Firepower 2100 Series용 Cisco ASA 시작 가이드

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

여기에 명시된 다른 모든 보증에도 불구하고 이러한 공급업체의 모든 문서 파일 및 소프트웨어는 모든 결점을 포함하여 "있는 그대로" 제공됩니다. CISCO 및 위에 언급된 모든 공급업체는 상품성, 특정 목적에의 적합성, 타인의 권리 비침해 또는 처리, 사용, 거래 행위로 발생하는 문제에 대한 묵시적 보증을 포함하여(단, 이에 한하지 않음) 묵시적이든 명시적이든 모든 종류의 보증을 부인합니다.

CISCO 또는 그 공급자는 이 설명서의 사용 또는 사용할 수 없음으로 인한 모든 파생적, 부수적, 직접, 간접, 특별, 징벌적 또는 기타 모든 손해(영업 이익 손실, 영업 중단, 영업 정보 손실, 또는 그 밖의 금전적 손실로 인한 손해를 포함하되 이에 제한되지 않음)에 대하여 어떠한 경우에도 책임을 지지 않으며, 이는 CISCO 또는 그 공급자가 그와 같은 손해의 가능성을 사전에 알고 있던 경우에도 마찬가지입니다.

이 문서에서 사용된 모든 IP(인터넷 프로토콜) 주소와 전화 번호는 실제 주소와 전화 번호가 아닙니다. 이 문서에 포함된 예제, 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.

목 차

시작하기 1

Firepower 2100용 ASA 정보 **1**

FirePOWER 2100이 ASA에서 작동하는 방식 **1**

ASA 및 FXOS 관리 **2**

라이선스 요건 **2**

지원되지 않는 기능 **3**

네트워크에 있는 Firepower 2100 **4**

인터페이스 연결 **5**

Firepower 2100 전원 켜기 **6**

(옵션) Firepower Chassis Manager에서 추가 인터페이스 활성화 **6**

ASDM 실행 및 라이선싱 구성 **7**

ASA 구성 **11**

ASA 및 FXOS CLI 액세스 **12**

ASA 또는 FXOS 콘솔에 연결 **12**

데이터 인터페이스에서 FXOS에 대한 관리 액세스 구성 **13**

SSH를 통해 FXOS에 연결 **14**

FXOS 관리 IP 주소 또는 게이트웨이 변경 **16**

다음 단계 **20**

Firepower Chassis Manager 설정 21

개요 **21**

인터페이스 **22**

인터페이스 구성 **23**

EtherChannel 추가 **23**

모니터링 인터페이스 **24**

논리적 디바이스 **25**

플랫폼 설정 **25**

NTP: 시간 설정 **26**

SSH: SSH 구성 26
SNMP 28
SNMP 정보 28
SNMP 알림 28
SNMP 보안 레벨 및 권한 29
지원되는 SNMP 보안 모델/레벨의 조합 29
SNMPv3 보안 기능 30
SNMP 지원 30
SNMP 구성 31
HTTPS: 포트 변경 33
DHCP: 관리 클라이언트에 대한 DHCP 서버 구성 34
Syslog: Syslog 메시징 구성 34
DNS: DNS 서버 구성 38
FIPS 및 공통 기준: FIPS 및 공통 기준 모드 활성화 38
액세스 목록: 관리 액세스 구성 39
시스템 업데이트 40
사용자 관리 41
사용자 계정 정보 41
계정 유형 41
사용자 역할 41
사용자 계정 만료 42
사용자 계정에 대한 지침 42
사용자 추가 43
사용자 설정 구성 45

1 장

시작하기

이 장에서는 네트워크에 있는 Firepower 2100에서 ASA를 구축하는 방법 및 초기 컨피그레이션을 수행하는 방법을 설명합니다.

- Firepower 2100용 ASA 정보, 1 페이지
- 인터페이스 연결, 5 페이지
- Firepower 2100 전원 켜기, 6 페이지
- (옵션) Firepower Chassis Manager에서 추가 인터페이스 활성화, 6 페이지
- ASDM 실행 및 라이선싱 구성, 7 페이지
- ASA 구성, 11 페이지
- ASA 및 FXOS CLI 액세스, 12 페이지
- 다음 단계, 20 페이지

Firepower 2100용 ASA 정보

Firepower 2100 하드웨어는 Cisco ASA 소프트웨어 또는 Firepower Threat Defense 소프트웨어 중 하나를 실행할 수 있습니다. 이 가이드에서는 Firepower 2100에서 ASA를 사용하는 방법을 설명합니다.

참고 ASA와 Firepower Threat Defense 간을 전환하려면 디바이스에 이미지를 재설치해야 합니다. Cisco ASA 또는 Firepower Threat Defense 디바이스 이미지 재설치를 참조하십시오.

FirePOWER 2100이 ASA에서 작동하는 방식

Firepower 2100은 ASA용 단일 애플리케이션 어플라이언스입니다. Firepower 2100은 FXOS(Firepower eXtensible Operating System)라는 기본 운영 체제를 실행합니다. FXOS에서 기본 운영 파라미터 및 하

드웨어 인터페이스 설정을 구성해야 합니다. 이러한 설정으로는 인터페이스 활성화, EtherChannel, NTP, 이미지 관리 등의 설정이 있습니다. Firepower Chassis Manager 웹 인터페이스 또는 FXOS CLI를 사용할 수 있습니다. 그런 다음 ASDM 또는 ASA CLI를 사용하여 ASA 운영 체제에서 보안 정책을 구성할 수 있습니다.

ASA 및 FXOS 관리

ASA 및 FXOS 운영 체제는 관리 1/1 인터페이스를 공유합니다. 이 인터페이스에는 ASA와 FXOS에 연결하기 위한 별도의 IP 주소가 있습니다.

참고 이 인터페이스는 ASA에서는 관리 1/1이라고 하며 FXOS에서는 MGMT, 관리 0 또는 다른 유사한 이름으로 표시될 수 있습니다. 이 가이드에서는 일관성과 간소화를 위해 이 인터페이스를 관리 1/1이라고 부릅니다.

일부 기능은 FXOS에서 모니터링해야 하며 그 외 기능은 ASA에서 모니터링해야 합니다. 따라서 지속적인 유지 보수를 위해 두 가지 운영 체제를 활용해야 합니다. FXOS에서의 초기 컨피그레이션의 경우 SSH 또는 브라우저(https://192.168.45.45)를 사용하여 기본 192.168.45.45 IP 주소에 연결할 수 있습니다.

ASA의 초기 컨피그레이션의 경우 ASDM을 사용하여 https://192.168.45.1/admin에 연결할 수 있습니다. 나중에 ASDM의 어떤 인터페이스에서든 SSH 액세스를 구성할 수 있습니다.

두 운영 체제는 콘솔 포트에서 사용할 수 있습니다. 초기 연결 시 FXOS CLI에 액세스합니다. **connect asa** 명령을 사용하여 ASA CLI에 액세스할 수 있습니다.

또한, ASA 데이터 인터페이스에서 FXOS 관리를 허용하고 SSH, HTTPS 및 SNMP 액세스를 구성할 수 있습니다. 이 기능은 원격 관리에 유용합니다.

라이선스 요건

Firepower 2100의 ASA는 Cisco Smart Software Licensing을 사용합니다. 인터넷 액세스가 필요한 일반 Smart Software Licensing을 사용하거나 오프라인 관리를 위해 영구 라이선스 예약 또는 Satellite 서버를 구성할 수 있습니다. 이러한 오프라인 라이선싱 방법에 대한 자세한 내용은 Cisco ASA Series 기능 라이선스를 참조하십시오. 이 가이드는 일반 Smart Software Licensing에 적용됩니다.

License Authority에 등록할 때까지 특별 라이선스가 필요한 기능의 컨피그레이션을 변경할 수는 없지만 작업은 달리 영향을 받지 않습니다. 라이선스가 있는 기능은 다음과 같습니다.

- 보안 상황(3개 이상)
- 강력한 암호화(3DES/AES)(통과하는 트래픽용)

표준 라이선스가 필요하지만 디바이스는 기본 기능에 대한 평가 모드에서 실행될 수 있습니다.

ASA는 기본적으로 관리 액세스용으로만 3DES 기능을 포함하므로 License Authority에 연결하고 ASDM을 즉시 사용할 수도 있습니다. ASDM 액세스를 위해 인터페이스는 관리 전용으로 설정되어 있어야 합니다. 또는 강력한 암호화(3DES/AES) 라이선스 전체가 활성화되어 있어야 합니다. 기본 컨

피그레이션은 관리 전용으로 설정된 관리 1/1 인터페이스를 포함합니다. Smart Software Licensing 계정에서 ASA에 대한 등록 토큰을 요청할 때 **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)** 체크 박스를 선택하여 강력한 암호화 라이선스 전체를 적용하십시오(사용하기 위해서는 계정이 유효해야 함). 라이선싱에 대한 자세한 정보는 ASDM 실행 및 라이선싱 구성, 7페이지을 참조하십시오.

참고 Firepower 4100/9300 섀시과 달리 FXOS 컨피그레이션이 아닌 ASA에서 모든 라이선싱 컨피그레이션을 수행합니다.

지원되지 않는 기능

지원되지 않는 **ASA** 기능

Firepower 2100에서는 다음과 같은 ASA 기능이 지원되지 않습니다.

- 통합 라우팅 및 브리징
- 클러스터링
- KCD를 통한 클라이언트리스 SSL VPN
- ASA REST API
- ASA FirePOWER 모듈
- 봇넷 트래픽 필터
- 다음과 같은 검사:
  - SCTP 검사 맵(ACL을 사용하는 SCTP 스테이트풀 검사가 지원됨)
  - 배율
  - GTP/GPRS

지원되지 않는 **FXOS** 기능

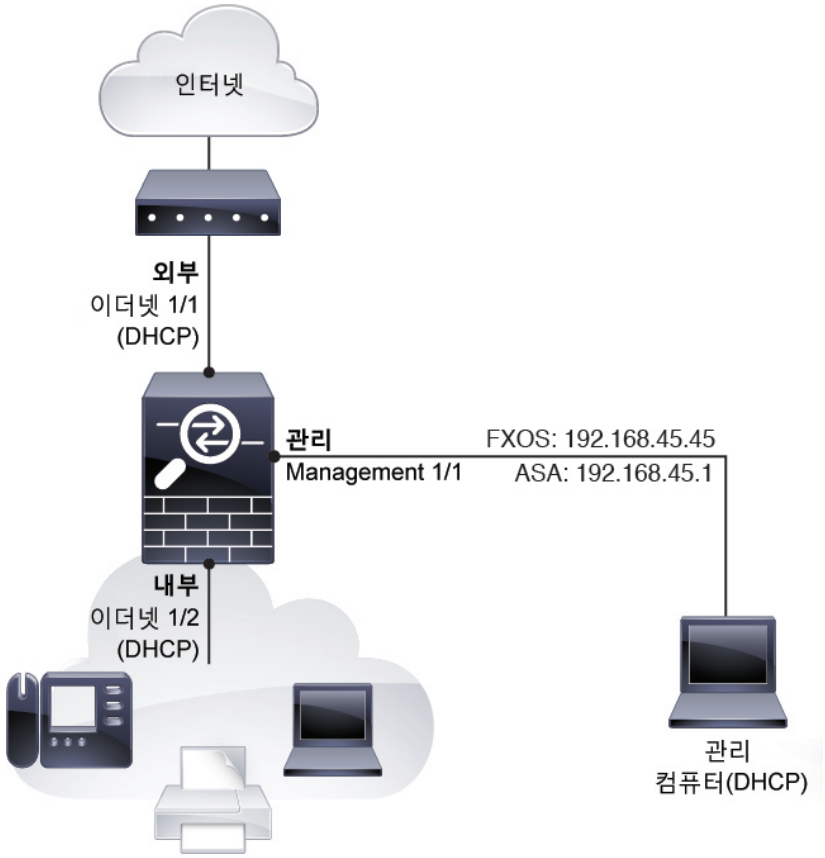
Firepower 2100에서는 다음과 같은 FXOS 기능이 지원되지 않습니다.

