



Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드, **2.2(2)**

초판: 2017년 08월 29일

최종 변경: 2017년 09월 20일

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

이 설명서의 제품 관련 사양 및 정보는 예고 없이 변경될 수 있습니다. 이 설명서의 모든 설명, 정보 및 권장 사항이 정확하다고 판단되더라도 어떠한 형태의 명시적이거나 묵시적인 보증도 하지 않습니다. 모든 제품의 해당 애플리케이션에 대한 사용은 전적으로 사용자에게 책임이 있습니다.

동봉한 제품의 소프트웨어 라이선스 및 제한된 보증은 제품과 함께 제공된 정보 패키지에 설명되어 있으며 본 문서에 참조를 통해 포함됩니다. 소프트웨어 라이선스 또는 제한된 보증을 찾을 수 없는 경우 CISCO 담당자에게 문의하여 복사본을 요청하십시오.

Cisco의 TCP 헤더 압축은 UNIX 운영 체제의 UCB(University of Berkeley) 공개 도메인 버전의 일부로서 UCB에서 개발된 프로그램을 적용하여 구현됩니다. All rights reserved. Copyright © 1981, Regents of the University of California.

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에서 언급한 공급자는 상품성, 특정 목적에의 적합성 및 비침해에 대한 보증을 포함하되 이에 제한되지 않으며 거래 과정, 사용 또는 거래 관행으로부터 발생하는 모든 명시적이거나 묵시적인 보증을 부인합니다.

Cisco 또는 해당 공급업체는 피해의 가능성에 대해 언급한 경우라도 이 설명서의 사용 또는 사용 불능으로 인해 발생하는 이익 손실, 데이터 손실 또는 손상을 포함하여(단, 이에 한하지 않음) 간접, 특별, 중대 또는 부수적 손해에 대해 어떠한 경우라도 책임을 지지 않습니다.

이 문서에서 사용된 모든 IP(Internet Protocol) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예, 명령 표시 출력, 네트워크 토폴로지 다이어그램 및 다른 그림은 이해를 돕기 위한 자료일 뿐이며, 실제 IP 주소나 전화 번호가 사용되었다면 이는 의도하지 않은 우연의 일치입니다.

Cisco 및 Cisco 로고는 미국 및 기타 국가에서 Cisco Systems, Inc. 및/또는 계열사의 상표 또는 등록 상표입니다. Cisco 상표 목록을 보려면 <http://www.cisco.com/go/trademarks>로 이동하십시오. 여기에 언급된 서드파티 상표는 해당 소유권자의 자산입니다. "파트너"라는 용어는 사용에 있어 Cisco와 기타 회사 간의 파트너 관계를 의미하지는 않습니다. (1110R)

© 2017 Cisco Systems, Inc. All rights reserved.



목 차

Firepower Security Appliance 소개	1
Firepower Security Appliance 정보	1
Firepower Chassis Manager 개요	1
새시 상태 모니터링	2
시작하기	5
작업 플로우	5
초기 컨피그레이션	6
Firepower Chassis Manager 로그인 또는 로그아웃	8
FXOS CLI 액세스	9
ASA용 라이선스 관리	11
Smart Software Licensing 정보	11
ASA용 Smart Software Licensing	12
Smart Software Manager 및 어카운트	12
오프라인 관리	12
영구 라이선스 예약	13
Satellite 서버	13
가상 어카운트별로 관리되는 라이선스 및 디바이스	13
평가판 라이선스	13
Smart Software Manager 통신	14
디바이스 등록 및 토큰	14
License Authority와의 정기적인 통신	14
규정 위반 상태	15
Smart Call Home 인프라	15
Smart Software Licensing 사전 요구 사항	15
Smart Software Licensing 지침	16
Smart Software Licensing의 기본값	16
일반 Smart Software Licensing 구성	16

- (선택 사항) HTTP 프록시 구성 16
- (선택 사항) Call Home URL 삭제 17
- License Authority에 Firepower Security Appliance 등록 17
- Smart License Satellite Server 구성 - Firepower 4100/9300 새시 18
- 영구 라이선스 예약 구성 19
 - 영구 라이선스 설치 19
 - (선택 사항) 영구 라이선스 반환 20
- Smart Software Licensing 기록 21
- 사용자 관리 23
 - 사용자 어카운트 23
 - 사용자 이름 지침 24
 - 비밀번호 지침 25
 - 원격 인증에 관한 지침 26
 - 사용자 역할 29
 - 로컬 인증 사용자의 비밀번호 프로필 29
 - 사용자 설정 구성 30
 - 세션 시간 제한 구성 33
 - 세션 시간 제한 절대값 구성 34
 - 최대 로그인 시도 횟수 설정 35
 - 사용자 잠금 상태 보기 및 지우기 36
 - 최소 비밀번호 길이 확인 구성 37
 - 로컬 사용자 어카운트 생성 37
 - 로컬 사용자 어카운트 삭제 39
 - 로컬 사용자 어카운트 활성화 또는 비활성화 39
 - 로컬 인증 사용자에 대한 비밀번호 기록 지우기 40
- 이미지 관리 41
 - 이미지 관리 정보 41
 - Cisco.com에서 이미지 다운로드 42
 - Firepower Security Appliance에 이미지 업로드 42
 - 이미지 무결성 확인 43
 - Firepower eXtensible 운영 체제 플랫폼 번들 업그레이드 43
 - 논리적 디바이스를 위한 이미지 버전 업데이트 44

- 날짜 및 시간 수동 설정 87
- SSH 구성 88
- 텔넷 구성 90
- SNMP 구성 90
 - SNMP 정보 91
 - SNMP 알림 91
 - SNMP 보안 레벨 및 권한 92
 - 지원되는 SNMP 보안 모델 및 레벨의 조합 92
 - SNMPv3 보안 기능 93
 - SNMP 지원 93
 - SNMP 활성화 및 SNMP 속성 구성 94
 - SNMP 트랩 생성 95
 - SNMP 트랩 삭제 96
 - SNMPv3 사용자 생성 96
 - SNMPv3 사용자 삭제 97
- HTTPS 구성 97
 - 인증서, 키 링 및 트러스트 포인트 98
 - 키 링 생성 99
 - 기본 키 링 재생성 99
 - 키 링에 대한 인증서 요청 생성 100
 - 기본 옵션을 사용하여 키 링에 대한 인증서 요청 생성 100
 - 고급 옵션을 사용하여 키 링에 대한 인증서 요청 생성 101
 - 트러스트 포인트 생성 103
 - 키 링에 인증서 가져오기 104
 - HTTPS 구성 105
 - HTTPS 포트 변경 106
 - 키 링 삭제 107
 - 트러스트 포인트 삭제 107
 - HTTPS 비활성화 108
- AAA 구성 108
 - AAA 정보 108
 - LDAP 제공자 구성 109

- LDAP 제공자 속성 구성 109
- LDAP 제공자 생성 110
- LDAP 제공자 삭제 113
- RADIUS 제공자 구성 113
 - RADIUS 제공자 속성 구성 113
 - RADIUS 제공자 생성 114
 - RADIUS 제공자 삭제 115
- TACACS+ 제공자 구성 116
 - TACACS+ 제공자 속성 구성 116
 - TACACS+ 제공자 생성 116
 - TACACS+ 제공자 삭제 117
- Syslog 구성 118
- DNS 서버 구성 121
- 인터페이스 관리 123
 - Firepower Security Appliance 인터페이스 정보 123
 - 인터페이스 페이지 123
 - 인터페이스 유형 124
 - 하드웨어 바이패스 쌍 125
 - 점보 프레임 지원 126
 - 인터페이스 속성 편집 126
 - 인터페이스의 관리 상태 변경 127
 - 포트 채널 생성 127
 - 브레이크아웃 케이블 구성 129
- 논리적 디바이스 131
 - 논리적 디바이스 정보 131
 - 논리적 디바이스 페이지 132
 - 독립형 논리적 디바이스 생성 133
 - 독립형 ASA 논리적 디바이스 생성 133
 - 독립형 위협 방어 논리적 디바이스 생성 135
- 클러스터 구축 137
 - 클러스터링 정보 - Firepower 4100/9300 새시 137
 - 기본 유닛 및 보조 유닛 역할 138

- 클러스터 제어 링크 138
 - 새시 간 클러스터링을 위한 클러스터 제어 링크 크기 조정 139
 - 새시 간 클러스터링을 위한 클러스터 제어 링크 이중화 139
 - 새시 간 클러스터링을 위한 클러스터 제어 링크 안정성 140
 - 클러스터 제어 링크 네트워크 140
- 관리 네트워크 140
- 관리 인터페이스 140
- 스팬 EtherChannel 140
- 사이트 간 클러스터링 141
- 클러스터링의 사전 요구 사항 142
- 클러스터링 지침 143
- 클러스터링 기본값 146
- ASA 클러스터링 구성 147
- Firepower Threat Defense 클러스터링 구성 149
- 사이트 간 클러스터링 예시 153
 - Spanned EtherChannel 투명 모드 북-남 사이트 간 예시 153
 - Spanned EtherChannel 투명 모드 동-서 사이트 간 예시 154
- 클러스터링 기록 155
- 서비스 체이닝 구성 156
 - 서비스 체이닝 정보 156
 - 서비스 체이닝 사전 요구 사항 156
 - 서비스 체이닝 지침 157
 - 독립형 논리적 디바이스에 Radware DefensePro 서비스 체인 구성 157
 - 인트라 새시 클러스터에 Radware DefensePro 서비스 체인 구성 159
 - UDP/TCP 포트 열기 및 vDP 웹 서비스 활성화 160
- 논리적 디바이스 관리 161
 - 애플리케이션 콘솔 또는 데코레이터에 연결 161
 - 논리적 디바이스 삭제 162
 - 논리적 디바이스와 연결되지 않은 애플리케이션 인스턴스 삭제 162
 - ASA를 투명 방화벽 모드로 변경 163
 - Firepower Threat Defense 논리적 디바이스에서 인터페이스 변경 164
 - ASA 논리적 디바이스에서 인터페이스 변경 165

- 보안 모듈/엔진 관리 167
 - FXOS 보안 모듈/보안 엔진 정보 167
 - 보안 모듈 서비스 해제/서비스 다시 시작 169
 - 보안 모듈/엔진 승인 169
 - 보안 모듈/엔진 재설정 170
 - 보안 모듈/엔진 재초기화 170
 - 보안 모듈/엔진 전원 켜기/끄기 171
- 컨피그레이션 가져오기/내보내기 173
 - 컨피그레이션 가져오기/내보내기 정보 173
 - 컨피그레이션 파일 내보내기 174
 - 자동 컨피그레이션 내보내기 예약 175
 - 컨피그레이션 내보내기 미리 알림 설정 176
 - 컨피그레이션 파일 가져오기 176
- 트러블슈팅 179
 - 패킷 캡처 179
 - 패킷 캡처 세션 생성 또는 편집 180
 - 패킷 캡처의 필터 구성 182
 - 패킷 캡처 세션 시작 및 중지 183
 - 패킷 캡처 파일 다운로드 184
 - 패킷 캡처 세션 삭제 184
 - 네트워크 연결성 테스트 185
 - 포트 채널 상태 판단 186
 - 소프트웨어 장애 복구 188
 - 손상된 파일 시스템 복구 193



Firepower Security Appliance 소개

- [Firepower Security Appliance 정보, 1페이지](#)
- [Firepower Chassis Manager 개요, 1페이지](#)
- [새시 상태 모니터링, 2페이지](#)

Firepower Security Appliance 정보

Cisco Firepower 4100/9300 새시는 네트워크 및 콘텐츠 보안 솔루션을 위한 차세대 플랫폼입니다. Firepower 4100/9300 새시는 Cisco ACI(Application Centric Infrastructure) 보안 솔루션의 일부로, 확장성, 제어 일관성 및 관리 간소화를 위해 구축된 민첩한 개방형 보안 플랫폼을 제공합니다.

Firepower 4100/9300 새시에서 제공하는 기능은 다음과 같습니다.

- 모듈형 새시 기반 보안 시스템 — 고성능의 유연한 입/출력 컨피그레이션 및 확장성을 제공합니다.
- Firepower Chassis Manager — 그래픽 사용자 인터페이스에서는 현재 새시 상태를 간단하게 시각적으로 표시하며 간소화된 새시 기능 컨피그레이션을 제공합니다.
- FXOS CLI — 기능 구성, 새시 상태 모니터링 및 고급 트러블슈팅 기능 액세스를 위해 명령 기반 인터페이스를 제공합니다.
- FXOS REST API — 사용자가 새시를 프로그래밍 방식으로 구성 및 관리할 수 있습니다.

Firepower Chassis Manager 개요

Firepower eXtensible 운영 체제는 플랫폼 설정 및 인터페이스 컨피그레이션, 디바이스 프로비저닝, 시스템 상태 모니터링을 쉽게 수행할 수 있도록 지원하는 웹 인터페이스를 제공합니다. 사용자 인터페이스 상단에 있는 내비게이션 바를 통해 다음에 액세스할 수 있습니다.

- Overview(개요) — Overview(개요) 페이지에서 Firepower 새시의 상태를 쉽게 모니터링할 수 있습니다. 자세한 내용은 [새시 상태 모니터링, 2페이지](#)를 참조하십시오.

- **Interfaces(인터페이스)** — **Interfaces(인터페이스)** 페이지에서 새시에 설치된 인터페이스의 상태를 확인하고, 인터페이스 속성을 편집하며, 인터페이스를 활성화 또는 비활성화하고, 포트 채널을 생성할 수 있습니다. 자세한 내용은 [인터페이스 관리, 123 페이지](#)를 참조하십시오.
- **Logical Devices(논리적 디바이스)** — **Logical Devices(논리적 디바이스)** 페이지에서 논리적 디바이스를 생성, 편집 및 삭제할 수 있습니다. 자세한 내용은 [논리적 디바이스, 131 페이지](#)를 참조하십시오.
- **Security Modules/Security Engine(보안 모듈/보안 엔진)** — **Security Modules/Security Engine(보안 모듈/보안 엔진)** 페이지에서 보안 모듈/엔진의 상태를 확인하고 전원 주기, 다시 초기화, 승인 및 해제와 같은 다양한 기능을 수행할 수 있습니다. 자세한 내용은 [보안 모듈/엔진 관리, 167 페이지](#)를 참조하십시오.
- **Platform Settings(플랫폼 설정)** — **Platform Settings(플랫폼 설정)** 페이지에서 날짜 및 시간, SSH, SNMP, HTTPS, AAA, Syslog 및 DNS 등 새시 설정을 구성할 수 있습니다. 자세한 내용은 [플랫폼 설정, 85 페이지](#)를 참조하십시오.
- **System Settings(시스템 설정)** — **System(시스템)** 메뉴에서 다음 설정을 관리할 수 있습니다.
 - **Licensing(라이선싱)** — **Licensing(라이선싱)** 페이지에서 Smart Call Home 설정을 구성하고 Firepower 새시를 License Authority에 등록할 수 있습니다. 자세한 내용은 [ASA용 라이선스 관리, 11 페이지](#)를 참조하십시오.
 - **Updates(업데이트)** — **Updates(업데이트)** 페이지에서 Firepower 새시에 플랫폼 번들 및 애플리케이션 이미지를 업로드할 수 있습니다. 자세한 내용은 [이미지 관리, 41 페이지](#)를 참조하십시오.
 - **User Management(사용자 관리)** — **User Management(사용자 관리)** 페이지에서 Firepower 4100/9300 새시에 대한 사용자 설정을 구성하고 사용자 어카운트를 정의할 수 있습니다. 자세한 내용은 [사용자 관리, 23 페이지](#)를 참조하십시오.

새시 상태 모니터링

Overview(개요) 페이지에서 Firepower 4100/9300 새시의 상태를 쉽게 모니터링할 수 있습니다.

Overview(개요) 페이지에서는 다음 요소가 제공됩니다.

- **Device Information(디바이스 정보)** — **Overview(개요)** 페이지 상단에는 Firepower 4100/9300 새시에 대한 다음 정보가 포함되어 있습니다.
 - **Chassis name(새시 이름)** — 초기 컨피그레이션 중 새시에 할당된 이름이 표시됩니다.
 - **IP address(IP 주소)** — 초기 컨피그레이션 중 새시에 할당된 관리 IP 주소가 표시됩니다.
 - **Model(모델)** — Firepower 4100/9300 새시 모델이 표시됩니다.
 - **Version(버전)** — 새시에서 실행 중인 FXOS 버전 번호가 표시됩니다.
 - **Operational State(작동 상태)** — 새시의 작동 가능 상태가 표시됩니다.

- Chassis uptime(새시 업타임) — 시스템이 마지막으로 재시작된 이후 경과한 시간이 표시됩니다.
- Shutdown(종료) 버튼 — Firepower 4100/9300 새시를 정상적으로 종료합니다([Firepower 4100/9300 새시 전원 끄기](#), 78 페이지 참조).



참고 Security Modules/Security Engine(보안 모듈/보안 엔진) 페이지에서 보안 모듈/엔진의 전원을 켜고 끌 수 있습니다([보안 모듈/엔진 전원 켜기/끄기](#), 171 페이지 참조).

- Reboot(재부팅) 버튼 — Firepower 4100/9300 새시를 정상적으로 종료합니다([Firepower 4100/9300 새시 재부팅](#), 77 페이지 참조).



참고 Security Modules/Security Engine(보안 모듈/보안 엔진) 페이지에서 보안 모듈/엔진을 재설정할 수 있습니다([보안 모듈/엔진 재설정](#), 170 페이지 참조).

- Uptime Information(업타임 정보) 아이콘 — 새시 및 설치된 보안 모듈/엔진의 업타임을 보려면 아이콘 위에 마우스를 올려놓습니다.
- Visual Status Display(시각적 상태 표시) — Device Information(디바이스 정보) 섹션에서는 새시를 시각적으로 표시하여 새시에 설치된 구성 요소를 보여주고 해당 구성 요소에 대한 일반적인 상태 정보를 제공합니다. Visual Status Display(시각적 상태 표시)에 나타난 포트 위에 마우스를 올려놓으면 인터페이스 이름, 속도, 유형, 관리자 상태 및 작동 상태와 같은 추가 정보를 얻을 수 있습니다. 여러 보안 모듈이 있는 모델의 경우, Visual Status Display(시각적 상태 표시)에 나타난 모듈에 마우스를 올려놓으면 디바이스 이름, 템플릿 유형, 관리자 상태 및 작동 상태와 같은 추가 정보를 얻을 수 있습니다.
- Detailed Status Information(상세한 상태 정보) — Visual Status Display(시각적 상태 표시)에서는 상세한 새시의 상태 정보가 포함된 표가 제공됩니다. 상태 정보는 Faults(결함), Interfaces(인터페이스), Devices(디바이스), License(라이선스) 및 Inventory(인벤토리)의 5가지 섹션으로 나뉩니다. 확인하려는 정보의 요약 영역을 클릭하여 표에 있는 각 해당 섹션에 대한 요약을 확인할 수 있으며 각 섹션에 대한 추가적인 세부사항을 확인할 수 있습니다.

시스템은 새시에 대해 다음과 같은 상세한 상태 정보를 제공합니다.

- Faults(결함) — 시스템에서 생성된 결함이 나열됩니다. 결함은 Critical(중대), Major(주요), Minor(사소), Warning(경고) 및 Info(정보)의 심각도별로 정렬됩니다. 나열된 각 결함에 대해 심각도, 결함 설명, 원인, 발생 횟수 및 최근 발생 시간을 확인할 수 있습니다. 또한, 결함 확인 여부를 확인할 수 있습니다.

결함 중 하나를 클릭하여 해당 결함에 대한 추가적인 세부사항을 확인하거나 결함을 확인할 수 있습니다.



참고 결함의 근본 원인이 해결되면 해당 결함은 다음 폴링 간격 동안 목록에서 자동으로 지워집니다. 사용자가 특정 결함에 대한 해결책과 관련된 작업을 진행 중인 경우, 결함을 확인하여 해당 결함이 현재 해결 중이라는 사실을 다른 사용자에게 알릴 수 있습니다.

- **Interfaces(인터페이스)** — 시스템에 설치된 인터페이스가 나열됩니다. **All Interfaces(모든 인터페이스)** 탭 — 인터페이스 이름, 작동 상태, 관리 상태, 수신된 바이트 수, 전송된 바이트 수가 표시됩니다. 하드웨어 우회 탭에는 **Firepower Threat Defense** 애플리케이션에서 하드웨어 우회 기능에 대해 지원되는 인터페이스 쌍만 표시됩니다. 각 쌍의 경우, 작동 상태 인 비활성화됨(하드웨어 우회가 쌍에 대해 구성되지 않음), 스탠바이(하드웨어 우회가 구성되었지만 현재 활성 상태가 아님) 및 바이패스(하드웨어 우회가 활성 상태임)가 표시됩니다.
- **Devices(디바이스)** — 시스템에 구성된 논리적 디바이스가 나열되고 각 논리적 디바이스의 세부사항(예: 디바이스 이름, 디바이스 상태, 애플리케이션 템플릿 유형, 작동 상태, 관리 상태, 이미지 버전, 관리 IP 주소 및 ASDM URL)이 제공됩니다.
- **License(라이선스)** — **Smart Licensing** 활성화 여부가 표시되며 **Firepower** 라이선스의 현재 등록 상태가 제공되고 새시의 라이선스 권한 부여 정보가 표시됩니다.
- **Inventory(인벤토리)** — 새시에 설치된 구성 요소가 나열되고 해당 구성 요소와 관련된 세부사항(예: 구성 요소 이름, 코어 수, 설치 위치, 작동 상태, 작동 가능성, 용량, 전원, 열, 시리즈 번호, 모델 번호, 부품 번호 및 벤더)이 제공됩니다.



시작하기

- [작업 플로우, 5페이지](#)
- [초기 컨피그레이션, 6페이지](#)
- [Firepower Chassis Manager 로그인 또는 로그아웃, 8페이지](#)
- [FXOS CLI 액세스, 9페이지](#)

작업 플로우

다음 절차에서는 Firepower 4100/9300 새시 구성 시 완료해야 하는 기본 작업을 보여줍니다.

절차

- 단계 1** Firepower 4100/9300 새시 하드웨어를 구성합니다([Cisco Firepower Security Appliance 하드웨어 설치 가이드](#) 참조).
 - 단계 2** 초기 컨피그레이션을 완료합니다([초기 컨피그레이션, 6 페이지](#) 참조).
 - 단계 3** Firepower Chassis Manager에 로그인합니다([Firepower Chassis Manager 로그인 또는 로그아웃, 8 페이지](#) 참조).
 - 단계 4** 날짜 및 시간을 설정합니다([날짜 및 시간 설정, 85 페이지](#) 참조).
 - 단계 5** DNS 서버를 구성합니다([DNS 서버 구성, 121 페이지](#) 참조).
 - 단계 6** 제품 라이선스를 등록합니다([ASA용 라이선스 관리, 11 페이지](#) 참조).
 - 단계 7** 사용자를 구성합니다([사용자 관리, 23 페이지](#) 참조).
 - 단계 8** 필요 시 소프트웨어 업데이트를 수행합니다([이미지 관리, 41 페이지](#) 참조).
 - 단계 9** 추가 플랫폼 설정을 구성합니다([플랫폼 설정, 85 페이지](#) 참조).
 - 단계 10** 인터페이스를 구성합니다([인터페이스 관리, 123 페이지](#) 참조).
 - 단계 11** 논리적 디바이스를 생성합니다([논리적 디바이스, 131 페이지](#) 참조).
-

초기 컨피그레이션

Firepower Chassis Manager 또는 FXOS CLI를 사용하여 시스템을 구성하고 관리할 수 있으려면 먼저 콘솔 포트를 통해 액세스하는 FXOS CLI를 사용하여 초기 컨피그레이션 작업 일부를 수행해야 합니다. FXOS CLI를 사용하여 처음으로 Firepower 4100/9300 새시에 액세스할 때 시스템을 구성하는 데 사용할 수 있는 설정 마법사가 나타납니다.

기존 백업 파일에서 시스템 컨피그레이션을 복원하거나 설정 마법사를 통해 수동으로 시스템을 설정하도록 선택할 수 있습니다. 시스템 복원을 선택할 경우 관리 네트워크에서 백업 파일에 접근할 수 있어야 합니다.

Firepower 4100/9300 새시의 단일 관리 포트에 대해 단 하나의 IPv4 주소, 게이트웨이, 서브넷 마스크 또는 단 하나의 IPv6 주소, 게이트웨이, 네트워크 접두사만 지정해야 합니다. 관리 포트 IP 주소로 IPv4 또는 IPv6 주소 중 하나를 구성할 수 있습니다.

시작하기 전에

1 Firepower 4100/9300 새시에서 다음 물리적 연결을 확인합니다.

- 콘솔 포트가 컴퓨터 터미널 또는 콘솔 서버에 물리적으로 연결되어 있습니다.
- 1Gbps 이더넷 관리 포트가 외부 허브, 스위치 또는 라우터에 연결되어 있습니다.

자세한 내용은 [Cisco Firepower Security Appliance 하드웨어 설치 가이드](#)를 참조하십시오.

2 콘솔 포트에 연결된 컴퓨터 터미널(또는 콘솔 서버)의 콘솔 포트 매개변수가 다음과 같은지 확인합니다.

- 9600 보(baud)
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

절차

단계 1 콘솔 포트에 연결합니다.

단계 2 Firepower 4100/9300 새시의 전원을 켭니다.

Firepower 4100/9300 새시가 부팅될 때 전원 켜짐 자가 테스트 메시지가 표시됩니다.

단계 3 구성되지 않은 시스템을 부팅하는 경우, 설정 마법사에서 시스템을 구성하는 데 필요한 다음 정보를 묻는 프롬프트를 표시합니다.

- 설정 모드(전체 시스템 백업에서 복원 또는 초기 설정)
- 강력한 비밀번호 시행 정책(강력한 비밀번호 지침에 대해서는 [사용자 어카운트, 23 페이지](#) 참조)

- 관리자 비밀번호
- 시스템 이름
- 관리 포트 IPv4 주소 및 서브넷 마스크 또는 IPv6 주소 및 접두사
- 기본 게이트웨이 IPv4 또는 IPv6 주소
- DNS 서버 IPv4 또는 IPv6 주소
- 기본 도메인 이름

단계 4 설정 요약을 검토하고 **yes**를 입력하여 설정을 저장하고 적용하거나 **no**를 입력하여 다시 설정 마법사로 돌아가 일부 설정을 변경합니다.
 설정 마법사를 다시 사용하도록 선택하는 경우 이전에 입력한 값이 괄호로 나타납니다. 이전에 입력한 값을 승인하려면 **Enter** 키를 누릅니다.

다음 예에서는 IPv4 관리 주소를 사용하여 컨피그레이션을 설정합니다.

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%958
Confirm the password for "admin": adminpassword%958
Enter the system name: foo
Physical Switch Mgmt0 IP address : 192.168.10.10
Physical Switch Mgmt0 IPv4 netmask: 255.255.255.0
IPv4 address of the default gateway: 192.168.10.1
Configure the DNS Server IP address? (yes/no) [n]: yes
  DNS IP address: 20.10.20.10
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforce Strong Password=no
  Physical Switch Mgmt0 IP Address=192.168.10.10
  Physical Switch Mgmt0 IP Netmask=255.255.255.0
  Default Gateway=192.168.10.1
  IPv6 value=0
  DNS Server=20.10.20.10
  Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
다음 예에서는 IPv6 관리 주소를 사용하여 컨피그레이션을 설정합니다.
```

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Fabric interconnect. Continue? (y/n): y
Enforce strong password? (y/n) [y]: n
Enter the password for "admin": adminpassword%652
Confirm the password for "admin": adminpassword%652
Enter the system name: foo
Physical Switch Mgmt0 IP address : 2001::107
Physical Switch Mgmt0 IPv6 prefix: 64
IPv6 address of the default gateway: 2001::1
Configure the DNS Server IPv6 address? (yes/no) [n]: yes
  DNS IP address: 2001::101
Configure the default domain name? (yes/no) [n]: yes
  Default domain name: domainname.com
Following configurations will be applied:
  Switch Fabric=A
  System Name=foo
  Enforced Strong Password=no
  Physical Switch Mgmt0 IPv6 Address=2001::107
```

```
Physical Switch Mgmt0 IPv6 Prefix=64
Default Gateway=2001::1
Ipv6 value=1
DNS Server=2001::101
Domain Name=domainname.com
Apply and save the configuration (select 'no' if you want to re-enter)? (yes/no): yes
```

Firepower Chassis Manager 로그인 또는 로그아웃

유효한 사용자 어카운트를 사용하여 로그인해야 Firepower Chassis Manager를 사용하여 Firepower 4100/9300 새시를 구성할 수 있습니다. 사용자 어카운트에 대한 자세한 내용은 [사용자 관리, 23 페이지](#)의 내용을 참조하십시오.

어떤 활동 없이 일정 기간이 경과하는 경우, 시스템에서 자동으로 로그아웃됩니다. 기본적으로 10분 동안 사용하지 않을 경우 시스템에서 로그아웃됩니다. 이 시간 제한 설정을 구성하려면 [세션 시간 제한 구성, 33 페이지](#)의 내용을 참조하십시오. 또한, 세션이 활성화된 경우에도 특정 기간 이후에 시스템에서 사용자가 로그아웃되는 시간 제한 절대값 설정을 구성할 수 있습니다. 이 시간 제한 절대값 설정을 구성하려면 [세션 시간 제한 절대값 구성, 34 페이지](#)의 내용을 참조하십시오.

Firepower Chassis Manager에서 자동으로 로그아웃되는 모든 시스템 변경 사항 목록은 [Firepower Chassis Manager 세션 종료를 야기하는 시스템 변경 사항, 69 페이지](#)의 내용을 참조하십시오.



참고

선택적으로 특정 로그인 실패 횟수만 허용한 후에 지정된 시간 동안 사용자가 잠기도록 Firepower Chassis Manager를 구성할 수 있습니다. 이 옵션은 시스템에서 공통 기준 인증 컴플라이언스를 달성하기 위해 제공된 숫자 중 하나입니다. 자세한 내용은 [보안 인증 컴플라이언스, 49 페이지](#)를 참조하십시오.

절차

단계 1 다음을 수행하여 Firepower Chassis Manager에 로그인합니다.

- a) 지원되는 브라우저를 사용하여 주소 표시줄에 다음 URL을 입력합니다.
`https://<chassis_mgmt_ip_address>`

여기서 <chassis_mgmt_ip_address>는 초기 컨피그레이션 시 입력한 Firepower 4100/9300 새시의 IP 주소 또는 호스트 이름입니다.

참고 지원되는 브라우저에 대한 정보는 사용 중인 버전에 대한 릴리스 노트를 참조하십시오 (<http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html> 참조).

- b) 사용자 이름 및 비밀번호를 입력합니다.
- c) **Login**(로그인)을 클릭합니다.

로그인하면 Firepower Chassis Manager가 열리고 Overview(개요) 페이지가 표시됩니다.

단계 2 Firepower Chassis Manager에서 로그아웃하려면 네비게이션 바에서 사용자 이름을 가리킨 다음 **Logout**(로그아웃)을 선택합니다.

Firepower Chassis Manager에서 로그아웃되고 로그인 화면으로 돌아갑니다.

FXOS CLI 액세스

콘솔 포트에 연결된 터미널을 사용하여 FXOS CLI에 연결할 수 있습니다. 콘솔 포트에 연결된 컴퓨터 터미널(또는 콘솔 서버)의 콘솔 포트 매개변수가 다음과 같은지 확인합니다.

- 9600 보(baud)
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

SSH 및 텔넷을 사용하여 FXOS CLI에 연결할 수도 있습니다. Firepower eXtensible 운영 체제는 최대 8개의 동시 SSH 연결을 지원합니다. SSH를 사용하여 연결하려면 Firepower 4100/9300 채시의 IP 주소 또는 호스트 이름을 알아야 합니다.

다음 구문 예시 중 하나를 사용하여 SSH, 텔넷 또는 Putty로 로그인할 수 있습니다.



참고 SSH 로그인에서는 대/소문자를 구분합니다.

SSH를 사용하는 Linux 터미널의 경우:

- **sshucs-auth-domain\username@{UCSM-ip-address|UCMS-ipv6-address}**
`ssh ucs-example\jsmith@192.0.20.11`
`ssh ucs-example\jsmith@2001::1`
- **ssh -lucs-auth-domain\username {UCSM-ip-address|UCSM-ipv6-address|UCSM-host-name}**
`ssh -l ucs-example\jsmith 192.0.20.11`
`ssh -l ucs-example\jsmith 2001::1`
- **ssh {UCSM-ip-address|UCSM-ipv6-address|UCSM-host-name} -lucs-auth-domain\username**
`ssh 192.0.20.11 -l ucs-example\jsmith`
`ssh 2001::1 -l ucs-example\jsmith`
- **sshucs-auth-domain\username@{UCSM-ip-address|UCSM-ipv6-address}**
`ssh ucs-ldap23\jsmith@192.0.20.11`
`ssh ucs-ldap23\jsmith@2001::1`

텔넷을 사용하는 Linux 터미널의 경우:



참고 텔넷은 기본적으로 비활성화되어 있습니다. 텔넷 활성화에 대한 지침은 [텔넷 구성, 90 페이지](#)의 내용을 참조하십시오.

- **telnet ucs-UCSM-host-name ucs-auth-domain\username**
`telnet ucs-qa-10`
`login: ucs-ldap23\blradmin`

- `telnetucs-{UCSM-ip-address|UCSM-ipv6-address}ucs-auth-domain\username`

```
telnet 10.106.19.12 2052
ucs-qa-10-A login: ucs-ldap23\bladmin
```

Putty 클라이언트의 경우:

- Login as: `ucs-auth-domain\username`

```
Login as: ucs-example\jsmith
```



참고 기본 인증이 로컬로 설정되고 콘솔 인증이 LDAP으로 설정된 경우 `ucs-local\admin` 을 사용하여 Putty 클라이언트에서 패브릭 인터커넥트에 로그인할 수 있습니다. 여기서 `admin`은 로컬 어카운트의 이름입니다.



3 장

ASA용 라이선스 관리

Cisco Smart Software Licensing을 사용하면 중앙 집중식으로 라이선스 풀을 구매하고 관리할 수 있습니다. 각 유닛의 라이선스 키를 관리할 필요 없이 손쉽게 디바이스를 구축하거나 사용 중단할 수 있습니다. Smart Software Licensing은 라이선스 사용량과 수요를 한 번에 확인하게 해줍니다.



참고

이 섹션은 Firepower 4100/9300 채시의 ASA 논리적 디바이스에만 적용됩니다. Firepower Threat Defense 논리적 디바이스의 라이선싱에 대한 자세한 내용은 Firepower Management Center 컨피그레이션 가이드를 참조하십시오.

- [Smart Software Licensing 정보, 11페이지](#)
- [Smart Software Licensing 사전 요구 사항, 15페이지](#)
- [Smart Software Licensing 지침, 16페이지](#)
- [Smart Software Licensing의 기본값, 16페이지](#)
- [일반 Smart Software Licensing 구성, 16페이지](#)
- [Smart License Satellite Server 구성 - Firepower 4100/9300 채시, 18페이지](#)
- [영구 라이선스 예약 구성, 19페이지](#)
- [Smart Software Licensing 기록, 21페이지](#)

Smart Software Licensing 정보

이 섹션에서는 Smart Software Licensing이 적용되는 방법에 대해 설명합니다.



참고 이 섹션은 Firepower 4100/9300 새시의 ASA 논리적 디바이스에만 적용됩니다. Firepower Threat Defense 논리적 디바이스의 라이선싱에 대한 자세한 내용은 Firepower Management Center 컨피그레이션 가이드를 참조하십시오.

ASA용 Smart Software Licensing

Firepower 4100/9300 새시의 ASA 애플리케이션의 경우, Smart Software Licensing 컨피그레이션은 Firepower 4100/9300 새시 슈퍼바이저와 애플리케이션으로 나뉩니다.

- Firepower 4100/9300 새시 — 슈퍼바이저에 모든 Smart Software Licensing 인프라를 구성합니다 (License Authority와 통신하는 데 필요한 파라미터 포함). Firepower 4100/9300 새시 자체는 작동하기 위한 라이선스가 필요하지 않습니다.



참고 새시 간 클러스터링을 위해 클러스터에서 각 새시에 동일한 Smart Licensing 방법을 활성화해야 합니다.

- ASA 애플리케이션 — 애플리케이션에서 모든 라이선스 엔타이틀먼트를 구성합니다.

Smart Software Manager 및 어카운트

디바이스 라이선스를 1개 이상 구매한 경우, Cisco Smart Software Manager에서 라이선스를 관리할 수 있습니다.

<https://software.cisco.com/#module/SmartLicensing>

Smart Software Manager를 활용하면 조직에서 사용할 마스터 어카운트를 만들 수 있습니다.



참고 아직 어카운트가 없는 경우 [새 어카운트 설정](#) 링크를 클릭합니다. Smart Software Manager를 활용하면 조직에서 사용할 마스터 어카운트를 만들 수 있습니다.

기본적으로 라이선스는 마스터 어카운트의 기본 가상 어카운트에 할당됩니다. 어카운트 관리자로서 선택적으로 추가 가상 어카운트를 생성할 수 있습니다. 예를 들어, 지역, 부서 또는 자회사에 대해 어카운트를 생성할 수 있습니다. 여러 가상 어카운트를 활용하면 많은 라이선스 및 디바이스를 더 쉽게 관리할 수 있습니다.

오프라인 관리

디바이스에서 인터넷에 액세스할 수 없으며 License Authority에 등록할 수 없는 경우, 오프라인 라이선싱을 구성할 수 있습니다.

영구 라이선스 예약

보안상의 이유로 디바이스에서 인터넷에 액세스할 수 없는 경우 선택적으로 각 ASA에 대해 영구 라이선스를 요청할 수 있습니다. 영구 라이선스에는 License Authority에 대한 주기적인 액세스가 필요하지 않습니다. PAK 라이선스와 같이 라이선스를 구매하고 ASA용 라이선스 키를 설치합니다. 그러나 PAK 라이선스와 달리 Smart Software Manager를 사용하여 라이선스를 얻고 관리합니다. 일반 Smart Licensing 모드와 영구 라이선스 예약 모드 간을 쉽게 전환할 수 있습니다.

모든 기능을 활성화하는 라이선스를 얻을 수 있습니다(최대 보안 상황 및 캐리어 라이선스가 있는 표준 계층). 라이선스는 Firepower 4100/9300 새시에서 관리되지만 ASA가 사용을 허용하도록 ASA 컨피그레이션에서 엔타이틀먼트를 요청해야 합니다.

Satellite 서버

보안상의 이유로 디바이스에서 인터넷에 액세스할 수 없는 경우 선택적으로 로컬 Smart Software Manager Satellite 서버를 VM(가상 머신)으로 설치할 수 있습니다. Satellite에서는 Smart Software Manager 기능의 하위 집합을 제공하며, 모든 로컬 디바이스에 대한 필수 라이선싱 서비스를 제공할 수 있도록 허용합니다. Satellite의 경우에만 라이선스 사용량을 동기화하려면 기본 License Authority에 주기적으로 연결해야 합니다. 예약하여 동기화하거나 수동으로 동기화할 수 있습니다.

Satellite 애플리케이션을 다운로드 및 구축하고 나면 인터넷을 사용하여 Cisco SSM에 데이터를 전송하지 않고도 다음 기능을 수행할 수 있습니다.

- 라이선스 활성화 또는 등록
- 회사의 라이선스 확인
- 회사 엔터티 간 라이선스 양도

자세한 내용은 [Smart Account Manager Satellite](#)의 Smart Software Manager Satellite 설치 및 컨피그레이션 가이드를 참조하십시오.

가상 어카운트별로 관리되는 라이선스 및 디바이스

라이선스 및 디바이스는 가상 어카운트별로 관리됩니다. 가상 어카운트의 디바이스에서만 해당 어카운트에 할당된 라이선스를 사용할 수 있습니다. 추가 라이선스가 필요할 경우 다른 가상 어카운트의 미사용 라이선스를 이전할 수 있습니다. 또한, 가상 어카운트 간에 디바이스를 이전할 수도 있습니다.

Firepower 4100/9300 새시만 디바이스로 등록되며, 새시의 ASA 애플리케이션은 고유한 라이선스를 요청합니다. 예를 들어, 보안 모듈이 3개 있는 Firepower 9300 새시의 경우 새시는 디바이스 1개로 간주되지만 모듈은 별도의 라이선스를 3개 사용합니다.

평가판 라이선스

Firepower 4100/9300 새시는 두 가지 유형의 평가판 라이선스를 지원합니다.

- 새시 레벨 평가 모드 — Firepower 4100/9300 새시가 Licensing Authority에 등록되기 전에 평가 모드로 90일(총 사용량) 동안 작동됩니다. ASA는 이 모드에서 특정 엔타이틀먼트를 요청할 수 없으며, 기본 엔타이틀먼트만 활성화됩니다. 이 기간이 끝나면 Firepower 4100/9300 새시는 컴플라이언스 위반 상태가 됩니다.
- 엔타이틀먼트 기반 평가 모드 — Firepower 4100/9300 새시가 Licensing Authority에 등록되고 나면 ASA에 할당 가능한 시간 기반 평가 라이선스를 얻을 수 있습니다. ASA에서 평소와 같이 엔타이틀먼트를 요청하십시오. 시간 기반 라이선스가 만료되면 시간 기반 라이선스를 갱신하거나 영구 라이선스를 얻어야 합니다.



참고 강력한 암호화(3DES/AES)를 위한 평가 라이선스는 받을 수 없습니다. 즉, 영구 라이선스만 이 엔타이틀먼트를 지원합니다.

Smart Software Manager 통신

이 섹션에서는 디바이스가 Smart Software Manager와 통신하는 방법을 설명합니다.

디바이스 등록 및 토큰

각 가상 어카운트에서 등록 토큰을 생성할 수 있습니다. 이 토큰은 기본적으로 30일간 유효합니다. 각 새시를 구축할 때 또는 기존 새시를 등록할 때 이 토큰 ID와 엔타이틀먼트 레벨을 입력합니다. 기존 토큰이 만료되면 새 토큰을 생성할 수 있습니다.

구축 후 시작할 때 또는 기존 새시에서 이러한 파라미터를 수동으로 구성한 후에 새시가 Cisco License Authority에 등록됩니다. 새시를 토큰과 함께 등록하면 License Authority는 새시와 License Authority 간의 통신을 위한 ID 인증서를 발급합니다. 이 인증서는 6개월마다 갱신되지만 1년간 유효합니다.

License Authority와의 정기적인 통신

디바이스는 30일마다 License Authority와 통신합니다. Smart Software Manager에서 변경하는 경우 디바이스에서 권한 부여를 새로고침하여 변경 사항을 즉시 적용할 수 있습니다. 또는 디바이스에서 예정대로 통신할 때까지 기다릴 수 있습니다.

선택적으로 HTTP 프록시를 구성할 수 있습니다.

Firepower 4100/9300 새시는 적어도 90일마다 직접 또는 HTTP 프록시를 통해 인터넷에 액세스할 수 있어야 합니다. 일반 라이선스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 디바이스는 최대 90일간 Call Home 없이 작동할 수 있습니다. 유예 기간이 지나면 License Authority와 통신해야 합니다. 그렇지 않으면 특별 라이선스가 필요한 기능의 컨피그레이션을 변경할 수 없지만 작업은 달리 영향을 받지 않습니다.

규정 위반 상태

디바이스는 다음과 같은 상황에서 컴플라이언스 위반 상태가 될 수 있습니다.

- 과다 사용 — 디바이스에서 사용 불가능한 라이선스를 사용하는 경우
- 라이선스 만료 — 시간 기반 라이선스가 만료되는 경우
- 통신 부재 — 디바이스에서 권한 재부여를 위해 Licensing Authority에 연결하지 못하는 경우

어카운트가 컴플라이언스 위반 상태인지 또는 컴플라이언스 위반 상태에 근접한지를 확인하려면, Firepower 4100/9300 새시에서 현재 사용 중인 엔타이틀먼트와 Smart Account의 엔타이틀먼트를 비교해야 합니다.

컴플라이언스 위반 상태인 경우 특별 라이선스가 필요한 기능의 컨피그레이션을 변경할 수 없지만 작업은 달리 영향을 받지 않습니다. 예를 들어, 표준 라이선스 제한을 통한 기존 상황을 계속 실행할 수 있으며 이러한 컨피그레이션을 수정할 수 있지만 새로운 상황을 추가할 수는 없습니다.

Smart Call Home 인프라

기본적으로, Smart Call Home 프로파일은 Licensing Authority의 URL을 지정하는 FXOS 컨피그레이션에 있습니다. 이 프로파일은 제거할 수 없습니다. 라이선스 프로파일의 유일한 컨피그레이션 옵션은 License Authority의 대상 주소 URL입니다. Cisco TAC에서 지시하지 않는 한 License Authority URL을 변경해서는 안 됩니다.

Smart Software Licensing 사전 요구 사항

- 이 장은 Firepower 4100/9300 새시에 있는 ASA 논리적 디바이스에만 적용됩니다. Firepower Threat Defense 논리적 디바이스의 라이선싱에 대한 자세한 내용은 Firepower Management Center 컨피그레이션 가이드를 참조하십시오.
- Cisco Smart Software Manager에서 마스터 어카운트를 만듭니다.
<https://software.cisco.com/#module/SmartLicensing>
아직 어카운트가 없는 경우 **새 어카운트 설정** 링크를 클릭합니다. Smart Software Manager를 활용하면 조직에서 사용할 마스터 어카운트를 만들 수 있습니다.
- **Cisco Commerce Workspace**에서 라이선스를 1개 이상 구매합니다. 홈페이지의 **Find Products and Solutions**(제품 및 솔루션 찾기) 검색 필드에서 플랫폼을 검색합니다. 일부 라이선스는 무료이지만 Smart Software Licensing 어카운트에 추가해야 합니다.
- 새시에서 Licensing Authority와 통신할 수 있도록 새시에서 인터넷 액세스 또는 HTTP 프록시 액세스를 보장합니다.
- 새시에서 Licensing Authority의 이름을 확인할 수 있도록 DNS 서버를 구성합니다.
- 새시의 시간을 설정합니다.

- ASA 라이선싱 엔타이틀먼트를 구성하기 전에 Firepower 4100/9300 새시에서 Smart Software Licensing 인프라를 구성합니다.

Smart Software Licensing 지침

장애 조치 및 클러스터링을 위한 **ASA** 지침

각 Firepower 4100/9300 새시를 License Authority 또는 Satellite 서버에 등록해야 합니다. 보조 유닛에는 추가 비용이 없습니다. 영구 라이선스 예약의 경우, 각 새시의 개별 라이선스를 구매해야 합니다.

Smart Software Licensing의 기본값

Firepower 4100/9300 새시 기본 컨피그레이션에는 Licensing Authority의 URL을 지정하는 Smart Call Home 프로필 “SLProf”가 포함되어 있습니다.

일반 Smart Software Licensing 구성

Cisco License Authority와 통신하기 위해 선택적으로 HTTP 프록시를 구성할 수 있습니다. License Authority에 등록하려면 Smart Software License 어카운트에서 얻은 Firepower 4100/9300 새시에 등록 토큰 ID를 입력해야 합니다.

절차

-
- 단계 1 (선택 사항) HTTP 프록시 구성, 16 페이지
 - 단계 2 License Authority에 Firepower Security Appliance 등록, 17 페이지
-

(선택 사항) HTTP 프록시 구성

네트워크에서 인터넷 액세스를 위해 HTTP 프록시를 사용하는 경우, Smart Software Licensing에 대한 프록시 주소를 구성해야 합니다. 이 프록시는 일반적으로 Smart Call Home에도 사용됩니다.



참고 인증을 사용하는 HTTP 프록시는 지원되지 않습니다.

절차

-
- 단계 1 **System**(시스템) > **Licensing**(라이선싱) > **Call Home**을 선택합니다.

Call Home 페이지에서는 License Authority의 대상 주소 URL 구성 및 HTTP 프록시 구성을 위한 필드가 제공됩니다.

참고 Cisco TAC에서 지시하지 않는 한 License Authority URL을 변경해서는 안 됩니다.

단계 2 Server Enable(서버 활성화) 드롭다운 목록에서 **on(켜짐)**을 선택합니다.

단계 3 **Server URL**(서버 URL) 및 **Server Port**(서버 포트) 필드에 프록시 IP 주소와 포트를 입력합니다. 예를 들어, HTTPS 서버에 대해 포트 443을 입력합니다.

단계 4 **Save**(저장)를 클릭합니다.

(선택 사항) Call Home URL 삭제

다음 절차를 사용하여 이전에 구성한 Call Home URL을 삭제합니다.

절차

단계 1 **System**(시스템) > **Licensing**(라이선싱) > **Call Home**을 선택합니다.

단계 2 **Call home Configuration**(Call home 컨피그레이션) 영역에서 **Delete**(삭제)를 선택합니다.

License Authority에 Firepower Security Appliance 등록

Firepower 4100/9300 새시를 등록하면 License Authority에서는 Firepower 4100/9300 새시와 License Authority 간의 통신을 위해 ID 인증서를 발급합니다. 또한, Firepower 4100/9300 새시를 적절한 가상 어카운트에 할당합니다. 일반적으로 이 절차는 1회 수행됩니다. 그러나 예를 들어 나중에 통신 문제 때문에 ID 인증서가 만료되는 경우 Firepower 4100/9300 새시를 다시 등록해야 할 수 있습니다.

절차

단계 1 Smart Software Manager 또는 Smart Software Manager Satellite에서 이 Firepower 4100/9300 새시를 추가할 가상 어카운트의 등록 토큰을 요청 및 복사합니다.

Smart Software Manager Satellite를 사용하여 등록 토큰을 요청하는 방법에 대한 자세한 내용은 Cisco Smart Software Manager Satellite 사용자 가이드(http://www.cisco.com/web/software/286285517/138897/Smart_Software_Manager_satellite_4.1.0_User_Guide.pdf)를 참조하십시오.

단계 2 Firepower Chassis Manager에서 **System**(시스템) > **Licensing**(라이선싱) > **Smart License**(스마트 라이선스)를 선택합니다.

단계 3 **Enter Product Instance Registration Token**(제품 인스턴스 등록 토큰 입력) 필드에 등록 토큰을 입력합니다.

단계 4 **Register**(등록)를 클릭합니다.

Firepower 4100/9300 새시에서 License Authority 등록을 시도합니다.

디바이스의 등록을 취소하려면 **Unregister**(등록 취소)를 클릭합니다.

Firepower 4100/9300 새시의 등록을 취소하면 어카운트에서 해당 디바이스가 제거됩니다. 디바이스의 모든 라이선스 엔타이틀먼트 및 인증서가 제거됩니다. 새 Firepower 4100/9300 새시의 라이선스를 위해 공간을 비워두려면 등록을 취소할 수 있습니다. 또는 Smart Software Manager에서 해당 디바이스를 제거할 수 있습니다.

Smart License Satellite Server 구성 - Firepower 4100/9300 새시

다음 절차에서는 Smart License Satellite Server를 사용하도록 Firepower 4100/9300 새시를 구성하는 방법을 보여줍니다.

시작하기 전에

- [Smart Software Licensing 사전 요구 사항, 15 페이지](#)에 나열된 모든 사전 요구 사항을 완료합니다.
- Cisco.com에서 [Smart License Satellite OVA](#) 파일을 다운로드하고 VMwareESXi 서버에 이 파일을 설치 및 구성합니다. 자세한 내용은 [Smart Software Manager Satellite 설치 가이드](#)를 참조하십시오.
- 인증서 체인이 아직 없는 경우, 다음 절차를 사용하여 하나를 요청합니다.
 - 키 링을 생성합니다([키 링 생성, 99 페이지](#)).
 - 키 링에 대한 인증서 요청을 생성합니다([기본 옵션을 사용하여 키 링에 대한 인증서 요청 생성, 100 페이지](#)).
 - 이 인증서 요청을 트러스트 앵커 또는 인증 기관에 전송하여 키 링에 대한 인증서 체인을 얻습니다.

자세한 내용은 [인증서, 키 링 및 트러스트 포인트, 98 페이지](#)를 참조하십시오.

절차

- 단계 1 **System**(시스템) > **Licensing**(라이선싱) > **Call Home**을 선택합니다.
- 단계 2 **Call home Configuration**(Call Home 컨피그레이션) 영역에서 **Address**(주소) 필드의 기본 URL을 Satellite URL(https://ip_address/Transportgateway/services/DeviceRequestHandler)로 교체합니다.
- 단계 3 새 트러스트 포인트를 생성합니다. FXOS CLI를 사용하여 새 트러스트 포인트를 생성해야 합니다.
- 단계 4 **License Authority**에 **Firepower Security Appliance** 등록, [17 페이지](#). Smart License Manager Satellite에서 등록 토큰을 요청하고 복사해야 합니다.

영구 라이선스 예약 구성

영구 라이선스를 Firepower 4100/9300 새시에 할당할 수 있습니다. 이 범용 예약을 통해 디바이스에서 무제한으로 모든 엔타이틀먼트를 사용하도록 허용할 수 있습니다.



참고

시작하기 전에 Smart Software Manager에서 사용할 수 있도록 영구 라이선스를 구매해야 합니다. 모든 어카운트가 영구 라이선스 예약에 대해 승인되지 않습니다. 이 기능을 구성하려고 시도하기 전에 이 기능에 대해 Cisco의 승인을 받아야 합니다.

영구 라이선스 설치

다음 절차에서는 Firepower 4100/9300 새시에 영구 라이선스를 할당하는 방법을 보여줍니다.

절차

- 단계 1 **System > Licensing > Permanent License**를 선택합니다.
- 단계 2 예약 요청 코드를 생성하려면 **Generate**를 클릭합니다. 예약 요청 코드를 클립보드에 복사합니다.
- 단계 3 Cisco Smart Software Manager 포털에서 Smart Software Manager 인벤토리 화면으로 이동하고 **Licenses**(라이선스) 탭을 클릭합니다.
<https://software.cisco.com/#SmartLicensing-Inventory>
Licenses(라이선스) 탭은 어카운트와 관련된 모든 기존 라이선스(일반 및 영구 라이선스)를 표시합니다.
- 단계 4 **License Reservation**(라이선스 예약)을 클릭하고 생성된 예약 요청 코드를 상자에 붙여넣습니다.
- 단계 5 **Reserve License**(라이선스 예약)를 클릭합니다.
Smart Software Manager는 권한 부여 코드를 생성합니다. 코드를 다운로드하거나 클립보드에 복사할 수 있습니다. 이 시점에 라이선스는 Smart Software Manager에서 사용되고 있습니다.
License Reservation(라이선스 예약) 버튼이 보이지 않는 경우, 어카운트에 영구 라이선스 예약 권한이 없음을 의미합니다. 이 경우, 영구 라이선스 예약을 비활성화하고 일반 스마트 라이선스 명령을 다시 입력해야 합니다.
- 단계 6 Firepower Chassis Manager에서 **Authorization Code** 텍스트 상자에 생성된 권한 부여 코드를 입력합니다.
- 단계 7 **Install**(설치)을 클릭합니다.
Firepower 4100/9300 새시의 라이선스가 PLR로 완전히 부여되고 나면 **Permanent License**(영구 라이선스) 페이지에 라이선스 상태가 표시되며 영구 라이선스를 반환하는 옵션이 제공됩니다.
- 단계 8 ASA 논리적 디바이스에서 기능 엔타이틀먼트를 활성화합니다. 엔타이틀먼트를 활성화하려면 [ASA 라이선싱](#) 장을 참조하십시오.

(선택 사항) 영구 라이선스 반환

더 이상 영구 라이선스가 필요하지 않은 경우, 이 절차를 수행하여 해당 라이선스를 Smart Software Manager에 공식적으로 반환해야 합니다. 모든 단계를 따르지 않는 경우, 라이선스는 사용 중인 상태로 유지되며 다른 곳에서 사용할 수 없습니다.

절차

-
- 단계 1 **System > Licensing > Permanent License**를 선택합니다.
 - 단계 2 **Return**을 클릭하여 반환 코드를 생성합니다. 반환 코드를 클립보드에 복사합니다. Firepower 4100/9300 새시의 라이선스가 즉시 해제되고 평가 상태로 이동됩니다.
 - 단계 3 Smart Software Manager 인벤토리 화면으로 이동하고 **Product Instances**(제품 인스턴스) 탭을 클릭합니다.
<https://software.cisco.com/#SmartLicensing-Inventory>
 - 단계 4 UDI(범용 디바이스 식별자)를 사용하여 Firepower 4100/9300 새시를 검색합니다.
 - 단계 5 **Actions**(작업) > **Remove**(제거)를 선택하고 생성된 반환 코드를 상자에 붙여넣습니다.
 - 단계 6 **Remove Product Instance**(제품 인스턴스 제거)를 클릭합니다.
영구 라이선스가 사용 가능한 풀로 반환됩니다.
-

Smart Software Licensing 기록

기능 이름	플랫폼 릴리스	설명
Firepower 4100/9300 새시용 Cisco Smart Software Licensing	1.1(1)	<p>Smart Software Licensing을 사용하면 라이선스 풀을 구입하고 관리할 수 있습니다. 스마트 라이선스는 특정 시리얼 번호에 연결되어 있지 않습니다. 각 유닛의 라이선스 키를 관리할 필요 없이 손쉽게 디바이스를 구축하거나 사용 중단할 수 있습니다. Smart Software Licensing은 라이선스 사용량과 수요를 한 번에 확인하게 해줍니다. Smart Software Licensing 컨피그레이션은 Firepower 4100/9300 새시 슈퍼바이저와 보안 모듈로 나뉩니다.</p> <p>다음 화면을 도입했습니다.</p> <p>System(시스템) > Licensing(라이선싱) > Call Home</p> <p>System(시스템) > Licensing(라이선싱) > Smart License(스마트 라이선스)</p>



사용자 관리

- 사용자 어카운트, 23페이지
- 사용자 이름 지침, 24페이지
- 비밀번호 지침, 25페이지
- 원격 인증에 관한 지침, 26페이지
- 사용자 역할, 29페이지
- 로컬 인증 사용자의 비밀번호 프로필, 29페이지
- 사용자 설정 구성, 30페이지
- 세션 시간 제한 구성, 33페이지
- 세션 시간 제한 절대값 구성, 34페이지
- 최대 로그인 시도 횟수 설정, 35페이지
- 사용자 잠금 상태 보기 및 지우기, 36페이지
- 최소 비밀번호 길이 확인 구성, 37페이지
- 로컬 사용자 어카운트 생성, 37페이지
- 로컬 사용자 어카운트 삭제, 39페이지
- 로컬 사용자 어카운트 활성화 또는 비활성화, 39페이지
- 로컬 인증 사용자에 대한 비밀번호 기록 지우기, 40페이지

사용자 어카운트

사용자 계정을 사용하여 시스템에 액세스합니다. 로컬 사용자 어카운트는 최대 48개 구성할 수 있습니다. 각 사용자 계정에는 고유한 사용자 이름 및 비밀번호가 있어야 합니다.

관리자 계정

관리자 계정은 기본 사용자 계정이며 수정하거나 삭제할 수 없습니다. 이 계정은 시스템 관리자 또는 슈퍼 사용자(superuser) 계정이며 전체 권한을 갖습니다. 관리자 어카운트에는 기본 비밀번호가 할당되지 않으므로 초기 시스템 설정 시 비밀번호를 선택해야 합니다.

