러스터를 구축할 때 사전 구성되어 있습니다. ASA에서 관리 인터페이스 파라미터를 변경할 수도 있지만 이 절차에서는 데이터 인터페이스에 중점을 두고 있습니다. 관리 인터페이스는 Spanned 인터페이스와는 달리 개별 인터페이스입니다. 자세한 내용은 관리 인터페이스, 7 페이지를 참조하십시오.

시작하기 전에

- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 시작합니다. 현재 시스템 구성 모드을 입력합니다.
- 투명 모드의 경우 브리지 그룹을 구성합니다.
- 다중 섀시가 있는 클러스터를 위해 Spanned EtherChannel을 사용할 경우, 클러스터링이 완전히 활성화될 때까지 포트 채널 인터페이스가 나타나지 않습니다. 이러한 요구 사항으로 인해 클러스터의 액티브 노드가 아닌 노드에는 트래픽이 전달되지 않습니다.

프로시저

단계 **1** 상황 모드에 따라

- 단일 모드에서는 **Configuration(**구성**) > Device Setup(**디바이스 설정**) > Interface Settings(**인터페이스 설정**) > Interfaces(**인터페이스**)** 창을 선택합니다.
- 다중 모드의 경우 시스템 실행 영역에서 **Configuration(**구성**) > Context Management(**상황 관리**) > Interfaces(**인터페이스**)** 창을 선택합니다.

단계 **2** 인터페이스를 선택하고 **Edit(**수정**)**을 클릭합니다.

Edit Interface(인터페이스 편집**)** 대화 상자가 나타납니다.

단계 **3** 다음을 설정합니다.

- (EtherChannel의 경우) **MIO** 포트 채널 **ID** — FXOS에서 사용된 것과 동일한 ID를 입력합니다.
- **Enable Interface(**인터페이스 활성화**)**(기본적으로 선택되어 있음)

이 화면에 있는 필드의 나머지 부분은 이 절차의 뒷부분에서 설명합니다.

단계 **4** MAC 주소 및 선택적 파라미터를 구성하려면 **Advanced(**고급**)** 탭을 클릭합니다.

- **MAC Address Cloning(MAC** 주소 복제**)** 영역에서 EtherChannel의 수동 전역 MAC 주소를 설정합니다. 스탠바이 MAC 주소는 무시되므로 설정하지 마십시오. 잠재적인 네트워크 연결 문제를 방지하기 위해 Spanned EtherChannel에 대한 MAC 주소를 구성해야 합니다. 수동 구성된 MAC 주소를 사용할 경우, 해당 MAC 주소가 현재 제어 유닛에 유지됩니다. MAC 주소를 구성하지 않은 상태에서 제어 유닛을 변경하는 경우 새 제어 유닛에서는 인터페이스의 새 MAC 주소를 사용하며, 이로 인해 네트워크가 잠시 중단될 수 있습니다.

  다중 상황 모드에서 상황 간에 인터페이스를 공유할 경우, 대신 MAC 주소의 자동 생성을 활성화해야 하며 이렇게 해야 MAC 주소를 수동으로 설정할 필요가 없습니다. 공유되지 않는 인터페이스에 이 명령을 사용하여 MAC 주소를 수동으로 구성해야 합니다.

- **ASA Cluster(ASA** 클러스터**)** 영역에서 사이트 간 클러스터링을 위해 **Site specific MAC Addresses(**사이트별 **MAC** 주소**)**를 설정하고, 라우팅 모드의 경우 **Add(**추가**)**를 클릭하고 사이트 ID(1~8)에 대해 MAC 주소 및 IP 주소를 지정하여 사이트에 대한 IP 주소를 설정합니다. 최대 8개의 사이트에 대해 이 작업을 반복합니다. 사이트별 IP 주소는 전역 IP 주소와 동일한 서브넷에 있

어야 합니다. 유닛에서 사용한 사이트별 MAC 주소 및 IP 주소는 각 유닛의 부트스트랩 구성에서 지정한 사이트 ID에 따라 달라집니다.

단계 **5** (선택 사항) 이 EtherChannel에 VLAN 하위 인터페이스를 구성합니다. 이 절차의 나머지는 하위 인터페이스에 적용됩니다.

단계 **6** (다중 상황 모드) 이 절차를 완료하기 전에 상황에 인터페이스를 할당해야 합니다.

a) 변경 사항을 적용하려면 **OK(**확인**)**를 클릭합니다.

b) 인터페이스를 할당합니다.

c) 구성할 상황을 변경하려면 **Device List(**디바이스 목록**)** 창의 액티브 디바이스 IP 주소 아래에서 상황 이름을 두 번 클릭합니다.

d) **Configuration(**구성**) > Device Setup(**디바이스 설정**) > Interfaces(**인터페이스**)** 창을 선택하고 사용자 지정하려는 포트 채널 인터페이스를 선택한 다음 **Edit(**편집**)**를 클릭합니다.

Edit Interface(인터페이스 편집**)** 대화 상자가 나타납니다.

단계 **7** **General(**일반**)** 탭을 클릭합니다.

단계 **8** (투명 모드) **Bridge Group(**브리지 그룹**)** 드롭다운 목록에서 이 인터페이스를 할당할 브릿지 그룹을 선택합니다.

단계 **9** **Interface Name(**인터페이스 이름**)** 필드에 최대 48자의 이름을 입력합니다.

단계 **10** **Security level(**보안 수준**)** 필드에 0(가장 낮음)~100(가장 높음) 범위의 레벨을 입력합니다.

단계 **11** (투명 모드) IPv4 주소의 경우 **Use Static IP(**고정 **IP** 사용**)** 라디오 버튼을 클릭하고 IP 주소 및 마스크를 입력합니다. DHCP 및 PPPoE는 지원되지 않습니다. 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. 투명 모드의 경우, EtherChannel 인터페이스가 아닌 브리지 그룹 인터페이스의 IP 주소를 구성해야 합니다.

단계 **12** (라우팅 모드) IPv6 주소를 구성하려면 **IPv6** 탭을 클릭합니다.

투명 모드의 경우, EtherChannel 인터페이스가 아닌 브리지 그룹 인터페이스의 IP 주소를 구성해야 합니다.

a) **Enable IPv6(IPv6** 활성화**)** 확인란을 선택합니다.

b) **Interface IPv6 Addresses(**인터페이스 **IPv6** 주소**)** 영역에서 **Add(**추가**)**를 클릭합니다.

Add IPv6 Address for Interface(인터페이스에 대한 **IPv6** 주소 추가**)** 대화 상자가 나타납니다.

참고
Enable address autoconfiguration(주소 자동 구성 활성화**)** 옵션은 지원되지 않습니다. 링크-로컬 주소의 수동 구성도 지원되지 않습니다.

c) **Address/Prefix Length(**주소/프리픽스 길이**)** 필드에 전역 IPv6 주소 및 IPv6 접두사 길이를 입력합니다. 예를 들어, 2001:DB8::BA98:0:3210/64와 같이 입력합니다.

d) (선택 사항) Modified EUI-64 인터페이스 ID를 호스트 주소로 사용하려면 **EUI-64** 확인란을 선택합니다. 이 경우 **Address/Prefix Length(**주소/프리픽스 길이**)** 필드에 접두사만 입력합니다.

e) **OK(**확인**)**를 클릭합니다.

단계 **13** **OK(**확인**)**를 클릭하여 **Interfaces(**인터페이스**)** 화면으로 돌아갑니다.

단계 **14** **Apply(**적용**)**를 클릭합니다.

ASA: 클러스터 구성 맞춤화

클러스터를 구축한 후에 부트스트랩 설정을 변경하거나 추가 옵션을 구성하려는 경우(예: 클러스터링 상태 모니터링, TCP 연결 복제 지연, 플로우 모빌리티 및 기타 최적화), 제어 유닛에서 해당 작업을 수행할 수 있습니다.

기본 ASA 클러스터 파라미터 구성

제어 노드에서 클러스터 설정을 맞춤화할 수 있습니다.

시작하기 전에

- 다중 상황 모드에서는 제어 유닛의 시스템 실행 영역에서 이 절차를 완료합니다. 현재 시스템 구성 모드가 아닌 경우 **Configuration(**구성**)** > **Device List(**디바이스 목록**)** 창의 활성 디바이스 IP 주소 아래에서 **System(**시스템**)** 을 두 번 클릭합니다.
- 로컬 유닛의 **Member Name(**멤버 이름**)** 및 기타 여러 옵션은 FXOS 섀시에서만 설정될 수 있습니다. 또는 이러한 옵션은 클러스터링을 비활성화하는 경우, ASA에서만 변경될 수 있습니다. 따라서 다음 절차에는 포함되지 않습니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)**를 선택합니다.

단계 **2** (선택 사항) 다음 파라미터(선택 사항)를 구성합니다.

- **Cluster Member Limit(**클러스터 멤버 제한**)**— 클러스터 멤버의 최대 수를 2~16 사이로 구성합니다. 기본값은 16입니다. 클러스터 유닛 수가 최대 16개 유닛보다 작을 경우 실제 계획된 유닛 수를 설정하는 것이 좋습니다. 최대 유닛을 설정하면 클러스터가 리소스를 더 잘 관리할 수 있습니다. 예를 들어, 포트 주소 변환(PAT)을 사용하는 경우, 제어 유닛은 계획된 구성원 수에 맞춰 포트 블록을 할당할 수 있으며, 사용하지 않을 추가 유닛을 위해 포트를 미리 확보해 둘 필요가 없습니다.
- **Site Periodic GARP(**사이트 주기 **GARP)** — ASA는 전환 대상 인프라를 최신 상태로 유지하기 위해 Gratuitous ARP(GARP) 패킷을 생성합니다. 각 사이트에서 가장 높은 우선 순위를 지닌 멤버는 전역 MAC/IP 주소에 대해 GARP 트래픽을 주기적으로 생성합니다. GARP는 각 Spanned EtherChannel에 대한 각 유닛 및 사이트 MAC 및 IP 주소용 사이트 ID를 설정할 때 기본적으로 활성화되어 있습니다. 1~1000000초 사이로 GARP 간격을 설정합니다. 기본값은 290초입니다.

  사이트별 MAC 및 IP 주소를 사용할 때 클러스터에서 온 패킷은 사이트별 MAC 주소 및 IP 주소를 사용하는 반면 클러스터가 수신한 패킷은 전역 MAC 주소 및 IP 주소를 사용합니다. 트래픽이 전역 MAC 주소에서 정기적으로 생성되지 않는 경우, 전역 MAC 주소에 대한 스위치에서 MAC

주소 시간 초과가 발생할 수 있습니다. 시간 초과 후에 전역 MAC 주소로 향하는 트래픽이 전체 스위칭 인프라를 통해 플러딩되어 성능 및 보안 문제를 유발할 수 있습니다.

- **Enable connection rebalancing for TCP traffic across all the ASAs in the cluster(**클러스터의 모든 **ASA**에서 **TCP** 트래픽의 연결 리밸런싱 활성화**)** — 연결 리밸런싱을 활성화합니다. 이 매개변수는 기본적으로 비활성화되어 있습니다. 이 매개변수는 부트스트랩 구성의 일부가 아니며, 제어 노드에서 데이터 노드로 복제됩니다. 활성화할 경우 ASA는 초당 연결 수에 대한 정보를 주기적으로 교환하며, 초당 연결 수가 많은 디바이스에서 로드가 적은 디바이스로 새 연결을 오프로드합니다. 기존 연결은 이동되지 않습니다. 또한 이 명령은 초당 연결 수를 기반으로만 리밸런싱되므로 각 노드에 설정된 총 연결 수는 고려되지 않으며 총 연결 수가 동일하지 않을 수 있습니다. 빈도는 1에서 360초 사이이며, 로드 정보를 교환하는 빈도를 지정합니다. 기본값은 5일입니다.

  연결이 다른 노드로 오프로드되면 비대칭 연결이 됩니다.

  사이트 간 토폴로지에 대한 연결 리밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 대한 새 연결이 리밸런싱됩니다.

- **Enable cluster load monitor(**클러스터 로드 모니터 활성화**)** - 총 연결 수, CPU 및 메모리 사용량, 버퍼 삭제를 포함하여 클러스터 멤버에 대한 트래픽 로드를 모니터링할 수 있습니다. 로드가 너무 높은 경우 나머지 유닛이 로드를 처리할 수 있는 경우 유닛에서 클러스터링을 수동으로 비활성화하도록 선택하거나 외부 스위치의 로드 밸런싱을 조정할 수 있습니다. 이 기능은 기본적으로 활성화되어 있습니다. 예를 들어, 각 섀시에 보안 모듈 3개가 장착된 Firepower 9300에서 섀시 간 클러스터링을 구성한 경우, 한 섀시의 보안 모듈 2개가 클러스터에서 이탈하면 해당 섀시로 유입되는 트래픽이 남은 모듈 하나로 집중되어 해당 모듈에 과부하가 걸릴 수 있습니다. 트래픽 로드를 주기적으로 모니터링할 수 있습니다. 로드가 너무 높은 경우 유닛에서 수동으로 클러스터링을 비활성화하도록 선택할 수 있습니다.

  다음 값을 설정합니다.

  - **Time Interval(**시간 간격**)** - 모니터링 메시지 간의 시간(초)을 10~360초 사이로 설정합니다. 기본값은 20초입니다.
  - **Number of Intervals(**간격 수**)** - ASA가 데이터를 유지 관리하는 간격 수를 1~60 사이의 값으로 설정합니다. 기본값은 30입니다.

  트래픽 로드를 확인하려면 **Monitoring(**모니터링**)** > **ASA Clusters(ASA** 클러스터**)** > **Cluster Load-Monitoring(**클러스터 로드 모니터링**)**을 참조하십시오.

- **Enable health monitoring of this device within the cluster(**클러스터 내에서 이 디바이스의 상태 모니터링 활성화**)** — 클러스터 유닛 상태 검사 기능을 활성화하고 유닛 간의 하트비트 상태 메시지 시간 간격을 0.3초 및 45초 사이에서 결정합니다. 기본값은 3초입니다. 참고: 새 유닛을 클러스터에 추가하는 경우와 ASA 또는 스위치에서 토폴로지를 변경하는 경우, 클러스터가 완료될 때까지 이 기능을 일시적으로 비활성화하고 비활성화된 인터페이스에 대해 인터페이스 모니터링을 비활성화해야 합니다(**Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Interface Health Monitoring(**클러스터 인터페이스 상태 모니터링**)**). 클러스터 및 토폴로지 변경이 완료되면 이러한 기능을 다시 활성화할 수 있습니다. 유닛 상태를 확인하기 위해 ASA 클러스터 유닛에서는 다른 유닛에 대한 클러스터 제어 링크에서 하트비트 메시지를 보냅니다. 유닛이 피어 유닛

의 하트비트 메시지를 대기 시간 내에 수신하지 않을 경우, 해당 피어 유닛은 응답하지 않거나 중지된 상태로 간주됩니다.

- **Debounce Time(**디바운스 시간**)** — ASA에서 인터페이스를 실패 상태로 간주하고 유닛이 클러스터에서 제거되기 전에 디바운스 시간을 구성합니다. 이 기능을 통해 인터페이스 장애 탐지를 더 빠르게 수행할 수 있습니다. 디바운스 시간을 더 낮게 구성하면 오탐의 가능성이 증가합니다. 인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA는 지정되어 있는 밀리초 동안 대기합니다. 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 유닛이 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 유닛에서 실패한 것으로 표시되는 것을 방지할 수 있습니다. 기본 디바운스 시간은 500ms이며 범위는 300ms~9초입니다.

- **Replicate console output(**콘솔 출력 복제**)** — 데이터 유닛에서 제어 유닛으로 콘솔 복제를 활성화합니다. 이 기능은 기본적으로 비활성화되어 있습니다. ASA에서는 중요한 특정 이벤트 발생 시 일부 메시지를 콘솔에 직접 출력합니다. 콘솔 복제를 활성화할 경우, 데이터 유닛에서는 콘솔 메시지를 제어 유닛에 전송하므로 클러스터의 콘솔 포트 하나만 모니터링하면 됩니다. 이 매개변수는 부트스트랩 컨피그레이션의 일부가 아니며, 제어 유닛에서 데이터 유닛으로 복제됩니다.

- **Enable Clustering Flow Mobility(**클러스터링 플로우 모빌리티 활성화**)**입니다. LISP 검사 구성, 42 페이지을 참조하십시오.

- **Enable Director Localization for inter-DC cluster(DC** 간 클러스터를 위해 관리자 현지화 활성화**)** — 데이터 센터에 대한 사이트 간 클러스터링을 위해 성능을 개선하고 왕복 시간 레이턴시를 줄이기 위해 관리자 현지화를 활성화할 수 있습니다. 새로운 연결은 일반적으로 로드 밸런싱 상태이며 지정된 사이트 내부의 클러스터 멤버가 소유합니다. 그러나 ASA는 모든 사이트에서 멤버에 관리자 역할을 할당합니다. 관리자 현지화를 사용하면 추가 관리자 역할이 활성화됩니다. 즉, 소유자와 동일한 사이트의 로컬 관리자와 모든 사이트의 전역 관리자 역할이 활성화됩니다. 소유자와 관리자를 동일한 사이트에서 유지하면 성능이 향상됩니다. 또한 원래 소유자가 실패할 경우, 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다. 전역 관리자는 클러스터 멤버가 다른 사이트에서 소유하는 연결에 대한 패킷을 수신하는 경우 사용됩니다.

- **Site Redundancy(**사이트 이중화**)** — 사이트 장애로부터 플로우를 보호하기 위해 사이트 이중화를 활성화할 수 있습니다. 연결 백업 소유자가 소유자와 같은 사이트에 있으면 사이트 장애로부터 플로우를 보호하기 위해 다른 사이트에서 추가 백업 소유자가 선택됩니다. 관리자 현지화 및 사이트 이중화는 별도의 기능입니다. 이 기능 중 하나 또는 나머지를 구성하거나 둘 다 구성할 수도 있습니다.

- **Enable config sync Acceleration(**설정 동기화 가속 활성화**)** - 데이터 유닛에 제어 유닛과 설정이 동일한 경우 동기화 설정을 건너뛰고 더 빠르게 참여합니다. 이 기능은 기본적으로 활성화되어 있습니다. 이 기능은 각 유닛에서 구성되며 제어 유닛에서 데이터 유닛으로 복제되지 않습니다.

  참고
  일부 구성 명령은 가속화된 클러스터 참가와 호환되지 않습니다. 이러한 명령이 유닛에 존재하는 경우, 가속화된 클러스터 참가가 활성화된 경우에도 구성 동기화가 항상 발생합니다. 가속화된 클러스터 참가가 작동하려면 호환되지 않는 구성을 제거해야 합니다. 호환되지 않는 구성을 보려면 **show cluster info unit-join-acceleration incompatible-config**를 사용합니다.

- **Enable parallel configuration replicate(**병렬 구성 복제 활성화**)** - 제어 유닛을 활성화하여 데이터 유닛과 구성 변경 사항을 병렬로 동기화합니다. 그렇지 않으면 동기화가 순차적으로 이루어지며 시간이 더 걸릴 수 있습니다.
- **Concurrent Join(**동시 조인**)**— 노드가 순차적으로 조인하는 대신 동시에 조인할 수 있습니다. NAT 및 VPN 분산 모드가 활성화된 경우 동시 조인을 사용할 수 없습니다. 호환되지 않는 구성을 보려면 **Monitoring(**모니터링**)** > **ASA Cluster(ASA** 클러스터**)** > **ASA Cluster Concurrent Join(ASA** 클러스터 동시 조인**)**을 참조하십시오.
- 플로우 상태 새로 고침 **Keepalive** 간격 - 플로우 소유자에서 관리자 및 백업 소유자로의 흐름 상태 새로 고침 메시지(clu_keepalive 및 clu_update 메시지)에 대한 keepalive 간격을 15~20초 사이로 설정합니다. 기본값은 15입니다. 클러스터 제어 링크의 트래픽 양을 줄이기 위해 간격을 기본값보다 길게 설정할 수 있습니다.
- **CPU Health Check Threshold(CPU** 상태 확인 임계값**)**- 클러스터 제어 링크에서 상태 검사를 일시 중단하도록 CPU 사용량 임계값을 구성합니다. 백분율을 70~100 사이로 설정합니다. 기본값은 90입니다. 클러스터 노드 CPU 사용량이 높으면 상태 확인이 일시 중단되고 노드가 비정상으로 표시되지 않습니다.

단계 **3** **Cluster Control Link(**클러스터 제어 링크**)** 영역에서 클러스터 제어 링크 MTU를 구성할 수 있습니다. 이 영역의 다른 옵션은 ASA에서 구성할 수 없습니다.

- **MTU** - 클러스터 제어 링크 인터페이스의 최대 전송 단위가 데이터 인터페이스의 가장 높은 MTU보다 100바이트 이상 높도록 지정합니다. MTU를 최댓값인 9184바이트로 설정하는 것이 좋습니다. 최솟값은 1400바이트입니다. 또한 Cisco에서는 클러스터 제어 링크 MTU를 2561과 8362 사이로 설정하지 않는 것을 권장합니다. 블록 풀 처리로 인해 이 MTU 크기는 시스템 작동에 최적이 아닙니다. 클러스터 제어 링크 트래픽에는 데이터 패킷 전달이 포함되므로 클러스터 제어 링크는 데이터 패킷의 전체 크기와 클러스터 트래픽 오버헤드를 모두 수용해야 합니다.

  예를 들어 최대 MTU가 9184이므로 가장 높은 데이터 인터페이스 MTU는 9084가 될 수 있는 반면, 클러스터 제어 링크는 9184로 설정할 수 있습니다.

단계 **4** (선택 사항) (Firepower 9300만 해당) **VPN** 그룹화 모드. 분산 Site-to-Site VPN 구성, 44 페이지을 참조하십시오.

단계 **5** (선택 사항) (Firepower 9300만 해당) **Parallel Join of Units Per Chassis(**섀시당 유닛의 병렬 참가**)** 영역에서 트래픽이 모듈 간에 고르게 분산되도록 섀시에서 보안 모듈이 클러스터에 동시에 참가하는지 확인할 수 있습니다. 모듈이 다른 모듈보다 훨씬 먼저 참가하는 경우, 다른 모듈이 로드를 아직 공유할 수 없기 때문에 이 모듈은 원하는 트래픽보다 더 많은 트래픽을 받을 수 있습니다.

- **Minimum Units Required to Join(**참가하는 데 필요한 최소 유닛 수**)** — 모듈이 클러스터에 참가하기 전에 준비해야 하는 동일한 섀시의 최소 모듈 수를 1~3 범위에서 지정합니다. 기본값은 1인데 이는 모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하지 않는 것을 의미합니다. 예를 들어, 값을 3으로 설정하는 경우, 각 모듈이 클러스터에 참가하기 전에 최대 지연 시간 동안 대기하거나 3개의 모듈이 모두 준비 상태가 될 때까지 대기합니다. 3개 모듈 모두 클러스터에 거의 동시에 참가하도록 요청하며 동일한 시간대에 트래픽을 수신하기 시작합니다.
- **Maximum Join Delay(**최대 참가 지연**)** — 모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하는 것을 중지하기 전의 최대 지연 시간(분)을 0~30분 범위에서 지정합니다. 기본값은

0인데 이는 모듈이 클러스터에 참가하기 전에 다른 모듈이 준비할 동안 대기하지 않는 것을 의미합니다. 최소 유닛 수를 1로 설정하는 경우 이 값은 0이어야 합니다. 최소 유닛 수를 2 또는 3으로 설정하는 경우 이 값은 1 이상이어야 합니다. 이 타이머는 모듈별로 할당되지만 첫 번째 모듈이 클러스터에 참가하면 모든 다른 모듈 타이머가 종료되고 나머지 모듈은 클러스터에 참가합니다.