- FXOS 컨피그레이션 백업 및 복원
- FXOS를 위한 외부 AAA 인증

네트워크에 있는 **Firepower 2100**

다음 그림에는 Firepower 2100에서의 ASA에 대한 기본 네트워크 구축이 나와 있습니다.

그림 ***1:*** 네트워크에 있는 ***Firepower 2100***의 ***ASA***



이 가이드에 설명되어 있는 초기 설정 이후에 다음 작업을 통한 기본 컨피그레이션으로 위의 네트워크 구축을 활성화합니다.

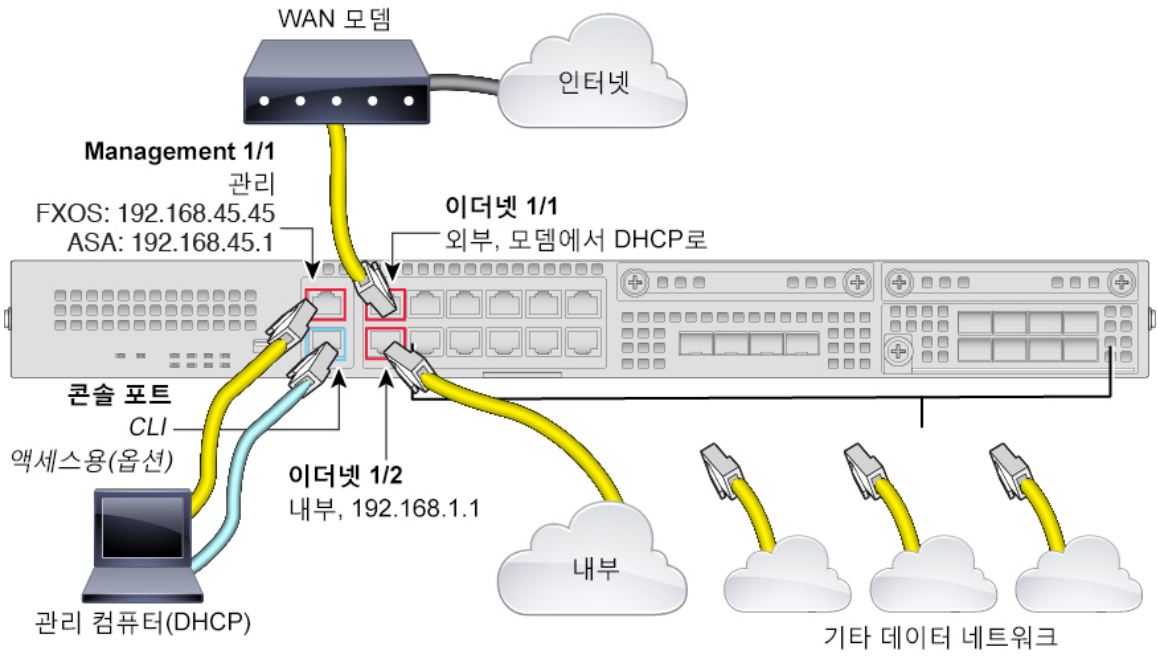
- 내부 **-->** 외부 트래픽 흐름(NAT 포함)
- **DHCP**의 외부 **IP** 주소
- FXOS 및 ASA 관리를 위한 관리 **1/1**. DHCP IP 주소는 이 네트워크에 있는 관리 컴퓨터용으로 FXOS에서 제공됩니다.

인터페이스 연결

관리 1/1 인터페이스에서 Firepower 2100을 관리합니다. FXOS 및 ASA에 동일한 관리 컴퓨터를 사용할 수 있습니다. FXOS IP 주소에서 Firepower Chassis Manager에 연결하여 섀시 컨피그레이션을 수행합니다. 그런 다음 ASDM을 사용하여 ASA IP 주소에 연결해 ASA 컨피그레이션을 완료합니다.

기본 컨피그레이션은 또한 이더넷 1/1을 외부로, 이더넷 1/2를 내부로 구성합니다.

그림 ***2: Firepower 2100*** 인터페이스에 케이블 연결



절차

단계 **1** 관리 1/1(MGMT로 레이블이 지정됨)에 대한 이더넷을 사용하여 관리 컴퓨터를 연결합니다.

단계 **2** (선택 사항) 관리 컴퓨터를 콘솔 포트에 연결합니다. Firepower 2100은 DB-9~RJ-45 시리얼 케이블과 함께 제공되므로 연결을 설정하려면 서드파티 시리얼-USB 케이블이 필요합니다. 운영 체제에 필요한 모든 USB 시리얼 드라이버를 설치해야 합니다.

단계 **3** 외부 네트워크를 이더넷 1/1 포트(WAN으로 레이블이 지정됨)에 연결합니다. Smart Software Licensing의 경우 ASA는 License Authority에 액세스하기 위해 인터넷 액세스를 필요로 합니다.

단계 **4** 내부 네트워크를 이더넷 1/2에 연결하고 필요에 따라 다른 데이터 인터페이스에 연결합니다.

Firepower 2100 전원 켜기

시스템 전원은 섀시 뒷면에 있는 로커 전원 스위치로 제어됩니다. 전원 스위치는 정상적인 종료를 지원하는 소프트 알림 스위치로 구현되어 시스템 소프트웨어 및 데이터 손상의 위험을 줄여줍니다.

절차

단계 **1** 전원 케이블을 Firepower 2100에 연결하고 전기 콘센트에 꽂습니다.

단계 **2** 섀시 뒷면에 있는 전원 스위치를 1 위치로 누릅니다.
섀시의 전원을 끄려면 섀시 뒷면에 있는 전원 스위치를 0 위치로 누릅니다. 스위치가 ON(켜짐)에서 OFF(꺼짐)로 토글된 경우 시스템에서 최종적으로 전원이 꺼지는 데 몇 초 정도가 걸릴 수 있습니다. 이 시간 동안 섀시 전면에 있는 전원 LED가 녹색으로 깜박입니다. 전원 LED가 완전히 꺼질 때까지 전원을 제거하지 마십시오.

단계 **3** 섀시 전면의 전원 LED를 확인합니다. 섀시의 전원이 켜져 있으면 LED가 녹색으로 표시됩니다.

단계 **4** 섀시 전면의 시스템 LED를 확인합니다. 시스템이 전원 켜기 진단을 통과하면 녹색으로 표시됩니다.

(옵션) Firepower Chassis Manager에서 추가 인터페이스 활성화

기본적으로 관리 1/1, 이더넷 1/1 및 이더넷 1/2 인터페이스는 섀시에 대해 물리적으로 활성화되어 있고 ASA 컨피그레이션에서 논리적으로 활성화되어 있습니다. 추가 인터페이스를 사용하려면 이 절차를 사용하여 인터페이스를 섀시에 대해 활성화한 다음 나중에 ASA 컨피그레이션에서 활성화해야 합니다. EtherChannel(포트 채널이라고도 함)을 추가할 수도 있습니다.

시작하기 전에

- Firepower 2100은 Active(활성) 상태인 LACP(Link Aggregation Control Protocol) 모드의 EtherChannel만 지원합니다. 최고의 호환성을 위해 연결 스위치 포트를 Active(활성) 모드로 설정하는 것이 좋습니다.
- 기본값인 관리 IP 주소를 변경하려면 FXOS 관리 IP 주소 또는 게이트웨이 변경, 16페이지를 참조하십시오.

절차

단계 **1** 관리 1/1 인터페이스에 연결된 관리 컴퓨터에서 **https://192.168.45.45** URL로 이동하여 Firepower Chassis Manager를 시작합니다.

단계 **2** 기본 사용자 이름(**admin**)과 비밀번호(**Admin123**)를 입력합니다.

System(시스템) > **User Management**(사용자 관리) > **Local Users**(로컬 사용자) 페이지에서 비밀번호를 즉시 변경하는 것이 좋습니다.

관리 IP 주소를 변경하려면 FXOS 관리 IP 주소 또는 게이트웨이 변경, 16페이지를 참조하십시오.

단계 **3** Firepower Chassis Manager에서 **Interfaces**(인터페이스) 탭을 클릭합니다.

단계 **4** 인터페이스를 활성화하거나 비활성화하려면 **Admin State**(관리 상태) 슬라이더를 클릭합니다. 체크 마크는 활성화된 것을 표시하는 반면 X는 비활성화된 것을 표시합니다.

참고 관리 1/1 인터페이스는 이 표에서 **MGMT**로 표시됩니다.

단계 **5** (선택 사항) EtherChannel을 추가합니다.

참고 EtherChannel 멤버 포트는 ASA에서 볼 수 있지만 FXOS에서만 EtherChannel 및 포트 멤버십을 구성할 수 있습니다.

a) 인터페이스 표 위에 있는 **Add Port Channel**(포트 채널 추가)을 클릭합니다.