관리자 어카운트는 항상 활성 상태이며 만료되지 않습니다. 관리자 어카운트는 비활성 상태로 구성할 수 없습니다.

로컬 인증 사용자 어카운트

로컬 인증 사용자 어카운트는 새시를 통해 직접 인증되며, 관리자 또는 AAA 권한을 보유한 사용자에 의해 활성화 또는 비활성화될 수 있습니다. 로컬 사용자 계정이 비활성화되면 사용자가 로그인할 수 없습니다. 비활성화된 로컬 사용자 계정에 대한 컨피그레이션 세부사항은 데이터베이스에 의해 삭제되지 않습니다. 비활성화된 로컬 사용자 어카운트를 다시 활성화하면 해당 어카운트는 사용자 이름 및 비밀번호를 포함하여 기존 컨피그레이션으로 다시 활성화됩니다.

원격 인증 사용자 어카운트

원격 인증 사용자 어카운트는 LDAP, RADIUS 또는 TACACS+를 통해 인증되는 모든 사용자 어카운트를 가리킵니다.

사용자가 로컬 사용자 어카운트와 원격 사용자 어카운트를 동시에 유지할 경우 로컬 사용자 어카운트에 정의된 역할이 원격 사용자 어카운트의 역할을 재정의합니다.

원격 인증 지침에 대한 자세한 내용과 원격 인증 제공자를 구성 및 삭제하는 방법을 확인하려면 다음 항목을 참조하십시오.

- [원격 인증에 관한 지침, 26 페이지](#)
- [LDAP 제공자 구성, 109 페이지](#)
- [RADIUS 제공자 구성, 113 페이지](#)
- [TACACS+ 제공자 구성, 116 페이지](#)

사용자 계정 만료

미리 정의된 시간에 만료하도록 사용자 계정을 구성할 수 있습니다. 만료 시간이 되면 사용자 어카운트가 비활성화됩니다.

기본적으로 사용자 계정은 만료되지 않습니다.

만료일이 지정된 사용자 계정을 구성한 후에는 이 어카운트가 만료되지 않도록 재구성할 수 없습니다. 그러나 계정에 최신 만료일을 사용할 수 있도록 구성할 수는 있습니다.

사용자 이름 지침

사용자 이름은 Firepower Chassis Manager 및 FXOS CLI의 로그인 ID로도 사용됩니다. 사용자 어카운트에 로그인 ID를 할당할 때 다음 지침 및 제한 사항을 고려합니다.

- 로그인 ID는 1~32자이며 다음을 포함할 수 있습니다.

- 모든 영문자
 - 모든 숫자
 - _(밑줄)
 - -(대시)
 - .(점)
- 로그인 ID는 고유해야 합니다.
 - 로그인 ID는 영문자로 시작해야 합니다. 로그인 ID는 숫자 또는 특수 문자(예: 밑줄)로 시작할 수 없습니다.
 - 로그인 ID는 대/소문자를 구분합니다.
 - 전부 숫자로 된 로그인 ID는 만들 수 없습니다.
 - 사용자 어카운트를 만든 후에는 로그인 ID를 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 생성해야 합니다.

비밀번호 지침

로컬에서 인증되는 각 사용자 계정에는 비밀번호가 필요합니다. 관리자 또는 AAA 권한이 있는 사용자는 사용자 비밀번호에 대한 비밀번호 보안 강도를 확인하도록 시스템을 구성할 수 있습니다. 비밀번호 강도 확인이 활성화되면 각 사용자는 강력한 비밀번호를 사용해야 합니다.

각 사용자는 강력한 비밀번호를 사용하는 것이 좋습니다. 로컬로 인증된 사용자를 위해 비밀번호 보안 강도 확인을 활성화한 경우, Firepower eXtensible 운영 체제에서는 다음 요건을 충족하지 않는 비밀번호를 거부합니다.

- 최소 8자, 최대 80자를 포함해야 합니다.



참고 공통 기준 요건을 준수하도록 시스템에서 15자의 최소 비밀번호 길이를 선택적으로 구성할 수 있습니다. 자세한 내용은 [최소 비밀번호 길이 확인 구성, 37 페이지](#)를 참조하십시오.

- 하나 이상의 대문자 영문자를 포함해야 합니다.
- 하나 이상의 소문자 영문자를 포함해야 합니다.
- 하나 이상의 영숫자가 아닌(특수) 문자를 포함해야 합니다.
- aaabbb와 같이 한 문자가 3번 이상 연속적으로 반복되어서는 안 됩니다.
- 어떤 순서로도 3개의 연속되는 숫자 또는 문자(예: passwordABC 또는 password321)를 포함해서는 안 됩니다.
- 사용자 이름 또는 사용자 이름의 역순과 같아서는 안 됩니다.

- 비밀번호 사전 검사를 통과해야 합니다. 예를 들어, 비밀번호에 표준 사전 단어를 사용해서는 안 됩니다.
- \$(달러 기호), ?(물음표), =(등호) 기호를 포함해서는 안 됩니다.
- 로컬 사용자 및 관리자 어카운트는 비어 있지 않아야 합니다.

원격 인증에 관한 지침

지원되는 원격 인증 서비스 중 하나에 대해 시스템이 구성되어 있는 경우 Firepower 4100/9300 새시에서 시스템과 통신할 수 있도록 해당 서비스에 대한 제공자를 생성해야 합니다. 다음 지침은 사용자 권한 부여에 영향을 미칩니다.

원격 인증 서비스의 사용자 계정

사용자 어카운트는 로컬 Firepower 4100/9300 새시에 또는 원격 인증 서버에 존재할 수 있습니다.

Firepower Chassis Manager 또는 FXOS CLI에서 원격 인증 서비스로 로그인한 사용자의 임시 세션을 볼 수 있습니다.

원격 인증 서비스의 사용자 역할

원격 인증 서버에 사용자 어카운트를 생성하는 경우 해당 어카운트는 Firepower 4100/9300 새시에서 작업하는 데 필요한 역할을 포함해야 하며 해당 역할의 이름이 FXOS에서 사용되는 이름과 일치해야 합니다. 역할 정책에 따라 사용자가 로그인하지 못하거나 읽기 전용 권한만 가질 수도 있습니다.

원격 인증 제공자의 사용자 특성

RADIUS 및 TACAS+ 컨피그레이션에서는 각 원격 인증 제공자(이를 통해 사용자가 Firepower Chassis Manager 또는 FXOS CLI에 로그인)의 Firepower 4100/9300 새시에 대한 사용자 특성을 구성해야 합니다. 이 사용자 특성에는 각 사용자에게 할당된 역할 및 로컬이 저장됩니다.

사용자가 로그인하면 FXOS에서 다음을 수행합니다.

- 1 원격 인증 서비스에 대해 쿼리합니다.
- 2 사용자를 검증합니다.
- 3 사용자가 검증된 경우 사용자에게 할당된 역할 및 로컬을 확인합니다.

다음 표에서는 FXOS에서 지원하는 원격 인증 제공자의 사용자 특성 요구 사항을 비교합니다.

인증 제공자	맞춤형 특성	스키마 확장	특성 ID 요구 사항
LDAP	선택 사항	<p>다음 중 하나를 선택하여 수행할 수 있습니다.</p> <ul style="list-style-type: none"> LDAP 스키마를 확장하지 않고 요구 사항에 맞는 기존의 미사용 특성을 구성합니다. LDAP 스키마를 확장하고 CiscoAVPair와 같은 고유한 이름으로 맞춤형 특성을 생성합니다. 	<p>Cisco LDAP 구현에서는 유니코드 형식의 특성이 필요합니다.</p> <p>CiscoAVPair 맞춤형 특성을 생성하려는 경우 특성 ID로 1.3.6.1.4.1.9.287247.1을 사용합니다.</p> <p>샘플 OID는 다음 섹션에서 제공됩니다.</p>
RADIUS	선택 사항	<p>다음 중 하나를 선택하여 수행할 수 있습니다.</p> <ul style="list-style-type: none"> RADIUS 스키마를 확장하지 않고 요구 사항에 맞는 기존의 미사용 특성을 사용합니다. RADIUS 스키마를 확장하고 cisco-avpair와 같은 고유한 이름으로 커스텀 특성을 생성합니다. 	<p>Cisco RADIUS 구현에 대한 벤더 ID는 009, 특성에 대한 벤더 ID는 001입니다.</p> <p>다음 구문의 예에는 cisco-avpair 특성을 생성하려는 경우 여러 사용자 역할 및 로컬을 지정하는 방법이 나와 있습니다.</p> <pre>shell:roles="admin,aaa" shell:locales="L1,abc".</pre> <p>여러 값을 구분하는 기호로 쉼표 ","를 사용합니다.</p>

인증 제공자	맞춤형 특성	스키마 확장	특성 ID 요구 사항
TACAS	필수	스키마를 확장하고 <code>cisco-av-pair</code> 라는 이름으로 맞춤형 특성을 생성해야 합니다.	<p><code>cisco-av-pair</code> 이름은 TACACS+ 제공자에 대한 특성 ID를 제공하는 문자열입니다.</p> <p>다음 구문의 예에는 <code>cisco-av-pair</code> 특성을 생성하는 경우 여러 사용자 역할 및 로컬을 지정하는 방법이 나와 있습니다.</p> <pre>cisco-av-pair-shell:roles="admin aaa" shell:locales*"L1 abc".</pre> <p><code>cisco-av-pair</code> 특성 구문에 별표(*)를 사용하면 로컬에 선택 사항 플래그가 지정됩니다. 그러면 동일한 권한 부여 프로필을 사용하는 다른 Cisco 디바이스에 대한 인증이 실패하지 않습니다. 여러 값을 구분하는 기호로 공백을 사용합니다.</p>

LDAP 사용자 특성에 대한 샘플 OID

다음은 맞춤형 CiscoAVPair 특성에 대한 샘플 OID입니다.

```
CN=CiscoAVPair,CN=Schema,
CN=Configuration,CN=X
objectClass: top
objectClass: attributeSchema
cn: CiscoAVPair
distinguishedName: CN=CiscoAVPair,CN=Schema,CN=Configuration,CN=X
instanceType: 0x4
uSNCreated: 26318654
attributeID: 1.3.6.1.4.1.9.287247.1
attributeSyntax: 2.5.5.12
isSingleValued: TRUE
showInAdvancedViewOnly: TRUE
adminDisplayName: CiscoAVPair
adminDescription: UCS User Authorization Field
oMSyntax: 64
LDAPDisplayName: CiscoAVPair
```

name: CiscoAVPair
 objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,CN=X

사용자 역할

시스템에는 다음과 같은 사용자 역할이 있습니다.

관리자

전체 시스템에 대한 완전한 읽기 및 쓰기 액세스 권한이 있습니다. 이 역할에는 기본적으로 기본 관리자 어카운트가 할당되며 이는 변경할 수 없습니다.

읽기 전용

시스템 컨피그레이션에 대한 읽기 전용 액세스 권한이 있습니다(시스템 상태를 수정할 권한은 없음).

작업

NTP 컨피그레이션, Smart Licensing용 Smart Call Home 컨피그레이션, 시스템 로그(syslog 서버 및 결함 포함)에 대한 읽기 및 쓰기 액세스 권한이 있습니다. 나머지 시스템에 대해서는 읽기 액세스 권한이 있습니다.

AAA 관리자

사용자, 역할, AAA 컨피그레이션에 대한 읽기 및 쓰기 액세스 권한이 있습니다. 나머지 시스템에 대해서는 읽기 액세스 권한이 있습니다.

로컬 인증 사용자의 비밀번호 프로필

비밀번호 프로필에는 로컬에서 인증된 모든 사용자의 비밀번호 기록 및 비밀번호 변경 간격 속성이 포함됩니다. 로컬에서 인증된 각 사용자에게는 다른 비밀번호 프로필을 지정할 수 없습니다.

비밀번호 기록 수

비밀번호 기록 횟수를 사용하면 로컬에서 인증된 사용자가 같은 비밀번호를 반복적으로 재사용하는 것을 방지할 수 있습니다. 이 속성이 구성된 경우 Firepower 새시에서는 로컬로 인증된 사용자가 이전에 사용한 비밀번호를 최대 15개 저장합니다. 비밀번호는 가장 최근 비밀번호부터 먼저 시간 순서대로 저장되어 기록 횟수 임계값에 도달했을 때 가장 오래된 비밀번호만 재사용할 수 있도록 합니다.

비밀번호를 재사용하려면 사용자는 우선 비밀번호 기록 횟수에 구성되는 비밀번호의 수를 만들고 사용해야 합니다. 예를 들어 비밀번호 기록 횟수를 8로 설정한 경우, 로컬에서 인증된 사용자는 9번째 비밀번호가 만료될 때까지 첫 번째 비밀번호를 재사용할 수 없습니다.

기본적으로 비밀번호 기록 수는 0으로 설정되어 있습니다. 이 값은 기록 횟수를 비활성화하며 사용자가 이전 비밀번호를 언제든지 재사용할 수 있도록 합니다.

필요한 경우, 로컬에서 인증된 사용자의 비밀번호 기록 횟수를 지우고 이전 비밀번호 재사용을 활성화할 수 있습니다.

비밀번호 변경 간격

비밀번호 변경 간격을 사용하면 로컬에서 인증된 사용자가 지정된 시간 내에 수행 가능한 비밀번호 변경 횟수를 제한할 수 있습니다. 다음 표에서는 비밀번호 변경 간격의 두 가지 컨피그레이션 옵션을 설명합니다.

간격 컨피그레이션	설명	예
비밀번호 변경 허용 안 함	이 옵션은 로컬에서 인증된 사용자가 비밀번호 변경 후 지정된 시간 이내에는 비밀번호를 변경할 수 없도록 합니다. 변경 불가 간격을 1~745시간으로 지정할 수 있습니다. 기본적으로 변경 불가 간격은 24시간입니다.	예를 들어 로컬에서 인증된 사용자가 비밀번호를 변경한 후 48시간 이내에 비밀번호를 변경하지 못하도록 하려면 다음을 설정합니다. <ul style="list-style-type: none"> • 변경 지속 간격 - 비활성화 • 변경 불가 간격 - 48
변경 간격 내에서 비밀번호 변경 허용	이 옵션은 로컬에서 인증된 사용자가 사전 정의된 간격 내에 비밀번호를 변경할 수 있는 최대 횟수를 지정합니다. 변경 간격을 1~745시간으로 지정하고 비밀번호 변경 최대 횟수를 0~10으로 지정할 수 있습니다. 기본적으로 로컬에서 인증된 사용자는 48시간 간격 내에 비밀번호를 최대 2번 변경하는 것이 허용됩니다.	예를 들어 로컬에서 인증된 사용자가 비밀번호를 변경한 후 24시간 이내에 비밀번호를 최대 1번 변경할 수 있도록 하려면 다음과 같이 설정합니다. <ul style="list-style-type: none"> • 변경 지속 간격 - 활성화 • 변경 횟수 - 1 • 변경 간격 - 24

사용자 설정 구성

절차

-
- 단계 1 **System**(시스템) > **User Management**(사용자 관리)를 선택합니다.
 - 단계 2 **Settings**(설정) 탭을 클릭합니다.
 - 단계 3 다음 필드에 필수 정보를 입력합니다.

Name	설명
Default Authentication (기본 인증) 필드	원격 로그인 과정에서 사용자가 인증되는 기본 방법입니다. 다음 중 하나일 수 있습니다. <ul style="list-style-type: none"> • Local(로컬) — 사용자 계정이 Firepower 새시에서 로컬로 정의되어야 합니다. • Radius — 사용자 계정이 Firepower 새시에 지정된 RADIUS 서버에서 정의되어야 합니다. • TACACS — 사용자 계정이 Firepower 새시에 지정된 TACACS+ 서버에서 정의되어야 합니다. • LDAP — 사용자 계정이 Firepower 새시에 지정된 LDAP/MS-AD 서버에서 정의되어야 합니다. • None(없음) — 사용자 어카운트가 Firepower 새시에서 로컬인 경우, 사용자가 원격으로 로그인할 때 비밀번호가 필요하지 않습니다.
Console Authentication (콘솔 인증) 필드	콘솔 포트를 통해 FXOS CLI에 연결할 때 사용자가 인증되는 방법입니다. 다음 중 하나일 수 있습니다. <ul style="list-style-type: none"> • Local(로컬) — 사용자 계정이 Firepower 새시에서 로컬로 정의되어야 합니다. • Radius — 사용자 계정이 Firepower 새시에 지정된 RADIUS 서버에서 정의되어야 합니다. • TACACS — 사용자 계정이 Firepower 새시에 지정된 TACACS+ 서버에서 정의되어야 합니다. • LDAP — 사용자 계정이 Firepower 새시에 지정된 LDAP/MS-AD 서버에서 정의되어야 합니다. • None(없음) — 사용자 어카운트가 Firepower 새시에서 로컬인 경우, 사용자가 콘솔 포트를 사용하여 FXOS CLI에 연결할 때 비밀번호가 필요하지 않습니다.
원격 사용자 설정	

Name	설명
원격 사용자 역할 정책	<p>사용자가 로그인을 시도하고 원격 인증 제공자가 인증 정보와 함께 사용자 역할을 제공하지 않는 경우, 발생하는 결과를 제어합니다.</p> <ul style="list-style-type: none"> • Assign Default Role(기본 역할 할당) — 사용자가 읽기 전용 사용자 역할로 로그인할 수 있습니다. • No Login(로그인 안 함) — 사용자 이름 및 비밀번호가 올바른 경우에도 사용자가 시스템에 로그인할 수 없습니다.
로컬 사용자 설정	
Password Strength Check (비밀번호 보안 강도 확인) 확인란	이 확인란을 선택한 경우 모든 로컬 사용자 비밀번호는 강력한 비밀번호에 대한 지침을 준수해야 합니다(비밀번호 지침, 25 페이지 참조).
History Count (기록 수) 필드	<p>사용자가 이전에 사용한 비밀번호를 재사용하기 전에 생성해야 하는 고유한 비밀번호 수입니다. 기록 수는 최근 항목부터 시간순으로 저장되며, 기록 수 임계값에 도달할 경우 가장 오래된 비밀번호만 재사용할 수 있습니다.</p> <p>이 값은 0~15으로 선택할 수 있습니다.</p> <p>History Count(기록 수) 필드를 0으로 설정하여 기록 수를 비활성화하고 사용자가 언제든지 이전에 사용한 비밀번호를 재사용하게 할 수 있습니다.</p>
Change During Interval (해당 간격 동안 변경) 필드	<p>로컬로 인증된 사용자가 비밀번호를 변경할 수 있는 시기를 제어합니다. 다음을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> • Enable(활성화) — 로컬로 인증된 사용자는 Change Interval(변경 간격) 및 Change Count(변경 횟수)에 대한 설정을 기준으로 비밀번호를 변경할 수 있습니다. • Disable(비활성화) — 로컬로 인증된 사용자는 No Change Interval(변경 안 함 간격)에 지정된 기간 동안 비밀번호를 변경할 수 없습니다.
Change Interval (변경 간격) 필드	<p>Change Count(변경 횟수) 필드에 지정된 비밀번호 변경 횟수가 적용되는 시간입니다.</p> <p>이 값은 1~745시간으로 선택할 수 있습니다.</p> <p>예를 들어, 이 필드가 48로 설정되고 Change Count(변경 횟수) 필드가 2로 설정된 경우 로컬로 인증된 사용자는 48시간 이내에 비밀번호를 최대 2번 변경할 수 있습니다.</p>

Name	설명
Change Count (변경 횟수) 필드	로컬로 인증된 사용자가 변경 간격 동안 비밀번호를 변경할 수 있는 최대 횟수입니다. 이 값은 0~10으로 선택할 수 있습니다.
No Change Interval (변경 안 함 간격) 필드	로컬로 인증된 사용자가 새로 생성된 비밀번호를 변경하기 전에 기다려야 하는 최소 시간입니다. 이 값은 1~745시간으로 선택할 수 있습니다. 이 간격은 Change During Interval (해당 간격 동안 변경) 속성이 Disable (비활성화)로 설정되지 않은 경우 무시됩니다.

단계 4 **Save**(저장)를 클릭합니다.

세션 시간 제한 구성

FXOS CLI를 사용하여 Firepower 4100/9300 새시가 사용자 세션을 닫기 전에 사용자 활동 없이 경과할 수 있는 시간을 지정할 수 있습니다. 콘솔 세션 및 HTTPS, SSH 및 텔넷 세션에 대해 서로 다른 설정을 구성할 수 있습니다.

최대 3,600초(60분)의 시간 제한 값을 설정할 수 있습니다. 기본값은 600초입니다. 이 설정을 비활성화하려면 세션 시간 제한 값을 0으로 설정합니다.

절차

- 단계 1 보안 모드를 시작합니다.
Firepower-chassis # **scope security**
- 단계 2 기본 권한 부여 보안 모드를 시작합니다.
Firepower-chassis /security # **scopedefault-auth**
- 단계 3 HTTPS, SSH 및 텔넷 세션에 대한 유희 시간 제한을 설정합니다.
Firepower-chassis /security/default-auth # **set session-timeout seconds**
- 단계 4 (선택 사항) 콘솔 세션에 대한 유희 시간 제한을 설정합니다.
Firepower-chassis /security/default-auth # **set con-session-timeout seconds**
- 단계 5 (선택 사항) 세션 및 세션 시간 제한 절대값 설정을 확인합니다.
Firepower-chassis /security/default-auth # **show detail**

예제:

```

Default authentication:
Admin Realm: Local
Operational Realm: Local
Web session refresh period(in secs): 600
Session timeout(in secs) for web, ssh, telnet sessions: 600
Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
Serial Console Session timeout(in secs): 600
Serial Console Absolute Session timeout(in secs): 3600
Admin Authentication server group:
Operational Authentication server group:
Use of 2nd factor: No

```

세션 시간 제한 절대값 구성

Firepower 4100/9300 새시에는 세션 사용과 관계없이 세션 시간 제한 절대값 기간이 경과한 후에 사용자 세션을 닫는 세션 시간 제한 절대값 설정이 있습니다. 이 시간 제한 절대값 기능은 직렬 콘솔, SSH, HTTPS를 비롯한 모든 액세스 형식에 적용됩니다.

직렬 콘솔 세션에 대해 세션 시간 제한 절대값을 별도로 구성할 수 있습니다. 이렇게 하면 다른 형태의 액세스에 대한 시간 제한은 유지하면서 디버깅 요구 사항에 대한 직렬 콘솔 세션 시간 제한 절대값을 비활성화할 수 있습니다.

세션 시간 제한 절대값은 기본적으로 3,600초(60분)로 설정되며 FXOS CLI를 사용하여 변경할 수 있습니다. 이 설정을 비활성화하려면 세션 시간 제한 절대값을 0으로 설정합니다.

절차

- 단계 1 보안 모드를 시작합니다.
Firepower-chassis # **scope security**
- 단계 2 기본 권한 부여 보안 모드를 시작합니다.
Firepower-chassis /security # **scopedefault-auth**
- 단계 3 세션 시간 제한 절대값을 설정합니다.
Firepower-chassis /security/default-auth # **set absolute-session-timeout seconds**
- 단계 4 (선택 사항) 개별 콘솔 세션 시간 제한 절대값을 설정합니다.
Firepower-chassis /security/default-auth # **set con-absolute-session-timeout seconds**
- 단계 5 (선택 사항) 세션 및 세션 시간 제한 절대값 설정을 확인합니다.
Firepower-chassis /security/default-auth # **show detail**

예제:

```

Default authentication:
Admin Realm: Local
Operational Realm: Local
Web session refresh period(in secs): 600
Session timeout(in secs) for web, ssh, telnet sessions: 600

```

```
Absolute Session timeout(in secs) for web, ssh, telnet sessions: 3600
Serial Console Session timeout(in secs): 600
Serial Console Absolute Session timeout(in secs): 3600
Admin Authentication server group:
Operational Authentication server group:
Use of 2nd factor: No
```

최대 로그인 시도 횟수 설정

허용된 최대 횟수만큼 로그인 시도에 실패하면 지정된 시간 동안 사용자가 사용할 수 없도록 Firepower 4100/9300 새시를 구성할 수 있습니다. 설정된 최대 로그인 시도 횟수를 초과하는 경우 사용자가 사용할 수 없도록 시스템이 잠깁니다. 사용자가 잠겼음을 나타내는 알림은 나타나지 않습니다. 이 경우 사용자는 로그인을 시도하기 전에 지정된 시간 동안 기다려야 합니다.

최대 로그인 시도 횟수를 구성하려면 다음 단계를 수행합니다.



참고

- 최대 로그인 시도 횟수를 초과하고 나면 시스템에서 모든 유형의 사용자 어카운트(관리자 포함)가 잠깁니다.
- 성공하지 못한 로그인 시도의 기본 최대 수는 0회입니다. 최대 로그인 시도 횟수를 초과한 후에 사용자가 사용할 수 없도록 시스템이 잠기는 기본 시간은 30분(1,800초)입니다.
- 사용자의 잠금 상태를 확인하고 사용자의 잠금 상태를 지우는 단계에 대해서는 [사용자 잠금 상태 보기 및 지우기, 36 페이지](#)의 내용을 참조하십시오.

이 옵션은 시스템에서 공통 기준 인증 컴플라이언스를 달성하기 위해 제공된 숫자 중 하나입니다. 자세한 내용은 [보안 인증 컴플라이언스, 49 페이지](#)를 참조하십시오.

절차

- 단계 1** FXOS CLI에서 보안 모드를 시작합니다.

```
scopesystem
scopesecurity
```
- 단계 2** 최대 로그인 시도 실패 횟수를 설정합니다.

```
setmax-login-attempts
```

max_login
max_login 값은 0~10의 정수입니다.
- 단계 3** 최대 로그인 시도 횟수에 도달하고 나서 사용자가 사용할 수 없도록 시스템이 잠긴 상태로 유지되어야 하는 시간(초 단위)을 지정합니다.

```
setuser-account-unlock-time
```

unlock_time

- 단계 4 컨피그레이션을 커밋합니다.
commit-buffer

사용자 잠금 상태 보기 및 지우기

관리 사용자는 최대 로그인 시도 수 CLI 설정에 지정된 최대 로그인 시도 실패 횟수를 초과한 후 Firepower 4100/9300 새시을 사용하지 못하는 사용자의 잠금 상태를 확인하고 지울 수 있습니다. 자세한 내용은 [최대 로그인 시도 횟수 설정, 35 페이지](#)를 참조하십시오.

절차

- 단계 1 FXOS CLI에서 보안 모드를 시작합니다.
scopesystem
scopesecurity
- 단계 2 문제가 있는 사용자의 사용자 정보(잠금 상태 포함)를 표시합니다.
Firepower-chassis /security # **show local-user userdetail**

예제:

```
로컬 사용자:
이름:
성:
이메일:
전화번호:
만료: 해당 없음
비밀번호:
사용자 잠금 상태: 잠김
어카운트 상태: 활성
사용자 역할:
이름: 읽기 전용
사용자 SSH 공개 키:
```

- 단계 3 (선택 사항) 사용자의 잠금 상태를 지웁니다.
Firepower-chassis /security # **scope local-user user**
Firepower-chassis /security/local-user # **clear lock-status**

최소 비밀번호 길이 확인 구성

최소 비밀번호 길이 확인을 활성화하는 경우, 지정된 최소 문자 수를 지닌 비밀번호를 생성해야 합니다. 예를 들어 `min_length`(최소 길이) 옵션을 15로 설정하는 경우, 15자 이상을 사용하는 비밀번호를 생성해야 합니다. 이 옵션은 시스템에서의 공통 기준 인증 컴플라이언스를 위해 허용되는 숫자 중 하나입니다. 자세한 내용은 [보안 인증 컴플라이언스, 49 페이지](#)를 참조하십시오.

최소 비밀번호 길이 확인을 구성하려면 다음 단계를 수행합니다.

절차

-
- 단계 1 FXOS CLI에서 보안 모드를 시작합니다.
 - 단계 2 `scopesystem`
`scopesecurity`
 - 단계 3 비밀번호 프로파일 보안 모드를 시작합니다.
`scopepassword-profile`
 - 단계 4 최소 비밀번호 길이를 지정합니다.
`setmin-password-length min_length`
 - 단계 5 컨피그레이션을 커밋합니다.
`commit-buffer`
-

로컬 사용자 어카운트 생성

절차

-
- 단계 1 **System**(시스템) > **User Management**(사용자 관리)를 선택합니다.
 - 단계 2 **Local Users**(로컬 사용자) 탭을 클릭합니다.
 - 단계 3 **Add User**(사용자 추가)를 클릭하여 **Add User**(사용자 추가) 대화 상자를 엽니다.
 - 단계 4 다음 필드에 사용자 필수 정보를 입력합니다.

Name	설명
User Name(사용자 이름) 필드	이 어카운트에 로그인할 때 사용되는 어카운트 이름입니다. 이 이름은 고유해야 하며 사용자 어카운트 이름에 대한 지침 및 제한 사항을 따라야 합니다(사용자 이름 지침, 24 페이지 참조). 사용자를 저장하고 나면 로그인 ID를 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 생성해야 합니다.

Name	설명
First Name(이름) 필드	사용자의 이름입니다. 이 필드는 최대 32자를 포함할 수 있습니다.
Last Name(성) 필드	사용자의 성입니다. 이 필드는 최대 32자를 포함할 수 있습니다.
Email(이메일) 필드	사용자의 이메일 주소입니다.
Phone Number(전화번호) 필드	사용자의 전화번호입니다.
Password(비밀번호) 필드	이 어카운트의 비밀번호입니다. 비밀번호 보안 강도 확인을 활성화한 경우, 사용자의 비밀번호가 더욱 강력해지며 Firepower eXtensible 운영 체제는 다음 보안 강도 확인 요건을 충족하지 않는 비밀번호를 거부합니다(비밀번호 지침, 25 페이지 참조).
Confirm Password(비밀번호 확인) 필드	확인을 위해 두 번째로 입력하는 비밀번호입니다.
Account Status(계정 상태) 필드	상태가 Active(활성) 로 설정된 경우, 사용자는 이 로그인 ID와 비밀번호를 사용하여 Firepower Chassis Manager 및 FXOS CLI에 로그인할 수 있습니다.
User Role(사용자 역할) 목록	<p>사용자 어카운트에 할당할 권한에 해당하는 역할입니다(사용자 역할, 29 페이지 참조).</p> <p>모든 사용자에게는 기본적으로 읽기 전용 역할이 할당되며 이 역할은 선택 해제할 수 없습니다. 여러 역할을 할당하려면 Ctrl을 누른 상태로 원하는 역할을 클릭합니다.</p> <p>참고 사용자 역할 및 권한 변경 사항은 다음에 사용자가 로그인한 이후에 적용됩니다. 사용자 어카운트에 새 역할을 할당하거나 사용자 어카운트에서 기존 역할을 제거할 때 사용자가 로그인하는 경우, 활성화된 세션이 이전 역할 및 권한을 사용하여 작업을 계속합니다.</p>
Account Expires(계정 만료) 확인란	<p>이 확인란을 선택한 경우, Expiration Date(만료일) 필드에 지정된 날짜가 지나면 이 어카운트가 만료되어 사용할 수 없게 됩니다.</p> <p>참고 만료일이 지정된 사용자 계정을 구성한 후에는 이 어카운트가 만료되지 않도록 재구성할 수 없습니다. 그러나 계정에 최신 만료일을 사용할 수 있도록 구성할 수는 있습니다.</p>
Expiry Date(만료일) 필드	<p>어카운트가 만료되는 날짜입니다. 날짜는 yyyy-mm-dd 형식이어야 합니다.</p> <p>필드 끝의 달력 아이콘을 클릭하여 달력을 표시하고 만료일을 선택할 수 있습니다.</p>

단계 5 **Add**(추가)를 클릭합니다.

로컬 사용자 어카운트 삭제

절차

단계 1 **System**(시스템) > **User Management**(사용자 관리)를 선택합니다.

단계 2 **Local Users**(로컬 사용자) 탭을 클릭합니다.

단계 3 삭제할 사용자 어카운트의 행에서 **Delete**(삭제)를 클릭합니다.

단계 4 **Confirm**(확인) 대화 상자에서 **Yes**(예)를 클릭합니다.

로컬 사용자 어카운트 활성화 또는 비활성화

로컬 사용자 어카운트를 활성화하거나 비활성화하려면 사용자에게 관리자 또는 AAA 권한이 있어야 합니다.

절차

단계 1 **System**(시스템) > **User Management**(사용자 관리)를 선택합니다.

단계 2 **Local Users**(로컬 사용자) 탭을 클릭합니다.

단계 3 활성화하거나 비활성화할 사용자 어카운트의 행에서 **Edit**(편집)(연필 아이콘)을 클릭합니다.

단계 4 **Edit User**(사용자 편집) 대화 상자에서 다음 중 하나를 수행합니다.

- 사용자 어카운트를 활성화하려면 **Account Status**(어카운트 상태) 필드에서 **Active**(활성) 라디오 버튼을 클릭합니다.
- 사용자 어카운트를 비활성화하려면 **Account Status**(어카운트 상태) 필드에서 **Inactive**(비활성) 라디오 버튼을 클릭합니다.

관리자 사용자 계정은 항상 활성 상태로 설정됩니다. 수정할 수 없습니다.

단계 5 **Save**(저장)를 클릭합니다.

로컬 인증 사용자에게 대한 비밀번호 기록 지우기

절차

-
- 단계 1** 보안 모드를 시작합니다.
Firepower-chassis # **scopesecurity**
- 단계 2** 지정된 사용자 어카운트에 대한 로컬 사용자 보안 모드를 시작합니다.
Firepower-chassis /security # **scope local-user** *user-name*
- 단계 3** 지정된 사용자 어카운트에 대한 비밀번호 기록을 지웁니다.
Firepower-chassis /security/local-user # **clear password-history**
- 단계 4** 시스템 컨피그레이션에 트랜잭션을 커밋합니다.
Firepower-chassis /security/local-user # **commit-buffer**
-

다음 예에서는 비밀번호 기록을 지우고 트랜잭션을 커밋합니다.

```
Firepower-chassis # scope security
Firepower-chassis /security # scope local-user admin
Firepower-chassis /security/local-user # clear password-history
Firepower-chassis /security/local-user* # commit-buffer
Firepower-chassis /security/local-user #
```



이미지 관리

- [이미지 관리 정보](#), 41페이지
- [Cisco.com에서 이미지 다운로드](#), 42페이지
- [Firepower Security Appliance에 이미지 업로드](#), 42페이지
- [이미지 무결성 확인](#), 43페이지
- [Firepower eXtensible 운영 체제 플랫폼 번들 업그레이드](#), 43페이지
- [논리적 디바이스를 위한 이미지 버전 업데이트](#), 44페이지
- [펌웨어 업그레이드](#), 45페이지

이미지 관리 정보

Firepower 4100/9300 새시에서는 다음과 같은 두 가지 기본 이미지 유형을 사용합니다.



참고

모든 이미지는 보안 부팅을 통해 디지털로 서명되고 검증됩니다. 이미지를 수정하지 마십시오. 이미지를 수정하면 검증 오류를 수신하게 됩니다.

- 플랫폼 번들 — Firepower 플랫폼 번들은 Firepower Supervisor 및 Firepower 보안 모듈/엔진에서 작동하는 여러 개별 이미지가 모여 있는 컬렉션입니다. 플랫폼 번들은 Firepower eXtensible 운영 체제 소프트웨어 패키지입니다.
- 애플리케이션 — 애플리케이션 이미지는 Firepower 4100/9300 새시의 보안 모듈/엔진에 구축할 소프트웨어 이미지입니다. 애플리케이션 이미지는 CSP(Cisco Secure Package) 파일로 전송되며, 논리적 디바이스를 생성하거나 이후 논리적 디바이스 생성에 대비하기 위해 보안 모듈/엔진에 구축될 때까지 수퍼바이저에 저장됩니다. Firepower Supervisor에 저장된 동일한 애플리케이션 이미지 유형에 대해 여러 가지 다른 버전이 있을 수 있습니다.

**참고**

플랫폼 번들 이미지와 하나 이상의 애플리케이션 이미지를 모두 업그레이드하려면 먼저 플랫폼 번들을 업그레이드해야 합니다.

Cisco.com에서 이미지 다운로드

시작하기 전에

Cisco.com 어카운트가 있어야 합니다.

절차

- 단계 1 **System(시스템) > Updates(업데이트)**를 선택합니다.
Available Updates(사용 가능한 업데이트) 페이지는 새시에서 사용 가능한 FXOS 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.
- 단계 2 페이지 하단에서 **Download latest updates from CCO(CCO에서 최신 업데이트 다운로드)** 링크를 클릭합니다.
Firepower 4100/9300 새시에 대한 소프트웨어 다운로드 페이지가 브라우저에서 새 탭으로 열립니다.
- 단계 3 적절한 소프트웨어 이미지를 찾은 다음 로컬 컴퓨터에 다운로드합니다.

Firepower Security Appliance에 이미지 업로드

시작하기 전에

업로드할 이미지를 로컬 컴퓨터에서 사용할 수 있는지 확인합니다.

절차

- 단계 1 **System(시스템) > Updates(업데이트)**를 선택합니다.
Available Updates(사용 가능한 업데이트) 페이지는 새시에서 사용 가능한 Firepower eXtensible 운영 체제 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.
- 단계 2 **Upload Image(이미지 업로드)**를 클릭하여 Upload Image(이미지 업로드) 대화 상자를 엽니다.
- 단계 3 **Browse(찾아보기)**를 클릭하여 업로드할 이미지로 이동한 다음 해당 이미지를 선택합니다.
- 단계 4 **Upload(업로드)**를 클릭합니다.
선택한 이미지는 Firepower 4100/9300 새시에 업로드됩니다.
- 단계 5 특정 소프트웨어 이미지의 경우 이미지 업로드 후 엔드 유저 라이선스 계약이 함께 표시됩니다. 시스템 프롬프트에 따라 엔드 유저 라이선스 계약에 동의합니다.

이미지 무결성 확인

이미지 무결성은 새로운 이미지가 Firepower 4100/9300 새시에 추가되는 경우 자동으로 확인됩니다. 필요한 경우, 다음 절차를 사용하여 이미지 무결성을 수동으로 확인할 수 있습니다.

절차

- 단계 1 **System(시스템) > Updates(업데이트)**를 선택합니다.
Available Updates(사용 가능한 업데이트) 페이지는 새시에서 사용 가능한 Firepower eXtensible 운영 체제 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.
- 단계 2 확인할 이미지에 대해 **Verify(확인)**(체크 마크 아이콘)를 클릭합니다.
이미지의 무결성이 확인되며 Image Integrity(이미지 무결성) 필드에 상태가 표시됩니다.

Firepower eXtensible 운영 체제 플랫폼 번들 업그레이드

시작하기 전에

Cisco.com에서 플랫폼 번들 소프트웨어 이미지를 다운로드([Cisco.com에서 이미지 다운로드](#), 42 페이지 참조)한 다음 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다([Firepower Security Appliance에 이미지 업로드](#), 42 페이지 참조).



참고 업그레이드 프로세스에는 일반적으로 20~30분이 소요됩니다.

독립형 논리적 디바이스를 실행 중인 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스를 업그레이드하는 중인 경우 또는 인프라 새시 클러스터를 실행 중인 Firepower 9300 보안 어플라이언스를 업그레이드하는 중인 경우, 트래픽은 업그레이드 중에 디바이스를 통과하지 않습니다.

새시 간 클러스터의 일부인 Firepower 9300 또는 Firepower 4100 Series 보안 어플라이언스를 업그레이드하는 중인 경우, 트래픽은 업그레이드 중에 업그레이드되고 있는 디바이스를 통과하지 않습니다. 그러나 클러스터에 있는 다른 디바이스는 트래픽을 계속 전달합니다.

절차

- 단계 1 **System(시스템) > Updates(업데이트)**를 선택합니다.

Available Updates(사용 가능한 업데이트) 페이지는 새시에서 사용 가능한 Firepower eXtensible 운영 체제 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.

- 단계 2 업그레이드할 FXOS 플랫폼 번들에 대해 **Upgrade(업그레이드)**를 클릭합니다. 시스템은 설치할 소프트웨어 패키지를 먼저 확인합니다. 시스템은 현재 설치된 애플리케이션과 지정된 FXOS 플랫폼 소프트웨어 패키지 간에 비호환성이 있는지 알려줍니다. 또한 기존 세션이 종료되고 시스템이 업그레이드의 일부로 재부팅되어야 한다고 경고합니다.
- 단계 3 **Yes(예)**를 클릭하여 설치를 계속할지 확인하거나 **No(아니요)**를 클릭하여 설치를 취소합니다. Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다.

논리적 디바이스를 위한 이미지 버전 업데이트

시작하기 전에



참고

Firepower Threat Defense 논리적 디바이스의 초기 생성 이후에 Firepower Threat Defense 논리적 디바이스를 Firepower Chassis Manager 또는 FXOS CLI를 사용하여 업그레이드하지 마십시오. Firepower Threat Defense 논리적 디바이스를 업그레이드하려면 Firepower Management Center를 사용해야 합니다. 자세한 내용은 Firepower System 릴리스 노트를 참조하십시오. <http://www.cisco.com/c/en/us/support/security/defense-center/products-release-notes-list.html>

또한, Firepower Threat Defense 논리적 디바이스에 대한 업데이트는 **Logical Devices(논리적 디바이스) > Edit(편집) 및 System(시스템) > Updates(업데이트)** 페이지(Firepower Chassis Manager의 페이지)에 반영되지 않습니다. 이러한 페이지에서 표시된 버전은 Firepower Threat Defense 논리적 디바이스를 생성하는 데 사용된 소프트웨어 버전(CSP 이미지)을 나타냅니다.

Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드([Cisco.com에서 이미지 다운로드, 42 페이지](#) 참조)한 다음 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다([Firepower Security Appliance에 이미지 업로드, 42 페이지](#) 참조).

플랫폼 번들 이미지와 하나 이상의 애플리케이션 이미지를 모두 업그레이드하려면 먼저 플랫폼 번들을 업그레이드해야 합니다.

절차

- 단계 1 **Logical Devices(논리적 디바이스)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.

Logical Devices(논리적 디바이스) 페이지에는 새시에 구성된 논리적 디바이스의 목록이 표시됩니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.

- 단계 2 업데이트할 논리적 디바이스의 **Update Version**(버전 업데이트)을 클릭하여 **Update Image Version**(이미지 버전 업데이트) 대화 상자를 엽니다.
- 단계 3 **New Version**(새 버전)의 경우, 업데이트할 소프트웨어 버전을 선택합니다.
- 단계 4 **OK**(확인)를 클릭합니다.

펌웨어 업그레이드

다음 절차를 사용하여 Firepower 4100/9300 새시에서 펌웨어를 업그레이드합니다.

절차

- 단계 1 웹 브라우저를 사용하여 <http://www.cisco.com/go/firepower9300-software> 또는 <http://www.cisco.com/go/firepower4100-software>로 이동합니다.
Firepower 4100/9300 새시에 대한 소프트웨어 다운로드 페이지가 브라우저에서 열립니다.
- 단계 2 Cisco.com에서 적절한 펌웨어 패키지를 찾은 다음 Firepower 4100/9300 새시에서 액세스할 수 있는 서버로 다운로드합니다.
- 단계 3 Firepower 4100/9300 새시에서 펌웨어 모드를 시작합니다.
Firepower-chassis # **scopefirmware**
- 단계 4 FXOS 펌웨어 이미지를 Firepower 4100/9300 새시에 다운로드합니다.
Firepower-chassis /firmware # **download image URL**
다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.
 - **ftp:// username@hostname / path**
 - **scp:// username@hostname / path**
 - **sftp:// username@hostname / path**
 - **tftp:// hostname : port-num / path**
- 단계 5 다음 명령을 사용하여 다운로드 프로세스를 모니터링합니다.
Firepower-chassis /firmware # **show download task image_name detail**
- 단계 6 다운로드가 완료되면 다음 명령을 입력하여 펌웨어 패키지의 콘텐츠를 볼 수 있습니다.
Firepower-chassis /firmware # **show package image_name expand**
- 단계 7 다음 명령을 입력하여 펌웨어 패키지의 버전 번호를 볼 수 있습니다.
Firepower-chassis /firmware # **show package**
이 버전 번호는 펌웨어 패키지 설치 시 다음과 같은 단계에서 사용됩니다.
- 단계 8 펌웨어 패키지를 설치합니다.

- a) 펌웨어 설치 모드를 시작합니다.

```
Firepower-chassis /firmware # scope firmware-install
```

- b) 펌웨어 패키지를 설치합니다.

```
Firepower-chassis /firmware/firmware-install # install firmware pack-version version_number
```

시스템에서는 펌웨어 패키지를 검증하며, 검증 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있다고 알립니다.

- c) 검증을 계속하려면 **yes**를 입력합니다.

시스템에서는 펌웨어 패키지를 검증한 후, 설치 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있으며 업데이트 프로세스 도중 시스템이 재부팅될 것이라고 알립니다.

- d) 설치를 계속하려면 **yes**를 입력합니다. 업그레이드 프로세스 도중 Firepower 4100/9300 새시의 전원을 껐다가 다시 켜지 마십시오.

단계 9 업그레이드 프로세스를 모니터링하려면 다음을 수행합니다.

```
Firepower-chassis /firmware/firmware-install # show detail
```

단계 10 설치가 완료되고 나면 다음 명령을 입력하여 현재 펌웨어 버전을 볼 수 있습니다.

```
Firepower-chassis /firmware/firmware-install # top
```

```
Firepower-chassis # scope chassis 1
```

```
Firepower-chassis /firmware # show sup version
```

다음 예에서는 펌웨어를 버전 1.0.10으로 업그레이드합니다.

```
Firepower-chassis# scope firmware
Firepower-chassis /firmware # download image
tftp://10.10.10.1/fxos-k9-fpr9k-firmware.1.0.10.SPA
Firepower-chassis /firmware # show download-task fxos-k9-fpr9k-firmware.1.0.10.SPA detail
```

Download task:

```
File Name: fxos-k9-fpr9k-firmware.1.0.10.SPA
Protocol: Tftp
Server: 10.10.10.1
Port: 0
Userid:
Path:
```

```
Downloaded Image Size (KB): 2104
Time stamp: 2015-12-04T23:51:57.846
State: Downloading
```

```
Transfer Rate (KB/s): 263.000000
```

```
Current Task: unpacking image fxos-k9-fpr9k-firmware.1.0.10.SPA on primary(
FSM-STAGE:sam:dme:FirmwareDownloaderDownload:UnpackLocal)
```

```
Firepower-chassis /firmware # show package fxos-k9-fpr9k-firmware.1.0.10.SPA expand
```

```
Package fxos-k9-fpr9k-firmware.1.0.10.SPA:
```

```
Images:
  fxos-k9-fpr9k-fpga.1.0.5.bin
  fxos-k9-fpr9k-rommon.1.0.10.bin
```

```
Firepower-chassis /firmware # show package
```

Name	Version
-----	-----
fxos-k9-fpr9k-firmware.1.0.10.SPA	1.0.10

```
Firepower-chassis /firmware # scope firmware-install
```

```
Firepower-chassis /firmware/firmware-install # install firmware pack-version 1.0.10
```

```
Verifying FXOS firmware package 1.0.10. Verification could take several minutes.
```


Do you want to proceed? (yes/no):yes

FXOS SUP ROMMON: Upgrade from 1.0.10 to 1.0.10
FXOS SUP FPGA : Upgrade from 1.04 to 1.05

This operation upgrades SUP firmware on Security Platform.

Here is the checklist of things that are recommended before starting the install operation

- (1) Review current critical/major faults
- (2) Initiate a configuration backup

Attention:

The system will be reboot to upgrade the SUP firmware.

The upgrade operation will take several minutes to complete.

PLEASE DO NOT POWER RECYCLE DURING THE UPGRADE.

Do you want to proceed? (yes/no):yes

Upgrading FXOS SUP firmware software package version 1.0.10

command executed



보안 인증 컴플라이언스

- 보안 인증 컴플라이언스, 49페이지
- FIPS 모드 활성화, 50페이지
- 공통 기준 모드 활성화, 51페이지
- SSH 호스트 키 생성, 51페이지
- IPSec 보안 채널 구성, 52페이지
- 트러스트 포인트에 대한 정적 CRL 구성, 57페이지
- 인증서 해지 목록 확인 정보, 58페이지
- CRL의 정기적인 다운로드 구성, 62페이지
- NTP 서버 인증 활성화, 64페이지
- LDAP 키 링 인증서 설정, 65페이지
- IP 액세스 목록 구성, 65페이지
- 클라이언트 인증서 인증 활성화, 66페이지

보안 인증 컴플라이언스

미국 연방 정부 기관에서는 경우에 따라 미국 국방부 및 글로벌 인증 기관에서 수립한 보안 표준을 준수하는 장비와 소프트웨어만 사용해야 합니다. Firepower 4100/9300 새시는 이러한 여러 보안 인증 표준에 대해 컴플라이언스를 지원합니다.

이러한 표준에 대한 컴플라이언스를 지원하는 기능을 활성화하는 단계에 대해서는 다음 항목을 참조하십시오.

- FIPS 모드 활성화, 50 페이지
- 공통 기준 모드 활성화, 51 페이지
- IPSec 보안 채널 구성, 52 페이지

- 트러스트 포인트에 대한 정적 CRL 구성, 57 페이지
- 인증서 해지 목록 확인 정보, 58 페이지
- CRL의 정기적인 다운로드 구성, 62 페이지
- NTP 서버 인증 활성화, 64 페이지
- LDAP 키 링 인증서 설정, 65 페이지
- IP 액세스 목록 구성, 65 페이지
- 클라이언트 인증서 인증 활성화, 66 페이지
- 최소 비밀번호 길이 확인 구성, 37 페이지
- 최대 로그인 시도 횟수 설정, 35 페이지
- 사용자 역할, 29 페이지



참고

이러한 항목에서는 Firepower 4100/9300 새시에서의 인증 컴플라이언스 활성화에 대해서만 설명합니다. Firepower 4100/9300 새시에서 인증 컴플라이언스를 활성화하더라도 연결된 논리적 디바이스에 컴플라이언스가 자동으로 전파되지는 않습니다.

FIPS 모드 활성화

Firepower 4100/9300 새시에서 FIPS 모드를 활성화하려면 다음 단계를 수행합니다.

절차

- 단계 1 Firepower 4100/9300 새시에 관리 사용자로 로그인합니다.
- 단계 2 **Platform Settings**를 선택하여 Platform Settings(플랫폼 설정) 창을 엽니다.
- 단계 3 **FIPS/CC mode**를 선택하여 FIPS 및 공통 기준 창을 엽니다.
- 단계 4 FIPS에 대해 **Enable** 확인란을 선택합니다.
- 단계 5 **Save**를 클릭하여 컨피그레이션을 저장합니다.
- 단계 6 프롬프트에 따라 시스템을 재부팅합니다.

다음에 할 작업

FXOS 릴리스 2.0.1 이전 버전의 경우 디바이스의 첫 번째 설정 시 생성된 기존 SSH 호스트 키가 1024 비트로 하드 코딩되어 있습니다. FIPS 및 공통 기준 인증 요건을 준수하려면 기존의 호스트 키를 삭제하고 **SSH 호스트 키 생성, 51 페이지**에 자세히 나와 있는 절차를 사용하여 새로운 호스트 키를 생성해야 합니다. 이러한 추가 단계를 수행하지 않으면 FIPS 모드가 활성화된 상태에서 디바이스가 재

부팅된 이후에 SSH를 사용하여 수퍼바이저에 연결할 수 없습니다. FXOS 2.0.1 이후 버전을 사용하여 초기 설정을 수행한 경우, 호스트 키를 새로 생성할 필요가 없습니다.

공통 기준 모드 활성화

Firepower 4100/9300 새시에서 공통 기준 모드를 활성화하려면 다음 단계를 수행합니다.

절차

-
- 단계 1 Firepower 4100/9300 새시에 관리 사용자로 로그인합니다.
 - 단계 2 **Platform Settings**를 선택하여 Platform Settings(플랫폼 설정) 창을 엽니다.
 - 단계 3 **FIPS/CC mode**를 선택하여 FIPS 및 공통 기준 창을 엽니다.
 - 단계 4 공통 기준에 대해 **Enable** 확인란을 선택합니다.
 - 단계 5 **Save**를 클릭하여 컨피그레이션을 저장합니다.
 - 단계 6 프롬프트에 따라 시스템을 재부팅합니다.
-

다음에 할 작업

FXOS 릴리스 2.0.1 이전 버전의 경우 디바이스의 첫 번째 설정 시 생성된 기존 SSH 호스트 키가 1024비트로 하드 코딩되어 있습니다. FIPS 및 공통 기준 인증 요건을 준수하려면 기존의 호스트 키를 삭제하고 [SSH 호스트 키 생성, 51 페이지](#)에 자세히 나와 있는 절차를 사용하여 새로운 호스트 키를 생성해야 합니다. 이러한 추가 단계를 수행하지 않으면 공통 기준 모드가 활성화된 상태에서 디바이스가 재부팅된 이후에 SSH를 사용하여 수퍼바이저에 연결할 수 없습니다. FXOS 2.0.1 이후 버전을 사용하여 초기 설정을 수행한 경우, 호스트 키를 새로 생성할 필요가 없습니다.

SSH 호스트 키 생성

FXOS 릴리스 2.0.1 이전 버전의 경우 디바이스의 초기 설정 시 생성된 기존 SSH 호스트 키가 1024비트로 하드 코딩되었습니다. FIPS 및 공통 기준 인증을 준수하려면 기존의 호스트 키를 삭제하고 새로운 호스트 키를 생성해야 합니다. 자세한 내용은 [FIPS 모드 활성화, 50 페이지](#) 또는 [공통 기준 모드 활성화, 51 페이지](#)를 참고하십시오.

기존의 SSH 호스트 키를 삭제하고 새로운 인증-준수 호스트 키를 생성하려면 다음 단계를 수행합니다.

절차

-
- 단계 1 FXOS CLI에서 서비스 모드를 시작합니다.
`scopesystem`
`scopeservices`

- 단계 2 SSH 호스트 키를 삭제합니다.
deletessh-serverhost-key
- 단계 3 컨피그레이션을 커밋합니다.
commit-buffer
- 단계 4 SSH 호스트 키 크기를 2048비트로 설정합니다.
setssh-serverhost-keyrsa 2048
- 단계 5 컨피그레이션을 커밋합니다.
commit-buffer
- 단계 6 새로운 SSH 호스트 키를 생성합니다.
createssh-serverhost-key
commit-buffer
- 단계 7 새로운 호스트 키 크기를 확인합니다.
showssh-serverhost-key
호스트 키 크기: 2048

IPSec 보안 채널 구성

Firepower 4100/9300 새시에서 IPSec을 구성하여 공용 네트워크를 통과하는 데이터 패킷에 대한 엔드 투 엔드 데이터 암호화 및 인증 서비스를 제공할 수 있습니다. 이 옵션은 시스템에서 공통 기준 인증 컴플라이언스를 달성하기 위해 제공된 숫자 중 하나입니다. 자세한 내용은 [보안 인증 컴플라이언스, 49 페이지](#)를 참조하십시오.



참고 IKE와 SA 연결 간에 일치하는 암호화 키 보안 강도가 적용되도록 구성하는 경우(아래 절차에서 sa-strength-enforcement를 yes(예)로 설정):

SA 적용이 활성화된 경우	IKE 협상 키 크기가 ESP 협상 키 크기보다 작은 경우, 연결이 실패합니다. IKE 협상 키 크기가 ESP 협상 키 크기보다 크거나 같은 경우, SA 적용 확인을 통과하며 연결이 성공합니다.
SA 적용이 비활성화된 경우	SA 적용 확인을 통과하며 연결이 성공합니다.

IPSec 보안 채널을 구성하려면 다음 단계를 수행합니다.