예를 들어, 최소 유닛 수를 3으로 설정하고 최대 지연을 5분으로 설정합니다. 모듈 1이 나타나면 5분 타이머가 시작됩니다. 2분 후에 모듈 2가 나타나고 5분 타이머가 시작됩니다. 1분 후에 모듈 3이 나타나므로 4분으로 표시될 때는 이제 모든 모듈이 클러스터에 참가하게 되며, 모든 모듈은 타이머가 완료될 때까지 대기하지 않습니다. 모듈 3이 나타나지 않으면 모듈 1이 5분 타이머 종료 시 클러스터에 참가하게 되고, 모듈 2 또한 참가하게 되는데(타이머에 아직 2분이 남아 있는 경우에도) 이는 타이머가 완료할 때까지 대기하지 않습니다.

단계 **6** **Apply(**적용**)**를 클릭합니다.

인터페이스 상태 모니터링 및 자동 재참가 설정 구성

필수가 아닌 인터페이스(예: 관리 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다. 모든 포트 채널 ID 또는 단일 물리적 인터페이스 ID를 모니터링할 수 있습니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Interface Health Monitoring(**클러스터 인터페이스 상태 모니터링**)**을 선택합니다.

단계 **2** **Monitored Interfaces(**모니터링되는 인터페이스**)** 상자에서 인터페이스를 선택하고 **Add(**추가**)**를 클릭하여 **Unmonitored Interfaces(**모니터링되지 않는 인터페이스**)** 상자로 이동합니다.

인터페이스 상태 메시지에 링크 장애가 감지됩니다. 지정된 논리적 인터페이스에 대한 모든 물리적 포트가 특정 유닛에서 오류가 발생했지만 다른 유닛에 있는 동일한 논리적 인터페이스에서 활성 포트가 있는 경우 이 유닛은 클러스터에서 제거됩니다. 유닛에서 대기 시간 내에 인터페이스 상태 메시지를 수신하지 않을 경우, ASA에서 클러스터의 멤버를 제거하기까지 걸리는 시간은 인터페이스의 유형에 따라, 그리고 해당 유닛이 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 좌우됩니다. 상태 선택은 모든 인터페이스에 대해 기본적으로 활성화됩니다.

필수가 아닌 인터페이스(예: 관리 인터페이스)에 대한 상태 모니터링을 비활성화할 수 있습니다. 모든 포트 채널 ID 또는 단일 물리적 인터페이스 ID를 지정할 수 있습니다. 상태 모니터링은 VNI 또는 BVI 같은 VLAN 하위 인터페이스 또는 가상 인터페이스에서 수행되지 않습니다. 클러스터 제어 링크의 모니터링을 구성할 수 없습니다. 이 링크는 항상 모니터링됩니다.

토폴로지 변경 사항(예: 데이터 인터페이스 추가 또는 제거, ASA, Firepower 4100/9300 섀시 또는 스위치에서 인터페이스 활성화 또는 비활성화, 추가 스위치를 추가하여 VSS, vPC, StackWise 또는 StackWise Virtual 구성)이 발생할 경우 상태 검사 기능(**Configuration(**구성**)** > **Device Management(**디

바이스 관리) > High Availability and Scalability(고가용성 및 확장성) > ASA Cluster(ASA 클러스터))을 비활성화하고 비활성화된 인터페이스에 대한 인터페이스 모니터링도 비활성화해야 합니다. 토폴로지 변경이 완료되고 컨피그레이션 변경 사항이 모든 유닛과 동기화되면 상태 검사 기능을 다시 사용할 수 있습니다.

단계 3 인터페이스, 시스템 또는 클러스터 제어 링크에 장애가 발생할 경우, **Auto Rejoin(**자동 다시 참가**)** 탭을 클릭하여 자동 다시 참가 설정을 맞춤화합니다. 각 유형에 대해 **Edit(**편집**)**을 클릭하여 다음을 설정합니다.

- **Maximum Rejoin Attempts(**최대 다시 참가 시도 횟수**)** — **unlimited(**무제한**)** 또는 0~65535 사이의 값을 설정하여 클러스터에 다시 참가하려고 시도하는 횟수를 정의합니다. **0**은 자동 다시 참가를 비활성화합니다. 기본값은 클러스터 인터페이스의 경우 **Unlimited(**무제한**)**이며 데이터 인터페이스 및 시스템의 경우 **3**입니다.
- **Rejoin Interval(**다시 참가 간격**)** — 2~60 사이의 간격을 설정하여 다시 참가 시도 간의 간격 기간(분)을 정의합니다. 기본값은 **5**분입니다. 유닛이 클러스터에 다시 참가하려고 시도하는 최대 총 시간은 마지막 장애 시간으로부터 14400분(10일)으로 제한됩니다.
- **Interval Variation(**간격 변수**)** — 1과 3 사이의 간격 변수 설정에 따라 간격 기간이 증가하는지 여부를 정의합니다. **1**(변경 없음), **2**(2 x 이전 간격) 또는 **3**(3 x 이전 간격)입니다. 예를 들어, 간격 기간을 5분으로 설정하고 변수를 2로 설정하면 첫 번째 시도가 5분 후에 일어나고 두 번째 시도는 10분(2 x 5), 세 번째 시도는 20분(2 x 10) 후에 일어납니다. 기본값은 클러스터 인터페이스의 경우 **1**이며 데이터 인터페이스 및 시스템의 경우 **2**입니다.

기본 설정을 복원하려면 **Restore Defaults(**기본값 복원**)**를 클릭합니다.

섀시 하트비트 장애에 대한 **Auto Rejoin(**자동 다시 조인**)** 설정과 일치하도록 섀시 다시 조인을 설정하려면 **Chassis Heartbeat Delay Auto-Rejoin(**섀시 하트비트 지연 자동 다시 조인**)**을 선택합니다. 기본적으로 섀시 하트비트에 장애가 발생한 다음 복구되면 노드 클러스터에 즉시 다시 조인합니다. 그러나 이 옵션을 구성하면 **Auto Rejoin(**자동 다시 조인**)** 화면의 설정에 따라 다시 조인하게 됩니다.

단계 4 **Apply(**적용**)**를 클릭합니다.

클러스터 TCP 복제 지연 구성

관리자/백업 플로우 생성을 지연시켜 짧은 수명의 플로우와 관련된 "불필요한 작업"을 제거하는 데 도움을 주기 위해 TCP 연결에 대해 클러스터 복제 지연을 활성화합니다. 관리자/백업 플로우가 생성되기 전에 유닛에서 오류가 발생하는 경우, 이러한 플로우는 복구될 수 없습니다. 마찬가지로 플로우가 생성되기 전에 트래픽이 다른 유닛으로 리밸런싱되며 플로우는 복구될 수 없습니다. TCP 임의화를 비활성화하도록 설정한 트래픽에 대해 TCP 복제 지연을 활성화하지 않아야 합니다.

프로시저

단계 1 **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster Replication(ASA** 클러스터 복제**)**을 선택합니다.

단계 2 **Add(**추가**)**를 클릭하고 다음 값을 설정합니다.

- **Replication delay(**복제 지연**)** — 1~15 사이의 초를 설정합니다.
- **HTTP** — 모든 HTTP 트래픽에 대해 지연을 설정합니다. 이 설정은 기본적으로 5초 동안 활성화됩니다.
- 소스 기준
  - **Source(**소스**)** — 소스 IP 주소를 설정합니다.
  - Service(서비스) — (선택 사항) 소스 포트를 설정합니다. 일반적으로 소스 또는 대상 포트 중 하나를 설정합니다. 둘 다 설정하지는 마십시오.
- 대상 기준
  - **Source(**소스**)** — 대상 IP 주소를 설정합니다.
  - **Service(**서비스**)** — (선택 사항) 대상 포트를 설정합니다. 일반적으로 소스 또는 대상 포트 중 하나를 설정합니다. 둘 다 설정하지는 마십시오.

단계 **3** **OK(**확인**)**를 클릭합니다.

단계 **4** **Apply(**적용**)**를 클릭합니다.

사이트 간 기능 구성

사이트 간 클러스터링의 경우, 구성을 맞춤화하여 이중화 및 안정성을 개선할 수 있습니다.

클러스터 플로우 모빌리티 구성

서버가 사이트 간에 이동하는 경우 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

LISP 검사 정보

사이트 간에 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

LISP 정보

VMware VMotion과 같은 데이터 센터 가상 머신 모빌리티를 통해 서버는 클라이언트에 대한 연결을 유지하면서 데이터 센터 간에 데이터를 마이그레이션할 수 있습니다. 그러한 데이터 센터 서버 모빌리티를 지원하려면 라우터는 이동 시 서버에 대한 인그레스 경로를 업데이트할 수 있어야 합니다. Cisco LISP(Locator/ID Separation Protocol) 아키텍처는 디바이스 ID 또는 EDI(endpoint identifier)를 해당 위치 또는 RLOC(routing locator)에서 두 개의 서로 다른 숫자 공간으로 분리하여, 서버 마이그레이션을 클라이언트에 투명하게 만듭니다. 예를 들어 서버가 새 사이트로 이동하고 클라이언트가 서버로 트래픽을 전송하면, 라우터가 트래픽을 새 위치로 리디렉션합니다.

LISP에는 LISP ETR(egress tunnel router), ITR(ingress tunnel router), FHR(first hop router), MR(map resolver), MS(map server) 같은 특정 역할의 라우터 및 서버가 필요합니다. 서버에 대한 FHR(first hop router)은 서버가 다른 라우터에 연결된 것을 감지하면, 클라이언트에 연결된 ITR이 트래픽을 가로채고 캡슐화하여 새로운 서버 위치로 전송할 수 있도록 다른 모든 라우터 및 데이터베이스를 업데이트합니다.

Secure Firewall ASA LISP 지원

ASAASAASA는 LISP 자체를 실행하지 않습니다. 그러나 위치 변경을 위해 LISP 트래픽을 검사한 다음 원활한 클러스터링 작동을 위해 이 정보를 사용할 수 있습니다. LISP 통합이 없으면 서버가 새 사이트로 이전할 경우, 원래의 플로우 소유자 대신 새 사이트의 ASA 클러스터 멤버로 트래픽이 전달됩니다. 새 ASA가 트래픽을 이전 사이트의 ASA로 전달하면, 이전 ASA는 서버에 도달하기 위해 트래픽을 다시 새 사이트로 전송합니다. 이 트래픽 플로우는 차선책이며, "tromboning" 또는 hair-pinning"으로 알려져 있습니다.

LISP 통합 시 ASA 클러스터 멤버는 FHR(first hop router)과 ETR 또는 ITR 간에 전달되는 LISP 트래픽을 검사할 수 있으며, 그런 다음 플로우 소유자가 새 사이트에 있도록 변경할 수 있습니다.

LISP 지침

- ASA 클러스터 멤버는 FHR과 사이트의 ITR 또는 ETR 사이에 상주해야 합니다. ASA 클러스터 자체는 확장 세그먼트의 FHR이 될 수 없습니다.
- 완전히 분산된 플로우만 지원됩니다. 중앙 집중식 플로우, 반 분산 플로우 또는 개별 노드에 속한 플로우는 새 소유자로 이동하지 않습니다. 반 분산 플로우에는, 상위 플로우를 소유하는 동일한 ASA가 모든 하위 플로우도 소유하는 SIP 같은 애플리케이션이 포함됩니다.
- 클러스터는 계층 3 및 4 플로우 상태만 이동하므로, 일부 애플리케이션 데이터가 손실될 수 있습니다.
- 수명이 짧은 플로우 또는 비즈니스 크리티컬 플로우의 경우 소유자를 이동하는 것이 의미가 없을 수 있습니다. 검사 정책을 구성할 때 이 기능으로 지원되는 트래픽의 유형을 제어할 수 있으며, 플로우 모빌리티를 필수 트래픽으로 제한해야 합니다.

ASA LISP 구현

이 기능에는 몇 가지 상호 연결된 구성이 포함됩니다(모두 이 장에서 설명).

1. (선택 사항) Limit inspected EIDs based on the host or server IP address(호스트 또는 서버 IP 주소를 기반으로 검사된 EID 제한) - FHR(first hop router)은 ASA 클러스터와 관련되지 않은 호스트 또는 네트워크에 대한 EID-notify 메시지를 전송할 수 있습니다. 그러면 사용자는 클러스터와 관련된 서버 또는 네트워크로만 EDI를 제한할 수 있습니다. 예를 들어 클러스터와 관련된 사이트가 2개뿐이지만 LISP가 3개 사이트에서 실행 중인 경우, 클러스터와 관련된 2개 사이트에 대한 EID만 포함해야 합니다.
2. LISP traffic inspection(LISP 트래픽 검사) - ASA는 FHR(first hop router)과 ITR 또는 ETR 간에 EID-notify 메시지를 보낼 수 있도록 UDP 포트 4342에서 LISP 트래픽을 검사합니다. ASA는 EID 및 사이트 ID를 상호 연결하는 EID 테이블을 유지 보수합니다. 예를 들면, FHR(first hop router)의 소스 IP 주소 및 ITR 또는 ETR의 목적지 주소로 LISP 트래픽을 검사해야 합니다. LISP 트래픽에는 관리자가 할당되지 않으며, LISP 트래픽 자체는 클러스터 상태 공유에 참여하지 않습니다.
3. Service Policy to enable flow mobility on specified traffic(지정된 트래픽에서 플로우 모빌리티 활성화를 위한 서비스 정책) - 비즈니스 크리티컬 트래픽에서 플로우 모빌리티를 활성화해야 합니다. 예를 들어 플로우 모빌리티를 HTTPS 트래픽 또는 특정 서버에 대한 트래픽으로 제한할 수 있습니다.

4. Site IDs(사이트 ID) - ASA는 각 클러스터 노드에 대해 사이트 ID를 사용하여 새로운 소유자를 확인합니다.
5. Cluster-level configuration to enable flow mobility(플로우 모빌리티 활성화를 위한 클러스터 레벨 구성) - 또한 클러스터 레벨에서 플로우 모빌리티를 활성화해야 합니다. 이 켜기/끄기 토글을 사용하면 특정 클래스의 트래픽 또는 애플리케이션에 대한 플로우 모빌리티를 손쉽게 활성화 또는 비활성화할 수 있습니다.

LISP 검사 구성

서버가 사이트 간에 이동하는 경우 플로우 모빌리티를 활성화하기 위해 LISP 트래픽을 검사할 수 있습니다.

시작하기 전에

- Firepower 4100/9300 섀시 관리자(Supervisor)에서 섀시의 사이트 ID를 설정합니다.
- LISP 트래픽은 기본 검사 트래픽 클래스에 포함되지 않으므로 이 절차를 수행하는 중에 LISP 트래픽에 대해 별도의 클래스를 구성해야 합니다.

프로시저

단계 **1** (선택 사항) IP 주소를 기반으로 하는 검사된 EID로 제한하고 LISP 사전 공유 키를 구성하려면 다음과 같이 LISP 검사 맵을 구성합니다.

a) **Configuration(**구성**)** > **Firewall(**방화벽**)** > **Objects(**개체**)** > **Inspect Maps(**검사 맵**)** > **LISP**를 선택합니다.
b) 새 맵을 추가하려면 **Add(**추가**)**를 클릭합니다.
c) 이름(최대 40자) 및 설명을 입력합니다.
d) **Allowed-EID access-list(**허용된 **EID** 액세스 목록**)**에 대해 **Manage(**관리**)**를 클릭합니다.

ACL Manager가 열립니다.

FHR(first hop router) 또는 ITR/ETR은 ASA 클러스터와 관련되지 않은 호스트 또는 네트워크에 대한 EID-notify 메시지를 전송할 수 있습니다. 그러면 사용자는 클러스터와 관련된 서버 또는 네트워크로만 EID를 제한할 수 있습니다. 예를 들어 클러스터와 관련된 사이트가 2개뿐이지만 LISP가 3개 사이트에서 실행 중인 경우, 클러스터와 관련된 2개 사이트에 대한 EID만 포함해야 합니다.

e) 방화벽 구성 가이드에 따라 ACE가 하나 이상 있는 ACL을 추가합니다.
f) 필요한 경우, **Validation Key(**검증 키**)**를 입력합니다.

암호화 키를 복사한 경우 **Encrypted(**암호화됨**)** 라디오 버튼을 클릭합니다.

g) **OK(**확인**)**를 클릭합니다.

단계 **2** LISP 검사를 구성하려면 서비스 정책 규칙을 추가합니다.

a) **Configuration(**구성**)** > **Firewall(**방화벽**)** > **Service Policy Rules(**서비스 정책 규칙**)**를 선택합니다.
b) **Add(**추가**)**를 클릭합니다.
c) **Service Policy(**서비스 정책**)** 페이지에서 규칙을 인터페이스에 또는 전역으로 적용합니다.

   기존 서비스 정책을 사용하려는 경우, 해당 정책에 규칙을 추가합니다. 기본적으로 ASA에는 **global_policy**라고 하는 전역 정책이 포함되어 있습니다. 정책을 전역으로 적용하지 않으려는 경우 인터페이스별로 하나의 서비스 정책을 생성할 수도 있습니다. LISP 검사는 트래픽에 양방향으로 적용되므로 소스 및 대상 인터페이스 모두에서 서비스 정책을 적용할 필요가 없습니다. 트래픽이 양쪽 방향의 클래스와 일치할 경우 규칙을 적용하는 인터페이스로 들어가거나 나가는 모든 트래픽이 영향을 받습니다.

d) **Traffic Classification Criteria(**트래픽 분류 기준**)** 페이지에서 **Create a new traffic class(**새 트래픽 클래스 생성**)**를 클릭하고 **Traffic Match Criteria(**트래픽 일치 기준**)** 아래에서 **Source and Destination IP Address(**소스 및 대상 **IP** 주소**)(ACL** 사용**)**를 선택합니다.
e) 다음을 클릭합니다.
f) 검사를 원하는 트래픽을 지정합니다. UDP 포트 4342에서 FHR(first hop router) 및 ITR 또는 ETR 간에 트래픽을 지정해야 합니다. IPv4 및 IPv6 ACL이 모두 수락됩니다.
g) 다음을 클릭합니다.
h) **Rule Actions(**규칙 작업**)** 마법사 페이지 또는 탭에서 **Protocol Inspection(**프로토콜 검사**)** 탭을 선택합니다.
i) **LISP** 확인란을 선택합니다.
j) (선택 사항) 생성한 검사 맵을 선택하려면 **Configure(**구성**)**를 클릭합니다.
k) **Finish(**완료**)**를 클릭하여 서비스 정책 규칙을 저장합니다.

단계 **3** 중요한 트래픽에 대한 플로우 모빌리티를 활성화하려면 서비스 정책 규칙을 추가합니다.

a) **Configuration(**구성**)** > **Firewall(**방화벽**)** > **Service Policy Rules(**서비스 정책 규칙**)**를 선택합니다.
b) **Add(**추가**)**를 클릭합니다.
c) **Service Policy(**서비스 정책**)** 페이지에서 LISP 검사에 사용했던 동일한 서비스 정책을 선택합니다.
d) **Traffic Classification Criteria(**트래픽 분류 기준**)** 페이지에서 **Create a new traffic class(**새 트래픽 클래스 생성**)**를 클릭하고 **Traffic Match Criteria(**트래픽 일치 기준**)** 아래에서 **Source and Destination IP Address(**소스 및 대상 **IP** 주소**)(ACL** 사용**)**를 선택합니다.
e) 다음을 클릭합니다.
f) 서버가 사이트를 변경하는 경우 가장 최적의 사이트에 다시 할당할 비즈니스 크리티컬 트래픽을 지정합니다. 예를 들어 플로우 모빌리티를 HTTPS 트래픽 또는 특정 서버에 대한 트래픽으로 제한할 수 있습니다. IPv4 및 IPv6 ACL이 모두 수락됩니다.
g) 다음을 클릭합니다.
h) **Rule Actions(**규칙 작업**)** 마법사 페이지 또는 탭에서 **Cluster(**클러스터**)** 탭을 선택합니다.
i) **Enable Cluster flow-mobility triggered by LISP EID messages(LISP EID** 메시지에 의해 트리거된 클러스터 플로우 모빌리티 활성화**)** 확인란을 선택합니다.
j) **Finish(**완료**)**를 클릭하여 서비스 정책 규칙을 저장합니다.

단계 4 **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)**을 선택하고 **Enable Clustering flow mobility(**클러스터링 플로우 모빌리티 활성화**)** 확인란을 선택합니다.

단계 5 **Apply(**적용**)**를 클릭합니다.

분산 Site-to-Site VPN 구성

기본적으로 클러스터에서는 중앙 집중식 사이트 간 VPN 모드를 사용합니다. 클러스터링의 확장성을 활용하기 위해 분산 사이트 간 VPN 모드를 활성화할 수 있습니다.

분산 Site-to-Site VPN 정보

분산 모드에서 사이트 간 IPsec IKEv2 VPN 연결은 클러스터의 노드 전체에서 분산됩니다. 클러스터 노드 전체에서 VPN 연결을 분산시키면 클러스터의 용량 및 처리량 모두를 완전히 활용하며 특히 중앙 집중식 VPN 기능 이상으로 VPN 지원을 크게 확장합니다.

분산 *VPN* 연결 역할

클러스터의 여러 노드에 대한 연결을 로드 밸런싱할 수 있습니다. 연결 역할은 정상적인 작동이 이루어지고 있고 가용성이 높은 상황에서 연결을 처리하는 방법을 결정합니다. 분산 VPN 모드에서 실행 중인 경우 다음 역할이 클러스터 노드에 할당됩니다.

- 액티브 세션 소유자 — 연결을 처음으로 수신하는 노드 또는 백업 세션을 액티브 세션으로 전환한 유닛입니다. 소유자는 IKE 및 IPsec 터널과 연결된 모든 트래픽을 포함하여 전체 세션에 대한 패킷을 처리하고 상태를 유지 관리합니다.
- 백업 세션 소유자 — 기존 액티브 세션에 대한 백업 세션을 처리하는 노드입니다. 액티브 세션 소유자에 장애가 발생하는 경우 백업 세션 소유자는 액티브 세션 소유자가 되며 다른 노드에서 새로운 백업 세션이 설정됩니다.
- 전달자 — VPN 세션에 연결된 트래픽이 VPN 세션을 소유하지 않는 노드에 전송될 경우, 해당 노드는 클러스터 제어 링크를 사용하여 트래픽을 VPN 세션을 소유한 노드로 전달합니다.
- 오케스트레이터 — 오케스트레이터(항상 클러스터의 제어 노드)는 ASR(액티브 세션 재배포)을 실행할 때 어떤 세션이 이동하는지와 어디로 이동하는지를 계산합니다. 오케스트레이터는 소유자 노드 X에게 N개의 세션을 Y 노드로 이동하도록 요청합니다. 노드 X는 작업을 완료하면 이동할 수 있었던 세션 수를 지정하고 오케스트레이터에 다시 응답합니다.

분산 *VPN* 세션 특징

분산 사이트 간 VPN 세션에는 다음과 같은 특징이 있습니다. 그 외의 경우 VPN 연결은 한 클러스터에 있지 않으면 일반적인 방식으로 작동합니다.

- VPN 세션은 세션 수준에서 클러스터 전체에 분산됩니다. VPN 연결을 위해 동일한 클러스터 노드에서 IKE 및 IPsec 터널과 모든 트래픽을 처리하는 것을 의미합니다. VPN 세션 트래픽이 해당 VPN 세션을 소유하지 않는 클러스터 노드에 전송되는 경우, 트래픽이 VPN 세션을 소유하는 클러스터 노드로 전달됩니다.

- VPN 세션에는 클러스터 전반에서 고유한 세션 ID가 있습니다. 세션 ID를 사용하여 트래픽이 검증되고 전달 의사 결정이 이루어지며 IKE 협상이 완료됩니다.
- 사이트 간 VPN 허브 및 스포크 구성에서 클라이언트가 클러스터를 통해 연결할 때(헤어피닝이라고 함) 들어오고 나가는 세션 트래픽이 다른 클러스터 노드에 있을 수 있습니다.
- 백업 세션을 다른 섀시의 보안 모듈에 할당하도록 요청할 수 있습니다. 이렇게 하면 섀시 장애로부터 보호할 수 있습니다. 또는 클러스터의 노드에서 백업 세션을 할당하도록 선택할 수 있습니다. 이렇게 하면 노드 장애에 대해서만 보호됩니다. 클러스터에 두 개의 섀시가 있는 경우, 원격 섀시 백업이 권장됩니다.