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

c) **Enable**(활성화) 체크 박스를 선택하여 포트 채널을 활성화합니다.
Type(유형) 드롭다운 목록을 무시합니다. 유일하게 사용 가능한 유형은 **Data**(데이터)입니다.

d) **Admin Speed**(관리 속도) 드롭다운 목록에서 모든 멤버 인터페이스의 속도를 선택합니다.
속도(및 선택한 기타 설정)를 사용할 수 없는 인터페이스를 선택하는 경우 가장 빠른 가능한 속도가 자동으로 적용됩니다.

e) 모든 멤버 인터페이스에 대해 **Auto Negotiation**(자동 협상) **Yes**(예) 또는 **No**(아니요) 라디오 버튼을 클릭합니다.

f) **Admin Duplex**(관리 듀플렉스) 드롭다운 목록에서 모든 멤버 인터페이스에 대해 듀플렉스를 선택합니다.

g) **Available Interface**(사용 가능한 인터페이스) 목록에서 추가하려는 인터페이스를 선택하고 **Add Interface**(인터페이스 추가)를 클릭합니다.
동일한 유형과 속도를 가진 인터페이스는 최대 16개까지 추가할 수 있습니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다.

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

h) **OK**(확인)를 클릭합니다.

ASDM 실행 및 라이선싱 구성

ASDM을 실행하고 디바이스를 Smart Software License 서버에 등록합니다.

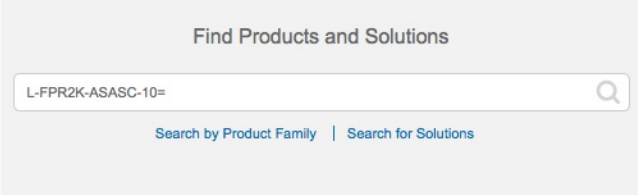
시작하기 전에

- ASDM을 실행하기 위한 요구 사항은 Cisco.com의 ASDM 릴리스 노트를 참조하십시오.

- 이 절차에서는 이더넷 1/1 외부 인터페이스를 인터넷에 연결했으며 기본 컨피그레이션을 사용 중인 것으로 가정합니다. 네트워크에 있는 Firepower 2100, 4 페이지를 참조하십시오.
- Cisco Smart Software Manager에서 마스터 계정을 만듭니다.

  아직 계정이 없는 경우 새 계정 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.
- Cisco Smart Software Licensing 계정은 일부 기능(export-compliance 플래그를 사용하여 활성화됨)을 사용하려면 강력한 암호화(3DES/AES) 라이선스 자격을 얻어야 합니다.
- 계정에 필요로 하는 사용 가능한 라이선스(최소 표준 라이선스 포함)가 포함되어 있는지 확인합니다. Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 Smart Software License 계정에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace에서 **Find Products and Solutions**(제품 및 솔루션 찾기) 검색 필드를 사용합니다. 다음 라이선스 PID를 검색합니다.

  그림 ***3:*** 라이선스 검색



  - 표준 라이선스 — L-FPR2100-ASA=. 표준 라이선스는 무료이지만 Smart Software Licensing 계정에 추가해야 합니다.
  - 5개의 상황 라이선스 — L-FPR2K-ASASC-5=. 상황 라이선스는 부가 라이선스입니다. 요구 사항에 맞게 여러 라이선스를 구매하십시오.
  - 10개의 상황 라이선스 — L-FPR2K-ASASC-10=. 상황 라이선스는 부가 라이선스입니다. 요구 사항에 맞게 여러 라이선스를 구매하십시오.
  - 강력한 암호화(3DES/AES) 라이선스 — L-FPR2K-ENC-K9=. 이 라이선스는 무료입니다. 이 라이선스는 기존의 Satellite 서버 버전(이전 2.3.0 버전)을 사용하는 ASA에만 필요하지만 추적 용도를 위해 사용자 계정에 추가해야 합니다.

참고 장애 조치 쌍의 경우 표준 라이선스를 두 장치에 모두 적용(암호화도 동일하게 적용)해야 합니다. 상황 라이선스의 경우 기본 장치에만 적용하면 됩니다.

절차

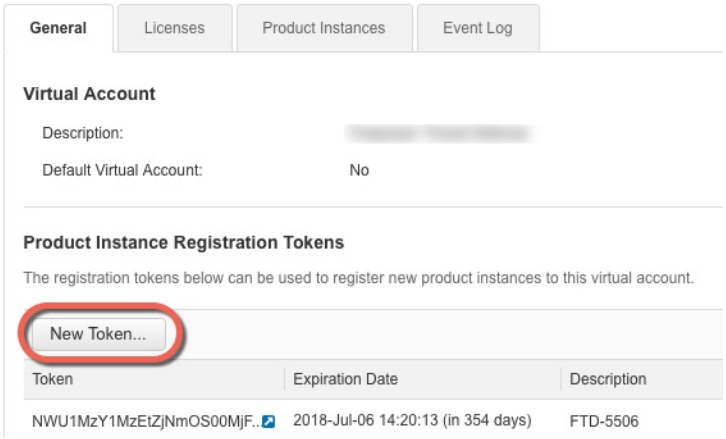
단계 **1** Smart Software Manager(Cisco Smart Software Manager)에서 이 디바이스를 추가하려는 가상 계정에 대한 등록 토큰을 요청 및 복사합니다.

a) **Inventory(**인벤토리**)**를 클릭합니다.

그림 ***4:*** 인벤토리

b) **General(**일반**)** 탭에서 **New Token(**새 토큰**)**을 클릭합니다.

그림 ***5:*** 새 토큰

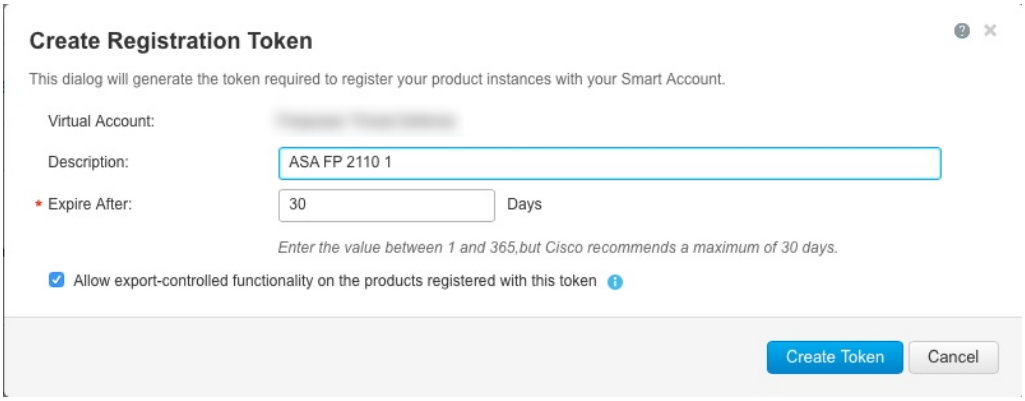


c) **Create Registration Token(**등록 토큰 생성**)** 대화 상자에서 다음 설정을 입력한 다음 **Create Token(**토큰 생성**)**을 클릭합니다.

- 설명
- **Expire After(**다음 이후에 만료**)** — 30일로 설정하는 것이 좋습니다.

- **Allow export-controlled functionality on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)** — export-compliance 플래그를 활성화합니다.

그림 ***6:*** 등록 토큰 생성



토큰이 인벤토리에 추가됩니다.

d) 토큰의 오른쪽에 있는 화살표 아이콘을 클릭하여 **Token(**토큰**)** 대화 상자를 열면 토큰 ID를 클립보드에 복사할 수 있습니다. 나중에 절차에서 ASA를 등록해야 하는 경우 사용하기 위해 이 토큰을 준비해 두십시오.

그림 ***7:*** 토큰 보기

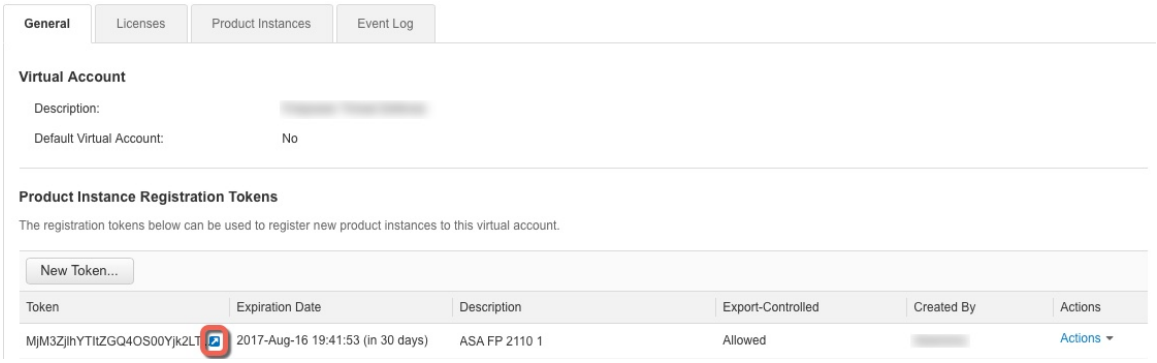
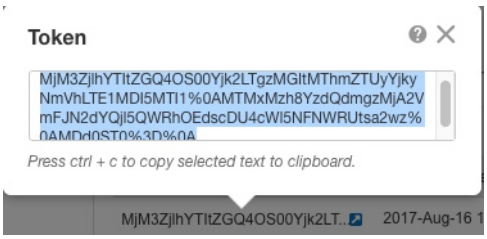


그림 ***8:*** 토큰 복사



단계 **2** 관리 1/1에 연결된 관리 컴퓨터에서 웹 브라우저를 실행하고 **https://192.168.45.1/admin** URL로 이동합니다. **Cisco ASDM** 웹 페이지가 나타납니다.

단계 **3** 사용 가능한 옵션 **Install ASDM Launcher(ASDM** 시작 관리자 설치**)** 또는 **Run ASDM(ASDM** 실행**)** 중 하나를 클릭합니다.

단계 **4** 선택한 옵션에 따라 ASDM을 구동하기 위한 화면의 지침을 수행합니다. **Cisco ASDM-IDM Launcher**가 나타납니다.

단계 **5** 사용자 이름과 비밀번호 필드를 비워두고 **OK(**확인**)**를 클릭합니다. 기본 ASDM 창이 나타납니다.

단계 **6** **Configuration(**컨피그레이션**)** > **Device Management(**디바이스 관리**)** > **Licensing(**라이선싱**)** > **Smart Licensing(**스마트 라이선싱**)**을 선택합니다.

단계 **7** **Enable Smart license configuration(**스마트 라이선스 컨피그레이션 활성화**)**을 선택합니다.

단계 **8** **Feature Tier(**기능 계층**)** 드롭다운 메뉴에서 **Standard(**표준**)**를 선택합니다.
표준 계층만 사용 가능합니다..

단계 **9** (선택 사항) 상황 라이선스의 경우 상황 수를 입력합니다.
상황의 최대 수는 모델에 따라 다릅니다. 라이선스 없이 2개의 상황을 사용할 수 있습니다.

- Firepower 2110 — 25개의 상황
- Firepower 2120 — 25개의 상황
- Firepower 2130 — 30개의 상황
- Firepower 2140 — 40개의 상황

단계 **10** **Apply(**적용**)**를 클릭합니다.