절차

단계 1 FXOS CLI에서 보안 모드를 시작합니다.

```
scopesystem  
scopesecurity
```

단계 2 키 링을 생성합니다.

```
enterkeyringssp  
!createcertreqsubject-name subject-nameip ip
```

단계 3 연결된 인증서 요청 정보를 입력합니다.

```
entercertreq
```

단계 4 국가를 설정합니다.

```
setcountry 국가
```

단계 5 DNS를 설정합니다.

```
setdns dns
```

단계 6 이메일을 설정합니다.

```
sete-mail email
```

단계 7 IP 정보를 설정합니다.

```
setfi-a-ip fi-a-ip  
setfi-a-ipv6 fi-a-ipv6  
setfi-b-ip fi-b-ip  
setfi-b-ipv6 fi-b-ipv6  
setipv6 ipv6
```

단계 8 지역을 설정합니다.

```
setlocality 지역
```

단계 9 조직 이름을 설정합니다.

```
setorg-name org-name
```

단계 10 조직 단위 이름을 설정합니다.

```
setorg-unit-name org-unit-name
```

단계 11 비밀번호를 설정합니다.

```
!setpassword
```

단계 12 상태를 설정합니다.

```
setstate state
```

단계 13 certreq에 대한 주체 이름을 설정합니다.

```
setsubject-name subject-name
```

단계 14 종료합니다.

```
exit
```

단계 15 모듈러스를 설정합니다.

```
setmodulus modulus
```

단계 16 인증서 요청에 대한 재생성을 설정합니다.

```
setregenerate { yes | no }
```

단계 17 트러스트 포인트를 설정합니다.

```
settrustpointinterca
```

단계 18 종료합니다.

```
exit
```

단계 19 새로 생성한 트러스트 포인트를 입력합니다.

```
entertrustpointinterca
```

단계 20 인증서 서명 요청을 생성합니다.

```
setcertchain
```

예제:

```
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgIBADANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBACMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQlUxCzAJBgNVBAMMAkNBMR0wGAYJKoZIhvcNAQkBFgtzc3BAC3NwLm5l
dDAeFw0xNjEyMDgxOTMzNTJaFw0yNjEyMDYxOTMzNTJaMHAcCzAJBgNVBAYTAiVT
MQswCQYDVQQIDAJDQTEMMAoGA1UEBwwDU0pDMQ4wDAYDVQQKDAVDaXNjbzENMA5G
A1UECwwEU1RCVTELMakGA1UEAwwCQ0ExGjAYBgkqhkiG9w0BCQEWc3NzcEBzc3Au
bmV0MIICijANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA2ukWyMLQuLqTvhq7
zFb3Oz/iyDG/ui6mrLIYn8wE3E39XcXA1/x9IHCmxFKNJdD7EbsggfOuy0Bj+Y4s
+uZ1VapBXV/JrAie7bNn3ZYrI29yuyOrIqoi9k9gL/oRBzH18BwBwGHBOz3hGrSK
Yc2yhsq9y/6yI3nSuLZm6ybmUKjTa+B4YuhDTz4hl/I9x/J5nbGiab3vLDKss1nO
xP9+1+Lc690V18/mNPWdJcJDI+U/L9keYs/rbZdRSeXy9kMae42+4FIRHDJjPcSN
Yw1g/gcR2F7QUKRygKckJKXDX2QliGYSetlSHj18O87o5s/pmQAWWRGkKpfDv3oH
cMPgI2T9rC0D8NNcgPXj9PFKfexoNGGwNTO85fK3kjgModWbdeMG3EihxEEOUPD0
Fdu0HrTM5lvwb+vr5wE9HsAiMJ8UuujmHqH5mlwyy3Me+cEDHo0hLeNs+AFrqEXQ
e9S+KZC/dq/9zOLpRsVqSfJsAuVI/QdPDbWShjflE/fP2Wj01PqXywQydzymVvgE
wEZaoFg+mlGJm0+q4RDvnpzEviOYNsAGmOkILh5HQ/eYDcxvd0qbORWb31H32ySl
Ila6UTT9+vnND1f838fxvNvr8nyGD2S/LVaxnZlO4jcSIvtdizbbT8u5B4VcLKIC
x0vkqjo6RvNZJ52sUaD9C3UodTUCAwEAAaOBgTB/MC8GA1UdHwQoMCYwJKAioCCG
Hmh0dHA6Ly8xOTIuMTY4LjQuMjkvcm9vdGNhLmNybdAdBgNVHQ4EFgQU7Jg01A74
jpx8U0APk76pVfYQQ5AwHwYDVR0jBBgwFoAU7Jg01A74jpx8U0APk76pVfYQQ5Aw
DAYDVR0TBAAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEA2ukWyMLQuLqTvhq7
W7DRmszPUWQ7edor7yxuQzHLVFFOwYRudsyXbv7INR3rJ/X1cRQj9+KidWWVxpo
pFahRhzyXVZ10DHKIzGTQS3jiHgrF3Z8ohWbL15L7PEDlrxMBoJvabPeQRgTmY/n
XZJ7qRYbypO3gUMCaCZ12raJc3/DIpbQ29yweCbUkc9qiHKA0IbnvAxoroHWmBld
94LrJcggfMQTuNJQszJiVVsYJfZ+utlDp2QwfdDv7B0JkwTBjdwRSfotEbc5R18n
BNXYHqxuoNMmqbS3KjCLXcH6xIN8t+Ukfp89hvJt/fluj+s/VJSVZWK4tAwvR7w1
QngCKRjW6FYpzeyNBctiJ07wO+Wt4e3KhIjJdyvA9hFixWcVGdf2r6QW5BYbgGOK
DkHb/gdr/bcdLBKN/PtSJ+prSrpBSaA6rJX8D9UmfhqqN/3f+sS1fM4qWORJc6G2
gAcg7AjEQ/odo512vAI8p8idOg/Wv1O17mavzLpcue05cwMCX9fKxKZZZ/+7Pk19Y
ZrXS6uMn/CGnViptn0w+uJ1IRj1oulk+/ZyPtBvFHUkFRnhoWj5SMFyds2Iaaty1
47N2ViaZBxhU3GICaH+3O+8rs9Kkz9tBZDSnEJVZA6yxaNCVP1bRUO20G3oRTmSx
8iLBJN+BXggxMmG8ssHisgw=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
```



```

MIIFqDCCA5CgAwIBAgIBBDANBgkqhkiG9w0BAQsFADBwMQswCQYDVQQGEwJVUzEL
MAkGA1UECAwCQ0ExDDAKBgNVBAMMA1NKQzEOMAwGA1UECgwFQ2lzY28xDTALBgNV
BAsMBFNUQUIUxCzAJBgNVBAMMAkNBMRRowGAYJKoZIhvcNAQkBFgtzc3BAc3NwLm5l
dDAeFw0xNjEyMTUyMTM0NTRaFw0yNjEyMTMyMTM0NTRaMHwxCzAJBgNVBAYTAIVT
MQswCQYDVQQIDAJDQTEPMA0GA1UECgwGbmV3c3RnMRAwDgYDVQQLDAduZXdzdGJl
MRMwEQYDVQQDDAppbnRlcm0xLWNhMSgwJgYJKoZIhvcNAQkBFhlpbnRlcm0xLWNh
QGluZGVybTEtY2EubmV0MIICljANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEA
wLpNnyEx5I4P8uDoWKWF3IZseghLANsodxuAUmhmwKekd0OpZZxHMw1wSO4IBX5
4itJS0xyXFzPmeptG3OXvNqCcsT+4BXI3DoGgPMULccc4NesHeg2z8+q3SPA6uZh
iseWNvKfnUjixbQEBtcrWBiSKnZuOz1cpuBn34gtgeFFoCEXN+EZVpPESiandVh
8pCPlipc/08ZJ3o9GW2j0eHJN84sguEDL812ROejQvpmfqGUq11stkIuh+wB+V
VRhUBVG7pV57I6DHeeRp6cDMLXaM3iMTelhdShyo5YUaRJMak/t8kCqhtGXfuLII
E2AkxKXeeveR9n6cpQd5JiNzCT/t9IQL/T/CCqMICRXLFP LCS9o5S5O2B6QFgcTZ
yKR6hsmwe22wpK8QI7/5oWNXl0lb96hHJ7RPbG7RXYqmcLiXY/d2j9/RuNoPJawI
hLkfoldPA28xlnfB1azCmMmdPcBO6cbUQfCj5hSmk3StVQKJcJaujz55TGGd1
GjnxDMX9twzw7Ee51895Xmtr24qqaCXJoW/dPhcIIXRdJPMsTJ4yPG0BieuRwd0p
i8w/rFwbHzv4C9Fthw1JrRxH1yeHJHrLIZgJ5txSaVUIgrgVCJaf6/jrRRWoRJwt
AvznzYql2dZPCcEAYgP7JcaQpvdpuDgq++NgBtygiqECAwEAANBMD8wDAYDVR0T
BAUwAwEB/zAvBgNVHR8EKDAmMCSglqAghh5odHRwOi8vMTkyLjE2OC40LjI5L2lu
dGVybzS5jcmwwDQYJKoZIhvcNAQELBQADggIBAG/XujJh5G5UWo+cwTSitAezWbJA
h1dAiXZ/OYWZSxkFRliErKdupLqL0ThjnX/wRFfEXbrBQwm5kWAUUDr97D1Uz+2A
8LC5I8SWKXmyf0jUtsnEQbDZb33oVL7yXJk/A0SF0jihpPheMA+YRazalT9xj9KH
PE7nHCJMbb2ptrHUyvBrKSYrSeEqOpQU2+otnFyV3rS9aelgVjuaWyaWoc3lZ1Oi
CC2tJvY3NnM56j5iesxUCeY/SZ2/ECXN7RRBViLHmA3gFKmWf3xeNiKkxmJCxOaa
UWPC1x2V66I8DG9uUzlWy79O2dy52aAphAHC6hqlzb6v+gw1Tld7UxaqVd8CD5W
ATjNs+ifkJS1h5ERxHjgcurZXOpR+NwPwF+UDzbMXxx+KAAXCI6ltCd8Pb3wOUC3
PKvwEXalcCcxGx71eRLpWPZFyEoi4N2NGE9OXRjz0K/KERZgNhsIw3bQMjcw3aX6
OXskEuKgsayctnWyxVqNnqvuz06kqyubh4+ZgGKZ5LNEXYmGNz3oED1rUN636Tw
SjGAPHgeROzyTFDixCeiaROIgDp/Hwvb0/+uThIe89g8WZ0djTKFUM8uBO3f+II
/cbuyBO1+JrDMq8NkAjkIJI1p1c3WbfCue/qcwtcfUBYZ4i53a56UNF5E0rpy/8
B/+07Me/p2y9Luqa
-----END CERTIFICATE-----
ENDOFBUF
    
```

단계 21 인증서 서명 요청을 표시합니다.

showcertreq

예제:

```

Firepower-chassis# /security/keyring # show certreq
Certificate request subject name: SSP
Certificate request ip address: 192.168.0.111
Certificate request FI A ip address: 0.0.0.0
Certificate request FI B ip address: 0.0.0.0
Certificate request e-mail name:
Certificate request ipv6 address: ::
Certificate request FI A ipv6 address: ::
Certificate request FI B ipv6 address: ::
Certificate request country name: US
State, province or county (full name): CA
Locality name (eg, city): SJC
Organisation name (eg, company): Cisco
Organisational Unit Name (eg, section): Sec
DNS name (subject alternative name):
Request:
-----BEGIN CERTIFICATE REQUEST-----
    
```

```

MIICwTCCAakCAQAwVTELMakGA1UEBhMCVVMxZzA1BjBGNVBAgMAkNBMQwwCgYDVQQH
DANTSkMxDjAMBGNVBAoMBUNpc2NvMQ0wCwYDVQQLDARTVEJVMQwwCgYDVQQDDANT
U1AwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAAoIBAQDq292Rq3t0laoxPbfE
p/ITKr6rxFhPqSSbtm6sXer//VZFiDTWODockDItuf4Kja215mIS0RyvEYVeRgAs
wbN459wm0BASd8xCjIhsuHDV7yHu539BnvRW6Q2o+gHeSRwckqjCIK/tsIxsPkV0
6OduZYXk2bnsLWs6tNk3uzOIT2Q0FcZ1ET66C8fyyKWTrmvcZjDjkMm2nDFsPIX9
39TYPItDkJE3PocqyaCqmT4uobOuvQeLJh/efkBvwhb4BF8vzwRpHWTdjjU5YnR1
qiR4q7j1RmzVFxCDY3IVP/KDBoa5NyCLEUZCEP5QCQFDzIRETZwVOKtxUVG0Nljd
K5TxAgMBAAGgJzAIBGkqhkiG9w0BCQ4xGDAWMBQGA1UdEQQNMAuCA1NTUicEwKgA
rjANBgkqhkiG9w0BAQsFAAOCQAQEARTRBoInxXkBYNIVeEoFCqKttu3+Hc7UdyoRM
2L2pjx5OHbQICC+8NRVRMYujTnp67BWuUZZI03dGP4/lbN6bC9P3CvkZdKUsJkN0
m1Ye9dgz7MO/KEcosarmoMI9WB8LlweVdt6ycSdJzs9shOxwT6TAZPwL7gq/1ShF
Rjh6sq5W9p6E0SjYefK62E7MatRjDjS8DXoxj6gfn9DqK15iVpkK2QqT5rneSGj+
R+20TcUnT0h/S5K/bySEM/3U1gFxQCOzbzPuHkj28kXAVczmTxXEkJBFLVduWN06
DT3u0xImiPR1sqW1jpMwbhC+ZGDtvgKjKHToagup9+8R9IMcBQ==
-----END CERTIFICATE REQUEST-----

```

- 단계 22 IPSec 모드를 시작합니다.
scopeipsec
- 단계 23 로그 상세 레벨을 설정합니다.
setlog-level log_level
- 단계 24 IPSec 연결을 생성하고 입력합니다.
enterconnection connection_name
- 단계 25 IPSec 모드를 터널 또는 전송으로 설정합니다.
setmode tunnel_or_transport
- 단계 26 로컬 IP 주소를 설정합니다.
setlocal-addr ip_address
- 단계 27 원격 IP 주소를 설정합니다.
setremote-addr ip_address
- 단계 28 터널 모드를 사용하는 경우, 원격 서브넷을 설정합니다.
setremote-subnet ip/mask
- 단계 29 (선택 사항) 원격 ID를 설정합니다.
setremote-ike-ident remote_identity_name
- 단계 30 키 링 이름을 설정합니다.
setkeyring-name 이름
- 단계 31 (선택 사항) 키 링 비밀번호를 설정합니다.
setkeyring-passwd passphrase
- 단계 32 (선택 사항) IKE-SA 수명을 분 단위로 설정합니다.
setike-rekey-time 분
minutes 값은 60~1440 사이의 정수가 가능합니다.
- 단계 33 (선택 사항) 하위 SA 수명을 분 단위(30~480분)로 설정합니다.
setesp-rekey-time 분
minutes 값은 30~480의 정수가 될 수 있습니다.

- 단계 34 (선택 사항) 초기 연결 시 수행할 재전송 시퀀스 수를 설정합니다.
setkeyringtries *retry_number*
retry_number 값은 1~5의 정수가 될 수 있습니다.
- 단계 35 (선택 사항) 인증서 해지 목록 확인을 활성화하거나 비활성화합니다.
setrevoke-policy { *relaxed* | *strict* }
- 단계 36 연결을 활성화합니다.
setadmin-stateenable
- 단계 37 모든 연결을 다시 로드합니다.
reload-conns
- 단계 38 (선택 사항) IPsec에 기존의 트러스트 포인트 이름을 추가합니다.
createauthority *trustpoint_name*
- 단계 39 IKE와 SA 연결 간에 일치하는 암호화 키 보안 강도가 적용되도록 구성합니다.
setsa-strength-enforcement *yes_or_no*

트러스트 포인트에 대한 정적 CRL 구성

해지된 인증은 CRL(인증 해지 목록)에 보관됩니다. 클라이언트 애플리케이션은 CRL을 사용하여 서버의 인증을 확인합니다. 서버 애플리케이션은 CRL을 활용하여 더 이상 신뢰할 수 없는 클라이언트 애플리케이션의 액세스 요청을 수락 또는 거부합니다.

Firepower 4100/9300 새시를 구성하여 CRL(인증 해지 목록) 정보를 사용하여 피어 인증서를 검증할 수 있습니다. 이 옵션은 시스템에서 공통 기준 인증 컴플라이언스를 달성하기 위해 제공된 숫자 중 하나입니다. 자세한 내용은 [보안 인증 컴플라이언스, 49 페이지](#)를 참조하십시오.

CRL 정보를 사용하여 피어 인증서를 검증하려면 다음 단계를 수행합니다.

절차

- 단계 1 FXOS CLI에서 보안 모드를 시작합니다.
scopesecurity
- 단계 2 트러스트 포인트 모드를 시작합니다.
scopetrustpoint *trustname*
- 단계 3 취소 모드를 시작합니다.
scoperevoke
- 단계 4 CRL 파일을 다운로드합니다.
importcrl *protocol://user_id@CA_or_CRL_issuer_IP/tmp/DoDCA1CRL1.crl*
- 단계 5 (선택 사항) CRL 정보 가져오기 프로세스의 상태를 표시합니다.
showimport-taskdetail

단계 6 인증서 해지 방법을 CRL 전용으로 설정합니다.
`setcertrevokemethod{crl}`

인증서 해지 목록 확인 정보

CRL(인증서 해지 목록) 확인 모드를 IPSec, HTTPS 및 보안 LDAP 연결에서 Strict(엄격) 또는 Relaxed(완화) 중 하나로 구성할 수 있습니다.

동적(비정적) CRL 정보는 X.509 인증서의 CDP 정보에서 수집되며 동적 CRL 정보를 나타냅니다. 정적 CRL 정보는 시스템 관리를 통해 수동으로 다운로드되며 FXOS 시스템의 로컬 CRL 정보를 나타냅니다. 동적 CRL 정보는 인증서 체인에서 현재 처리 중인 인증서에 대해서만 처리됩니다. 정적 CRL은 전체 피어 인증서 체인에 적용됩니다.

보안 IPSec, LDAP 및 HTTPS 연결에 대한 인증서 해지 확인을 활성화 또는 비활성화하기 위한 단계에 대해서는 [IPSec 보안 채널 구성, 52 페이지](#), [LDAP 제공자 생성, 110 페이지](#) 및 [HTTPS 구성, 105 페이지](#)의 내용을 참조하십시오.



참고

- 인증서 해지 확인 모드를 Strict(엄격)로 설정한 경우, 피어 인증서 체인이 레벨 1 이상인 경우에만 정적 CRL을 적용할 수 있습니다. 피어 인증서 체인이 루트 CA 인증서만 포함하고 피어 인증서가 루트 CA에 의해 서명된 경우를 예로 들 수 있습니다.
- IPSec에 대해 정적 CRL을 구성할 때 가져온 CRL 파일에 인증 키 식별자(authkey) 필드가 있어야 합니다. 그렇지 않으면 IPSec에서 해당 파일을 유효하지 않은 것으로 간주합니다.
- 정적 CRL은 동일한 발급자의 동적 CRL보다 우선적으로 적용됩니다. 피어 인증서를 검증할 때 동일한 발급자의 유효한(확인된) 정적 CRL이 있는 경우, 피어 인증서의 CDP는 무시됩니다.

다음 표에는 인증서 해지 목록 확인 설정 및 인증서 검증에 따른 연결 결과가 나와 있습니다.

표 1: 로컬 정적 CRL 없이 Strict(엄격)로 설정된 인증서 해지 확인 모드

로컬 정적 CRL 없음	LDAP 연결	IPSec 연결	클라이언트 인증서 인증
피어 인증서 체인 확인	전체 인증서 체인 필요	전체 인증서 체인 필요	전체 인증서 체인 필요
피어 인증서 체인에서 CDP 확인	전체 인증서 체인 필요	전체 인증서 체인 필요	전체 인증서 체인 필요
피어 인증서 체인의 루트 CA 인증서에 대한 CDP 확인	예	해당 없음	예

로컬 정적 CRL 없음	LDAP 연결	IPSec 연결	클라이언트 인증서 인증
피어 인증서 체인의 모든 인증서 검증 장애	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 모든 인증서가 취소됨	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 하나의 CDP가 누락됨	Syslog 메시지와 함께 연결 실패	피어 인증서: syslog 메시지와 함께 연결 실패 중간 CA: 연결 실패	Syslog 메시지와 함께 연결 실패
유효한 서명이 있는 피어 인증서 체인에서 하나의 CDP CRL이 비어 있음	연결 성공	연결 성공	Syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 모든 CDP를 다운로드할 수 없음	Syslog 메시지와 함께 연결 실패	피어 인증서: syslog 메시지와 함께 연결 실패 중간 CA: 연결 실패	Syslog 메시지와 함께 연결 실패
인증서에 CDP가 있지만 CDP 서버가 다운됨	Syslog 메시지와 함께 연결 실패	피어 인증서: syslog 메시지와 함께 연결 실패 중간 CA: 연결 실패	Syslog 메시지와 함께 연결 실패
인증서에 CDP가 있고 서버가 작동 중이며 CRL이 CDP에 있지만 CRL에 유효하지 않은 서명이 있음	Syslog 메시지와 함께 연결 실패	피어 인증서: syslog 메시지와 함께 연결 실패 중간 CA: 연결 실패	Syslog 메시지와 함께 연결 실패

표 2: 로컬 정적 CRL이 있으며 Strict(엄격)로 설정된 인증서 해지 확인 모드

로컬 정적 CRL 있음	LDAP 연결	IPSec 연결
피어 인증서 체인 확인	전체 인증서 체인 필요	전체 인증서 체인 필요
피어 인증서 체인에서 CDP 확인	전체 인증서 체인 필요	전체 인증서 체인 필요
피어 인증서 체인의 루트 CA 인증서에 대한 CDP 확인	예	해당 없음
피어 인증서 체인의 모든 인증서 검증 장애	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패

로컬 정적 CRL 있음	LDAP 연결	IPSec 연결
피어 인증서 체인에서 모든 인증서가 취소됨	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 하나의 CDP가 누락됨(인증서 체인 레벨이 1임)	연결 성공	연결 성공
피어 인증서 체인에서 하나의 CDP CRL이 비어 있음(인증서 체인 레벨이 1임)	연결 성공	연결 성공
피어 인증서 체인에서 모든 CDP를 다운로드할 수 없음(인증서 체인 레벨이 1임)	연결 성공	연결 성공
인증서에 CDP가 있지만 CDP 서버가 다운됨(인증서 체인 레벨이 1임)	연결 성공	연결 성공
인증서에 CDP가 있고 서버가 작동 중이며 CRL이 CDP에 있지만 CRL에 유효하지 않은 서명이 있음(인증서 체인 레벨이 1임)	연결 성공	연결 성공
피어 인증서 체인 레벨이 1보다 높음	Syslog 메시지와 함께 연결 실패	CDP와 결합된 경우 연결 성공 CDP가 없는 경우 syslog 메시지와 함께 연결 실패

표 3: 로컬 정적 CRL 없이 Relaxed(완화)로 설정된 인증서 해지 확인 모드

로컬 정적 CRL 없음	LDAP 연결	IPSec 연결	클라이언트 인증서 인증
피어 인증서 체인 확인	전체 인증서 체인	전체 인증서 체인	전체 인증서 체인
피어 인증서 체인에서 CDP 확인	전체 인증서 체인	전체 인증서 체인	전체 인증서 체인
피어 인증서 체인의 루트 CA 인증서에 대한 CDP 확인	예	해당 없음	예
피어 인증서 체인의 모든 인증서 검증 장애	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패

로컬 정적 CRL 없음	LDAP 연결	IPSec 연결	클라이언트 인증서 인증
피어 인증서 체인에서 모든 인증서가 취소됨	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 하나의 CDP가 누락됨	연결 성공	연결 성공	Syslog 메시지와 함께 연결 실패
유효한 서명이 있는 피어 인증서 체인에서 하나의 CDP CRL이 비어 있음	연결 성공	연결 성공	연결 성공
피어 인증서 체인에서 모든 CDP를 다운로드할 수 없음	연결 성공	연결 성공	연결 성공
인증서에 CDP가 있지만 CDP 서버가 다운됨	연결 성공	연결 성공	연결 성공
인증서에 CDP가 있고 서버가 작동 중이며 CRL이 CDP에 있지만 CRL에 유효하지 않은 서명이 있음	연결 성공	연결 성공	연결 성공

표 4: 로컬 정적 CRL이 있으며 Relaxed(완화)로 설정된 인증서 해지 확인 모드

로컬 정적 CRL 있음	LDAP 연결	IPSec 연결
피어 인증서 체인 확인	전체 인증서 체인	전체 인증서 체인
피어 인증서 체인에서 CDP 확인	전체 인증서 체인	전체 인증서 체인
피어 인증서 체인의 루트 CA 인증서에 대한 CDP 확인	예	해당 없음
피어 인증서 체인의 모든 인증서 검증 장애	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패
피어 인증서 체인에서 모든 인증서가 취소됨	Syslog 메시지와 함께 연결 실패	Syslog 메시지와 함께 연결 실패

로컬 정적 CRL 있음	LDAP 연결	IPSec 연결
피어 인증서 체인에서 하나의 CDP가 누락됨(인증서 체인 레벨이 1임)	연결 성공	연결 성공
피어 인증서 체인에서 하나의 CDP CRL이 비어 있음(인증서 체인 레벨이 1임)	연결 성공	연결 성공
피어 인증서 체인에서 모든 CDP를 다운로드할 수 없음(인증서 체인 레벨이 1임)	연결 성공	연결 성공
인증서에 CDP가 있지만 CDP 서버가 다운됨(인증서 체인 레벨이 1임)	연결 성공	연결 성공
인증서에 CDP가 있고 서버가 작동 중이며 CRL이 CDP에 있지만 CRL에 유효하지 않은 서명이 있음(인증서 체인 레벨이 1임)	연결 성공	연결 성공
피어 인증서 체인 레벨이 1보다 높음	Syslog 메시지와 함께 연결 실패	CDP와 결합된 경우 연결 성공 CDP가 없는 경우 syslog 메시지와 함께 연결 실패

CRL의 정기적인 다운로드 구성

시스템에서 CRL을 정기적으로 다운로드하도록 구성하여 인증서 검증에 새 CRL이 1~24시간마다 사용되도록 할 수 있습니다.

이 기능과 함께 다음 프로토콜 및 인터페이스를 사용할 수 있습니다.

- FTP
- SCP
- SFTP
- TFTP
- USB

**참고**

- SCEP 및 OCSP는 지원되지 않습니다.
- 정기적인 다운로드는 CRL당 하나만 구성할 수 있습니다.
- 트러스트 포인트당 하나의 CRL이 지원됩니다.

**참고**

기간은 1시간 간격으로만 구성할 수 있습니다.

정기적인 CRL 다운로드를 구성하려면 다음 단계를 수행합니다.

시작하기 전에

CRL 정보를 사용하여 피어 인증서를 검증하려면 Firepower 4100/9300 채시를 이미 구성했는지 확인합니다. 자세한 내용은 [트러스트 포인트에 대한 정적 CRL 구성, 57 페이지](#)를 참조하십시오.

절차

단계 1 FXOS CLI에서 보안 모드를 시작합니다.

scopesecurity

단계 2 트러스트 포인트 모드를 시작합니다.

scopetrustpoint

단계 3 취소 모드를 시작합니다.

scoperevoke

단계 4 취소 컨피그레이션을 편집합니다.

shconfig

단계 5 기본 컨피그레이션을 설정합니다.

예제:

```
set certrevokemethod crl
set crl-poll-filename rootCA.crl
set crl-poll-path /users/myname
set crl-poll-period 1
set crl-poll-port 0
set crl-poll-protocol scp
! set crl-poll-pwd
set crl-poll-server 182.23.33.113
set crl-poll-user myname
```

단계 6 컨피그레이션 파일을 종료합니다.

exit

단계 7 (선택 사항) 새 CRL을 다운로드하여 새 컨피그레이션을 테스트합니다.

예제:

```
Firepower-chassis /security/trustpoint/ revoke # sh import-task
```

Import task:

File Name	Protocol	Server	Port	Userid	State
rootCA.crl	Scp	182.23.33.113	0	myname	Downloading

NTP 서버 인증 활성화

Firepower 4100/9300 새시에서 NTP 서버 인증을 활성화하려면 다음 단계를 수행합니다.



참고

- NTP 인증 기능은 활성화하는 경우, 구성된 모든 서버에 전역적으로 적용됩니다.
- NTP 서버 인증에는 SHA1만 지원됩니다.
- 서버 인증을 위해서는 키 ID와 키 값이 필요합니다. 키 ID는 메시지 다이제스트를 컴퓨팅할 때 어떤 키 값을 사용할지 클라이언트와 서버에 알리는 데 사용됩니다. 키 값은 ntp-keygen을 사용하여 파생된 고정 값입니다.

절차

- 단계 1 ntp 4.2.8p8을 다운로드합니다.
- 단계 2 ntpd openssl이 활성화되어 있는 NTP 서버를 설치합니다.
- 단계 3 NTP 키 ID와 키 값을 생성합니다.
ntp-keygen-M
생성된 키를 사용하여 다음 단계를 수행합니다.
- 단계 4 Firepower 4100/9300 새시에 관리 사용자로 로그인합니다.
- 단계 5 **Platform Settings**를 선택하여 Platform Settings(플랫폼 설정) 창을 엽니다.
- 단계 6 Set Time Source(시간 소스 설정) 영역에서 **Use NTP server** 라디오 버튼을 클릭합니다.
- 단계 7 생성된 SHA1 문자열 및 키가 있는 NTP 서버를 추가합니다.
- 단계 8 **Save(저장)**를 클릭하여 NTP 서버 컨피그레이션을 저장합니다.
- 단계 9 **Enable ntp-authentication** 확인란을 선택합니다.
- 단계 10 **Save(저장)**를 클릭합니다.

LDAP 키 링 인증서 설정

Firepower 4100/9300 새시에서 TLS 연결을 지원하도록 보안 LDAP 클라이언트 키 링 인증서를 구성할 수 있습니다. 이 옵션은 시스템에서 공통 기준 인증 컴플라이언스를 달성하기 위해 제공된 숫자 중 하나입니다. 자세한 내용은 [보안 인증 컴플라이언스, 49 페이지](#)를 참조하십시오.



참고 공통 기준 모드가 활성화된 경우, SSL을 활성화해야 하며 서버 DNS 정보를 사용하여 키 링 인증서를 생성해야 합니다.

SSL이 LDAP 서버 항목에 대해 활성화된 경우, 연결을 구성할 때 키 링 정보가 참조 및 확인됩니다.

LDAP 서버 정보는 보안 LDAP 연결(SSL이 활성화된 상태)에 대한 CC 모드에서 DNS 정보여야 합니다.

보안 LDAP 클라이언트 키 링 인증서를 구성하려면 다음 단계를 수행합니다.

절차

단계 1 FXOS CLI에서 보안 모드를 시작합니다.

scopesecurity

단계 2 LDAP 모드를 시작합니다.

scopeldap

단계 3 LDAP 서버 모드를 시작합니다.

enterserver {server_ip|server_dns}

단계 4 LDAP 키 링을 설정합니다.

setkeyring keyring_name

단계 5 컨피그레이션을 커밋합니다.

commit-buffer

IP 액세스 목록 구성

기본적으로 Firepower 4100/9300 새시는 로컬 웹 서버에 대한 모든 액세스를 거부합니다. 각 IP 블록의 허용된 서비스 목록을 사용하여 IP 액세스 목록을 구성해야 합니다.

IP 액세스 목록은 다음 프로토콜을 지원합니다.

- HTTPS
- SNMP

• SSH

IP 주소(v4 또는 v6)의 각 블록의 경우, 각 서비스에 대해 최대 25개의 서로 다른 서브넷을 구성할 수 있습니다. 서브넷과 접두사가 모두 0인 경우 서비스에 무제한으로 액세스할 수 있습니다.

절차

-
- 단계 1 Firepower 4100/9300 새시에 관리 사용자로 로그인합니다.
- 단계 2 **Platform Settings**를 선택하여 Platform Settings(플랫폼 설정) 페이지를 엽니다.
- 단계 3 **Access List**를 선택하여 Access List(액세스 목록) 영역을 엽니다.
- 단계 4 이 영역에서 IP 액세스 목록에 나열된 IPv4 및 IPv6 주소를 확인, 추가, 삭제할 수 있습니다. IPv4 블록을 추가하려면 유효한 IPv4 IP 주소 및 접두사 [0~32] 길이를 입력하고 프로토콜을 선택해야 합니다.
- IPv6 블록을 추가하려면 유효한 IPv6 IP 주소 및 접두사 [0~128] 길이를 입력하고 프로토콜을 선택해야 합니다.
-

클라이언트 인증서 인증 활성화

LDAP와 함께 클라이언트 인증서를 사용하도록 시스템을 활성화하여 HTTPS 액세스에 대해 사용자를 인증할 수 있습니다. Firepower 4100/9300 새시에서 기본 인증 컨피그레이션은 크리덴셜 기반입니다.



참고

인증서 인증이 활성화된 경우, 이 인증은 HTTPS에 대해 허용되는 유일한 인증 형식입니다. 인증서 해지 확인은 클라이언트 인증서 인증 기능의 FXOS 2.1.1 릴리스에 지원되지 않습니다.

이 기능을 사용하려면 클라이언트 인증서는 다음 요건을 충족해야 합니다.

- 사용자 이름이 X509 특성 주체 대체 이름 - 이메일에 포함되어야 합니다.
- 클라이언트 인증서에 해당 인증서를 수퍼바이저의 트러스트 포인트로 가져온 루트 CA의 서명이 있어야 합니다.

절차

-
- 단계 1 FXOS CLI에서 서비스 모드를 시작합니다.
- ```
scopesystem
scopesecurity
```
- 단계 2 (선택 사항) HTTPS 인증의 옵션을 확인합니다.

### **sethttpsauth-type**

#### **예제:**

```
Firepower-chassis /system/services # set https auth-type
cert-auth Client certificate based authentication
cred-auth Credential based authentication
```

단계 3 HTTPS 인증을 클라이언트 기반으로 설정합니다.

#### **sethttpsauth-typecert-auth**

단계 4 컨피그레이션을 커밋합니다.

#### **commit-buffer**

---





## 시스템 관리

- Firepower Chassis Manager 세션 종료를 야기하는 시스템 변경 사항, 69페이지
- 관리 IP 주소 변경, 70페이지
- 애플리케이션 관리 IP 변경, 71페이지
- Firepower 4100/9300 새시 이름 변경, 74페이지
- 사전 로그인 배너, 75페이지
- Firepower 4100/9300 새시 재부팅, 77페이지
- Firepower 4100/9300 새시 전원 끄기, 78페이지
- 신뢰할 수 있는 ID 인증서 설치, 78페이지

## Firepower Chassis Manager 세션 종료를 야기하는 시스템 변경 사항

다음 시스템 변경 사항으로 인해 사용자가 Firepower Chassis Manager에서 자동으로 로그아웃될 수 있습니다.

- 시스템 시간을 10분 이상 수정하는 경우
- Firepower Chassis Manager 또는 FXOS CLI를 사용하여 시스템이 재부팅되거나 종료되는 경우
- Firepower 4100/9300 새시에서 FXOS 버전을 업그레이드하는 경우
- FIPS 또는 공통 기준 모드를 활성화 또는 비활성화하는 경우

**참고**

위와 같은 변경 사항이 적용된 경우 외에 활동 없이 일정 시간이 경과하는 경우, 사용자는 시스템에서 자동으로 로그아웃됩니다. 기본적으로 10분 동안 사용하지 않을 경우 시스템에서 로그아웃됩니다. 이 시간 제한 설정을 구성하려면 [세션 시간 제한 구성, 33 페이지](#)의 내용을 참조하십시오. 또한, 세션이 활성화된 경우에도 특정 기간 이후에 시스템에서 사용자가 로그아웃되는 시간 제한 절대값 설정을 구성할 수 있습니다. 이 시간 제한 절대값 설정을 구성하려면 [세션 시간 제한 절대값 구성, 34 페이지](#)의 내용을 참조하십시오.

## 관리 IP 주소 변경

### 시작하기 전에

Firepower 4100/9300 새시의 관리 IP 주소를 FXOS CLI에서 변경할 수 있습니다.

**참고**

관리 IP 주소를 변경한 후, 새 주소를 사용하여 Firepower Chassis Manager 또는 FXOS CLI에 대한 모든 연결을 다시 설정해야 합니다.

### 절차

단계 1 FXOS CLI에 연결합니다([FXOS CLI 액세스, 9 페이지](#) 참조).

단계 2 다음과 같이 IPv4 관리 IP 주소를 구성합니다.

- a) Fabric-interconnect a에 대한 범위를 설정합니다.  
Firepower-chassis# **scopefabric-interconnecta**
- b) 다음 명령을 입력하여 현재 관리 IP 주소를 확인합니다.  
Firepower-chassis /fabric-interconnect # **show**
- c) 다음 명령을 입력하여 새로운 관리 IP 주소 및 게이트웨이를 구성합니다.  
Firepower-chassis /fabric-interconnect # **setout-of-band staticip ip\_address netmask network\_mask gw gateway\_ip\_address**
- d) 시스템 컨피그레이션에 트랜잭션을 커밋합니다.  
Firepower-chassis /fabric-interconnect\* # **commit-buffer**

단계 3 다음과 같이 IPv6 관리 IP 주소를 구성합니다.

- a) Fabric-interconnect a에 대한 범위를 설정합니다.  
Firepower-chassis# **scopefabric-interconnecta**
- b) 관리 IPv6 컨피그레이션의 범위를 설정합니다.  
Firepower-chassis /fabric-interconnect # **scopeipv6-config**
- c) 다음 명령을 입력하여 현재 관리 IPv6 주소를 확인합니다.  
Firepower-chassis /fabric-interconnect/ipv6-config # **show ipv6-if**



- d) 다음 명령을 입력하여 새로운 관리 IP 주소 및 게이트웨이를 구성합니다.  

```
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band static ipv6 ipv6_address ipv6-prefix prefix_length ipv6-gw gateway_address
```
- e) 시스템 컨피그레이션에 트랜잭션을 커밋합니다.  

```
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
```

다음 예에서는 IPv4 관리 인터페이스 및 게이트웨이를 구성합니다.

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # show

Fabric Interconnect:
 ID OOB IP Addr OOB Gateway OOB Netmask OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability

 A 192.0.2.112 192.0.2.1 255.255.255.0 :: ::
 64 Operable
Firepower-chassis /fabric-interconnect # set out-of-band static ip 192.0.2.111 netmask 255.255.255.0 gw 192.0.2.1
Warning: When committed, this change may disconnect the current CLI session
Firepower-chassis /fabric-interconnect* #commit-buffer
Firepower-chassis /fabric-interconnect #
```

다음 예에서는 IPv6 관리 인터페이스 및 게이트웨이를 구성합니다.

```
Firepower-chassis# scope fabric-interconnect a
Firepower-chassis /fabric-interconnect # scope ipv6-config
Firepower-chassis /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
 IPv6 Address Prefix IPv6 Gateway

 2001::8998 64 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001::8999 ipv6-prefix 64 ipv6-gw 2001::1
Firepower-chassis /fabric-interconnect/ipv6-config* # commit-buffer
Firepower-chassis /fabric-interconnect/ipv6-config #
```

## 애플리케이션 관리 IP 변경

FXOS CLI의 Firepower 4100/9300 새시에 연결되어 있는 애플리케이션에서 관리 IP 주소를 변경할 수 있습니다. 이렇게 하려면 먼저 FXOS 플랫폼 레벨에서 IP 정보를 변경한 다음 애플리케이션 레벨에서 IP 정보를 변경해야 합니다.



**참고**

Firepower Chassis Manager를 사용하여 이러한 변경을 수행하려고 시도하면 서비스가 중단될 수 있습니다. 서비스 중단 가능성을 없애려면 FXOS CLI를 사용하여 이러한 변경을 수행해야 합니다.

## 절차

단계 1 FXOS CLI에 연결합니다. (FXOS CLI 액세스, 9 페이지를 참조하십시오.)

단계 2 논리적 디바이스로 범위를 한정합니다.

**scopessa**

**scopelogical-device** *logical\_device\_name*

단계 3 관리 부트스트랩으로 범위를 한정하고 새로운 관리 부트스트랩 파라미터를 구성합니다. 구축 간에는 차이점이 있습니다.

ASA 논리적 디바이스의 독립형 컨피그레이션의 경우:

a) 논리적 디바이스 관리 부트스트랩을 입력합니다.

**scopemgmt-bootstrap** *ASA*

b) 슬롯의 IP 모드를 시작합니다.

**scope ipv4\_or\_6 slot\_number default**

c) (IPv4만 해당) 새 IP 주소를 설정합니다.

**setip ipv4\_addressmask network\_mask**

d) (IPv6만 해당) 새 IP 주소를 설정합니다.

**setip ipv6\_addressprefix-length prefix\_length\_number**

e) 게이트웨이 주소를 설정합니다.

**setgateway gateway\_ip\_address**

f) 컨피그레이션을 커밋합니다.

**commit-buffer**

ASA 논리적 디바이스의 클러스터형 컨피그레이션의 경우:

a) 클러스터 관리 부트스트랩을 입력합니다.

**scopeclass-cluster-bootstrap** *ASA*

b) (IPv4만 해당) 새 가상 IP를 설정합니다.

**setvirtualipv4 ip\_addressmask network\_mask**

c) (IPv6만 해당) 새 가상 IP를 설정합니다.

**setvirtualipv6 ipv6\_addressprefix-length prefix\_length\_number**

d) 새 IP 풀을 설정합니다.

**setippool start\_ip end\_ip**

e) 게이트웨이 주소를 설정합니다.

**setgateway gateway\_ip\_address**

f) 컨피그레이션을 커밋합니다.

**commit-buffer**

Firepower Threat Defense의 독립형 및 클러스터형 컨피그레이션의 경우:

a) 논리적 디바이스 관리 부트스트랩을 입력합니다.

**scopemgmt-bootstrap** *ftd*

b) 슬롯의 IP 모드를 시작합니다.

**scope** *ipv4\_or\_6 slot\_number firepower*

- c) (IPv4만 해당) 새 IP 주소를 설정합니다.  
**setip** *ipv4\_addressmask network\_mask*
- d) (IPv6만 해당) 새 IP 주소를 설정합니다.  
**setip** *ipv6\_addressprefix-length prefix\_length\_number*
- e) 게이트웨이 주소를 설정합니다.  
**setgateway** *gateway\_ip\_address*
- f) 컨피그레이션을 커밋합니다.  
**commit-buffer**

**참고** 클러스터형 컨피그레이션의 경우, Firepower 4100/9300 새시에 연결된 각 애플리케이션의 새 IP 주소를 설정해야 합니다. 새시 간 클러스터 또는 HA 컨피그레이션을 보유한 경우, 두 새시 모두에서 각 애플리케이션에 대해 이 단계를 반복해야 합니다.

**단계 4** 각 애플리케이션에 대한 관리 부트스트랩 정보를 지웁니다.

- a) ssa 모드로 범위를 한정합니다.  
**scopessa**
- b) 슬롯으로 범위를 한정합니다.  
**scopeslot** *slot\_number*
- c) 애플리케이션 인스턴스로 범위를 한정합니다.  
**scopeapp-instance** *asa\_or\_fid*
- d) 관리 부트스트랩 정보를 지웁니다.  
**clearmgmt-bootstrap**
- e) 컨피그레이션을 커밋합니다.  
**commit-buffer**

**단계 5** 애플리케이션을 비활성화합니다.

**disable**

**commit-buffer**

**참고** 클러스터형 컨피그레이션의 경우, Firepower 4100/9300 새시에 연결된 각 애플리케이션의 관리 부트스트랩 정보를 지우고 비활성화해야 합니다. 새시 간 클러스터 또는 HA 컨피그레이션을 보유한 경우, 두 새시 모두에서 각 애플리케이션에 대해 이 단계를 반복해야 합니다.

**단계 6** 애플리케이션이 오프라인 상태인 경우 슬롯이 다시 온라인 상태가 되면 애플리케이션을 다시 활성화합니다.

- a) 다시 ssa 모드로 범위를 한정합니다.  
**scopessa**
- b) 슬롯으로 범위를 한정합니다.  
**scopeslot** *slot\_number*
- c) 애플리케이션 인스턴스로 범위를 한정합니다.  
**scopeapp-instance** *asa\_or\_fid*
- d) 애플리케이션을 활성화합니다.  
**enable**

e) 컨피그레이션을 커밋합니다.

**commit-buffer**

**참고** 클러스터형 컨피그레이션의 경우, Firepower 4100/9300 새시에 연결된 각 애플리케이션을 다시 활성화하려면 이 단계를 반복해야 합니다. 새시 간 클러스터 또는 HA 컨피그레이션을 보유한 경우, 두 새시 모두에서 각 애플리케이션에 대해 이 단계를 반복해야 합니다.

## Firepower 4100/9300 새시 이름 변경

시작하기 전에

Firepower 4100/9300 새시에 사용되는 이름을 FXOS CLI에서 변경할 수 있습니다.

절차

**단계 1** FXOS CLI에 연결합니다(FXOS CLI 액세스, 9 페이지 참조).

**단계 2** 시스템 모드를 시작합니다.

```
Firepower-chassis-A# scopesystem
```

**단계 3** 현재 이름을 확인합니다.

```
Firepower-chassis-A /system # show
```

**단계 4** 새 이름을 구성합니다.

```
Firepower-chassis-A /system # setname device_name
```

**단계 5** 시스템 컨피그레이션에 트랜잭션을 커밋합니다.

```
Firepower-chassis-A /fabric-interconnect* # commit-buffer
```

다음 예에서는 디바이스 이름을 변경합니다.

```
Firepower-chassis-A# scope system
Firepower-chassis-A /system # set name New-name
Warning: System name modification changes FC zone name and redeploys them non-disruptively
Firepower-chassis-A /system* # commit-buffer
Firepower-chassis-A /system # show

Systems:
 Name Mode System IP Address System IPv6 Address

 New-name Stand Alone 192.168.100.10 ::
New-name-A /system #
```

## 사전 로그인 배너

사전 로그인 배너를 사용하면 사용자가 Firepower Chassis Manager에 로그인할 때 배너 텍스트가 표시되며, 사용자는 사용자 이름 및 비밀번호를 묻는 프롬프트가 표시되기 전에 메시지 화면에서 **OK**(확인)를 클릭해야 합니다. 사전 로그인 배너가 구성되어 있지 않은 경우에는 바로 사용자 이름 및 비밀번호 프롬프트가 표시됩니다.

구성되어 있는 경우에는 사용자가 FXOS CLI에 로그인하면 비밀번호를 묻는 프롬프트가 표시되기 전에 배너 텍스트가 표시됩니다.

## 사전 로그인 배너 생성

### 절차

- 
- 단계 1** FXOS CLI에 연결합니다([FXOS CLI 액세스, 9 페이지](#) 참조).
- 단계 2** 보안 모드를 시작합니다.  
Firepower-chassis# **scopesecurity**
- 단계 3** 배너 보안 모드를 시작합니다.  
Firepower-chassis /security # **scopebanner**
- 단계 4** 다음 명령을 입력하여 사전 로그인 배너를 생성합니다.  
Firepower-chassis /security/banner # **create pre-login-banner**
- 단계 5** 사용자가 Firepower Chassis Manager 또는 FXOS CLI에 로그인하기 전에 FXOS가 사용자에게 표시해야 할 메시지를 지정합니다.  
Firepower-chassis /security/banner/pre-login-banner\* # **set message**  
사전 로그인 배너 메시지 텍스트를 입력할 대화 상자를 실행합니다.
- 단계 6** 프롬프트에서 사전 로그인 배너 메시지를 입력합니다. 이 필드에 임의의 표준 ASCII 문자를 입력할 수 있습니다. 각 라인에 최대 192자를 포함할 수 있는 여러 라인의 텍스트를 입력할 수 있습니다. 각 라인 사이에서 **Enter** 키를 누릅니다.  
입력한 후 라인에서 ENDOFBUF를 입력하고 완료하려면 **Enter** 키를 누릅니다.  
설정 메시지 대화 상자를 취소하려면 **Ctrl+C**를 누릅니다.
- 단계 7** 시스템 컨피그레이션에 트랜잭션을 커밋합니다.  
Firepower-chassis /security/banner/pre-login-banner\* # **commit-buffer**
- 

다음 예에서는 사전 로그인 배너를 생성합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # create pre-login-banner
Firepower-chassis /security/banner/pre-login-banner* # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
```

```
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

## 사전 로그인 배너 수정

### 절차

- 
- 단계 1 FXOS CLI에 연결합니다(FXOS CLI 액세스, 9 페이지 참조).
- 단계 2 보안 모드를 시작합니다.  
Firepower-chassis# **scopesecurity**
- 단계 3 배너 보안 모드를 시작합니다.  
Firepower-chassis /security # **scopebanner**
- 단계 4 pre-login-banner 배너 보안 모드를 시작합니다.  
Firepower-chassis /security/banner # **scope pre-login-banner**
- 단계 5 사용자가 Firepower Chassis Manager 또는 FXOS CLI에 로그인하기 전에 FXOS가 사용자에게 표시해야 할 메시지를 지정합니다.  
Firepower-chassis /security/banner/pre-login-banner # **set message**  
사전 로그인 배너 메시지 텍스트를 입력할 대화 상자를 실행합니다.
- 단계 6 프롬프트에서 사전 로그인 배너 메시지를 입력합니다. 이 필드에 임의의 표준 ASCII 문자를 입력할 수 있습니다. 각 라인에 최대 192자를 포함할 수 있는 여러 라인의 텍스트를 입력할 수 있습니다. 각 라인 사이에서 **Enter** 키를 누릅니다.  
입력한 후 라인에서 ENDOFBUF를 입력하고 완료하려면 **Enter** 키를 누릅니다.  
설정 메시지 대화 상자를 취소하려면 Ctrl+C를 누릅니다.
- 단계 7 시스템 컨피그레이션에 트랜잭션을 커밋합니다.  
Firepower-chassis /security/banner/pre-login-banner\* # **commit-buffer**
- 

다음 예에서는 사전 로그인 배너를 수정합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # scope pre-login-banner
Firepower-chassis /security/banner/pre-login-banner # set message
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Enter prelogin banner:
>Welcome to the Firepower Security Appliance
>**Unauthorized use is prohibited**
>ENDOFBUF
Firepower-chassis /security/banner/pre-login-banner* # commit-buffer
Firepower-chassis /security/banner/pre-login-banner #
```

## 사전 로그인 배너 삭제

### 절차

단계 1 FXOS CLI에 연결합니다(FXOS CLI 액세스, 9 페이지 참조).

단계 2 보안 모드를 시작합니다.

```
Firepower-chassis# scopesecurity
```

단계 3 배너 보안 모드를 시작합니다.

```
Firepower-chassis /security # scopebanner
```

단계 4 시스템에서 사전 로그인 배너를 삭제합니다.

```
Firepower-chassis /security/banner # delete pre-login-banner
```

단계 5 시스템 컨피그레이션에 트랜잭션을 커밋합니다.

```
Firepower-chassis /security/banner* # commit-buffer
```

다음 예에서는 사전 로그인 배너를 삭제합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope banner
Firepower-chassis /security/banner # delete pre-login-banner
Firepower-chassis /security/banner* # commit-buffer
Firepower-chassis /security/banner #
```

## Firepower 4100/9300 새시 재부팅

### 절차

단계 1 Overview(개요)를 선택하여 Overview(개요) 페이지를 엽니다.

단계 2 Overview(개요) 페이지 오른쪽 상단에서 Chassis Uptime(새시 업타임) 옆에 있는 **Reboot(재부팅)**를 클릭합니다.

단계 3 **Yes(예)**를 클릭하여 Firepower 4100/9300 새시의 전원을 끌 것을 확인합니다.

시스템에 구성되어 있는 모든 논리적 디바이스를 정상적으로 종료한 다음 최종적으로 Firepower 4100/9300 새시의 전원을 끄고 재시작하기 전에 각 보안 모듈/엔진의 전원을 끕니다. 이 프로세스에는 약 15~20분이 소요됩니다.

## Firepower 4100/9300 새시 전원 끄기

### 절차

- 
- 단계 1 **Overview**(개요)를 선택하여 **Overview**(개요) 페이지를 엽니다.
  - 단계 2 **Overview**(개요) 페이지 오른쪽 상단에서 **Chassis Uptime**(새시 업타임) 옆에 있는 **Shutdown**(종료)을 클릭합니다.
  - 단계 3 **Yes**(예)를 클릭하여 Firepower 4100/9300 새시의 전원을 끌 것을 확인합니다.  
시스템에 구성되어 있는 모든 논리적 디바이스를 정상적으로 종료한 다음 최종적으로 Firepower 4100/9300 새시의 전원을 끄기 전에 각 보안 모듈/엔진의 전원을 끕니다.
- 

## 신뢰할 수 있는 ID 인증서 설치

초기 컨피그레이션 이후 Firepower 4100/9300 새시 웹 애플리케이션과 함께 사용하기 위해 자체 서명 SSL 인증서가 생성됩니다. 인증서가 자체 서명되므로 클라이언트 브라우저는 이 인증서를 자동으로 신뢰하지 않습니다. 새 클라이언트 브라우저가 처음으로 Firepower 4100/9300 새시 웹 인터페이스에 액세스할 때 브라우저는 SSL 경고를 발생시켜 사용자에게 Firepower 4100/9300 새시에 액세스하기 전에 인증서를 수락하도록 요청합니다. 다음 절차를 사용하면 FXOS CLI를 사용하여 CSR(인증서 서명 요청)을 생성하고 Firepower 4100/9300 새시와 함께 사용하기 위해 결과 ID 인증서를 설치할 수 있습니다. 이 ID 인증서를 사용하면 클라이언트 브라우저에서 연결을 신뢰할 수 있으며 경고 없이 웹 인터페이스를 불러올 수 있습니다.

### 절차

- 
- 단계 1 FXOS CLI에 연결합니다. (**FXOS CLI 액세스, 9 페이지**를 참조하십시오.)
  - 단계 2 보안 모듈을 입력합니다.  
**scopesecurity**
  - 단계 3 키 링을 생성합니다.  
**createkeyring keyring\_name**
  - 단계 4 개인 키에 대한 모듈러스 크기를 설정합니다.  
**setmodulus 크기**
  - 단계 5 컨피그레이션을 커밋합니다.  
**commit-buffer**
  - 단계 6 CSR 필드를 구성합니다. 인증서는 기본 옵션(예: 주제-이름)을 사용하여 생성할 수 있으며, 선택적으로 로컬 및 조직과 같은 정보가 인증서에 포함되도록 허용하는 고급 옵션을 사용할 수 있습니다. CSR 필드를 구성할 때 시스템에서 인증서 비밀번호를 묻습니다.  
**createcertreqcertreq subject\_name**



비밀번호  
**setcountry** 국가  
**setstate** 주/도  
**setlocality** 지역  
**setorg-name** *organization\_name*  
**setorg-unit-name** *organization\_unit\_name*  
**setsubject-name** *subject\_name*

단계 7 컨피그레이션을 커밋합니다.

**commit-buffer**

단계 8 인증 기관에 제공하기 위해 CSR을 내보냅니다.

a) 전체 CSR을 표시합니다.

**showcertreq**

b) \"-----BEGIN CERTIFICATE REQUEST-----\"로 시작되고 \"-----END CERTIFICATE REQUEST-----\"로 종료(및 포함)되는 출력을 복사합니다.

예제:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC6zCCAQMCAQAwdzELMAkGA1UEBhMCVVMxEzARBgNVBAGMCKNhbG1mb3JuaWEEx
ETAPBgNVBACMCFNhb3N1MRYwFAyDQVQKDA1DaXNjbyBTeXN0ZW1zMzQwCgYD
VQQLDANUQUxGjAYBgNVBAMMEWZwNDEyMC50ZXN0LmXvY2FsMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs0ON5gagkfZ2fi4JVEANG+7YGgcHbnUt7LpV
yMChnKOPJjBwkUMNQAlmQsRQDcbJ232/sK0fMSnyqOL8JzC7itxeVEZRyz7/ax7W
GNveg/XP+zd03nt4GXM63FsrPcPmA7EwgqDSL0ShtBEV10hhf4+Nw4pKCZ+eSSkS
JkTb1ZHakV9bttYg3kf/UEUUGk/EyrVq3B+u2DsooPVq76mTm8BwYMqHbJEv4Pmu
RjWE88yEvVwH7JTEij9OvxbatjDjVSJHZBURtCanvyBvGuLP/Q/Nmv3Lo3G9ITbL
L5gIYZVatTxp6HTUezH2MIiZ0avU6d1tB9rnyxgGth5dPV0dhQIDAQABO8wLQYJ
KoZIHvcNAQkOMSAwHjAcBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbdANBgkq
hkiG9w0BAQsFAAOCAQEAZUfCbwx9vt5aVdcL+tATu5xFE3LA310ck6Gj1Nv6W/6r
jBNLxusYi1rZZcW+CgnvNs4ArqYGyNVBySOavJO/VvQ1KfyxxJ10Ikyx3RzEjgK0
zzyoyrG+EZXC5ShiraS8HuWvE2wFM2wwWNtHWtvcQy55+/hDPD2Bv8pQOC2Zng3I
kLFG1dxWf1xAxLzf5J+AuIQ0CM5HzM9Zm8zREoWT+xHtLSqAqg/aCuomN9/vEwyU
OYfoJMvAqC6AZyUnMfUfCoyuLpLwgkxkx80gyaRdnea5RhiGjYQ21DXYDjEXp7rCx9
+6bvDl1n70JCegHdcWtP75SaNyaBEPk00365rTckbw==
-----END CERTIFICATE REQUEST-----
```

단계 9 certreq 모드를 종료합니다.

**exit**

단계 10 키 링 모드를 종료합니다.

**exit**

단계 11 **참고** 모든 인증서는 FXOS로 가져오기 위해 Base64 형식이어야 합니다. 인증 기관에서 받은 인증서 또는 체인이 다른 형식인 경우 먼저 OpenSSL과 같은 SSL 툴로 변환해야 합니다. 인증서 체인을 보관하기 위해 새 트러스트 포인트를 생성합니다.

**createtrustpoint** *trustpoint\_name*

단계 12 트러스트 포인트에서 생성된 CSR을 설정합니다.

**setcertchain**

- 단계 13 참고** 중간 인증서를 사용하는 인증 기관의 경우 루트 및 중간 인증서를 결합해야 합니다. 텍스트 파일의 맨 위에 루트 인증서를 붙여넣으면 모든 BEGIN CERTIFICATE 및 END CERTIFICATE 플래그를 포함하여 체인의 각 중간 인증서가 뒤따르게 됩니다. 해당하는 전체 텍스트 블록을 트러스트 포인트에 복사하여 붙여넣습니다. 화면의 지침에 따라 8단계에서 복사한 CSR 출력을 입력합니다.