클러스터 이벤트의 분산 *VPN* 처리

Event(이벤트**)**	분산 **VPN**
노드 장애	장애가 발생한 이 노드에 있는 모든 액티브 세션의 경우, 다른 노드에 있는 백업 세션이 액티브 세션이 되며 백업 세션은 백업 전략에 따라 다른 노드에서 재할당됩니다.
섀시 장애	원격 섀시 백업 전략을 사용 중인 경우 장애가 발생한 섀시의 모든 액티브 세션에 대해 다른 섀시의 노드에 있는 백업 세션이 액티브 상태가 됩니다. 노드가 대체되면 이러한 현재 액티브 세션에 대한 백업 세션이 대체된 섀시에 있는 노드에 재할당됩니다. 균일 백업 전략을 사용 중인 경우 액티브 세션과 백업 세션이 모두 장애가 발생한 섀시에 있는 경우 연결이 끊어집니다. 다른 섀시의 노드에 있는 백업 세션을 포함하는 모든 액티브 세션은 이러한 세션으로 대체됩니다. 새 백업 세션이 남아 있는 섀시의 다른 노드에 할당됩니다.
클러스터 노드 비활성화	클러스터 노드에 있는 모든 액티브 세션이 비활성화되면 다른 노드에 있는 백업 세션이 액티브 세션이 되며 백업 전략에 따라 다른 노드에서 백업 세션을 재할당합니다.
클러스터 노드 조인	새 노드의 VPN 클러스터 모드가 분산 모드로 설정되지 않은 경우 제어 노드에서 모드 변경을 요청합니다. VPN 모드가 호환 가능한 상태가 되면 정상 작동 플로우에서 클러스터 노드에 액티브 세션 및 백업 세션이 할당됩니다.

IPsec IKEv2 수정 사항

IKEv2는 다음 방식으로 분산 사이트 간 VPN 모드에서 수정됩니다.

- ID는 IP/포트 튜플 대신 사용됩니다. 이렇게 하면 패킷에서 적절한 전달 의사 결정이 가능하며 기타 클러스터 멤버에 나타날 수 있는 이전 연결의 정리가 가능합니다.
- 단일 IKEv2 세션을 식별하는 (SPI) 식별자는 로컬에서 생성되며 클러스터 전체에서 고유한 임의 8바이트 값입니다. SPI에서는 타임스탬프 및 클러스터 노드 ID를 임베드합니다. IKE 협상 패킷

을 수신했는데 타임스탬프 또는 클러스터 노드 ID 검사에 장애가 발생하면 패킷이 삭제되고 이유를 나타내는 메시지가 기록됩니다.

- 클러스터 멤버 전체에서 분할되어 NAT-T 협상에 장애가 발생하는 것을 방지하기 위해 IKEv2 처리가 수정되었습니다. IKEv2가 인터페이스에서 활성화되면 새 ASP가 도메인을 분류하며 *cluster_isakmp_redirect* 및 규칙이 추가됩니다.

클러스터 내의 분산 사이트 간 *VPN*을 위한 고가용성

다음 기능은 보안 모듈 또는 섀시의 단일 장애에 대비하여 복원력을 제공합니다.

- 모든 섀시의 클러스터에 있는 다른 보안 모듈에서 백업되어 있는 VPN 세션은 보안 모듈 장애를 견딜 수 있습니다.
- 다른 섀시에서 백업되어 있는 VPN 세션은 섀시 장애를 견딜 수 있습니다.
- 제어 노드가 VPN 사이트 간 세션 손실 없이 변경할 수 있습니다.

클러스터가 안정화되기 전에 추가 장애가 발생하는 경우, 액티브 세션 및 백업 세션 둘 다 장애가 발생한 노드에 있으면 연결이 끊어질 수 있습니다.

노드가 VPN 클러스터 모드 비활성화, 클러스터 노드 재로드 및 기타 예상된 섀시 변경과 같은 정상적인 방식으로 클러스터를 벗어날 경우 세션 손실을 방지하기 위해 모든 시도가 수행됩니다. 이러한 유형의 작업을 수행하는 동안 클러스터가 작업 간에 세션 백업을 다시 설정할 수 있는 시간을 부여받는 한, 세션은 손실되지 않습니다. 마지막 클러스터 노드에서 정상 종료가 트리거되는 경우, 기존 세션이 정상적으로 해제됩니다.

CMPv2

CMPv2 ID 인증서 및 키 쌍은 클러스터 노드 전체에서 동기화됩니다. 그러나, 클러스터의 제어 노드만 CMPv2 인증서를 자동으로 갱신하고 키를 재생성합니다. 제어 노드는 갱신 시 이러한 새 ID 인증서와 키를 모든 클러스터 노드와 동기화합니다. 이 방법으로 클러스터의 모든 노드가 인증을 위해 CMPv2 인증서를 활용하고 모든 노드가 제어 노드로도 인계받을 수 있습니다.

분산 사이트 간 **VPN**에 대한 라이선스

클러스터의 각 멤버에 있는 분산 사이트 간 VPN에 통신 사업자 라이선스가 필요합니다.

각 VPN 연결에는 두 개의 기타 *VPN* 라이선스 세션(기타 *VPN* 라이선스는 *Essentials* 라이선스의 일부임)이 필요합니다. 하나는 액티브 세션용이고 하나는 백업 세션용입니다. 각 세션에 두 개의 라이선스를 사용하기 때문에 클러스터의 최대 VPN 세션 용량은 라이선스가 부여된 용량의 절반을 초과할 수 없습니다.

분산 사이트 간 **VPN** 사전 요건

모델 지원

- Firepower 9300
- 최대 2개의 섀시에서 최대 6개의 모듈을 지원합니다. 각 섀시에 설치된 보안 모듈의 수량은 다를 수 있지만 동일한 배포를 사용하는 것이 좋습니다.

최대 **VPN** 세션 수

각 보안 모듈은 6개 노드 전체에서 최댓값인 약 36,000개의 세션에 대해 최대 6,000개의 VPN 세션을 지원합니다.

클러스터 노드에서 지원되는 세션의 실제 수는 플랫폼 용량, 할당된 라이선스 및 상황별 리소스 할당에 따라 결정됩니다. 사용률이 한도에 가까울 경우 각 클러스터 노드의 최대 용량에 도달하지 않은 경우에도 세션 생성이 실패할 수 있습니다. 이는 액티브 세션 할당이 외부 스위칭에 의해 결정되며, 백업 세션 할당이 내부 클러스터 알고리즘에 따라 결정되기 때문입니다. 고객은 사용률을 적절하게 조정하고 균일하지 않은 배포를 위한 공간을 확보하는 것이 좋습니다.

분산 사이트 간 **VPN** 지침

방화벽 모드

분산 사이트 간 VPN은 라우팅 모드에서만 지원됩니다.

상황 모드

분산 사이트 간 VPN은 단일 모드와 다중 상황 모드 둘 다에서 작동합니다. 하지만, 다중 상황 모드에서는 액티브 세션 재배포가 상황 수준이 아니라 시스템 수준에서 수행됩니다. 이렇게 하면 상황과 연결된 액티브 세션이 모르는 사이에 지원 불가능한 로드를 생성하면서 다른 상황과 연결된 액티브 세션을 포함하는 클러스터 멤버로 이동하는 것이 방지됩니다.

지원되지 않는 검사

다음 유형의 검사는 지원되지 않거나 분산 사이트 간 VPN 모드에서 비활성화됩니다.

- CTIQBE
- DCERPC
- H323, H225, RAS
- IPsec pass-through
- MGCP
- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH
- RTSP
- SCCP(Skinny)
- SUNRPC

- TFTP
- WAAS
- WCCP
- XDMCP

추가 지침

- 분산 사이트 간 VPN 모드에서는 IKEv2 IPsec 사이트 간 VPN만 지원됩니다. IKEv1은 지원되지 않습니다. IKEv1 사이트 간은 중앙 집중식 VPN 모드에서 지원됩니다.
- 사이트 간 클러스터링은 지원되지 않습니다.
- 분산 사이트 간 VPN 모드에서는 인터페이스 PAT를 사용할 수 없습니다.

분산 사이트 간 VPN 활성화

VPN 세션을 위한 클러스터링의 확장성을 활용하려면 분산 사이트 간 VPN을 활성화합니다.

참고 중앙 집중식 모드와 분산형 모드 간에 VPN 모드를 변경하려면 클러스터 의 모든 노드를 다시 로드해야 합니다. 백업 모드의 변경은 동적이며 변경 시 세션이 종료되지 않습니다.

시작하기 전에

VPN 컨피그레이션 가이드 에 따라 사이트 간 VPN을 구성합니다.

프로시저

단계 1 **Configuration(**구성**) > Device Management(**디바이스 관리**) > High Availability and Scalability(**고가용성 및 확장성**) > ASA Cluster(ASA** 클러스터**)**를 선택합니다.

단계 2 **VPN Cluster Mode(VPN** 클러스터 모드**)** 영역에서 클러스터에 대해 **VPN Mode(VPN** 모드**)(Centralized(**중앙 집중식**)** 또는 **Distributed(**분산**))**를 선택합니다.

단계 3 **Backup Distribution Mode(**백업 배포 모드**)(Flat(**균일**)** 또는 **Remote-chassis(**원격-섀시**))**를 선택합니다.

균일 백업 모드에서 스탠바이 세션은 다른 클러스터 유닛에서 설정됩니다. 이 경우 사용자가 모듈 장애로부터 보호될 수 있지만 섀시 장애가 반드시 방지되는 것은 아닙니다.

원격 섀시 백업 모드에서 스탠바이 세션은 클러스터에서 다른 섀시의 노드에서 설정됩니다. 이 경우 사용자가 모듈 장애와 섀시 장애로부터 보호됩니다.

원격 섀시가 단일 섀시 환경에서 구성된 경우(의도적으로 또는 장애로 인해 구성된 경우) 다른 섀시가 조인할 때까지 백업이 생성되지 않습니다.

단계 4 **Apply(**적용**)**를 클릭합니다.

다시 로드하라는 프롬프트가 표시됩니다. 이 설정은 다시 로드하기 전에 모든 데이터 노드에 복제됩니다. 클러스터 모든 노드가 다시 로드됩니다.

분산 S2S VPN 세션 재배포

액티브 세션 재배포는 클러스터 노드 전체에서 액티브 VPN 세션의 로드를 재배포합니다. 세션 시작 및 종료의 동적인 특성으로 인해 액티브 세션 재배포는 모든 클러스터 노드 전체에서 세션의 균형을 유지하는 최선의 작업입니다. 반복된 재배포 작업은 균형을 최적화합니다.

재배포는 언제든지 실행될 수 있으며 클러스터에서 토폴로지를 변경한 이후에 실행되어야 하고 새 노드가 클러스터에 참가한 이후에 실행하는 것이 좋습니다. 재배포의 목적은 안정적인 VPN 클러스터를 생성하는 것입니다. 안정적인 VPN 클러스터에는 노드 전체에 걸쳐 거의 동일한 수의 액티브 세션 및 백업 세션이 있습니다.

세션을 이동하기 위해 백업 세션이 액티브 세션이 되고 새 백업 세션을 호스트하기 위해 다른 노드가 선택됩니다. 세션의 이동은 액티브 세션의 백업 위치와 해당 특정 백업 노드에 이미 있는 액티브 세션의 수에 따라 달라집니다. 백업 세션 노드가 어떠한 이유로 액티브 세션을 호스트할 수 없는 경우, 원래 노드는 세션의 소유자로 유지됩니다.

다중 상황 모드에서는 액티브 세션 재배포가 개별 상황 수준이 아니라 시스템 수준에서 수행됩니다. 한 상황의 액티브 세션이 다른 상황의 더 많은 액티브 세션을 포함하는 노드를 이동하여 해당 클러스터 노드에서 더 많은 로드를 생성할 수 있기 때문에 이 작업은 상황 수준에서 수행되지 않습니다.

시작하기 전에

- 재배포 활동을 모니터링하려는 경우 시스템 로그를 활성화합니다.
- 이 절차는 클러스터의 제어 노드에서 수행해야 합니다.

프로시저

단계 1 액티브 세션 및 백업 세션이 클러스터 전체에서 분산되는 방식을 확인하려면 **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > ASA Cluster(ASA** 클러스터**) > Cluster Summary(**클러스터 요약**) > VPN Cluster Summary(VPN** 클러스터 요약**)**를 선택합니다.

재배포할 세션 수와 클러스터에서의 로드에 따라 이 작업에 시간이 걸릴 수 있습니다. 재배포 활동이 수행될 때 다음 구문(및 기타 시스템 세부 정보는 여기에 표시되지 않음)을 포함하는 Syslog가 제공됩니다.

Syslog 구문	참고
VPN 세션 재배포가 시작됨	제어 노드만
*orig-member-name*에서 *dest-member-name*으로 *number* 세션을 이동하기 위한 요청을 전송함	제어 노드만

Syslog 구문	참고
*member-name*에 세션 재배포 메시지를 전송하지 못함	제어 노드만
*orig-member-name*에서 *dest-member-name*으로 *number* 세션을 이동하기 위한 요청을 수신함	데이터 노드만
number 세션을 *member-name*으로 이동함	명명된 클러스터로 이동된 활성 세션의 수입니다.
*dest-member-name*에서 세션 이동 응답을 수신하지 못함	제어 노드만
VPN 세션이 완료됨	제어 노드만
클러스터 토폴로지 변경이 탐지됨. VPN 세션 재배포가 중단됨.	

단계 **2** **Redistribution(**재배포**)**을 클릭합니다.

단계 **3** 재배포 활동의 결과를 확인하려면 **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > ASA Cluster(ASA** 클러스터**) > Cluster Summary(**클러스터 요약**) > VPN Cluster Summary(VPN** 클러스터 요약**)**를 새로 고칩니다.

재배포에 성공했으며 실질적인 시스템 또는 세션 활동이 없는 경우, 시스템의 균형이 조정되고 이 작업이 완료됩니다.

그렇지 않으면, 재배포 프로세스를 반복하여 균형을 조정하고 시스템을 안정시킵니다.

FXOS: 클러스터 노드 제거

다음 섹션에서는 클러스터에서 노드를 일시적으로 또는 영구적으로 제거하는 방법을 설명합니다.

임시 제거

하드웨어나 네트워크 장애 등의 이유 때문에 클러스터 노드가 클러스터에서 자동으로 제거됩니다. 이 제거는 조건을 수정할 때까지 임시로 적용되며, 클러스터에 다시 참여할 수 있습니다. 클러스터링을 수동으로 비활성화할 수도 있습니다.

디바이스가 현재 클러스터에 있는지 확인하려면, 애플리케이션에서 **show cluster info** 명령을 사용해 Firewall Chassis Manager **Logical Devices(**논리적 디바이스**)** 페이지:

- 애플리케이션에서 클러스터링 비활성화 - 애플리케이션 CLI를 사용하여 클러스터링을 비활성화할 수 있습니다. **cluster remove unit** *name* 명령을 입력해 로그인한 노드 외의 모든 노드를 제거합니다. 부트스트랩 설정과 제어 노드에서 동기화한 마지막 설정도 그대로 유지되므로 나중에 설정이 유실되는 일 없이 노드를 다시 추가할 수 있습니다. 이 명령을 데이터 노드에 입력해서 제어 노드를 제거하면 새로운 제어 노드가 선택됩니다.

  디바이스가 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 재개하려면 클러스터링을 다시 활성화합니다. 관리 인터페이스에서는 부트스트랩 구성에서 노드로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 노드가 클러스터에서 여전히 비활성 상태인 경우(예를 들어 클러스터링이 비활성화된 구성을 저장한 경우)에는 관리 인터페이스가 비활성화됩니다.

  클러스터링을 다시 활성화하려면 ASA에 **cluster group** *name*을 입력하고 **enable**을(를) 입력합니다.

- 애플리케이션 인스턴스 비활성화 - **Logical Devices(**논리적 디바이스**)** 페이지의 Firewall Chassis Manager에서 슬라이더 활성화됨( )을(를) 클릭합니다. 나중에 슬라이더 비활성화됨( )을(를) 사용하여 다시 활성화할 수 있습니다.

- 보안 모듈/엔진 종료 - **Security Module/Engine(**보안 모듈/엔진**)** 페이지의 Firewall Chassis Manager에서 전원 끄기 아이콘을 클릭합니다.

- 섀시 종료 - **Overview(**개요**)** 페이지의 Firewall Chassis Manager에서 종료 아이콘을 클릭합니다.

영구 제거

다음 방법을 사용하면 클러스터 노드를 영구적으로 제거할 수 있습니다.

- 논리적 디바이스 삭제 - **Logical Devices(**논리적 디바이스**)** 페이지의 Firewall Chassis Manager에서 삭제( )을(를) 클릭합니다. 이제 독립형 논리적 디바이스, 새 클러스터를 구축하거나 동일한 클러스터에 새 논리적 디바이스를 추가할 수 있습니다.

- 서비스에서 섀시 또는 보안 모듈 제거 - 서비스에서 디바이스를 제거하면, 교체 하드웨어를 클러스터의 새 노드로 추가할 수 있습니다.

ASA: 클러스터 멤버 관리

클러스터를 배치한 후에는 컨피그레이션을 변경하고 클러스터 멤버를 관리할 수 있습니다.

멤버 비활성화

클러스터의 멤버를 비활성화하려면, 클러스터링 구성은 그대로 유지한 상태로 노드의 클러스터링을 비활성화합니다.

참고 수동으로 또는 상태 확인 장애를 통해 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며, 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 다시 시작하려면 클러스터링을 다시 활성화합니다. 또는 클러스터에서 노드를 모두 제거할 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 노드로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 노드가 클러스터에서 여전히 비활성 상태인 경우(예를 들어 클러스터링이 비활성화된 구성을 저장한 경우)에는 관리 인터페이스가 비활성화됩니다. 추가 구성을 위해서는 콘솔 포트를 사용해야 합니다.

시작하기 전에

- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우Configuration(구성) > Device List(디바이스 목록) 창의 활성 디바이스 IP 주소에서 **System(**시스템**)**을 더블 클릭합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)**을 선택합니다.

단계 **2** **Participate in ASA cluster(ASA** 클러스터에 참여**)** 확인란의 선택을 취소합니다.

참고
Configure ASA cluster settings(ASA 클러스터 설정 구성**)** 확인란의 선택을 취소하지 마십시오. 취소할 경우 모든 클러스터 컨피그레이션이 지워지며 ASDM이 연결된 모든 관리 인터페이스를 비롯한 모든 인터페이스도 종료됩니다. 이 경우 연결을 복원하려면 콘솔 포트의 CLI에 액세스해야 합니다.

단계 **3** **Apply(**적용**)**를 클릭합니다.

제어 유닛에서 데이터유닛 비활성화

데이터 노드를 비활성화하려면 다음 단계를 수행합니다.

참고 ASA가 비활성화되면 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 트래픽 흐름을 재개하려면 클러스터링을 다시 활성화합니다. 관리 인터페이스에서는 클러스터 IP 풀에서 노드로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 노드가 클러스터에서 여전히 비활성 상태인 경우(예를 들어 클러스터링이 비활성화된 구성을 저장한 경우)에는 관리 인터페이스가 비활성화됩니다. 추가 구성을 위해서는 콘솔 포트를 사용해야 합니다.

시작하기 전에

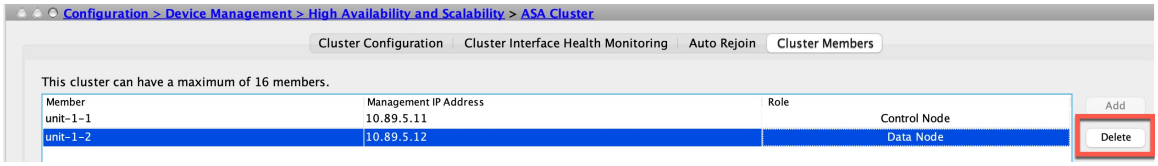
다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우**Configuration(**구성**) > Device List(**디바이스 목록**)** 창의 활성 디바이스 IP 주소에서 **System(**시스템**)**을 더블 클릭합니다.

프로시저

단계 **1** **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Members(**클러스터 멤버**)**를 선택합니다.

단계 **2** 제거할 데이터 노드를 선택하고 **Delete(**삭제**)**를 클릭합니다.

그림 ***1:*** 노드 삭제



데이터 노드 부트스트랩 구성이 그대로 유지되므로, 구성이 손실되는 일 없이 데이터 노드를 나중에 다시 추가할 수 있습니다.

단계 **3** **Apply(**적용**)**를 클릭합니다.

클러스터 재참가

노드가 클러스터에서 제거된 경우, 예를 들어 실패한 인터페이스의 경우 또는 멤버를 수동으로 비활성화한 경우, 클러스터를 수동으로 다시 조인해야 합니다.

시작하기 전에

- 클러스터링을 다시 활성화하려면 콘솔 포트를 사용해야 합니다. 다른 인터페이스는 종료됩니다. 예외는 ASDM에서 클러스터링을 수동으로 비활성화한 경우이며 구성을 저장하지 않고 다시 로

드한 경우 ASDM에서 클러스터링을 다시 활성화할 수 있습니다. 다시 로드한 후에 관리 인터페이스가 비활성화되므로 콘솔 액세스는 클러스터링을 다시 활성화하기 위한 유일한 방법입니다.

- 다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우**Configuration(**구성**) > Device List(**디바이스 목록**)** 창의 활성 디바이스 IP 주소에서 **System(**시스템**)**을 더블 클릭합니다.
- 클러스터를 다시 조인하기 전에 장애가 해결되었는지 확인하십시오.

프로시저

단계 **1** 아직 ASDM 액세스 권한이 있는 경우, ASDM을 다시 활성화할 노드에 연결하여 ASDM에서 클러스터링을 다시 활성화할 수 있습니다.

클러스터링은 새 멤버로 추가하지 않는 한 제어 노드에서 데이터 노드에 대한 클러스터링을 다시 활성화할 수 없습니다.

a) **Configuration(**구성**) > Device Management(**디바이스 관리**) > High Availability and Scalability(**고가용성 및 확장성**) > ASA Cluster(ASA** 클러스터**)** 를 선택합니다.
b) **Participate in ASA cluster(ASA** 클러스터에 참가**)** 확인란을 선택합니다.
c) **Apply(**적용**)**를 클릭합니다.

단계 **2** ASDM을 사용할 수 없는 경우: 콘솔에서 클러스터 구성 모드를 시작합니다.

cluster group *name*

예제**:**

```
ciscoasa(config)# cluster group pod1
```

단계 **3** 클러스터링을 활성화합니다.

enable

제어 유닛 변경

⚠

주의 제어 노드를 변경하는 가장 좋은 방법은 제어 노드의 클러스터링을 비활성화한 후 새 제어가 선택될 때까지 기다렸다가 클러스터링을 다시 활성화하는 것입니다. 제어 노드가 될 정확한 노드를 지정해야 할 경우, 이 섹션의 절차를 참조하십시오. 그러나 중앙 집중식 기능의 경우, 이 절차를 통해 제어 노드를 강제로 변경하면 모든 연결이 끊어지며 새 제어 노드에서 연결을 다시 설정해야 합니다.

제어 노드를 변경하려면 다음 단계를 수행합니다.

시작하기 전에

다중 상황 모드의 경우, 시스템 실행 영역에서 이 절차를 수행합니다. 이미 시스템 구성 모드가 아닌 경우Configuration(구성) > Device List(디바이스 목록) 창의 활성 디바이스 IP 주소에서 **System(**시스템**)**을 더블 클릭합니다.

프로시저

단계 **1** **Monitoring** > **ASA Cluster** > **Cluster Summary**를 선택합니다.

단계 **2** 드롭다운 목록에서 제어가 될 데이터 노드를 선택하고 제어 노드로 설정하려면 버튼을 클릭합니다.

단계 **3** 제어 노드 변경을 확인하라는 메시지가 표시됩니다. **Yes(**예**)**를 클릭합니다.

단계 **4** ASDM을 종료하고 기본 클러스터 IP 주소를 사용하여 다시 연결합니다.