단계 **11** **Register(**등록**)**를 클릭합니다.

단계 **12** **ID Token(ID** 토큰**)** 필드에 등록 토큰을 입력합니다.

단계 **13** **Register(**등록**)**를 클릭합니다.
ASA를 사전 구성된 외부 인터페이스를 사용하는 License Authority에 등록하고 구성된 라이선스 자격에 대한 권한 부여를 요청합니다. 계정에서 허용하는 경우 License Authority는 강력한 암호화(3DES/AES) 라이선스도 적용합니다. 라이선스 상태를 확인하려면 **Monitoring(**모니터링**) > Properties(**속성**) > Smart License(**스마트 라이선스**)**를 선택합니다.

ASA 구성

ASDM을 사용하면 마법사를 통해 기본 및 고급 기능을 구성할 수 있습니다. 또한, 수동으로 마법사에 포함되지 않은 기능을 구성할 수 있습니다.

절차

단계 1 **Wizards**(마법사) > **Startup Wizard**(시작 마법사)를 클릭하고 **Modify existing configuration**(기존 컨피그레이션 수정) 라디오 버튼을 클릭합니다.

단계 2 **Startup Wizard**(시작 마법사)에서는 다음 항목을 구성하는 방법을 안내합니다.

- 활성화 비밀번호
- 인터페이스(내부 및 외부 인터페이스 IP 주소 변경 및 구성한 인터페이스 활성화 포함) (옵션) Firepower Chassis Manager에서 추가 인터페이스 활성화, 6페이지
- 정적 경로
- DHCP 서버(관리 1/1 인터페이스에 대한 DHCP 서버를 설정하지 않음)
- 기타...

단계 3 (선택 사항) **Wizards**(마법사) 메뉴에서 다른 마법사를 실행합니다.

단계 4 ASA를 계속 구성하려면 Navigating the Cisco ASA Series Documentation(Cisco ASA Series 문서 탐색)에서 사용 중인 소프트웨어 버전에 대해 사용 가능한 문서를 참조하십시오.

ASA 및 FXOS CLI 액세스

이 섹션은 FXOS 및 ASA 콘솔에 연결하는 방법, ASA 데이터 인터페이스에서 FXOS, SSH, HTTPS 및 SNMP 액세스를 구성하는 방법, SSH를 사용하여 FXOS에 연결하는 방법을 설명합니다.

ASA 또는 FXOS 콘솔에 연결

Firepower 2100 콘솔 포트는 사용자를 FXOS CLI에 연결합니다. FXOS CLI에서 ASA 콘솔에 연결한 다음 반대로 다시 연결할 수 있습니다.

시작하기 전에

한 번에 하나의 콘솔 연결만 유지할 수 있습니다. FXOS 콘솔에서 ASA 콘솔에 연결하는 경우 이 연결은 텔넷 또는 SSH 연결과 달리 영구 콘솔 연결입니다.

절차

단계 1 관리 컴퓨터를 콘솔 포트에 연결합니다. Firepower 2100은 DB-9~RJ-45 시리얼 케이블과 함께 제공되므로 연결을 설정하려면 서드파티 시리얼-USB 케이블이 필요합니다. 운영 체제에 필요한 모든 USB 시리얼 드라이버를 설치해야 합니다. 다음 시리얼 설정을 사용하십시오.

- 9600보드

- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

FXOS CLI에 연결합니다.

단계 **2** ASA에 연결합니다.
connect asa

예제:

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

단계 **3** FXOS 콘솔로 돌아가려면 **Ctrl+a**, **d**를 입력합니다.

데이터 인터페이스에서 **FXOS**에 대한 관리 액세스 구성

데이터 인터페이스의 Firepower 2100에서 FXOS를 관리하려는 경우 SSH, HTTPS 및 SNMP 액세스를 구성할 수 있습니다. 이 기능은 디바이스를 원격으로 관리하려는 경우와 격리된 네트워크에서 관리 1/1을 유지하려는 경우 유용합니다. 로컬 액세스용으로 관리 1/1을 계속해서 사용할 수 있습니다. 하나의 게이트웨이만 지정할 수 있기 때문에 ASA 데이터 인터페이스로 트래픽을 전달하는 것과 동시에 FXOS에 대한 관리 1/1에서의 원격 액세스를 허용할 수 없습니다. 기본적으로 FXOS 관리 게이트웨이는 ASA의 내부 경로입니다.

ASA는 FXOS 액세스용으로 비표준 포트를 사용합니다. 표준 포트는 동일한 인터페이스에 있는 ASA에서 사용하기 위해 예약되어 있습니다. ASA가 FXOS로 트래픽을 전달할 때 비표준 대상 포트를 각 프로토콜(FXOS에서 HTTPS 포트를 변경하지 않음)에 대한 FXOS 포트로 변환합니다. 패킷 대상 IP 주소(ASA 인터페이스 IP 주소)도 FXOS에서 사용하기 위해 내부 주소로 변환됩니다. 소스 주소는 변경되지 않습니다. 트래픽을 반환하기 위해 ASA는 데이터 라우팅 테이블을 사용하여 올바른 이그레스 인터페이스를 결정합니다. 관리 애플리케이션용 ASA 데이터 IP 주소에 액세스할 때 FXOS 사용자 이름을 사용하여 로그인해야 합니다. ASA 사용자 이름은 ASA 관리 액세스에만 적용됩니다.

또한, FXOS 관리 트래픽 시작 기능을 ASA 데이터 인터페이스에서 활성화할 수 있습니다. 이 기능은 예를 들어 SNMP 트랩 또는 NTP 및 DNS 서버 액세스에 필요합니다. 기본적으로 FXOS 관리 트래픽 시작 기능은 DNS 및 NTP 서버 통신(Smart Software Licensing 통신에 필요)을 위한 ASA 외부 인터페이스에 대해 활성화됩니다.

시작하기 전에

- 단일 상황 모드만 해당합니다.
- ASA 관리 전용 인터페이스는 제외됩니다.

- VPN 터널을 ASA 데이터 인터페이스에 사용할 수 없으며 FXOS에 직접 액세스할 수 없습니다. SSH를 위한 해결 방법으로, ASA에 VPN을 사용하고 *ASA* CLI에 액세스한 다음 **connect fxos** 명령을 사용하여 FXOS CLI에 액세스할 수 있습니다. SSH, HTTPS 및 SNMPv3는 암호화될 수 있으므로 데이터 인터페이스에 직접 연결하는 것이 안전합니다.

절차

단계 **1** ASDM에서 **Configuration(**컨피그레이션**)** > **Firewall(**방화벽**)** > **Advanced(**고급**)** > **FXOS Remote Management(FXOS** 원격 관리**)**를 선택합니다.

단계 **2** FXOS 원격 관리를 활성화합니다.

a) 탐색 창에서 **HTTPS**, **SNMP** 또는 **SSH**를 선택합니다.

b) **Add(**추가**)**를 클릭하고 관리를 허용하려는 **Interface(**인터페이스**)**를 설정하고 연결이 허용된 **IP Address(IP** 주소**)**를 설정한 다음 **OK(**확인**)**를 클릭합니다.
각 프로토콜 유형별로 여러 항목을 만들 수 있습니다. 다음 기본값을 사용하지 않으려면 **Port(**포트**)**를 설정합니다.

- HTTPS 기본 포트 — 3443
- SNMP 기본 포트 — 3061
- SSH 기본 포트 — 3022

단계 **3** FXOS가 ASA 인터페이스에서 관리 연결을 시작하도록 허용합니다.

a) 탐색 창에서 **FXOS Traffic Initiation(FXOS** 트래픽 시작**)**을 선택합니다.

b) **Add(**추가**)**를 클릭하고 FXOS 관리 트래픽을 보내야 할 ASA 인터페이스를 활성화합니다. 기본적으로 외부 인터페이스는 활성화되어 있습니다.

단계 **4** **Apply(**적용**)**를 클릭합니다.

단계 **5** Firepower Chassis Manager(기본값: https://192.168.45.45, 사용자 이름: **admin**, 비밀번호: **Admin123**)에 연결합니다.

단계 **6** **Platform Settings(**플랫폼 설정**)** 탭을 클릭하고 **SSH**, **HTTPS** 또는 **SNMP**를 활성화합니다.
SSH와 HTTPS는 기본적으로 활성화되어 있습니다.

단계 **7** **Platform Settings(**플랫폼 설정**)** 탭의 **Access List(**액세스 목록**)**를 구성하여 관리 주소를 허용합니다.
SSH와 HTTPS는 기본적으로 관리 1/1 192.168.45.0 네트워크만 허용합니다. ASA의 **FXOS Remote Management(FXOS** 원격 관리**)** 컨피그레이션에서 지정한 주소를 허용해야 합니다.

SSH를 통해 FXOS에 연결

관리 1/1에서 기본 IP 주소인 192.168.45.45를 사용하여 FXOS에 연결할 수 있습니다. 원격 관리를 구성하는 경우(데이터 인터페이스에서 FXOS에 대한 관리 액세스 구성, 13페이지) 기본적으로 3022인 비표준 포트에서 데이터 인터페이스 IP 주소에 연결할 수도 있습니다.

SSH를 사용하여 ASA에 연결하려면 먼저 ASA 일반 작업 컨피그레이션 가이드에 따라 SSH 액세스를 구성해야 합니다.

FXOS에서 ASA CLI에 연결할 수 있으며 그 반대로도 연결할 수 있습니다.

FXOS는 최대 8개의 SSH 연결을 허용합니다.

시작하기 전에

관리 IP 주소를 변경하려면 FXOS 관리 IP 주소 또는 게이트웨이 변경, 16페이지를 참조하십시오.

절차

단계 **1** 관리 1/1에 연결된 관리 컴퓨터에서 관리 IP 주소(기본값: https://192.168.45.45, 사용자 이름: **admin**, 비밀번호: **Admin123**)에 대한 SSH 연결을 수행합니다.
어떤 사용자 이름으로도 로그인할 수 있습니다(사용자 추가, 43페이지 참조). 원격 관리를 구성하는 경우 포트 3022(기본 포트)에서 ASA 데이터 인터페이스 IP 주소에 대한 SSH 연결을 수행합니다.

단계 **2** ASA CLI에 연결합니다.
connect asa

FXOS CLI로 돌아가려면 **Ctrl+a**, **d**를 입력합니다.

예제:

```
firepower-2100# connect asa
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.
ciscoasa>
```

단계 **3** ASA에서 SSH 액세스를 구성한 후 SSH를 통해 ASA에 연결하는 경우 FXOS CLI에 연결합니다.
connect fxos

FXOS에 대한 인증을 수행하라는 프롬프트가 표시됩니다. 기본 사용자 이름(**admin**)과 비밀번호(**Admin123**)를 사용합니다. ASA CLI로 돌아가려면 **exit**을 입력하거나 **Ctrl-Shift-6**, **x**를 입력합니다.