**예제:**

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
>-----BEGIN CERTIFICATE-----
>MIICDCCAbOgAwIBAgIQYIutxPDPw6BOP3uKNgJHZDAKBggqhkjOPQQDAjBTMRUw
>EwYKcZImiZPyLQBGryFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>MB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTc1NjU2
>WhcNMjAwNzI4MTgwNjU2WjBTMRUwEwYKcZImiZPyLQBGryFbG9jYWwxGDAWBgoJ
>kiaJk/IsZAEZFghuYWF1c3RpbjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4t
>UEMtQ0EwWTATBgcqhkiOPOQIBBggqhkjOPQMBBwNCAASvEA27V1EnqlgMtLkvJ6rx
>GXRpXWIEyuiBM4eQRoqZKnkeJUkmlxmqlubaDHPJ5TMGfJQYszLBRJPq+mdrKcDl
>o2kwZzATBgrBgEEAYI3FAIEBh4EAEMAQTAOBgNVHQ8BAf8EBAMCAYYwDwYDVR0T
>AQH/BAUwAwEB/zAdBgNVHQ4EFgQUyInbDHPfFwEEBcbxGSgQW7pOVIkWEAYJKwYB
>BAGCxxUBBAMCAQAwCgYIKoZIzj0EAwIDSAARQIhAP++QJTUmniB/AxPDDN63Lqy
>18odMDoFTkG4p3Tb/2yMAiAtMYhlsvlGcxsQVow0xZVRugSdoOak6n7wCjTFX9jr
>RA==
>-----END CERTIFICATE-----
>ENDOFBUF
```

- 단계 14** 컨피그레이션을 커밋합니다.

**commit-buffer**

- 단계 15** 트러스트 포인트 모드를 종료합니다.

**exit**

- 단계 16** 키 링 모드를 시작합니다.

**scopekeyring keyring\_name**

- 단계 17** 13단계에서 생성한 트러스트 포인트와 CSR용으로 생성된 키 링을 연결합니다.

**settrustpoint trustpoint\_name**

- 단계 18** 서버용으로 서명된 ID 인증서를 가져옵니다.

**setcert**

- 단계 19** 인증 기관에서 제공하는 ID 인증서의 내용을 붙여넣습니다.

**예제:**

```
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
>-----BEGIN CERTIFICATE-----
>MIIE8DCCBjAgAwIBAgITRQAAAAreh1UWgiTzvgAAAAACjAKBggqhkjOPQQDAjBT
>MRUwEwYKcZImiZPyLQBGryFbG9jYWwxGDAWBgoJkiaJk/IsZAEZFghuYWF1c3RpbjEg
>bjEgMB4GA1UEAxMXbmFhdXN0aW4tTkFBVVNUSU4tUEMtQ0EwHhcNMTUwNzI4MTMw
>OTU0WhcNMTgwNDI4MTMwOTU0WjBTMRUwEwYKcZImiZPyLQBGryFbG9jYWwxGDAWBgoJ
>aWZvcn5pYTERMA8GA1UEBxMIU2FuIEpvc2UxXjAUBGNVBAoTDUNpc2NvIFN5c3Rl
>bXMxNDkKbG9uYVBA8GA1UEBxMIU2FuIEpvc2UxXjAUBGNVBAoTDUNpc2NvIFN5c3Rl
>MA0GCsGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCzQ43mBqCR9nZ+Lg1UQA0b7tga
>BwdudS3sulXIwKGo48mMHCRCQw1ADWZCxFANxsnbfb+wrR8xKfKo4vwnMLuK3F5U
>RlHLPv9rHtYY296D9c/7N3Tee3gZczrcWys9w+YDsTCCoNIuhKG0ERXXSGF/j43D
>ikoJn55JKRImRMHVkdopX1u21iDeR/9QRRSCT8TKtWrcH67Yoyig9WrvqZObwHBg
>yodsks/g+a5GNYTzzIS9XafsLMSKP06/Ftq2MONVIkdkFRG0Jqe/IG8a4s/9D82a
>/cujcb0hNssvmAhh1Vq1PGnodNR7MfYwgjM5q9Tp3W0H2ufLGAA2H109XR2FAGMB
>AAGjggJYMICVDACBgNVHREFTATghFmcDQxMjAudGVzdC5sb2NhbDAdBgNVHQ4E
>FgQU/1WpstieYExs8D1ZWcuHwZwPtU5QwHwYDVR0jBBgwFoAUyInbDHPfFwEEBcbx
```

```
>GSgQW7pOVIkwgdwGA1UdHwSB1DCB0TCBzqCBy6CByIaBxWxkYXA6Ly8vQ049bmFh
>dXN0aW4tTkFBVVNUSU4tUEMtQ0EsQ049bmFhdXN0aW4tcGMsQ049Q0RQLENOPVB1
>YmxpYyUyMEt1eSUyMFN1cnZpY2VzLENOFVN1cnZpY2VzLENOPUNvbmZpZ3VyYXRp
>b24sREM9bmFhdXN0aW4sREM9bG9jYWw/Y2VydG1maWNhdGVsZXZvY2F0aW9uTG1z
>dD9iYXN1P29iamVjdENsYXNzPWNSTERpc3RyaWJldGlvb1BvaW50IHMBggrBgEF
>BQcBAQSBvzCBvDCBuQYIKwYBBQUHMAKGgaxsZGFwOi8vL0NOPW5hYXVzdGluLU5B
>QVVTVE1OLVBDLUNBLENOPUFJQSxDTj1QdWJsaWMLMjBLZXk1MjBTZXJ2aWN1cyxD
>Tj1TZXJ2aWN1cyxDj1Db25maWd1cmF0aW9uLERDPW5hYXVzdGluLERDPWxvY2Fs
>P2NBQ2VydG1maWNhdGU/YmFzZT9vYmplY3RDbGFzcz1jZXJ0aWZpY2F0aW9uQXV0
>aG9yaXR5MCEGCSsGAQQBgjcUAQUHhIAVwBLAGIAUwBIAHIAHgBIAHIwDgYDVROp
>AQH/BAQDAgWgMBMGA1UdJQMMAAoGCCsGAQUFBwMBMAoGCCqGSM49BAMCA0GAMEUC
>IFew7NcJirEtFRvxyjkQ4/dVo2oI6CRB308WQbYHNUu/AiEA7UdObiSJBG/PBZjm
>sgoIK60akbjotOTvUdUd9b6K1Uw=
>-----END CERTIFICATE-----
>ENDOFBUF
```

단계 20 키 링 모드를 종료합니다.  
**exit**

단계 21 보안 모드를 종료합니다.  
**exit**

단계 22 시스템 모드를 시작합니다.  
**scopesystem**

단계 23 서비스 모드를 시작합니다.  
**scopeservices**

단계 24 새 인증서를 사용하도록 FXOS 웹 서비스를 구성합니다.  
**sethttpskeyring keyring\_name**

단계 25 컨피그레이션을 커밋합니다.  
**commit-buffer**

단계 26 HTTPS 서버와 연결된 키 링을 표시합니다. 여기에는 이 절차의 3단계에서 생성한 키 링 이름이 반영 되어야 합니다. 화면 출력에 기본 키 링 이름이 표시되는 경우, HTTPS 서버가 아직 새 인증서를 사용 하도록 업데이트되지 않은 것입니다.  
**showhttps**

**예제:**

```
fp4120 /system/services # show https
Name: https
 Admin State: Enabled
 Port: 443
 Operational port: 443
 Key Ring: firepower_cert
 Cipher suite mode: Medium Strength
 Cipher suite: ALL:!ADH:!EXPORT40:!EXPORT56:!LOW:!RC4:!MD5:!IDEA:+HIGH:+MEDIUM:+EXP:+eNULL
```

단계 27 가져온 인증서의 내용을 표시하고 해당 **Certificate Status**(인증서 상태) 값이 **Valid**(유효함)로 표시되 는지 확인합니다.  
**scopesecurity**

**showkeyring keyring\_namedetail**

## 예제:

```

fp4120 /security # scope security
fp4120 /security # show keyring firepower_cert detail
Keyring firepower_cert:
 RSA key modulus: Mod2048
 Trustpoint CA: firepower_chain
Certificate status: Valid
Certificate:
Data:
 Version: 3 (0x2)
 Serial Number:
 45:00:00:00:0a:de:86:55:16:82:24:f3:be:00:00:00:00:00:00:0a
 Signature Algorithm: ecdsa-with-SHA256
 Issuer: DC=local, DC=naaustin, CN=naaustin-NAAUSTIN-PC-CA
 Validity
 Not Before: Apr 28 13:09:54 2016 GMT
 Not After : Apr 28 13:09:54 2018 GMT
 Subject: C=US, ST=California, L=San Jose, O=Cisco Systems, OU=TAC,
 CN=fp4120.test.local
 Subject Public Key Info:
 Public Key Algorithm: rsaEncryption
 Public-Key: (2048 bit)
 Modulus:
 00:b3:43:8d:e6:06:a0:91:f6:76:7e:2e:09:54:40:
 0d:1b:ee:d8:1a:07:07:6e:75:2d:ec:ba:55:c8:c0:
 a1:9c:a3:8f:26:30:70:91:43:0d:40:0d:66:42:c4:
 50:0d:c6:c9:db:7d:bf:b0:ad:1f:31:29:f2:a8:e2:
 fc:27:30:bb:8a:dc:5e:54:46:51:cb:3e:ff:6b:1e:
 d6:18:db:de:83:f5:cf:fb:37:74:de:7b:78:19:73:
 3a:dc:5b:2b:3d:c3:e6:03:b1:30:82:a0:d2:2e:84:
 a1:b4:11:15:d7:48:61:7f:8f:8d:c3:8a:4a:09:9f:
 9e:49:29:12:26:44:c1:d5:91:da:29:5f:5b:b6:d6:
 20:de:47:ff:50:45:14:82:4f:c4:ca:b5:6a:dc:1f:
 ae:d8:3b:28:a0:f5:6a:ef:a9:93:9b:c0:70:60:ca:
 87:6c:91:2f:e0:f9:ae:46:35:84:f3:cc:84:bd:5c:
 07:ec:94:c4:8a:3f:4e:bf:16:da:b6:30:e3:55:22:
 47:64:15:11:b4:26:a7:bf:20:6f:1a:e2:cf:fd:0f:
 cd:9a:fd:cb:a3:71:bd:21:36:cb:2f:98:08:61:95:
 5a:b5:3c:69:e8:74:d4:7b:31:f6:30:82:33:39:ab:
 d4:e9:dd:6d:07:da:e7:cb:18:06:b6:1e:5d:3d:5d:
 1d:85
 Exponent: 65537 (0x10001)
 X509v3 extensions:
 X509v3 Subject Alternative Name:
 DNS:fp4120.test.local
 X509v3 Subject Key Identifier:
 FF:55:A9:B2:D8:84:60:4C:6C:F0:39:59:59:CB:87:67:03:ED:BB:94
 X509v3 Authority Key Identifier:
 keyid:C8:89:DB:0C:73:EB:17:01:04:05:C6:F1:19:28:10:5B:BA:4E:54:89
 X509v3 CRL Distribution Points:
 Full Name:
 URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=naaustin-pc,CN=CDP,
 CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
 DC=local?certificateRevocationList?base?objectClass=cRLDistributionPoint

 Authority Information Access:
 CA Issuers - URI:ldap:///CN=naaustin-NAAUSTIN-PC-CA,CN=AIA,
 CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=naaustin,
 DC=local?cACertificate?base?objectClass=certificationAuthority
 1.3.6.1.4.1.311.20.2:
 ..W.e.b.S.e.r.v.e.r
 X509v3 Key Usage: critical
 Digital Signature, Key Encipherment
 X509v3 Extended Key Usage:
 TLS Web Server Authentication
 Signature Algorithm: ecdsa-with-SHA256
 30:45:02:20:57:b0:ec:d7:09:8a:b1:2d:15:1b:f2:c6:39:10:
 e3:f7:55:a3:6a:08:e8:24:41:df:4f:16:41:b6:07:35:4b:bf:
 02:21:00:ed:47:4e:6e:24:89:04:6f:cf:05:98:e6:b2:0a:08:
 2b:ad:1a:91:b8:e8:b4:e4:ef:51:d5:1d:f5:be:8a:d5:4c

```







## 플랫폼 설정

- 날짜 및 시간 설정, 85페이지
- SSH 구성, 88페이지
- 텔넷 구성, 90페이지
- SNMP 구성, 90페이지
- HTTPS 구성, 97페이지
- AAA 구성, 108페이지
- Syslog 구성, 118페이지
- DNS 서버 구성, 121페이지

## 날짜 및 시간 설정

날짜 및 시간을 수동으로 설정하거나 현재 시스템 시간을 보려면 NTP 페이지를 사용하여 시스템에서 NTP(Network Time Protocol)를 구성합니다.

NTP 설정은 Firepower 4100/9300 새시와 새시에 설치된 논리적 디바이스 간에 자동으로 동기화됩니다.



참고

Firepower 4100/9300 새시에서 Firepower Threat Defense를 구축 중인 경우, Firepower 4100/9300 새시에 NTP를 구성해야 Smart Licensing이 제대로 작동하고 디바이스 등록 시 적절한 타임스탬프를 보장할 수 있습니다. Firepower 4100/9300 새시와 Firepower Management Center에는 동일한 NTP 서버를 사용해야 합니다.

NTP를 사용 중인 경우, **Current Time**(현재 시간) 탭에서 전체 동기화 상태를 볼 수 있습니다. 또는 **Time Synchronization**(시간 동기화) 탭에 있는 **NTP Server**(NTP 서버) 테이블의 **Server Status**(서버 상태) 필드를 확인하여 구성된 각 NTP 서버의 동기화 상태를 볼 수 있습니다. 시스템이 특정한 NTP 서버와 동기화될 수 없는 경우, 자세한 내용을 보기 위해 서버 상태 옆에 있는 정보 아이콘 위에 마우스 커서를 올려 놓을 수 있습니다.

## 구성된 날짜 및 시간 보기

### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **NTP**를 선택합니다.

단계 2 **Current Time**(현재 시간) 탭을 클릭합니다.  
디바이스에 구성된 날짜, 시간 및 표준 시간대가 표시됩니다.

NTP를 사용 중인 경우, **Current Time**(현재 시간) 탭에서 전체 동기화 상태를 볼 수 있습니다. **Time Synchronization**(시간 동기화) 탭에 있는 **NTP Server**(NTP 서버) 테이블에서 **Server Status**(서버 상태) 필드를 확인하여 구성된 각 NTP 서버의 동기화 상태를 볼 수도 있습니다. 시스템이 특정한 NTP 서버와 동기화될 수 없는 경우, 자세한 내용을 보기 위해 서버 상태 옆에 있는 정보 아이콘 위에 마우스 커서를 올려 놓을 수 있습니다.

## 표준 시간대 설정

### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **NTP**를 선택합니다.

단계 2 **Current Time**(현재 시간) 탭을 클릭합니다.

단계 3 **Time Zone**(표준 시간대) 드롭다운 목록에서 Firepower 새시에 적절한 표준 시간대를 선택합니다.

## NTP를 사용하여 날짜 및 시간 설정

NTP는 네트워크 시스템 간에 정확하게 동기화된 시간을 제공하는 계층적 서버 시스템을 구현하는 데 사용됩니다. 정밀한 타임 스탬프가 포함된 CRL 검증과 같이 시간에 민감한 작업에는 이러한 정확성이 필요합니다. 최대 4개의 NTP 서버를 구성할 수 있습니다.



참고 FXOS 2.2(2) 이상 버전에서는 NTP 버전 3을 사용합니다.



## 절차

- 단계 1 **Platform Settings**(플랫폼 설정) > **NTP**를 선택합니다.
- 단계 2 **Time Synchronization**(시간 동기화) 탭을 클릭합니다.
- 단계 3 **Set Time Source**(시간 소스 설정)에서 **Use NTP Server**(NTP 서버 사용).
- 단계 4 사용할 각 NTP 서버(최대 4개)에 대해 **NTP Server**(NTP 서버) 필드에 NTP 서버의 IP 주소 또는 호스트 이름을 입력하고 **Add**(추가)를 클릭합니다.
- 단계 5 **Save**(저장)를 클릭합니다.

Firepower 새시는 NTP 서버 정보가 지정된 상태로 구성됩니다.

**NTP Server**(NTP 서버) 테이블에서 **Server Status**(서버 상태) 필드를 살펴보면 각 서버의 동기화 상태를 볼 수 있습니다. 시스템이 특정한 NTP 서버와 동기화될 수 없는 경우, 자세한 내용을 보기 위해 서버 상태 옆에 있는 정보 아이콘 위에 마우스 커서를 올려 놓을 수 있습니다.

**참고** 시스템 시간을 10분 이상 수정하는 경우, 시스템에서 로그아웃되며 Firepower Chassis Manager에 다시 로그인해야 합니다.

## NTP 서버 삭제

### 절차

- 단계 1 **Platform Settings**(플랫폼 설정) > **NTP**를 선택합니다.
- 단계 2 **Time Synchronization**(시간 동기화) 탭을 클릭합니다.
- 단계 3 제거할 각 NTP 서버에 대해 **NTP Server**(NTP 서버) 테이블에서 해당 서버의 **Delete**(삭제) 아이콘을 클릭합니다.
- 단계 4 **Save**(저장)를 클릭합니다.

## 날짜 및 시간 수동 설정

이 섹션에서는 Firepower 새시에 날짜 및 시간을 수동으로 설정하는 방법을 설명합니다.

## 절차

- 
- 단계 1 **Platform Settings**(플랫폼 설정) > **NTP**를 선택합니다.
- 단계 2 **Time Synchronization**(시간 동기화) 탭을 클릭합니다.
- 단계 3 **Set Time Source**(시간 소스 설정)에서 **Set Time Manually**(수동으로 시간 설정)를 클릭합니다.
- 단계 4 **Date**(날짜) 드롭다운 목록을 클릭하여 달력을 표시한 다음, 달력에서 사용 가능한 컨트롤을 사용하여 날짜를 설정합니다.
- 단계 5 해당하는 드롭다운 목록을 사용하여 시간을 시, 분 및 오전/오후로 지정합니다.  
 팁 **Get System Time**(시스템 시간 가져오기)을 클릭하여 Firepower Chassis Manager 연결에 사용 중인 시스템에 구성된 것과 일치하도록 날짜 및 시간을 설정할 수 있습니다.
- 단계 6 **Save**(저장)를 클릭합니다.  
 Firepower 새시는 날짜 및 시간이 지정된 상태로 구성됩니다.
- 참고 시스템 시간을 10분 이상 수정하는 경우, 시스템에서 로그아웃되며 Firepower Chassis Manager에 다시 로그인해야 합니다.
- 

## SSH 구성

다음 절차에서는 Firepower 새시에 대한 SSH 액세스를 활성화하거나 비활성화하는 방법과 FXOS 새시를 SSH 클라이언트로 활성화하는 방법을 설명합니다. SSH는 기본적으로 활성화되어 있습니다.

## 절차

- 
- 단계 1 **Platform Settings**(플랫폼 설정) > **SSH** > **SSH Server**(SSH 서버)를 선택합니다.
- 단계 2 Firepower 새시에 대한 SSH 액세스를 활성화하려면 **Enable SSH**(SSH 활성화) 확인란을 선택합니다. SSH 액세스를 비활성화하려면 **Enable SSH**(SSH 활성화) 확인란의 선택을 취소합니다.
- 단계 3 서버의 **Encryption Algorithm**(암호화 알고리즘)에 대해 각각의 허용되는 암호화 알고리즘의 확인란을 선택합니다.  
 참고 3des-cbc는 공통 기준에서 지원되지 않습니다. 공통 기준 모드가 FXOS 새시에서 활성화되어 있는 경우, 3des-cbc를 암호화 알고리즘으로 사용할 수 없습니다.
- 단계 4 서버의 **Key Exchange Algorithm**(키 교환 알고리즘)에 대해 각각의 허용되는 DH(Diffie-Hellman) 키 교환의 확인란을 선택합니다. DH 키 교환에서는 어느 한쪽에서 단독으로 확인할 수 없는 공유 암호를 제공합니다. 이 키 교환은 서명 및 호스트 키와 연계하여 호스트 인증을 제공합니다. 이 키 교환 방법은 명시적 서버 인증을 제공합니다. DH 키 교환 방법 사용에 대한 자세한 내용은 RFC 4253을 참조하십시오.
- 단계 5 서버의 **Mac Algorithm**(Mac 알고리즘)에 대해 각각의 허용되는 무결성 알고리즘의 확인란을 선택합니다.
- 단계 6 서버의 **Host Key**(호스트 키)에 대해 RSA 키 쌍에 대한 모듈러스 크기를 입력합니다.

모듈러스 값(비트 단위)은 1024~2048 범위의 8의 배수입니다. 지정하는 키 모듈러스 크기가 클수록 RSA 키 쌍을 생성하는 데 오래 걸립니다. 권장되는 값은 2048입니다.

- 단계 7 서버의 **Volume Rekey Limit**(볼륨 키 재생성 제한)에 대해 FXOS가 세션에서 연결을 해제하기 전에 연결을 통해 허용되는 트래픽 양(KB 단위)을 설정합니다.
- 단계 8 서버의 **Time Rekey Limit**(시간 키 재생성 제한)에 대해 FXOS가 세션에서 연결을 해제하기 전에 SSH 세션이 유효 상태가 될 수 있는 시간(분 단위)을 설정합니다.
- 단계 9 **Save**(저장)를 클릭합니다.
- 단계 10 FXOS 새시 SSH 클라이언트를 맞춤화하려면 **SSH Client**(SSH 클라이언트) 탭을 클릭합니다.
- 단계 11 **Strict Host Keycheck**(엄격한 호스트 키 확인)에 대해 **enable**(활성화), **disable**(비활성화) 또는 **prompt**(프롬프트)를 선택하여 SSH 호스트 키 확인을 제어합니다.
- **enable**(활성화) — 호스트 키가 FXOS의 알려진 호스트 파일에 없는 경우 연결이 거부됩니다. 시스템/서비스 범위에서 **enter ssh-host** 명령을 사용하여 FXOS CLI에서 수동으로 호스트를 추가해야 합니다.
  - **prompt**(프롬프트) — 호스트 키가 새시에 저장되어 있지 않은 경우 호스트 키를 수락 또는 거부하라는 프롬프트가 표시됩니다.
  - **disable**(비활성화) — (기본값) 이전에 저장한 호스트 키가 없는 경우 새시가 호스트 키를 자동으로 수락합니다.
- 단계 12 클라이언트의 **Encryption Algorithm**(암호화 알고리즘)에 대해 각각의 허용되는 암호화 알고리즘의 확인란을 선택합니다.
- 참고** 3des-cbc는 공통 기준에서 지원되지 않습니다. 공통 기준 모드가 FXOS 새시에서 활성화되어 있는 경우, 3des-cbc를 암호화 알고리즘으로 사용할 수 없습니다.
- 단계 13 클라이언트의 **Key Exchange Algorithm**(키 교환 알고리즘)에 대해 각각의 허용되는 DH(Diffie-Hellman) 키 교환의 확인란을 선택합니다. DH 키 교환에서는 어느 한쪽에서 단독으로 확인할 수 없는 공유 암호를 제공합니다. 이 키 교환은 서명 및 호스트 키와 연계하여 호스트 인증을 제공합니다. 이 키 교환 방법은 명시적 서버 인증을 제공합니다. DH 키 교환 방법에 대한 자세한 내용은 RFC 4253을 참조하십시오.
- 단계 14 클라이언트의 **Mac Algorithm**(Mac 알고리즘)에 대해 각각의 허용되는 무결성 알고리즘의 확인란을 선택합니다.
- 단계 15 클라이언트의 **Volume Rekey Limit**(볼륨 키 재생성 제한)에 대해 FXOS가 세션에서 연결을 해제하기 전에 연결을 통해 허용되는 트래픽 양(KB 단위)을 설정합니다.
- 단계 16 클라이언트의 **Time Rekey Limit**(시간 키 재생성 제한)에 대해 FXOS가 세션에서 연결을 해제하기 전에 SSH 세션이 유효 상태가 될 수 있는 시간(분 단위)을 설정합니다.
- 단계 17 **Save**(저장)를 클릭합니다.

## 텔넷 구성

다음 절차에서는 Firepower 새시에 대한 텔넷 액세스를 활성화하거나 비활성화하는 방법을 설명합니다. 텔넷은 기본적으로 비활성화되어 있습니다.



**참고** 텔넷 컨피그레이션은 현재 CLI를 사용하는 경우에만 사용할 수 있습니다.

### 절차

- 
- 단계 1** 시스템 모드를 시작합니다.  
Firepower-chassis #**scope system**
- 단계 2** 시스템 서비스 모드를 시작합니다.  
Firepower-chassis /system #**scope services**
- 단계 3** Firepower 새시에 대한 텔넷 액세스를 구성하려면 다음 중 하나를 수행합니다.
- Firepower 새시에 대한 텔넷 액세스를 허용하려면 다음 명령을 입력합니다.  
Firepower-chassis /system/services # **enable telnet-server**
  - Firepower 새시에 대한 텔넷 액세스를 허용하지 않으려면 다음 명령을 입력합니다.  
Firepower-chassis /system/services # **disable telnet-server**
- 단계 4** 시스템 컨피그레이션에 트랜잭션을 커밋합니다.  
Firepower /system/services # **commit-buffer**
- 

다음 예에서는 텔넷을 활성화하고 트랜잭션을 커밋합니다.

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /services # enable telnet-server
Firepower-chassis /services* # commit-buffer
Firepower-chassis /services #
```

## SNMP 구성

SNMP 페이지에서 Firepower 새시에 SNMP(Simple Network Management Protocol)를 구성할 수 있습니다. 자세한 내용은 다음 항목을 참고하십시오.

## SNMP 정보

SNMP(Simple Network Management Protocol)는 애플리케이션 레이어 프로토콜로서 SNMP 관리자와 에이전트 간 통신을 위한 메시지 형식을 제공합니다. SNMP는 네트워크의 디바이스를 모니터링하고 관리할 수 있도록 표준화된 프레임워크 및 공용어를 제공합니다.

SNMP 프레임워크는 세 부분으로 구성됩니다.

- SNMP 관리자 — SNMP를 사용하는 네트워크 디바이스의 활동을 제어하고 모니터링하는 데 사용되는 시스템입니다.
- SNMP 에이전트 — Firepower 새시에 대한 데이터를 유지하고 필요에 따라 데이터를 SNMP 관리자에게 보고하는 Firepower 새시 내부의 소프트웨어 구성 요소입니다. Firepower 새시에는 에이전트 및 MIB 모음이 포함되어 있습니다. SNMP 에이전트를 활성화하고 관리자와 에이전트 간의 관계를 생성하려면 Firepower Chassis Manager 또는 FXOS CLI에서 SNMP를 활성화하고 구성합니다.
- MIB(managed information base) — SNMP 에이전트에 있는 관리 객체의 모음입니다.

Firepower 새시는 SNMPv1, SNMPv2c 및 SNMPv3를 지원합니다. SNMPv1 및 SNMPv2c는 모두 커뮤니티 기반 보안 유형을 사용합니다. SNMP는 다음과 같이 정의됩니다.

- RFC 3410(<http://tools.ietf.org/html/rfc3410>)
- RFC 3411(<http://tools.ietf.org/html/rfc3411>)
- RFC 3412(<http://tools.ietf.org/html/rfc3412>)
- RFC 3413(<http://tools.ietf.org/html/rfc3413>)
- RFC 3414(<http://tools.ietf.org/html/rfc3414>)
- RFC 3415(<http://tools.ietf.org/html/rfc3415>)
- RFC 3416(<http://tools.ietf.org/html/rfc3416>)
- RFC 3417(<http://tools.ietf.org/html/rfc3417>)
- RFC 3418(<http://tools.ietf.org/html/rfc3418>)
- RFC 3584(<http://tools.ietf.org/html/rfc3584>)

## SNMP 알람

SNMP의 핵심 기능 중 하나는 SNMP 에이전트의 알람을 생성하는 것입니다. SNMP 관리자는 이러한 알람에 대해 요청을 보낼 필요가 없습니다. 알람은 잘못된 사용자 인증, 재시작, 연결 종료, 네이버 라우터와의 연결 끊김, 기타 중대한 이벤트를 나타낼 수 있습니다.

Firepower 새시는 SNMP 알람을 트랩 또는 정보로 생성합니다. SNMP 관리자가 트랩을 수신할 때 승인을 전송하지 않으며 Firepower 새시에서는 트랩 수신 여부를 확인할 수 없으므로 트랩은 정보보다 신뢰성이 떨어집니다. 정보 요청을 수신한 SNMP 관리자는 SNMP 응답 PDU(Protocol Data Unit)로 메

시지를 승인합니다. Firepower 새시에서 PDU를 수신하지 않을 경우 정보 요청을 다시 보낼 수 있습니다.

## SNMP 보안 레벨 및 권한

SNMPv1, SNMPv2c, SNMPv3은 각각 서로 다른 보안 모델을 나타냅니다. 보안 모델 및 선택된 보안 레벨의 조합을 통해 SNMP 메시지 처리 시 적용할 보안 메커니즘이 결정됩니다.

보안 레벨은 SNMP 트랩과 연결된 메시지를 보는 데 필요한 권한을 결정합니다. 권한 레벨은 메시지가 공개되지 않도록 보호하거나 인증해야 할지 결정합니다. 지원되는 보안 레벨은 어떤 보안 모델이 구현되었는지에 따라 달라집니다. SNMP 보안 레벨은 다음 권한을 하나 이상 지원합니다.

- noAuthNoPriv — 인증도 암호화도 없음
- authNoPriv — 인증은 있지만 암호화 없음
- authPriv — 인증 및 암호화 있음

SNMPv3는 보안 모델 및 보안 레벨을 모두 제공합니다. 보안 모델은 사용자 및 사용자가 속한 역할에 대해 설정되는 인증 전략입니다. 보안 레벨은 보안 모델 내에서 허용된 보안 레벨입니다. 보안 모델과 보안 레벨의 조합을 통해 SNMP 패킷 처리 시 적용할 보안 메커니즘이 결정됩니다.

## 지원되는 SNMP 보안 모델 및 레벨의 조합

다음 표에서는 보안 모델 및 레벨의 조합에 대해 설명합니다.

**표 5: SNMP 보안 모델 및 레벨**

| 모델  | 레벨           | 인증       | 암호화 | 결과                                               |
|-----|--------------|----------|-----|--------------------------------------------------|
| v1  | noAuthNoPriv | 커뮤니티 문자열 | 아니요 | 인증에 커뮤니티 문자열 일치를 사용합니다.                          |
| v2c | noAuthNoPriv | 커뮤니티 문자열 | 아니요 | 인증에 커뮤니티 문자열 일치를 사용합니다.                          |
| v3  | noAuthNoPriv | 사용자 이름   | 아니요 | 인증에 사용자 이름 일치를 사용합니다.                            |
| v3  | authNoPriv   | HMAC-SHA | 아니요 | HMAC SHA(Secure Hash Algorithm)를 기반으로 인증을 제공합니다. |

| 모델 | 레벨       | 인증       | 암호화 | 결과                                                                                                                               |
|----|----------|----------|-----|----------------------------------------------------------------------------------------------------------------------------------|
| v3 | authPriv | HMAC-SHA | DES | HMAC-SHA 알고리즘을 기반으로 인증을 제공합니다. DES(Data Encryption Standard) 56비트 암호화 및 CBC(Cipher Block Chaining) DES(DES-56) 표준 기반의 인증을 제공합니다. |

## SNMPv3 보안 기능

SNMPv3에서는 네트워크를 통한 인증 프레임과 암호화 프레임의 조합을 통해 디바이스에 대한 보안 액세스를 제공합니다. SNMPv3에서는 구성된 사용자에게 의한 관리 작업만 승인하고 SNMP 메시지를 암호화합니다. SNMPv3 USM(User-Based Security Model)은 SNMP 메시지 레벨 보안을 가리키며 다음 서비스를 제공합니다.

- 메시지 통합 — 메시지가 무단으로 변경 또는 손상되지 않았는지, 그리고 데이터 시퀀스가 비약의적인 방식으로 발생할 수 있는 것보다 더 많이 변경되지 않았는지 확인합니다.
- 메시지 출처 인증 — 수신 데이터를 만든 사용자의 클레임된 ID가 확인되도록 보장합니다.
- 메시지 기밀 보호 및 암호화 — 미승인 개인, 엔터티 또는 프로세스에 정보가 제공되거나 공개되지 않도록 합니다.

## SNMP 지원

Firepower 새시는 SNMP에 다음을 지원합니다.

### MIB 지원

Firepower 새시는 MIB에 대해 읽기 전용 액세스를 지원합니다.

### SNMPv3 사용자를 위한 인증 프로토콜

Firepower 새시는 SNMPv3 사용자를 위해 HMAC-SHA-96(SHA) 인증 프로토콜을 지원합니다.

**SNMPv3** 사용자를 위한 **AES** 개인 프로토콜

Firepower 새시는 SNMPv3 메시지 암호화를 위한 개인 프로토콜 중 하나로 AES(Advanced Encryption Standard)를 사용하며 RFC 3826을 준수합니다.

개인 비밀번호(priv) 옵션에서는 SNMP 보안 암호화를 위해 DES 또는 128비트 AES 암호화를 선택할 수 있습니다. AES-128 컨피그레이션을 활성화하는 경우 SNMPv3 사용자를 위한 개인 비밀번호가 있으면 Firepower 새시에서는 개인 비밀번호를 사용하여 128비트 AES 키를 생성합니다. AES 개인 비밀번호는 최소 8자입니다. 비밀번호가 일반 텍스트로 지정된 경우 최대 64자로 지정할 수 있습니다.

**SNMP 활성화 및 SNMP 속성 구성**

## 절차

단계 1 **Platform Settings**(플랫폼 설정) > **SNMP**를 선택합니다.

단계 2 **SNMP** 영역에서 다음 필드를 입력합니다.

| Name                                             | 설명                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Admin State</b> (관리 상태) 확인란                   | SNMP를 활성화할지 아니면 비활성화할지 선택합니다. 이 서비스는 시스템에 SNMP 서버와의 통합이 포함되는 경우에만 활성화합니다.                                                                                                                                                                                                                                                                                                                                                      |
| <b>Port</b> (포트) 필드                              | Firepower 새시가 SNMP 호스트와 통신할 때 사용할 포트입니다. 기본 포트를 변경할 수 없습니다.                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Community/Username</b> (커뮤니티/사용자 이름) 필드       | Firepower 새시가 SNMP 호스트에 전송하는 모든 트랩 메시지에 포함되는 기본 SNMP v1 또는 v2 커뮤니티 이름이나 SNMP v3 사용자 이름입니다.<br><br>영숫자 문자열은 1자~32자로 입력합니다. @ (at 기호), \ (백슬래시), " (큰따옴표), ? (물음표) 또는 공백을 사용하지 마십시오. 기본값은 public입니다.<br><br><b>Community/Username</b> (커뮤니티/사용자 이름) 필드가 이미 설정된 경우, 비어 있는 필드의 오른쪽에 <b>Set: Yes</b> (설정: 예)라고 적혀 있습니다. <b>Community/Username</b> (커뮤니티/사용자 이름) 필드에 값이 아직 없는 경우, 비어 있는 필드의 오른쪽에 <b>Set: No</b> (설정: 아니요)라고 적혀 있습니다. |
| <b>System Administrator Name</b> (시스템 관리자 이름) 필드 | SNMP 구현을 책임지는 담당자입니다.<br><br>이메일 주소 또는 이름과 전화번호 등 최대 255자의 문자열을 입력합니다.                                                                                                                                                                                                                                                                                                                                                         |
| <b>Location</b> (위치) 필드                          | SNMP 에이전트(서버)가 실행되는 호스트의 위치입니다.<br><br>최대 510자의 영숫자 문자열을 입력합니다.                                                                                                                                                                                                                                                                                                                                                                |



단계 3 **Save(저장)**를 클릭합니다.

### 다음에 할 작업

SNMP 트랩 및 사용자를 생성합니다.

## SNMP 트랩 생성

### 절차

단계 1 **Platform Settings(플랫폼 설정) > SNMP**를 선택합니다.

단계 2 **SNMP Traps(SNMP 트랩)** 영역에서 **Add(추가)**를 클릭합니다.

단계 3 **Add SNMP Trap(SNMP 트랩 추가)** 대화 상자에서 다음 필드를 입력합니다.

| Name                                      | 설명                                                                                                                                                                                                                      |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 호스트 이름 필드                                 | Firepower 새시가 트랩을 전송해야 하는 SNMP 호스트의 호스트 이름 또는 IP 주소입니다.                                                                                                                                                                 |
| <b>Community/Username(커뮤니티/사용자 이름)</b> 필드 | Firepower 새시가 SNMP 호스트에 트랩을 전송할 때 포함하는 SNMP v1 또는 v2 커뮤니티 이름이나 SNMP v3 사용자 이름입니다. 이는 SNMP 서비스에 대해 구성된 커뮤니티 또는 사용자 이름과 동일해야 합니다.<br><br>영숫자 문자열은 1자~32자로 입력합니다. @ (at 기호), \ (백슬래시), " (큰따옴표), ? (물음표) 또는 공백을 사용하지 마십시오. |
| <b>Port(포트)</b> 필드                        | Firepower 새시가 트랩을 위해 SNMP 호스트와 통신할 때 사용할 포트입니다.<br><br>1~65535의 정수를 입력합니다.                                                                                                                                              |
| <b>Version(버전)</b> 필드                     | 트랩에 사용할 SNMP 버전 및 모델입니다. 다음 중 하나일 수 있습니다. <ul style="list-style-type: none"> <li>• V1</li> <li>• V2</li> <li>• V3</li> </ul>                                                                                            |

| Name                   | 설명                                                                                                                                                                                                                      |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type(유형) 필드            | <p><b>V2</b> 또는 <b>V3</b> 버전을 선택하는 경우, 전송할 트랩의 유형입니다. 다음 중 하나일 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 트랩</li> <li>• 정보</li> </ul>                                                                         |
| v3 Privilege(v3 권한) 필드 | <p><b>V3</b> 버전을 선택하는 경우, 트랩과 연관된 권한입니다. 다음 중 하나일 수 있습니다.</p> <ul style="list-style-type: none"> <li>• <b>Auth</b> — 인증은 있지만 암호화 없음</li> <li>• <b>Noauth</b> — 인증도 암호화도 없음</li> <li>• <b>Priv</b> — 인증 및 암호화</li> </ul> |

단계 4 **OK**(확인)를 클릭하여 **Add SNMP Trap**(SNMP 트랩 추가) 대화 상자를 닫습니다.

단계 5 **Save**(저장)를 클릭합니다.

## SNMP 트랩 삭제

### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **SNMP**를 선택합니다.

단계 2 **SNMP Traps**(SNMP 트랩) 영역에서 삭제할 트랩에 해당하는 테이블의 행에 있는 **Delete**(삭제) 아이콘을 클릭합니다.

## SNMPv3 사용자 생성

### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **SNMP**를 선택합니다.

단계 2 **SNMP Users**(SNMP 사용자) 영역에서 **Add**(추가)를 클릭합니다.

단계 3 **Add SNMP User**(SNMP 사용자 추가) 대화 상자에서 다음 필드를 입력합니다.

| Name                                    | 설명                                                                                                                 |
|-----------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Name(이름) 필드                             | SNMP 사용자에게 할당된 사용자 이름입니다.<br>최대 32개의 문자 또는 숫자를 입력합니다. 이름은 문자로 시작해야 하며 _(밑줄), .(마침표), @(앳 기호) 및 -(하이픈)을 지정할 수 있습니다. |
| Auth Type(인증 유형) 필드                     | 권한 부여 유형: <b>SHA</b>                                                                                               |
| Use AES-128(AES-128 사용) 확인란             | 이 확인란을 선택한 경우, 이 사용자는 AES-128 암호화를 사용합니다.                                                                          |
| Password(비밀번호) 필드                       | 이 사용자의 비밀번호입니다.                                                                                                    |
| Confirm Password(비밀번호 확인) 필드            | 확인을 위해 다시 한 번 입력하는 비밀번호입니다.                                                                                        |
| Privacy Password(개인 비밀번호) 필드            | 이 사용자의 개인 비밀번호입니다.                                                                                                 |
| Confirm Privacy Password(개인 비밀번호 확인) 필드 | 확인을 위해 다시 한 번 입력하는 개인 비밀번호입니다.                                                                                     |

단계 4 **OK**(확인)를 클릭하여 **Add SNMP User**(SNMP 사용자 추가) 대화 상자를 닫습니다.

단계 5 **Save**(저장)를 클릭합니다.

## SNMPv3 사용자 삭제

### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **SNMP**를 선택합니다.

단계 2 **SNMP Users**(SNMP 사용자) 영역에서 삭제할 사용자에게 해당하는 테이블의 행에 있는 **Delete**(삭제) 아이콘을 클릭합니다.

## HTTPS 구성

이 섹션에서는 Firepower 4100/9300 새시에 HTTPS를 구성하는 방법을 설명합니다.

**참고**

Firepower Chassis Manager 또는 FXOS CLI를 사용하여 HTTPS 포트를 변경할 수 있습니다. 다른 모든 HTTPS 컨피그레이션은 FXOS CLI를 사용하는 경우에만 수행할 수 있습니다.

## 인증서, 키 링 및 트러스트 포인트

HTTPS에서는 PKI(Public Key Infrastructure)의 구성 요소를 사용하여 두 디바이스, 이를테면 클라이언트의 브라우저와 Firepower 4100/9300 채시 간의 보안 통신을 설정합니다.

### 암호화 키 및 키 링

각 PKI 디바이스는 비대칭 RSA(Rivest-Shamir-Adleman) 암호화 키의 쌍을 보유합니다. 개인 키와 공개 키로 구성된 이 쌍은 내부 키 링에 저장됩니다. 두 키 중 하나로 암호화된 메시지는 나머지 키로 해독할 수 있습니다. 암호화된 메시지를 보낼 때 발신자는 수신자의 공개 키로 메시지를 암호화하며 수신자는 자신의 개인 키로 그 메시지를 해독합니다. 발신자는 알려진 메시지를 자신의 개인 키로 암호화(‘서명’이라고도 함)하여 공개 키에 대한 소유권을 입증할 수도 있습니다. 수신자가 해당 공개 키를 사용하여 성공적으로 메시지를 해독할 수 있다면 발신자가 해당 개인 키를 소유하고 있음이 입증됩니다. 암호화 키의 길이는 다양하지만, 일반적으로 512~2048비트입니다. 일반적으로 키는 길수록 더 안전합니다. FXOS에서는 초기 2048비트 키 쌍으로 기본 키 링을 제공하며, 사용자가 추가 키 링을 생성할 수 있습니다.

클러스터 이름이 변경되거나 인증서가 만료되는 경우 기본 키 링 인증서를 수동으로 재생성해야 합니다.

### 인증서

안전한 통신을 위해 두 디바이스는 먼저 디지털 인증서를 교환합니다. 인증서는 디바이스 ID에 대해 서명된 정보와 함께 디바이스 공개 키를 포함하는 파일입니다. 단순히 암호화된 통신을 지원하기 위해 디바이스에서 자신의 키 쌍 및 자체 서명된 인증서를 생성할 수 있습니다. 원격 사용자가 자체 서명 인증서가 있는 디바이스에 연결하는 경우 사용자는 디바이스의 ID를 쉽게 확인할 방법이 없으며 사용자의 브라우저는 초기에 인증 경고를 표시합니다. 기본적으로 FXOS에는 기본 키 링의 공개 키를 포함하는 자체 서명 인증서가 내장되어 있습니다.

### 트러스트 포인트

신뢰할 수 있는 출처 또는 트러스트 포인트로부터 디바이스의 ID를 확인하는 서드파티 인증서를 얻어 설치하면 FXOS에 대해 더 강력한 인증을 제공할 수 있습니다. 서드파티 인증서는 해당 인증서를 발급하는 트러스트 포인트에서 서명되며, 루트 CA(인증 기관), 중간 CA 또는 루트 CA로 연결되는 트러스트 체인의 일부인 트러스트 앵커가 될 수 있습니다. 새 인증서를 얻으려면 FXOS를 통해 인증서 요청을 생성하고 트러스트 포인트에 요청을 제출해야 합니다.

**중요**

인증서는 Base64 인코딩 X.509(CER) 형식이어야 합니다.

## 키 링 생성

FXOS는 기본 키 링을 포함하여 최대 8개의 키 링을 지원합니다.

### 절차

- 
- 단계 1 보안 모드를 시작합니다.  
Firepower-chassis #**scope security**
  - 단계 2 키 링을 생성하고 이름을 지정합니다.  
Firepower-chassis # **createkeyring** *keyring-name*
  - 단계 3 SSL 키 길이(비트)를 설정합니다.  
Firepower-chassis # **setmodulus** {**mod1024** | **mod1536** | **mod2048** | **mod512**}
  - 단계 4 트랜잭션을 커밋합니다.  
Firepower-chassis # **commit-buffer**
- 

다음 예에서는 키 크기가 1024비트인 키 링을 생성합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # create keyring kr220
Firepower-chassis /security/keyring* # set modulus mod1024
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

### 다음에 할 작업

이 키 링에 대한 인증서 요청을 생성합니다.

## 기본 키 링 재생성

클러스터 이름이 변경되거나 인증서가 만료되는 경우 기본 키 링 인증서를 수동으로 재생성해야 합니다.

### 절차

- 
- 단계 1 보안 모드를 시작합니다.  
Firepower-chassis #**scope security**
  - 단계 2 기본 키 링의 키 링 보안 모드를 시작합니다.  
Firepower-chassis /security # **scopekeyring default**
  - 단계 3 기본 키 링을 재생성합니다.  
Firepower-chassis /security/keyring # **setregenerate yes**
  - 단계 4 트랜잭션을 커밋합니다.  
Firepower-chassis # **commit-buffer**

다음 예에서는 기본 키 링을 재생성합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring default
Firepower-chassis /security/keyring* # set regenerate yes
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

## 키 링에 대한 인증서 요청 생성

### 기본 옵션을 사용하여 키 링에 대한 인증서 요청 생성

#### 절차

- 단계 1 보안 모드를 시작합니다.  
Firepower-chassis #**scope security**
- 단계 2 키 링의 컨피그레이션 모드를 시작합니다.  
Firepower-chassis /security # **scope keyring** *keyring-name*
- 단계 3 지정된 IPv4 또는 IPv6 주소 또는 패브릭 인터커넥트의 이름을 사용하여 인증서 요청을 생성합니다. 인증서 요청에 대한 비밀번호를 입력하라는 프롬프트가 표시됩니다.  
Firepower-chassis /security/keyring # **create certreq** {ip [*ipv4-addr* | *ipv6-v6*] |**subject-name** *name*}
- 단계 4 트랜잭션을 커밋합니다.  
Firepower-chassis /security/keyring/certreq # **commit-buffer**
- 단계 5 인증서 요청을 표시합니다. 이 요청은 복사하여 트러스트 앵커 또는 인증 기관에 보낼 수 있습니다.  
Firepower-chassis /security/keyring # **show certreq**

다음 예에서는 기본 옵션을 사용하여 키 링에 대한 IPv4 주소로 인증서 요청을 생성하고 표시합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq ip 192.168.200.123 subject-name sjc04
Certificate request password:
Confirm certificate request password:
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name:
Certificate request country name:
State, province or county (full name):
Locality (eg, city):
Organization name (eg, company):
Organization Unit name (eg, section):
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwZjZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKnl1t8qMZO4UGqILKFXQQc2c8b/vW2rnRF80PhKbhghLAlYZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHO4SwccAUXQ5Zngf45YtXlWsyLwUWV4
Ore/zgTk/WCd56RF0BvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGG
```

```

LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQQMA6CBnNhbWMwNlECsEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCsxN0qUHYGFoQw56RwQueLTNPnrndqUwuZHU003Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWicTWgHh8BimOb/0OKuG8kwfIGGsED1Av
TTYvUP+BZ9OFiPbRIA718S+V8ndXr1HejiQGx1DNqoN+odCXFc5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----

Firepower-chassis /security/keyring #

```

### 다음에 할 작업

- BEGIN(시작) 및 END(끝) 라인을 포함하여 인증서 요청의 텍스트를 복사하여 파일에 저장합니다. 키 링에 대한 인증서를 얻으려면 파일을 인증서 요청과 함께 트러스트 앵커 또는 인증 기관에 전송합니다.
- 트러스트 포인트를 생성하고 트러스트 앵커에서 수신한 신뢰할 수 있는 인증서에 대한 인증서 체인을 설정합니다.

## 고급 옵션을 사용하여 키 링에 대한 인증서 요청 생성

### 절차

- 
- 단계 1** 보안 모드를 시작합니다.  
Firepower-chassis #**scope security**
- 단계 2** 키 링의 컨피그레이션 모드를 시작합니다.  
Firepower-chassis /security # **scope keyring** *keyring-name*
- 단계 3** 인증서 요청을 생성합니다.  
Firepower-chassis /security/keyring # **createcertreq**
- 단계 4** 회사가 위치한 국가의 국가 코드를 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set country** *country name*
- 단계 5** 요청과 연관된 DNS(도메인 이름 서버) 주소를 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set dns** *DNS Name*
- 단계 6** 인증서 요청과 연관된 이메일 주소를 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set e-mail** *E-mail name*
- 단계 7** Firepower 4100/9300 새시의 IP 주소를 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set ip** {*certificate request ip-address*|*certificate request ip6-address* }
- 단계 8** 인증서를 요청하는 회사의 본사가 위치한 도시 또는 지역을 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set locality** *locality name (eg, city)*
- 단계 9** 인증서를 요청하는 조직을 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set org-name** *organization name*
- 단계 10** 조직 단위를 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set org-unit-name** *organizational unit name*

- 단계 11 선택적으로 인증서 요청에 대한 비밀번호를 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set password** *certificate request password*
- 단계 12 인증서를 요청하는 회사의 본사가 위치한 시/도를 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set state** *state, province or county*
- 단계 13 Firepower 4100/9300 새시의 정규화된 도메인 이름을 지정합니다.  
Firepower-chassis /security/keyring/certreq\* # **set subject-name** *certificate request name*
- 단계 14 트랜잭션을 커밋합니다.  
Firepower-chassis /security/keyring/certreq # **commit-buffer**
- 단계 15 인증서 요청을 표시합니다. 이 요청은 복사하여 트러스트 앵커 또는 인증 기관에 보낼 수 있습니다.  
Firepower-chassis /security/keyring # **show certreq**

다음 예에서는 고급 옵션을 사용하여 키 링에 대한 IPv4 주소로 인증서 요청을 생성하고 표시합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # create certreq
Firepower-chassis /security/keyring/certreq* # set ip 192.168.200.123
Firepower-chassis /security/keyring/certreq* # set subject-name sjc04
Firepower-chassis /security/keyring/certreq* # set country US
Firepower-chassis /security/keyring/certreq* # set dns bg1-samc-15A
Firepower-chassis /security/keyring/certreq* # set email test@cisco.com
Firepower-chassis /security/keyring/certreq* # set locality new york city
Firepower-chassis /security/keyring/certreq* # set org-name "Cisco Systems"
Firepower-chassis /security/keyring/certreq* # set org-unit-name Testing
Firepower-chassis /security/keyring/certreq* # set state new york
Firepower-chassis /security/keyring/certreq* # commit-buffer
Firepower-chassis /security/keyring/certreq # show certreq
Certificate request subject name: sjc04
Certificate request ip address: 192.168.200.123
Certificate request e-mail name: test@cisco.com
Certificate request country name: US
State, province or county (full name): New York
Locality name (eg, city): new york city
Organization name (eg, company): Cisco
Organization Unit name (eg, section): Testing
Request:
-----BEGIN CERTIFICATE REQUEST-----
MIIBfTCB5wIBADARMQ8wDQYDVQQDEwZzYW1jMDQwZ8wDQYJKoZIhvcNAQEBBQAD
gY0AMIGJAoGBALpKnl8qMZO4UGqILKFXQQc2c8b/vW2rnRF80PhKbghLAlYZ1F
JqcYEG5Yl1+vgohLBTd45s0GC8m4RTLJWHo4SwccAUXQ5Zngf45YtXlWsyUwV4
0re/zgTk/WCd56RfOBvWR2Dtztu2pGA14sd761zLxt29K7R8mzj6CAUVAgMBAAGg
LTArBgkqhkiG9w0BCQ4xHjAcMBoGA1UdEQEB/wQMA6CBnNhbWMwNiECSEiXjAN
BgkqhkiG9w0BAQQFAAOBgQCcsxN0qUHYGFoQw56RwQueLTnPnrndqUwuZHUU03Teg
nhsyu4satpyiPqVV9viKZ+spvc6x5PWICTWgHhH8BimOb/0OKuG8kwfIGGsED1Av
TTYvUP+BZ9OFiPbRIA718S+V8ndXrlHejiQGx1DNqon+odCXPC5kjoXD01ZTL09H
BA==
-----END CERTIFICATE REQUEST-----
Firepower-chassis /security/keyring/certreq #
```

### 다음에 할 작업

- BEGIN(시작) 및 END(끝) 라인을 포함하여 인증서 요청의 텍스트를 복사하여 파일에 저장합니다. 키 링에 대한 인증서를 얻으려면 파일을 인증서 요청과 함께 트러스트 앵커 또는 인증 기관에 전송합니다.



- 트러스트 포인트를 생성하고 트러스트 앵커에서 수신한 신뢰할 수 있는 인증서에 대한 인증서 체인을 설정합니다.

## 트러스트 포인트 생성

### 절차

단계 1 보안 모드를 시작합니다.

```
Firepower-chassis #scope security
```

단계 2 트러스트 포인트를 생성합니다.

```
Firepower-chassis /security # createtrustpoint name
```

단계 3 이 트러스트 포인트에 대한 인증서 정보를 지정합니다.

```
Firepower-chassis /security/trustpoint # setcertchain [certchain]
```

명령에 인증서 정보를 지정하지 않은 경우, 루트 CA(인증 기관)에 인증 경로를 정의하는 트러스트 포인트 목록 또는 인증서를 입력하라는 프롬프트가 표시됩니다. 해당 정보를 입력한 후 다음 행에 ENDOFBUF를 입력하여 완료합니다.

**중요** 인증서는 Base64 인코딩 X.509(CER) 형식이어야 합니다.

단계 4 트랜잭션을 커밋합니다.

```
Firepower-chassis /security/trustpoint # commit-buffer
```

다음 예에서는 트러스트 포인트를 생성하고 트러스트 포인트에 대한 인증서를 제공합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # create trustpoint tPoint10
Firepower-chassis /security/trustpoint* # set certchain
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Trustpoint Certificate Chain:
> -----BEGIN CERTIFICATE-----
> MIIDMCCApmgAwIBAgIBADANBgkqhkiG9w0BAQQFADB0MQswCQYDVQQGEwJVUzEL
> BxMMU2FuIEpvc2UsIENENMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBASt
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCCyU
> ZgAMivyCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bf5wZVNAGMBAAGGJTAjBgkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG1CaJoJaVMhzC190306Mg51zq1zXcz75+VFj2I6rH9asckClD3mkOVx5gJU
> Ptt5CVQpNgNldvbDPSSxretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
> jtcEMyZ+f7+3yh421ido3n04MIgeBgNVHSMegZYwgZOAFLLNjtcEMyZ+f7+3yh42
> 1ido3n04oXikdJB0MQswCQYDVQQGEwJVUzELMAkGA1UECBMCQ0EwFDASBgNVBAcT
> ClNhbnRhIENsYXhMRswGQYDVQQKEwJodW92YSBTeXN0ZW1zIEluYy4xFDASBgNV
> BAsTC0VuZ2luZWVyaW5nMQswCQYDVQQDEwZ0ZXN0Q0GCAQAwDAYDVR0TBAUwAwEB
> /zANBgkqhkiG9w0BAQQFAAOBgQAhWaRwXNR6B4g6Lsnr+fptHv+WVhB5fKqGQgXc
> wR4pYiO4z42/j9Ijenh75tCKMhW51az8cop1EBmOcyuhf5C6vasrenn1ddkkYt4
> PR0vxGc40whuiozBolesmsmjBbedUCwQgdFDWhDIzJwK5+N3x/kfa2EHU6id1avt
> 4YL5Jg==
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/trustpoint* # commit-buffer
Firepower-chassis /security/trustpoint #
```

## 다음에 할 작업

트러스트 앵커 또는 인증 기관에서 키 링 인증서를 받고 키 링으로 가져옵니다.

# 키 링에 인증서 가져오기

## 시작하기 전에

- 키 링 인증서에 대한 인증서 체인을 포함하는 트러스트 포인트를 구성합니다.
- 트러스트 앵커 또는 인증 기관에서 키 링 인증서를 얻습니다.

## 절차

단계 1 보안 모드를 시작합니다.

```
Firepower-chassis #scope security
```

단계 2 인증서를 받을 키 링의 컨피그레이션 모드를 시작합니다.

```
Firepower-chassis /security # scopekeyring keyring-name
```

단계 3 키 링 인증서를 얻은 트러스트 앵커 또는 인증 기관에 대해 트러스트 포인트를 지정합니다.

```
Firepower-chassis /security/keyring # settrustpoint name
```

단계 4 키 링 인증서를 입력하고 업로드하기 위해 대화 상자를 실행합니다.

```
Firepower-chassis /security/keyring # setcert
```

프롬프트에서 트러스트 앵커 또는 인증 기관에서 받은 인증서 텍스트를 붙여넣습니다. 인증서의 다음 행에 ENDOFBUF를 입력하여 인증서 입력을 완료합니다.

**중요** 인증서는 Base64 인코딩 X.509(CER) 형식이어야 합니다.

단계 5 트랜잭션을 커밋합니다.

```
Firepower-chassis /security/keyring # commit-buffer
```

다음 예에서는 트러스트 포인트를 지정하고 키 링에 인증서를 가져옵니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # scope keyring kr220
Firepower-chassis /security/keyring # set trustpoint tPoint10
Firepower-chassis /security/keyring* # set cert
Enter lines one at a time. Enter ENDOFBUF to finish. Press ^C to abort.
Keyring certificate:
> -----BEGIN CERTIFICATE-----
> MIIB/zCCAwwCAQAwgZkxkCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTEVMBMGAA1UE
> BxMMU2FuIEpvc2UsIENMRUwEwYDVQQKEwxFeGFtcGx1IEluYy4xEzARBgNVBASt
> ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
> 9w0BCQEWZHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
> AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
> ZgAMivYCsKgb/6CjQtsofvtrmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
> GMbkPayV1QjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAGMBAAGgJTAjbGkq
> hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
> gYEAG61CaJoJaVMhzC1903O6Mg51zq1zXcz75+VFj2I6rH9asckC1d3mkOVx5gJU
```

```
> Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtv1WvfhevskV0j6
> mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
> -----END CERTIFICATE-----
> ENDOFBUF
Firepower-chassis /security/keyring* # commit-buffer
Firepower-chassis /security/keyring #
```

### 다음에 할 작업

HTTPS 서비스를 키 링으로 구성합니다.

## HTTPS 구성



주의

HTTPS에서 사용하는 포트 및 키 링 변경을 포함하여 HTTPS 컨피그레이션을 완료한 후 트랜잭션을 저장하거나 커밋하자마자 모든 현재 HTTP 및 HTTPS 세션이 종료됩니다.

### 절차

- 단계 1 시스템 모드를 시작합니다.  
Firepower-chassis# **scope system**
- 단계 2 시스템 서비스 모드를 시작합니다.  
Firepower-chassis /system # **scope services**
- 단계 3 HTTPS 서비스를 활성화합니다.  
Firepower-chassis /system/services # **enable https**
- 단계 4 (선택 사항) HTTPS 연결에 사용할 포트를 지정합니다.  
Firepower-chassis /system/services # **set https port *port-num***
- 단계 5 (선택 사항) HTTPS용으로 생성한 키 링의 이름을 지정합니다.  
Firepower-chassis /system/services # **set https keyring *keyring-name***
- 단계 6 (선택 사항) 도메인에서 사용하는 암호 그룹의 보안 레벨을 지정합니다.  
Firepower-chassis /system/services # **set https cipher-suite-mode *cipher-suite-mode***  
*cipher-suite-mode*는 다음 키워드 중 하나가 될 수 있습니다.
  - **high-strength**
  - **medium-strength**
  - **low-strength**
  - **custom**— 사용자 정의 암호 그룹 사양 문자열을 지정할 수 있습니다.
- 단계 7 (선택 사항) **cipher-suite-mode**가 **custom**으로 설정된 경우, 도메인에 대해 암호 그룹 보안의 맞춤형 레벨을 지정합니다.  
Firepower-chassis /system/services # **set https cipher-suite *cipher-suite-spec-string***

`cipher-suite-spec-string`은 최대 256자를 포함할 수 있으며 OpenSSL 암호 그룹 사양을 준수해야 합니다. 공백 또는 특수 문자를 사용할 수 없습니다. 단, !(느낌표), +(덧셈 기호), -(하이픈), :(콜론)은 사용할 수 있습니다. 자세한 내용은 [http://httpd.apache.org/docs/2.0/mod/mod\\_ssl.html#sslcipher-suite](http://httpd.apache.org/docs/2.0/mod/mod_ssl.html#sslcipher-suite)를 참조하십시오.

예를 들어 FXOS에서 기본값으로 사용하는 중간 강도 사양 문자열은 다음과 같습니다.  
`ALL:!ADH:!EXPORT56:!LOW:RC4+RSA:+HIGH:+MEDIUM:+EXP:+eNULL`

**참고** 이 옵션은 `cipher-suite-mode`가 `custom`이 아닌 값으로 설정된 경우 무시됩니다.

**단계 8** (선택 사항) 인증서 해지 목록 확인을 활성화하거나 비활성화합니다.

```
setrevoke-policy { relaxed | strict }
```

**단계 9** 시스템 컨피그레이션에 트랜잭션을 커밋합니다.

```
Firepower-chassis /system/services # commit-buffer
```

다음 예에서는 HTTPS를 활성화하고, 포트 번호를 443으로 설정한 다음, 키 링 이름 `kring7984`로 설정하고, 암호 그룹 보안 레벨을 `High`(높음)으로 설정한 후, 트랜잭션을 커밋합니다.

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # enable https
Firepower-chassis /system/services* # set https port 443
Warning: When committed, this closes all the web sessions.
Firepower-chassis /system/services* # set https keyring kring7984
Firepower-chassis /system/services* # set https cipher-suite-mode high
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

## HTTPS 포트 변경

HTTPS 서비스는 기본적으로 포트 443에서 활성화되어 있습니다. HTTPS는 비활성화할 수 없지만 HTTPS 연결에 사용할 포트는 변경할 수 있습니다.

### 절차

**단계 1** **Platform Settings**(플랫폼 설정) > **HTTPS**를 선택합니다.

**단계 2** HTTPS 연결에 사용할 포트를 **Port**(포트) 필드에 입력합니다. 1~65535의 정수를 지정합니다. 이 서비스는 기본적으로 포트 443에서 활성화됩니다.

**단계 3** **Save**(저장)를 클릭합니다.

Firepower 새시는 HTTPS 포트가 지정된 상태로 구성됩니다.