클러스터 전체에서 명령 실행

클러스터의 모든 멤버 또는 특정 멤버에 명령을 보내려면 다음 단계를 수행합니다. 모든 멤버에 **show** 명령을 보내면 모든 출력이 수집되고 해당 내용이 현재 유닛의 콘솔에 표시됩니다. 또는 클러스터 전체의 통계를 확인하기 위해 제어 유닛에서 입력할 수 있는 show 명령이 있습니다. **capture** 및 **copy**와 같은 다른 명령의 경우 클러스터 전체 실행을 활용할 수도 있습니다.

시작하기 전에

Tools(툴**)** > **Command Line Interface(**명령줄 인터페이스**)**를 선택하여 Command Line Interface 툴에서 이 절차를 수행합니다.

프로시저

모든 멤버 또는 유닛 이름을 지정한 경우 특정 멤버에 명령을 전송합니다.

cluster exec [unit *unit_name*] *command*

예제**:**

```
cluster exec show xlate
```

멤버 이름을 확인하려면 **cluster exec unit ?** 또는 **show cluster info** 명령을 입력합니다(현재 유닛을 제외한 모든 이름을 보려는 경우).

예

클러스터에 있는 모든 유닛의 동일한 캡처 파일을 TFTP 서버에 동시에 복사하려면 다음 명령을 제어 유닛에 입력합니다.

```
cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

유닛당 하나씩인 여러 PCAP 파일이 TFTP 서버에 복사됩니다. 목적지 캡처 파일의 이름 뒤에는 유닛 이름이 자동으로 연결되며 capture1_asa1.pcap, capture1_asa2.pcap 같은 형식이 됩니다. 이 예에서 asa1 및 asa2는 클러스터 유닛 이름 입니다.

cluster exec show memory 명령에 대한 다음 샘플 출력에는 클러스터의 각 멤버에 대한 메모리 정보가 나와 있습니다.

```
cluster exec show memory
unit-1-1(LOCAL):*******************************************************
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:*******************************************************************
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:*******************************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)
```

ASA: ASA 클러스터 모니터링 - Firepower 4100/9300 섀시

클러스터의 상태 및 연결을 모니터링하고 문제를 해결할 수 있습니다.

참고 ASA의 클러스터 제어 링크의 패킷을 FXOS와 비교할 때 FXOS 패킷 수가 ASA에 표시된 것보다 더 많습니다. ASA에서는 클러스터 제어 링크 IP 주소로 향하는 패킷만 입력 패킷으로 계산됩니다. 데이터 인터페이스에 다시 주입되는 전달된 패킷은 데이터 인터페이스의 입력 통계 및 클러스터 제어 링크의 출력 통계에만 포함됩니다.

클러스터 상태 모니터링

클러스터 상태 모니터링에 대한 내용은 다음 화면을 참조하십시오.

- **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > Cluster Summary(**클러스터 요약**)**

  이 창에는 연결된 유닛에 대한 클러스터 정보 및 클러스터의 다른 유닛에 대한 정보가 표시됩니다. 이 창에서 기본 유닛을 변경할 수도 있습니다.

- **Cluster Dashboard(**클러스터 대시보드**)**

  기본 유닛의 홈 페이지에서 Cluster Dashboard(클러스터 대시보드) 및 Cluster Firewall Dashboard(클러스터 방화벽 대시모드)를 사용하여 클러스터를 모니터링할 수 있습니다.

클러스터 전체 패킷 캡처

클러스터의 패킷을 캡처하는 방법에 대한 내용은 다음 화면을 참조하십시오.

Wizards(마법사**) > Packet Capture Wizard(**패킷 캡처 마법사**)**

클러스터 전체의 문제를 해결하기 위해 제어 노드에서 클러스터별 트래픽의 캡처를 활성화할 수 있습니다. 이 경우 클러스터의 모든 데이터 노드에서 캡처가 자동으로 활성화됩니다.

클러스터 리소스 모니터링

클러스터 리소스 모니터링에 대한 내용은 다음 을 참조하십시오.

- **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > System Resources Graphs(**시스템 리소스 그래프**) > CPU**

  이 창을 사용하여 클러스터 전반의 CPU 사용률을 보여 주는 그래프 또는 표를 생성할 수 있습니다.

- **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > System Resources Graphs(**시스템 리소스 그래프**) > Memory(**메모리**)**.

  이 창을 사용하여 클러스터 멤버 전반의 가용 메모리 및 사용한 메모리를 보여 주는 그래프 또는 표를 생성할 수 있습니다.

클러스터 트래픽 모니터링

클러스터 트래픽 모니터링에 대한 내용은 다음 을 참조하십시오.

- **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > Traffic Graphs(**트래픽 그래프**) > Connections(**연결**)**.

  이 창을 사용하여 클러스터 전반의 연결을 보여 주는 그래프 또는 표를 생성할 수 있습니다.

- **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > Traffic Graphs(**트래픽 그래프**) > Throughput(**처리량**)**.

  이 창을 사용하여 클러스터 전반의 트래픽 처리량을 보여 주는 그래프 또는 표를 생성할 수 있습니다.

- **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > Cluster Load-Monitoring(**클러스터 로드 모니터링**)**

이 섹션에는 로드 모니터-정보 및 로드-모니터 세부 정보 창이 포함됩니다. **Load Monitor-Information(**로드 모니터-정보**)**에는 마지막 간격 동안의 클러스터 멤버에 대한 트래픽 로드가 표시되며, 구성된 총 간격 수(기본적으로 30개)에 대한 평균도 표시됩니다. **Load-Monitor Details(**로드-모니터 세부 정보**)** 창을 사용하여 각 간격에서 각 측정값의 값을 확인합니다.

클러스터 제어 링크 모니터링

클러스터 상태 모니터링에 대한 내용은 다음 화면을 참조하십시오.

Monitoring(모니터링**) > Properties(**속성**) > System Resources Graphs(**시스템 리소스 그래프**) > Cluster Control Link(**클러스터 제어 링크**)**.

이 창을 사용하면 클러스터 제어 링크 수신 및 전송 용량 사용률을 보여 주는 그래프 또는 표를 생성할 수 있습니다.

클러스터 라우팅 모니터링

클러스터 라우팅에 대한 내용은 다음 화면을 참조하십시오.

- **Monitoring(**모니터링**)** > **Routing(**라우팅**)** > **LISP-EID Table(LISP-EID** 테이블**)**

  EID 및 사이트 ID를 보여주는 ASA EID 테이블을 표시합니다.

분산 **S2S VPN** 모니터링

VPN 클러스터 상태 모니터링에 대한 내용은 다음 화면을 참조하십시오.

- **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > ASA Cluster(ASA** 클러스터**) > Cluster Summary(**클러스터 요약**) > VPN Cluster Summary(VPN** 클러스터 요약**)**

  클러스터 전체에서 세션의 배포를 표시하고 세션을 재배포하는 기능을 제공합니다.

- **Monitoring(**모니터링**) > VPN > VPN Statistics(VPN** 통계**) > Sessions(**세션**)**

  제어 및 데이터 클러스터 노드가 모두 나열됩니다. 자세한 내용을 보려면 노드를 클릭하십시오.

클러스터링의 로깅 구성

클러스터링의 로깅 구성에 대한 내용은 다음 화면을 참조하십시오.

Configuration(구성**) > Device Management(**디바이스 관리**) > Logging(**로깅**) > Syslog Setup(Syslog** 설정**)**

클러스터의 각 노드에서는 시스템 로그 메시지를 독립적으로 생성합니다. 명령을 사용하면 디바이스 ID가 동일하거나 다른 시스템 로그 메시지를 생성하여 클러스터의 동일한 또는 다른 노드에서 메시지가 표시되도록 할 수 있습니다.

분산 S2S VPN 트러블슈팅

분산 **VPN** 알림

분산 VPN을 실행하는 클러스터에서 다음 오류 상황이 발생하는 경우, 식별된 구문이 포함된 메시지가 있는 알림을 받게 됩니다.

상태	알림
클러스터에 참가하려고 시도할 때 기존 또는 참가 중인 클러스터 데이터 노드가 분산 VPN 모드에 있지 않은 경우 다음을 수행합니다.	새 클러스터 멤버(*member-name*)가 vpn 모드 불일치 때문에 거부되었습니다. 및 제어 노드(*control-name*)는 다음과 같은 이유로 유닛(unit-name)의 등록 요청을 거부합니다. VPN 모드 기능이 제어 노드 구성과 호환되지 않습니다.
라이선싱이 분산 VPN에 대한 클러스터 멤버에서 적절하게 구성되어 있지 않은 경우:	오류: 제어 노드가 요청한 클러스터 vpn-mode가 분산 모드로 변경되었습니다. 통신 사업자 라이선스의 누락으로 인해 모드를 변경할 수 없습니다.
타임스탬프 또는 멤버 ID가 수신된 IKEv2 패킷의 SPI에서 유효하지 않은 경우:	만료 SPI 수신됨 또는 손상된 SPI 탐지됨
클러스터가 백업 세션을 생성할 수 없는 경우:	IKEv2 세션에 대한 백업을 생성하지 못했습니다.
IKEv2 IC(초기 연락처) 처리 오류:	IKEv2 협상이 오류로 인해 중단됨: 백업에서 오래된 백업 세션이 발견됨
재배포 문제:	*member-name*에 세션 재배포 메시지를 전송하지 못함 *member-name* 으로부터 세션 이동 응답을 수신하지 못했습니다(제어 노드에만 해당).
세션 재배포를 수행하는 동안 토폴로지가 변경되는 경우:	클러스터 토폴로지 변경이 탐지됨. VPN 세션 재배포가 중단됨.

다음 상황 중 한 가지가 발생했을 수 있습니다.

- Nexus 7K 스위치가 **port-channel load-balance src-dst l4port** 명령을 사용하는 로드 밸런싱 알고리즘으로 레이어 4 포트를 사용하여 구성된 경우 사이트 간 VPN 세션은 클러스터에 있는 섀시 중 하나에만 배포되고 있습니다. 클러스터 세션 할당의 예는 다음과 같습니다.

```
SSP-Cluster/data node(cfg-cluster)# show cluster vpn-sessiondb distribution
```

```
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

사이트 간 IKEv2 VPN이 소스 및 대상 포트에 모두 포트 500을 사용하므로 IKE 패킷은 Nexus 7K와 섀시 사이에서 연결된 포트 채널의 링크 중 하나에만 전송됩니다.

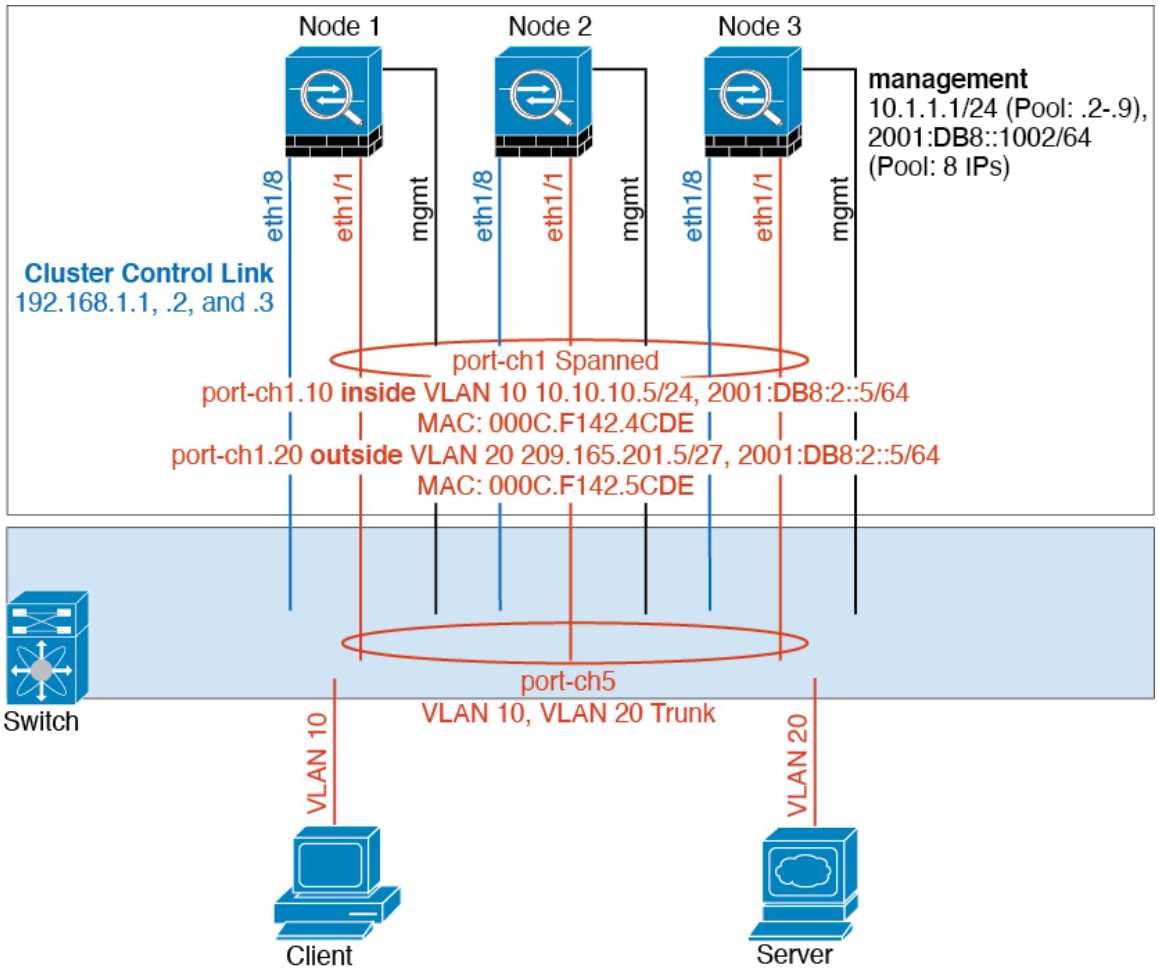
port-channel load-balance src-dst ip-l4port를 사용하여 Nexus 7K 로드 밸런싱 알고리즘을 IP 및 레이어 4 포트로 변경합니다. 그러면 IKE 패킷이 모든 링크와 모든 노드에 전송됩니다.

더 즉각적인 조정을 위해 클러스터의 제어 노드에서는 **cluster redistribute vpn-sessiondb**를 실행하여 액티브 VPN 세션을 다른 섀시의 클러스터 노드로 재배포합니다.

ASA 클러스터링의 예

이러한 예에는 일반적인 구축이 포함됩니다.

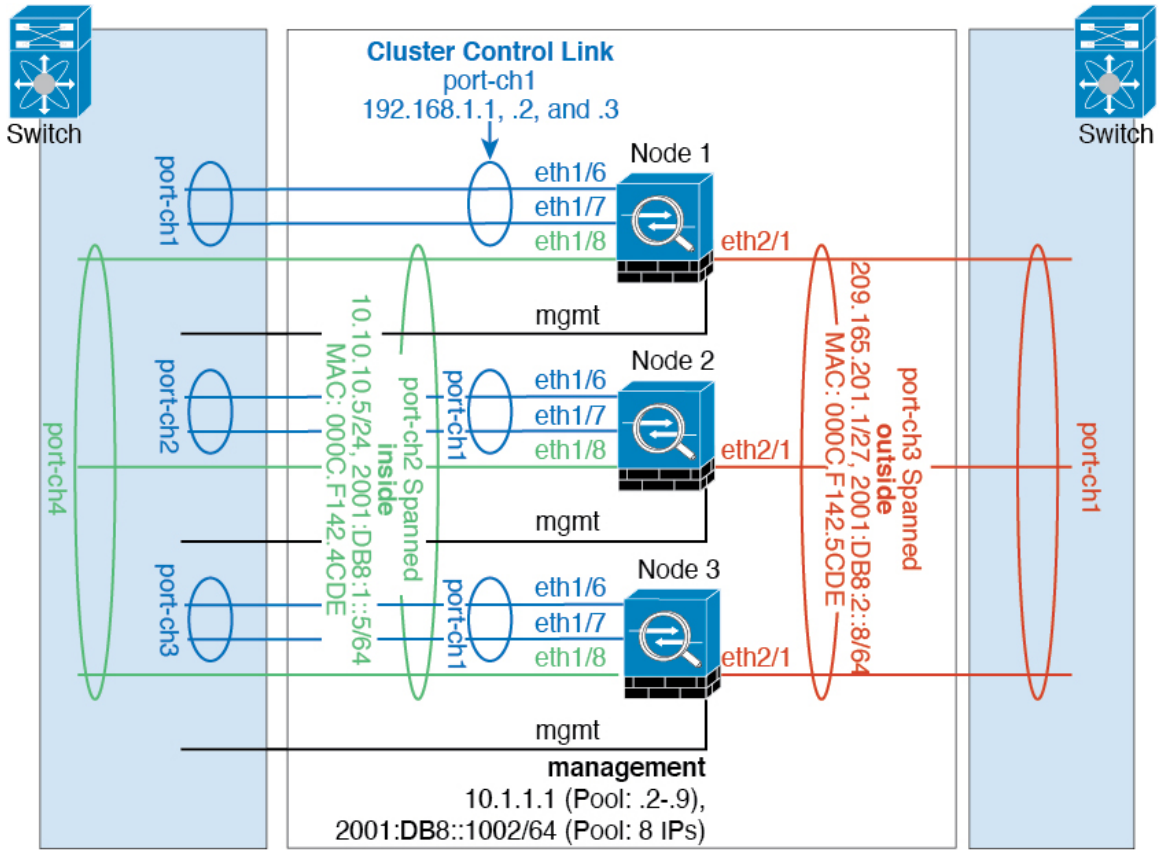
단일화된 방화벽



서로 다른 보안 도메인의 데이터 트래픽은 서로 다른 VLAN에 연결됩니다. 예를 들어, VLAN 10은 내부 네트워크용이고 VLAN 20은 외부 네트워크용입니다. 각 ASA에는 외부 스위치 또는 라우터에 연결된 하나의 물리적 포트가 있습니다. 트렁킹이 활성화되어 있으므로 물리적 링크의 모든 패킷은 캡슐화된 802.1q입니다. ASA는 VLAN 10과 VLAN 20 사이의 방화벽입니다.

스팬 EtherChannel을 사용할 경우, 모든 데이터 링크가 스위치 측의 단일한 EtherChannel로 그룹화됩니다. ASA를 사용할 수 없게 될 경우, 스위치에서 나머지 유닛 간의 트래픽을 리밸런싱합니다.

트래픽 분리



내부 네트워크와 외부 네트워크 간의 트래픽을 물리적으로 분리하려는 경우가 있습니다.

위의 다이어그램에 표시된 것과 같이, 왼쪽에는 내부 스위치에 연결되는 스팬 EtherChannel이 하나 있고 오른쪽에는 외부 스위치에 연결되는 스팬 EtherChannel이 있습니다. 필요한 경우 각 EtherChannel에 VLAN 하위 인터페이스를 생성할 수도 있습니다.

라우팅 모드 사이트 간 클러스터링을 위한 OTV 구성

Spanned EtherChannel의 라우팅 모드에 대한 사이트 간 클러스터링의 성공 여부는 적절한 구성 및 OTV의 모니터링에 달려 있습니다. OTV는 DCI를 통해 패킷을 전달함으로써 중요한 역할을 수행합니다. OTV는 전달 테이블에서 MAC 주소를 학습하는 경우에만 DCI를 통해 유니캐스트 패킷을 전달합니다. OTV 전달 테이블에서 MAC 주소를 학습하지 못하면 유니캐스트 패킷을 삭제합니다.