예제:

```
ciscoasa# connect fxos
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.

FXOS 2.2(2.32) kp2110

kp2110 login: admin
Password: Admin123
Last login: Sat Jan 23 16:20:16 UTC 2017 on pts/1
Successful login attempts for user 'admin' : 4
Cisco Firepower Extensible Operating System (FX-OS) Software

[…]

kp2110#
kp2110# exit
Remote card closed command session. Press any key to continue.
Connection with fxos terminated.
Type help or '?' for a list of available commands.
```

```
ciscoasa#
```

FXOS 관리 IP 주소 또는 게이트웨이 변경

FXOS CLI의 Firepower 2100 섀시에서 관리 IP 주소를 변경할 수 있습니다. 기본 주소는 192.168.45.45입니다. 기본 게이트웨이를 변경할 수도 있습니다. 기본 게이트웨이는 ASA로 트래픽을 보내는 0.0.0.0으로 설정됩니다. 대신 관리 1/1 네트워크에서 라우터를 사용하려는 경우 게이트웨이 IP 주소를 변경할 수 있습니다. 또한, 새로운 네트워크에 맞게 관리 연결에 대한 액세스 목록을 변경해야 합니다.

일반적으로 FXOS 관리 1/1 IP 주소는 ASA 관리 1/1 IP 주소와 동일한 네트워크에 있으며 ASA에서 ASA IP 주소 또한 변경해야 합니다.

시작하기 전에

- 관리 IP 주소를 변경한 후, 새 주소를 사용하여 모든 Firepower Chassis Manager와 SSH 연결을 다시 설정해야 합니다.
- DHCP 서버가 기본적으로 관리 1/1에서 활성화되어 있으므로 관리 IP 주소를 변경하기 전에 DHCP를 비활성화해야 합니다.

절차

단계 **1** 콘솔 포트에 연결합니다(ASA 및 FXOS CLI 액세스, 12페이지 참조). 연결 손실을 방지하려면 콘솔 포트에 연결하는 것이 좋습니다.

단계 **2** DHCP 서버를 비활성화합니다.
scope system

scope services

disable dhcp-server

commit-buffer

관리 IP 주소를 변경한 후 새 클라이언트 IP 주소를 사용하여 DHCP를 다시 활성화할 수 있습니다. 또한, **Platform Settings(**플랫폼 설정**)** > **DHCP**에서 Firepower Chassis Manager의 DHCP 서버를 활성화 및 비활성화할 수 있습니다.

예제:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # disable dhcp-server
firepower-2110 /system/services* # commit-buffer
```

단계 **3** IPv4 관리 IP 주소 및 게이트웨이(옵션)를 구성합니다.

a) fabric-interconnect a의 범위를 설정합니다.
scopefabric-interconnecta

예제:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect #
```

b) 현재 관리 IP 주소를 확인합니다.
show

예제:

```
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.45.45    0.0.0.0         0.0.0.0          ::               ::
     64     Operable
```

c) 새로운 관리 IP 주소 및 새로운 기본 게이트웨이(옵션)를 구성합니다.
setout-of-band staticip *ip_address***netmask** *network_mask***gw** *gateway_ip_address*
현재 설정된 게이트웨이를 유지하려면 **gw** 키워드를 생략합니다. 마찬가지로 게이트웨이를 변경하는 동안 기존의 관리 IP 주소를 유지하려면 **ip** 및 **netmask** 키워드를 생략합니다.

예제:

```
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.4.1 netmask
255.255.255.0
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* #
```

단계 **4** IPv6 관리 IP 주소 및 게이트웨이를 구성합니다.

a) fabric-interconnect a의 범위를 설정한 다음 IPv6 컨피그레이션을 설정합니다.
scopefabric-interconnecta

scopeipv6-config

예제:

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config #
```

b) 현재 관리 IPv6 주소를 확인합니다.
show ipv6-if

예제:

```
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                            Prefix     IPv6 Gateway
    ------------------------------------ ---------- ------------
```

```
    ::                                      ::          ::
```

c) 새로운 관리 IPv6 주소 및 게이트웨이를 구성합니다.
Firepower-chassis /fabric-interconnect/ipv6-config # **setout-of-band staticipv6** *ipv6_address***ipv6-prefix** *prefix_length***ipv6-gw** *gateway_address*

현재 설정된 게이트웨이를 유지하려면 **ipv6-gw** 키워드를 생략합니다. 마찬가지로 게이트웨이를 변경하는 동안 기존의 관리 IP 주소를 유지하려면 **ipv6** 및 **ipv6-prefix** 키워드를 생략합니다.

예제:

```
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::34
 ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* #
```

단계 **5** 새로운 네트워크에서 관리 연결을 허용하도록 HTTPS, SSH 및 SNMP용 액세스 목록을 삭제한 후에 새로 추가합니다.

a) 시스템/서비스의 범위를 설정합니다.
scope system

scope services

예제:

```
firepower-2110# scope system
firepower-2110 /system # scope services
```

b) 현재 액세스 목록을 확인합니다.
show ip-block

예제:

```
firepower-2110 /system/services # show ip-block

Permitted IP Block:
    IP Address      Prefix Length Protocol
    --------------- ------------- --------
    192.168.45.0               24 https
    192.168.45.0               24 ssh
firepower-2140 /system/services #
```

c) 새 액세스 목록을 추가 합니다.
IPv4의 경우:

enterip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

IPv6의 경우:

enteripv6-block *ipv6_address prefix* [**https** | **snmp** | **ssh**]

IPv4의 경우 모든 네트워크를 허용하려면 **0.0.0.0** 및 접두사 **0**을 입력합니다. IPv6의 경우 모든 네트워크를 허용하려면 **::** 및 접두사 **0**을 입력합니다. Firepower Chassis Manager의 **Platform Settings(**플랫폼 설정**)** > **Access List(**액세스 목록**)**에서 액세스 목록을 추가할 수도 있습니다.

예제:

```
firepower-2110 /system/services # enter ip-block 192.168.4.0 24 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ip-block 192.168.4.0 24 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 https
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 ssh
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* # enter ipv6-block 2001:DB8:: 64 snmp
firepower-2110 /system/services/ip-block* # exit
firepower-2110 /system/services* #
```

a) 이전 액세스 목록을 삭제합니다.
IPv4의 경우:

delete ip-block *ip_address prefix* [**http** | **snmp** | **ssh**]

IPv6의 경우:

delete ipv6-block *ipv6_address prefix* [**https** | **snmp** |

ssh]

```
firepower-2110 /system/services # delete ip-block 192.168.45.0 24 https
firepower-2110 /system/services* # delete ip-block 192.168.45.0 24 ssh
firepower-2110 /system/services* #
```

단계 **6** (선택 사항) IPv4 DHCP 서버를 다시 활성화합니다.
scope system

scope services

enable dhcp-server *start_ip_address end_ip_address*

또한, **Platform Settings(**플랫폼 설정**)** > **DHCP**에서 Firepower Chassis Manager의 DHCP 서버를 활성화 및 비활성화할 수 있습니다.

예제:

```
firepower-2110# scope system
firepower-2110 /system # scope services
firepower-2110 /system/services # enable dhcp-server 192.168.4.10 192.168.4.20
```

단계 **7** 컨피그레이션을 저장합니다.
commit-buffer

예제:

```
firepower-2110 /system/services* # commit-buffer
```

다음 예에서는 IPv4 관리 인터페이스 및 게이트웨이를 구성합니다.

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # show

Fabric Interconnect:
    ID   OOB IP Addr     OOB Gateway     OOB Netmask     OOB IPv6 Address OOB IPv6 Gateway
 Prefix Operability
    ---- --------------- --------------- --------------- ---------------- ----------------
 ------ -----------
    A    192.168.2.112    192.168.2.1     255.255.255.0   2001:DB8::2     2001:DB8::1
  64     Operable
firepower-2110 /fabric-interconnect # set out-of-band static ip 192.168.2.111 netmask
255.255.255.0 gw 192.168.2.1
Warning: When committed, this change may disconnect the current CLI session
firepower-2110 /fabric-interconnect* # commit-buffer
firepower-2110 /fabric-interconnect #
```

다음 예에서는 IPv6 관리 인터페이스 및 게이트웨이를 구성합니다.

```
firepower-2110# scope fabric-interconnect a
firepower-2110 /fabric-interconnect # scope ipv6-config
firepower-2110 /fabric-interconnect/ipv6-config # show ipv6-if

Management IPv6 Interface:
    IPv6 Address                          Prefix     IPv6 Gateway
    ------------------------------------ ---------- ------------
    2001:DB8::2                           64         2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config # set out-of-band static ipv6 2001:DB8::2
ipv6-prefix 64 ipv6-gw 2001:DB8::1
firepower-2110 /fabric-interconnect/ipv6-config* # commit-buffer
firepower-2110 /fabric-interconnect/ipv6-config #
```

다음 단계

- ASA를 계속 구성하려면 Navigating the Cisco ASA Series Documentation(Cisco ASA Series 문서 탐색)에서 사용 중인 소프트웨어 버전에 대해 사용 가능한 문서를 참조하십시오.
- 새시 설정을 구성하려면 Firepower Chassis Manager 설정, 21 페이지의 내용을 참조하십시오.

2 장

Firepower Chassis Manager 설정

Firepower 2100은 디바이스의 기본 작업을 제어하기 위해 FXOS를 실행합니다. GUI Firepower Chassis Manager 또는 FXOS CLI를 사용하여 이러한 기능을 구성할 수 있습니다. 이 문서에서는 Firepower Chassis Manager에 대해 다루고 있습니다. 모든 보안 정책 및 기타 작업은 CLI 또는 ASDM을 사용하여 ASA OS에서 구성됩니다.

- 개요, 21 페이지
- 인터페이스, 22 페이지
- 논리적 디바이스, 25 페이지
- 플랫폼 설정, 25 페이지
- 시스템 업데이트, 40 페이지
- 사용자 관리, 41 페이지

개요

Overview(개요**)** 탭에서 Firepower 2100의 상태를 쉽게 모니터링할 수 있습니다. **Overview(**개요**)** 탭에는 다음과 같은 요소가 있습니다.

- 디바이스 정보 - **Overview(**개요**)** 탭 상단에는 Firepower 2100에 대한 다음 정보가 포함되어 있습니다.
  - 섀시 이름 — 섀시에 할당된 이름이 표시됩니다. 기본적으로 이름은 **firepower-**모델(예: firepower-2140)입니다. 이 이름은 CLI 프롬프트에 나타납니다. 섀시 이름을 변경하려면 FXOS CLI **scope system / set name** 명령을 사용합니다.
  - IP 주소 — 섀시에 할당된 관리 IP 주소가 표시됩니다.
  - 모델 — Firepower 2100 모델이 표시됩니다.
  - 버전 — 섀시에서 실행 중인 ASA 버전 번호가 표시됩니다.
  - 작동 상태 — 섀시의 작동 가능 상태가 표시됩니다.