HTTPS 포트를 변경한 후에는 현재의 모든 HTTPS 세션이 종료됩니다. 사용자는 다음과 같이 새 포트를 사용하여 Firepower Chassis Manager에 다시 로그인해야 합니다.

```
https://<chassis_mgmt_ip_address>:<chassis_mgmt_port>
```

이때 `<chassis_mgmt_ip_address>`는 사용자가 초기 컨피그레이션을 설정하는 동안 입력한 Firepower 새시의 IP 주소 또는 호스트 이름이며 `<chassis_mgmt_port>`는 방금 구성한 HTTPS 포트입니다.

## 키 링 삭제

### 절차

- 단계 1 보안 모드를 시작합니다.  
Firepower-chassis #**scope security**
- 단계 2 이름이 지정된 키 링을 삭제합니다.  
Firepower-chassis /security # **deletekeyring name**
- 단계 3 트랜잭션을 커밋합니다.  
Firepower-chassis /security # **commit-buffer**

다음 예에서는 키 링을 삭제합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # delete keyring key10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

## 트러스트 포인트 삭제

시작하기 전에

트러스트 포인트가 키 링에서 사용되지 않음을 확인합니다.

### 절차

- 단계 1 보안 모드를 시작합니다.  
Firepower-chassis# **scopesecurity**
- 단계 2 이름이 지정된 트러스트 포인트를 삭제합니다.  
Firepower-chassis /security # **deletetrustpoint name**
- 단계 3 트랜잭션을 커밋합니다.  
Firepower-chassis /security # **commit-buffer**

다음 예에서는 트러스트 포인트를 삭제합니다.

```
Firepower-chassis# scope security
Firepower-chassis /security # delete trustpoint tPoint10
Firepower-chassis /security* # commit-buffer
Firepower-chassis /security #
```

## HTTPS 비활성화

### 절차

- 
- 단계 1 시스템 모드를 시작합니다.  
Firepower-chassis# **scope system**
- 단계 2 시스템 서비스 모드를 시작합니다.  
Firepower-chassis /system # **scope services**
- 단계 3 HTTPS 서비스를 비활성화합니다.  
Firepower-chassis /system/services # **disable https**
- 단계 4 시스템 컨피그레이션에 트랜잭션을 커밋합니다.  
Firepower-chassis /system/services # **commit-buffer**
- 

다음 예에서는 HTTPS를 비활성화하고 트랜잭션을 커밋합니다.

```
Firepower-chassis# scope system
Firepower-chassis /system # scope services
Firepower-chassis /system/services # disable https
Firepower-chassis /system/services* # commit-buffer
Firepower-chassis /system/services #
```

## AAA 구성

이 섹션에서는 인증, 권한 부여 및 어카운팅에 대해 설명합니다. 자세한 내용은 다음 항목을 참고하십시오.

## AAA 정보

AAA는 컴퓨터 리소스에 대한 액세스 제어를 위한 서비스의 집합으로, 정책을 시행하고 사용량을 평가하며 서비스에 대한 청구에 필요한 정보를 제공합니다. 이 과정은 효과적인 네트워크 관리 및 보안을 위해 중요한 부분으로 간주됩니다.

### 인증

인증은 액세스를 부여하기 전에 보통 사용자 이름과 비밀번호를 입력하도록 요구하는 방식으로 효과적인 사용자 확인 방법을 제공합니다. AAA 서버는 사용자의 인증 자격 증명을 데이터베이스에 저장된 다른 사용자의 자격 증명과 비교합니다. 자격 증명이 일치하면 사용자는 네트워크에 액세스할 수 있습니다. 자격 증명이 일치하지 않으면, 인증에 실패하고 네트워크 액세스가 거부됩니다.

다음 세션을 포함하는 새시에 대한 관리 연결을 인증하도록 Firepower 4100/9300 새시를 구성할 수 있습니다.

- HTTPS

- SSH
- 시리얼 콘솔

#### 권한 부여

권한 부여는 정책을 구현하는 프로세스로 사용자의 액세스가 허용된 활동, 리소스 또는 서비스 유형을 판단하는 것입니다. 사용자가 인증되면 해당 사용자는 다양한 액세스 또는 활동 유형에 대한 허가를 받을 수 있습니다.

#### 어카운팅

어카운팅은 사용자가 액세스 중 소비하는 리소스를 측정합니다. 여기에는 시스템 사용 시간, 사용자가 세션 중 보내거나 받는 데이터의 양 등이 포함됩니다. 어카운팅은 세션 통계 및 사용량 정보 기록을 통해 이루어지며 이는 권한 부여 제어, 청구, 경향 분석, 리소스 활용도 및 용량 계획 활동에 사용됩니다.

#### 인증, 권한 부여, 어카운팅 간 상호 작용

인증을 단독으로 사용하거나 권한 부여 및 어카운팅과 함께 사용할 수 있습니다. 권한 부여에서는 항상 사용자를 먼저 인증해야 합니다. 어카운팅을 단독으로 사용하거나 인증 및 권한 부여와 함께 사용할 수 있습니다.

#### AAA 서버

AAA 서버는 액세스 제어를 위해 사용되는 네트워크 서버입니다. 인증은 사용자를 식별합니다. 권한 부여는 인증된 사용자가 액세스할 수 있는 리소스와 서비스를 결정하는 정책을 구현합니다. 어카운팅은 청구 및 분석을 위해 사용되는 시간과 데이터를 추적합니다.

#### 로컬 데이터베이스 지원

Firepower 새시에서는 사용자 프로필로 채울 수 있는 로컬 데이터베이스를 유지 관리합니다. AAA 서버 대신 로컬 데이터베이스를 사용하여 사용자 인증, 권한 부여 및 어카운팅을 제공할 수 있습니다.

## LDAP 제공자 구성

### LDAP 제공자 속성 구성

이 작업에서 구성하는 속성은 이 유형의 모든 제공자 연결에 대한 기본 설정입니다. 개별 제공자에 이러한 속성의 설정이 포함되어 있는 경우에는 Firepower eXtensible 운영 체제에서 해당 설정을 사용하고 기본 설정을 무시합니다.

Active Directory를 LDAP 서버로 사용하는 경우에는 Active Directory 서버에서 사용자 계정을 생성하여 Firepower eXtensible 운영 체제와 바인딩합니다. 이 어카운트에는 만료되지 않는 비밀번호가 제공되어야 합니다.

## 절차

단계 1 **Platform Settings**(플랫폼 설정) > **AAA**를 선택합니다.

단계 2 **LDAP** 탭을 클릭합니다.

단계 3 **Properties**(속성) 영역에서 다음 필드를 입력합니다.

| Name                      | 설명                                                                                                                                                                                                                                                                                            |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Timeout</b> (시간 제한) 필드 | 시간이 초과되기 전에 시스템이 LDAP 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다.<br><br>1~60초의 정수를 입력합니다. 기본값은 30초입니다. 이 속성은 필수입니다.                                                                                                                                                                                  |
| <b>Attribute</b> (특성) 필드  | 사용자 역할 및 로케일에 대한 값을 저장하는 LDAP 특성입니다. 이 속성은 항상 이름값 쌍입니다. 시스템은 이 특성 이름과 일치하는 값에 대해 사용자 레코드를 쿼리합니다.                                                                                                                                                                                              |
| <b>Base DN</b> (기본 DN) 필드 | 원격 사용자가 로그인하고 시스템에서 사용자 이름에 기초한 사용자 DN을 얻으려고 시도할 때 서버에서 검색을 시작해야 하는 LDAP 계층 구조에서 특정한 고유 이름입니다. 기본 DN 길이는 최대 255자에서 CN=\$userid 길이를 뺀 값으로 설정할 수 있습니다. 여기서 \$userid는 LDAP 인증을 사용하여 Firepower 새시에 액세스하려는 원격 사용자를 나타냅니다.<br><br>이 속성은 필수입니다. 이 탭에서 기본 DN을 지정하지 않으면 정의하는 각 LDAP 제공자에 하나씩 지정해야 합니다. |
| <b>Filter</b> (필터) 필드     | LDAP 검색은 정의된 필터와 일치하는 사용자 이름으로 제한됩니다.<br><br>이 속성은 필수입니다. 이 탭에서 필터를 지정하지 않으면 정의하는 각 LDAP 제공자에 하나씩 지정해야 합니다.                                                                                                                                                                                   |

단계 4 **Save**(저장)를 클릭합니다.

### 다음에 할 작업

LDAP 제공자를 생성합니다.

## LDAP 제공자 생성

Firepower eXtensible 운영 체제에서는 최대 16개의 LDAP 제공자를 지원합니다.



시작하기 전에

Active Directory를 LDAP 서버로 사용하는 경우에는 Active Directory 서버에서 사용자 계정을 생성하여 Firepower eXtensible 운영 체제와 바인딩합니다. 이 어카운트에는 만료되지 않는 비밀번호가 제공되어야 합니다.

**절차**

단계 1 Platform Settings(플랫폼 설정) > AAA를 선택합니다.

단계 2 LDAP 탭을 클릭합니다.

단계 3 추가할 각 LDAP 제공자에 대해 다음을 수행합니다.

- a) LDAP Providers(LDAP 제공자) 영역에서 Add(추가)를 클릭합니다.
- b) Add LDAP Provider(LDAP 제공자 추가) 대화 상자에서 다음 필드를 작성합니다.

| Name                                                    | 설명                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Hostname/FDQN (or IP Address)(호스트 이름/FDQN(또는 IP 주소)) 필드 | LDAP 제공자가 있는 호스트 이름 또는 IP 주소입니다. SSL을 활성화한 경우, 이 필드는 LDAP 데이터베이스의 보안 인증서에 있는 CN(일반 이름)과 정확하게 일치해야 합니다.                                                                                                                                                                                          |
| Order(순서) 필드                                            | Firepower eXtensible 운영 체제에서 사용자를 인증하기 위해 이 제공자를 사용하는 순서입니다.<br><br>Firepower eXtensible 운영 체제에서 Firepower Chassis Manager 또는 FXOS CLI에 정의되어 있는 다른 제공자에 기반하여 다음으로 사용 가능한 순서를 할당하려면 1~16의 정수를 입력하거나 lowest-available 또는 0(숫자 0)을 입력합니다.                                                          |
| Bind DN(바인드 DN) 필드                                      | 기본 DN에 속하는 모든 객체에 대한 읽기 및 검색 권한이 있는 LDAP 데이터베이스 어카운트의 DN(고유 이름)입니다.<br><br>지원되는 최대 문자열 길이는 ASCII 255자입니다.                                                                                                                                                                                       |
| Base DN(기본 DN) 필드                                       | 원격 사용자가 로그인하고 시스템에서 사용자 이름에 기초한 사용자 DN을 얻으려고 시도할 때 서버에서 검색을 시작해야 하는 LDAP 계층 구조에서 특정한 고유 이름입니다. 기본 DN 길이는 최대 255자에서 CN=\$userid 길이를 뺀 값으로 설정할 수 있습니다. 여기서 \$userid는 LDAP 인증을 사용하여 Firepower Chassis Manager 또는 FXOS CLI에 액세스하려는 원격 사용자를 나타냅니다.<br><br>이 값은 기본 DN의 기본값이 LDAP 탭에 설정되지 않은 경우 필요합니다. |
| Port(포트) 필드                                             | Firepower Chassis Manager 또는 FXOS CLI에서 LDAP 데이터베이스와 통신할 때 사용하는 포트입니다. 표준 포트 번호는 389입니다.                                                                                                                                                                                                        |

| Name                           | 설명                                                                                                                                                                                                                                                                                                         |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Enable SSL(SSL 활성화) 확인란</b> | <p>이 확인란을 선택한 경우, LDAP 데이터베이스와의 통신에 암호화가 필요합니다. 이 확인란이 선택되지 않은 경우, 인증 정보는 암호화되지 않은 텍스트로 전송됩니다.</p> <p>LDAP은 STARTTLS를 사용합니다. 이는 포트 389를 사용하여 암호화된 통신을 허용합니다.</p>                                                                                                                                           |
| <b>Filter(필터) 필드</b>           | <p>LDAP 검색은 정의된 필터와 일치하는 사용자 이름으로 제한됩니다.</p> <p>이 값은 기본 필터가 LDAP 탭에 설정되지 않은 경우 필요합니다.</p>                                                                                                                                                                                                                  |
| <b>Attribute(특성) 필드</b>        | <p>사용자 역할 및 로케일에 대한 값을 저장하는 LDAP 특성입니다. 이 속성은 항상 이름값 쌍입니다. 시스템은 이 특성 이름과 일치하는 값에 대해 사용자 레코드를 쿼리합니다.</p> <p>이 값은 기본 특성이 LDAP 탭에 설정되지 않은 경우 필요합니다.</p>                                                                                                                                                       |
| <b>Key(키) 필드</b>               | <p><b>Bind DN(바인드 DN)</b> 필드에 지정된 LDAP 데이터베이스 계정의 비밀번호. 공백, \$(섹션 기호), ?(물음표) 또는 =(등호)를 제외한 모든 표준 ASCII 문자를 입력할 수 있습니다.</p>                                                                                                                                                                                |
| <b>Confirm Key(키 확인) 필드</b>    | <p>확인을 위해 반복되는 LDAP 데이터베이스 비밀번호입니다.</p>                                                                                                                                                                                                                                                                    |
| <b>Timeout(시간 제한) 필드</b>       | <p>시간이 초과되기 전에 시스템이 LDAP 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다.</p> <p>1~60초의 정수를 입력하거나 0(숫자 0)을 입력하여 LDAP 탭에 지정된 전역 시간제한 값을 사용합니다. 기본값은 30초입니다.</p>                                                                                                                                                          |
| <b>Vendor(벤더) 필드</b>           | <p>이 선택사항으로 LDAP 제공자 또는 서버 상세 정보를 제공하는 벤더를 식별합니다.</p> <ul style="list-style-type: none"> <li>• LDAP 제공자가 Microsoft Active Directory인 경우 <b>MS-AD</b>를 선택합니다.</li> <li>• LDAP 제공자가 Microsoft Active Directory가 아닌 경우 <b>Open LDAP(LDAP 열기)</b>을 선택합니다.</li> </ul> <p>기본값은 <b>Open LDAP(LDAP 열기)</b>입니다.</p> |

c) **OK(확인)**를 클릭하여 **Add LDAP Provider(LDAP 제공자 추가)** 대화 상자를 닫습니다.

단계 4 **Save(저장)**를 클릭합니다.

단계 5 (선택 사항) 인증 해지 목록 확인을 활성화합니다.

```
Firepower-chassis /security/ldap/server # set revoke-policy {strict | relaxed}
```

**참고** 이 컨피그레이션은 SSL 연결을 활성화한 경우에만 적용됩니다.

## LDAP 제공자 삭제

### 절차

단계 1 **Platform Settings(플랫폼 설정) > AAA**를 선택합니다.

단계 2 **LDAP** 탭을 클릭합니다.

단계 3 **LDAP Providers(LDAP 제공자)** 영역에서 삭제할 LDAP 제공자에 해당하는 테이블의 행에 있는 **Delete(삭제)** 아이콘을 클릭합니다.

## RADIUS 제공자 구성

### RADIUS 제공자 속성 구성

이 작업에서 구성하는 속성은 이 유형의 모든 제공자 연결에 대한 기본 설정입니다. 개별 제공자에 이러한 속성의 설정이 포함되어 있는 경우에는 Firepower eXtensible 운영 체제에서 해당 설정을 사용하고 기본 설정을 무시합니다.

### 절차

단계 1 **Platform Settings(플랫폼 설정) > AAA**를 선택합니다.

단계 2 **RADIUS** 탭을 클릭합니다.

단계 3 **Properties(속성)** 영역에서 다음 필드를 입력합니다.

| Name                     | 설명                                                                                                           |
|--------------------------|--------------------------------------------------------------------------------------------------------------|
| <b>Timeout(시간 제한) 필드</b> | 시간 제한이 초과되기 전에 시스템이 RADIUS 데이터베이스에 연결을 시도하는 데 필요한 시간(초)입니다.<br>1~60초의 정수를 입력합니다. 기본값은 5초입니다.<br>이 속성은 필수입니다. |

| Name               | 설명                                  |
|--------------------|-------------------------------------|
| Retries(재시도 횟수) 필드 | 요청에 실패한 것으로 간주하기 전에 연결을 재시도할 횟수입니다. |

단계 4 **Save(저장)**를 클릭합니다.

### 다음에 할 작업

RADIUS 제공자를 생성합니다.

## RADIUS 제공자 생성

Firepower eXtensible 운영 체제는 최대 16개의 RADIUS 제공자를 지원합니다.

### 절차

단계 1 **Platform Settings(플랫폼 설정)** > **AAA**를 선택합니다.

단계 2 **RADIUS** 탭을 클릭합니다.

단계 3 추가할 각 RADIUS 제공자에 대해 다음을 수행합니다.

- RADIUS Providers(RADIUS 제공자)** 영역에서 **Add(추가)**를 클릭합니다.
- Add RADIUS Provider(RADIUS 제공자 추가)** 대화 상자에서 다음 필드를 입력합니다.

| Name                                                           | 설명                                                                                                                                                                                                                                     |
|----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hostname/FDQN (or IP Address)(호스트 이름/FDQN(또는 IP 주소))</b> 필드 | RADIUS 제공자가 있는 호스트 이름 또는 IP 주소입니다.                                                                                                                                                                                                     |
| <b>Order(순서)</b> 필드                                            | Firepower eXtensible 운영 체제에서 사용자를 인증하기 위해 이 제공자를 사용하는 순서입니다.<br><br>Firepower eXtensible 운영 체제에서 Firepower Chassis Manager 또는 FXOS CLI에 정의되어 있는 다른 제공자에 기반하여 다음으로 사용 가능한 순서를 할당하려면 1~16의 정수를 입력하거나 lowest-available 또는 0(숫자 0)을 입력합니다. |
| <b>Key(키)</b> 필드                                               | 데이터베이스에 대한 SSL 암호화 키입니다.                                                                                                                                                                                                               |
| <b>Confirm Key(키 확인)</b> 필드                                    | 확인을 위해 다시 한 번 입력하는 SSL 암호화 키입니다.                                                                                                                                                                                                       |

| Name                                    | 설명                                                                                                                                                |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Authorization Port</b> (권한 부여 포트) 필드 | Firepower Chassis Manager 또는 FXOS CLI에서 RADIUS 데이터베이스와 통신할 때 사용하는 포트입니다. 유효한 범위는 1~65535입니다. 표준 포트 번호는 1700입니다.                                   |
| <b>Timeout</b> (시간 제한) 필드               | 시간 제한이 초과되기 전에 시스템이 RADIUS 데이터베이스에 연결을 시도하는 데 필요한 시간(초)입니다.<br>1~60초의 정수를 입력하거나 0(숫자 0)을 입력하여 <b>RADIUS</b> 탭에 지정된 전역 시간 제한 값을 사용합니다. 기본값은 5초입니다. |
| <b>Retries</b> (재시도 횟수) 필드              | 요청에 실패한 것으로 간주하기 전에 연결을 재시도할 횟수입니다.<br>원하는 경우 0~5의 정수를 입력합니다. 값을 지정하지 않은 경우, Firepower Chassis Manager에서는 <b>RADIUS</b> 탭에 지정된 값을 사용합니다.          |

c) **OK**(확인)를 클릭하여 **Add RADIUS Provider**(RADIUS 제공자 추가) 대화 상자를 닫습니다.

단계 4 **Save**(저장)를 클릭합니다.

## RADIUS 제공자 삭제

### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **AAA**를 선택합니다.

단계 2 **RADIUS** 탭을 클릭합니다.

단계 3 **RADIUS Providers**(RADIUS 제공자) 영역에서 삭제할 RADIUS 제공자에 해당하는 테이블의 행에 있는 **Delete**(삭제) 아이콘을 클릭합니다.

## TACACS+ 제공자 구성

### TACACS+ 제공자 속성 구성

이 작업에서 구성하는 속성은 이 유형의 모든 제공자 연결에 대한 기본 설정입니다. 개별 제공자에 이러한 속성의 설정이 포함되어 있는 경우에는 Firepower eXtensible 운영 체제에서 해당 설정을 사용하고 기본 설정을 무시합니다.

#### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **AAA**를 선택합니다.

단계 2 **TACACS** 탭을 클릭합니다.

단계 3 **Properties**(속성) 영역에서 다음 필드를 입력합니다.

| Name                      | 설명                                                                                                            |
|---------------------------|---------------------------------------------------------------------------------------------------------------|
| <b>Timeout</b> (시간 제한) 필드 | 시간이 초과되기 전에 시스템이 TACACS+ 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다.<br>1~60초의 정수를 입력합니다. 기본값은 5초입니다.<br>이 속성은 필수입니다. |

단계 4 **Save**(저장)를 클릭합니다.

#### 다음에 할 작업

TACACS+ 제공자를 만듭니다.

### TACACS+ 제공자 생성

Firepower eXtensible 운영 체제는 최대 16개의 TACACS+ 제공자를 지원합니다.

#### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **AAA**를 선택합니다.

단계 2 **TACACS** 탭을 클릭합니다.

단계 3 추가할 각 TACACS+ 제공자에 대해 다음을 수행합니다.

- a) **TACACS Providers**(TACACS 제공자) 영역에서 **Add**(추가)를 클릭합니다.
- b) **Add TACACS Provider**(TACACS 제공자 추가) 대화 상자에서 다음 필드를 입력합니다.

| Name                                                            | 설명                                                                                                                                                                                                                                     |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Hostname/FDQN (or IP Address)</b> (호스트 이름/FDQN(또는 IP 주소)) 필드 | TACACS+ 제공자가 있는 호스트 이름 또는 IP 주소입니다.                                                                                                                                                                                                    |
| <b>Order</b> (순서) 필드                                            | Firepower eXtensible 운영 체제에서 사용자를 인증하기 위해 이 제공자를 사용하는 순서입니다.<br><br>Firepower eXtensible 운영 체제에서 Firepower Chassis Manager 또는 FXOS CLI에 정의되어 있는 다른 제공자에 기반하여 다음으로 사용 가능한 순서를 할당하려면 1~16의 정수를 입력하거나 lowest-available 또는 0(숫자 0)을 입력합니다. |
| <b>Key</b> (키) 필드                                               | 데이터베이스에 대한 SSL 암호화 키입니다.                                                                                                                                                                                                               |
| <b>Confirm Key</b> (키 확인) 필드                                    | 확인을 위해 다시 한 번 입력하는 SSL 암호화 키입니다.                                                                                                                                                                                                       |
| <b>Port</b> (포트) 필드                                             | Firepower Chassis Manager 또는 FXOS CLI에서 TACACS+ 데이터베이스와 통신할 때 사용하는 포트입니다.<br><br>1~65535의 정수를 입력합니다. 기본 포트는 49입니다.                                                                                                                     |
| <b>Timeout</b> (시간 제한) 필드                                       | 시간이 초과되기 전에 시스템이 TACACS+ 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다.<br><br>1~60초의 정수를 입력하거나 0(숫자 0)을 입력하여 TACACS+ 탭에 지정된 전역 시간 제한 값을 사용합니다. 기본값은 5초입니다.                                                                                       |

c) **OK**(확인)를 클릭하여 **Add TACACS Provider**(TACACS 제공자 추가) 대화 상자를 닫습니다.

단계 4 **Save**(저장)를 클릭합니다.

## TACACS+ 제공자 삭제

### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **AAA**를 선택합니다.

단계 2 **TACACS** 탭을 클릭합니다.

단계 3 **TACACS Providers**(TACACS 제공자) 영역에서 삭제할 TACACS+ 제공자에 해당하는 테이블의 행에 있는 **Delete**(삭제) 아이콘을 클릭합니다.

## Syslog 구성

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 기록하면 로그와 알람을 집계하는 데 도움이 됩니다. syslog 서비스는 메시지를 수신하고 파일로 저장하거나 간단한 컨피그레이션 파일에 따라 인쇄합니다. 이 로깅 양식을 통해 로그를 안전하게 장기 보관할 수 있습니다. 로그는 일상적인 문제 해결과 사고 처리에 모두 유용합니다.

### 절차

단계 1 **Platform Settings**(플랫폼 설정) > **Syslog**를 선택합니다.

단계 2 로컬 대상을 구성합니다.

- a) **Local Destinations**(로컬 대상) 탭을 클릭합니다.
- b) **Local Destinations**(로컬 대상) 탭에서 다음 필드를 입력합니다.

| Name                          | 설명                                                                                                                                                                                                                                                                    |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Console</b> (콘솔) 섹션        |                                                                                                                                                                                                                                                                       |
| <b>Admin State</b> (관리 상태) 필드 | Firepower 새시에서 콘솔에 syslog 메시지가 표시되도록 할지 선택합니다.<br><br>콘솔에 syslog 메시지를 표시하고 로그에 추가하려는 경우 <b>Enable</b> (활성화) 확인란을 선택합니다. <b>Enable</b> (활성화) 확인란을 선택하지 않은 경우, syslog 메시지는 로그에 추가되지만 콘솔에 표시되지 않습니다.                                                                     |
| <b>Level</b> (레벨) 필드          | <b>Console - Admin State</b> (콘솔 - 관리 상태)의 <b>Enable</b> (활성화) 확인란을 선택한 경우, 콘솔에 표시할 가장 낮은 메시지 레벨을 선택합니다. Firepower 새시에서 콘솔에 해당 레벨 이상의 메시지가 표시됩니다. 다음 중 하나일 수 있습니다. <ul style="list-style-type: none"> <li>• 긴급 상황</li> <li>• 경고</li> <li>• <b>Critical</b></li> </ul> |
| <b>Monitor</b> (모니터) 섹션       |                                                                                                                                                                                                                                                                       |



| Name                         | 설명                                                                                                                                                                                                                                                                                                                                                               |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Admin State(관리 상태) 필드</b> | Firepower 새시에서 모니터에 syslog 메시지가 표시되도록 할지 선택합니다.<br><br>모니터에 syslog 메시지를 표시하고 로그에 추가하려는 경우 <b>Enable(활성화)</b> 확인란을 선택합니다. <b>Enable(활성화)</b> 확인란을 선택하지 않은 경우, syslog 메시지는 로그에 추가되지만 모니터에 표시되지 않습니다.                                                                                                                                                               |
| <b>Level(수준) 드롭다운 목록</b>     | <b>Monitor - Admin State(모니터 - 관리 상태)의 Enable(활성화)</b> 확인란을 선택한 경우, 모니터에 표시할 가장 낮은 메시지 레벨을 선택합니다. 모니터에 해당 레벨 이상의 메시지가 표시됩니다. 다음 중 하나일 수 있습니다. <ul style="list-style-type: none"> <li>• 긴급 상황</li> <li>• 경고</li> <li>• <b>Critical</b></li> <li>• 오류</li> <li>• 경고(들)</li> <li>• <b>Notifications(알림)</b></li> <li>• <b>Information</b></li> <li>• 디버깅</li> </ul> |

c) **Save(저장)**를 클릭합니다.

**단계 3** 원격 대상을 구성합니다.

- a) **Remote Destination(원격 대상)** 탭을 클릭합니다.
- b) **Remote Destination(원격 대상)** 탭에서 Firepower 새시에서 생성된 메시지를 저장할 수 있는 최대 3개의 외부 로그에 대해 다음 필드를 입력합니다.  
 원격 대상에 syslog 메시지를 전송하여 외부 syslog 서버의 사용 가능한 디스크 공간에 따라 메시지를 아카이브할 수 있으며, 저장된 기록 데이터를 조작할 수 있습니다. 예를 들어 특정 유형의 syslog 메시지가 기록될 때 실행할 작업을 지정하고, 로그에서 데이터를 추출하고 보고를 위해 기록을 다른 파일에 저장하거나, 사이트별 스크립트를 사용하여 통계를 추적할 수 있습니다.

| Name                         | 설명                                                            |
|------------------------------|---------------------------------------------------------------|
| <b>Admin State(관리 상태) 필드</b> | 원격 로그 파일에 syslog 메시지를 저장하려는 경우 <b>Enable(활성화)</b> 확인란을 선택합니다. |

| Name                                        | 설명                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Level(수준)</b> 드롭다운 목록                    | <p>시스템에서 저장하도록 할 가장 낮은 메시지 레벨을 선택합니다. 시스템에서는 원격 파일에 해당 레벨 이상의 메시지를 저장합니다. 다음 중 하나일 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 긴급 상황</li> <li>• 경고</li> <li>• <b>Critical</b></li> <li>• 오류</li> <li>• 경고(들)</li> <li>• <b>Notifications(알림)</b></li> <li>• <b>Information</b></li> <li>• 디버깅</li> </ul>      |
| <b>Hostname/IP Address(호스트 이름/IP 주소)</b> 필드 | <p>원격 로그 파일이 있는 호스트 이름 또는 IP 주소입니다.</p> <p><b>참고</b> IP 주소 대신 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.</p>                                                                                                                                                                                                                    |
| <b>Facility(기능)</b> 드롭다운 목록                 | <p>파일 메시지의 기반으로 사용할 syslog 서버에 대한 시스템 로그를 선택합니다. 다음 중 하나일 수 있습니다.</p> <ul style="list-style-type: none"> <li>• <b>Local0</b></li> <li>• <b>Local1</b></li> <li>• <b>Local2</b></li> <li>• <b>Local3</b></li> <li>• <b>Local4</b></li> <li>• <b>Local5</b></li> <li>• <b>Local6</b></li> <li>• <b>Local7</b></li> </ul> |

c) **Save(저장)**를 클릭합니다.

**단계 4** 로컬 소스를 구성합니다.

a) **Local Sources(로컬 소스)** 탭을 클릭합니다.

b) **Local Sources(로컬 소스)** 탭에서 다음 필드를 입력합니다.

| Name                                     | 설명                                                                                          |
|------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Faults Admin State</b> (결함 관리 상태) 필드  | 시스템 결함 기록을 활성화할지 선택합니다. <b>Enable</b> (활성화) 확인란을 선택한 경우, Firepower 새시에서 모든 시스템 결함이 기록됩니다.   |
| <b>Audits Admin State</b> (감사 관리 상태) 필드  | 감사 기록을 활성화할지 선택합니다. <b>Enable</b> (활성화) 확인란을 선택한 경우, Firepower 새시에서 모든 감사 로그 이벤트가 기록됩니다.    |
| <b>Events Admin State</b> (이벤트 관리 상태) 필드 | 시스템 이벤트 기록을 활성화할지 선택합니다. <b>Enable</b> (활성화) 확인란을 선택한 경우, Firepower 새시에서 모든 시스템 이벤트가 기록됩니다. |

c) **Save**(저장)를 클릭합니다.

## DNS 서버 구성

시스템에서 호스트 이름-IP 주소를 확인해야 하는 경우 DNS 서버를 지정해야 합니다. 예를 들어 DNS 서버를 구성하지 않으면 Firepower 새시에서 설정을 구성할 때 `www.cisco.com` 등의 이름을 사용할 수 없습니다. 서버의 IP 주소(IPv4 또는 IPv6 주소 중 하나가 될 수 있음)를 사용해야 합니다. 최대 4개까지 DNS 서버를 구성할 수 있습니다.



**참고** 여러 DNS 서버를 구성할 때 시스템에서는 임의의 순서로 서버만 검색합니다. 로컬 관리 명령에 DNS 서버 조회가 필요한 경우, 임의의 순서로 3개의 DNS 서버만 검색할 수 있습니다.

### 절차

- 단계 1 **Platform Settings**(플랫폼 설정) > **DNS**를 선택합니다.
- 단계 2 **Enable DNS Server**(DNS 서버 활성화) 확인란을 선택합니다.
- 단계 3 추가할 각 DNS 서버(최대 4개)에 대해 **DNS Server**(DNS 서버) 필드에 DNS 서버의 IP 주소를 입력하고 **Add**(추가)를 클릭합니다.
- 단계 4 **Save**(저장)를 클릭합니다.





# 9 장

## 인터페이스 관리

- [Firepower Security Appliance 인터페이스 정보, 123페이지](#)
- [인터페이스 속성 편집, 126페이지](#)
- [인터페이스의 관리 상태 변경, 127페이지](#)
- [포트 채널 생성, 127페이지](#)
- [브레이크아웃 케이블 구성, 129페이지](#)

## Firepower Security Appliance 인터페이스 정보

Firepower 4100/9300 새시는 단일 인터페이스뿐만 아니라 EtherChannel(포트 채널) 인터페이스도 지원됩니다. EtherChannel 인터페이스는 동일한 유형의 멤버 인터페이스를 최대 16개 포함할 수 있습니다.

### 인터페이스 페이지

Firepower Chassis Manager의 Interfaces(인터페이스) 페이지에서 새시에 설치된 인터페이스의 상태를 확인하고, 인터페이스 속성을 편집하며, 인터페이스를 활성화 또는 비활성화하고, 포트 채널을 생성할 수 있습니다.

Interfaces(인터페이스) 페이지는 다음의 두 가지 섹션으로 구성됩니다.

- 상위 섹션에는 Firepower 새시에 설치된 인터페이스가 시각적으로 표시됩니다. 인터페이스에 마우스를 올려놓으면 해당 인터페이스에 대한 자세한 정보를 얻을 수 있습니다.

인터페이스에서는 다음과 같은 색상 코드를 통해 현재 상태를 표시합니다.

- 녹색 — 인터페이스가 설치 및 활성화되어 있습니다.
- 어두운 회색 — 인터페이스가 설치되었지만 비활성화되어 있습니다.
- 빨간색 — 인터페이스의 작동 상태에 문제가 있습니다.

- 밝은 회색 — 인터페이스가 설치되지 않았습니다.



**참고** 포트 채널에서 포트 역할을 하는 인터페이스는 이 목록에 나타나지 않습니다.

- 하위 섹션에는 **All Interfaces**(모든 인터페이스) 및 하드웨어 우회의 두 가지 탭이 들어 있습니다. **All Interfaces**(모든 인터페이스) 탭에서 각 인터페이스를 활성화하거나 비활성화할 수 있습니다. 또한, **Edit**(편집)을 클릭하면 속도 및 인터페이스 유형 등 인터페이스 속성을 편집할 수 있습니다. 하드웨어 우회에 대해서는 [하드웨어 바이패스 쌍, 125 페이지](#)의 내용을 참조하십시오.



**참고** 포트 채널 48 클러스터 유형 인터페이스는 멤버 인터페이스를 포함하지 않은 경우 **Operation State**(작동 상태)를 **failed**(장애 발생)로 표시합니다. 새시 내 클러스터링의 경우 이 EtherChannel이 멤버 인터페이스를 필요로 하지 않으므로 이 작동 상태를 무시할 수 있습니다.

## 인터페이스 유형

각 인터페이스는 다음 유형 중 하나일 수 있습니다.

- **Data**(데이터)(기본값) -- 데이터 인터페이스는 논리적 디바이스 간에 공유할 수 없습니다.
- **Management**(관리) -- 관리 인터페이스는 논리적 디바이스 간에 공유할 수 있습니다. 논리적 디바이스당 관리 인터페이스 1개만 할당할 수 있습니다.

Firepower Threat Defense 애플리케이션 내에서 물리적 관리 인터페이스는 논리적 진단 인터페이스와 논리적 관리 인터페이스 간에 공유됩니다. 논리적 관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 Firepower Management Center에 설치하고 등록하는 데 사용됩니다. 또한, 별도의 SSH 서버를 실행하며 자체 로컬 인증, IP 주소 및 정적 라우팅을 사용합니다. CLI에서 **configure network** 명령을 사용하여 설정을 구성하고 Management Center**Devices**(디바이스) > **Device Management**(디바이스 관리) > **Devices**(디바이스) > **Management**(관리) 영역에서 IP 주소를 변경할 수 있습니다.

논리적 진단 인터페이스는 Management Center**Devices**(디바이스) > **Device Management**(디바이스 관리) > **Interfaces**(인터페이스) 화면에서 나머지 데이터 인터페이스와 함께 구성할 수 있습니다. 진단 인터페이스 사용은 선택 사항입니다. 진단 인터페이스 및 데이터 인터페이스는 LDAP 또는 RADIUS 외부 인증을 허용합니다. 예를 들어, 데이터 인터페이스에서 SSH 액세스를 허용하지 않으려면 SSH 액세스에 대해 진단 인터페이스를 구성할 수 있습니다. 진단 인터페이스는 관리 트래픽만 허용하며 통과 트래픽은 허용하지 않습니다.

- **Firepower-eventing**(Firepower 이벤트) -- 이 인터페이스는 Firepower Threat Defense 디바이스의 보조 관리 인터페이스입니다. 이 인터페이스를 사용하려면 Firepower Threat Defense CLI에서 해당 IP 주소 및 기타 파라미터를 구성해야 합니다. 예를 들어, 이벤트(예: 웹 이벤트)와 관리 트래픽을 구분할 수 있습니다. Firepower Management Center 명령 참조에서 **configure network** 명령을 참조하십시오.

- Cluster(클러스터) -- 클러스터형 논리적 디바이스에 사용되는 특수 인터페이스 유형입니다. 이 유형은 유닛 클러스터 간 통신을 지원하는 클러스터 제어 링크에 자동으로 할당됩니다. 기본적으로 클러스터 제어 링크는 포트 채널 48에서 자동으로 생성됩니다.



**참고** Firepower Management Center 또는 Firepower Threat Defense CLI를 사용하여 두 개의 업링크, 브레이크아웃 또는 데이터 포트 인터페이스를 인라인 쌍으로 구성할 수 있습니다. 두 개의 포트가 인라인 쌍으로 구성되면 하나의 단일한 인터페이스 역할을 수행합니다. 그런 다음 이 컨피그레이션이 FXOS 새시에 전파됩니다.

인라인 쌍에는 다음과 같은 제한 사항이 있습니다.

- 두 개의 포트 인터페이스는 고유해야 합니다. 포트는 하나의 인라인 쌍에 조인하면 다른 인라인 쌍에 조인할 수 없습니다.
- 업링크 포트, 데이터 포트 또는 브레이크아웃 포트만 인라인 쌍으로 구성할 수 있습니다.

자세한 내용은 Firepower Management Center 컨피그레이션 가이드에서 “IPS 전용 인터페이스의 인라인 집합 구성” 항목을 참조하십시오.

## 하드웨어 바이패스 쌍

Firepower Threat Defense의 경우, Firepower 9300 및 4100 Series에서 특정 인터페이스 모듈을 사용하면 하드웨어 우회 기능을 활성화할 수 있습니다. 하드웨어 우회는 정전 중에도 인라인 인터페이스 쌍 사이에서 트래픽이 계속 통과하게 해줍니다. 이 기능은 소프트웨어 또는 하드웨어 장애가 발생할 경우 네트워크 연결을 유지하는 데 사용될 수 있습니다.

하드웨어 우회 기능은 하드웨어 우회 애플리케이션 내에 구성됩니다. 이러한 인터페이스는 하드웨어 우회 쌍으로 사용할 필요가 없으며, ASA와 Firepower Threat Defense 애플리케이션 둘 다에 대해 일반 인터페이스로 사용할 수 있습니다. 하드웨어 우회 가능 인터페이스는 브레이크아웃 포트용으로 구성할 수 없습니다. 하드웨어 우회 기능을 사용하려는 경우, 포트를 EtherChannel로 구성하지 마십시오. 그렇지 않으면 이러한 인터페이스를 일반 인터페이스 모드에서 EtherChannel 멤버로 포함할 수 있습니다.

Firepower Threat Defense는 다음 모델에서 특정 네트워크 모듈의 인터페이스 쌍에 대해 하드웨어 우회를 지원합니다.

- Firepower 9300
- Firepower 4100 Series

이러한 모델에 대해 지원되는 하드웨어 우회 네트워크 모듈은 다음과 같습니다.

- Firepower 6포트 1G SX FTW 네트워크 모듈 싱글 와이드(FPR-NM-6X1SX-F)
- Firepower 6포트 10G SR FTW 네트워크 모듈 싱글 와이드(FPR-NM-6X10SR-F)
- Firepower 6포트 10G LR FTW 네트워크 모듈 싱글 와이드(FPR-NM-6X10LR-F)

- Firepower 2포트 40G SR FTW 네트워크 모듈 싱글 와이드(FPR-NM-2X40G-F)
- Firepower 8포트 1G 구리 FTW 네트워크 모듈 싱글 와이드(FPR-NM-8X1G-F)

하드웨어 우회에서는 다음 포트 쌍만 사용할 수 있습니다.

- 1 및 2
- 3 및 4
- 5 및 6
- 7 및 8

## 점보 프레임 지원

Firepower 4100/9300 새시는 기본적으로 활성화되어 있는 점보 프레임을 지원합니다. Firepower 4100/9300 새시에 설치되어 있는 특정한 논리적 디바이스에서 점보 프레임 지원을 활성화하려면 논리적 디바이스에서 인터페이스에 적절한 MTU 설정을 구성해야 합니다.

Firepower 4100/9300 새시에 있는 애플리케이션에 대해 지원되는 최대 MTU는 9184입니다.

## 인터페이스 속성 편집

### 절차

- 
- 단계 1** **Interfaces**(인터페이스)를 선택하여 **Interfaces**(인터페이스) 페이지를 엽니다. **Interfaces**(인터페이스) 페이지는 페이지 상단에 현재 설치된 인터페이스를 시각적으로 표시하며 아래 표에서 설치된 인터페이스 목록을 제공합니다.
  - 단계 2** 편집할 인터페이스의 행에서 **Edit**(편집)을 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** (선택 사항) **Type**(유형) 드롭다운 목록에서 **data**(데이터)를 선택하여 이 인터페이스를 데이터 인터페이스로 구성하거나, **firepower-eventing**(Firepower 이벤트)을 선택하여 인터페이스를 Firepower 이벤트 인터페이스로 구성하거나, **mgmt**(관리)를 선택하여 인터페이스를 관리 인터페이스로 구성합니다.  
**참고** **Cluster**(클러스터) 유형은 선택하지 마십시오.
  - 단계 5** (선택 사항) **Speed**(속도) 드롭다운 목록에서 인터페이스 속도를 선택합니다.
  - 단계 6** **OK**(확인)를 클릭합니다.
-



## 인터페이스의 관리 상태 변경

### 절차

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

Interfaces(인터페이스) 페이지는 페이지 상단에 현재 설치된 인터페이스를 시각적으로 표시하며 아래 표에서 설치된 인터페이스 목록을 제공합니다.

**단계 2** 관리 상태를 변경할 각 인터페이스에 다음 중 한 가지 작업을 수행합니다.

- 인터페이스의 관리 상태를 Enabled(활성화됨)로 설정하려면 활성화할 인터페이스의 State(상태) 열에서 **Disabled(비활성화됨)** 스위치를 클릭하여 설정을 **Enabled(활성화됨)**로 변경합니다. **Yes(예)**를 클릭하여 변경을 확인합니다.

인터페이스의 관리 상태가 Enabled(활성화됨)로 변경됩니다. 해당 인터페이스의 시각적 표시가 회색에서 녹색으로 변경됩니다.

- 인터페이스의 관리 상태를 Disabled(비활성화됨)로 설정하려면 비활성화할 인터페이스의 State(상태) 열에서 **Enabled(활성화됨)** 스위치를 클릭하여 설정을 **Disabled(비활성화됨)**로 변경합니다. **Yes(예)**를 클릭하여 변경을 확인합니다.

인터페이스의 관리 상태가 Disabled(비활성화됨)로 변경됩니다. 해당 인터페이스의 시각적 표시가 녹색에서 회색으로 변경됩니다.

## 포트 채널 생성

EtherChannel(포트 채널)은 동일한 유형의 멤버 인터페이스를 최대 16개 포함할 수 있습니다.

Firepower 4100/9300 새시가 EtherChannel을 생성하는 경우, EtherChannel은 물리적 링크가 작동 중인 경우에도 사용자가 논리적 디바이스에 할당할 때까지 **Suspended(유예)** 상태로 유지됩니다. EtherChannel은 다음 상황에서 **Suspended(유예)** 상태가 됩니다.

- EtherChannel은 독립형 논리적 디바이스에 대한 데이터 또는 관리 포트에 추가됩니다.
- EtherChannel은 클러스터의 일부인 논리적 디바이스에 대한 관리 또는 CCL 포트에 추가됩니다.
- EtherChannel은 클러스터의 일부인 논리적 디바이스에 대한 데이터 포트에 추가되며, 하나 이상의 보안 모듈이 클러스터에 조인됩니다.

EtherChannel은 논리적 디바이스에 할당될 때까지 작동하지 않습니다. 논리적 디바이스에서 EtherChannel이 제거되거나 논리적 디바이스가 삭제된 경우, EtherChannel은 **Suspended(유예)** 상태로 되돌아갑니다.

시작하기 전에

Firepower 4100/9300 새시는 활성화된 LACP(Link Aggregation Control Protocol) 모드에서 EtherChannel 만 지원합니다. 최고의 호환성을 위해 연결 스위치 포트를 Active(활성) 모드로 설정하는 것이 좋습니다.

## 절차

- 
- 단계 1 **Interfaces**(인터페이스)를 선택하여 **Interfaces**(인터페이스) 페이지를 엽니다. **Interfaces**(인터페이스) 페이지는 페이지 상단에 현재 설치된 인터페이스를 시각적으로 표시하며 아래 표에서 설치된 인터페이스 목록을 제공합니다.
  - 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. 포트 채널 48은 클러스터형 논리적 디바이스를 구축할 때 클러스터 제어 링크용으로 예약됩니다. 클러스터 제어 링크에 포트 채널 48을 사용하지 않으려면 EtherChannel을 다른 ID로 구성하고 인터페이스를 Cluster(클러스터) 유형으로 선택하면 됩니다. 클러스터 EtherChannel에 인터페이스를 할당하지 마십시오.
  - 단계 4 포트 채널을 활성화하려면 **Enable**(활성화) 확인란을 선택합니다. 포트 채널을 비활성화하려면 **Enable**(활성화) 확인란의 선택을 취소합니다.
  - 단계 5 **Type**(유형) 드롭다운 목록에서 포트 채널 유형을 **Data**(데이터), **Mgmt**(관리) 또는 **Cluster**(클러스터) 중 하나로 선택합니다.
  - 단계 6 유형을 선택하지 않은 경우, **Interfaces**(인터페이스) 탭을 클릭합니다.
  - 단계 7 포트 채널에 인터페이스를 추가하려면 **Available Interface**(사용 가능한 인터페이스) 목록에서 인터페이스를 선택하고 **Add Interface**(인터페이스 추가)를 클릭하여 Member ID(멤버 ID) 목록으로 인터페이스를 이동합니다. 유형 및 속도가 동일한 인터페이스를 최대 16개 추가할 수 있습니다.  
 팁 한 번에 여러 인터페이스를 추가할 수 있습니다. 여러 개별 인터페이스를 선택하려면 **Ctrl** 키를 누른 상태에서 원하는 인터페이스를 클릭합니다. 인터페이스의 범위를 선택하려면 범위의 첫 번째 인터페이스를 선택한 다음 **Shift** 키를 누른 상태에서 범위의 마지막 인터페이스를 클릭하여 선택합니다.
  - 단계 8 포트 채널에서 인터페이스를 제거하려면 Member ID(멤버 ID) 목록의 인터페이스 오른쪽에 있는 **Delete**(삭제) 버튼을 클릭합니다.
  - 단계 9 **Settings**(설정) 탭을 클릭합니다.
  - 단계 10 **Speed**(속도) 드롭다운 목록에서 포트 채널 속도를 선택합니다.
  - 단계 11 **OK**(확인)를 클릭합니다.
-

## 브레이크아웃 케이블 구성

다음 절차에서는 Firepower 4100/9300 새시와 함께 사용할 브레이크아웃 케이블을 구성하는 방법을 보여줍니다. 브레이크아웃 케이블을 사용하여 1개의 40Gbps 포트 대신 4개의 10Gbps 포트를 제공할 수 있습니다.

시작하기 전에

하드웨어 우회 가능 인터페이스는 브레이크아웃 포트용으로 구성할 수 없습니다.

### 절차

- 
- 단계 1 Interfaces(인터페이스)를 선택하여 Interfaces(인터페이스) 페이지를 엽니다.**  
Interfaces(인터페이스) 페이지는 페이지 상단에 현재 설치된 인터페이스를 시각적으로 표시하며 아래 표에서 설치된 인터페이스 목록을 제공합니다.
- 브레이크아웃 케이블을 지원할 수 있지만 현재 그렇게 구성되어 있지 않은 인터페이스는 해당 인터페이스 행에 **Breakout Port(브레이크아웃) 포트** 아이콘으로 표시되어 있습니다. 이미 브레이크아웃 케이블을 사용하도록 구성된 인터페이스의 경우, 개별 브레이크아웃 인터페이스가 별도로 나열되어 있습니다(예: Ethernet 2/1/1, 2/1/2, 2/1/3, 2/1/4).
- 단계 2** 1개의 40Gbps 인터페이스를 4개의 10Gbps 인터페이스로 변환하려면 다음을 수행합니다.
- 변환할 인터페이스의 **Breakout Port(브레이크아웃 포트)** 아이콘을 클릭합니다.  
Breakout Port Creation(브레이크아웃 포트 생성) 대화 상자가 열리면서 계속 진행할 것인지 확인을 요청하고 새시가 재부팅된다고 경고합니다.
  - 확인하려면 **Yes(예)**를 클릭합니다.  
Firepower 새시가 재부팅되고 지정된 인터페이스가 4개의 10Gbps 인터페이스로 변환됩니다.
- 단계 3** 4개의 10Gbps 브레이크아웃 인터페이스를 다시 1개의 40Gbps 인터페이스로 변환하려면 다음을 수행합니다.
- 브레이크아웃 인터페이스 중 하나에 대해 **Delete(삭제)**를 클릭합니다.  
확인 대화 상자가 열리면서 계속 진행할 것인지 확인을 요청하고 4개의 브레이크아웃 인터페이스가 모두 삭제되며 새시가 재부팅된다고 경고합니다.
  - 확인하려면 **Yes(예)**를 클릭합니다.  
Firepower 새시가 재부팅되고 지정된 인터페이스가 1개의 40Gbps 인터페이스로 변환됩니다.
-





## 논리적 디바이스

- 논리적 디바이스 정보, 131페이지
- 독립형 논리적 디바이스 생성, 133페이지
- 클러스터 구축, 137페이지
- 서비스 체이닝 구성, 156페이지
- 논리적 디바이스 관리, 161페이지

### 논리적 디바이스 정보

논리적 디바이스를 생성할 때 Firepower 4100/9300 새시 수퍼바이저는 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈/엔진에 푸시하여 논리적 디바이스를 구축합니다. 내장 새시 클러스터의 경우에는 Firepower 새시에 설치된 모든 보안 모듈에 푸시하여 구축합니다.

다음 2가지 유형의 논리적 디바이스 중 하나를 생성할 수 있습니다.

- 독립형 — Firepower 새시에 설치된 각 보안 모듈/엔진에 독립형 논리적 디바이스를 생성할 수 있습니다.
- 클러스터 — 클러스터링으로 여러 개의 보안 모듈을 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. Firepower 9300과 같은 다중 모듈 디바이스는 내장 새시 클러스터링을 지원합니다.



#### 참고

여러 보안 모듈을 지원하는 Firepower 4100/9300 새시에는 독립형 또는 클러스터 중 한 가지 유형의 논리적 디바이스만 생성할 수 있습니다. 즉, 보안 모듈 3개가 설치된 경우, 보안 모듈 하나에 독립형 논리적 디바이스를 생성한 다음 나머지 논리적 디바이스 2개를 사용하여 클러스터를 생성할 수 없습니다.

**참고**

독립형 논리적 디바이스를 구성 중인 경우, 새시에 있는 모든 모듈에 동일한 소프트웨어 유형을 설치해야 하며 다른 소프트웨어 유형은 현재 지원되지 않습니다. 모듈은 특정 디바이스 유형의 다른 버전을 실행할 수 있지만 모든 모듈은 동일한 유형의 논리적 디바이스로 구성되어야 합니다.

## 논리적 디바이스 페이지

논리적 디바이스를 생성, 편집 및 삭제하려면 Firepower Chassis Manager의 Logical Devices(논리적 디바이스) 페이지를 사용합니다. Logical Devices(논리적 디바이스) 페이지에는 각 Firepower 4100/9300 새시보안 모듈/엔진에 설치된 논리적 디바이스의 정보 영역이 포함되어 있습니다.

각 논리적 디바이스 영역의 헤더에서는 다음 정보가 제공됩니다.

- 논리적 디바이스의 고유한 이름
- 보안 모듈/엔진(ASA 또는 FTD)에 설치된 주요 애플리케이션의 이름
- 논리적 디바이스 모드(독립형 또는 클러스터형)
- Status(상태) — 논리적 디바이스의 상태를 보여줍니다.
  - ok(확인) — 논리적 디바이스 컨피그레이션이 완료되었습니다.
  - incomplete-configuration(불완전한 컨피그레이션) — 논리적 디바이스 컨피그레이션이 완료되지 않았습니다.

각 논리적 디바이스 영역에서는 다음 정보가 제공됩니다.

- Security Module(보안 모듈) — 보안 모듈이 표시됩니다.
- Ports(포트) — 애플리케이션 인스턴스에 할당된 포트가 표시됩니다.
- Application(애플리케이션) — 보안 모듈에서 실행되는 애플리케이션이 표시됩니다.
- Version(버전) — 보안 모듈에서 실행되는 애플리케이션의 소프트웨어 버전 번호가 표시됩니다.

**참고**

Firepower Threat Defense 논리적 디바이스에 대한 업데이트는 Firepower Management Center를 사용하여 수행되며 **Logical Devices(논리적 디바이스) > Edit(편집)** 및 **System(시스템) > Updates(업데이트)** 페이지(Firepower Chassis Manager)에 반영되지 않습니다. 이러한 페이지에서 표시된 버전은 Firepower Threat Defense 논리적 디바이스를 생성하는 데 사용된 소프트웨어 버전(CSP 이미지)을 나타냅니다.

- Management IP(관리 IP) — 논리적 디바이스 관리 IP로 할당된 로컬 IP 주소가 표시됩니다.
- Management URL(관리 URL) — 애플리케이션 인스턴스에 할당된 관리 URL이 표시됩니다.

- Gateway(게이트웨이) — 애플리케이션 인스턴스에 할당된 네트워크 게이트웨이 주소가 표시됩니다.
- Management Port(관리 포트) — 애플리케이션 인스턴스에 할당된 관리 포트가 표시됩니다.
- Status(상태) — 애플리케이션 인스턴스의 상태가 표시됩니다.
  - Online(온라인) — 애플리케이션이 실행 및 작동되고 있습니다.
  - Offline(오프라인) — 애플리케이션이 중지되었으며 작동 불가능합니다.
  - Installing(설치 중) — 애플리케이션 설치가 진행 중입니다.
  - Not Installed(설치되지 않음) — 애플리케이션이 설치되지 않았습니다.
  - Install Failed(설치 실패) — 애플리케이션 설치에 실패했습니다.
  - Starting(시작 중) — 애플리케이션이 시작되고 있습니다.
  - Start Failed(시작 실패) — 애플리케이션 시작에 실패했습니다.
  - Started(시작됨) — 애플리케이션이 시작되었으며 앱 에이전트 하트비트를 대기 중입니다.
  - Stopping(중지 중) — 애플리케이션이 중지되고 있습니다.
  - Stop Failed(중지 실패) — 애플리케이션을 오프라인으로 설정할 수 없습니다.
  - Not Responding(응답하지 않음) — 애플리케이션이 응답하지 않습니다.
  - Updating(업데이트 중) — 애플리케이션 소프트웨어 업그레이드가 진행 중입니다.
  - Update Failed(업데이트 실패) — 애플리케이션 소프트웨어 업그레이드에 실패했습니다.
  - Update Succeeded(업데이트 성공) — 애플리케이션 소프트웨어 업그레이드에 성공했습니다.

## 독립형 논리적 디바이스 생성

Firepower 새시에 설치된 각 보안 모듈/엔진에 대해 독립형 논리적 디바이스를 생성할 수 있습니다.

### 독립형 ASA 논리적 디바이스 생성

Firepower 4100/9300 새시에 설치된 각각의 보안 모듈/엔진에 독립형 논리적 디바이스를 생성할 수 있습니다. Firepower 9300과 같은 다중 모듈 디바이스에서는 클러스터가 구성되어 있는 경우 독립형 논리적 디바이스를 생성할 수 없습니다. 독립형 디바이스를 구성하려면 먼저 클러스터를 삭제해야 합니다.



#### 참고

선택적으로 서드파티 Radware DefensePro 가상 플랫폼을 보안 모듈의 ASA 방화벽보다 먼저 실행되는 DDoS 탐지 및 완화 서비스로 설치할 수 있습니다([서비스 체이닝 정보](#), 156 페이지 참조).



## 참고

하나의 새시 내의 모든 모듈에 동일한 소프트웨어 유형을 설치해야 합니다. 다른 소프트웨어 유형은 지원되지 않습니다. 모듈은 특정 디바이스 유형의 다른 버전을 실행할 수 있지만 모든 모듈은 동일한 유형의 논리적 디바이스로 구성되어야 합니다.

## 시작하기 전에

- 논리적 디바이스에 사용할 보안 모듈/엔진에 이미 논리적 디바이스가 구성되어 있는 경우, 먼저 기존의 논리적 디바이스를 삭제해야 합니다([논리적 디바이스 삭제](#), 162 페이지 참조).
- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드([Cisco.com에서 이미지 다운로드](#), 42 페이지 참조)한 다음 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다([Firepower Security Appliance에 이미지 업로드](#), 42 페이지 참조).
- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다.
- Firepower 4100/9300 새시에서 라우팅된 방화벽 모드 ASA만 구축할 수 있습니다. ASA를 투명 방화벽 모드로 변경하려면 이 절차를 완료한 다음 [ASA를 투명 방화벽 모드로 변경](#), 163 페이지의 내용을 참조하십시오.

## 절차

- 단계 1 Logical Devices(논리적 디바이스)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다. Logical Devices(논리적 디바이스) 페이지에는 새시에 구성된 논리적 디바이스의 목록이 표시됩니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
- 단계 2 Add Device(디바이스 추가)**를 클릭하여 Add Device(디바이스 추가) 대화 상자를 엽니다.
- 단계 3 Device Name(디바이스 이름)**에 논리적 디바이스의 이름을 제공합니다.
- 단계 4 Template(템플릿)**에서 Cisco Adaptive Security Appliance를 선택합니다.
- 단계 5 Image Version(이미지 버전)**은 ASA 소프트웨어 버전을 선택합니다.
- 단계 6 Device Mode(디바이스 모드)**에서 Standalone(독립형) 라디오 버튼을 클릭합니다.
- 단계 7 OK(확인)**를 클릭합니다.  
Provisioning - device name(프로비저닝 - 디바이스 이름) 창이 표시됩니다.
- 단계 8 Data Ports(데이터 포트)** 영역을 확장하고 디바이스에 할당할 각 포트를 클릭합니다.
- 단계 9** 화면 중앙의 디바이스 아이콘을 클릭합니다.  
ASA Configuration(ASA 컨피그레이션) 대화 상자가 나타납니다.
- 단계 10 General Information(일반 정보)** 탭에서 다음 작업을 수행합니다.
  - a) 다중 모듈 디바이스 예를 들어 Firepower 9300과 같은 디바이스에서 Security Module Selection(보안 모듈 선택사항) 아래에 있는 보안 모듈을 클릭하여 이 논리적 디바이스에 사용할 보안 모듈을 선택합니다.
  - b) **Management Interface(관리 인터페이스)** 드롭다운 목록에서 논리적 디바이스에 사용할 관리 인터페이스를 선택합니다.
  - c) DEFAULT(기본값)에서 관리 인터페이스를 구성합니다.