샘플 OTV 구성

```
//Sample OTV config:
//3151 – Inside VLAN, 3152 – Outside VLAN, 202 – CCL VLAN
//aaaa.1111.1234 – ASA inside interface global vMAC
//0050.56A8.3D22 – Server MAC

feature ospf
```

```
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown

otv-isis default
  vpn Overlay1
```

```
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

사이트 장애 때문에 OTV 필터 수정 필요

사이트가 다운되면, 전역 MAC 주소를 더 이상 차단하지 않을 것이기 때문에 OTV에서 필터를 제거해야 합니다 몇 가지 추가 구성이 필요합니다.

작동하는 사이트의 OTV 스위치에서 ASA 전역 MAC 주소에 대한 정적 항목을 추가해야 합니다. 정적 항목을 추가하면 다른 쪽의 OTV는 오버레이 인터페이스에서 이러한 항목을 추가할 수 있습니다. 서버 및 클라이언트가 ASA에 대한 ARP 항목을 이미 가지고 있으면(기존 연결의 경우 그러함) ARP를 다시 전송하지 않을 것이므로 이 단계가 필요합니다. 따라서 OTV는 전달 테이블에서 ASA 전역 MAC 주소를 학습할 수 없게 됩니다. OTV는 전달 테이블에 전역 MAC 주소를 가지고 있지 않으며 OTV 설계 단위로 오버레이 인터페이스를 통해 유니 캐스트 패킷을 플러드하지 않을 것이므로, 서버에서 전역 MAC 주소로 보내는 유니캐스트 패킷이 삭제되고 기존 연결이 끊어집니다.

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

다른 사이트가 복원되면 필터를 다시 추가하고 OTV에서 이 정적 항목을 제거해야 합니다. 전역 MAC 주소에 대한 오버레이 항목을 지우려면 두 OTV에서 동적 MAC 주소 테이블을 지우는 것이 매우 중요합니다.

MAC 주소 테이블 지우기

사이트가 다운되고 전역 MAC 주소의 정적 항목이 OTV에 추가되면, 다른 OTV가 오버레이 인터페이스의 전역 MAC 주소를 학습하도록 해야 합니다. 다른 사이트가 나타나면 이러한 항목을 지워야 합니다. OTV의 전달 테이블에 이러한 항목이 없는지 확인하려면 MAC 주소 테이블을 지우십시오.

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
```

```
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP 캐시 모니터링

OTV는 OTV 인터페이스를 통해 학습한 IP 주소의 프록시 ARP에 대한 ARP 캐시를 유지 관리합니다.

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

사이트 간 클러스터링 예시

다음 예에는 지원되는 클러스터 구축에 대한 내용이 나와 있습니다.

사이트별 **MAC** 및 **IP** 주소가 있는 **Spanned EtherChannel** 라우팅 모드의 예

다음 예에서는 게이트웨이 라우터와 각 사이트의 내부 네트워크 사이에 위치한(이스트-웨스트 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버를 보여줍니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부 네트워크용 Spanned EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 섀시를 포괄합니다.

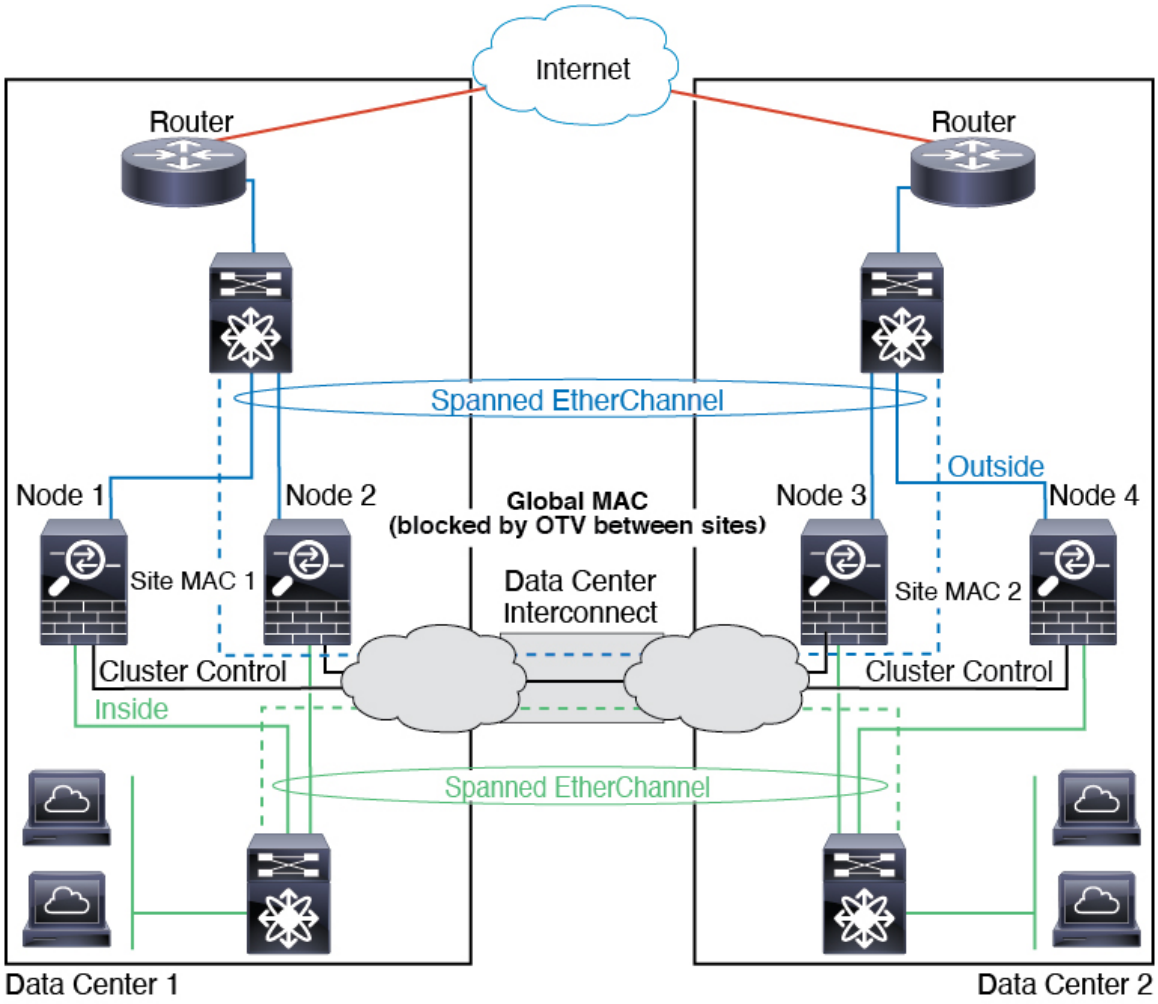
OTV(Overlay Transport Virtualization) 또는 이와 유사한 방법으로 데이터 VLAN이 사이트 전반에 확장됩니다. 트래픽이 클러스터로 향할 때 DCI를 통과하여 반대쪽 사이트에 가지 않도록 전역 MAC 주소를 차단하는 필터를 추가해야 합니다. 어떤 사이트의 클러스터 노드가 연결할 수 없게 되면 트래픽이 다른 사이트의 클러스터 노드에 성공적으로 도달할 수 있도록 모든 필터를 제거해야 합니다. VACL을 사용하여 전역 MAC 주소를 필터링해야 합니다.F3-Series 라인 카드가 포함된 Nexus 등 일부 스위치의 경우 전역 MAC 주소에서 ARP 패킷을 차단하려면 ARP 검사도 사용해야 합니다. ARP 검사를 수행하려면 ASA에서 사이트 MAC 주소와 사이트 IP 주소를 모두 설정해야 합니다. 사이트 MAC 주소만 구성하는 경우ARP 검사를 비활성화해야 합니다.

클러스터는 내부 네트워크의 게이트웨이 역할을 합니다. 모든 클러스터 노드에서 공유되는 전역 가상 MAC은 패킷 수신에만 사용됩니다. 발신 패킷은 각 DC 클러스터의 사이트별 MAC 주소를 사용합니다. 이 기능은 스위치가 서로 다른 두 포트의 두 사이트로부터 동일한 전역 MAC 주소를 학습하지 못하게 하는 한편, MAC 플래핑(flapping)을 일으킵니다. 대신 스위치는 사이트 MAC 주소만 학습합니다.

이 시나리오에서:

- 클러스터에서 전송한 모든 이그레스(egress) 패킷은 사이트 MAC 주소를 사용하며 데이터 센터에서 지역화됩니다.

- 클러스터에 대한 모든 인그레스 패킷은 전역 MAC 주소를 사용하여 전송되므로, 양 사이트의 어느 노드에서나 수신할 수 있습니다. OTV의 필터는 데이터 센터 내에서 트래픽을 지역화합니다.



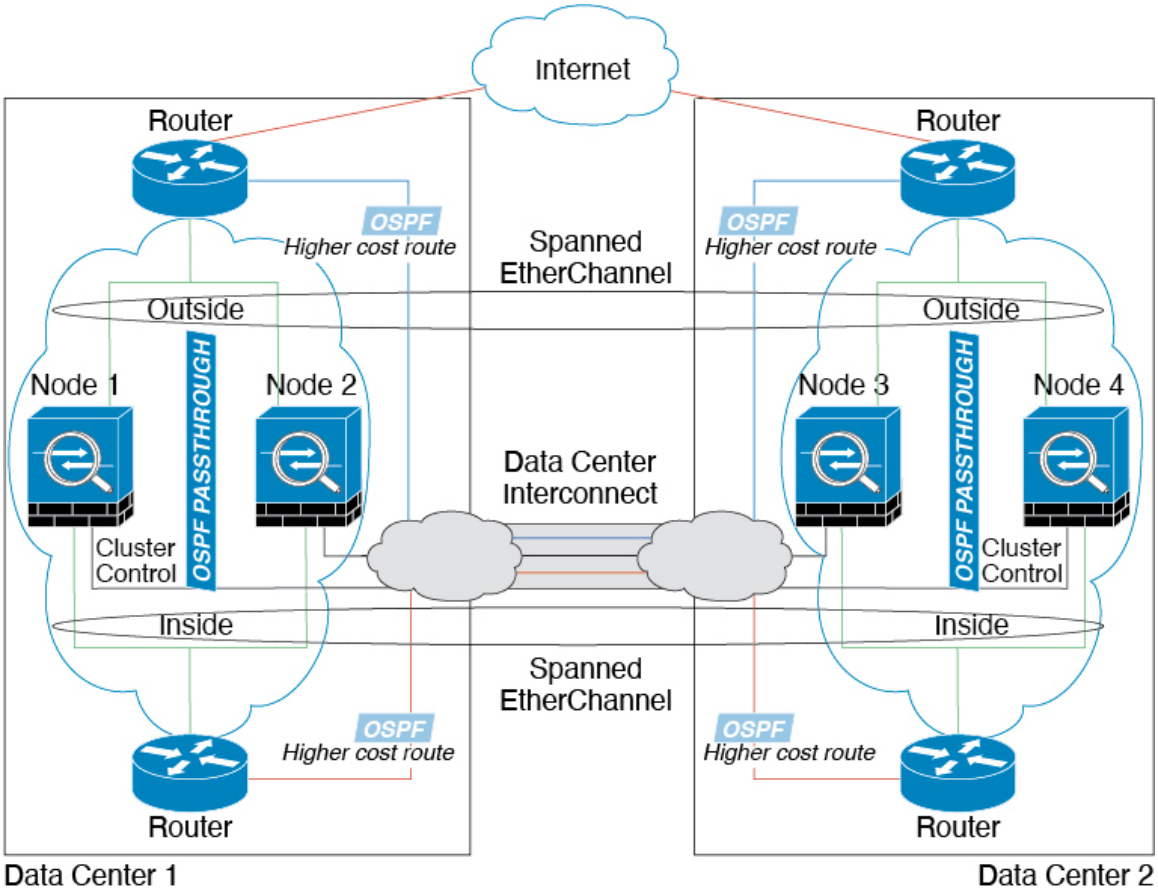
Spanned EtherChannel 투명 모드 노스-사우스 사이트 간의 예

다음 예에서는 내부 라우터와 외부 라우터의 사이에 위치한(노스-사우스 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버가 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부용 스팬 EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 섀시를 포괄합니다.

각 데이터 센터의 내부 및 외부 라우터에서는 투명 ASA를 통과하는 OSPF를 사용합니다. MAC과 달리 라우터 IP는 모든 라우터마다 고유합니다. DCI를 통해 비용이 높은 경로를 할당하면 특정 사이트의 모든 클러스터 멤버가 가동 중지되지 않는 한 각 데이터 센터 내에서 트래픽이 유지됩니다. ASA를 통과하는 비용이 낮은 경로의 경우, 클러스터의 각 사이트에 있는 같은 브리지 그룹을 거쳐 비대칭 연결을 유지해야 합니다. 어느 한 사이트의 모든 클러스터 멤버에 오류가 발생할 경우, 각 라우터의 트래픽은 DCI를 통해 다른 사이트의 클러스터 멤버로 이동합니다.

각 사이트의 스위치 구현 과정에는 다음 사항이 포함될 수 있습니다.

- 사이트 간 VSS, vPC, StackWise 또는 StackWise Virtual - 이 시나리오에서는 데이터 센터 1에 스위치 하나를 설치하고 데이터 센터 2에 다른 스위치를 설치합니다. 한 가지 옵션은 각 데이터 센터의 클러스터 노드가 로컬 스위치에만 연결하는 반면 중복 스위치 트래픽은 DCI를 통과하는 것입니다. 이 경우 연결의 대부분은 각 데이터 센터에 로컬로 저장됩니다. DCI에서 추가 트래픽을 처리할 수 있는 경우, 선택에 따라 각 노드를 DCI 전반의 스위치에 연결할 수 있습니다. 이 경우 트래픽이 데이터 센터 전반에 분산되므로 DCI의 성능이 매우 뛰어나야 합니다.
- 각 사이트의 로컬 VSS, vPC, StackWise 또는 StackWise Virtual - 더 나은 스위치 이중화를 위해 각 사이트에 2개의 개별 이중화 스위치 쌍을 설치할 수 있습니다. 이 경우 여전히 클러스터 노드의 Spanned EtherChannel은 두 로컬 스위치에만 연결된 데이터 센터 1 섀시 및 이러한 로컬 스위치에 연결된 데이터 센터 2 섀시로 이루어져 있지만, 사실상 Spanned EtherChannel은 "분리"되어 있습니다. 각 로컬 중복 스위치 시스템은 스팬 EtherChannel을 사이트 로컬 EtherChannel로 간주합니다.

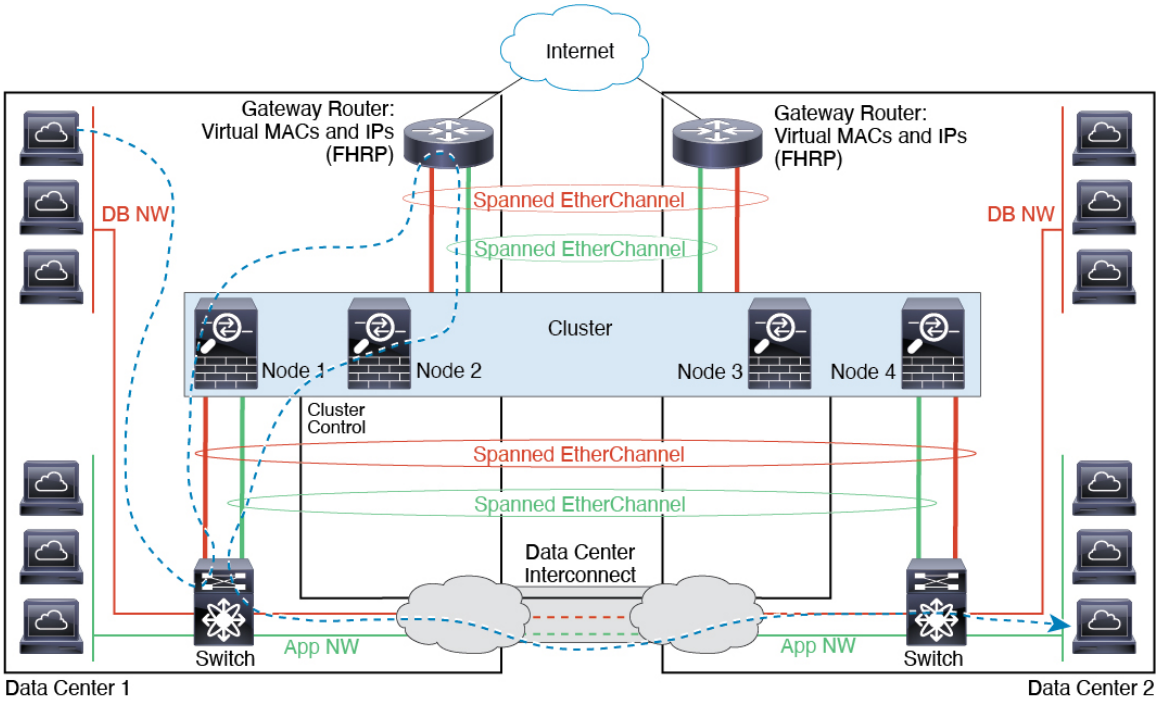


Spanned EtherChannel 투명 모드 이스트-웨스트 사이트 간의 예

다음 예에서는 게이트웨이 라우터와 각 사이트의 두 내부 네트워크, 즉 애플리케이션 네트워크 및 DB 네트워크의 사이에 위치한(이스트-웨스트 삽입) 2개 데이터 센터 각각에 2개의 클러스터 멤버가 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버

는 내부 및 외부에 있는 애플리케이션 및 DB 네트워크에 대한 스팬 EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 섀시를 포괄합니다.

각 사이트의 게이트웨이 라우터는 HSRP와 같은 FHRP를 사용하여 각 사이트에 동일한 목적지 가상 MAC 및 IP 주소를 제공합니다. 의도치 않은 MAC 주소 플래핑(flapping)을 피하는 좋은 방법은. 이러한 항목이 없으면, 사이트 1의 게이트웨이가 사이트 2의 게이트웨이와 통신할 경우 해당 트래픽이 ASA를 통과해 내부 인터페이스에서 사이트 2에 도달하려고 시도하여 문제를 일으킬 수 있습니다. OTV(Overlay Transport Virtualization) 또는 이와 유사한 방법으로 데이터 VLAN이 사이트 전반에 확장됩니다. 트래픽이 게이트웨이 라우터로 예정된 경우 트래픽에서 다른 사이트에 DCI를 전달하는 것을 방지하려면 필터를 추가해야 합니다. 한 개의 사이트에서 게이트웨이 라우터에 연결할 수 없는 경우, 필터를 제거해야 트래픽이 다른 사이트의 게이트웨이 라우터에 전송될 수 있습니다.



클러스터링에 대한 참조

이 섹션에는 클러스터링이 작동하는 방식에 대한 자세한 정보가 포함되어 있습니다.

ASA 기능 및 클러스터링

일부 ASA 기능은 ASA 클러스터링이 지원되지 않으며, 일부 기능은 제어 노드에서만 지원됩니다. 기타 기능의 경우 올바르게 사용하는 데 필요한 주의 사항이 있을 수 있습니다.

클러스터링으로 지원되지 않는 기능

이러한 기능은 클러스터링을 사용하도록 설정한 경우 구성할 수 없으며 명령이 거부됩니다.

- TLS 프록시를 사용하는 Unified Communication 기능

- 원격 액세스 VPN(SSL VPN 및 IPsec VPN)
- Virtual Tunnel Interface(VTI)
- IS-IS 라우팅
- 다음과 같은 애플리케이션 감시:
  - CTIQBE
  - H323, H225, RAS
  - IPsec 통과
  - MGCP
  - MMP
  - RTSP
  - SCCP(Skinny)
  - WAAS
  - WCCP
- 봇네트 트래픽 필터
- Auto Update Server
- DHCP 클라이언트, 서버, 프록시 DHCP 릴레이가 지원됩니다.
- VPN 로드 밸런싱
- 장애 조치
- 통합 라우팅 및 브리징
- DCD(데드 연결 탐지)
- FIPS mode(FIPS 모드)

클러스터링을 위한 중앙 집중식 기능

다음 기능은 제어 노드에서만 지원되며 클러스터에 확장되지 않습니다.

참고 중앙 집중식 기능의 트래픽은 클러스터 제어 링크를 통해 멤버 노드에서 제어 노드로 전달됩니다.

리밸런싱 기능을 사용할 경우, 중앙 집중식 기능의 트래픽은 트래픽이 중앙 집중식 기능으로 분류되기 전에 비 제어 노드로 리밸런싱될 수 있습니다. 이렇게 되면 해당 트래픽은 제어 노드로 다시 전송됩니다.

중앙 집중식 기능의 경우 제어 노드에 오류가 발생하면 모든 연결이 취소되며 새 제어 노드에서 연결을 다시 설정해야 합니다.

- 다음과 같은 애플리케이션 감시:
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- 고정 경로 모니터링
- 네트워크 액세스에 대한 인증 및 권한 부여. 어카운팅이 분산됨
- 필터링 서비스
- 사이트 간 VPN

  중앙 집중식 모드에서 VPN 연결은 클러스터의 제어 노드로만 설정됩니다. VPN 클러스터링의 기본 모드입니다. 사이트 간 VPN은 S2S IKEv2 VPN 연결이 노드 전체에 분산되어 있는 분산 VPN 모드에서도 구축될 수 있습니다.
- IGMP 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 플레인 포워딩은 클러스터 전체에 분산됨)
- PIM 멀티캐스트 컨트롤 플레인 프로토콜 처리(데이터 플레인 포워딩은 클러스터 전체에 분산됨)
- 동적 라우팅

개별 유닛에 적용되는 기능

이러한 기능은 전체 클러스터 또는 제어 노드가 아닌 각 ASA 노드에 적용됩니다.

- QoS — QoS 정책은 구성 복제의 일부로 클러스터 전체와 동기화됩니다. 그러나 정책은 각 노드에서 독립적으로 시행됩니다. 예를 들어, 출력에 대한 정책 시행을 구성할 경우 특정 ASA에 있는 트래픽에서 적응 속도 및 적응 버스트 값이 시행됩니다. 3개 노드로 구성되고 트래픽이 균일하게 분산된 클러스터의 경우, 적응 속도는 클러스터 속도의 3배가 됩니다.

- 위협 탐지 — 위협 탐지는 각 노드에서 독립적으로 작동됩니다. 예를 들어, 상위 통계는 노드별로 적용됩니다. 포트 검사 탐지 기능의 경우, 검사 트래픽이 모든 노드 간에 로드 밸런싱되고 한 노드에 모든 트래픽이 표시되지 않으므로 이 기능은 작동하지 않습니다.
- 리소스 관리 — 다중 상황 모드에서 리소스 관리는 로컬 사용량을 기준으로 각 노드에 개별적으로 시행됩니다.
- LISP 트래픽 — UDP 포트 4342의 LISP 트래픽은 각각의 수신 노드에서 검사되지만, 관리자는 할당되지 않습니다. 각 노드는 EDI 테이블에 추가되어 클러스터 전체에서 공유되지만, LISP 트래픽 자체는 클러스터 상태 공유에 참여하지 않습니다.

네트워크 액세스 및 클러스터링용 **AAA**

네트워크 액세스용 AAA는 인증, 권한 부여, 어카운팅이라는 세 가지 구성 요소로 이루어져 있습니다. 인증 및 권한 부여는 클러스터 데이터 노드에 대한 데이터 구조의 복제를 통해 클러스터링 제어 노드에서 중앙 집중식 기능으로 구현됩니다. 제어 노드가 선택된 경우, 새 제어 노드에서는 설정된 인증 완료 사용자 및 관련 인증 작업을 중단 없이 계속 가동하는 데 필요한 모든 정보를 보유하게 됩니다. 사용자 인증의 유휴 및 절대 시간 제한은 제어 노드가 변경될 경우 유지됩니다.

어카운팅은 클러스터에서 분산된 기능으로 구현됩니다. 어카운팅은 플로우 기준으로 수행되므로, 플로우에 대한 어카운팅이 구성되면 플로우를 소유한 클러스터 노드에서는 어카운팅 시작 및 중지 메시지를 AAA 서버에 보냅니다.

연결 설정

연결 제한은 클러스터 전체에서 시행됩니다(구성 > 방화벽 > 서비스 정책 페이지 참조). 각 노드에는 브로드캐스트 메시지를 기반으로 한 클러스터 전체의 카운터 값이 표시됩니다. 효율성을 고려하여 클러스터 전체에 구성된 연결 제한이 제한 수에 정확하게 적용되지 않을 수 있습니다. 각 노드는 언제든지 클러스터 전체 카운터 값을 과대 평가하거나 과소 평가할 수 있습니다. 그러나 로드 밸런싱된 클러스터에서는 시간이 지남에 따라 정보가 업데이트됩니다.

FTP 및 클러스터링

- 다른 클러스터 멤버가 FTP 데이터 채널 및 제어 채널의 플로우를 소유한 경우, 데이터 채널 소유자 유닛에서는 유휴 시간 제한 업데이트를 제어 채널 소유자에게 주기적으로 전송하고 유휴 시간 제한 값을 업데이트합니다. 그러나 제어 플로우 소유자가 다시 로드되고 제어 플로우가 다시 호스팅된 경우, 부모/자식 플로우 관계가 더 이상 유지되지 않으며 제어 플로우 유휴 시간 제한도 업데이트되지 않습니다.
- FTP 액세스용 AAA를 사용할 경우 제어 노드에서는 제어 채널 플로우를 중앙 집중화합니다.

ICMP 검사

클러스터를 통과하는 ICMP 및 ICMP 오류 패킷의 플로우는 ICMP/ICMP 오류 검사의 활성화 여부에 따라 달라집니다. ICMP 검사를 사용하지 않으면 ICMP는 단방향 플로우가며 관리자 플로우 지원이 없습니다. ICMP 검사를 사용하면 ICMP 플로우가 양방향이 되며, 관리자/백업 플로우에 의해 백업됩니다. 검사된 ICMP 플로우의 한 가지 차이점은 전달된 패킷의 관리자 처리에 있습니다. 관리자는 패킷을 전달자에게 반환하는 대신 ICMP 에코 응답 패킷을 플로우 소유자에게 전달합니다.

멀티캐스트 라우팅 및 클러스터링

제어 유닛에서는 fast-path 전달이 설정될 때까지 모든 멀티캐스트 라우팅 패킷과 데이터 패킷을 처리합니다. 연결이 설정되면 각 데이터 유닛에서 멀티캐스트 데이터 패킷을 전달할 수 있습니다.

NAT 및 클러스터링

NAT는 클러스터의 전체 처리량에 영향을 미칠 수 있습니다. 로드 밸런싱 알고리즘은 IP 주소와 포트를 기반으로 할 뿐만 아니라 NAT로 인해 인바운드 및 아웃바운드 패킷의 IP 주소 및/또는 포트가 서로 달라질 수 있으므로, 인바운드 및 아웃바운드 NAT 패킷을 클러스터의 다른 ASA에 전송할 수 있습니다. 패킷이 NAT 소유자가 아닌 ASA에 전달되면 해당 패킷은 클러스터 제어 링크를 통해 소유자에게 전달되며 이때 클러스터 제어 링크에 매우 많은 양의 트래픽이 발생합니다. 보안 및 정책 확인 결과에 따라 NAT 소유자가 패킷에 대해 연결을 생성하지 않을 수 있으므로 수신 노드는 소유자에 대한 전달 플로우를 생성하지 않습니다.

클러스터링에 NAT를 계속 사용하려면 다음 지침을 숙지하십시오.

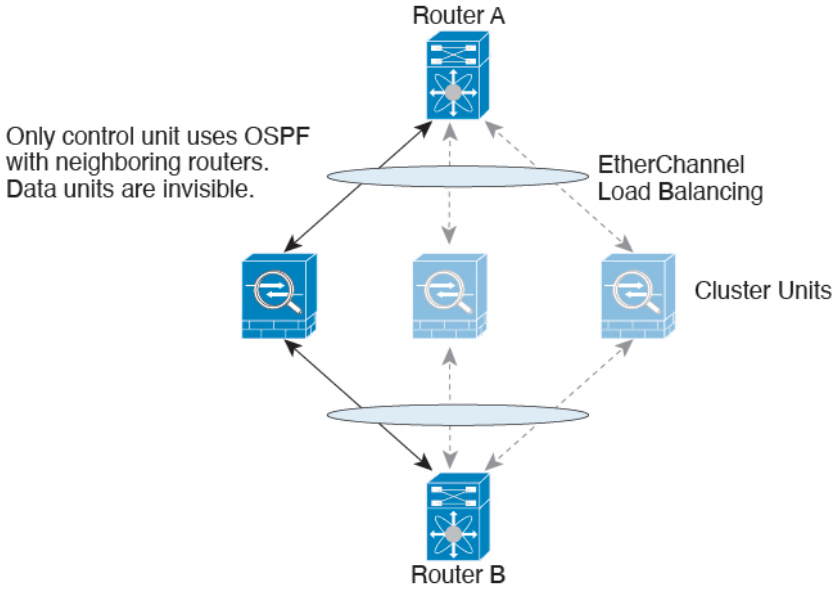
- 포트 블록 할당이 있는 PAT - 이 기능에 대한 다음 지침을 참조하십시오.
  - 호스트당 최대 제한은 클러스터 전체 제한이 아니며 각 노드에서 개별적으로 적용됩니다. 호스트당 최대 제한이 1로 구성된 3-노드 클러스터에서 호스트의 트래픽이 3개 노드 모두에 로드 밸런싱되는 경우 각 노드에 하나씩 3개의 블록이 할당될 수 있습니다.
  - 백업 풀의 백업 노드에서 생성된 포트 블록은 호스트당 최대 제한을 적용할 때 고려되지 않습니다.
  - 완전히 새로운 IP 범위로 PAT 풀을 수정하는 즉석 PAT 규칙 수정을 수행할 경우, 새 풀이 작동하게 되는 동안 여전히 전환 중이던 xlate 백업 요청에 대해 xlate 백업 생성이 실패하게 됩니다. 이러한 동작은 포트 블록 할당 기능과 관련이 없으며, 풀이 분산되고 트래픽이 클러스터 노드 전체에서 부하 분산되는 클러스터 구축 과정에서만 발생하는 일시적인 PAT 풀 문제입니다.
  - 클러스터에서 작업할 때는 단순히 블록 할당 크기를 변경할 수 없습니다. 새 크기는 클러스터에서 각 디바이스를 다시 로드한 후에만 적용됩니다. 각 디바이스를 다시 로드하지 않으려면 모든 블록 할당 규칙을 삭제하고 해당 규칙과 관련된 모든 xlate를 지우는 것이 좋습니다. 그런 다음 블록 크기를 변경하고 블록 할당 규칙을 다시 생성할 수 있습니다.
- 동적 PAT에 대한 NAT 풀 주소 분산 - PAT 풀을 구성하면 클러스터는 풀의 각 IP 주소를 포트 블록으로 나눕니다. 기본적으로 각 블록은 512포트이지만 포트 블록 할당 규칙을 구성하는 경우에는 블록 설정이 대신 사용됩니다. 이러한 블록은 클러스터의 노드 간에 균등하게 분산되므로 각 노드에는 PAT 풀의 각 IP 주소에 대해 하나 이상의 블록이 있습니다. 따라서 예상되는 PAT 처리된 연결 수에 충분한 경우 클러스터의 PAT 풀에 IP 주소를 하나만 포함할 수 있습니다. PAT 풀 NAT 규칙에 예약된 포트 1~1023을 포함하도록 옵션을 구성하지 않는 한 포트 블록은 1024~65535 포트 범위를 포함합니다.
- 여러 규칙에서 PAT 풀 재사용 - 여러 규칙에서 동일한 PAT 풀을 사용하려면 규칙에서 인터페이스 선택에 주의해야 합니다. 모든 규칙에서 특정 인터페이스를 사용하거나 또는 모든 규칙에서 "any(임의의)"를 사용해야 합니다. 규칙 전체에서 특정 인터페이스와 "any(임의의)"를 혼합할 수 없거나, 시스템에서 클러스터의 오른쪽 노드에 대한 반환 트래픽을 일치시키지 못할 수 있습니다. 규칙 당 고유한 PAT 풀을 사용하는 것은 가장 신뢰할 수 있는 옵션입니다.

- 라운드 로빈 없음 - 클러스터링에서는 PAT 풀을 위한 라운드 로빈을 지원하지 않습니다.
- 확장 PAT 없음 - 클러스터링에서 확장 PAT가 지원되지 않습니다.