- 섀시 업타임 — 시스템이 마지막으로 재시작된 이후 경과한 시간이 표시됩니다.
- 업타임 정보 아이콘 — 아이콘 위에 마우스를 올려놓으면 섀시 및 ASA 보안 엔진의 업타임을 볼 수 있습니다.

- 시각적 상태 표시 — 디바이스 정보 섹션에서는 섀시를 시각적으로 표현하여 섀시에 설치된 구성 요소를 보여주고 해당 구성 요소에 대한 일반적인 상태 정보를 제공합니다. 시각적 상태 표시에 나타난 포트에 마우스 커서를 대면 인터페이스 이름, 속도, 유형, 관리자 상태 및 작동 상태와 같은 추가 정보를 얻을 수 있습니다.
- 상세한 상태 정보 — 시각적 상태 표시에서는 섀시의 상세한 상태 정보가 포함된 표를 제공합니다. 상태 정보는 결함, 인터페이스, 디바이스, 인벤토리 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 섀시에 대해 다음의 상세한 상태 정보를 제공합니다.

  - **Faults(**결함**)** — 시스템에서 생성된 결함이 나열됩니다. 결함은 중대, 주요, 사소, 경고 및 정보의 심각도별로 정렬됩니다. 나열된 각 결함에 대해 심각도, 결함 설명, 원인, 발생 횟수 및 최근 발생 시간을 확인할 수 있습니다. 또한 결함 승인 여부를 확인할 수 있습니다.

    결함 중 하나를 클릭하여 해당 결함에 대한 추가적인 세부사항을 확인하거나 결함을 승인할 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 승인하여 해당 결함이 현재 해결 중이라는 사실을 다른 사용자에게 알릴 수 있습니다.

  - **Interfaces(**인터페이스**)** — 시스템에 설치된 인터페이스가 나열되고 인터페이스 이름, 작동상태, 관리 상태, 수신된 바이트 수, 전송된 바이트 수가 표시됩니다.
    인터페이스 중 하나를 클릭하여 마지막 15분 동안 해당 인터페이스에서 이루어진 입력 및 출력 바이트 수를 그래픽으로 확인할 수 있습니다.
  - **Devices(**디바이스**)** — ASA가 표시되고 세부 사항(예: 디바이스 이름, 디바이스 상태, 애플리케이션, 작동 상태, 관리 상태, 이미지 버전 및 관리 IP 주소)이 제공됩니다.
  - **Inventory(**인벤토리**)** — 섀시에 설치된 구성 요소가 나열되고 해당 구성 요소와 관련된 세부사항(예: **구성 요소** 이름, 코어 수, 설치 위치, 작동 상태, 작동 가능성, 용량, 전원, 열, 시리얼 번호, 모델 번호, 부품 번호 및 벤더)이 제공됩니다.

인터페이스

FXOS에서는 물리적 인터페이스를 관리할 수 있습니다. 인터페이스를 사용하려면 FXOS에서 인터페이스를 물리적으로 활성화하고 ASA에서 논리적으로 활성화해야 합니다.

Firepower 2100은 기본적으로 활성화되어 있는 점보 프레임을 지원합니다. 최대 MTU는 9184입니다.관리 인터페이스에 대한 자세한 내용은 ASA 및 FXOS 관리, 2페이지를 참조하십시오.

인터페이스 구성

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

절차

단계 **1** 인터페이스 탭을 클릭합니다.

단계 **2** 인터페이스를 활성화하거나 비활성화하려면 **Admin State(**관리 상태**)** 슬라이더를 클릭합니다. 체크 마크는 활성화된 것을 표시하는 반면 X는 비활성화된 것을 표시합니다.

참고 관리 1/1 인터페이스는 이 표에서 **MGMT**로 표시됩니다.

단계 **3** 속도 또는 듀플렉스를 편집하려는 인터페이스의 **Edit(**편집**)**(연필 아이콘)을 클릭합니다.

참고 관리 1/1 인터페이스는 활성화 또는 비활성화만 가능하며 해당 속성을 편집할 수는 없습니다.

단계 **4** 인터페이스를 활성화하려면 **Enable(**활성화**)** 체크 박스를 선택합니다.

단계 **5** **Admin Speed(**관리 속도**)** 드롭다운 목록에서 인터페이스의 속도를 선택합니다.

단계 **6** **Auto Negotiation(**자동 협상**) Yes(**예**)** 또는 **No(**아니요**)** 라디오 버튼을 클릭합니다.

단계 **7** **Admin Duplex(**관리 듀플렉스**)** 드롭다운 목록에서 인터페이스의 듀플렉스를 선택합니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

EtherChannel 추가

EtherChannel(포트 채널이라고도 함)은 동일한 유형 및 속도의 멤버 인터페이스를 최대 16개 포함할 수 있습니다.

참고 EtherChannel 멤버 포트는 ASA에서 볼 수 있지만 FXOS에서만 EtherChannel 및 포트 멤버십을 구성할 수 있습니다.

시작하기 전에

Firepower 2100은 LACP(Link Aggregation Control Protocol)가 Active(활성) 또는 On(켜짐) 모드일 때 EtherChannel을 지원합니다. 기본적으로 LACP 모드는 Active(활성)로 설정되어 있으며 CLI에서 이 모드를 On(켜짐)으로 변경할 수 있습니다. 최고의 호환성을 위해 연결 스위치 포트를 Active(활성) 모드로 설정하는 것이 좋습니다.

절차

단계 **1** **인터페이스** 탭을 클릭합니다.

단계 **2** 인터페이스 표 위에 있는 **Add Port Channel(**포트 채널 추가**)**을 클릭합니다.

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

단계 **4** **Enable(**활성화**)** 체크 박스를 선택하여 포트 채널을 활성화합니다.
Type(유형**)** 드롭다운 목록을 무시합니다. 유일하게 사용 가능한 유형은 **Data(**데이터**)**입니다.

단계 **5** **Admin Speed(**관리 속도**)** 드롭다운 목록에서 모든 멤버 인터페이스의 속도를 선택합니다.
속도(및 선택한 기타 설정)를 사용할 수 없는 인터페이스를 선택하는 경우 가장 빠른 가능한 속도가 자동으로 적용됩니다.

단계 **6** 모든 멤버 인터페이스에 대해 **Auto Negotiation(**자동 협상**) Yes(**예**)** 또는 **No(**아니요**)** 라디오 버튼을 클릭합니다.

단계 **7** **Admin Duplex(**관리 듀플렉스**)** 드롭다운 목록에서 모든 멤버 인터페이스에 대해 듀플렉스를 선택합니다.

단계 **8** **Available Interface(**사용 가능한 인터페이스**)** 목록에서 추가하려는 인터페이스를 선택하고 **Add Interface(**인터페이스 추가**)**를 클릭합니다.
동일한 유형과 속도를 가진 인터페이스는 최대 16개까지 추가할 수 있습니다. 채널 그룹에 추가된 첫 번째 인터페이스에서는 올바른 유형과 속도를 결정합니다.

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

단계 **9** **OK(**확인**)**를 클릭합니다.

모니터링 인터페이스

Interfaces(인터페이스**)** 탭에서 섀시에 설치된 인터페이스의 상태를 볼 수 있습니다. 하위 섹션에는 Firepower 섀시에 설치된 인터페이스 테이블이 있습니다. 상위 섹션에서는 Firepower 섀시에 설치된 인터페이스를 시각적으로 표시합니다. 상위 섹션에 있는 인터페이스 중 하나에 마우스를 올려놓으면 해당 인터페이스에 대한 자세한 정보를 얻을 수 있습니다.

인터페이스에는 현재 상태를 표시하는 다음과 같은 색상 코드가 지정됩니다.

- 녹색 — 작동 상태가 가동 중입니다.
- 어두운 회색 — 관리 상태가 비활성화 상태입니다.
- 빨간색 — 작동 상태가 중단 상태입니다.
- 밝은 회색 — SFP가 설치되지 않았습니다.

논리적 디바이스

Logical Devices(논리적 디바이스**)** 페이지에는 ASA에 대한 정보 및 상태가 표시됩니다. 슬라이더를 사용하여 트러블슈팅 목적으로 ASA를 비활성화하거나 다시 활성화할 수도 있습니다(체크 마크는 활성화된 것을 표시하는 반면 X는 비활성화된 것을 표시함).

ASA의 헤더에서는 다음과 같은 **Status(**상태**)**가 제공됩니다.

- **ok(**확인**)** — 논리적 디바이스 컨피그레이션이 완료되었습니다.
- **incomplete-configuration(**불완전한 컨피그레이션**)** — 논리적 디바이스 컨피그레이션이 완료되지 않았습니다.

논리적 디바이스 영역에서는 ASA에 대한 자세한 **Status(**상태**)**도 제공됩니다.

- **Online(**온라인**)** — ASA가 실행 및 작동되고 있습니다.
- **Offline(**오프라인**)** — ASA가 중지되었으며 작동 불가능합니다.
- **Installing(**설치 중**)** — ASA 설치가 진행 중입니다.
- **Not Installed(**설치되지 않음**)** — ASA가 설치되지 않았습니다.
- **Install Failed(**설치 실패**)** — ASA 설치에 실패했습니다.
- **Starting(**시작 중**)** — ASA가 시작되고 있습니다.
- **Start Failed(**시작 실패**)** — ASA 시작에 실패했습니다.
- **Started(**시작됨**)** — ASA가 시작되었으며 앱 에이전트 하트비트를 대기 중입니다.
- **Stopping(**중지 중**)** — ASA가 중지되고 있습니다.
- **Stop Failed(**중지 실패**)** — ASA를 오프라인으로 설정할 수 없습니다.
- **Not Responding(**응답하지 않음**)** — ASA가 응답하지 않습니다.
- **Updating(**업데이트 중**)** — ASA 소프트웨어 업그레이드가 진행 중입니다.
- **Update Failed(**업데이트 실패**)** — ASA 소프트웨어 업그레이드에 실패했습니다.
- **Update Succeeded(**업데이트 성공**)** — ASA 소프트웨어 업그레이드에 성공했습니다.

플랫폼 설정

Platform Settings(플랫폼 설정**)** 탭을 사용하면 시간과 관리 액세스를 포함하여 기본 FXOS 작업을 설정할 수 있습니다.