이 정보는 보안 모듈/엔진 컨피그레이션에서 관리 인터페이스를 구성하는 데 사용됩니다. 이 관리 IP 주소는 또한 ASDM에 연결하는 데 사용할 IP 주소입니다.

- 1 **Address Type**(주소 유형) 드롭다운 목록에서 주소 유형을 선택합니다.
- 2 **Management IP**(관리 IP) 필드에서 로컬 IP 주소를 구성합니다.
- 3 **Network Mask**(네트워크 마스크) 또는 **Prefix Length**(접두사 길이)를 입력합니다.
- 4 **Network Gateway**(네트워크 게이트웨이) 주소를 입력합니다.

단계 11 **Settings**(설정) 탭에서 **Password**(비밀번호) 필드에 “admin” 사용자의 비밀번호를 입력합니다.

단계 12 **OK**(확인)를 클릭하여 ASA Configuration(ASA 컨피그레이션) 대화 상자를 닫습니다.

단계 13 **Save**(저장)를 클릭합니다.

Firepower eXtensible 운영 체제에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈/엔진에 입력하여 논리적 디바이스를 구축합니다.

## 독립형 위협 방어 논리적 디바이스 생성

Firepower 4100/9300 새시에 설치된 각각의 보안 모듈/엔진에 독립형 논리적 디바이스를 생성할 수 있습니다. Firepower 9300과 같은 다중 모듈 디바이스에서는 클러스터가 구성되어 있는 경우 독립형 논리적 디바이스를 생성할 수 없습니다. 독립형 디바이스를 구성하려면 먼저 클러스터를 삭제해야 합니다.



**참고** 선택적으로 서드파티 Radware DefensePro 가상 플랫폼을 보안 모듈의 Firepower Threat Defense 논리적 디바이스보다 먼저 실행되는 DDoS 탐지 및 완화 서비스로 설치할 수 있습니다([서비스 체이닝 정보](#), 156 페이지 참조).




**참고** 하나의 새시 내의 모든 모듈에 동일한 소프트웨어 유형을 설치해야 합니다. 다른 소프트웨어 유형은 지원되지 않습니다. 모듈은 특정 디바이스 유형의 다른 버전을 실행할 수 있지만 모든 모듈은 동일한 유형의 논리적 디바이스로 구성되어야 합니다.

### 시작하기 전에

- 논리적 디바이스에 사용할 보안 모듈/엔진에 이미 논리적 디바이스가 구성되어 있는 경우, 먼저 기존의 논리적 디바이스를 삭제해야 합니다([논리적 디바이스 삭제](#), 162 페이지 참조).
- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드([Cisco.com에서 이미지 다운로드](#), 42 페이지 참조)한 다음 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다([Firepower Security Appliance에 이미지 업로드](#), 42 페이지 참조).

- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 최소 하나 이상의 데이터 유형 인터페이스도 구성해야 합니다. 선택적으로 Firepower 이벤트 인터페이스를 생성하여 모든 이벤트 트래픽(예: 웹 이벤트)을 전달할 수도 있습니다.

## 절차

- 단계 1 Logical Devices(논리적 디바이스)**를 선택하여 **Logical Devices(논리적 디바이스)** 페이지를 엽니다. Logical Devices(논리적 디바이스) 페이지에는 새시에 구성된 논리적 디바이스의 목록이 표시됩니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
- 단계 2 Add Device(디바이스 추가)**를 클릭하여 **Add Device(디바이스 추가)** 대화 상자를 엽니다.
- 단계 3 Device Name(디바이스 이름)**에 논리적 디바이스의 이름을 제공합니다. 이 이름은 Firepower 4100/9300 새시 수퍼바이저가 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 보안 모듈/엔진 컨피그레이션에 사용되는 디바이스 이름이 아닙니다.
- 단계 4 Template(템플릿)**에서 **Cisco Firepower Threat Defense**를 선택합니다.
- 단계 5 Image Version(이미지 버전)**에서 Threat Defense 소프트웨어 버전을 선택합니다.
- 단계 6 Device Mode(디바이스 모드)**에서 **Standalone(독립형)** 라디오 버튼을 클릭합니다.
- 단계 7 OK(확인)**를 클릭합니다.  
Provisioning - device name(프로비저닝 - 디바이스 이름) 창이 표시됩니다.
- 단계 8 Data Ports(데이터 포트)** 영역을 확장하고 디바이스에 할당할 각 포트를 클릭합니다. 하드웨어 우회 가능 포트는 다음 아이콘을 사용하여 표시됩니다. . 하드웨어 우회 쌍에서 두 인터페이스를 할당하지 않을 경우, 할당을 의도적으로 설정하기 위한 경고 메시지가 표시됩니다. 하드웨어 우회 기능을 사용할 필요가 없으므로 원하는 경우 단일 인터페이스를 할당할 수 있습니다.
- 단계 9** 화면 중앙의 디바이스 아이콘을 클릭합니다.  
컨피그레이션 대화 상자가 나타납니다.
- 단계 10 General Information(일반 정보)** 탭에서 다음 작업을 수행합니다.
- a) 다중 모듈 디바이스 예를 들어 Firepower 9300과 같은 디바이스에서 Security Module Selection(보안 모듈 선택사항) 아래에 있는 보안 모듈을 클릭하여 이 논리적 디바이스에 사용할 보안 모듈을 선택합니다.
  - b) **Management Interface(관리 인터페이스)** 드롭다운 목록에서 논리적 디바이스에 사용할 관리 인터페이스를 선택합니다.  
하드웨어 우회 가능 인터페이스를 관리 인터페이스로 할당할 경우, 할당을 의도적으로 설정하기 위한 경고 메시지가 표시됩니다.
  - c) Management(관리)에서 관리 인터페이스를 구성합니다.
    - 1 **Address Type(주소 유형)** 드롭다운 목록에서 주소 유형을 선택합니다.
    - 2 **Management IP(관리 IP)** 필드에서 로컬 IP 주소를 구성합니다.
    - 3 **Network Mask(네트워크 마스크)** 또는 **Prefix Length(접두사 길이)**를 입력합니다.
    - 4 **Network Gateway(네트워크 게이트웨이)** 주소를 입력합니다.

단계 11 **Settings(설정)** 탭에서 다음 작업을 수행합니다.

- a) 등록하는 동안 Firepower Management Center와 디바이스 간에 공유할 키를 **Registration Key(등록 키)** 필드에 입력합니다.
- b) **Password(비밀번호)** 필드에 디바이스의 비밀번호를 입력합니다.
- c) **Firepower Management Center IP** 필드에 Firepower Management Center를 관리하기 위한 IP 주소를 입력합니다.
- d) **Search Domains(검색 도메인)** 필드에 디바이스의 검색 도메인 목록을 쉼표로 구분하여 입력합니다.
- e) 방화벽 모드를 **Transparent(투명)** 또는 **Routed(라우팅)** 중에서 선택합니다.
- f) **DNS Servers(DNS 서버)** 필드에 디바이스가 사용할 DNS 서버 목록을 쉼표로 구분하여 입력합니다.
- g) **Fully Qualified Hostname(정규화된 호스트 이름)** 필드에 Threat Defense 디바이스의 정규화된 이름을 입력합니다.
- h) Firepower 이벤트를 전송해야 할 인터페이스를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다.  
Firepower 이벤트에 사용할 인터페이스를 지정하려면 인터페이스를 *Firepower* 이벤트 인터페이스로 구성해야 합니다. 자세한 내용은 [Firepower Security Appliance 인터페이스 정보, 123 페이지](#)를 참조하십시오.

단계 12 **Agreement(계약)** 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 13 **OK(확인)**를 클릭하여 컨피그레이션 대화 상자를 닫습니다.

단계 14 **Save(저장)**를 클릭합니다.

Firepower eXtensible 운영 체제에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈/엔진에 입력하여 논리적 디바이스를 구축합니다.

## 클러스터 구축

클러스터링을 사용하면 여러 개의 디바이스를 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. 여러 개의 모듈을 포함하는 Firepower 9300은 단일 새시 내의 모든 모듈을 클러스터로 그룹화하는 인프라 새시 클러스터링을 지원합니다. 또한, 여러 새시를 함께 그룹화하는 새시 간 클러스터링을 사용할 수 있습니다(Firepower 4100 Series 같은 단일 모듈 디바이스의 경우 새시 간 클러스터링은 유일한 옵션임).

## 클러스터링 정보 - Firepower 4100/9300 새시

클러스터는 하나의 논리적 유닛으로 작동하는 여러 개의 디바이스로 구성됩니다. Firepower 4100/9300 새시에서 클러스터를 구축하려면 다음 작업을 수행합니다.

- 유닛 간 통신에 사용되는 클러스터 제어 링크(기본적으로, 포트 채널 48)를 생성합니다. 내장 새시 클러스터링(Firepower 9300 전용)의 경우, 이 링크는 클러스터 통신에 Firepower 9300 백플레인을 활용합니다. 새시 간 클러스터링의 경우, 새시 간의 통신을 위해 물리적 인터페이스를 이 EtherChannel에 수동으로 할당해야 합니다.
- 애플리케이션 내부에 클러스터 부트스트랩 컨피그레이션을 생성합니다.  
클러스터를 구축할 때, Firepower 4100/9300 새시 수퍼바이저는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 유닛에 최소한의 부트스트랩 컨피그레이션을 푸시합니다. 클러스터링 환경을 맞춤화하려는 경우, 사용자가 일부 부트스트랩 컨피그레이션을 애플리케이션 내부에 구성할 수 있습니다.
- 데이터 인터페이스를 스패 인터페이스로 클러스터에 할당합니다.  
내장 새시 클러스터링의 경우, 스패 인터페이스는 새시 간 클러스터링과 마찬가지로 EtherChannel에 국한되지 않습니다. Firepower 9300 수퍼바이저는 EtherChannel 기술을 내부에 사용하여 트래픽을 공유 인터페이스의 다중 모듈에 로드 밸런싱하므로 모든 데이터 인터페이스 유형이 스패 모드에서 작동합니다. 새시 간 클러스터링의 경우, 모든 데이터 인터페이스에 스패 EtherChannel을 사용해야 합니다.



**참고** 개별 인터페이스는 지원되지 않습니다(관리 인터페이스는 제외).

- 관리 인터페이스를 클러스터의 모든 유닛에 할당합니다.

다음 섹션에서는 클러스터링 개념 및 구현에 대한 자세한 정보를 제공합니다.

## 기본 유닛 및 보조 유닛 역할

클러스터의 멤버 중 하나는 기본 유닛입니다. 기본 유닛은 자동으로 결정됩니다. 그 외 멤버는 모두 보조 유닛입니다.

모든 컨피그레이션은 기본 유닛에서만 수행해야 하며, 컨피그레이션은 이후에 보조 유닛에 복제됩니다.

## 클러스터 제어 링크

클러스터 제어 링크는 포트 채널 48 인터페이스를 사용하여 자동으로 생성됩니다. 내장 새시 클러스터링의 경우, 이 인터페이스에는 멤버 인터페이스가 없습니다. 새시 간 클러스터링의 경우, EtherChannel에 인터페이스를 하나 이상 추가해야 합니다. 이 클러스터 유형 EtherChannel은 내장 새시 클러스터링을 위한 클러스터 통신에 Firepower 9300 백플레인을 활용합니다.

2-멤버 새시 간 클러스터의 경우 클러스터 제어 링크를 하나의 새시에서 다른 새시로 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.

### 새시 간 클러스터링을 위한 클러스터 제어 링크 크기 조정

가능한 경우, 각 새시의 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.
- 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.

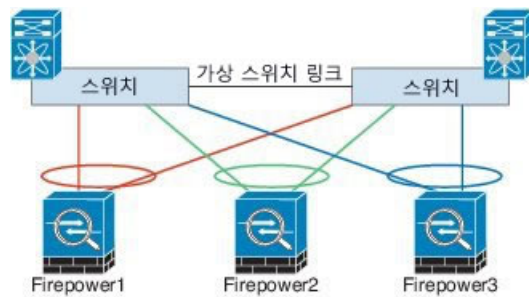


**참고**

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

### 새시 간 클러스터링을 위한 클러스터 제어 링크 이중화

다음 다이어그램에는 VSS(Virtual Switching System) 또는 vPC(Virtual Port Channel) 환경에서 EtherChannel을 클러스터 제어 링크로 사용하는 방법이 나와 있습니다. EtherChannel의 모든 링크가 활성화되어 있습니다. 스위치가 VSS 또는 vPC의 일부일 경우 동일한 EtherChannel 내에서 Firepower 4100/9300 새시 인터페이스를 연결하여 VSS 또는 vPC의 스위치와 별도로 분리할 수 있습니다. 이러한 별도의 스위치는 단일 스위치 역할을 수행하므로, 스위치 인터페이스는 동일한 EtherChannel 포트 채널 인터페이스의 멤버입니다. 이러한 EtherChannel은 스펠 EtherChannel이 아니라 디바이스 로컬입니다.



## 새시 간 클러스터링을 위한 클러스터 제어 링크 안정성

클러스터 제어 링크 기능을 보장하려면 유닛 간의 RTT(왕복 시간)가 20ms 미만이어야 합니다. 이러한 최대 레이턴시는 서로 다른 지리적 사이트에 설치된 클러스터 멤버와의 호환성을 개선합니다. 레이턴시를 확인하려면 유닛 간의 클러스터 제어 링크에서 Ping을 수행합니다.

클러스터 제어 링크는 오류가 나거나 삭제된 패킷이 없는 안정적인 상태여야 합니다. 예를 들어, 사이트 간 구축 시에는 전용 링크를 사용해야 합니다.

## 클러스터 제어 링크 네트워크

Firepower 4100/9300 새시는 새시 ID와 슬롯 ID(127.2.chassis\_id.slot\_id)를 기반으로 하는 각 유닛에 대해 클러스터 제어 링크 인터페이스 IP 주소를 자동으로 생성합니다. 이 IP 주소는 FXOS에서 또는 애플리케이션 내에서 수동으로 설정할 수 없습니다. 클러스터 제어 링크 네트워크에서는 유닛 간에 라우터가 포함될 수 없으며, 레이어 2 스위칭만 허용됩니다. 사이트 간 트래픽의 경우, OTV(Overlay Transport Virtualization)를 사용하는 것이 좋습니다.

## 관리 네트워크

모든 유닛을 단일 관리 네트워크에 연결하는 것이 좋습니다. 이러한 네트워크는 클러스터 제어 링크와 분리되어 있습니다.

## 관리 인터페이스

클러스터에 관리 유형 인터페이스를 할당할 수 있습니다. 이 인터페이스는 스패 인터페이스와는 다른 특수 개별 인터페이스입니다. 관리 인터페이스를 사용하면 각 유닛에 직접 연결할 수 있습니다.

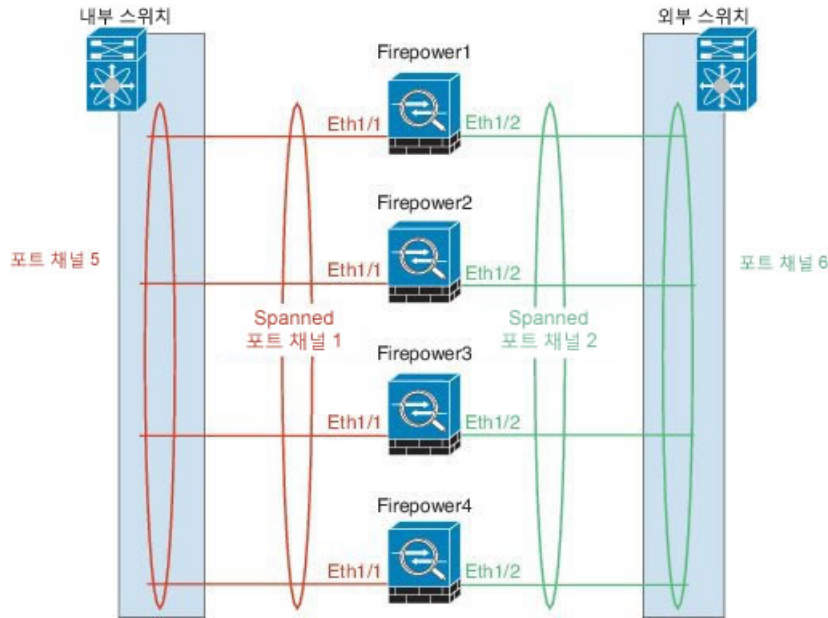
ASA의 경우, 기본 클러스터 IP 주소는 현재 기본 유닛에 항상 속해 있는 클러스터를 위한 고정 주소입니다. 주소의 범위를 구성하여 현재 기본 유닛을 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 합니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 기본 유닛이 변경될 경우 기본 클러스터 IP 주소는 새 기본 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다. 로컬 IP 주소는 라우팅에 사용되며 문제 해결에도 도움이 됩니다. 예를 들어, 현재 기본 유닛에 항상 연결되어 있는 기본 클러스터 IP 주소에 연결하여 클러스터를 관리할 수 있습니다. 로컬 IP 주소에 연결하여 개별 멤버를 관리할 수 있습니다. TFTP 또는 syslog 같은 아웃바운드 관리 트래픽의 경우, 기본 유닛을 비롯한 각 유닛에서 로컬 IP 주소를 사용하여 서버에 연결합니다.

Firepower Threat Defense의 경우, 동일한 네트워크의 각 유닛에 관리 IP 주소를 할당합니다. 각 유닛을 Management Center에 추가할 때 이러한 IP 주소를 사용합니다.

## 스팬 EtherChannel

새시당 하나 이상의 인터페이스를 클러스터 내의 모든 새시를 포괄하는 EtherChannel로 그룹화할 수 있습니다. EtherChannel에서는 채널에서 사용 가능한 모든 활성 인터페이스 전반의 트래픽을 취합합니다. 스패 EtherChannel은 라우팅 및 투명 방화벽 모드에서 모두 구성할 수 있습니다. 라우팅 모드의 경우 EtherChannel은 단일 IP 주소를 통해 라우팅된 인터페이스로 구성됩니다. 투명 모드의 경우 IP

주소가 BVI에 할당되며 브리지 그룹 멤버 인터페이스에는 할당되지 않습니다. EtherChannel은 기본적인 작동 시 로드 밸런싱을 함께 제공합니다.



### 사이트 간 클러스터링

사이트 간 설치의 경우 권장 지침을 준수하여 클러스터링을 활용할 수 있습니다.

개별 사이트 ID에 속하는 각 클러스터 새시를 구성할 수 있습니다.

사이트 ID는 사이트별 MAC 주소 및 IP 주소와 함께 작동합니다. 클러스터에서 가져온 패킷은 사이트별 MAC 주소 및 IP 주소를 사용하는 반면 클러스터에서 수신된 패킷은 글로벌 MAC 주소 및 IP 주소를 사용합니다. 이 기능은 스위치가 다른 두 개의 포트에서 두 개의 사이트의 동일한 글로벌 MAC 주소를 확인하는 것을 방지합니다. 대신 사이트 MAC 주소만 확인합니다. 사이트별 MAC 주소 및 IP 주소는 Spanned EtherChannels만 사용하는 라우팅 모드에 대해 지원됩니다.

또한, 사이트 ID는 LISP 검사를 사용하여 플로우 모빌리티를 활성화하는 데 사용되며, 관리자 현지화는 성능을 개선하고 데이터 센터에 대한 사이트 간 클러스터링을 위해 왕복 시간 레이턴시를 줄이는 데 사용됩니다.

사이트 간 클러스터링에 대한 자세한 내용은 다음 섹션을 참조하십시오.

- 데이터 센터 인터커넥트 크기 조정 —클러스터링의 사전 요구 사항, 142 페이지
- 사이트 간 지침 —클러스터링 지침, 143 페이지
- 사이트 간 예시 —사이트 간 클러스터링 예시, 153 페이지

## 클러스터링의 사전 요구 사항

새시 간 하드웨어 및 소프트웨어 요건

클러스터의 모든 새시는 다음과 같아야 합니다.

- **Firepower 4100 Series:** 모든 새시는 동일한 모델이어야 합니다. Firepower 9300의 경우 모든 보안 모듈은 동일한 유형이어야 합니다. 새시에 있는 모든 모듈은 빈 슬롯을 포함하여 클러스터에 속해야 하지만, 각 새시에는 서로 다른 수량의 보안 모듈을 설치할 수 있습니다.
- 이미지 업그레이드 시 동일한 FXOS 소프트웨어 예외를 실행해야 합니다.
- 클러스터에 할당한 인터페이스와 동일한 인터페이스 컨피그레이션(예: 동일한 관리 인터페이스, EtherChannels, 활성화된 인터페이스, 속도 및 듀플렉스)을 포함해야 합니다. 동일한 인터페이스 ID와 용량이 일치하는 한, 새시에서 서로 다른 네트워크 모듈 유형을 사용할 수 있으며, 인터페이스가 동일한 Spanned EtherChannel에서 성공적으로 번들링될 수 있습니다. 모든 데이터 인터페이스는 새시 간 클러스터링에서 EtherChannel이어야 합니다.
- 동일한 NTP 서버를 사용해야 합니다. Firepower Threat Defense의 경우 Firepower Management Center 또한 동일한 NTP 서버를 사용해야 합니다. 시간을 수동으로 설정하지 마십시오.
- ASA의 경우 각 FXOS 새시를 License Authority 또는 Satellite 서버에 등록해야 합니다. 보조 유닛에는 추가 비용이 없습니다. 영구 라이선스 예약의 경우, 각 새시의 개별 라이선스를 구매해야 합니다. Firepower Threat Defense의 경우 모든 라이선싱이 Firepower Management Center에서 처리됩니다.

새시 간 클러스터링을 위한 스위치 사전 요구 사항

- Firepower 4100/9300 새시에서 클러스터링을 구성하기 전에 스위치 컨피그레이션을 완료하고 새시의 모든 EtherChannel을 스위치에 성공적으로 연결합니다.
- 지원되는 스위치의 목록은 [Cisco FXOS 호환성](#)을 참조하십시오.

새시 간 클러스터링을 위한 데이터 센터 인터커넥트 크기 조정

클러스터 제어 링크 트래픽용 DCI(Data Center Interconnect) 대역폭은 다음 계산과 같이 예약해야 합니다.

$$\frac{\text{사이트당 클러스터 멤버의 수}}{2} \times \text{멤버당 클러스터 제어 링크 크기}$$

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.

- 4개 사이트에 멤버가 2개인 경우:
  - 총 클러스터 멤버 4개



- 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.

## 클러스터링 지침

### 모델

- Firepower 9300의 ASA — 내장 새시 및 새시 간, 사이트 간 클러스터링에 대해 지원됨
- Firepower 4100 Series의 ASA — 새시 간 및 사이트 간 클러스터링에 대해 지원됨
- Firepower 9300의 Firepower Threat Defense — 내장 새시 및 새시 간 클러스터링에 대해 지원됨
- Firepower 4100 Series의 Firepower Threat Defense — 새시 간 클러스터링에 대해 지원됨
- Radware DefensePro — ASA와의 내장 새시 클러스터링에 대해 지원됨
- Radware DefensePro — Firepower Threat Defense와의 내장 새시 클러스터링에 대해 지원됨

### 새시 간 클러스터링을 위한 스위치

- ASR 9006의 경우 기본이 아닌 MTU를 설정하려면 ASR 인터페이스 MTU를 클러스터 디바이스 MTU보다 14바이트 높게 설정합니다. 그렇지 않으면 **mtu-ignore** 옵션을 사용하지 않는 한 OSPF 인접 피어링 시도에 실패할 수 있습니다. 클러스터 디바이스 MTU는 ASR IPv4 MTU와 일치해야 합니다.

- 클러스터 제어 링크 인터페이스용 스위치의 경우, 선택적으로 클러스터 유닛에 연결된 스위치 포트에서 Spanning Tree PortFast를 활성화하여 새 유닛에 대한 조인 프로세스 속도를 높일 수 있습니다.
- 스위치에서 Spanned EtherChannel의 번들링 속도가 저하될 경우, 스위치의 개별 인터페이스에 대해 빠른 LACP 속도를 활성화할 수 있습니다. Nexus Series 같은 일부 스위치는 ISSU(서비스 중 소프트웨어 업그레이드)를 수행할 때 빠른 LACP 속도를 지원하지 않습니다. 따라서 클러스터링과 ISSU를 함께 사용하지 않는 것이 좋습니다.
- 스위치에서는 **source-dest-ip** 또는 **source-dest-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 있기 때문입니다.
- 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.
- 수퍼바이저 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-distributionfixed
```

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

#### 새시 간 클러스터링을 위한 EtherChannel

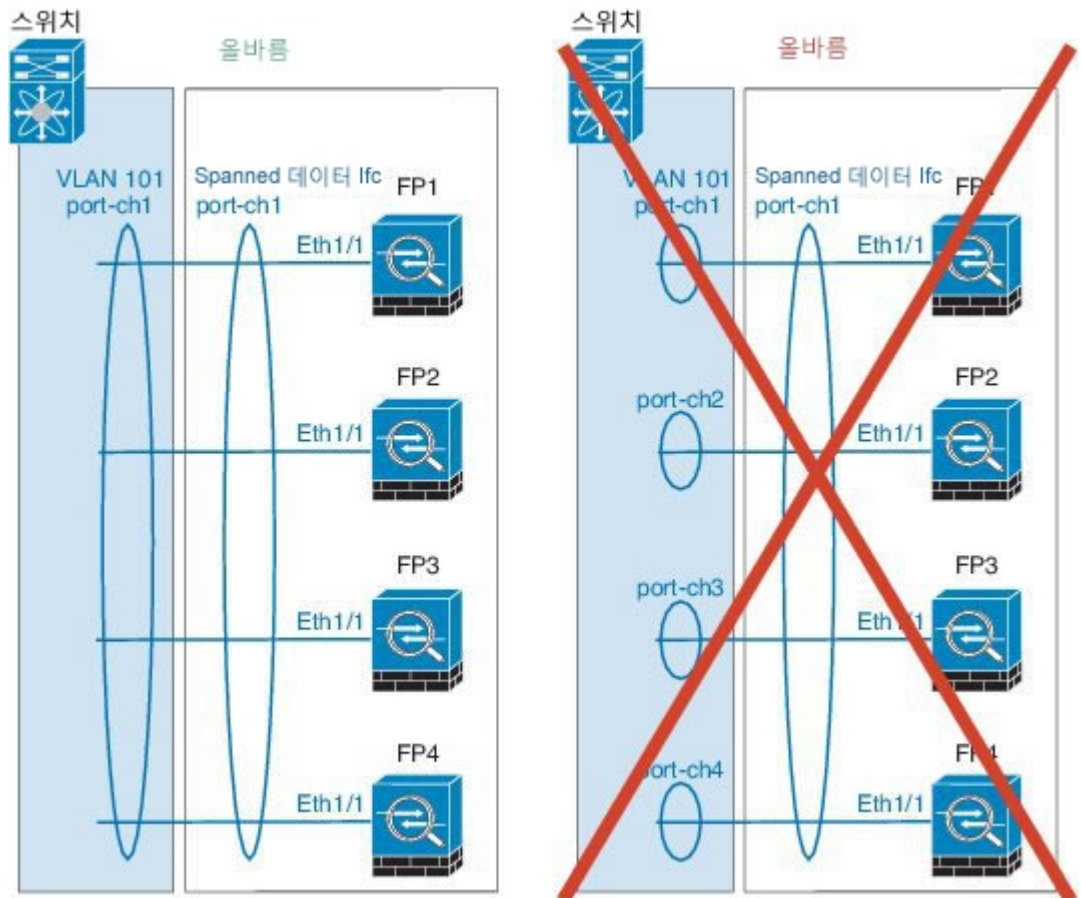
- 연결 스위치의 경우, EtherChannel 모드를 Active(활성)로 설정합니다. On(켜짐) 모드는 Firepower 4100/9300 새시에서 지원되지 않으며 클러스터 제어 링크에서도 지원되지 않습니다.
- FXOS EtherChannel은 기본적으로 LACP 속도가 보통으로 설정되어 있습니다. 이렇게 설정하면 포트-채널 멤버를 번들링하는 데 30초 넘게 걸릴 수 있으므로 이로 인해 클러스터 인터페이스 상태 확인에 장애가 발생하여 클러스터에서 유닛이 제거될 수 있습니다. 따라서 LACP 속도를 빠르게 변경하는 것이 좋습니다. 다음 예에서는 "기본" lacp 정책을 다음과 같이 수정합니다.

```
firepower# scope org
firepower /org # scope lacppolicy default
firepower /org/lacppolicy# set lacp-rate fast
firepower /org* # commit-buffer
```

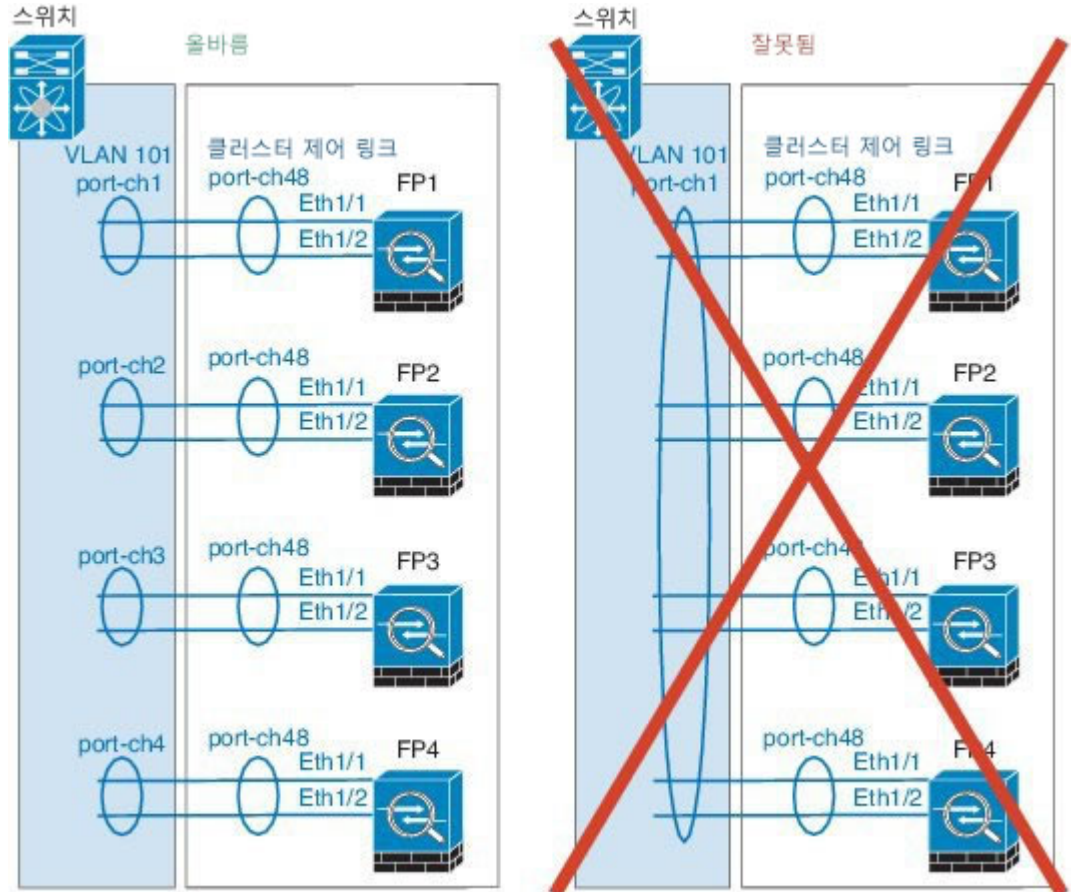


**참고** Nexus Series 같은 일부 스위치는 ISSU(서비스 중 소프트웨어 업그레이드)를 수행할 때 빠른 LACP 속도를 지원하지 않습니다. 따라서 클러스터링과 ISSU를 함께 사용하지 않는 것이 좋습니다.

- 15.1(1)S2 이전 Catalyst 3750-X Cisco IOS 소프트웨어 버전에서는 클러스터 유닛에서 EtherChannel 과 스위치 스택 간 연결을 지원하지 않았습니다. 기본 스위치 설정으로 클러스터 유닛 EtherChannel 이 교차 스택에 연결되어 있는 상태에서 마스터 스위치의 전원이 꺼질 경우, 나머지 스위치에 연결된 EtherChannel은 작동하지 않습니다. 호환성을 개선하려면 **stack-mac persistent timer** 명령을 재로드 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 컨피그레이션과 디바이스-로컬 EtherChannel 컨피그레이션 — Spanned EtherChannel과 디바이스-로컬 EtherChannel에 맞게 스위치를 구성해야 합니다.
  - Spanned EtherChannel — 클러스터의 모든 멤버 전체를 포괄하는 클러스터 유닛 *Spanned EtherChannels*의 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.



추가 지침

- 이중화를 위해 EtherChannel을 VSS 또는 vPC에 연결하는 것이 좋습니다.
- 새시 내에서 일부 보안 모듈을 클러스터링하여 독립형 모드에서 다른 보안 모듈을 실행할 수 없습니다. 클러스터에 모든 보안 모듈을 포함해야 합니다.

## 클러스터링 기본값

클러스터 제어 링크는 포트 채널 48을 사용합니다.

## ASA 클러스터링 구성

Firepower 4100/9300 새시 관리자(Supervisor)에서 손쉽게 클러스터를 구축할 수 있습니다. 모든 초기 컨피그레이션은 유닛마다 자동으로 생성됩니다. 새시 간 클러스터링의 경우 각 새시를 개별적으로 구성해야 합니다. 새시 하나에 클러스터를 구축한 다음 쉽게 구축하기 위해 첫 번째 새시의 부트스트랩 컨피그레이션을 다음 새시에 복사합니다.

### 시작하기 전에

- 모듈을 설치하지 않은 경우에도 Firepower 9300 새시에서 3개의 모듈 슬롯 모두에 대해 클러스터링을 활성화해야 합니다. 3개의 모듈을 모두 구성하지 않은 경우, 클러스터가 나타나지 않습니다.
- **Interfaces**(인터페이스) 탭에서 포트 채널 48 클러스터 유형 인터페이스는 멤버 인터페이스를 포함하지 않은 경우 **Operation State**(작동 상태)를 **failed**(실패함)로 표시합니다. 새시 내 클러스터링의 경우 이 EtherChannel이 멤버 인터페이스를 필요로 하지 않으므로 이 작동 상태를 무시할 수 있습니다.
- Firepower 4100/9300 새시에서 라우팅된 방화벽 모드 ASA 클러스터만 구축할 수 있습니다. ASA 클러스터를 투명 방화벽 모드로 변경하려면 이 절차를 완료한 다음 [ASA를 투명 방화벽 모드로 변경, 163 페이지](#)의 내용을 참조하십시오.

### 절차

- 단계 1** 클러스터를 구축하기 전에 데이터 유형 인터페이스 또는 EtherChannel(포트 채널이라고도 함)을 하나 이상 추가합니다. [포트 채널 생성, 127 페이지](#) 또는 [인터페이스 속성 편집, 126 페이지](#)를 참조하십시오.  
또한 데이터 인터페이스를 구축한 후에 클러스터에 추가할 수 있습니다.  
새시 간 클러스터링의 경우, 모든 데이터 인터페이스는 멤버 인터페이스가 최소 1개 있는 EtherChannel 이어야 합니다. 각 새시에서 동일한 EtherChannel을 추가합니다.
- 단계 2** 관리 유형 인터페이스 또는 EtherChannel을 추가합니다. [포트 채널 생성, 127 페이지](#) 또는 [인터페이스 속성 편집, 126 페이지](#)를 참조하십시오.  
새시 간 클러스터링의 경우, 각 새시에서 동일한 관리 인터페이스를 추가합니다.
- 단계 3** 새시 간 클러스터링의 경우, 멤버 인터페이스를 클러스터 제어 링크로 사용할 port-channel 48에 추가합니다.  
멤버 인터페이스를 포함하지 않은 경우, 논리적 디바이스를 구축할 때 Firepower Chassis Manager에서는 이 클러스터를 인트라 새시 클러스터로 간주하고 **Chassis ID**(새시 ID) 필드를 표시하지 않습니다. 각 새시에서 동일한 멤버 인터페이스를 추가합니다.
- 단계 4** **Logical Devices**(논리적 디바이스)를 선택하여 **Logical Devices**(논리적 디바이스) 페이지를 엽니다. **Logical Devices**(논리적 디바이스) 페이지에는 새시에 구성된 논리적 디바이스의 목록이 표시됩니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
- 단계 5** **Add Device**(디바이스 추가)를 클릭하여 **Add Device**(디바이스 추가) 대화 상자를 엽니다.

기존 클러스터가 있는 경우, 클러스터를 제거하고 새로 추가하라는 프롬프트가 표시됩니다. 보안 모듈의 모든 클러스터 관련 컨피그레이션은 새 정보로 대체됩니다.

**단계 6 Device Name(디바이스 이름)**에 논리적 디바이스의 이름을 제공합니다. 이 이름은 Firepower 4100/9300 새시 수퍼바이저가 클러스터링 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 보안 모듈 컨피그레이션에 사용되는 클러스터 이름이 아닙니다.

**단계 7 Template(템플릿)**에서 **Cisco Adaptive Security Appliance**를 선택합니다.

**단계 8 Image Version(이미지 버전)**은 ASA 소프트웨어 버전을 선택합니다.

**단계 9 Device Mode(디바이스 모드)**에서 **Cluster(클러스터)** 라디오 버튼을 클릭합니다.

**단계 10 Create New Cluster(새 클러스터 생성)** 라디오 버튼을 클릭합니다.

**단계 11 OK(확인)**를 클릭합니다.

독립형 디바이스가 구성되어 있는 경우, 이 디바이스를 새 클러스터로 교체하라는 프롬프트가 표시됩니다. **Provisioning - device name(프로비저닝 - 디바이스 이름)** 창이 표시됩니다.

모든 인터페이스는 클러스터에 기본적으로 할당되어 있습니다.

**단계 12** 화면 중앙의 디바이스 아이콘을 클릭합니다.

ASA Configuration(ASA 컨피그레이션) 대화 상자가 나타나며 **Cluster Information(클러스터 정보)** 탭이 선택되어 있습니다.

**단계 13 Chassis ID(새시 ID)** 필드에 새시 ID를 입력합니다. 클러스터의 각 새시는 고유 ID를 사용해야 합니다.

**단계 14** 사이트 간 클러스터링의 경우 **Site ID(사이트 ID)** 필드에 이 새시의 사이트 ID를 1~8로 입력합니다.

**단계 15 Cluster Key(클러스터 키)** 필드에서 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 구성합니다. 공유 비밀은 1~63자로 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.

**단계 16 Cluster Group Name(클러스터 그룹 이름)**(보안 모듈 컨피그레이션의 클러스터 그룹 이름)을 설정합니다.

이름은 1~38자로 된 ASCII 문자열이어야 합니다.

**단계 17 Management Interface(관리 인터페이스)**를 클릭하고 이전에 생성한 관리 인터페이스를 선택합니다.

**단계 18** 관리 인터페이스의 **Address Type(주소 유형)**을 선택합니다.

이 정보는 보안 모듈 컨피그레이션의 관리 인터페이스를 구성하는 데 사용됩니다.

a) **Management IP Pool(관리 IP 풀)** 필드에서 하이픈으로 구분되는 시작 및 종료 주소를 입력하여 로컬 IP 주소의 풀을 구성합니다. 이 주소 중 하나는 인터페이스의 각 클러스터 유닛에 할당됩니다.

최소한 클러스터에 있는 유닛 수에 상응하는 개수의 주소를 포함해야 합니다. Firepower 9300의 경우, 모든 모듈 슬롯을 채우지 않은 경우에도 새시당 3개의 주소를 포함해야 합니다. 클러스터를 확장하려는 경우, 추가 주소를 포함하십시오. 현재 기본 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.

b) **Network Mask(네트워크 마스크)** 또는 **Prefix Length(접두사 길이)**를 입력합니다.

c) **Network Gateway(네트워크 게이트웨이)**를 입력합니다.

d) **Virtual IP address**(가상 IP 주소)를 입력합니다.

이 IP 주소는 같은 네트워크의 클러스터 풀 주소로 있어야 하지만 풀의 일부는 아닙니다.

단계 19 **Settings**(설정) 탭에서 **Password**(비밀번호)에 “admin” 사용자의 비밀번호를 입력합니다.

단계 20 **OK**(확인)를 클릭하여 ASA Configuration(ASA 컨피그레이션) 대화 상자를 닫습니다.

단계 21 **Save**(저장)를 클릭합니다.

Firepower 4100/9300 새시 관리자(Supervisor)는 지정된 소프트웨어 버전을 다운로드하고 클러스터 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 각 보안 모듈에 입력하여 클러스터를 구축합니다.

단계 22 새시 간 클러스터링의 경우, 다음 새시를 클러스터에 추가합니다.

a) 첫 번째 새시 Firepower Chassis Manager에서 오른쪽 상단에 있는 **Show Cluster Detail**(클러스터 세부사항 표시) 아이콘을 클릭하여 표시된 클러스터 컨피그레이션을 복사합니다.

b) 다음 새시에 있는 Firepower Chassis Manager에 연결하고 이 절차에 따라 논리적 디바이스를 추가합니다.

c) **Join an Existing Cluster**(기존 클러스터에 조인)를 선택합니다.

d) **Copy config**(컨피그레이션 복사) 확인란을 클릭하고 **OK**(확인)를 클릭합니다. 이 확인란을 선택하지 않은 경우, 수동으로 첫 번째 새시 컨피그레이션에 맞게 설정을 입력해야 합니다.

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

f) 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보가 대부분 미리 입력되어 있지만 다음 설정을 변경해야 합니다.

- **Chassis ID**(새시 ID) — 고유한 새시 ID를 입력합니다.

- **Site ID**(사이트 ID) — 올바른 사이트 ID를 입력합니다.

- **Cluster Key**(클러스터 키) — (미리 입력되지 않음) 동일한 클러스터 키를 입력합니다.

**OK**(확인)를 클릭합니다.

g) **Save**(저장)를 클릭합니다.

단계 23 클러스터링 컨피그레이션을 사용자 정의하려면 기본 유닛 보안 모듈에 연결합니다.

## Firepower Threat Defense 클러스터링 구성

Firepower 4100/9300 새시 관리자(Supervisor)에서 손쉽게 클러스터를 구축할 수 있습니다. 모든 초기 컨피그레이션은 유닛마다 자동으로 생성됩니다. 새시 간 클러스터링의 경우 각 새시를 개별적으로 구성해야 합니다. 새시 하나에 클러스터를 구축한 다음 쉽게 구축하기 위해 첫 번째 새시의 부트스트랩 컨피그레이션을 다음 새시에 복사합니다.

## 시작하기 전에

- 모듈을 설치하지 않은 경우에도 Firepower 9300 새시에서 3개의 모듈 슬롯 모두에 대해 클러스터링을 활성화해야 합니다. 3개의 모듈을 모두 구성하지 않은 경우, 클러스터가 나타나지 않습니다.
- **Interfaces(인터페이스)** 탭에서 포트 채널 48 클러스터 유형 인터페이스는 멤버 인터페이스를 포함하지 않은 경우 **Operation State(작동 상태)**를 **failed(실패함)**로 표시합니다. 새시 내 클러스터링의 경우 이 EtherChannel이 멤버 인터페이스를 필요로 하지 않으므로 이 작동 상태를 무시할 수 있습니다.

## 절차

- 단계 1** 클러스터를 구축하기 전에 데이터 유형 인터페이스 또는 EtherChannel(포트 채널이라고도 함)을 하나 이상 추가합니다.  
또한 데이터 인터페이스를 구축한 후에 클러스터에 추가할 수 있습니다.  
새시 간 클러스터링의 경우, 모든 데이터 인터페이스는 멤버 인터페이스가 최소 1개 있는 EtherChannel 이어야 합니다. 각 새시에서 동일한 EtherChannel을 추가합니다.
- 단계 2** 관리 유형 인터페이스 또는 EtherChannel을 추가합니다.  
새시 간 클러스터링의 경우, 각 새시에서 동일한 관리 인터페이스를 추가합니다.
- 단계 3** 새시 간 클러스터링의 경우, 멤버 인터페이스를 클러스터 제어 링크로 사용할 port-channel 48에 추가합니다.  
멤버 인터페이스를 포함하지 않은 경우, 논리적 디바이스를 구축할 때 Firepower Chassis Manager에서는 이 클러스터를 인트라 새시 클러스터로 간주하고 **Chassis ID(새시 ID)** 필드를 표시하지 않습니다. 각 새시에서 동일한 멤버 인터페이스를 추가합니다.
- 단계 4** (선택 사항) Firepower 이벤트 인터페이스를 추가합니다.  
이 인터페이스는 Firepower Threat Defense 디바이스의 보조 관리 인터페이스입니다. 이 인터페이스를 사용하려면 Firepower Threat Defense CLI에서 해당 IP 주소 및 기타 파라미터를 구성해야 합니다. 예를 들어, 이벤트(예: 웹 이벤트)와 관리 트래픽을 구분할 수 있습니다 Firepower Management Center 명령 참조에서 **configure network** 명령을 참조하십시오.  
새시 간 클러스터링의 경우, 각 새시에 동일한 이벤트 인터페이스를 추가합니다.
- 단계 5** **Logical Devices(논리적 디바이스)**를 선택하여 **Logical Devices(논리적 디바이스)** 페이지를 엽니다. **Logical Devices(논리적 디바이스)** 페이지에는 새시에 구성된 논리적 디바이스의 목록이 표시됩니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
- 단계 6** **Add Device(디바이스 추가)**를 클릭하여 **Add Device(디바이스 추가)** 대화 상자를 엽니다. 기존의 논리적 디바이스가 있는 경우, 디바이스를 제거하고 새로 추가하라는 프롬프트가 표시됩니다. 디바이스의 모든 컨피그레이션은 새 정보로 대체됩니다.



**단계 7 Device Name(디바이스 이름)**에 논리적 디바이스의 이름을 제공합니다. 이 이름은 Firepower 4100/9300 새시 수퍼바이저가 클러스터링/관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 논리적 디바이스 컨피그레이션에 사용되는 클러스터 이름이 아닙니다.

**단계 8 Template(템플릿)**에서 **Cisco Firepower Threat Defense**를 선택합니다.


**단계 9 Image Version(이미지 버전)**의 경우 Firepower Threat Defense 소프트웨어 버전을 선택합니다. 이 버전이 FXOS 버전 및 Firepower Management Center 버전과 호환되는지 확인해야 합니다.

**단계 10 Device Mode(디바이스 모드)**에서 **Cluster(클러스터)** 라디오 버튼을 클릭합니다.

**단계 11 Create New Cluster(새 클러스터 생성)** 라디오 버튼을 클릭합니다.

**단계 12 OK(확인)**를 클릭합니다.

독립형 디바이스가 구성되어 있는 경우, 이 디바이스를 새 클러스터로 교체하라는 프롬프트가 표시됩니다. **Provisioning - device name(프로비저닝 - 디바이스 이름)** 창이 표시됩니다.

모든 인터페이스는 클러스터에 기본적으로 할당되어 있습니다. 하드웨어 우회 가능 포트는 다음 아이콘을 사용하여 표시됩니다. . 하드웨어 우회 쌍에서 두 인터페이스를 할당하지 않을 경우, 할당을 의도적으로 설정하기 위한 경고 메시지가 표시됩니다. 하드웨어 우회 기능을 사용할 필요가 없으므로 원하는 경우 단일 인터페이스를 할당할 수 있습니다. 하드웨어 바이패스 포트는 EtherChannel 멤버로 지원되지 않으므로 새시 간 클러스터링에서 지원되지 않습니다.

**단계 13** 화면 중앙의 디바이스 아이콘을 클릭합니다.

**Cisco Firepower Threat Defense Configuration(Cisco Firepower Threat Defense 컨피그레이션)** 대화상자가 나타납니다.

**단계 14 Cluster Information(클러스터 정보)** 탭에서 다음 작업을 수행합니다.

- a) **Chassis ID(새시 ID)** 필드에 새시 ID를 입력합니다. 클러스터의 각 새시는 고유 ID를 사용해야 합니다.
- b) **Cluster Key(클러스터 키)** 필드에서 클러스터 제어 링크의 제어 트래픽에 대한 인증 키를 구성합니다.  
공유 비밀은 1~63자로 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.
- c) **Cluster Group Name(클러스터 그룹 이름)**(논리적 디바이스 컨피그레이션의 클러스터 그룹 이름)을 설정합니다.  
이름은 1~38자로 된 ASCII 문자열이어야 합니다.
- d) **Management Interface(관리 인터페이스)** 드롭다운 목록에서 논리적 디바이스에 사용할 관리 인터페이스를 선택합니다.  
하드웨어 우회 가능 인터페이스를 관리 인터페이스로 할당할 경우, 할당을 의도적으로 설정하기 위한 경고 메시지가 표시됩니다.

**단계 15 Settings(설정)** 탭에서 다음 작업을 수행합니다.

- a) 등록하는 동안 Firepower Management Center와 클러스터 멤버 간에 공유할 키를 **Registration Key(등록 키)** 필드에 입력합니다.
- b) **Password(비밀번호)** 필드에 클러스터의 관리 사용자 비밀번호를 입력합니다.
- c) **Firepower Management Center IP** 필드에 Firepower Management Center를 관리하기 위한 IP 주소를 입력합니다.

- d) **Search Domains**(검색 도메인) 필드에 관리 네트워크의 검색 도메인 목록을 쉼표로 구분하여 입력합니다.
- e) **Firewall Mode**(방화벽 모드) 드롭다운 목록에서 **Transparent**(투명) 또는 **Routed**(라우팅됨)를 선택합니다.
- f) **DNS Servers**(DNS 서버) 필드에 Firepower Threat Defense 디바이스가 관리 네트워크에서 사용해야 하는 DNS 서버 목록을 쉼표로 구분하여 입력합니다.
- g) **Fully Qualified Hostname**(정규화된 호스트 이름) 필드에 Firepower Threat Defense 디바이스의 정규화된 이름을 입력합니다.
- h) **Eventing Interface**(이벤트 인터페이스) 드롭다운 목록에서 Firepower 이벤트가 전송되어야 할 인터페이스를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다. Firepower 이벤트에 사용할 별도의 인터페이스를 지정하려면 인터페이스를 *Firepower* 이벤트 인터페이스로 구성해야 합니다. 하드웨어 우회 가능 인터페이스를 이벤트 인터페이스로 할당할 경우, 의도적으로 할당하려는 것인지를 확인하기 위한 경고 메시지가 표시됩니다.

단계 16 **Interface Information**(인터페이스 정보) 탭에서 클러스터에 있는 각 보안 모듈의 관리 IP 주소를 구성합니다. **Address Type**(주소 유형) 드롭다운 목록에서 주소 유형을 선택한 다음 각 보안 모듈에 대해 다음 작업을 수행합니다.

**참고** 모듈을 설치하지 않은 경우에도 새시에 있는 3개의 모듈 슬롯 모두에 대해 IP 주소를 설정해야 합니다. 3개의 모듈을 모두 구성하지 않은 경우, 클러스터가 나타나지 않습니다.

- a) **Management IP**(관리 IP) 필드에서 IP 주소를 구성합니다.  
각 모듈에 동일한 네트워크의 IP 주소를 지정합니다.
- b) **Network Mask**(네트워크 마스크) 또는 **Prefix Length**(접두사 길이)를 입력합니다.
- c) **Network Gateway**(네트워크 게이트웨이) 주소를 입력합니다.

단계 17 **Agreement**(계약) 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 18 **OK**(확인)를 클릭하여 **Cisco Firepower Threat Defense Configuration**(Cisco Firepower Threat Defense 컨피그레이션) 대화 상자를 닫습니다.

단계 19 **Save**(저장)를 클릭합니다.

Firepower 4100/9300 새시 관리자(Supervisor)는 지정된 소프트웨어 버전을 다운로드하고 클러스터 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 각 보안 모듈에 입력하여 클러스터를 구축합니다.

단계 20 새시 간 클러스터링의 경우, 다음 새시를 클러스터에 추가합니다.

- a) 첫 번째 새시 Firepower Chassis Manager에서 오른쪽 상단에 있는 **Show Cluster Detail**(클러스터 세부사항 표시) 아이콘을 클릭하여 표시된 클러스터 컨피그레이션을 복사합니다.
- b) 다음 새시에 있는 Firepower Chassis Manager에 연결하고 이 절차에 따라 논리적 디바이스를 추가합니다.
- c) **Join an Existing Cluster**(기존 클러스터에 조인)를 선택합니다.
- d) **Copy config**(컨피그레이션 복사) 확인란을 클릭하고 **OK**(확인)를 클릭합니다. 이 확인란을 선택하지 않은 경우, 수동으로 첫 번째 새시 컨피그레이션에 맞게 설정을 입력해야 합니다.
- e) **Copy Cluster Details**(클러스터 세부사항 복사) 상자에서 첫 번째 새시의 클러스터 컨피그레이션에 붙여 넣고 **OK**(확인)를 클릭합니다.

f) 화면 중앙의 디바이스 아이콘을 클릭합니다. 클러스터 정보가 대부분 미리 입력되어 있지만 다음 설정을 변경해야 합니다.

- **Chassis ID(새시 ID)** — 고유한 새시 ID를 입력합니다.
- **Cluster Key(클러스터 키)** — (미리 입력되지 않음) 동일한 클러스터 키를 입력합니다.
- **Management IP(관리 IP)** — 각 모듈의 관리 주소를 다른 클러스터 멤버와 동일한 네트워크에 있는 고유한 IP 주소로 변경합니다.

OK(확인)를 클릭합니다.

g) **Save(저장)**를 클릭합니다.

단계 21 관리 IP 주소를 사용하여 각 유닛을 Firepower Management Center에 개별적으로 추가한 다음 웹 인터페이스에서 클러스터로 그룹화합니다.

모든 클러스터 유닛은 Firepower Management Center에 추가하기 전에 FXOS에서 성공적으로 구성된 클러스터에 있어야 합니다.

## 사이트 간 클러스터링 예시

다음 예에는 지원되는 클러스터 구축에 대한 내용이 나와 있습니다.

### Spanned EtherChannel 투명 모드 북-남 사이트 간 예시

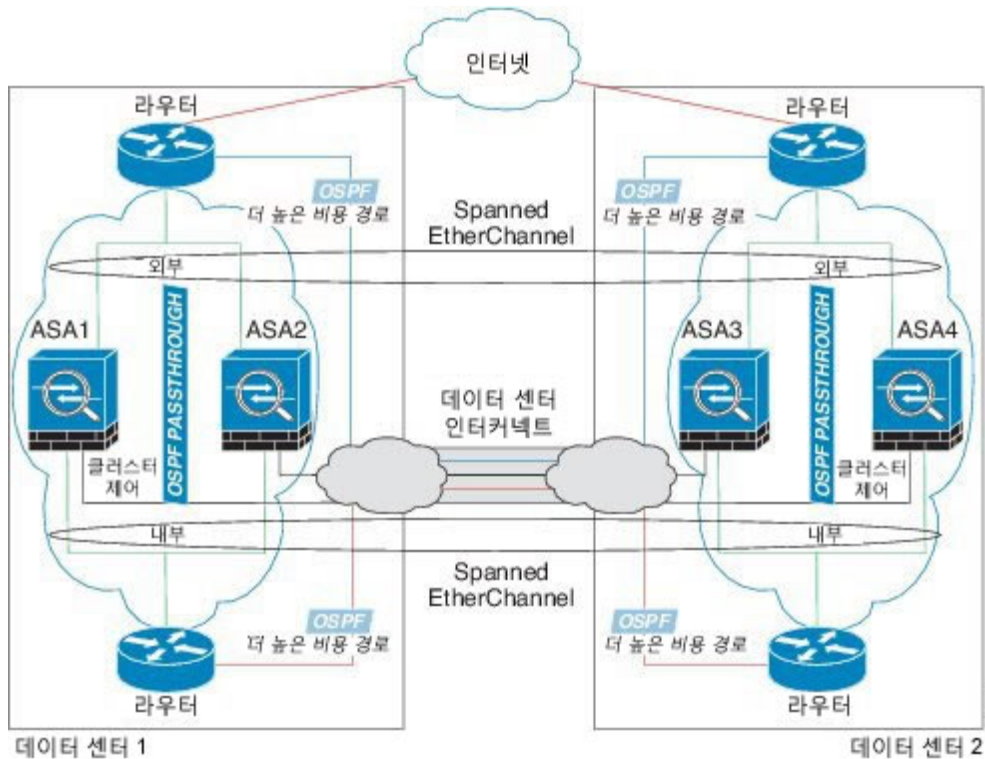
다음 예에서는 내부 라우터와 외부 라우터의 사이에 위치(북-남 삽입)한 2개 데이터 센터 각각에 2개의 클러스터 멤버가 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부용 Spanned EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 새시에 있습니다.

각 데이터 센터의 내부 및 외부 라우터는 투명 ASA를 통과하는 OSPF를 사용합니다. MAC과 달리 라우터 IP는 모든 라우터에서 고유합니다. DCI 전반에 비용이 높은 경로를 할당하면 특정 사이트의 모든 클러스터 멤버가 다운되지 않는 한 각 데이터 센터 내에서 트래픽이 유지됩니다. ASA를 통과하는 비용이 낮은 경로의 경우, 클러스터의 각 사이트에 있는 동일한 브리지 그룹을 거쳐 비대칭 연결을 유지해야 합니다. 어떤 사이트의 모든 클러스터 멤버에 장애가 발생하는 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** — 이 시나리오의 경우 데이터 센터 1에 하나의 스위치를 설치하고, 나머지 하나는 데이터 센터 2에 설치합니다. 각 데이터 센터의 클러스터 유닛에 사용할 수 있는 한 가지 옵션은 로컬 스위치에만 연결하는 한편, VSS/vPC 트래픽이 DCI를 통과하도록 하는 것입니다. 이 경우 연결의 대부분은 각 데이터 센터에 로컬로 저장됩니다. DCI에서 추가 트래픽을 처리할 수 있는 경우, 선택적으로 DCI 전반의 두 스위치에 각 유닛을 연결할 수 있습니다. 이 경우 트래픽이 데이터 센터 전반에 분산되므로 DCI의 성능이 매우 뛰어나야 합니다.

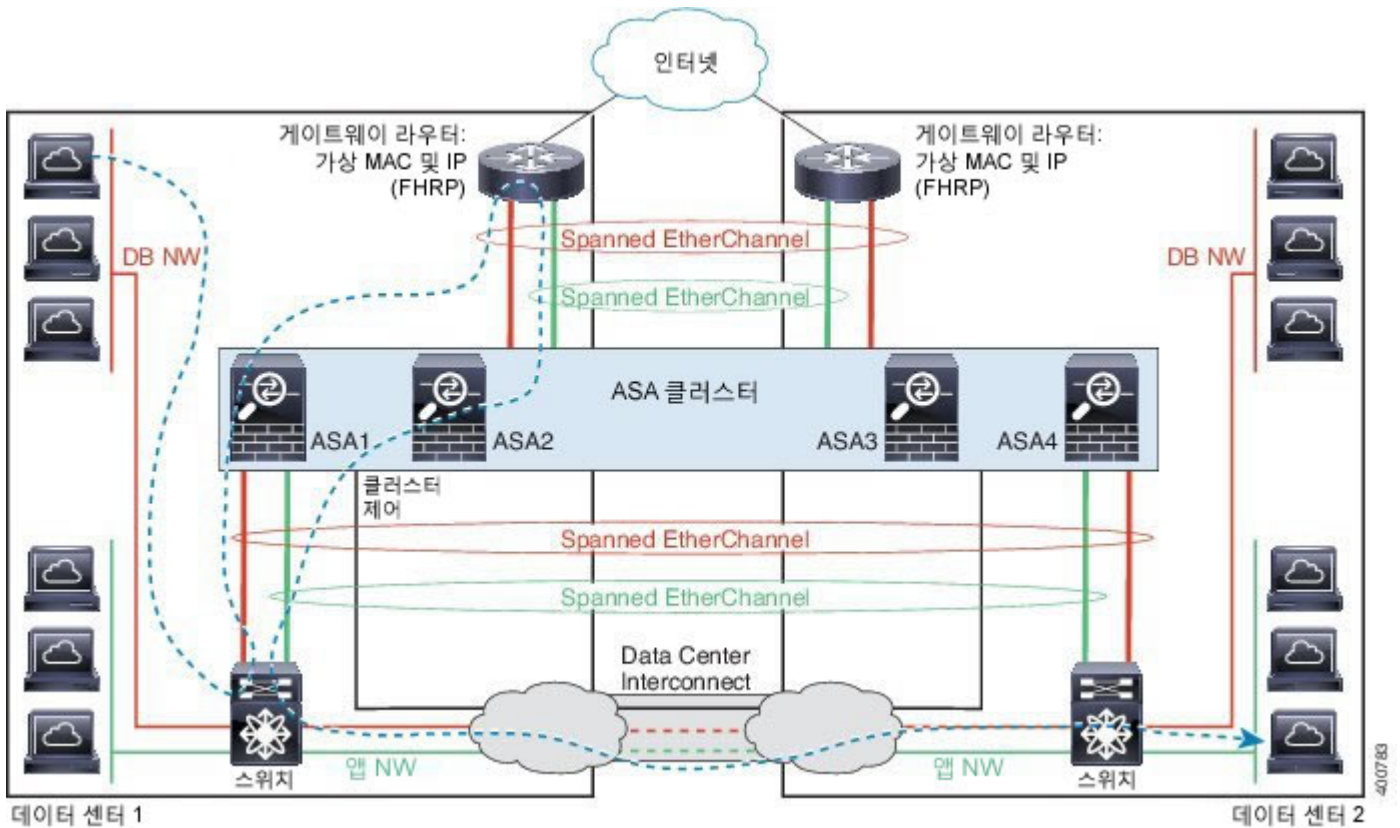
- 각 사이트의 로컬 VSS/vPC — 스위치 이중화를 개선하기 위해 각 사이트에 별도의 VSS/vPC 쌍을 2개씩 설치할 수 있습니다. 이 경우 여전히 클러스터 유닛의 Spanned EtherChannel은 두 로컬 스위치에만 연결된 데이터 센터 1 새시 및 이 로컬 스위치에 연결된 데이터 센터 2 새시로 이루어져 있으나, 사실상 Spanned EtherChannel은 "분리"되어 있습니다. 각 로컬 VSS/vPC에서는 Spanned EtherChannel을 사이트-로컬 EtherChannel로 간주합니다.



### Spanned EtherChannel 투명 모드 동-서 사이트 간 예시

다음 예에서는 게이트웨이 라우터와 각 사이트의 두 내부 네트워크, 즉 애플리케이션 네트워크 및 DB 네트워크의 사이에 위치(동-서 삽입)한 2개 데이터 센터 각각에 2개의 클러스터 멤버가 있습니다. 클러스터 멤버는 DCI를 통해 클러스터 제어 링크로 연결됩니다. 각 사이트의 클러스터 멤버는 내부 및 외부의 애플리케이션 네트워크와 DB 네트워크에서 Spanned EtherChannel을 사용하여 로컬 스위치에 연결됩니다. 각 EtherChannel은 클러스터의 모든 새시에 있습니다.

각 사이트의 게이트웨이 라우터는 HSRP와 같은 FHRP를 사용하여 각 사이트에 동일한 대상 가상 MAC 및 IP 주소를 제공합니다. 의도하지 않은 MAC 주소 플래깅을 방지하기 위한 좋은 방법은 게이트웨이 라우터의 실제 MAC 주소를 ASA MAC 주소 테이블에 정적으로 추가하는 것입니다. 이 항목이 없으면 사이트 1의 게이트웨이가 사이트 2의 게이트웨이와 통신할 경우, 해당 트래픽이 ASA를 통과하고 내부 인터페이스에서 사이트 2에 도달하려고 시도하여 문제가 발생할 수 있습니다. 데이터 VLAN은 OTV(Overlay Transport Virtualization)(또는 유사한 것)를 사용하여 사이트 간에 확장됩니다. 트래픽이 게이트웨이 라우터로 향할 때 DCI를 통과하여 반대쪽 사이트에 가지 않도록 필터를 추가해야 합니다. 어떤 사이트의 게이트웨이 라우터가 연결할 수 없게 되면 트래픽이 다른 사이트의 게이트웨이 라우터에 전송될 수 있도록 필터를 제거해야 합니다.



vPC/VSS 옵션에 대한 자세한 내용은 [Spanned EtherChannel 투명 모드 북-남 사이트 간 예시](#), 153 페이지의 내용을 참조하십시오.

## 클러스터링 기록

| 기능 이름                                                     | 플랫폼 릴리스 | 기능 정보                                                                                                                                                |
|-----------------------------------------------------------|---------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cisco ASA를 위한 내장 새시 클러스터링                                 | 1.1.1   | Firepower 9300 새시 내에서 모든 ASA 보안 모듈을 클러스터링할 수 있습니다.<br>추가된 화면: <b>Logical Devices</b> (논리적 디바이스) > <b>Configuration</b> (컨피그레이션)                      |
| 6개의 ASA 모듈을 위한 새시 간 클러스터링                                 | 1.1.3   | 이제 ASA를 위한 새시 간 클러스터링을 활성화할 수 있습니다. 최대 6개의 새시에 최대 6개의 모듈을 포함할 수 있습니다.<br>수정된 화면: <b>Logical Devices</b> (논리적 디바이스) > <b>Configuration</b> (컨피그레이션)   |
| Firepower 9300의 Firepower Threat Defense에서 내장 새시 클러스터링 지원 | 1.1.4   | Firepower 9300은 Firepower Threat Defense 애플리케이션이 있는 내장 새시 클러스터링을 지원합니다.<br>수정된 화면: <b>Logical Devices</b> (논리적 디바이스) > <b>Configuration</b> (컨피그레이션) |

| 기능 이름                                          | 플랫폼 릴리스 | 기능 정보                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Firepower 4100/9300 새시의 ASA에 대한 새시 간 클러스터링 개선  | 2.1.1   | 이제 ASA 클러스터를 구축할 때 각 Firepower 4100/9300 새시에 대해 사이트 ID를 구성할 수 있습니다. 이전에는 ASA 애플리케이션 내에서 사이트 ID를 구성해야 했습니다. 이 새로운 기능 덕분에 초기 구축이 쉬워졌습니다. 사이트 ID는 더 이상 ASA 컨피그레이션 내에서 설정할 수 없습니다. 또한, 사이트 간 클러스터링과의 최고의 호환성을 위해 ASA 9.7(1)과 FXOS 2.1.1로 업그레이드하는 것이 좋습니다. 이 업그레이드에는 안정성과 성능에 대한 여러 가지 개선 사항이 포함되어 있습니다.<br>수정된 화면: <b>Logical Devices</b> (논리적 디바이스) > <b>Configuration</b> (컨피그레이션) |
| 6개의 Firepower Threat Defense 모듈을 위한 새시 간 클러스터링 | 2.1.1   | 이제 Firepower Threat Defense를 위한 새시 간 클러스터링을 활성화할 수 있습니다. 최대 6개의 새시에 최대 6개의 모듈을 포함할 수 있습니다.<br>수정된 화면: <b>Logical Devices</b> (논리적 디바이스) > <b>Configuration</b> (컨피그레이션)                                                                                                                                                                                                          |

## 서비스 체이닝 구성

Cisco Firepower 4100/9300 새시는 단일 블레이드에서 여러 서비스(예: 방화벽 및 서드파티 DDoS 애플리케이션)를 지원할 수 있습니다. 이러한 애플리케이션 및 서비스를 함께 연결하면 서비스 체인을 구성할 수 있습니다.

## 서비스 체이닝 정보

현재 지원되는 서비스 체이닝 컨피그레이션에서 서드파티 Radware DefensePro 가상 플랫폼은 ASA 방화벽보다 먼저 실행되거나 Firepower Threat Defense보다 먼저 실행되도록 설치될 수 있습니다. Radware DefensePro는 Firepower 4100/9300 새시에서 DDoS(Distributed Denial-of-Service) 탐지 및 완화 기능을 제공하는 KVM 기반 가상 플랫폼입니다. 서비스 체이닝이 Firepower 4100/9300 새시에서 활성화된 경우, 네트워크의 트래픽은 기본 ASA 또는 Firepower Threat Defense 방화벽에 도달하기 전에 먼저 DefensePro 가상 플랫폼을 통과해야 합니다.

Radware DefensePro 가상 플랫폼은 *Radware vDP*(가상 DefensePro) 또는 간단하게 *vDP*라고도 합니다. Radware DefensePro 가상 플랫폼은 경우에 따라 링크 테크레이터라고도 합니다.

## 서비스 체이닝 사전 요구 사항

Firepower 4100/9300 새시에서 Radware DefensePro를 구축하기 전에 Firepower 4100/9300 새시가 **etc/UTC** 표준 시간대와 함께 NTP 서버를 사용하도록 구성해야 합니다. Firepower 4100/9300 새시의 날짜 및 시간 설정에 대한 자세한 내용은 [날짜 및 시간 설정, 85 페이지](#)의 내용을 참조하십시오.

## 서비스 체이닝 지침

### 모델

- Radware DefensePro 플랫폼은 Firepower 9300 보안 어플라이언스에서만 지원됩니다.
- Radware DefensePro 플랫폼은 다음 보안 어플라이언스의 Firepower Threat Defense에 지원됩니다.
  - Firepower 9300
  - Firepower 4110 - 데코레이터를 논리적 디바이스로 동시에 구축해야 합니다. 논리적 디바이스를 이 디바이스에서 이미 구성한 후에는 데코레이터를 설치할 수 없습니다.
  - Firepower 4120 - 데코레이터를 논리적 디바이스로 동시에 구축해야 합니다. 논리적 디바이스를 이 디바이스에서 이미 구성한 후에는 데코레이터를 설치할 수 없습니다.
  - Firepower 4140
  - Firepower 4150

### 추가 지침

- 서비스 체이닝은 새시 간 클러스터 컨피그레이션에서 지원되지 않습니다. 그러나 Radware DefensePro 애플리케이션은 새시 간 클러스터 시나리오의 독립형 컨피그레이션에서 구축할 수 있습니다.
- DefensePro 애플리케이션은 최대 3개의 보안 모듈에서 별도의 인스턴스로 실행할 수 있습니다.

## 독립형 논리적 디바이스에 Radware DefensePro 서비스 체인 구성

다음 절차에서는 Radware DefensePro를 독립형 ASA 또는 Firepower Threat Defense 논리적 디바이스보다 먼저 단일 서비스 체인에 설치하는 방법을 보여줍니다.



### 참고

Radware vDP를 Firepower 4120 또는 4140 보안 어플라이언스의 ASA보다 먼저 설치하는 경우, FXOS CLI를 사용하여 데코레이터를 구축해야 합니다. Radware DefensePro를 Firepower 4100 디바이스의 ASA보다 먼저 서비스 체인에 설치 및 구성하는 방법에 대한 전체 CLI 지침은 FXOS CLI 컨피그레이션 가이드를 참조하십시오.

### 시작하기 전에

- Cisco.com에서 vDP 이미지를 다운로드([Cisco.com에서 이미지 다운로드](#), 42 페이지 참조)한 다음 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다([Firepower Security Appliance에 이미지 업로드](#), 42 페이지 참조).

- 인트라 새시 클러스터의 독립형 컨피그레이션에서 Radware DefensePro 애플리케이션을 구축할 수 있습니다. 인트라 새시 클러스터링에 대해서는 [인트라 새시 클러스터에 Radware DefensePro 서비스 체인 구성, 159 페이지](#)의 내용을 참조하십시오.

## 절차

- 
- 단계 1 vDP에 대해 별도의 관리 인터페이스를 사용하려는 경우 [인터페이스 속성 편집, 126 페이지](#)에 따라 인터페이스를 활성화하고 관리 유형으로 설정합니다. 그렇지 않으면 애플리케이션 관리 인터페이스를 공유할 수 있습니다.
  - 단계 2 **Logical Devices**(논리적 디바이스)를 선택하여 **Logical Devices**(논리적 디바이스) 페이지를 엽니다. **Logical Devices**(논리적 디바이스) 페이지에는 새시에 구성된 논리적 디바이스의 목록이 표시됩니다. 논리적 디바이스가 구성되어 있지 않은 경우, 이를 알리는 메시지가 표시됩니다.
  - 단계 3 독립형 ASA 또는 Firepower Threat Defense 논리적 디바이스([독립형 ASA 논리적 디바이스 생성, 133 페이지](#) 또는 [독립형 위협 방어 논리적 디바이스 생성, 135 페이지](#) 참조)를 생성합니다.
  - 단계 4 **Decorators**(데코레이터) 영역에서 vDP를 선택합니다. Radware: Virtual DefensePro - Configuration(Radware: Virtual DefensePro - 컨피그레이션) 창이 나타납니다. **General Information**(일반 정보) 탭에서 다음 필드를 구성합니다.
  - 단계 5 둘 이상의 vDP 버전을 Firepower 4100/9300 새시에 업로드한 경우, 사용할 버전을 **Version**(버전) 드롭다운에서 선택합니다.
  - 단계 6 **Management Interface**(관리 인터페이스) 드롭다운에서 이 절차의 1단계에서 생성한 관리 인터페이스를 선택합니다.
  - 단계 7 기본 **Address Type**(주소 유형)을 IPv4 only(IPv4 전용), IPv6 only(IPv6 전용) 또는 IPv4 and IPv6(IPv4 및 IPv6) 중에서 선택합니다.
  - 단계 8 다음 필드를 구성합니다. 필드는 이전 단계에서 선택한 **Address Type**(주소 유형)에 따라 달라집니다.
    - a) **Management IP**(관리 IP) 필드에서 로컬 IP 주소를 구성합니다.
    - b) IPv4 전용: **Network Mask**(네트워크 마스크)를 입력합니다.  
IPv6 전용: **Prefix Length**(접두사 길이)를 입력합니다.
    - c) **Network Gateway**(네트워크 게이트웨이) 주소를 입력합니다.
  - 단계 9 디바이스에 할당할 각 데이터 포트 옆에 있는 확인란을 클릭합니다.
  - 단계 10 **OK**(확인)를 클릭합니다.
  - 단계 11 **Save**(저장)를 클릭합니다.  
Firepower eXtensible 운영 체제에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈에 입력하여 논리적 디바이스를 구축합니다.
-



## 인트라 새시 클러스터에 Radware DefensePro 서비스 체인 구성

다음 절차에서는 Radware DefensePro 이미지를 설치하고 이 이미지를 ASA 또는 Firepower Threat Defense 인트라 새시 클러스터보다 먼저 서비스 체인에 구성하는 방법을 보여줍니다.

### 시작하기 전에

- Cisco.com에서 vDP 이미지를 다운로드([Cisco.com에서 이미지 다운로드](#), 42 페이지 참조)한 다음 해당 이미지를 Firepower 4100/9300 새시에 업로드합니다([Firepower Security Appliance에 이미지 업로드](#), 42 페이지 참조).

### 절차

- 단계 1 vDP에 대해 별도의 관리 인터페이스를 사용하려는 경우 [인터페이스 속성 편집](#), 126 페이지에 따라 인터페이스를 활성화하고 관리 유형으로 설정합니다. 그렇지 않으면 애플리케이션 관리 인터페이스를 공유할 수 있습니다.
- 단계 2 ASA 또는 Firepower Threat Defense 인트라 새시 클러스터([ASA 클러스터링 구성](#), 147 페이지 또는 [Firepower Threat Defense 클러스터링 구성](#), 149 페이지 참조)를 구성합니다. 인트라 새시 클러스터를 구성하는 마지막 절차에서 **Save(저장)**를 클릭하기 전에 먼저 다음 단계를 수행하여 vDP 테코레이터를 클러스터에 추가해야 합니다.
- 단계 3 **Decorators(테코레이터)** 영역에서 vDP를 선택합니다. **Radware: Virtual DefensePro - Configuration(Radware: Virtual DefensePro - 컨피그레이션)** 대화 상자가 나타납니다. **General Information(일반 정보)** 탭에서 다음 필드를 구성합니다.
- 단계 4 둘 이상의 vDP 버전을 Firepower 4100/9300 새시에 업로드한 경우, 사용할 vDP 버전을 **Version(버전)** 드롭다운에서 선택합니다.
- 단계 5 **Management Interface(관리 인터페이스)** 드롭다운에서 관리 인터페이스를 선택합니다.
- 단계 6 vDP 테코레이터에 할당할 각 데이터 포트 옆에 있는 확인란을 클릭합니다.
- 단계 7 **Interface Information(인터페이스 정보)** 탭을 클릭합니다.
- 단계 8 사용할 **Address Type(주소 유형)**을 IPv4 only(IPv4 전용), IPv6 only(IPv6 전용) 또는 IPv4 and IPv6(IPv4 및 IPv6) 중에서 선택합니다.
- 단계 9 각 보안 모듈에 대해 다음 필드를 구성합니다. 표시되는 필드는 이전 단계에서 선택한 **Address Type(주소 유형)**에 따라 달라집니다.
  - a) **Management IP(관리 IP)** 필드에서 로컬 IP 주소를 구성합니다.
  - b) IPv4 전용: **Network Mask(네트워크 마스크)**를 입력합니다.  
IPv6 전용: **Prefix Length(접두사 길이)**를 입력합니다.
  - c) **Network Gateway(네트워크 게이트웨이)** 주소를 입력합니다.
- 단계 10 **OK(확인)**를 클릭합니다.
- 단계 11 **Save(저장)**를 클릭합니다.  
Firepower eXtensible 운영 체제에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈에 입력하여 논리적 디바이스를 구축합니다.

- 단계 12 **Logical Devices**(논리적 디바이스)를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.
- 단계 13 구성된 논리적 디바이스 목록에서 vDP 항목으로 스크롤합니다. **Management IP(관리 IP)** 옆에 나열된 해당 특성을 확인합니다.

- **CLUSTER-ROLE** 요소가 DefensePro 인스턴스에 대해 *unknown*(알 수 없음)으로 표시되는 경우, DefensePro 애플리케이션을 시작하고 마스터 IP 주소를 구성하여 vDP 클러스터 생성을 완료해야 합니다.
- **CLUSTER-ROLE** 요소가 DefensePro 인스턴스에 대해 *primary*(기본) 또는 *secondary*(보조)로 표시되는 경우, 애플리케이션은 온라인 상태이며 클러스터에 구성되어 있습니다.

## UDP/TCP 포트 열기 및 vDP 웹 서비스 활성화

Radware APSolute Vision Manager 인터페이스는 다양한 UDP/TCP 포트를 사용하여 Radware vDP 애플리케이션과 통신합니다. vDP 애플리케이션이 APSolute Vision Manager와 통신하기 위해서는 이러한 포트에 액세스할 수 있으며 포트가 방화벽에 의해 차단되지 않음을 확인해야 합니다. 열어야 할 특정 포트에 대한 자세한 내용은 APSolute Vision 사용자 가이드의 다음 표를 참조하십시오.

- **APSolute Vision Server-WBM** 통신용 포트 및 운영 체제
- **Radware** 디바이스를 사용하는 **APSolute Vision Server**용 통신 포트

Radware APSolute Vision이 FXOS 새시에 구축된 Virtual DefensePro 애플리케이션을 관리하기 위해서는 FXOS CLI를 사용하여 vDP 웹 서비스를 활성화해야 합니다.

### 절차

- 단계 1 FXOS CLI에서 vDP 애플리케이션 인스턴스에 연결합니다.
- ```
connect module slotconsole
connect vdp
```
- 단계 2 vDP 웹 서비스를 활성화합니다.
- ```
manage secure-web status set enable
```
- 단계 3 vDP 애플리케이션 콘솔을 종료하고 FXOS 모듈 CLI로 돌아갑니다.
- ```
Ctrl ]
```

논리적 디바이스 관리

논리적 디바이스를 삭제하고, ASA를 투명 모드로 변환하고, 인터페이스 컨피그레이션을 변경할 수 있으며 기존의 논리적 디바이스에서 다른 작업을 수행할 수 있습니다.

애플리케이션 콘솔 또는 데코레이터에 연결

다음 절차를 사용하여 애플리케이션 또는 데코레이터 콘솔에 연결합니다.



참고

콘솔 액세스 시 문제가 발생한 경우, 다른 SSH 클라이언트를 시도하거나 SSH 클라이언트를 새 버전으로 업그레이드하는 것이 좋습니다.

절차

단계 1 애플리케이션 또는 데코레이터 콘솔에 연결하려면 다음을 수행합니다.

a) FXOS CLI에서 보안 모듈/엔진에 연결합니다.