- 제어 노드에 의해 관리되는 동적 NAT xlate - 제어 노드에서는 xlate 테이블을 유지하고 데이터 노드에 복제합니다. 동적 NAT가 필요한 연결이 데이터 노드에 전달되고 xlate가 테이블에 없을 경우, 제어 노드에서 xlate를 요청합니다. 데이터 노드에서는 이 연결을 소유합니다.
- 오래된 xlates - 연결 소유자의 xlate 유휴 시간이 업데이트되지 않습니다. 따라서 유휴 시간이 유휴 시간 제한을 초과할 수 있습니다. refcnt가 0인 구성된 시간 초과 값보다 큰 유휴 타이머 값은 오래된 xlate를 나타냅니다.
- Per-session PAT 기능 — 클러스터링에만 해당되는 것은 아니지만, 세Per-session PAT기능을 사용하면 PAT의 확장성이 개선되며 클러스터링을 수행할 때 각 데이터 노드에서 고유한 PAT 연결을 소유할 수 있게 됩니다. 이와 달리 multi-session PAT 연결은 제어 노드에 전달해야 하며 제어 노드에서 해당 연결을 소유하게 됩니다. 기본적으로 모든 TCP 트래픽 및 UDP DNS 트래픽은 세션 단위 PAT xlate를 사용하며, 여기서 ICMP 및 기타 모든 UDP 트래픽은 멀티 세션을 사용합니다. TCP 및 UDP에 대해 이러한 기본값을 변경하도록 세션 단위 NAT 규칙을 구성할 수 있지만, ICMP에 대해서는 세션 단위 PAT를 구성할 수 없습니다. 예를 들어, TCP/443을 통한 HTTPS TLS에 비해 최상의 성능 대안으로 UDP/443을 통한 Quic 프로토콜 사용이 증가함에 따라, UDP/443에 대해 세션별 PAT를 활성화해야 합니다. H.323, SIP, Skinny 등과 같이 다중 세션 PAT가 도움이 되는 트래픽의 경우 연결된 TCP 포트에 대해 세션 단위 PAT를 비활성화할 수 있습니다(이러한 H.323 및 SIP에 대한 UDP 포트는 기본적으로 이미 다중 세션임). 세션당 PAT에 대한 자세한 내용은 방화벽 설정 가이드를 참조하십시오.
- 다음을 검사할 수 있는 고정 PAT 없음
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 10,000개가 넘는 매우 많은 NAT 규칙이 있는 경우 디바이스 CLI에서 **asp rule-engine transactional-commit nat** 명령을 사용하여 트랜잭션 커밋 모델을 활성화해야 합니다. 그렇지 않으면 노드가 클러스터에 조인하지 못할 수 있습니다.

동적 라우팅 및 클러스터링

라우팅 프로세스는 제어 유닛에서만 실행되며, 경로는 제어 유닛을 통해 파악되고 보조 유닛에 복제됩니다. 라우팅 패킷이 데이터 유닛에 전송되면 해당 패킷은 제어 유닛에 리디렉션됩니다.

그림 2: 동적 라우팅



데이터 유닛이 제어 유닛에서 경로를 파악하면 각 유닛에서는 전달과 관련한 결정을 개별적으로 수행합니다.

OSPF LSA 데이터베이스는 제어 유닛에서 데이터 유닛으로 동기화되지 않습니다. 제어 유닛 전환이 있을 경우, 네이버 라우터에서 재시작을 감지하며 전환 작업은 투명하게 이루어지지 않습니다. OSPF 프로세스에서 IP 주소를 해당 라우터 ID로 선택합니다. 필수는 아니지만 고정 라우터 ID를 할당하면 클러스터 전반에 걸쳐 일관된 라우터 ID를 사용하도록 할 수 있습니다. 중단을 해결하려면 OSPF 무중단 전달 기능을 참조하십시오.

SCTP 및 클러스터링

로드 밸런싱으로 인해 모든 노드에서 SCTP 연결을 만들 수 있습니다. 멀티호밍 연결은 동일한 노드에 있어야 합니다.

SIP 검사 및 클러스터링

로드 밸런싱으로 인해 모든 노드에서 제어 플로우를 만들 수 있지만 하위 데이터 플로우는 동일한 노드에 상주해야 합니다.

TLS 프록시 구성은 지원되지 않습니다.

SNMP 및 클러스터링

SNMP 에이전트에서는 로컬 IP 주소로 각각의 개별 ASA를 폴링합니다. 클러스터의 통합 데이터는 폴링할 수 없습니다.

SNMP 폴링에는 기본 클러스터 IP 주소가 아닌 로컬 주소를 항상 사용해야 합니다. SNMP 에이전트에서 기본 클러스터 IP 주소를 폴링하면서 새 제어 노드가 선택된 경우, 새 제어 노드에 대한 폴링이 이루어지지 않습니다.

클러스터링과 함께 SNMPv3를 사용할 때 초기 클러스터 형성 후 새 클러스터 노드를 추가하면 SNMPv3 사용자가 새 노드에 복제되지 않습니다.사용자를 새 노드로 복제하거나 데이터 노드에서 직접 복제하려면 제어 노드에서 다시 추가해야 합니다.

STUN 및 클러스터링

STUN 검사는 핀홀이 복제될 때 장애 조치 및 클러스터 모드에서 지원됩니다. 그러나 트랜잭션 ID는 노드 간에 복제되지 않습니다. STUN 요청을 수신한 후 노드가 실패하고 다른 노드가 STUN 응답을 수신한 경우, STUN 응답은 삭제됩니다.

Syslog와 NetFlow 및 클러스터링

- Syslog - 클러스터의 각 노드에서는 고유한 syslog 메시지를 생성합니다. 각 노드에서 syslog 메시지 헤더 필드에 동일하거나 다른 디바이스 ID를 사용하도록 로깅을 구성할 수 있습니다. 예를 들어, 호스트 이름 구성은 클러스터의 모든 노드에 의해 복제 및 공유됩니다. 호스트 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, 모든 노드에서는 단일 노드에서 생성된 것처럼 보이는 syslog 메시지를 생성합니다. 클러스터 부트스트랩 구성에 할당된 로컬-노드 이름을 디바이스 ID로 사용하도록 로깅을 구성할 경우, syslog 메시지는 다른 노드에서 생성된 것처럼 보입니다.
- NetFlow — 클러스터의 각 노드에는 고유한 NetFlow 스트림이 있습니다. NetFlow 컬렉터에서는 각각의 ASA를 별도의 NetFlow 내보내기 디바이스로만 처리할 수 있습니다.

Cisco TrustSec 및 클러스터링

제어 노드에서만 보안 그룹 태그(SGT) 정보를 학습합니다. 그런 다음 제어 노드에서는 SGT를 데이터 노드에 제공하며, 데이터 노드에서는 보안 정책을 기준으로 SGT의 일치 여부를 결정할 수 있습니다.

Secure Firewall eXtensible 운영 체제(FXOS) 섀시에서의 VPN 및 클러스터링

ASA FXOS 클러스터는 중앙 집중식 또는 분산 S2S VPN에 함께 사용할 수 없는 다음 두 가지 모드 중 하나를 지원합니다.

- 중앙 집중식 VPN 모드. 기본 모드. 중앙 집중식 모드에서 VPN 연결은 클러스터의 제어 유닛으로만 설정됩니다.

  VPN 기능은 마스터 유닛에만 제한되며 클러스터 고가용성 기능을 사용하지 않습니다. 제어 유닛에 오류가 발생할 경우, 모든 기존 VPN 연결이 손실되며 VPN에 연결된 사용자에게는 서비스 중단 메시지가 표시됩니다. 새 제어 유닛이 선택되면 VPN 연결을 다시 설정해야 합니다.

  VPN 터널을 스팬 인터페이스 주소에 연결할 경우 연결이 제어 유닛에 자동으로 전달됩니다. VPN 관련 키 및 인증서는 모든 유닛에 복제됩니다.

- 분산 VPN 모드. 이 모드에서 S2S IPsec IKEv2 VPN 연결은 확장성을 제공하는 ASA 클러스터의 멤버 전체에서 분산됩니다. 클러스터 멤버 전체에서 VPN 연결을 분산시키면 클러스터의 용량 및 처리량 모두를 완전히 활용하며 특히 중앙 집중식 VPN 기능 이상으로 VPN 지원을 크게 확장합니다.

참고 중앙 집중식 VPN 클러스터링 모드는 S2S IKEv1 및 S2S IKEv2를 지원합니다.

분산 VPN 클러스터링 모드는 S2S IKEv2만 지원합니다.

분산 VPN 클러스터링 모드는 Firepower 9300에서만 지원됩니다.

원격 액세스 VPN은 중앙 집중식 또는 분산 VPN 클러스터링 모드에서 지원되지 않습니다.

성능 확장 요소

클러스터에 여러 유닛을 결합할 경우 총 클러스터 성능을 대략 최대 결합 처리량의 약 80%로 예측할 수 있습니다.

예를 들어 TCP 처리량의 경우 3개의 SM-40 모듈이 있는 Firepower 9300은 단독으로 실행하면 실제 방화벽 트래픽 중 약 135Gbps를 처리할 수 있습니다. 2개의 섀시의 경우 최대 통합 처리량은 270Gbps(2개 섀시 x 135Gbps)의 약 80%인 216Gbps입니다.

제어 유닛 선택

클러스터의 멤버는 클러스터 제어 링크로 통신을 수행하여 다음과 같은 방식으로 제어 '유닛을 선택합니다.

1. 클러스터를 구축할 때 각 유닛은 3초마다 선택 요청을 브로드캐스트합니다.
2. 다른 유닛의 우선순위가 더 높을 경우 해당 유닛이 선택 요청에 응답하게 됩니다. 우선순위는 클러스터를 구축할 때 설정되며 구성 불가능합니다.
3. 45초 후에 우선순위가 더 높은 다른 유닛에서 응답을 받지 못한 유닛은 제어 유닛이 됩니다.

참고 가장 우선순위가 높은 유닛이 공동으로 여러 개인 경우, 클러스터 유닛 이름과 일련 번호를 사용하여 제어 유닛을 결정합니다.

4. 유닛이 우선순위가 더 높은 클러스터에 참가한다고 해서 해당 유닛이 자동으로 제어 유닛이 되는 것은 아닙니다. 기존 제어 유닛은 응답이 중지되지 않는 한 항상 제어 유닛으로 유지되며 응답이 중지될 때에 새 제어 유닛이 선택됩니다.
5. 제어 유닛이 일시적으로 여러 개 있는 "스플릿 브레인" 시나리오에서는 우선 순위가 가장 높은 유닛이 역할을 유지하는 반면 다른 유닛은 데이터 유닛 역할로 돌아갑니다.

참고 유닛을 수동으로 강제 변경하여 제어 유닛이 되도록 할 수 있습니다. 중앙 집중식 기능의 경우 제어 유닛을 강제로 변경하면 모든 연결이 취소되며 새 제어 유닛에서 연결을 다시 설정해야 합니다.

클러스터 내의 고가용성

클러스터링에서는 섀시, 유닛 및 인터페이스의 상태를 모니터링하고 유닛 간의 연결 상태를 복제하여 고가용성을 제공합니다.

섀시 애플리케이션 모니터링

섀시 애플리케이션 상태 모니터링은 항상 활성화되어 있습니다. Firepower 4100/9300 섀시 수퍼바이저는 ASA 애플리케이션을 주기적으로(1초마다) 검사합니다. ASA가 작동 중인데 Firepower 4100/9300 섀시 수퍼바이저와 3초 동안 통신할 수 없는 경우, ASA에서는 syslog 메시지를 생성하고 클러스터를 떠납니다.

Firepower 4100/9300 섀시 수퍼바이저가 45초 후에 애플리케이션과 통신할 수 없는 경우, ASA를 다시 로드합니다. ASA가 수퍼바이저와 통신할 수 없는 경우, 클러스터에서 자신을 제거합니다.

유닛 상태 모니터링

각 유닛은 클러스터 제어 링크를 통해 브로드 캐스트 keepalive 하트 비트 패킷을 주기적으로 전송합니다. 제어 노드가 구성 가능한 시간 초과 기간 내에 데이터 노드에서 keepaliveheartbeat 패킷 또는 기타 패킷을 수신하지 않는 경우, 제어 노드는 클러스터에서 데이터 노드를 제거합니다. 데이터 노드가 제어 노드에서 패킷을 수신하지 않으면 나머지 노드에서 새 제어 노드가 선택됩니다.

네트워크 장애로 인해 노드가 실제로 장애가 발생한 것이 아니라 클러스터 제어 링크를 통해 노드가 서로 연결할 수 없는 경우, 클러스터는 격리된 데이터 노드가 자체 제어 노드를 선택하는 "스플릿 브레인" 시나리오로 전환될 수 있습니다. 예를 들어 두 클러스터 위치 간에 라우터가 실패하면 위치 1의 원래 제어 노드가 클러스터에서 위치 2 데이터 노드를 제거합니다. 한편, 위치 2의 노드는 자체 제어 노드를 선택하고 자체 클러스터를 구성합니다. 이 시나리오에서는 비대칭 트래픽이 실패할 수 있습니다. 클러스터 제어 링크가 복원되면 우선 순위가 더 높은 제어 노드가 제어 노드의 역할을 유지합니다. 자세한 내용은 제어 유닛 선택, 76 페이지를 참조하십시오.

인터페이스 모니터링

각 노드에서는 사용 중인 모든 하드웨어 인터페이스의 링크 상태를 모니터링하며 상태 변경 사항을 제어 노드에 보고합니다. 다중 섀시 클러스터링의 경우 Spanned EtherChannel은 클러스터 cLACP(Link Aggregation Control Protocol)를 사용합니다. 각 섀시에서는 링크 상태 및 cLACP 프로토콜 메시지를 모니터링하여 EtherChannel에서 포트가 아직 활성화된 상태인지 확인하고 인터페이스가 작동 중단 상태인지 ASA 애플리케이션에 정보를 제공합니다. 상태 모니터링을 활성화하면 기본적으로 물리적 인터페이스가 모니터링됩니다(EtherChannel 인터페이스에 대한 기본 EtherChannel 포함). 작동 상태인 명명된 인터페이스만 모니터링 대상이 될 수 있습니다. 예를 들어, EtherChannel의 모든 멤버 포트는 명명된 EtherChannel이 클러스터에서 제거되기 전에 장애가 발생해야 합니다(최소 포트 번들 설정에 따라). 선택적으로 인터페이스별 모니터링을 비활성화할 수 있습니다.

모니터링되는 인터페이스가 특정 노드에서 실패하지만 다른 노드에서는 활성 상태인 경우 해당 노드는 클러스터에서 제거됩니다. ASA에서 클러스터의 노드를 제거하기 전까지 걸리는 시간은 해당 노드가 설정된 멤버인지 또는 클러스터에 참가하는지에 따라 달라집니다. ASA에서는 노드가 클러스터에 참가하는 처음 90초 동안에는 인터페이스를 모니터링하지 않습니다. 이 시간 동안에는 인터페이스 상태가 변경되어도 ASA가 클러스터에서 제거되지 않습니다. 구성된 멤버의 경우 노드는 500밀리초 후에 제거됩니다.

다중 섀시 클러스터링의 경우 클러스터에서 EtherChannel을 추가 또는 삭제하는 경우 인터페이스 상태 모니터링은 각 섀시의 변경을 확인할 수 있도록 95초간 일시 중단됩니다.

데코레이터 애플리케이션 모니터링

인터페이스에서 Radware DefensePro 애플리케이션과 같은 데코레이터 애플리케이션을 설치하는 경우, ASA 및 데코레이터 애플리케이션 둘 다 클러스터에서 계속 작동해야 합니다. 유닛은 두 애플리케이션이 모두 작동할 때까지 클러스터에 참가하지 않습니다. 클러스터에 참가한 이후에 유닛은 3초마다 데코레이터 애플리케이션의 상태를 모니터링합니다. 데코레이터 애플리케이션이 작동하지 않으면 유닛이 클러스터에서 제거됩니다.

실패 이후 상태

클러스터의 노드에 오류가 발생할 경우, 해당 노드에서 호스팅하는 연결이 다른 노드로 원활하게 전송되며 트래픽에 대한 상태 정보가 제어 노드의 클러스터 제어 링크를 통해 공유됩니다.

제어 노드에 장애가 발생할 경우, 우선순위가 가장 높은(숫자가 가장 낮은) 클러스터의 다른 멤버가 제어 노드가 됩니다.

ASA는 실패 이벤트에 따라 클러스터에 다시 참가하려고 시도합니다.

참고 ASA가 비활성화되고 클러스터에 자동으로 다시 조인하지 못할 경우, 모든 데이터 인터페이스가 종료되며 관리 전용 인터페이스에서만 트래픽을 주고받을 수 있습니다. 관리 인터페이스에서는 클러스터 IP 풀에서 노드로 전송된 IP 주소를 사용하여 가동 상태를 유지합니다. 그러나 다시 로드해도 노드가 클러스터에서 여전히 비활성 상태인 경우 관리 인터페이스가 비활성화됩니다. 추가 구성을 위해서는 콘솔 포트를 사용해야 합니다.

클러스터 다시 참가

클러스터 멤버가 클러스터에서 제거된 후 해당 멤버가 클러스터에 다시 참가할 수 있는 방법은 처음에 제거된 이유에 따라 결정됩니다.

- 처음 참가 시 클러스터 제어 링크 장애 — 클러스터 제어 링크의 문제를 해결한 후에는 을 입력하여 클러스터링을 다시 활성화함으로써 클러스터에 수동으로 다시 참가해야 합니다.
- 클러스터 참가 후 클러스터 제어 링크 장애 — ASA에서는 자동으로 5분마다 무기한으로 다시 참가하려고 시도합니다. 이 동작은 구성 가능합니다.
- 데이터 인터페이스 장애 — ASA에서는 자동으로 5분, 10분, 마지막으로 20분 후에 다시 참가하도록 시도합니다. 20분 후에도 참가가 이루어지지 않을 경우 ASA에서는 클러스터링을 비활성화합니다. 데이터 인터페이스 문제를 해결한 후에는 ASA 콘솔 포트에서 **cluster group** *name*을 입력한 다음 .이 동작은 구성 가능합니다.
- 유닛 오류 — 유닛 상태 검사 오류로 인해 클러스터에서 유닛이 제거된 경우, 클러스터에 다시 참가할 수 있을지 여부는 오류의 원인에 따라 결정됩니다. 예를 들어, 일시적인 정전이 발생한 경우 클러스터 제어 링크가 작동 상태이면 전원을 다시 가동할 때 유닛이 클러스터에 다시 참가할 수 있습니다. 유닛은 5초마다 클러스터에 다시 참가하려고 시도합니다.

- 섀시 애플리케이션 통신 장애 — ASA에서 섀시 애플리케이션 상태가 복구되었는지 탐지할 경우, ASA에서는 클러스터에 즉시 다시 참가하려고 시도합니다. 또는 내부 오류에서와 동일한 다시 조인 설정을 사용하도록 ASA를 구성할 수 있습니다(아래 참조).
- 데코레이터 애플리케이션 장애 — ASA에서는 데코레이터 애플리케이션이 백업되었는지 감지할 경우 클러스터에 다시 참가합니다.
- 내부 오류 — 내부 장애 포함: 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등 유닛은 5분, 10분, 20분 간격으로 자동으로 클러스터에 다시 참가하려고 시도합니다. 이 동작은 구성 가능합니다.

데이터 경로 연결 상태 복제

모든 연결마다 클러스터 내에 하나의 소유자 및 최소 하나의 백업 소유자가 있습니다. 백업 소유자는 장애 발생 시 연결을 인계받는 대신 TCP/UDP 상태 정보를 저장하므로, 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있습니다. 백업 소유자는 일반적으로 관리자이기도 합니다.

일부 트래픽의 경우 TCP 또는 UDP 레이어 상위에 대한 상태 정보가 필요합니다. 클러스터링 지원에 대해 알아보거나 이러한 종류의 트래픽에 대한 지원이 부족한 경우 다음 표를 참조하십시오.

표 *2:* 클러스터 전반에 걸쳐 복제된 기능

트래픽	상태 지원	참고
가동 시간	예	시스템 가동 시간을 추적합니다.
ARP 테이블	예	—
MAC 주소 테이블	예	—
사용자 ID	예	AAA 규칙(uauth)을 포함하고합니다.
IPv6 네이버 데이터베이스	예	—
동적 라우팅	예	—
SNMP 엔진 ID	아니요	—
Firepower 4100/9300에 대한 분산 VPN(사이트 간)	예	백업 세션이 활성 세션이 되며 새 백업 세션이 생성됩니다.

클러스터에서 연결을 관리하는 방법

클러스터의 여러 노드에 대한 연결을 로드 밸런싱할 수 있습니다. 연결 역할은 정상적인 작동이 이루어지고 있고 가용성이 높은 상황에서 연결을 처리하는 방법을 결정합니다.

연결 역할

각 연결에 대해 정의된 다음 역할을 참조하십시오.

- 소유자 - 일반적으로 연결을 가장 처음 수신하는 노드입니다. 소유자 유닛에서는 TCP 상태를 유지하고 패킷을 처리합니다. 연결이 하나인 경우 소유자 유닛도 1개뿐입니다. 원래 소유자가 실패하고 새 노드가 연결에서 패킷을 수신하면, 관리자는 해당 노드로부터 새 소유자를 선택합니다.
- 백업 소유자 - 장애가 발생할 경우 연결이 새로운 소유자에게 원활하게 전송될 수 있도록 소유자로부터 수신한 TCP/UDP 상태 정보를 저장하는 노드입니다. 백업 소유자는 장애 발생 시 연결을 승계할 수 없습니다. 소유자를 사용할 수 없는 경우, 연결에서 (로드 밸런싱을 기준으로) 패킷을 받을 첫 번째 노드가 백업 소유자에 관련 상태 정보를 문의하면 해당 백업 소유자가 새로운 소유자가 될 수 있습니다.

  관리자(아래 설명 참조)는 소유자와 같은 노드가 아니라면 백업 소유자로도 사용됩니다. 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

  Firepower 9300의 클러스터링(섀시 하나에 클러스터 노드가 3개까지 포함될 수 있음)에서 백업 소유자가 소유자와 같은 섀시에 있으면 섀시 장애로부터 플로우를 보호하기 위해 다른 섀시에서 추가 백업 소유자가 선택됩니다.

  사이트 간 클러스터링에 대한 관리자 지역화를 활성화하는 경우에는 두 가지 백업 소유자 역할, 즉 로컬 백업 및 글로벌 백업이 있습니다. 소유자는 항상 자신과 동일한 사이트의 로컬 백업을 선택합니다(사이트 ID 기반). 글로벌 백업은 어느 사이트에든 있을 수 있으며, 로컬 백업과 동일한 노드일 수도 있습니다. 소유자는 연결 상태 정보를 두 백업에 모두 전송합니다.

  사이트 이중화를 활성화하는 경우 백업 소유자가 소유자와 같은 사이트에 있으면 사이트 장애로부터 플로우를 보호하기 위해 다른 사이트에서 추가 백업 소유자가 선택됩니다. 섀시 백업 및 사이트 백업은 서로 독립적이므로 경우에 따라서는 플로우에 섀시 백업과 사이트 백업이 모두 포함됩니다.