NTP: 시간 설정

클럭을 수동으로 설정하거나 NTP 서버(권장)를 사용할 수 있습니다. 최대 4개까지 NTP 서버를 구성할 수 있습니다.

시작하기 전에

- NTP는 기본적으로 Cisco NTP 서버인 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org로 구성됩니다.
- NTP 서버의 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다. DNS: DNS 서버 구성, 38페이지를 참조하십시오.

절차

단계 **1** **Platform Settings(**플랫폼 설정**)** 탭을 클릭하고 왼쪽 탐색 창에서 **NTP**를 클릭합니다. **Time Synchronization(**시간 동기화**)** 탭이 기본적으로 선택되어 있습니다.

단계 **2** NTP 서버를 사용하려면 다음 작업을 수행합니다.

a) **Use NTP Server(NTP** 서버 사용**)** 라디오 버튼을 클릭합니다.

b) IP 주소 또는 호스트 이름별로 최대 4개의 NTP 서버를 식별하려면 **Add(**추가**)**를 클릭합니다. NTP 서버의 호스트 이름을 사용하는 경우 이 절차의 뒷부분에서 DNS 서버를 구성합니다.

단계 **3** 수동으로 시간을 설정하려면 다음 작업을 수행합니다.

a) **Set Time Manually(**수동으로 시간 설정**)** 라디오 버튼을 클릭합니다.

b) **Date(**날짜**)** 드롭다운 목록을 클릭하여 달력을 표시한 다음 달력에서 사용 가능한 컨트롤을 사용하여 날짜를 설정합니다.

c) 해당하는 드롭다운 목록을 사용하여 시간을 시, 분 및 **AM/PM(**오전/오후**)**으로 지정합니다.

단계 **4** **Current Time(**현재 시간**)** 탭을 클릭하고 **Time Zone(**표준 시간대**)** 드롭다운 목록에서 섀시에 해당하는 표준 시간대를 선택합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

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

SSH: SSH 구성

다음 절차에서는 Firepower 섀시에 대한 SSH 액세스를 활성화하거나 비활성화하는 방법과 SSH 클라이언트로 섀시를 활성화하는 방법을 설명합니다. SSH 서버와 클라이언트는 기본적으로 활성화되어 있습니다.

시작하기 전에

절차

단계 **1** **Platform Settings(**플랫폼 설정**)** > **SSH** > **SSH Server(SSH** 서버**)**를 선택합니다.

단계 **2** Firepower 섀시에 대한 SSH 액세스를 제공하기 위해 SSH 서버를 활성화하려면 **Enable SSH(SSH** 활성화**)** 체크 박스를 선택합니다.

단계 **3** 서버의 **Encryption Algorithm(**암호화 알고리즘**)**에 대해 허용되는 각 암호화 알고리즘의 체크 박스를 선택합니다.

단계 **4** 서버의 **Key Exchange Algorithm(**키 교환 알고리즘**)**에 대해 허용되는 각 DH(Diffie-Hellman) 키 교환의 체크 박스를 선택합니다.
DH 키 교환에서는 어느 한쪽에서 단독으로 확인할 수 없는 공유 암호를 제공합니다. 이 키 교환은 서명 및 호스트 키와 연계하여 호스트 인증을 수행합니다. 이 키 교환 방식은 명시적 서버 인증을 수행합니다. DH 키 교환 방법 사용에 대한 자세한 내용은 RFC 4253을 참조하십시오.

단계 **5** 서버의 **Mac Algorithm(Mac** 알고리즘**)**에 대해 허용되는 각 무결성 알고리즘의 체크 박스를 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 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 유휴 상태가 될 수 있는 시간(분 단위)을 설정합니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

단계 **10** FXOS 섀시 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 호스트를 수동으로 추가해야 합니다.
- **prompt(**프롬프트**)** — 호스트 키가 섀시에 저장되어 있지 않은 경우 호스트 키를 수락하거나 거부하라는 프롬프트가 표시됩니다.
- **disable(**비활성화**)** — (기본값) 이전에 저장한 호스트 키가 없는 경우 섀시가 호스트 키를 자동으로 수락합니다.

단계 **12** 클라이언트의 **Encryption Algorithm(**암호화 알고리즘**)**에 대해 허용되는 각 암호화 알고리즘의 체크 박스를 선택합니다.

단계 **13** 클라이언트의 **Key Exchange Algorithm(**키 교환 알고리즘**)**에 대해 허용되는 각 DH(Diffie-Hellman) 키 교환의 체크 박스를 선택합니다.

DH 키 교환에서는 어느 한쪽에서 단독으로 확인할 수 없는 공유 암호를 제공합니다. 이 키 교환은 서명 및 호스트 키와 연계하여 호스트 인증을 수행합니다. 이 키 교환 방식은 명시적 서버 인증을 수행합니다. DH 키 교환 방법 사용에 대한 자세한 내용은 RFC 4253을 참조하십시오.

단계 **14** 클라이언트의 **Mac Algorithm(Mac** 알고리즘**)**에 대해 허용되는 각 무결성 알고리즘의 체크 박스를 선택합니다.

단계 **15** 클라이언트의 **Volume Rekey Limit(**볼륨 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 유휴 상태가 될 수 있는 시간(분 단위)을 설정합니다.

단계 **17** **Save(**저장**)**를 클릭합니다.

SNMP

SNMP 페이지를 사용하여 Firepower 섀시에서 SNMP(Simple Network Management Protocol)를 구성합니다.

SNMP 정보

SNMP는 SNMP 관리자 및 에이전트 간 통신에 메시지 형식을 제공하는 애플리케이션 레이어 프로토콜입니다. 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 쓰이는 시스템.
- SNMP 에이전트 — Firepower 섀시 데이터를 유지 관리하고 필요 시 데이터를 SNMP 관리자에 보고하는 Firepower 섀시에 포함된 소프트웨어 구성 요소입니다. Firepower 섀시는 MIB 컬렉션 및 에이전트를 포함합니다.
- MIB(managed information base) — SNMP 에이전트에 있는 관리되는 개체의 모음.

Firepower 섀시는 SNMPv1, SNMPv2c 및 SNMPv3를 지원합니다. SNMPv1 및 SNMPv2c 둘 다 커뮤니티 기반 보안 유형을 사용합니다.

SNMP 알림

SNMP의 핵심 기능 중 하나는 SNMP 에이전트가 보내는 알림을 생성하는 것입니다. 이러한 알림은 SNMP 관리자가 요청을 보낼 필요 없습니다. 알림은 잘못된 사용자 인증, 재시작, 연결 종료, 네이버 라우터와의 연결 끊김, 기타 중대한 이벤트를 나타낼 수 있습니다.

Firepower 섀시는 트랩 또는 알림 중 하나로 SNMP 알림을 생성합니다. 트랩은 SNMP 관리자가 트랩을 수신할 때 승인을 전송하지 않기 때문에 알림보다 신뢰성이 떨어지며 Firepower 섀시는 트랩 수신

여부를 확인할 수 없습니다. inform 요청을 수신한 SNMP 관리자는 SNMP 응답 PDU(protocol data unit)로 메시지를 승인합니다. Firepower 섀시가 PDU를 수신하지 못하는 경우 알림 요청을 다시 전송할 수 있습니다.

SNMP 보안 레벨 및 권한

SNMPv1, SNMPv2c, SNMPv3 각각은 서로 다른 보안 모델을 나타냅니다. 보안 모델 및 선택된 보안 레벨의 조합을 통해 SNMP 메시지 처리 시 적용할 보안 메커니즘을 결정합니다.

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 중 하나 이상의 권한 이상을 지원합니다.

- noAuthNoPriv — 인증 또는 암호화 없음
- authNoPriv — 인증은 있지만 암호화 없음
- authPriv — 인증 및 암호화

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

지원되는 SNMP 보안 모델/레벨의 조합

다음 표에서는 보안 모델 및 레벨의 조합에 대해 설명합니다.

표 *1: SNMP* 보안 모델 및 레벨

모델	레벨	인증	암호화	결과
v1	noAuthNoPriv	커뮤니티 문자열	없음	인증에 커뮤니티 문자열 매치를 사용합니다.
v2c	noAuthNoPriv	커뮤니티 문자열	없음	인증에 커뮤니티 문자열 매치를 사용합니다.
v3	noAuthNoPriv	Username	없음	인증에 사용자 이름 매치를 사용합니다.
v3	authNoPriv	HMAC-SHA	No(아니요)	HMAC SHA(Secure Hash Algorithm) 기반 인증을 제공합니다.

모델	레벨	인증	암호화	결과
v3	authPriv	HMAC-SHA	DES	HMAC-SHA 알고리즘 기반 인증을 제공합니다. CBC(Cipher Block Chaining) DES(DES-56) 표준 기반의 인증과 함께 DES(Data Encryption Standard) 56비트 암호화도 제공합니다.

SNMPv3 보안 기능

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

- 메시지 통합 — 메시지가 무단으로 변경 또는 손상되지 않았는지, 그리고 데이터 시퀀스가 비악의적인 방식으로 발생할 수 있는 것보다 더 많이 변경되지 않았는지 확인합니다.
- 메시지 출처 인증 — 수신 데이터를 만든 사용자의 클레임된 ID가 확인되도록 보장합니다.
- 메시지 기밀성 및 암호화 — 권한이 없는 개인, 엔티티 또는 프로세스에 정보가 노출 또는 사용되지 않도록 합니다.

SNMP 지원

Firepower 섀시는 SNMP에 다음을 지원합니다.

MIB 지원

Firepower 섀시는 MIB에 대해 읽기 전용 액세스를 지원합니다.

SNMPv3 사용자의 인증 프로토콜

Firepower 섀시는 SNMPv3 사용자에 대해 HMAC-SHA-96(SHA) 인증 프로토콜을 지원합니다.

SNMPv3 사용자를 위한 **AES** 프라이버시 프로토콜

SHA 기반 인증 외에 Firepower 섀시는 AES 128비트 AES(Advanced Encryption Standard)를 사용하여 프라이버시도 제공합니다. Firepower 섀시는 해당 프라이버시 비밀번호를 사용하여 128비트 AES 키를 생성합니다. AES 프라이버시 비밀번호는 8자 이상입니다. 암호가 일반 텍스트로 지정된 경우, 최대 80자를 지정할 수 있습니다.

SNMP 구성

SNMP를 활성화하고 트랩 및 SNMPv3 사용자를 추가합니다.

절차

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

단계 **2** **SNMP** 영역에서 다음 필드를 완성합니다.