```
Firepower-chassis # connectmodule slot_numberconsole
```

참고 여러 보안 모듈을 지원하지 않는 디바이스의 보안 엔진에 연결하려면 *slot_number*에 1을 사용합니다.

보안 모듈에 처음 연결하는 경우 FXOS 모듈 CLI에 액세스합니다.

b) 애플리케이션 또는 데코레이터에 연결하려면 디바이스에 적절한 명령을 입력합니다. Firepower-module1>**connect asa**

```
Firepower-module1>connect ftd
```

```
Firepower-module1>connect vdp
```

FXOS CLI의 슈퍼바이저 레벨에서 보안 모듈/엔진에 대한 후속 연결은 보안 모듈/엔진 OS에 직접 액세스됩니다.=

단계 2 (선택 사항) **Ctrl-A-D**를 입력하여 FXOS 모듈 CLI에 대한 애플리케이션 콘솔을 종료합니다.

Ctrl-]를 입력하여 FXOS 모듈 CLI에 대한 데코레이터 콘솔을 종료합니다.

트러블슈팅을 위해 FXOS 모듈 CLI에 액세스할 수 있습니다.

단계 3 FXOS CLI의 슈퍼바이저 레벨로 돌아갑니다.

a) 보안 모듈/엔진 콘솔을 종료하려면 ~를 입력합니다.

텔넷 애플리케이션을 종료합니다.

b) 텔넷 애플리케이션을 종료하려면 다음을 입력합니다.

```
telnet>quit
```

예

다음 예에서는 보안 모듈 1에 있는 ASA에 연결한 다음 종료하여 FXOS CLI의 슈퍼바이저 레벨로 다시 돌아갑니다.

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa
asa> ~
telnet> quit
Connection closed.
Firepower#
```

논리적 디바이스 삭제

절차

-
- 단계 1 **Logical Devices**(논리적 디바이스)를 선택하여 **Logical Devices**(논리적 디바이스) 페이지를 엽니다. **Logical Devices**(논리적 디바이스) 페이지에는 새시에 구성된 논리적 디바이스의 목록이 표시됩니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
 - 단계 2 삭제할 논리적 디바이스에 대해 **Delete**(삭제)를 클릭합니다.
 - 단계 3 **Yes**(예)를 클릭하여 논리적 디바이스를 삭제할 것을 확인합니다.
 - 단계 4 **Yes**(예)를 클릭하여 애플리케이션 컨피그레이션을 삭제할 것을 확인합니다.
-

논리적 디바이스와 연결되지 않은 애플리케이션 인스턴스 삭제

논리적 디바이스를 삭제하는 경우, 논리적 디바이스에 대한 애플리케이션 컨피그레이션도 삭제할지를 묻는 프롬프트가 표시됩니다. 애플리케이션 컨피그레이션을 삭제하지 않는 경우, 해당 애플리케이션 인스턴스를 삭제할 때까지 다른 애플리케이션을 사용하여 논리적 디바이스를 생성할 수 없습니다. 애플리케이션 인스턴스가 더 이상 논리적 디바이스와 연결된 상태가 아닌 경우 다음 절차를 사용하여 보안 모듈/엔진에서 애플리케이션 인스턴스를 삭제할 수 있습니다.

절차

-
- 단계 1 **Logical Devices**(논리적 디바이스)를 선택하여 **Logical Devices**(논리적 디바이스) 페이지를 엽니다. **Logical Devices**(논리적 디바이스) 페이지에는 새시에 구성된 논리적 디바이스의 목록이 표시됩니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다. 논리적 디바이스 목록 아래에서 논리적 디바이스와 연결되어 있지 않은 애플리케이션 인스턴스 목록을 확인할 수 있습니다.

단계 2 삭제할 애플리케이션 인스턴스에 대해 **Delete**(삭제)를 클릭합니다.

단계 3 **Yes**(예)를 클릭하여 애플리케이션 인스턴스를 삭제할 것을 확인합니다.

ASA를 투명 방화벽 모드로 변경

Firepower 4100/9300 새시에서 라우팅된 방화벽 모드 ASA만 구축할 수 있습니다. ASA를 투명 방화벽 모드로 변경하려면 초기 구축을 완료한 다음 ASA CLI 내에서 방화벽 모드를 변경합니다. 방화벽 모드를 변경하면 컨피그레이션이 지워지므로 Firepower 4100/9300 새시에서 컨피그레이션을 재구축하여 부트스트랩 컨피그레이션을 다시 확보해야 합니다. 그러면 ASA는 작업 부트스트랩 컨피그레이션에서 투명 모드로 유지됩니다.

절차

단계 1 애플리케이션 콘솔 또는 데코레이터에 연결, 161 페이지에 따라 ASA 콘솔에 연결합니다. 클러스터의 경우 기본 유닛에 연결합니다. 장애 조치 쌍의 경우 활성화된 유닛에 연결합니다.

단계 2 컨피그레이션 모드를 시작합니다.

enable

configure terminal

기본적으로 enable 비밀번호는 비어 있습니다.

단계 3 방화벽 모드를 투명으로 설정합니다.

firewall transparent

단계 4 컨피그레이션을 저장합니다.

write memory

클러스터 또는 장애 조치 쌍의 경우 이 컨피그레이션이 보조 유닛에 복제됩니다.

```
asa(config)# firewall transparent
asa(config)# write memory
Building configuration...
Cryptochecksum: 9f831dfb 60dffa8c 1d939884 74735b69

3791 bytes copied in 0.160 secs
[OK]
asa(config)#
Beginning configuration replication to Slave unit-1-2
End Configuration Replication to slave.

asa(config)#
```

단계 5 Firepower Chassis Manager **Logical Devices**(논리적 디바이스) 페이지에서 **Edit**(편집) 아이콘을 클릭하여 ASA를 편집합니다.

Provisioning(프로비저닝) 페이지가 나타납니다.

- 단계 6** 디바이스 아이콘을 클릭하여 부트스트랩 컨피그레이션을 편집합니다. 컨피그레이션에서 값을 변경하고 **OK(확인)**를 클릭합니다.
 하나 이상의 필드 값을 변경해야 합니다. 이 설정은 중요하지 않으므로 **Password(비밀번호)**를 새 비밀번호로 변경하는 것이 좋습니다.
 부트스트랩 컨피그레이션 변경에 대한 경고가 표시되면 **Yes(예)**를 클릭합니다.
- 단계 7** **Save(저장)**를 클릭하여 컨피그레이션을 ASA에 재구축합니다. 새시 간 클러스터 또는 장애 조치 쌍의 경우, 5~7단계를 반복하여 각 새시에서 부트스트랩 컨피그레이션을 재구축합니다.
 몇 분 정도 기다리면 새시/보안 모듈이 다시 로드되며 ASA가 다시 작동됩니다. 이제 ASA은 부트스트랩 컨피그레이션이 적용되지만, 투명 모드로 유지됩니다.

Firepower Threat Defense 논리적 디바이스에서 인터페이스 변경

Firepower Threat Defense 논리적 디바이스에서 인터페이스를 할당 또는 할당 해제하거나 관리 인터페이스를 교체할 수 있습니다. 그러면 Firepower Management Center에서 인터페이스 컨피그레이션을 동기화할 수 있습니다.

시작하기 전에

- 인터페이스를 구성하고 **인터페이스 속성 편집, 126 페이지** 및 **포트 채널 생성, 127 페이지**에 따라 임의의 EtherChannels을 추가합니다.
- 논리적 디바이스에 영향을 미치거나 Firepower Management Center에서 동기화를 요구하지 않고 할당된 EtherChannel의 멤버십을 편집할 수 있습니다.
- 이미 할당된 인터페이스를 EtherChannel에 추가하려는 경우(예: 모든 인터페이스가 기본적으로 클러스터에 할당됨), 먼저 논리적 디바이스에서 인터페이스의 할당을 해제한 다음 해당 인터페이스를 EtherChannel에 추가해야 합니다. 새 EtherChannel의 경우, 그런 다음 EtherChannel을 디바이스에 할당할 수 있습니다.
- 관리 또는 Firepower 이벤트 인터페이스를 관리 EtherChannel로 교체하려는 경우, 최소 1개의 할당되지 않은 데이터 멤버 인터페이스가 있는 EtherChannel을 생성한 다음 현재 관리 인터페이스를 EtherChannel로 교체해야 합니다. Firepower Threat Defense 디바이스가 재부팅(관리 인터페이스 변경으로 인해 재부팅 발생)된 후 Firepower Management Center에서 컨피그레이션을 동기화하고 나면 현재 할당되지 않은 관리 인터페이스를 EtherChannel에도 추가할 수 있습니다.
- 클러스터링 또는 고가용성을 위해, Firepower Management Center에서 컨피그레이션을 동기화하기 전에 모든 유닛에서 인터페이스를 추가하거나 제거해야 합니다. 새 인터페이스는 관리가 다운된 상태에서 추가되므로 인터페이스 모니터링에는 영향을 미치지 않습니다.

절차

- 단계 1 Firepower Chassis Manager에서 **Logical Devices**(논리적 디바이스)를 선택합니다.
- 단계 2 오른쪽 상단에서 **Edit**(편집) 아이콘을 클릭하여 논리적 디바이스를 편집합니다.
- 단계 3 **Data Ports**(데이터 포트) 영역에서 인터페이스의 선택을 취소하여 데이터 인터페이스의 할당을 해제합니다.
- 단계 4 **Data Ports**(데이터 포트) 영역에서 인터페이스를 선택하여 새로운 데이터 인터페이스를 할당합니다.
- 단계 5 다음과 같이 관리 또는 이벤트 인터페이스를 교체합니다.
이러한 유형의 인터페이스의 경우 변경 사항을 저장하고 나면 디바이스가 재부팅됩니다.
- 페이지 중앙의 디바이스 아이콘을 클릭합니다.
 - General/Cluster Information**(일반/클러스터 정보) 탭의 드롭다운 목록에서 새로운 **Management Interface**(관리 인터페이스)를 선택합니다.
 - Settings**(설정) 탭의 드롭다운 목록에서 새로운 **Eventing Interface**(이벤트 인터페이스)를 선택합니다.
 - OK**(확인)를 클릭합니다.
- 관리 인터페이스의 IP 주소를 변경하는 경우 Firepower Management Center에서 디바이스의 IP 주소도 변경해야 합니다. **Devices**(디바이스) > **Device Management**(디바이스 관리) > **Device/Cluster**(디바이스/클러스터)로 이동합니다. **Management**(관리) 영역에서 부트스트랩 컨피그레이션 주소와 일치하도록 IP 주소를 설정합니다.
- 단계 6 **Save**(저장)를 클릭합니다.
- 단계 7 Firepower Management Center에 로그인합니다.
- 단계 8 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 선택하고 Firepower Threat Defense 디바이스의 편집 아이콘(🔧)을 클릭합니다. 기본적으로는 **Interfaces**(인터페이스) 탭이 선택됩니다.
- 단계 9 **Interfaces**(인터페이스) 탭의 왼쪽 상단에 있는 **Sync Interfaces from device**(디바이스에서 인터페이스 동기화) 버튼을 클릭합니다.
- 단계 10 **Save**(저장)를 클릭합니다.
이제 **Deploy**(구축)를 클릭하고 할당된 디바이스에 정책을 구축할 수 있습니다. 변경 사항은 구축할 때까지 활성화되지 않습니다.

ASA 논리적 디바이스에서 인터페이스 변경

ASA 논리적 디바이스에서 관리 인터페이스를 할당, 할당 해제 또는 교체할 수 있습니다. ASDM은 새로운 인터페이스를 자동으로 검색합니다.

시작하기 전에

- 인터페이스를 구성하고 **인터페이스 속성 편집**, 126 페이지 및 **포트 채널 생성**, 127 페이지에 따라 임의의 EtherChannels을 추가합니다.

- 논리적 디바이스에 영향을 미치지 않고 할당된 EtherChannel의 멤버십을 편집할 수 있습니다.
- 이미 할당된 인터페이스를 EtherChannel에 추가하려는 경우(예: 모든 인터페이스가 기본적으로 클러스터에 할당됨), 먼저 논리적 디바이스에서 인터페이스의 할당을 해제한 다음 해당 인터페이스를 EtherChannel에 추가해야 합니다. 새 EtherChannel의 경우, 그런 다음 EtherChannel을 디바이스에 할당할 수 있습니다.
- 관리 인터페이스를 관리 EtherChannel로 교체하려는 경우, 최소 1개의 할당되지 않은 데이터 멤버 인터페이스가 있는 EtherChannel을 생성한 다음 현재 관리 인터페이스를 EtherChannel로 교체해야 합니다. ASA가 다시 로드(관리 인터페이스 변경으로 인해 재로드 발생)되고 나면 현재 할당되지 않은 관리 인터페이스를 EtherChannel에도 추가할 수 있습니다.
- 클러스터링 또는 장애 조치의 경우 새 인터페이스는 관리가 다운된 상태에서 추가되므로 인터페이스 모니터링에는 영향을 미치지 않습니다.

절차

-
- 단계 1 Firepower Chassis Manager에서 **Logical Devices**(논리적 디바이스)를 선택합니다.
 - 단계 2 오른쪽 상단에서 **Edit**(편집) 아이콘을 클릭하여 논리적 디바이스를 편집합니다.
 - 단계 3 **Data Ports**(데이터 포트) 영역에서 인터페이스의 선택을 취소하여 데이터 인터페이스의 할당을 해제합니다.
 - 단계 4 **Data Ports**(데이터 포트) 영역에서 인터페이스를 선택하여 새로운 데이터 인터페이스를 할당합니다.
 - 단계 5 관리 인터페이스를 다음과 같이 교체합니다.
이 유형의 인터페이스의 경우 변경 사항을 저장하고 나면 디바이스가 다시 로드됩니다.
 - a) 페이지 중앙의 디바이스 아이콘을 클릭합니다.
 - b) **General/Cluster Information**(일반/클러스터 정보) 탭의 드롭다운 목록에서 새로운 **Management Interface**(관리 인터페이스)를 선택합니다.
 - c) **OK**(확인)를 클릭합니다.
 - 단계 6 **Save**(저장)를 클릭합니다.
-



11 장

보안 모듈/엔진 관리

- [FXOS 보안 모듈/보안 엔진 정보, 167페이지](#)
- [보안 모듈 서비스 해제/서비스 다시 시작, 169페이지](#)
- [보안 모듈/엔진 승인, 169페이지](#)
- [보안 모듈/엔진 재설정, 170페이지](#)
- [보안 모듈/엔진 재초기화, 170페이지](#)
- [보안 모듈/엔진 전원 켜기/끄기, 171페이지](#)

FXOS 보안 모듈/보안 엔진 정보

Firepower Chassis Manager의 Security Modules/Security Engine(보안 모듈/보안 엔진) 페이지에서는 보안 모듈/엔진의 상태를 확인하고 해당 보안 모듈/엔진의 다음 기능을 수행할 수 있습니다.

- **Decommission(서비스 해제)/Recommission(서비스 다시 시작)(보안 모듈 전용)**— 보안 모듈의 서비스를 해제하면 보안 모듈이 유지 보수 모드가 됩니다. 특정한 결함 상태를 수정하기 위해 보안 모듈 서비스를 해제한 다음 다시 시작할 수도 있습니다. [보안 모듈 서비스 해제/서비스 다시 시작, 169 페이지](#)를 참조하십시오.
- **Acknowledge(승인)**— 새로 설치한 보안 모듈을 온라인 상태로 전환합니다. [보안 모듈/엔진 승인, 169 페이지](#)를 참조하십시오.
- **Power Cycle(전원 꺾다가 다시 켜기)**— 보안 모듈/엔진을 재시작합니다. [보안 모듈/엔진 재설정, 170 페이지](#)를 참조하십시오.
- **Reinitialize(재초기화)**— 보안 모듈/엔진에서 구축된 모든 애플리케이션 및 컨피그레이션을 제거하면서 보안 모듈/엔진 하드 디스크를 다시 포맷한 다음 시스템을 다시 시작합니다. 재초기화를 완료한 후에 논리적 디바이스가 보안 모듈/엔진에 대해 구성된 경우 Firepower eXtensible 운영 체제에서는 애플리케이션 소프트웨어를 다시 설치하고 논리적 디바이스를 다시 구축하며 애플리케이션을 자동 시작합니다. [보안 모듈/엔진 재초기화, 170 페이지](#)를 참조하십시오.



경고! 재초기화 동안 보안 모듈/엔진에서 모든 애플리케이션 데이터가 삭제됩니다. 보안 모듈/엔진의 재초기화 이전에 모든 애플리케이션 데이터를 백업하십시오.

- Power off/on(전원 끄기/켜기) — 보안 모듈/엔진의 전원 상태를 전환합니다. [보안 모듈/엔진 전원 켜기/끄기, 171 페이지](#)를 참조하십시오.

Security Modules/Security Engine(보안 모듈/보안 엔진) 페이지에서는 다음 정보가 제공됩니다.

- Hardware State(하드웨어 상태) — 보안 모듈/엔진 하드웨어의 상태가 표시됩니다.
 - Up(가동 중) — 보안 모듈/엔진의 전원이 성공적으로 켜지며 하드웨어 결함이 표시되지 않습니다.
 - Booting Up(부팅 중) — 보안 모듈/엔진의 전원이 켜지고 있습니다.
 - Down(다운) — 보안 모듈/엔진의 전원이 켜지지 않았거나 하드웨어 결함으로 인해 보안 모듈/엔진이 성공적으로 시작되지 않습니다.
 - Unassociated(연결되지 않음) — 보안 모듈/엔진에 연결된 논리적 디바이스가 없습니다.
 - Mismatch(불일치) — 보안 모듈 서비스가 해제되었거나 새 보안 모듈이 슬롯에 설치되었습니다. [Recommission\(서비스 다시 시작\)](#) 또는 [Acknowledge\(승인\)](#) 기능을 사용하여 보안 모듈을 작동 상태로 되돌립니다.
- Service State(서비스 상태) — 보안 모듈/엔진의 소프트웨어 상태가 표시됩니다.
 - Not-available(사용 불가능) — 보안 모듈이 새시 슬롯에서 제거되었습니다. 정상 작동 상태로 돌아가려면 보안 모듈을 다시 설치합니다.
 - Offline(오프라인) — 보안 모듈/엔진이 설치되어 있지만, 서비스가 해제되었거나 전원이 꺼졌거나 계속 부팅 중인 상태입니다.
 - Online(온라인) — 보안 모듈/엔진이 설치되어 있으며 정상 작동 모드입니다.
 - Not Responding(응답하지 않음) — 보안 모듈/엔진이 응답하지 않습니다.
 - Fault(결함) — 보안 모듈/엔진이 결함 상태입니다. 결함 상태를 유발할 수 있는 원인에 대한 자세한 내용은 시스템 결함 목록을 검토하십시오.
 - Token Mismatch(토큰 불일치) — 이전에 구성한 보안 모듈이 아닌 다른 보안 모듈이 새시 슬롯에 설치되었음을 나타냅니다. 이는 소프트웨어 설치 오류로 인해 발생할 수 있습니다. [Reinitialize\(재초기화\)](#) 기능을 사용하여 보안 모듈을 작동 상태로 되돌립니다.
- Power(전원) — 보안 모듈/엔진의 전원 상태가 표시됩니다.
 - On(켜짐) — Power off/on(전원 끄기/켜기) 기능을 사용하여 보안 모듈/엔진의 전원 상태를 전환합니다.
 - Off(꺼짐) — Power off/on(전원 끄기/켜기) 기능을 사용하여 보안 모듈/엔진의 전원 상태를 전환합니다.

- Application(애플리케이션) — 보안 모듈/엔진에 설치된 논리적 디바이스 유형이 표시됩니다.

보안 모듈 서비스 해제/서비스 다시 시작

보안 모듈의 서비스를 해제하는 경우 보안 모듈 객체가 컨피그레이션에서 삭제되고 보안 모듈이 관리되지 않는 상태가 됩니다. 보안 모듈에서 실행 중인 모든 논리적 디바이스 또는 소프트웨어는 비활성 상태가 됩니다.

보안 모듈의 사용을 일시적으로 중단하려는 경우 보안 모듈 서비스를 해제할 수 있습니다. 또한, 보안 모듈을 다시 시작해도 오류 상태를 해결할 수 없는 경우, 보안 모듈 서비스를 해제한 다음 다시 시작하여 보안 모듈을 재초기화하지 않고 오류 상태를 해결할 수 있는지 확인할 수 있습니다.

절차

-
- 단계 1 Security Modules(보안 모듈) 페이지를 열려면 **Security Modules(보안 모듈)**를 선택합니다.
 - 단계 2 보안 모듈 서비스를 해제하려면 해당 보안 모듈에 대해 **Decommission(서비스 해제)**을 클릭합니다. 보안 모듈 서비스를 다시 시작하려면 해당 보안 모듈에 대해 **Recommission(서비스 다시 시작)**을 클릭합니다.
 - 단계 3 **Yes(예)**를 클릭하여 지정된 보안 모듈 서비스를 해제 또는 다시 시작할 것을 확인합니다.
-

보안 모듈/엔진 승인

새로운 보안 모듈이 새시에 설치된 경우, 사용을 시작하기 전에 보안 모듈을 승인해야 합니다.

보안 모듈이 “불일치” 또는 “토큰 불일치” 상태로 표시되는 경우, 이는 슬롯에 설치된 보안 모듈에 이전에 슬롯에 설치했던 항목과 일치하지 않는 데이터가 있음을 나타냅니다. 보안 모듈에 기존 데이터가 있으며 새로운 슬롯에서 기존 데이터를 사용하려는 경우(즉, 보안 모듈이 실수로 잘못된 슬롯에 설치된 것이 아닌 경우), 보안 모듈을 재초기화해야 논리적 디바이스를 구축할 수 있습니다.

절차

-
- 단계 1 Security Modules/Security Engine(보안 모듈/보안 엔진) 페이지를 열려면 **Security Modules/Security Engine(보안 모듈/보안 엔진)**을 선택합니다.
 - 단계 2 승인할 보안 모듈/엔진에 대해 **Acknowledge(승인)**를 클릭합니다.
 - 단계 3 **Yes(예)**를 클릭하여 지정된 보안 모듈/엔진을 승인할 것을 확인합니다.
-

보안 모듈/엔진 재설정

절차

-
- 단계 1 Security Modules/Security Engine(보안 모듈/보안 엔진) 페이지를 열려면 **Security Modules/Security Engine**(보안 모듈/보안 엔진)을 선택합니다.
- 단계 2 재설정할 보안 모듈/엔진의 **Power Cycle**(전원 껐다가 다시 켜기)을 클릭합니다.
- 단계 3 다음 중 하나를 수행합니다.
- 시스템이 지정된 보안 모듈/엔진을 재설정하기 전에 보안 모듈/엔진에서 실행 중인 애플리케이션이 종료되기까지 최대 5분간 대기하도록 설정하려면 **Safe Power Cycle**(안전하게 전원 껐다가 다시 켜기)을 클릭합니다.
 - 시스템이 지정된 보안 모듈/엔진을 즉시 재설정하도록 하려면 **Power Cycle Immediately**(즉시 전원 껐다가 다시 켜기)를 클릭합니다.
-

보안 모듈/엔진 재초기화

보안 모듈/엔진이 재초기화된 경우 보안 모듈/엔진 하드 디스크가 포맷되며 설치된 모든 애플리케이션 인스턴스 및 컨피그레이션이 제거됩니다. 재초기화를 완료한 후에 논리적 디바이스가 보안 모듈/엔진에 대해 구성된 경우 Firepower eXtensible 운영 체제에서는 애플리케이션 소프트웨어를 다시 설치하고 논리적 디바이스를 다시 구축하며 애플리케이션을 자동 시작합니다.



- 경고!** 재초기화 동안 보안 모듈/엔진에서 모든 애플리케이션 데이터가 삭제됩니다. 보안 모듈/엔진의 재초기화 이전에 모든 애플리케이션 데이터를 백업하십시오.
-

절차

-
- 단계 1 Security Modules/Security Engine(보안 모듈/보안 엔진) 페이지를 열려면 **Security Modules/Security Engine**(보안 모듈/보안 엔진)을 선택합니다.
- 단계 2 재초기화할 보안 모듈/엔진에 대해 **Reinitialize**(재초기화)를 클릭합니다.
- 단계 3 **Yes(예)**를 클릭하여 지정된 보안 모듈/엔진을 재초기화할 것을 확인합니다. 보안 모듈/엔진이 재시작되며 보안 모듈의 모든 데이터가 삭제됩니다. 이 프로세스는 몇 분이 걸릴 수 있습니다.
-

보안 모듈/엔진 전원 켜기/끄기

절차

-
- 단계 1** Security Modules/Security Engine(보안 모듈/보안 엔진) 페이지를 열려면 **Security Modules/Security Engine**(보안 모듈/보안 엔진)을 선택합니다.
- 단계 2** 보안 모듈/엔진의 전원을 끄려면 다음을 수행합니다.
- 해당 보안 모듈/엔진의 **Power off**(전원 끄기)를 클릭합니다.
 - 다음 중 하나를 수행합니다.
 - 시스템에서 지정된 보안 모듈/엔진의 전원을 끄기 전에 보안 모듈/엔진에서 실행 중인 애플리케이션이 종료되기까지 최대 5분간 대기하도록 설정하려면 **Safe Power Off**(안전하게 전원 끄기)를 클릭합니다.
 - 시스템이 지정된 보안 모듈/엔진의 전원을 즉시 끄도록 설정하려면 **Power Off Immediately**(즉시 전원 끄기)를 클릭합니다.
- 단계 3** 보안 모듈/엔진의 전원을 켜려면 다음을 수행합니다.
- 해당 보안 모듈/엔진의 **Power on**(전원 켜기)을 클릭합니다.
 - Yes**(예)를 클릭하여 지정된 보안 모듈/엔진의 전원을 켤 것을 확인합니다.
-



컨피그레이션 가져오기/내보내기

- [컨피그레이션 가져오기/내보내기 정보, 173페이지](#)
- [컨피그레이션 파일 내보내기, 174페이지](#)
- [자동 컨피그레이션 내보내기 예약, 175페이지](#)
- [컨피그레이션 내보내기 미리 알림 설정, 176페이지](#)
- [컨피그레이션 파일 가져오기, 176페이지](#)

컨피그레이션 가져오기/내보내기 정보

컨피그레이션 내보내기 기능을 사용하여 Firepower 4100/9300 새시의 논리적 디바이스와 플랫폼 컨피그레이션 설정이 포함된 XML 파일을 원격 서버 또는 로컬 컴퓨터에 내보낼 수 있습니다. 나중에 해당 컨피그레이션 파일을 가져와서 컨피그레이션 설정을 Firepower 4100/9300 새시에 신속하게 적용하여 알려진 정상적인 컨피그레이션으로 돌아가거나 시스템 장애를 복구할 수 있습니다.

지침 및 제한 사항

- 컨피그레이션 파일의 콘텐츠를 수정하지 마십시오. 컨피그레이션 파일이 수정된 경우, 해당 파일을 사용하는 컨피그레이션 가져오기가 실패할 수 있습니다.
- 애플리케이션별 컨피그레이션 설정은 컨피그레이션 파일에 포함되어 있지 않습니다. 애플리케이션별 설정 및 컨피그레이션을 관리하기 위해 애플리케이션에서 제공하는 컨피그레이션 백업 툴을 사용해야 합니다.
- 컨피그레이션을 Firepower 4100/9300 새시에 가져올 때 Firepower 4100/9300 새시의 모든 기존 컨피그레이션(모든 논리적 디바이스 포함)이 삭제되며 가져오기 파일에 포함된 컨피그레이션으로 완전히 대체됩니다.
- 컨피그레이션을 내보낸 동일한 Firepower 4100/9300 새시에만 컨피그레이션 파일을 가져오는 것이 좋습니다.
- 가져오기 작업 중인 Firepower 4100/9300 새시의 플랫폼 소프트웨어 버전은 내보내기를 수행할 때와 동일한 버전이어야 합니다. 그렇지 않으면 가져오기 작업의 성공이 보장되지 않습니다.

Firepower 4100/9300 새시가 업그레이드 또는 다운그레이드될 때마다 백업 컨피그레이션을 내보내는 것이 좋습니다.

- 가져오기 작업 중인 Firepower 4100/9300 새시에는 내보내기를 수행할 때와 동일한 슬롯에 동일한 네트워크 모듈이 설치되어 있어야 합니다.
- 가져오기 작업 중인 Firepower 4100/9300 새시에는 가져오기 작업 중인 내보내기 파일에 정의된 모든 논리적 디바이스에 올바른 소프트웨어 애플리케이션 이미지가 설치되어 있어야 합니다.
- 애플리케이션에 EULA(엔드 유저 라이선스 계약)이 있는 논리적 디바이스가 가져오기 작업 중인 컨피그레이션 파일에 포함된 경우, 컨피그레이션 가져오기 또는 작업이 실패하기 전에 해당 애플리케이션에 대한 EULA가 Firepower 4100/9300 새시에서 허용되어야 합니다.
- 기존 백업 파일의 덮어쓰기를 방지하려면 백업 작업 시 파일 이름을 변경하거나 기존 파일을 다른 위치에 복사하십시오.

컨피그레이션 파일 내보내기

컨피그레이션 내보내기 기능을 사용하여 Firepower 4100/9300 새시의 논리적 디바이스와 플랫폼 컨피그레이션 설정이 포함된 XML 파일을 원격 서버 또는 로컬 컴퓨터에 내보냅니다.

컨피그레이션 내보내기 기능 사용에 대한 중요한 정보를 보려면 [컨피그레이션 가져오기/내보내기 정보](#)를 검토하십시오.

절차

- 단계 1 **System**(시스템) > **Configuration**(컨피그레이션) > **Export**(내보내기)를 선택합니다.
- 단계 2 컨피그레이션 파일을 로컬 컴퓨터에 내보내려면 **Export Locally**(로컬로 내보내기)를 클릭합니다. 컨피그레이션 파일이 생성되며 브라우저에 따라 이 파일이 기본 다운로드 위치에 자동으로 다운로드되거나 파일을 저장하라는 프롬프트가 표시될 수 있습니다.
- 단계 3 컨피그레이션 파일을 이전에 구성한 원격 서버에 내보내려면 사용할 원격 컨피그레이션에 대해 **Export**(내보내기)를 클릭합니다. 컨피그레이션 파일이 생성되며 특정 위치로 내보내기됩니다.
- 단계 4 컨피그레이션 파일을 새 원격 서버에 내보내려면 다음을 수행합니다.
 - a) **On-Demand Export**(온디맨드 내보내기) 아래에서 **Add On-Demand Configuration**(온디맨드 컨피그레이션 추가)을 클릭합니다.
 - b) 원격 서버와 통신할 때 사용할 프로토콜을 선택합니다. 프로토콜은 FTP, TFTP, SCP 또는 SFTP 중 하나가 가능합니다.
 - c) 백업 파일을 저장해야 하는 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 새시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브 또는 읽기/쓰기 미디어일 수 있습니다. IP 주소 대신 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.
 - d) 기본 포트 이외의 포트를 사용하는 경우 **Port**(포트) 필드에 포트 번호를 입력합니다.

- e) 원격 서버에 로그인할 때 시스템에서 사용해야 하는 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
- f) 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
- g) **Location(위치)** 필드에서 파일 이름을 포함하여 컨피그레이션 파일을 내보낼 전체 경로를 입력합니다. 파일 이름을 생략하는 경우 내보내기 절차에서 파일에 이름이 할당됩니다.
- h) **OK(확인)**를 클릭합니다.
원격 컨피그레이션이 On-Demand Export(온디맨드 내보내기) 테이블에 추가됩니다.
- i) 사용할 원격 컨피그레이션에 대해 **Export(내보내기)**를 클릭합니다.
컨피그레이션 파일이 생성되며 특정 위치로 내보내기됩니다.

자동 컨피그레이션 내보내기 예약

예약된 내보내기 기능을 사용하여 Firepower 4100/9300 새시의 논리적 디바이스와 플랫폼 컨피그레이션 설정이 포함된 XML 파일을 원격 서버 또는 로컬 컴퓨터에 자동으로 내보냅니다. 매일, 매주 또는 2주마다 실행되도록 내보내기를 예약할 수 있습니다. 예약된 내보내기 기능이 활성화된 시기를 기준으로 예약에 따라 컨피그레이션 내보내기가 실행됩니다. 따라서 예를 들어, 매주 수요일 오후 10시에 실행되도록 예약된 내보내기를 활성화하는 경우, 매주 수요일 오후 10시에 새로운 내보내기가 트리거됩니다.

컨피그레이션 내보내기 기능 사용에 대한 중요한 정보를 보려면 [컨피그레이션 가져오기/내보내기 정보](#)를 검토하십시오.

절차

- 단계 1** **System(시스템) > Configuration(컨피그레이션) > Export(내보내기)**를 선택합니다.
- 단계 2** **Schedule Export(내보내기 예약)**를 클릭합니다.
Configure Scheduled Export(예약된 내보내기 구성) 대화 상자가 표시됩니다.
- 단계 3** 원격 서버와 통신할 때 사용할 프로토콜을 선택합니다. 프로토콜은 FTP, TFTP, SCP 또는 SFTP 중 하나가 가능합니다.
- 단계 4** 예약된 내보내기를 활성화하려면 **Enable(활성화)** 확인란을 선택합니다.
참고 이 확인란을 사용하여 나중에 내보내기 예약을 활성화 또는 비활성화할 수 있습니다. 단, 예약된 내보내기를 활성화 또는 비활성화하는 경우에는 비밀번호를 다시 지정해야 합니다.
- 단계 5** 백업 파일을 저장해야 하는 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 새시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브 또는 읽기/쓰기 미디어일 수 있습니다.
IP 주소 대신 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.

- 단계 6 기본 포트 이외의 포트를 사용하는 경우 **Port(포트)** 필드에 포트 번호를 입력합니다.
- 단계 7 원격 서버에 로그인할 때 시스템에서 사용해야 하는 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
- 단계 8 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
- 단계 9 **Location(위치)** 필드에서 파일 이름을 포함하여 컨피그레이션 파일을 내보낼 전체 경로를 입력합니다. 파일 이름을 생략하는 경우 내보내기 절차에서 파일에 이름이 할당됩니다.
- 단계 10 컨피그레이션을 자동으로 내보낼 일정을 선택합니다. 이는 Daily(매일), Weekly(매주) 또는 BiWeekly(격주) 중 하나가 될 수 있습니다.
- 단계 11 **OK(확인)**를 클릭합니다.
예약된 내보내기가 생성됩니다. 예약된 내보내기를 활성화한 경우, 선택한 일정에 따라 지정된 위치에 컨피그레이션 파일이 자동으로 내보내집니다.

컨피그레이션 내보내기 미리 알림 설정

내보내기 미리 알림 기능을 사용하여 컨피그레이션 내보내기가 특정 일수 이내에 실행되지 않은 경우, 시스템이 결함을 생성하도록 설정합니다.

절차

- 단계 1 **System(시스템) > Configuration(컨피그레이션) > Export(내보내기)**를 선택합니다.
- 단계 2 컨피그레이션 내보내기 미리 알림을 활성화하려면 **Reminder to trigger an export(내보내기 트리거 미리 알림)** 아래에서 확인란을 선택합니다.
- 단계 3 미리 알림 결함을 생성하기 전에 컨피그레이션 내보내기 사이에서 시스템이 대기해야 하는 일수 (1~365)를 입력합니다.
- 단계 4 **Save Reminder(미리 알림 저장)**를 클릭합니다.

컨피그레이션 파일 가져오기

컨피그레이션 가져오기 기능을 사용하여 Firepower 4100/9300 새시에서 이전에 내보낸 컨피그레이션 설정을 적용할 수 있습니다. 이 기능을 사용하면 알려진 정상적인 컨피그레이션으로 돌아가거나 시스템 장애를 복구할 수 있습니다. 컨피그레이션 가져오기 기능 사용에 대한 중요한 정보를 보려면 [컨피그레이션 가져오기/내보내기 정보](#)를 검토하십시오.

절차

- 단계 1 System(시스템) > Configuration(컨피그레이션) > Import(가져오기)**를 선택합니다.
- 단계 2** 다음을 수행하여 로컬 컨피그레이션 파일에서 가져옵니다.
- a) **Choose File(파일 선택)**을 클릭하여 가져올 컨피그레이션 파일을 찾아 선택합니다.
 - b) **Import(가져오기)**를 클릭합니다.
확인 대화 상자가 열리면서 계속 진행할 것인지 확인을 요청하고 새시를 재시작해야 한다고 경고합니다.
 - c) **Yes(예)**를 클릭하여 지정한 컨피그레이션 파일을 가져올 것임을 확인합니다.
기존 컨피그레이션이 삭제되고 가져오기 파일에 지정된 컨피그레이션이 Firepower 4100/9300 새시에 적용됩니다. 가져오는 동안 Breakout 포트 컨피그레이션이 변경된 경우 Firepower 4100/9300 새시를 재시작해야 합니다.
- 단계 3** 다음을 수행하여 이전에 구성된 원격 서버에서 컨피그레이션 파일을 가져옵니다.
- a) **Remote Import(원격 가져오기)** 테이블에서 사용할 원격 컨피그레이션에 대해 **Import(가져오기)**를 클릭합니다.
확인 대화 상자가 열리면서 계속 진행할 것인지 확인을 요청하고 새시를 재시작해야 한다고 경고합니다.
 - b) **Yes(예)**를 클릭하여 지정한 컨피그레이션 파일을 가져올 것임을 확인합니다.
기존 컨피그레이션이 삭제되고 가져오기 파일에 지정된 컨피그레이션이 Firepower 4100/9300 새시에 적용됩니다. 가져오는 동안 Breakout 포트 컨피그레이션이 변경된 경우 Firepower 4100/9300 새시를 재시작해야 합니다.
- 단계 4** 다음을 수행하여 새 원격 서버의 컨피그레이션 파일에서 가져옵니다.
- a) **Remote Import(원격 가져오기)** 아래에서 **Add Remote Configuration(원격 컨피그레이션 추가)**을 클릭합니다.
 - b) 원격 서버와 통신할 때 사용할 프로토콜을 선택합니다. 프로토콜은 FTP, TFTP, SCP 또는 SFTP 중 하나가 가능합니다.
 - c) 기본 포트 이외의 포트를 사용하는 경우 **Port(포트)** 필드에 포트 번호를 입력합니다.
 - d) 백업 파일을 저장하는 위치의 IP 주소 또는 호스트 이름을 입력합니다. 이는 Firepower 4100/9300 새시가 네트워크를 통해 액세스할 수 있는 서버, 스토리지 어레이, 로컬 드라이브 또는 읽기/쓰기 미디어일 수 있습니다.
IP 주소 대신 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.
 - e) 원격 서버에 로그인할 때 시스템에서 사용해야 하는 사용자 이름을 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
 - f) 원격 서버 사용자 이름의 비밀번호를 입력합니다. 프로토콜이 TFTP일 경우 이 필드는 적용되지 않습니다.
 - g) **File Path(파일 경로)** 필드에서 파일 이름을 포함하여 컨피그레이션 파일의 전체 경로를 입력합니다.
 - h) **Save(저장)**를 클릭합니다.
원격 컨피그레이션이 Remote Import(원격 가져오기) 테이블에 추가됩니다.
 - i) 사용할 원격 컨피그레이션에 대해 **Import(가져오기)**를 클릭합니다.