- 관리자 - 전달자의 소유자 조회 요청을 처리하는 노드입니다. 소유자가 새 연결을 수신할 경우, 소유자 노드에서는 소스/대상 IP 주소와 포트의 해시를 기준으로 관리자를 선택하며 관리자에 메시지를 전송하여 새 연결을 등록합니다(아래에서 ICMP 해시 세부 정보 참조). 패킷이 소유자가 아닌 다른 노드에 전달될 경우, 해당 노드는 관리자에 어떤 노드가 소유자인지 조회하여 패킷이 전달될 수 있도록 합니다. 연결이 하나인 경우 관리자 유닛도 1개뿐입니다. 관리자가 실패하면 소유자는 새 관리자를 선택합니다.

  관리자는 소유자와 같은 노드가 아니면 백업 소유자로도 사용됩니다(위의 설명 참조). 소유자가 자신을 디렉터로 선택하면 별도의 백업 소유자가 선택됩니다.

  사이트 간 클러스터링에 대한 관리자 지역화를 활성화하는 경우에는 두 가지 관리자 역할, 즉 로컬 관리자와 전역 관리자가 있습니다. 소유자는 항상 자신과 동일한 사이트의 로컬 관리자를 선택합니다(사이트 ID 기반). 전역 관리자는 어느 사이트에든 있을 수 있으며, 로컬 관리자와 동일한 노드일 수도 있습니다. 원래 소유자가 실패하면 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다.

  ICMP/ICMPv6 해시 세부 정보:

  - 에코 패킷의 경우 소스 포트는 ICMP 식별자이고, 대상 포트는 0입니다.
  - 응답 패킷의 경우 소스 포트는 0이고, 대상 포트는 ICMP 식별자입니다.
  - 기타 패킷의 경우 소스 및 대상 포트가 모두 0입니다.

- 전달자 - 패킷을 소유자에 전달하는 노드입니다. 소유하지 않은 연결 패킷이 전달자 유닛에 수신될 경우, 전달자 유닛에서는 소유자 유닛의 관리자를 조회한 다음 이러한 연결을 수신하는 기타 모든 패킷의 소유자에 대한 플로우를 설정합니다. 관리자 유닛은 전달자가 될 수도 있습니다. 관리자 지역화를 활성화하면, 전달자는 항상 로컬 관리자를 쿼리합니다. 전달자는 로컬 관리자가 소유자를 모르는 경우에만 전역 관리자를 쿼리합니다. 클러스터 멤버가 다른 사이트의 소유인 연결에 대한 패킷을 수신하는 경우를 예로 들 수 있습니다. 전달자 유닛에서 SYN-ACK 패킷을 수신할 경우, 패킷의 SYN 쿠키에서 소유자를 직접 파생할 수 있으므로 관리자 유닛에 조회하지 않아도 됩니다. (TCP 시퀀스 임의 설정을 비활성화한 경우 SYN 쿠키는 사용되지 않으며, 책임자에게 쿼리해야 합니다.) DNS 및 ICMP 같이 짧은 플로우의 경우 쿼리 대신 전달자가 책임자에게 패킷을 즉시 전송하고 책임자가 소유자에게 전송합니다. 하나의 연결에 여러 개의 전달자 유닛이 있을 수 있습니다. 가장 효율적인 처리량 목표를 실현하려면 전달자가 없고 연결의 모든 패킷이 소유자 유닛에 전송되는 우수한 로드 밸런싱 방법을 사용합니다.

참고 클러스터링을 사용할 때는 TCP 시퀀스 임의 설정을 비활성화하지 않는 것이 좋습니다. SYN/ACK 패킷이 삭제될 수 있으므로 일부 TCP 세션이 설정되지 않을 가능성이 적습니다.

- 프래그먼트 소유자 - 프래그먼트화된 패킷의 경우 프래그먼트를 수신하는 클러스터 노드가 프래그먼트 소스 IP 주소, 대상 IP 주소 및 패킷 ID의 해시를 사용하여 프래그먼트 소유자를 결정합니다. 그런 다음 모든 프래그먼트가 클러스터 제어 링크를 통해 프래그먼트 소유자에게 전달됩니다. 첫 번째 프래그먼트만 스위치 로드 밸런싱 해시에 사용되는 5 튜플을 포함하기 때문에 프래그먼트는 다른 클러스터 노드로 로드 밸런싱될 수 있습니다. 다른 프래그먼트는 소스 및 대상 포트를 포함하지 않으며 다른 클러스터 노드에 로드 밸런싱될 수 있습니다. 프래그먼트 소유자는 패킷을 일시적으로 리어셈블하므로 소스/대상 IP 주소 및 포트의 해시를 기반으로 디렉터를 확인할 수 있습니다. 새 연결인 경우 프래그먼트 소유자가 연결 소유자로 등록됩니다. 기존 연결인 경우 프래그먼트 소유자는 클러스터 제어 링크를 통해 모든 프래그먼트를 제공된 연결 소유자에게 전달합니다. 그러면 연결 소유자가 모든 프래그먼트를 리어셈블합니다.

포트 주소 변환 연결

연결에 PAT(Port Address Translation)가 사용되는 경우, PAT 유형(per-session 또는 multi-session)이 클러스터의 어떤 멤버가 새 연결의 소유자가 될지에 영향을 미칩니다.

- Per-session PAT(세션 단위 PAT) - 연결에서 초기 패킷을 수신하는 노드가 소유자입니다.

  기본적으로 TCP 및 DNS UDP 트래픽은 per-session PAT를 사용합니다.

- Multi-session PAT(다중 세션 PAT) - 항상 제어 노드가 소유자입니다. multi-session PAT 연결이 초기에 데이터 노드에서 수신되면 데이터 노드는 해당 연결을 제어 노드로 전달합니다.

  기본적으로 UDP(DNS UDP 제외) 및 ICMP 트래픽은 multi-session PAT를 사용하므로, 항상 제어 노드에서 해당 연결을 소유합니다.

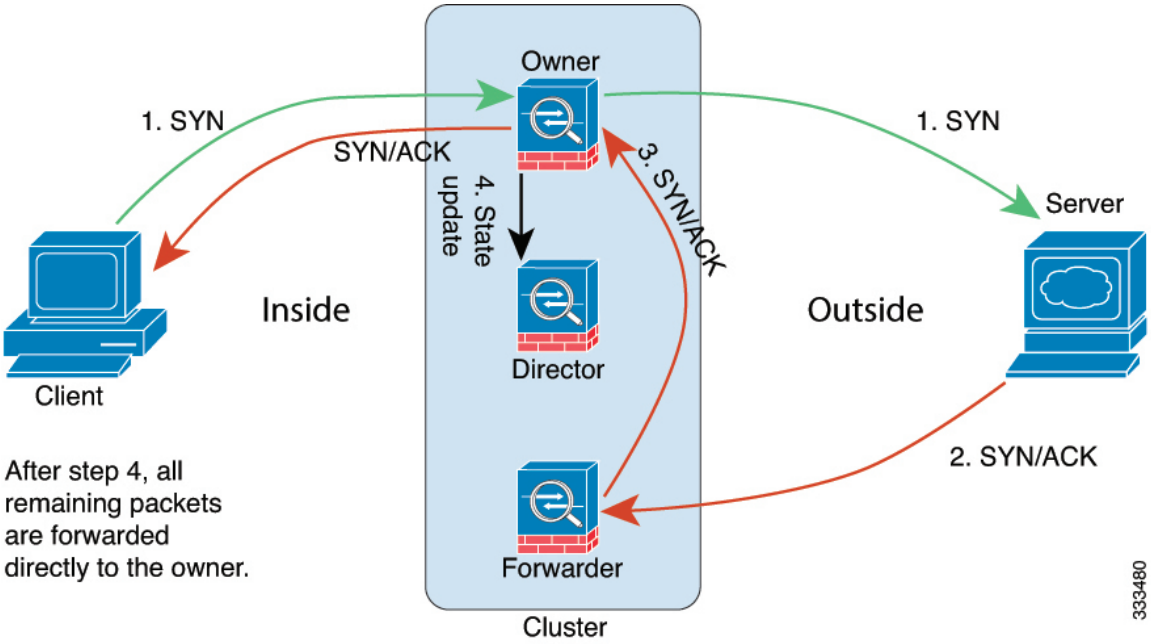
TCP 및 UDP에 대한 per-session PAT 기본값을 변경하여, 이러한 프로토콜에 대한 연결이 구성에 따라 세션 단위 또는 다중 세션으로 처리되도록 할 수 있습니다. ICMP의 경우 기본 multi-session PAT에서 변경할 수 없습니다. 세션당 PAT에 대한 자세한 내용은 방화벽 설정 가이드를 참조하십시오.

새 연결 소유권

로드 밸런싱을 통해 클러스터의 노드에 새 연결이 전송될 경우, 해당 노드에서는 연결의 양방향을 모두 소유합니다. 다른 노드에 연결 패킷이 전송될 경우, 해당 패킷은 클러스터 제어 링크를 통해 소유자 노드에 전달됩니다. 다른 노드에 반대 방향의 흐름이 전송될 경우, 이는 원래 노드로 다시 리디렉션됩니다.

TCP에 대한 샘플 데이터 플로우

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.



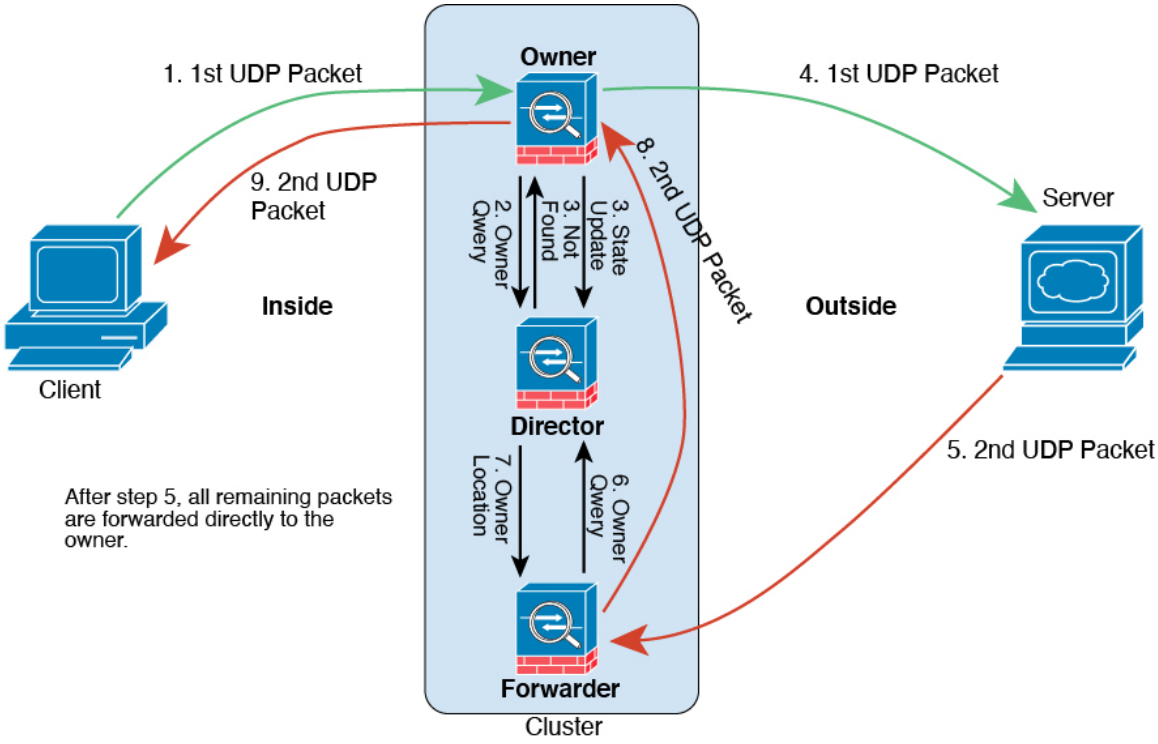
1. SYN 패킷은 클라이언트에서 시작되고 ASA에 전달(로드 밸런싱 방법을 기준으로)되며, 이 유닛이 소유자 유닛이 됩니다. 소유자 유닛에서는 플로우를 생성하고, 소유자 정보를 SYN 쿠키로 인코딩하며, 패킷을 서버에 전달합니다.
2. SYN-ACK 패킷은 서버에서 시작되고 다른 ASA에 전달(로드 밸런싱 방법을 기준으로)됩니다. 이 ASA는 전달자 유닛입니다.
3. 전달자 유닛에서는 연결을 소유하지 않으므로 SYN 쿠키에서 소유자 정보를 디코딩하고, 소유자에 대한 전달 플로우를 생성하며, SYN-ACK를 소유자 유닛에 전달합니다.
4. 소유자 유닛에서는 관리자 유닛에 상태 업데이트를 보내고, SYN-ACK를 클라이언트에 전달합니다.
5. 관리자 유닛에서는 소유자 유닛을 통해 상태 업데이트를 수신하고, 소유자에 대한 플로우를 생성하며, TCP 상태 정보는 물론 소유자를 기록합니다. 관리자 유닛은 연결의 백업 소유자 역할을 수행합니다.
6. 전달자 유닛에 전달된 모든 후속 패킷은 소유자 유닛에 전달됩니다.
7. 패킷이 추가 노드에 전달된 경우, 관리자에 쿼리하고 플로우를 설정합니다.

8. 플로우 결과의 상태가 변경되면 소유자 유닛과 관리자 유닛의 상태도 업데이트됩니다.

ICMP 및 UDP의 샘플 데이터 플로우

다음 예에는 새 연결을 설정하는 방법이 나와 있습니다.

1. 그림 *3: ICMP* 및 *UDP* 데이터 플로우



첫 번째 UDP 패킷은 클라이언트에서 시작되고 (로드 밸런싱 방법을 기준으로) ASA에 전달됩니다.

2. 첫 번째 패킷을 수신한 노드는 소스/대상 IP 주소 및 포트의 해시를 기반으로 선택된 관리자 노드에 쿼리합니다.
3. 관리자는 기존 플로우를 찾지 못하고 관리자 플로우를 생성하며 이전 노드로 패킷을 다시 전달합니다. 즉, 관리자가 이 플로우의 소유자를 선택했습니다.
4. 소유자가 플로우를 생성하고 관리자에게 상태 업데이트를 보내고 서버에 패킷을 전달합니다.
5. 두 번째 UDP 패킷은 서버에서 시작되어 전달자에게 전달됩니다.
6. 전달자는 관리자에게 소유권 정보를 쿼리합니다. DNS와 같이 짧은 플로우의 경우 쿼리하는 대신 전달자가 관리자에게 패킷을 즉시 전송하고 관리자가 소유자에게 전송합니다.
7. 관리자는 전달자에게 소유권 정보를 회신합니다.
8. 전달자는 전달 플로우를 생성하여 소유자 정보를 기록하고 소유자에게 패킷을 전달합니다.
9. 소유자는 패킷을 클라이언트에 전달합니다.

클러스터 전반에 걸쳐 새 **TCP** 연결 리밸런싱

업스트림 또는 다운스트림 라우터의 로드 밸런싱 기능을 사용하는 도중 흐름이 균일하게 분산되지 않을 경우, 초당 신규 연결 수가 더 많은 노드가 새 TCP 흐름을 다른 노드로 리디렉션하도록 신규 연결 재분산 기능을 구성할 수 있습니다. 기존 흐름은 다른 노드로 이동되지 않습니다.

이 명령은 초당 연결 수를 기반으로만 리밸런싱되므로 각 노드에 설정된 총 연결 수는 고려되지 않으며 총 연결 수가 동일하지 않을 수 있습니다.

연결이 다른 노드로 오프로드되면 비대칭 연결이 됩니다.

사이트 간 토폴로지에 대한 연결 리밸런싱을 구성하지 마십시오. 이렇게 할 경우 다른 사이트의 클러스터 멤버에 대한 새 연결이 리밸런싱됩니다.

ASA 클러스터링에 대한 기록 - Firepower 4100/9300

기능 이름	버전	기능 정보
데이터 노드는 동시에 클러스터에 조인 가능	9.24(1)	이전에는 제어 노드 한 번에 하나의 데이터 노드만 클러스터에 조인할 수 있었습니다. 구성 동기화에 시간이 오래 걸리면 데이터 노드를 조인하는 데 시간이 오래 걸릴 수 있습니다. 동시 조인은 기본적으로 활성화되어 있습니다. NAT 및 VPN 분산 모드가 활성화된 경우 동시 조인을 사용할 수 없습니다. 추가/수정된 화면: • **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availablility and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** • **Monitoring(**모니터링**)** > **ASA Cluster(ASA** 클러스터**)** > **ASA Cluster Concurrent Join(ASA** 클러스터 동시 조인**)**
클러스터 노드 조인 시 MTU ping 테스트는 더 작은 MTU 값으로도 시도해 봄으로써 더 많은 정보를 제공합니다.	9.24(1)	노드가 클러스터에 조인하면 클러스터 제어 링크 MTU와 일치하는 패킷 크기로 제어 노드에 ping을 전송하여 MTU 호환성을 확인합니다. ping에 실패하면 MTU를 2로 나누려고 시도하고 MTU ping이 성공할 때까지 2로 계속 나눕니다. 성공적인 ping 값은 MTU를 작동하는 값으로 고정하고 다시 시도할 수 있도록 **show cluster info trace**에 표시됩니다. ping이 실패하더라도 노드는 클러스터에 조인할 수 있습니다. 이 경우 최대한 빨리 MTU 불일치를 해결해야 합니다. MTU 크기를 권장 값으로 늘리는 것이 좋지만 스위치 구성을 변경할 수 없는 경우 클러스터 제어 링크에 대해 작동하는 값을 사용하여 클러스터를 구성할 수 있습니다. 추가/수정된 화면: **Monitoring(**모니터링**) >** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Summary(**클러스터 요약**)**
CPU가 높은 향상된 클러스터 제어 링크 상태 확인	9.24(1)	클러스터 노드 CPU 사용량이 높으면 상태 확인이 일시 중단되고 노드가 비정상으로 표시되지 않습니다. 상태 확인을 일시 중단하기 위한 CPU 사용 임계값을 구성할 수 있습니다. 추가/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availablility and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)**

기능 이름	버전	기능 정보
분산형 사이트 간 VPN 모드에 대한 동적 PAT 지원	9.24(1)	이제 분산형 모드에서 동적 PAT를 지원합니다. 그러나 인터페이스 PAT는 아직 지원되지 않습니다.
노드 조인 시 데이터 노드의 MTU ping 테스트	9.22(1)	노드가 클러스터에 조인하면 클러스터 제어 링크 MTU와 일치하는 패킷 크기로 제어 노드에 ping을 전송하여 MTU 호환성을 확인합니다. 이전에는 제어 노드에서만 ping을 전송했습니다. ping에 실패하면 알림이 생성되어 연결 스위치에서 MTU 불일치를 수정하고 다시 시도할 수 있습니다. 추가/수정된 화면: **Monitoring(**모니터링**) >** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Summary(**클러스터 요약**)**
섀시 하트비트 장애 후 클러스터 다시 조인하기 위해 구성 가능한 지연(Firepower 4100/9300)	9.20(2)	기본적으로 섀시 하트비트에 장애가 발생한 다음 복구되면 노드 클러스터에 즉시 다시 조인합니다. 그러나 **health-check chassis-heartbeat-delay-rejoin** 명령을 구성하는 경우 **health-check system auto-rejoin** 명령의 설정에 따라 다시 조인됩니다. 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Auto Rejoin(**자동 다시 조인**)**
플로우 상태에 대해 구성 가능한 클러스터 keepalive 간격	9.20(1)	플로우 소유자는 관리자 및 백업 소유자에게 keepalive(clu_keepalive 메시지)와 업데이트(clu_update 메시지)를 전송하여 플로우 상태를 새로 고칩니다. 이제 keepalive 간격을 설정할 수 있습니다. 기본값은 15초이며 15~55초 사이의 간격을 설정할 수 있습니다. 클러스터 제어 링크의 트래픽 양을 줄이기 위해 이 간격을 더 길게 설정할 수 있습니다. 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)**
편향된 언어 제거	9.19(1)	"Master" 및 "Slave"라는 용어가 포함된 명령, 명령 출력 및 시스템 로그 메시지가 "Control" 및 "Data"로 변경되었습니다. 신규/수정된 명령: **cluster control-nodeenable as-data-nodepromptshow cluster historyshow cluster info**
Firepower 4100/9300에서 클러스터링을 위한 개선된 PAT 포트 블록 할당	9.16(1)	개선된 PAT 포트 블록 할당을 통해 제어 유닛은 노드를 조인하기 위해 포트를 예약 상태로 유지하고 사용되지 않는 포트를 사전에 회수합니다. 할당을 최적화하기 위해 **cluster-member-limit** 명령을 사용하여 클러스터에 포함할 최대 노드를 설정할 수 있습니다. 그러면 제어 유닛은 계획된 노드 수에 포트 블록을 할당할 수 있으며, 사용하지 않을 추가 노드에 대해 포트를 예약할 필요가 없습니다. 기본값은 16 노드입니다. syslog 747046을 모니터링하여 새 노드에 사용할 수 있는 포트가 충분한지 확인할 수도 있습니다. 신규/수정된 화면 **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)** > **Cluster Member Limit(**클러스터 멤버 제한**)** 필드

기능 이름	버전	기능 정보
show cluster history 명령 개선 사항	9.16(1)	**show cluster history** 명령에 대한 추가 출력을 추가했습니다. 신규/수정된 명령: **show cluster history brief**, **show cluster history latest**, **show cluster history reverse**, **show cluster history time**
노드 조인에 대한 제어 노드의 MTU ping 테스트	9.16(1)	노드가 클러스터에 조인하면 제어 노드는 클러스터 제어 링크 MTU의 두 배 크기 패킷으로 데이터 노드에 ping을 전송하여 MTU 호환성을 확인합니다. ping에 실패하면 알림이 생성되어 연결 스위치에서 MTU 불일치를 수정하고 다시 시도할 수 있습니다. 추가/수정된 화면: **Monitoring(**모니터링**) >** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Summary(**클러스터 요약**)**
병렬로 데이터 유닛에 구성 동기화	9.14(1)	제어 유닛은 이제 기본적으로 구성 변경 사항을 데이터 유닛과 동시에 동기화합니다. 이전에는 동기화가 순차적으로 발생했습니다. 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)** > **Enable parallel configuration replicate(**병렬 구성 복제 활성화**)** 확인란
클러스터 가입 실패 또는 제거에 대한 메시지가 추가됨 **show cluster history**	9.14(1)	클러스터 유닛이 클러스터에 조인하지 못하거나 클러스터를 떠나는 경우를 위한 새 메시지가 **show cluster history** 명령에 추가되었습니다. 신규/수정된 명령: **show cluster history** 신규/수정된 화면: 없음
DCD(Dead Connection Detection)의 이니시에이터 및 응답자 정보와, 클러스터에서의 DCD 지원입니다.	9.13(1)	DCD(Dead Connection Detection)를 활성화하면, **show conn detail** 명령을 이용해 이니시에이터 및 응답자 정보를 얻을 수 있습니다. DCD(Dead Connection Detection)를 이용하면 비활성 연결을 유지할 수 있으며, **show conn** 출력은 엔드포인트를 얼마나 자주 조사했는지 알려줍니다. 또한 이제 DCD는 클러스터에서도 지원됩니다. 수정된 화면이 없습니다.
클러스터의 트래픽 로드 모니터링	9.13(1)	이제 총 연결 수, CPU 및 메모리 사용량, 버퍼 삭제를 포함한 클러스터 멤버의 트래픽 로드를 모니터링할 수 있습니다. 로드가 너무 높은 경우 나머지 유닛이 로드를 처리할 수 있는 경우 유닛에서 클러스터링을 수동으로 비활성화하도록 선택하거나 외부 스위치의 로드 밸런싱을 조정할 수 있습니다. 이 기능은 기본적으로 활성화되어 있습니다. 신규/수정된 화면: • **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)** > **Enable Cluster Load Monitor(**클러스터 로드 모니터 활성화**)** 확인란 • **Monitoring(**모니터링**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Load-Monitoring(**클러스터 로드 모니터링**)**

기능 이름	버전	기능 정보
가속화된 클러스터 참가	9.13(1)	데이터 유닛의 구성이 제어 유닛의 구성과 동일한 경우, 구성 동기화를 건너뛰고 더 빨리 조인합니다. 이 기능은 기본적으로 활성화되어 있습니다. 이 기능은 각 유닛에서 구성되며 제어 유닛에서 데이터 유닛으로 복제되지 않습니다. 참고 일부 구성 명령은 가속화된 클러스터 참가와 호환되지 않습니다. 이러한 명령이 유닛에 존재하는 경우, 가속화된 클러스터 참가가 활성화된 경우에도 구성 동기화가 항상 발생합니다. 가속화된 클러스터 참가가 작동하려면 호환되지 않는 구성을 제거해야 합니다. 호환되지 않는 구성을 보려면 **show cluster info unit-join-acceleration incompatible-config**를 사용합니다. 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)** > **Enable config sync acceleration(config** 동기화 가속 활성화**)** 확인란
클러스터링을 위한 사이트별 Gratuitous ARP	9.12(1)	ASA는 이제 스위칭 인프라를 최신 상태로 유지하기 위해 Gratuitous ARP(GARP) 패킷을 생성합니다. 각 사이트에서 가장 높은 우선 순위를 지닌 멤버는 정기적으로 전역 MAC/IP 주소에 대한 GARP 트래픽을 생성합니다. 사이트별 MAC 및 IP 주소를 사용할 때 클러스터에서 온 패킷은 사이트별 MAC 주소 및 IP 주소를 사용하는 반면 클러스터가 수신한 패킷은 전역 MAC 주소 및 IP 주소를 사용합니다. 트래픽이 전역 MAC 주소에서 정기적으로 생성되지 않는 경우, 전역 MAC 주소에 대한 스위치에서 MAC 주소 시간 초과가 발생할 수 있습니다. 시간 초과 후에 전역 MAC 주소로 향하는 트래픽이 전체 스위칭 인프라를 통해 플러딩되어 성능 및 보안 문제를 유발할 수 있습니다. GARP는 각 Spanned EtherChannel에 대한 각 유닛 및 사이트 MAC 주소용 사이트 ID를 설정할 때 기본적으로 활성화되어 있습니다. 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)** > **Site Periodic GARP(**사이트 주기적 **GARP)** 필드
Firepower 9300 섀시당 유닛의 병렬 클러스터 참가	9.10(1)	Firepower 9300에서는 이 기능을 통해 섀시에서 보안 모듈이 클러스터에 동시에 참가하게 되므로 트래픽이 모듈 간에 고르게 분산됩니다. 모듈이 다른 모듈보다 훨씬 먼저 참가하는 경우, 다른 모듈이 로드를 아직 공유할 수 없기 때문에 이 모듈은 원하는 트래픽보다 더 많은 트래픽을 받을 수 있습니다. 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** 신규/수정된 옵션: **Parallel Join of Units Per Chassis(**섀시당 유닛의 병렬 참가**)** 영역

기능 이름	버전	기능 정보
Firepower 4100/9300에 대한 클러스터 제어 링크 사용자 정의 가능한 IP 주소	9.10(1)	기본적으로 클러스터 제어 링크는 127.2.0.0/16 네트워크를 사용합니다. 이제 FXOS에서 클러스터를 구축하는 경우 네트워크를 설정할 수 있습니다. 섀시에서는 섀시 ID 및 슬롯 ID 127.2.*chassis_id*.*slot_id*를 기준으로 하여 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동 생성합니다. 그러나 일부 네트워킹 구축에서는 127.2.0.0/16 트래픽 통과를 허용하지 않습니다. 따라서 이제 FXOS에서 루프백(127.0.0.0/8) 및 멀티캐스트(224.0.0.0/4) 주소를 제외하고 클러스터 제어 링크의 맞춤형 /16 서브넷을 설정할 수 있습니다. 신규/수정된 Firewall Chassis Manager 화면: **Logical Devices(**논리적 디바이스**)** > **Add Device(**디바이스 추가**)** > **Cluster Information(**클러스터 정보**)** 신규/수정된 옵션: **CCL Subnet IP(CCL** 서브넷 **IP)** 필드
이제 클러스터 인터페이스 디바운스 시간이 가동 중단 상태에서 가동 상태로 변경되는 인터페이스에 적용됩니다.	9.10(1)	인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA에서는 **health-check monitor-interface debounce-time** 명령 또는 ASDM **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** 화면에 지정되어 있는 밀리초 동안 대기합니다. 이제 이 기능이 가동 중단 상태에서 가동 상태로 변경되는 인터페이스에 적용됩니다. 예를 들어 가동 중단 상태에서 가동 상태로 전환되는 EtherChannel의 경우(예: 스위치 다시 로드됨 또는 EtherChannel에서 스위치 활성화됨), 디바운스 시간이 더 길어 다른 클러스터 유닛이 포트 번들링 시 더 빨랐다는 이유만으로 인터페이스가 클러스터 유닛에서 실패한 것으로 표시되는 것을 방지할 수 있습니다. 화면은 수정하지 않았습니다.
내부 장애 발생 후 클러스터에 자동으로 다시 참가	9.9(2)	이전에는 많은 오류 상태로 인해 클러스터에서 클러스터 유닛이 제거되었으며 문제를 해결한 후에 클러스터에 수동으로 다시 참가해야 했습니다. 이제 유닛은 기본적으로 5분, 10분, 20분 간격으로 자동으로 클러스터에 다시 참가하려고 시도합니다. 이러한 값은 구성할 수 있습니다. 내부 장애로는 애플리케이션 동기화 시간 초과, 일치하지 않는 애플리케이션 상태 등이 있습니다. 신규 또는 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Auto Rejoin(**자동 다시 참가**)**
클러스터의 신뢰할 수 있는 전송 프로토콜 메시지에 대해 전송 관련 통계 표시	9.9(2)	이제 유닛당 클러스터의 신뢰할 수 있는 전송 버퍼 사용량을 볼 수 있어 버퍼가 제어 평면에서 가득 찬 경우 패킷 삭제 문제를 식별할 수 있습니다. 신규 또는 수정된 명령: **show cluster info transport cp detail**

기능 이름	버전	기능 정보
cluster remove unit 명령 동작이 **no enable** 동작과 일치합니다.	9.9(1)	이제 **cluster remove unit** 명령은 **no enable** 명령과 마찬가지로 클러스터링 또는 다시 로드를 수동으로 다시 활성화할 때까지 클러스터에서 유닛을 제거합니다. 이전에는 FXOS에서 부트스트랩 구성을 재구축하면 클러스터링이 다시 활성화되었습니다. 이제 부트스트랩 구성을 재구축하는 경우에도 비활성 상태가 유지됩니다. 그러나 ASA를 다시 로드하면 클러스터링이 다시 활성화됩니다. 신규/수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)**
섀시에 대해 향상된 섀시 상태 검사 장애 탐지	9.9(1)	이제 섀시 상태 검사의 보류 시간을 더 낮게 100밀리초로 구성할 수 있습니다. 이전에는 최소값이 300밀리초였습니다. 최소 결합 시간(간격 x 재시도 횟수)은 600밀리초보다 적을 수 없습니다. 신규 또는 수정된 명령: **app-agent heartbeat interval** ASDM은 지원되지 않습니다.
클러스터링를 위한 사이트 간 이중화	9.9 (1)	사이트 간 이중화를 통해 트래픽 플로우의 백업 소유자는 항상 소유자의 다른 사이트에 있게 됩니다. 이 기능은 사이트 장애가 발생하지 않도록 보호해줍니다. 신규 또는 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)**

기능 이름	버전	기능 정보
Firepower 9300에서 클러스터링을 사용하는 분산 Site-to-Site VPN	9.9(1)	Firepower 9300의 ASA 클러스터는 분산 모드에서 Site-to-Site VPN을 지원합니다. 분산 모드는 ASA 클러스터의 멤버 전체에 걸쳐 다수의 사이트 간 IPsec IKEv2 VPN 연결을 분산할 수 있는 기능을 제공합니다. 이는 중앙 집중식 모드에서처럼 제어 유닛에만 연결을 집중시키는 방식과 다릅니다. 이러한 기능은 중앙 집중식 VPN 기능보다 VPN 지원을 훨씬 더 확장하며 고가용성을 제공합니다. 분산 S2S VPN은 최대 2개의 섀시로 구성된 클러스터에서 실행되며, 각 섀시는 최대 3개의 모듈(총 6개의 클러스터 멤버)을 포함하고, 각 모듈은 최대 6,000개의 액티브 세션(총 12,000개)을 지원하며, 최댓값은 약 36,000개의 액티브 세션(총 72,000개)입니다. 신규 또는 수정된 화면: **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > ASA Cluster(ASA** 클러스터**) > VPN Cluster Summary(VPN** 클러스터 요약**)** **Monitoring(**모니터링**) > VPN > VPN Statistics(VPN** 통계**) > Sessions(**세션**)** **Configuration(**구성**) > Device Management(**디바이스 관리**) > High Availablility and Scalability(**고가용성 및 확장성**) > ASA Cluster(ASA** 클러스터**)** **Wizards(**마법사**) > Site-to-Site** **Monitoring(**모니터링**) > VPN > VPN Statistics(VPN** 통계**) > Sessions(**세션**)** **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > ASA Cluster(ASA** 클러스터**) > VPN Cluster Summary(VPN** 클러스터 요약**)** **Monitoring(**모니터링**) > ASA Cluster(ASA** 클러스터**) > ASA Cluster(ASA** 클러스터**) > System Resources Graphs(**시스템 리소스 그래프**) > CPU/Memory(CPU/**메모리**)** **Monitoring(**모니터링**) > Logging(**로깅**) > Real-Time Log Viewer(**실시간 로그 뷰어**)**
향상된 클러스터 유닛 상태 검사 장애 탐지	9.8(1)	이제 유닛 상태 검사의 보류 시간을 더 낮게 0.3초(최솟값)로 구성할 수 있습니다. 이전에는 최소값이 0.8초였습니다. 이 기능은 유닛 상태 검사 메시징 체계를 제어 평면의 *keepalives*에서 데이터 평면의 하트비트로 변경합니다. 하트비트를 사용하면 제어 평면 CPU 과다 사용 및 예약 지연의 영향을 받지 않으므로 클러스터링의 신뢰성과 응답성이 개선됩니다. 대기 시간을 낮게 구성하면 클러스터 제어 링크 메시징 활동이 증가합니다. 낮은 대기 시간을 구성하기 전에 네트워크를 분석하는 것이 좋습니다. 예를 들어, 한 번의 대기 시간 간격 동안 3개의 하트비트 메시지가 있으므로 클러스터 제어 링크를 통과하는 한 유닛에서 다른 유닛으로의 핑이 *holdtime*/3 이내에 반환되는지 확인하십시오. 대기 시간을 0.3 - 0.7초로 설정한 후에 ASA 소프트웨어를 다운그레이드하는 경우, 새로운 설정이 지원되지 않으므로 이 설정은 3초의 기본값으로 되돌아갑니다. 수정된 화면: **Configuration(**구성**) > Device Management(**디바이스 관리**) > High Availability and Scalability(**고가용성 및 확장성**) > ASA Cluster(ASA** 클러스터**)**

기능 이름	버전	기능 정보
인터페이스를 실패 상태로 표시하기 위해 구성 가능한 디바운스 시간 - Firepower 4100/9300 섀시	9.8(1)	이제 ASA가 인터페이스를 실패 상태로 간주하고 유닛이 클러스터에서 제거되기 전에 디바운스 시간을 구성할 수 있습니다. 이 기능을 통해 인터페이스 장애 탐지를 더 빠르게 수행할 수 있습니다. 디바운스 시간을 더 낮게 구성하면 오탐의 가능성이 증가합니다. 인터페이스 상태 업데이트가 발생하는 경우, 인터페이스를 실패로 표시하고 유닛이 클러스터에서 제거되기 전에 ASA는 지정되어 있는 밀리초 동안 대기합니다. 기본 디바운스 시간은 500밀리초이며 범위는 300밀리초~9초입니다. 신규 또는 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)**
Firepower 4100/9300 섀시에서 ASA에 대한 사이트 간 클러스터링 개선	9.7(1)	이제 ASA 클러스터를 구축할 때 각 Firepower 4100/9300 섀시에 대한 사이트 ID를 구성할 수 있습니다. 전에는 ASA 애플리케이션 내에서 사이트 ID를 구성해야 했습니다. 이 기능 덕분에 초기 구축이 수월해졌습니다. 더 이상 ASA 구성 내에서 사이트 ID를 설정할 수 없습니다. 또한 사이트 간 클러스터링과의 호환성을 최대한 활용하려면 안정성과 성능이 개선된 ASA 9.7(1) 및 FXOS 2.1.1로 업그레이드하는 것이 좋습니다. 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)**
관리자 현지화: 데이터 센터에 대한 사이트 간 클러스터링 개선 사항	9.7(1)	성능을 개선하고 데이터 센터에 대한 사이트 간 클러스터링을 위해 사이트 내부에서 트래픽을 유지하도록 관리자 현지화를 활성화할 수 있습니다. 새로운 연결은 일반적으로 로드 밸런싱 상태이며 지정된 사이트 내부의 클러스터 멤버가 소유합니다. 그러나 ASA는 모든 사이트에서 멤버에 관리자 역할을 할당합니다. 관리자 현지화를 사용하면 추가 관리자 역할이 활성화됩니다. 즉, 소유자와 동일한 사이트의 로컬 관리자와 모든 사이트의 전역 관리자 역할이 활성화됩니다. 소유자와 관리자를 동일한 사이트에서 유지하면 성능이 향상됩니다. 또한 원래 소유자가 실패할 경우, 로컬 관리자가 동일한 사이트에서 새로운 연결 소유자를 선택합니다. 전역 관리자는 클러스터 멤버가 다른 사이트에서 소유하는 연결에 대한 패킷을 수신하는 경우 사용됩니다. 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **Cluster Configuration(**클러스터 구성**)**
16개의 섀시에 대한 지원 - Firepower 4100 Series	9.6(2)	이제 Firepower 4100 Series에 대한 클러스터에 최대 16개의 섀시를 추가할 수 있습니다. 화면은 수정하지 않았습니다.
지원 - Firepower 4100 Series	9.6(1)	FXOS 1.1.4를 활용하여 ASA에서는 Firepower 4100 Series에서 최대 6개의 섀시에 대해 섀시 간 클러스터링을 지원합니다. 화면은 수정하지 않았습니다.

기능 이름	버전	기능 정보
라우팅 모드, Spanned EtherChannel 모드에서 사이트별 IP 주소에 대한 지원	9.6(1)	Spanned EtherChannel을 사용하는 라우팅 모드에서 사이트 간 클러스터링을 위해 이제 사이트별 MCA 주소에 추가하여 사이트별 IP 주소를 구성할 수 있습니다. 사이트의 IP 주소를 추가하면 라우팅 문제를 일으킬 수 있는 전역 MAC 주소의 ARP 응답이 DCI(Data Center Interconnect)를 통해 이동하는 것을 방지하기 위해 OTV(Overlay Transport Virtualization) 디바이스에서 ARP 검사를 사용할 수 있습니다. ARP 검사는 VACL을 사용하여 MAC 주소를 필터링할 수 없는 일부 스위치에 필요합니다. 수정된 화면: **Configuration(**구성**)** > **Device Setup(**디바이스 설정**)** > **Interface Settings(**인터페이스 설정**)** > **Interfaces(**인터페이스**)** > **Add/Edit EtherChannel Interface(EtherChannel** 인터페이스 추가/수정**)** > **Advanced(**고급**)**
16개 모듈을 위한 섀시 간 클러스터링 및 Firepower 9300 ASA 애플리케이션을 위한 사이트 간 클러스터링	9.5(2.1)	이제 FXOS 1.1.3에서 사이트 간 클러스터링을 확장하여 섀시 간 클러스터링을 활성화할 수 있습니다. 최대 16개의 모듈을 포함할 수 있습니다. 예를 들어 섀시 16개에 모듈 1개, 섀시 8개에 모듈 2개, 또는 모듈을 16개까지 제공하는 어떤 조합도 사용할 수 있습니다. 화면은 수정하지 않았습니다.
라우팅 방화벽 모드에서 Spanned EtherChannel에 대한 사이트 간 클러스터링 지원을 위한 사이트별 MAC 주소	9.5(2)	이제 라우팅 모드에서 Spanned EtherChannel에 대한 사이트 간 클러스터링을 사용할 수 있습니다. MAC 주소 플래핑을 방지하려면 각 인터페이스에 대한 사이트별 MAC 주소를 사이트의 유닛 간에 공유할 수 있도록 각 클러스터 멤버에 대한 사이트 ID를 구성합니다. 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)**
인터페이스 또는 클러스터 제어 링크 실패 시 자동 다시 참가 동작의 ASA 클러스터 맞춤화	9.5(2)	이제 인터페이스 또는 클러스터 제어 링크 작동이 실패할 경우 자동 다시 참가 동작을 맞춤화할 수 있습니다. 도입된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Auto Rejoin(**자동 다시 참가**)**
ASA 클러스터의 GTPv1 및 GTPv2 지원	9.5(2)	이제 ASA 클러스터는 GTPv1 및 GTPv2 검사를 지원합니다. 화면은 수정하지 않았습니다.
TCP 연결에 대한 클러스터 복제 지연	9.5(2)	이 기능은 관리자/백업 플로우 생성을 지연시켜 짧은 수명의 플로우와 관련된 "불필요한 작업"을 제거하는 데 도움이 됩니다. 도입된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster Replication(ASA** 클러스터 복제**)**

기능 이름	버전	기능 정보
사이트 간 플로우 모빌리티에 대한 LISP 검사	9.5(2)	Cisco LISP(Locator/ID Separation Protocol) 아키텍처는 디바이스 ID를 해당 위치에서 두 개의 서로 다른 숫자 공간으로 분리하여, 서버 마이그레이션을 클라이언트에 투명하게 만듭니다. ASA는 위치 변경을 위해 LISP 트래픽을 검사한 다음 원활한 클러스터링 작업을 위해 이 정보를 사용할 수 있습니다. ASA 클러스터 멤버는 첫 번째 홉 라우터와 ETR(Egress Tunnel Router) 또는 ITR(Ingress Tunnel Router) 사이를 통과하는 LISP 트래픽을 검사할 수 있으며 플로우 소유자가 새로운 사이트에 있도록 변경할 수 있습니다. 도입 또는 수정된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster(ASA** 클러스터**)** > **Cluster Configuration(**클러스터 구성**)** **Configuration(**구성**)** > **Firewall(**방화벽**)** > **Objects(**개체**)** > **Inspect Maps(**검사 맵**)** > **LISP** **Configuration(**구성**)** > **Firewall(**방화벽**)** > **Service Policy Rules(**서비스 정책 규칙**)** > **Protocol Inspection(**프로토콜 검사**)** **Configuration(**구성**)** > **Firewall(**방화벽**)** > **Service Policy Rules(**서비스 정책 규칙**)** > **Cluster(**클러스터**)** **Monitoring(**모니터링**)** > **Routing(**라우팅**)** > **LISP-EID Table(LISP-EID** 테이블**)**
장애 조치 및 ASA 클러스터링에서의 통신 사업자급 NAT 개선 사항 지원	9.5(2)	통신 사업자급 PAT나 대규모 PAT의 경우 NAT에서 포트 변환을 한 번에 하나씩 할당하도록 하는 대신 각 호스트에 포트 블록을 할당할 수 있습니다(RFC 6888 참조). 이 기능은 이제 장애 조치 및 ASA 클러스터 구축에서 지원됩니다. 화면은 수정하지 않았습니다.
추적 항목 클러스터링의 구성 가능한 레벨	9.5(2)	기본적으로 클러스터링 이벤트의 모든 레벨이 많은 낮은 레벨의 이벤트를 포함하여 추적 버퍼에 포함되어 있습니다. 더 높은 레벨의 이벤트로 추적을 제한하기 위해 클러스터에 대해 최소한의 추적 레벨을 설정할 수 있습니다. 화면은 수정하지 않았습니다.
Firepower 9300을 위한 섀시 내 ASA 클러스터링	9.4(1.150)	Firepower 9300 섀시 내에서 최대 3개의 보안 모듈을 클러스터링할 수 있습니다. 섀시의 모든 모듈은 클러스터에 속해야 합니다. 도입된 화면: **Configuration(**구성**)** > **Device Management(**디바이스 관리**)** > **High Availability and Scalability(**고가용성 및 확장성**)** > **ASA Cluster Replication(ASA** 클러스터 복제**)**

번역에 관하여
Cisco는 일부 지역에서 본 콘텐츠의 현지 언어 번역을 제공할 수 있습니다. 이러한 번역은 정보 제공의 목적으로만 제공되며, 불일치가 있는 경우 본 콘텐츠의 영어 버전이 우선합니다.