확인 대화 상자가 열리면서 계속 진행할 것인지 확인을 요청하고 새시를 재시작해야 한다고 경고합니다.

- j) **Yes(예)**를 클릭하여 지정한 컨피그레이션 파일을 가져올 것임을 확인합니다.
기존 컨피그레이션이 삭제되고 가져오기 파일에 지정된 컨피그레이션이 Firepower 4100/9300 새시에 적용됩니다. 가져오는 동안 Breakout 포트 컨피그레이션이 변경된 경우 Firepower 4100/9300 새시를 재시작해야 합니다.
-



트리블슈팅

- 패킷 캡처, 179페이지
- 네트워크 연결성 테스트, 185페이지
- 포트 채널 상태 판단, 186페이지
- 소프트웨어 장애 복구, 188페이지
- 손상된 파일 시스템 복구, 193페이지

패킷 캡처

패킷 캡처 툴은 연결 및 컨피그레이션 문제를 디버깅하는 데 사용되는 중요한 자산이며 Firepower 4100/9300 새시를 통과하는 트래픽 플로우를 이해하기 위해 사용됩니다. 패킷 캡처 툴을 사용하여 Firepower 4100/9300 새시에서 특정 고객 대상 포트 또는 애플리케이션 포트를 통과하는 트래픽을 기록할 수 있습니다.

여러 개의 패킷 캡처 세션을 생성할 수 있으며 각 세션에서는 여러 포트의 트래픽을 캡처할 수 있습니다. 패킷 캡처 세션에 포함된 각 포트의 경우 별도의 PCAP(패킷 캡처) 파일이 생성됩니다.

백플레인 포트 매핑

Firepower 4100/9300 새시는 내부 백플레인 포트에 다음 매핑을 사용합니다.

보안 모듈	포트 매핑	설명
보안 모듈 1/보안 엔진	Ethernet1/9	Internal-Data0/0
보안 모듈 1/보안 엔진	Ethernet1/10	Internal-Data0/1
보안 모듈 2	Ethernet1/11	Internal-Data0/0
보안 모듈 2	Ethernet1/12	Internal-Data0/1

보안 모듈	포트 매핑	설명
보안 모듈 3	Ethernet1/13	Internal-Data0/0
보안 모듈 3	Ethernet1/14	Internal-Data0/1

지침 및 제한 사항

패킷 캡처 툴에는 다음과 같은 제한 사항이 있습니다.

- 최대 100Mbps만 캡처할 수 있습니다.
- 패킷 캡처 세션을 실행하는 데 사용할 수 있는 스토리지 공간이 충분하지 않은 경우에도 패킷 캡처 세션을 생성할 수 있습니다. 패킷 캡처 세션을 시작하기 전에 사용할 수 있는 충분한 스토리지 공간이 있는지 확인해야 합니다.
- 여러 개의 패킷 캡처 세션 활성화를 지원하지 않습니다.
- 내부 스위치의 인그레스 단계에서만 캡처합니다.
- 내부 스위치에서 해석될 수 없는 패킷에서는 필터가 유효하지 않습니다(예: 보안 그룹 태그 및 네트워크 서비스 헤더 패킷).
- 추상화가 지원되지 않습니다(예: 포트 채널 및 서비스 체인).



참고 포트 채널에서 트래픽 캡처가 지원되지는 않지만 패킷 캡처 세션에서 포트 채널을 구성하는 개별 멤버 포트를 포함할 수는 있으며, 패킷 캡처 툴은 각 해당 멤버 포트에 대해 별도의 패킷 캡처 파일을 생성합니다.

- 캡처 세션이 계속 활성 상태인 경우 PCAP 파일을 복사하거나 내보낼 수 없습니다.
- 패킷 캡처 세션을 삭제하면 해당 세션에 연결된 패킷 캡처 파일도 모두 삭제됩니다.

패킷 캡처 세션 생성 또는 편집

절차

- 단계 1** **Tools(툴) > Packet Capture(패킷 캡처)**를 선택합니다.
Capture Session(캡처 세션) 탭은 현재 구성되어 있는 패킷 캡처 세션의 목록을 표시합니다. 패킷 캡처 세션이 현재 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
- 단계 2** 다음 중 하나를 수행합니다.
 - 패킷 캡처 세션을 생성하려면 **Capture Session(캡처 세션)** 버튼을 클릭합니다.
 - 기존의 패킷 캡처 세션을 편집하려면 해당 세션의 **Edit(편집)** 버튼을 클릭합니다.

Configure Packet Capture Session(패킷 캡처 세션 구성) 창이 표시됩니다. **Configure Packet Capture Session**(패킷 캡처 세션 구성) 창의 왼쪽에서 Firepower 4100/9300 새시에 구성된 특정한 논리적 디바이스를 선택하여 해당 논리적 디바이스를 표시할 수 있습니다. 이 표시는 패킷을 캡처할 대상 인터페이스를 선택하는 데 사용됩니다. **Configure Packet Capture Session**(패킷 캡처 세션 구성) 창의 오른쪽에는 패킷 캡처 세션을 정의하기 위한 필드가 포함되어 있습니다.

- 단계 3 Session Name**(세션 이름) 필드에 패킷 캡처 세션의 이름을 입력합니다.
- 단계 4 Buffer Size**(버퍼 크기) 목록에서 사전 구성된 값 중 하나를 선택하거나 **Custom in MB**(MB로 맞춤화)를 선택한 다음 원하는 버퍼 크기를 입력하여 이 패킷 캡처 세션에 사용할 버퍼 크기를 지정합니다. 지정된 버퍼 크기는 1~2,048MB여야 합니다.
- 단계 5 Snap Length**(스냅 길이) 필드에서 캡처할 패킷의 길이를 지정합니다. 유효한 값은 64~9006바이트입니다. 기본 스냅 길이는 1518바이트입니다.
- 단계 6** 이 패킷 캡처 세션을 실행할 때 기존 PCAP 파일을 덮어쓸지 아니면 PCAP 파일에 데이터를 추가할지 지정합니다.
- 단계 7 Configure Packet Capture Session**(패킷 캡처 세션 구성) 창의 왼쪽에서 패킷을 캡처할 논리적 디바이스의 이름을 클릭합니다.
디바이스에 할당된 모든 인터페이스를 비롯하여 선택한 논리적 디바이스가 표시됩니다.
- 단계 8** 논리적 디바이스에 할당된 고객 대상 포트의 트래픽을 캡처하려면 원하는 인터페이스를 클릭하여 해당 트래픽을 선택합니다.
- 단계 9** 백플레인 포트를 통해 전송되는 논리적 디바이스의 트래픽을 캡처하려면 다음을 수행합니다.
- 논리적 디바이스를 표시하는 상자를 클릭합니다.
Capture On(캡처 설정), **Application Port**(애플리케이션 포트) 및 **Application Capture Direction**(애플리케이션 캡처 방향) 필드는 **Configure Packet Capture Session**(패킷 캡처 세션 구성) 창의 오른쪽에서 사용할 수 있습니다.
 - Capture On**(캡처 설정) 드롭다운 목록에서 트래픽을 캡처할 백플레인 포트를 선택하거나 **All Backplane Ports**(모든 백플레인 포트)를 선택합니다.
- 단계 10** 논리적 디바이스와 특정 인터페이스 간의 트래픽을 캡처하려면 다음을 수행합니다.
- 논리적 디바이스를 표시하는 상자를 클릭합니다.
Capture On(캡처 설정), **Application Port**(애플리케이션 포트) 및 **Application Capture Direction**(애플리케이션 캡처 방향) 필드는 **Configure Packet Capture Session**(패킷 캡처 세션 구성) 창의 오른쪽에서 사용할 수 있습니다.
 - 논리적 디바이스(예: ASA)를 **Capture On**(캡처 설정) 드롭다운 목록에서 선택합니다.
 - Application Port**(애플리케이션 포트) 드롭다운 목록에서 오고 가는 트래픽을 캡처할 인터페이스를 선택합니다.
 - 논리적 디바이스에서 지정된 인터페이스를 향해 이동하는 트래픽만 캡처하려면 **Application Capture Direction**(애플리케이션 캡처 방향) 옆에 있는 **Egress Packets**(이그레스 패킷) 옵션을 클릭합니다.
 - 지정된 인터페이스를 오고 가는 트래픽을 캡처하려면 **Application Capture Direction**(애플리케이션 캡처 방향) 옆에 있는 **All Packets**(모든 패킷) 옵션을 클릭합니다.
- 단계 11** 캡처 중인 트래픽을 필터링합니다.
- Capture Filter**(캡처 필터) 필드의 **Apply Filter**(필터 적용) 옵션을 클릭합니다.

필터 구성을 위한 필드 집합이 제공됩니다.

- b) 필터를 생성해야 하는 경우 **Create Filter**(필터 생성)를 클릭합니다.
Create Packet Filter(패킷 필터 생성) 대화 상자가 표시됩니다. 자세한 내용은 [패킷 캡처의 필터 구성, 182 페이지](#)를 참조하십시오.
- c) **Apply**(적용) 드롭다운 목록에서 사용할 필터를 선택합니다.
- d) **To**(대상) 드롭다운 목록에서 필터를 적용할 인터페이스를 선택합니다.
- e) 추가 필터를 적용하려면 **Apply Another Filter**(다른 필터 적용)를 클릭한 다음 위 단계를 반복하여 추가 필터를 적용합니다.

단계 12 다음 중 하나를 수행합니다.

- 이 패킷 캡처 세션을 저장하고 바로 실행하려면 **Save and Run**(저장 및 실행) 버튼을 클릭합니다. 이 옵션은 다른 패킷 캡처 세션이 현재 실행 중이 아닌 경우에만 사용할 수 있습니다.
- 나중에 실행할 수 있도록 이 패킷 캡처 세션을 저장하려면 **Save**(저장) 버튼을 클릭합니다.

생성된 다른 세션과 함께 나열된 세션에 **Capture Session**(캡처 세션) 탭이 표시됩니다. **Save and Run**(저장 및 실행)을 선택한 경우, 패킷 캡처 세션이 패킷을 캡처합니다. 세션에서 PCAP 파일을 다운로드하기 전에 캡처를 중지해야 합니다.

패킷 캡처의 필터 구성

필터를 생성하여 패킷 캡처 세션에 포함된 트래픽을 제한할 수 있습니다. 패킷 캡처 세션을 생성하는 동안 특정 필터를 사용해야 하는 인터페이스를 선택할 수 있습니다.



참고

현재 실행 중인 패킷 캡처 세션에 적용된 필터를 수정하거나 삭제하는 경우, 변경 사항은 세션을 비활성화한 다음 다시 활성화할 때까지 적용되지 않습니다.

절차

- 단계 1 **Tools**(툴) > **Packet Capture**(패킷 캡처)를 선택합니다.
Capture Session(캡처 세션) 탭은 현재 구성되어 있는 패킷 캡처 세션의 목록을 표시합니다. 패킷 캡처 세션이 현재 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.

단계 2 다음 중 하나를 수행합니다.

- 필터를 생성하려면 **Add Filter**(필터 추가) 버튼을 클릭합니다.
- 기존 필터를 편집하려면 해당 필터의 **Edit**(편집) 버튼을 클릭합니다.

Create or Edit Packet Filter(패킷 필터 생성 또는 편집) 대화 상자가 표시됩니다.

- 단계 3 **Filter Name**(필터 이름) 필드에 패킷 캡처 필터의 이름을 입력합니다.
- 단계 4 특정 프로토콜을 필터링하려면 **Protocol**(프로토콜) 목록에서 선택하거나 **Custom**(맞춤화)을 선택한 다음 원하는 프로토콜을 입력합니다. 맞춤형 프로토콜은 10진수 형식(0~255)의 IANA 정의 프로토콜이어야 합니다.
- 단계 5 특정 EtherType을 필터링하려면 **EtherType** 목록에서 선택하거나 **Custom**(맞춤화)을 선택한 다음 원하는 EtherType을 입력합니다. 맞춤형 EtherType은 10진수 형식의 IANA 정의 EtherType이어야 합니다(예: IPv4 = 2048, IPv6 = 34525, ARP = 2054, SGT = 35081).
- 단계 6 내부 VLAN(포트를 인그레스하는 동안의 VLAN ID) 또는 외부 VLAN(Firepower 4100/9300 새시에서 추가한 VLAN ID)에 기반하여 트래픽을 필터링하려면 지정된 필드에 VLAN ID를 입력합니다.
- 단계 7 특정 소스 또는 대상의 트래픽을 필터링하려면 IP 주소와 포트를 입력하거나 지정된 소스 또는 대상 필드에 MAC 주소를 입력합니다.
참고 IPv4 또는 IPv6 주소를 사용하여 필터링할 수 있지만 동일한 패킷 캡처 세션에서 두 가지를 모두 필터링할 수는 없습니다.
- 단계 8 **Save**(저장)를 클릭하여 필터를 저장합니다.
 생성한 다른 필터와 함께 나열된 필터가 있는 **Filter List**(필터 목록) 탭이 표시됩니다.

패킷 캡처 세션 시작 및 중지

절차

- 단계 1 **Tools**(툴) > **Packet Capture**(패킷 캡처)를 선택합니다.
Capture Session(캡처 세션) 탭은 현재 구성되어 있는 패킷 캡처 세션의 목록을 표시합니다. 패킷 캡처 세션이 현재 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
- 단계 2 패킷 캡처 세션을 시작하려면 해당 세션의 **Enable Session**(세션 활성화) 버튼을 클릭한 다음 **Yes**(예)를 클릭하여 확인합니다.
참고 다른 세션을 실행하는 동안 패킷 캡처 세션을 시작할 수 없습니다.
 세션에 포함된 인터페이스의 PCAP 파일은 트래픽 수집을 시작합니다. 세션이 세션 데이터를 덮어쓰도록 구성된 경우, 기존 PCAP 데이터가 지워집니다. 그렇지 않은 경우, 데이터가 기존 파일에 추가됩니다(있는 경우).
 패킷 캡처 세션이 실행 중인 경우, 개별 PCAP 파일의 파일 크기는 트래픽이 캡처됨에 따라 증가합니다. 버퍼 크기 제한에 도달하면 시스템은 패킷 삭제를 시작하며 삭제 수 필드가 증가하는 것을 확인할 수 있습니다.
- 단계 3 패킷 캡처 세션을 중지하려면 해당 세션의 **Disable Session**(세션 비활성화) 버튼을 클릭한 다음 **Yes**(예)를 클릭하여 확인합니다.
 세션이 비활성화된 후에 PCAP 파일을 다운로드할 수 있습니다([패킷 캡처 파일 다운로드](#), 184 페이지 참조).

패킷 캡처 파일 다운로드

네트워크 패킷 분석기를 사용하여 분석할 수 있도록 세션에서 로컬 컴퓨터로 패킷 캡처(PCAP) 파일을 다운로드할 수 있습니다.

절차

-
- 단계 1** **Tools(툴) > Packet Capture(패킷 캡처)**를 선택합니다.
Capture Session(캡처 세션) 탭은 현재 구성되어 있는 패킷 캡처 세션의 목록을 표시합니다. 패킷 캡처 세션이 현재 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
- 단계 2** 패킷 캡처 세션에서 특정 인터페이스에 대한 PCAP 파일을 다운로드하려면 그 인터페이스에 해당하는 **Download(다운로드)** 버튼을 클릭합니다.
- 참고** 패킷 캡처 세션이 실행 중일 때는 PCAP 파일을 다운로드할 수 없습니다.
- 브라우저에 따라 지정된 PCAP 파일이 기본 다운로드 위치에 자동으로 다운로드되거나 파일을 저장하라는 프롬프트가 표시될 수 있습니다.
-

패킷 캡처 세션 삭제

개별 패킷 캡처 세션을 삭제(현재 실행 중이지 않은 경우)하거나 모든 비활성 상태의 패킷 캡처 세션을 삭제할 수 있습니다.

절차

-
- 단계 1** **Tools(툴) > Packet Capture(패킷 캡처)**를 선택합니다.
Capture Session(캡처 세션) 탭은 현재 구성되어 있는 패킷 캡처 세션의 목록을 표시합니다. 패킷 캡처 세션이 현재 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.
- 단계 2** 특정 패킷 캡처 세션을 삭제하려면 그 세션에 해당하는 **Delete(삭제)** 버튼을 클릭합니다.
- 단계 3** 모든 비활성 상태의 패킷 캡처 세션을 삭제하려면 패킷 캡처 세션 목록 위에 있는 **Delete All Sessions(모든 세션 삭제)** 버튼을 클릭합니다.
-

네트워크 연결성 테스트

시작하기 전에

호스트 이름 또는 IPv4 주소가 있는 네트워크에서 다른 디바이스를 ping하여 기본 네트워크 연결을 테스트하려면 **ping** 명령을 사용합니다. 호스트 이름 또는 IPv6 주소가 있는 네트워크에서 다른 디바이스를 ping하려면 **ping6** 명령을 사용합니다.

호스트 이름 또는 IPv4 주소가 있는 네트워크에서 다른 디바이스에 대한 경로를 추적하려면 **traceroute** 명령을 사용합니다. 호스트 이름 또는 IPv6 주소가 있는 네트워크에서 다른 디바이스에 대한 경로를 추적하려면 **traceroute6** 명령을 사용합니다.

- **ping** 및 **ping6** 명령은 `local-mgmt` 모드에서 사용할 수 있습니다.
- 또한, **ping** 명령은 `module` 모드에서 사용할 수 있습니다.
- **traceroute** 및 **traceroute6** 명령은 `local-mgmt` 모드에서 사용할 수 있습니다.
- 또한, **traceroute** 명령은 `module` 모드에서 사용할 수 있습니다.

절차

단계 1 다음 명령 중 하나를 입력하여 `local-mgmt` 또는 `module` 모드에 연결합니다.

- **connect local-mgmt**
- **connect module *module-ID* {console | telnet}**

예제:

```
FP9300-A# connect local-mgmt
FP9300-A(local-mgmt)#
```

단계 2 다음 명령을 사용하여 호스트 이름 또는 IPv4 주소가 있는 네트워크에서 다른 디바이스를 ping하여 기본 네트워크 연결을 테스트합니다.

ping {hostname | IPv4_address} [count number_packets] [deadline seconds] [interval seconds] [packet-size bytes]

예제:

이 예에서는 네트워크에 있는 다른 디바이스에 연결하여 ping을 12번 수행하는 방법을 보여줍니다.

```
FP9300-A(local-mgmt)# ping 198.51.100.10 count 12
PING 198.51.100.10 (198.51.100.10) from 203.0.113.5 eth0: 56(84) bytes of data.
64 bytes from 198.51.100.10: icmp_seq=1 ttl=61 time=0.264 ms
64 bytes from 198.51.100.10: icmp_seq=2 ttl=61 time=0.219 ms
64 bytes from 198.51.100.10: icmp_seq=3 ttl=61 time=0.234 ms
64 bytes from 198.51.100.10: icmp_seq=4 ttl=61 time=0.205 ms
64 bytes from 198.51.100.10: icmp_seq=5 ttl=61 time=0.216 ms
64 bytes from 198.51.100.10: icmp_seq=6 ttl=61 time=0.251 ms
64 bytes from 198.51.100.10: icmp_seq=7 ttl=61 time=0.223 ms
64 bytes from 198.51.100.10: icmp_seq=8 ttl=61 time=0.221 ms
64 bytes from 198.51.100.10: icmp_seq=9 ttl=61 time=0.227 ms
```

```
64 bytes from 198.51.100.10: icmp_seq=10 ttl=61 time=0.224 ms
64 bytes from 198.51.100.10: icmp_seq=11 ttl=61 time=0.261 ms
64 bytes from 198.51.100.10: icmp_seq=12 ttl=61 time=0.261 ms

--- 198.51.100.10 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11104ms
rtt min/avg/max/mdev = 51.005/51.062/51.164/0.064 ms

FP9300-A(local-mgmt)#
```

단계 3 다음 명령을 사용하여 호스트 이름 또는 IPv4 주소를 사용하여 네트워크에서 다른 디바이스에 대한 경로를 추적합니다.

```
traceroute {hostname | IPv4_address}
```

예제:

```
FP9300-A(local-mgmt)# traceroute 198.51.100.10
traceroute to 198.51.100.10 (198.51.100.10), 30 hops max, 40 byte packets
 1 198.51.100.57 (198.51.100.57) 0.640 ms 0.737 ms 0.686 ms
 2 net1-gw1-13.cisco.com (198.51.100.101) 2.050 ms 2.038 ms 2.028 ms
 3 net1-sec-gw2.cisco.com (198.51.100.201) 0.540 ms 0.591 ms 0.577 ms
 4 net1-fp9300-19.cisco.com (198.51.100.108) 0.336 ms 0.267 ms 0.289 ms

FP9300-A(local-mgmt)#
```

단계 4 (선택 사항) **exit**을 입력하여 local-mgmt 모드를 종료하고 최상위 레벨 모드로 돌아갑니다.

포트 채널 상태 판단

다음 단계를 수행하여 현재 정의된 포트 채널의 상태를 확인할 수 있습니다.

절차

단계 1 다음 명령을 입력하여 /eth-uplink/fabric 모드를 시작합니다.

- **connect eth-uplink**
- **scope fabric {a | b}**

예제:

```
FP9300-A# connect eth-uplink
FP9300-A /eth-uplink # scope fabric a
FP9300-A /eth-uplink/fabric #
```

단계 2 **show port-channel** 명령을 입력하여 각각의 관리 상태 및 작동 상태와 함께 현재 포트 채널 목록을 표시합니다.

예제:

```
FP9300-A /eth-uplink/fabric # show port-channel

Port Channel:
```

```

      Port Channel Id Name          Port Type          Admin
      State Oper State            State Reason
      -----
-----
      10                        Port-channel10    Data              Enabl
ed      Failed                    No operational members
      11                        Port-channel11    Data              Enabl
ed      Failed                    No operational members
      12                        Port-channel12    Data              Disab
led     Admin Down                Administratively down
      48                        Port-channel48    Cluster           Enabl
ed      Up
FP9300-A /eth-uplink/fabric #
    
```

단계 3 다음 명령을 입력하여 /port-channel 모드를 시작하고 개별 포트 채널 및 포트 정보를 표시합니다.

- scope port-channel ID

예제:

```

FP9300-A /eth-uplink/fabric/port-channel # top
FP9300-A# connect fxos
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2017, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

<--- remaining lines removed for brevity --->
FP9300-A (fxos) #
    
```

단계 4 show 명령을 입력하여 지정된 포트 채널에 대한 상태 정보를 표시합니다.

예제:

```

FP9300-A /eth-uplink/fabric/port-channel # show

Port Channel:
      Port Channel Id Name          Port Type          Admin
      State Oper State            State Reason
      -----
-----
      10                        Port-channel10    Data              Enabl
ed      Failed                    No operational members
FP9300-A /eth-uplink/fabric/port-channel #
    
```

단계 5 show member-port 명령을 입력하여 포트 채널의 멤버 포트에 대한 상태 정보를 표시합니다.

예제:

```

FP9300-A /eth-uplink/fabric/port-channel # show member-port

Member Port:
      Port Name            Membership          Oper State          State Reas
on
      -----
-----
      Ethernet2/3          Suspended          Failed              Suspended
      Ethernet2/4          Suspended          Failed              Suspended
FP9300-A /eth-uplink/fabric/port-channel #
    
```

포트 채널은 논리적 디바이스에 할당될 때까지 나타나지 않습니다. 포트 채널이 논리적 디바이스에서 제거되거나 논리적 디바이스가 삭제된 경우, 포트 채널은 **Suspended(유예)** 상태로 되돌아갑니다.

단계 6 추가 포트 채널 및 LACP 정보를 보려면 `/eth-uplink/fabric/port-channel` 모드를 종료하고 다음 명령을 입력하여 `fxos` 모드를 시작합니다.

- **top**
- **connect fxos**

예제:

단계 7 **show port-channel summary** 명령을 입력하여 현재 포트 채널에 대한 요약 정보를 표시합니다.

예제:

```
FP9300-A(fxos)# show port-channel summary
Flags: D - Down                P - Up in port-channel (members)
       I - Individual          H - Hot-standby (LACP only)
       s - Suspended           r - Module-removed
       S - Switched            R - Routed
       U - Up (port-channel)
       M - Not in use. Min-links not met

-----
Group Port-      Type      Protocol  Member Ports
  Name Channel
-----
10    Po10 (SD)   Eth       LACP      Eth2/3 (s)  Eth2/4 (s)
11    Po11 (SD)   Eth       LACP      Eth2/1 (s)  Eth2/2 (s)
12    Po12 (SD)   Eth       LACP      Eth1/4 (D)  Eth1/5 (D)
48    Po48 (SU)   Eth       LACP      Eth1/1 (P)  Eth1/2 (P)
```

추가 **show port-channel** 및 **show lacp** 명령은 `fxos` 모드에서 사용할 수 있습니다. 이러한 명령은 다양한 포트 채널 및 용량, 트래픽, 카운터, 사용량 등 LACP 정보를 표시하는 데 사용할 수 있습니다.

다음에 할 작업

포트 채널 생성 관련 정보는 [포트 채널 생성](#), 127 페이지의 내용을 참조하십시오.

소프트웨어 장애 복구

시작하기 전에

시스템을 성공적으로 부팅되지 못하게 하는 소프트웨어 장애가 발생하는 경우 다음 절차를 사용하여 새 버전의 소프트웨어를 부팅할 수 있습니다. 이 프로세스를 완료하려면 KickStart 이미지 TFTP 부팅이 필요하며 새 시스템 및 관리자 이미지를 다운로드한 다음 새 이미지를 사용하여 부팅해야 합니다.

특정한 FXOS 버전의 복구 이미지는 다음 위치 중 하나의 Cisco.com에서 다운로드할 수 있습니다.

- Firepower 9300 — <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 Series — <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

복구 이미지에는 3개의 개별 파일이 들어 있습니다. 예를 들어 아래는 FXOS 2.1.1.64용 최신 복구 이미지입니다.

Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA

절차

단계 1 ROMMON에 액세스합니다.

- 콘솔 포트에 연결합니다.
- 시스템을 재부팅합니다.
로딩이 시작되고 이 프로세스 동안 카운트다운 타이머가 표시됩니다.
- ROMMON 모드를 입력하려면 카운트다운 중에 **Escape(이스케이프)** 키를 누릅니다.

예제:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user
```

```
Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
```

```
Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa
```

```
find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA
bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA
```

```
Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.
```

```
rommon 1 >
```

단계 2 TFTP가 KickStart 이미지를 부팅합니다.

- a) 관리 IP 주소, 관리 넷마스크 및 게이트웨이 IP 주소가 올바르게 설정되었는지 확인합니다. **set** 명령을 사용하여 이러한 값을 볼 수 있습니다. **ping** 명령을 사용하여 TFTP 서버에 대한 연결을 테스트할 수 있습니다.

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

- b) KickStart 이미지를 Firepower 4100/9300 새시에서 액세스 가능한 TFTP 디렉토리에 복사합니다.
참고 KickStart 이미지 버전 번호는 번들 버전 번호와 일치하지 않습니다. FXOS 버전과 KickStart 이미지 간의 매핑을 보여주는 정보는 Cisco.com 소프트웨어 다운로드 페이지에서 확인할 수 있습니다.
- c) boot 명령을 사용하여 ROMMON에서 이미지를 부팅합니다.

```
boot tftp://<IP address>/<path to image>
```

참고 USB 미디어 디바이스를 Firepower 4100/9300 새시의 전면 패널에 있는 USB 슬롯에 삽입하여 ROMMON에서 KickStart를 부팅할 수도 있습니다. 시스템 실행 중에 USB 디바이스가 삽입된 경우, USB 디바이스를 인식하기 전에 시스템을 재부팅해야 합니다. 시스템에 이미지를 수신하는 중이며 그 다음에 KickStart 이미지가 로드될 것임을 나타내는 연속된 #이 표시됩니다.

예제:

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....
Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2
#####
```



```
#####
#####
File reception completed.
```

단계 3 방금 Firepower 4100/9300 새시에 로드한 KickStart 이미지와 일치하는 복구 시스템 및 관리자 이미지를 다운로드합니다.

a) 복구 시스템 및 관리자 이미지를 다운로드하려면 관리 IP 주소와 게이트웨이를 설정해야 합니다. USB를 통해 이 이미지를 다운로드할 수 없습니다.

```
switch(boot)# config terminal
switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address <ip address> <netmask>
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway <gateway>
switch(boot) (config)# exit
```

b) 원격 서버에서 부트플래시로 복구 시스템 및 관리자 이미지를 복사합니다.
switch(boot)# copy URL bootflash:

다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- ftp://username@hostname/path/image_name
- scp://username@hostname/path/image_name
- sftp://username@hostname/path/image_name
- tftp://hostname/path/image_name

예제:

```
switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:

switch(boot)# copy
  scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
```

c) 이미지를 Firepower 4100/9300 새시에 성공적으로 복사한 후에 nuova-sim-mgmt-nsg.0.1.0.001.bin에서 관리자 이미지에 기호화된 링크를 설정합니다. 이 링크는 로드 메커니즘이 어떤 관리자 이미지를 로드할지 알려줍니다. 이 기호화된 링크의 이름은 로드하려고 시도 중인 이미지와 관계없이 항상 nuova-sim-mgmt-nsg.0.1.0.001.bin이어야 합니다.

```
switch(boot)# copy bootflash:<manager-image>
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin
```

예제:

```
switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.

switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway 10.0.0.1
```

```

switch(boot) (config) # exit
switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot) #

```

단계 4 방금 다운로드한 시스템 이미지를 로드합니다.

```
switch(boot) # load bootflash:<system-image>
```

예제:

```
switch(boot) # load bootflash:fxos-k9-system.5.0.3.N2.4.11.69.SPA
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA
```

```

Manager image digital signature verification successful
...
System is coming up ... Please wait ...

```

```

Cisco FPR Series Security Appliance
FP9300-A login:

```

단계 5 복구 이미지를 로드한 후 다음 명령을 입력하여 시스템이 이전 이미지 로딩을 시도하지 못하게 합니다.

참고 이 단계는 복구 이미지를 로드한 후 바로 수행해야 합니다.

```

FP9300-A# scope org
FP9300-A /org # scope fw-platform-pack default
FP9300-A /org/fw-platform-pack # set platform-bundle-version ""
Warning: Set platform version to empty will result software/firmware incompatibility issue.
FP9300-A /org/fw-platform-pack* # commit-buffer

```

단계 6 Firepower 4100/9300 새시에서 사용할 플랫폼 번들 이미지를 다운로드 및 설치합니다. 자세한 내용은 [이미지 관리, 41 페이지](#)를 참조하십시오.

예제:

```

FP9300-A# scope firmware
FP9300-A /firmware # show download-task

```

```

Download task:
  File Name Protocol Server          Port      Userid      State

```

```

-----
fxos-k9.2.1.1.73.SPA
Tftp 192.168.1.2 0 Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
    
```

손상된 파일 시스템 복구

시작하기 전에

수퍼바이저의 온보드 플래시가 손상되었으며 시스템을 더 이상 성공적으로 시작할 수 없는 경우, 다음 절차를 사용하여 시스템을 복구할 수 있습니다. 이 프로세스를 완료하려면 KickStart 이미지 TFTP 부팅이 필요하며 플래시를 다시 포맷하고 새 시스템 및 관리자 이미지를 다운로드한 다음 새 이미지를 사용하여 부팅해야 합니다.



참고 이 절차에는 시스템 플래시 재포맷이 포함됩니다. 따라서 시스템이 복구된 후에 시스템을 완전히 다시 구성해야 합니다.

특정한 FXOS 버전의 복구 이미지는 다음 위치 중 하나의 Cisco.com에서 다운로드할 수 있습니다.

- Firepower 9300 — <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286287252&flowid=77282&softwareid=286287263>
- Firepower 4100 Series — <https://software.cisco.com/portal/pub/download/portal/select.html?&mdfid=286305187&flowid=79423&softwareid=286287263>

복구 이미지에는 3개의 개별 파일이 들어 있습니다. 예를 들어 아래는 FXOS 2.1.1.64용 복구 이미지입니다.

Recovery image (kickstart) for FX-OS 2.1.1.64.
fxos-k9-kickstart.5.0.3.N2.4.11.63.SPA

Recovery image (manager) for FX-OS 2.1.1.64.
fxos-k9-manager.4.1.1.63.SPA

Recovery image (system) for FX-OS 2.1.1.64.
fxos-k9-system.5.0.3.N2.4.11.63.SPA

절차

단계 1 ROMMON에 액세스합니다.

- a) 콘솔 포트에 연결합니다.
- b) 시스템을 재부팅합니다.

로딩이 시작되고 이 프로세스 동안 카운트다운 타이머가 표시됩니다.

- c) ROMMON 모드를 입력하려면 카운트다운 중에 **Escape(이스케이프)** 키를 누릅니다.

예제:

```
Cisco System ROMMON, version 1.0.09, RELEASE SOFTWARE
Copyright (c) 1994-2015 by Cisco Systems, Inc.
Compiled Sun 01/01/1999 23:59:59.99 by user

Current image running: Boot ROM0
Last reset cause: LocalSoft
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address aa:aa:aa:aa:aa:aa

find the string ! boot bootflash:/installables/switch/fxos-k9-kickstart.5.0.3.N2.0.00.00.SPA

bootflash:/installables/switch/fxos-k9-system.5.0.3.N2.0.00.00.SPA

Use BREAK, ESC or CTRL+L to interrupt boot.
use SPACE to begin boot immediately.
Boot interrupted.

rommon 1 >
```

단계 2 TFTP가 KickStart 이미지를 부팅합니다.

- a) 관리 IP 주소, 관리 넷마스크 및 게이트웨이 IP 주소가 올바르게 설정되었는지 확인합니다. **set** 명령을 사용하여 이러한 값을 볼 수 있습니다. **ping** 명령을 사용하여 TFTP 서버에 대한 연결을 테스트할 수 있습니다.

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "
rommon > address <ip-address>
rommon > netmask <network-mask>
rommon > gateway <default-gateway>
```

- b) KickStart 이미지를 Firepower 4100/9300 채시에서 액세스 가능한 TFTP 디렉토리에 복사합니다.

참고 KickStart 이미지 버전 번호는 번들 버전 번호와 일치하지 않습니다. FXOS 버전과 KickStart 이미지 간의 매핑을 보여주는 정보는 Cisco.com 소프트웨어 다운로드 페이지에서 확인할 수 있습니다.

- c) boot 명령을 사용하여 ROMMON에서 이미지를 부팅합니다.

```
boot tftp://<IP address>/<path to image>
```

참고 USB 미디어 디바이스를 Firepower 4100/9300 채시의 전면 패널에 있는 USB 슬롯에 삽입하여 ROMMON에서 KickStart를 부팅할 수도 있습니다. 시스템 실행 중에 USB 디바이스가 삽입된 경우, USB 디바이스를 인식하기 전에 시스템을 재부팅해야 합니다.

시스템에 이미지를 수신하는 중이며 그 다음에 KickStart 이미지가 로드될 것임을 나타내는 연속된 #이 표시됩니다.

예제:

```
rommon 1 > set
ADDRESS=
NETMASK=
GATEWAY=
SERVER=
IMAGE=
PS1="ROMMON ! > "

rommon 2 > address 10.0.0.2
rommon 3 > netmask 255.255.255.0
rommon 4 > gateway 10.0.0.1
rommon 5 > ping 10.0.0.2
..!!!!!!
Success rate is 100 percent (10/10)
rommon 6 > ping 192.168.1.2
..!!!!!!
Success rate is 100 percent (10/10)

rommon 7 > boot tftp://192.168.1.2/fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA
ADDRESS: 10.0.0.2
NETMASK: 255.255.255.0
GATEWAY: 10.0.0.1
SERVER: 192.168.1.2
IMAGE: fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA

TFTP_MACADDR: aa:aa:aa:aa:aa:aa
.....
Receiving fxos-k9-kickstart.5.0.3.N2.1.11.1.SPA from 192.168.1.2

#####
#####
#####

File reception completed.
```

단계 3 KickStart 이미지가 로드된 후 **init system** 명령을 사용하여 플래시를 다시 포맷합니다. **init system** 명령은 시스템에 다운로드한 모든 소프트웨어 이미지와 시스템의 모든 컨피그레이션을 비롯하여 플래시의 콘텐츠를 지웁니다. 이 명령은 완료하는 데 약 20~30분이 소요됩니다.

예제:

```
switch(boot)# init system

This command is going to erase your startup-config, licenses as well as the contents of
your bootflash:.

Do you want to continue? (y/n) [n] y

Detected 32GB flash...
Initializing the system
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test): done
Initializing startup-config and licenses
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test): done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test): done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test): done
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test): done
Formatting bootflash:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test): done
Formatting SAM partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test): done
```

```

Formatting Workspace partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done
Formatting Sysdebug partition:
mke2fs 1.35 (28-Feb-2004)
Checking for bad blocks (read-only test):           done

```

단계 4 복구 이미지를 Firepower 4100/9300 새시에 다운로드합니다.

- a) 복구 이미지를 다운로드하려면 관리 IP 주소와 게이트웨이를 설정해야 합니다. USB를 통해 이 이미지를 다운로드할 수 없습니다.

```

switch(boot)# config terminal
switch(boot) (config)# interface mgmt 0
switch(boot) (config-if)# ip address <ip address> <netmask>
switch(boot) (config-if)# no shutdown
switch(boot) (config-if)# exit
switch(boot) (config)# ip default-gateway <gateway>
switch(boot) (config)# exit

```

- b) 원격 서버에서 부트플래시로 세 복구 이미지를 모두 복사합니다.

```
switch(boot)# copy URL bootflash:
```

다음 구문 중 하나를 사용하여 가져올 파일의 URL을 지정합니다.

- **ftp://username@hostname/path/image_name**
- **scp://username@hostname/path/image_name**
- **sftp://username@hostname/path/image_name**
- **tftp://hostname/path/image_name**

예제:

```

switch(boot) # copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
bootflash:

switch(boot) # copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
bootflash:

switch(boot) # copy
scp://<username>@192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
bootflash:

```

- c) 이미지를 Firepower 4100/9300 새시에 성공적으로 복사한 후에 `nuova-sim-mgmt-nsg.0.1.0.001.bin`에서 관리자 이미지에 기호화된 링크를 설정합니다. 이 링크는 로드 메커니즘이 어떤 관리자 이미지를 로드할지 알려줍니다. 이 기호화된 링크의 이름은 로드하려고 시도 중인 이미지와 관계없이 항상 `nuova-sim-mgmt-nsg.0.1.0.001.bin`이어야 합니다.

```

switch(boot) # copy bootflash:<manager-image>
bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

```

예제:

```

switch(boot)# config terminal
Enter configuration commands, one per line. End with CNTL/Z.

switch(boot) (config)# interface mgmt 0

```

```

switch(boot) (config-if) # ip address 10.0.0.2 255.255.255.0
switch(boot) (config-if) # no shutdown
switch(boot) (config-if) # exit
switch(boot) (config) # ip default-gateway 10.0.0.1
switch(boot) (config) # exit
switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-system.5.0.3.N2.4.11.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy
  tftp://192.168.1.2/recovery_images/fxos-k9-manager.4.1.1.69.SPA
  bootflash:
Trying to connect to tftp server.....
Connection to server Established. Copying Started.....
/
TFTP get operation was successful
Copy complete, now saving to disk (please wait)...

switch(boot) # copy bootflash:fxos-k9-manager.4.1.1.69.SPA
  bootflash:nuova-sim-mgmt-nsg.0.1.0.001.bin

Copy complete, now saving to disk (please wait)...

switch(boot) #

```

단계 5 스위치를 다시 로드합니다.

```
switch(boot) # reload
```

예제:

```

switch(boot) # reload
This command will reboot this supervisor module. (y/n) ? y
[ 1866.310313] Restarting system.

```

```
!! Rommon image verified successfully !!
```

```

Cisco System ROMMON, Version 1.0.11, RELEASE SOFTWARE
Copyright (c) 1994-2016 by Cisco Systems, Inc.
Compiled Wed 11/23/2016 11:23:23.47 by builder
Current image running: Boot ROM1
Last reset cause: ResetRequest
DIMM Slot 0 : Present
DIMM Slot 1 : Present
No USB drive !!
BIOS has been locked !!

```

```

Platform FPR9K-SUP with 16384 Mbytes of main memory
MAC Address: bb:aa:77:aa:aa:bb

```

```

autoboot: Can not find autoboot file 'menu.lst.local'
Or can not find correct boot string !!

```

```
rommon 1 >
```

단계 6 KickStart 이미지 및 시스템 이미지에서 부팅합니다.

```
rommon 1 > boot <kickstart-image> <system-image>
```

참고 시스템 이미지를 로드하는 동안 라이선스 관리자 장애 메시지가 표시될 수 있습니다. 이러한 메시지는 안전하게 무시할 수 있습니다.

예제:

```
rommon 1 > dir
Directory of: bootflash:\

01/01/12 12:33a <DIR>          4,096 .
01/01/12 12:33a <DIR>          4,096 ..
01/01/12 12:16a <DIR>        16,384 lost+found
01/01/12 12:27a             34,333,696 fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA
01/01/12 12:29a            330,646,465 fxos-k9-manager.4.1.1.69.SPA
01/01/12 12:31a            250,643,172 fxos-k9-system.5.0.3.N2.4.11.69.SPA
01/01/12 12:34a            330,646,465 nuova-sim-mgmt-nsg.0.1.0.001.bin
      4 File(s) 946,269,798 bytes
      3 Dir(s)
```

```
rommon 2 > boot fxos-k9-kickstart.5.0.3.N2.4.11.69.SPA fxos-k9-system.5.0.3.N2.4.11.69.SPA
!! Kickstart Image verified successfully !!

Linux version: 2.6.27.47 (security@cisco.com) #1 SMP Thu Nov 17 18:22:00 PST 2016
[ 0.000000] Fastboot Memory at 0c100000 of size 201326592
Usage: init 0123456SsQqAaBbCcUu

INIT: version 2.86 booting

POST INIT Starts at Sun Jan 1 00:27:32 UTC 2012
S10mount-ramfs.supnuovaca Mounting /isan 3000m
Mounted /isan
Creating /callhome..
Mounting /callhome..
Creating /callhome done.
Callhome spool file system init done.
Platform is BS or QP MIO: 30
FPGA Version 0x00010500 FPGA Min Version 0x00000600
Checking all filesystems..r.r..r done.
Warning: switch is starting up with default configuration
Checking NVRAM block device ... done
.
FIPS power-on self-test passed
Unpack CMC Application software
Loading system software
Uncompressing system image: bootflash:/fxos-k9-system.5.0.3.N2.4.11.69.SPA

Manager image digital signature verification successful

...

System is coming up ... Please wait ...
nohup: appending output to `nohup.out'

---- Basic System Configuration Dialog ----

This setup utility will guide you through the basic configuration of
the system. Only minimal configuration including IP connectivity to
the Fabric interconnect and its clustering mode is performed through these steps.

Type Ctrl-C at any time to abort configuration and reboot system.
To back track or make modifications to already entered values,
complete input till end of section and answer no when prompted
to apply configuration.
```


You have chosen to setup a new Security Appliance. Continue? (y/n):

단계 7 이미지를 로드한 후, 초기 컨피그레이션 설정을 입력하라는 프롬프트가 표시됩니다. 자세한 내용은 [초기 컨피그레이션, 6 페이지](#)를 참조하십시오.

단계 8 Firepower 4100/9300 새시에서 사용할 플랫폼 번들 이미지를 다운로드합니다. 플랫폼 번들 이미지 버전은 시스템 복구에 사용한 이미지와 일치해야 합니다. 자세한 내용은 [이미지 관리, 41 페이지](#)를 참조하십시오.

예제:

```
FP9300-A# scope firmware
FP9300-A /firmware # show download-task

Download task:
-----
File Name Protocol Server          Port      Userid      State
-----
fxos-k9.2.1.1.73.SPA
      Tftp      192.168.1.2          0          Downloaded
FP9300-A /firmware # show package fxos-k9.2.1.1.73.SPA detail
Firmware Package fxos-k9.2.1.1.73.SPA:
  Version: 2.1(1.73)
  Type: Platform Bundle
  State: Active
Time Stamp: 2012-01-01T07:40:28.000
Build Date: 2017-02-28 13:51:08 UTC
FP9300-A /firmware #
```

단계 9 플랫폼 번들을 성공적으로 다운로드한 후에는 나중에 시스템을 로드할 때 사용할 수 있도록 KickStart 및 시스템 이미지를 수동으로 활성화해야 합니다. 실행 중인 버전과 제안된 시작 버전이 일치하기 때문에 이 절차를 사용하여 손상된 파일 시스템을 복구하는 경우 자동 활성화가 지원되지 않습니다.

a) Fabric-interconnect a에 대한 범위를 설정합니다.

```
FP9300-A# scope fabric-interconnect a
```

b) **show version** 명령을 사용하여 실행 중인 커널 버전과 실행 중인 시스템 버전을 확인합니다. 이러한 문자열을 사용하여 이미지를 활성화합니다.

```
FP9300-A /fabric-interconnect # show version
```

c) 다음 명령을 입력하여 이미지를 활성화합니다.

```
FP9300-A /fabric-interconnect # activate firmware
      kernel-version <running_kernel_version> system-version <running_system_version>
commit-buffer
```

참고 서버 상태가 “Disk Failed”(디스크 장애 발생)로 변경될 수 있습니다. 이 메시지에 대해서는 걱정하지 않아도 되며 절차를 계속 수행할 수 있습니다.

d) **show version** 명령을 사용하여 시작 버전이 올바르게 설정되었는지 확인하고 이미지의 활성화 상태를 모니터링합니다.

중요 상태가 “Activating”(활성화)에서 “Ready”(준비)로 변경될 때까지 다음 단계를 진행하지 마십시오.

```
FP9300-A /fabric-interconnect # show version
```

예제:

```

FP9300-A /firmware # top
FP9300-A# scope fabric-interconnect a
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers:
  Startup-Sys-Vers:
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

FP9300-A /fabric-interconnect # activate firmware kernel-version
5.0(3)N2(4.11.69) system-version 5.0(3)N2(4.11.69)
Warning: When committed this command will reset the end-point
FP9300-A /fabric-interconnect* # commit-buffer
FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Activating
  Act-Sys-Status: Activating
  Bootloader-Vers:

FP9300-A /fabric-interconnect # show version
Fabric Interconnect A:
  Running-Kern-Vers: 5.0(3)N2(4.11.69)
  Running-Sys-Vers: 5.0(3)N2(4.11.69)
  Package-Vers: 2.1(1.73)
  Startup-Kern-Vers: 5.0(3)N2(4.11.69)
  Startup-Sys-Vers: 5.0(3)N2(4.11.69)
  Act-Kern-Status: Ready
  Act-Sys-Status: Ready
  Bootloader-Vers:

```

단계 10 시스템을 재부팅합니다.

예제:

```

FP9300-A /fabric-interconnect # top
FP9300-A# scope chassis 1
FP9300-A /chassis # reboot no-prompt
Starting chassis reboot. Monitor progress with the command "show fsm status"
FP9300-A /chassis #

```

마지막으로 Firepower 4100/9300 새시의 전원을 끈 다음 다시 시작하기 전에 시스템은 각 보안 모듈/엔진의 전원을 끕니다. 이 프로세스에는 약 5~10분이 소요됩니다.

단계 11 시스템 상태를 모니터링합니다. 서버 상태는 “Discovery”(검색)에서 “Config”(구성)로 변경된 후 최종적으로 “Ok”(정상)가 되어야 합니다.

예제:

```

FP9300-A# show server status

```

Server	Slot	Status	Overall Status	Discovery
1/1	Equipped		Discovery	In Progress
1/2	Equipped		Discovery	In Progress
1/3	Empty			

```

FP9300-A# show server status

```

```

Server Slot Status Overall Status Discovery
-----
1/1 Equipped Config Complete
1/2 Equipped Config Complete
1/3 Empty

FP9300-A# show server status
Server Slot Status Overall Status Discovery
-----
1/1 Equipped Ok Complete
1/2 Equipped Ok Complete
1/3 Empty
    
```

Overall Status(전체 상태)가 “Ok”(정상)인 경우, 시스템이 복구된 것입니다. 하지만 그래도 보안 어플라이언스를 다시 구성(라이선스 컨피그레이션 포함)하고 논리적 디바이스를 다시 생성해야 합니다. 자세한 내용:

- Firepower 9300 빠른 시작 가이드 —<http://www.cisco.com/go/firepower9300-quick>
- Firepower 9300 컨피그레이션 가이드 —<http://www.cisco.com/go/firepower9300-config>
- Firepower 4100 Series 빠른 시작 가이드 —<http://www.cisco.com/go/firepower4100-quick>
- Firepower 4100 Series 컨피그레이션 가이드 —<http://www.cisco.com/go/firepower4100-config>



색 인

A

- 관리 IP 주소 [70](#)
 - 변경 [70](#)
- 구성 [99, 100, 101, 103, 104](#)
 - HTTPS [99, 100, 101, 103, 104](#)
- 기록, 비밀번호 [29](#)

B

- 날짜 [86, 87](#)
 - 보기 [86](#)
 - 수동 설정 [87](#)
- 날짜 및 시간 [85](#)
 - 구성 [85](#)
- 논리적 디바이스 [44, 132, 133, 135, 143, 147, 149, 161, 162](#)
 - 독립형 생성 [133, 135](#)
 - 삭제 [162](#)
 - 애플리케이션 인스턴스 삭제 [162](#)
 - 연결 [161](#)
 - 연결 종료 [161](#)
 - 이미지 버전 업데이트 [44](#)
 - 이해 [132](#)
 - 클러스터 생성 [143, 147, 149](#)
- 논리적 디바이스 연결 종료 [161](#)
- 논리적 디바이스에 연결 [161](#)
- 높은 레벨의 작업 목록 [5](#)

C

- 디바이스 이름 [74](#)
 - 변경 [74](#)

D

- DNS [121](#)

F

- 배너 [75, 76, 77](#)
 - pre-login [75, 76, 77](#)
- 보안 모듈 [169, 170, 171](#)
 - 서비스 해제 [169](#)
 - 승인 [169](#)
 - 재설정 [170](#)
 - 재초기화 [170](#)
 - 전원 끄기 [171](#)
 - 전원 켜기 [171](#)
- 보안 모듈 서비스 해제 [169](#)
- 보안 모듈 승인 [169](#)
- 보안 모듈 재설정 [170](#)
- 보안 모듈 재초기화 [170](#)
- 보안 모듈 전원 켜기/끄기 [171](#)
- 브레이크아웃 케이블 [129](#)
 - 구성 [129](#)
- 브레이크아웃 포트 [129](#)
- 비밀번호 [25, 29, 30](#)
 - 기록 수 [29](#)
 - 변경 간격 [30](#)
 - 보안 수준 확인 [30](#)
 - 지침 [25](#)
- 비밀번호 프로필 [29, 40](#)
 - 비밀번호 기록 지우기 [40](#)
 - 정보 [29](#)

G

- 사용자 [23, 24, 25, 29, 30, 37, 39, 40, 96, 97](#)
 - SNMP [96, 97](#)

사용자 (계속)

- 관리 [23](#)
- 기본 인증 [30](#)
- 로컬 인증 [29, 40](#)
- 명명 지침 [24](#)
- 비밀번호 지침 [25](#)
- 비활성화 [39](#)
- 삭제 [39](#)
- 생성 [37](#)
- 설정 [30](#)
- 역할 [29](#)
- 활성화 [39](#)

사용자 어카운트 [29, 40](#)

- 비밀번호 프로필 [29, 40](#)

사용자 인터페이스 [1](#)

- 개요 [1](#)

사전 로그인 배너 [75, 76, 77](#)

- 삭제 [77](#)
- 생성 [75](#)
- 수정 [76](#)

새시 [2, 6](#)

- 상태 모니터링 [2](#)
- 초기 컨피그레이션 [6](#)

새시 관리자 [1](#)

- 사용자 인터페이스 개요 [1](#)

새시 상태 모니터링 [2](#)세션 시간 제한 [33, 34](#)소프트웨어 장애 [188](#)

- 복구 중 [188](#)

손상된 파일 시스템 [193](#)

- 복구 중 [193](#)

시간 [86, 87](#)

- 보기 [86](#)
- 수동 설정 [87](#)

시간 제한 [33, 34](#)

- HTTPS, SSH 및 텔넷 [33, 34](#)
- 콘솔 [33, 34](#)

시스템 복구 [188, 193](#)

H

어카운트 [29, 40](#)

- 로컬 인증 [29, 40](#)

위협 방어 [135, 143, 149, 161, 162](#)

- 논리적 디바이스 삭제 [162](#)
- 독립형 Threat Defense 논리적 디바이스 생성 [135](#)

위협 방어 (계속)

- 애플리케이션 인스턴스 삭제 [162](#)
- 연결 [161](#)
- 연결 종료 [161](#)
- 클러스터 생성 [143, 149](#)

이미지 [41, 42, 43](#)

- Cisco.com에서 다운로드 [42](#)
- Firepower eXtensible 운영 체제 플랫폼 번들 업그레이드 [43](#)
- Firepower Security Appliance에 업로드 [42](#)
- 관리 [41](#)
- 무결성 확인 [43](#)

이미지 버전 [44](#)

- 업데이트 [44](#)

인증 [30](#)

- 기본값 [30](#)

인증서 [98](#)

- 정보 [98](#)

인터페이스 [126, 127](#)

- 관리 상태 [127](#)
- 구성 [126](#)
- 속성 [126](#)

I

자동 로그아웃 [69](#)작업 플로우 [5](#)재부팅 [77](#)정보 [91](#)

- 정보 [91](#)

J

초기 컨피그레이션 [6](#)

K

커뮤니티, SNMP [94](#)컨피그레이션 가져오기 [173](#)컨피그레이션 가져오기/내보내기 [173](#)

- 제한 사항 [173](#)

- 지침 [173](#)

컨피그레이션 내보내기 [173](#)콘솔 [33, 34](#)

- 시간 제한 [33, 34](#)

클러스터 **137, 143, 146, 147, 149**

 생성 **143, 147, 149**

 생성 시 기본값 **146**

 정보 **137**

클러스터링 **139, 140, 142, 144, 146**

 spanning-tree portfast **144**

 관리 **140**

 네트워크 **140**

 디바이스-로컬 EtherChannel, 스위치에서 구성 **146**

 멤버 요건 **142**

 소프트웨어 업그레이드 **142**

 소프트웨어 요건 **142**

 클러스터 제어 링크 **139**

 크기 **139**

키 링 **98, 99, 100, 101, 103, 104, 107**

 삭제 **107**

 생성 **99**

 인증서 가져오기 **104**

 인증서 요청 **100, 101**

 재생성 **99**

 정보 **98**

 트러스트 포인트 **103**

L

텔넷 **33, 34, 90**

 구성 **90**

 시간 제한 **33, 34**

통신 서비스 **94, 99, 100, 101, 103, 104**

 HTTPS **99, 100, 101, 103, 104**

 SNMP **94**

트랩 **91, 95, 96**

 삭제 **96**

 생성 **95**

 정보 **91**

트러블슈팅 **186**

 포트 채널 상태 **186**

트러스트 포인트 **98, 103, 107**

 삭제 **107**

 생성 **103**

 정보 **98**

M

패킷 캡처 **179, 180, 182, 183, 184**

 PCAP 파일 다운로드 **184**

패킷 캡처 (계속)

 패킷 캡처 세션 삭제 **184**

 패킷 캡처 세션 생성 **180**

 패킷 캡처 세션 시작 **183**

 패킷 캡처 세션 중지 **183**

 필터 **182**

패킷 캡처 세션 삭제 **184**

패킷 캡처 세션 생성 **180**

패킷 캡처 파일 다운로드 **184**

펌웨어 **45**

 업그레이드 **45**

펌웨어 업그레이드 **45**

포트 채널 **127, 186**

 status **186**

 구성 **127**

표준 시간대 **86, 87**

 설정 **86, 87**

프로필 **29**

 비밀번호 **29**

플랫폼 번들 **41, 42, 43**

 Cisco.com에서 다운로드 **42**

 Firepower Security Appliance에 업로드 **42**

 무결성 확인 **43**

 업그레이드 **43**

 정보 **41**

P

PCAP, 참조 패킷 캡처

PCAP 파일 **184**

 다운로드 **184**

ping **185**

PKI **98**

R

RADIUS **113, 114, 115**

RADIUS 제공자 **114, 115**

 삭제 **115**

 생성 **114**

rommon **45**

 업그레이드 **45**

RSA **98**

S

Smart Call Home **16**
 HTTP 프록시 구성 **16**
 SNMP **91, 92, 93, 94, 95, 96, 97**
 권한 **92**
 버전 3 보안 기능 **93**
 보안 레벨 **92**
 사용자 **96, 97**
 삭제 **97**
 생성 **96**
 알림 **91**
 정보 **91**
 지원 **91, 93**
 커뮤니티 **94**
 트랩 **95, 96**
 삭제 **96**
 생성 **95**
 활성화 **94**
 SNMPv3 **93**
 보안 기능 **93**
 SSH **33, 34, 88**
 구성 **88**
 시간 제한 **33, 34**
 syslog **118**
 로컬 대상 구성 **118**
 로컬 소스 구성 **118**

syslog (계속)
 원격 대상 구성 **118**
 system **6**
 초기 컨피그레이션 **6**

T

TACACS+ **116, 117**
 TACACS+ 제공자 **116, 117**
 삭제 **117**
 생성 **116**
 traceroute **185**
 연결 테스트 **185**

W

라이선스 **17**
 등록 **17**
 라이선스 등록 **17**
 로그인 또는 로그아웃 **8**
 로컬 인증 사용자 **29, 40**
 비밀번호 기록 지우기 **40**
 비밀번호 프로필 **29**
 활성화 **94**
 SNMP **94**