이름	설명
Admin State(관리 상태**)** 체크 박스	SNMP 활성화 또는 비활성화 여부. 시스템에 SNMP 서버와의 통합이 포함된 경우에만 이 서비스를 활성화합니다.
Port(포트**)** 필드	Firepower 섀시가 SNMP 호스트와 통신할 때 사용하는 포트입니다. 기본 포트를 변경할 수 없습니다.
Community/Username(커뮤니티/사용자 이름**)** 필드	Firepower 섀시가 SNMP 호스트에 전송하는 모든 트랩 메시지에 포함되는 기본 SNMP v1 또는 v2 커뮤니티 이름 또는 SNMP v3 사용자 이름입니다. 1자 ~ 32자의 영숫자 문자열을 입력합니다. @(앳 기호), \(백슬래시), "(큰따옴표), ?(물음표), 또는 공백은 사용하지 마십시오. 기본값은 public입니다. **Community/Username(**커뮤니티/사용자 이름**)** 필드가 이미 설정된 경우 빈 필드 오른쪽의 텍스트에 **Set: Yes(**설정**:** 예**)**가 표시됩니다. **Community/Username** 필드에 아직 값이 채워지지 않은 경우 빈 필드 오른쪽의 텍스트에 **Set: No(**설정**:** 아니요**)**가 표시됩니다.
System Administrator Name(시스템 관리자 이름**)** 필드	SNMP 구현을 책임지는 담당자입니다. 이메일 주소, 이름, 전화 번호 등 최대 255자의 문자열로 입력합니다.
Location(위치**)** 필드	SNMP 에이전트(서버가) 실행되는 호스트의 위치. 최대 510자의 영숫자 문자열을 입력합니다.

단계 **3** **SNMP Traps(SNMP** 트랩**)** 영역에서 **Add(**추가**)**를 클릭합니다.

단계 **4** **Add SNMP Trap(SNMP** 트랩 추가**)** 대화 상자에서 다음 필드를 작성합니다.

이름	설명
호스트 이름 필드	Firepower 섀시가 트랩을 전송해야 하는 SNMP 호스트의 호스트 이름 또는 IP 주소입니다.

이름	설명
Community/Username(커뮤니티/사용자 이름**)** 필드	Firepower 섀시가 SNMP 호스트에 트랩을 전송할 때 포함하는 SNMP v1 또는 v2 커뮤니티 이름 또는 SNMP v3 사용자 이름입니다. SNMP 서비스에 대해 구성된 커뮤니티 또는 사용자 이름과 같아야 합니다. 1자 ~ 32자의 영숫자 문자열을 입력합니다. @(앳 기호), \(백슬래시), "(큰따옴표), ?(물음표), 또는 공백은 사용하지 마십시오.
Port(포트**)** 필드	Firepower 섀시가 트랩을 위해 SNMP 호스트와 통신하는 포트입니다. 1 ~ 65535 범위의 정수를 입력합니다.
Version(버전**)** 필드	트랩에 사용할 SNMP 버전 및 모델. 다음 중 하나일 수 있습니다. • **V1** • **V2** • **V3**
Type(유형**)** 필드	버전을 **V2** 또는 **V3**로 선택한 경우 트랩 유형이 전송됩니다. 다음 중 하나일 수 있습니다. • **Traps** • **Informs**
v3 Privilege(v3 권한**)** 필드	버전으로 **V3**를 선택할 경우, 트랩과 관련된 권한. 다음 중 하나일 수 있습니다. • **Auth**—인증은 있지만 암호화 없음 • **Noauth**—인증도 암호화도 없음 • **Priv**—인증 및 암호화

단계 **5** **OK(**확인**)**를 클릭하여 **Add SNMP Trap(SNMP** 트랩 추가**)** 대화 상자를 닫습니다.

단계 **6** **SNMP Users(SNMP** 사용자**)** 영역에서 **Add(**추가**)**를 클릭합니다.

단계 **7** **Add SNMP User(SNMP** 사용자 추가**)** 대화 상자에서 다음 필드를 작성합니다.

이름	설명
Name(이름**)** 필드	SNMP 사용자에 지정된 사용자 이름. 최대 32자의 영숫자를 입력합니다. 이름은 문자로 시작해야 하며 _(밑줄), .(마침표). @(앳 기호), -(하이픈)으로 지정할 수도 있습니다.
Auth Type(인증 유형**)** 필드	권한 부여 유형: **SHA**.
Use AES-128(AES-128 사용**)** 체크 박스	선택하면 이 사용자는 AES-128 암호화를 사용합니다.
Password(비밀번호**)** 필드	이 사용자의 비밀번호
Confirm Password(비밀번호 확인**)** 필드	확인을 위해 다시 입력하는 비밀번호
Privacy Password(프라이버시 비밀번호**)** 필드	이 사용자의 프라이버시 비밀번호
Confirm Privacy Password(프라이버시 비밀번호 확인**)** 필드	확인을 위해 다시 입력하는 프라이버시 비밀번호

단계 **8** **OK(**확인**)**를 클릭하여 **Add SNMP User(SNMP** 사용자 추가**)** 대화 상자를 닫습니다.

단계 **9** **Save(**저장**)**를 클릭합니다.

HTTPS: 포트 변경

HTTPS 서비스는 기본적으로 포트 443에서 활성화되어 있습니다. HTTPS를 비활성화할 수는 없지만, HTTPS 연결에 사용할 포트를 변경할 수 있습니다.

시작하기 전에

443에서 HTTPS 포트를 변경하지 마십시오. ASA 데이터 인터페이스에서 HTTPS 액세스를 활성화하는 경우 기본 포트만 지원됩니다.

절차

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

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

단계 3 **Save(**저장**)**를 클릭합니다.
Firepower 섀시는 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 섀시의 IP 주소 또는 호스트 이름이며 <*chassis_mgmt_port*>는 방금 구성한 HTTPS 포트입니다.

DHCP: 관리 클라이언트에 대한 DHCP 서버 구성

관리 1/1 인터페이스에 연결된 클라이언트에 대해 DHCP 서버를 활성화할 수 있습니다. 기본적으로 서버는 192.168.45.10~192.168.45.12의 주소 범위로 활성화됩니다. 관리 IP 주소를 변경하려는 경우 DHCP를 비활성화해야 합니다(FXOS 관리 IP 주소 또는 게이트웨이 변경, 16페이지 참조). 그러면 새로운 네트워크에 대해 DHCP를 다시 활성화할 수 있습니다.

절차

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

단계 2 **Enable DHCP service(DHCP** 서비스 활성화**)** 체크 박스를 선택합니다.

단계 3 **Start IP(**시작 **IP)** 및 **End IP(**종료 **IP)** 주소를 입력합니다.

단계 4 **Save(**저장**)**를 클릭합니다.

Syslog: Syslog 메시징 구성

시스템 로깅은 디바이스의 메시지를 syslog 데몬을 실행 중인 서버로 수집하는 방식입니다. 중앙 syslog 서버에 로깅하면 로그와 경고를 종합하는 데 도움이 됩니다. 로그는 일상적인 트러블슈팅과 사고 처리에 모두 유용합니다.

이러한 syslog 메시지는 FXOS 섀시에만 적용됩니다. ASA syslog 메시지의 경우 ASA 컨피그레이션에서 로깅을 구성해야 합니다.

절차

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

단계 **2** 로컬 대상을 구성합니다.

a) **Local Destinations(**로컬 대상**)** 탭을 클릭합니다.

b) 다음 필드를 입력합니다.

이름	설명
콘솔	
관리자 상태	콘솔에서 syslog 메시지를 표시하려면 **Enable(**활성화**)** 체크 박스를 선택합니다.
레벨	콘솔에 표시하려는 가장 낮은 메시지 레벨을 클릭합니다. Firepower 섀시는 해당 레벨 이상의 메시지를 표시합니다. • 긴급 상황 • 알림 • **Critical(**중대**)**
플랫폼	
관리자 상태	플랫폼 syslog는 항상 활성화되어 있습니다.
레벨	표시하려는 가장 낮은 메시지 레벨을 선택합니다. Firepower 섀시는 해당 레벨 이상의 메시지를 표시합니다. 기본값은 **Informational(**정보**)**입니다. • 긴급 상황 • 알림 • **Critical(**중대**)** • 오류 • 경고**(**들**)** • **Notifications(**알림**)** • 정보 • 디버깅
File(파일**)**	

이름	설명
관리자 상태	syslog 메시지를 파일에 저장하려면 **Enable(**활성화**)** 체크 박스를 선택합니다.
레벨	저장하려는 가장 낮은 메시지 레벨을 선택합니다. 시스템에서는 해당 레벨 이상의 메시지를 저장합니다. • 긴급 상황 • 알림 • **Critical(**중대**)** • 오류 • 경고**(**들**)** • **Notifications(**알림**)** • 정보 • 디버깅
이름	파일 이름(최대 16자)을 설정합니다.
크기	시스템이 가장 오래된 메시지에 최신 메시지를 덮어쓰기 시작하기 전에 최대 파일 크기(바이트 단위)를 지정합니다. 범위는 4096~4194304바이트입니다.

c) **Save(**저장**)**를 클릭합니다.

단계 **3** 원격 대상을 구성합니다.

a) **Remote Destination(**원격 대상**)** 탭을 클릭합니다.

b) **Remote Destination(**원격 대상**)** 탭에서 Firepower 섀시에서 생성된 메시지를 저장할 수 있는 외부 로그 최대 3개의 다음 필드를 입력합니다.
원격 대상에 syslog 메시지를 전송하여 외부 syslog 서버의 사용 가능한 디스크 공간에 따라 메시지를 보관할 수 있으며, 저장한 후에 로그 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.

이름	설명
관리자 상태	원격 로그 파일에 syslog 메시지를 저장하려면 **Enable(**활성화**)** 체크 박스를 선택합니다.

이름	설명
레벨	시스템에서 저장하려는 가장 낮은 메시지 레벨을 선택합니다. 시스템은 원격 파일에 해당 수준 이상의 메시지를 저장합니다. • 긴급 상황 • 알림 • **Critical(**중대**)** • 오류 • 경고**(**들**)** • **Notifications(**알림**)** • 정보 • 디버깅
호스트 이름**/IP** 주소	syslog 서버의 호스트 이름 또는 IP 주소를 설정합니다. 참고 IP 주소 대신 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.
기능	파일 메시지의 기반으로 사용할 syslog 서버에 대한 시스템 로그를 선택합니다. • **Local0** • **Local1** • **Local2** • **Local3** • **Local4** • **Local5** • **Local6** • **Local7**

c) **Save(**저장**)**를 클릭합니다.

단계 **4** 로컬 소스를 구성합니다.

a) **Local Sources(**로컬 소스**)** 탭을 클릭합니다.

b) 다음 필드를 입력합니다.

이름	설명
Faults Admin State(결함 관리 상태**)**	시스템 결함 로깅의 활성화 여부. **Enable(**활성화**)** 체크 박스를 선택한 경우 Firepower 섀시가 모든 시스템 결함을 로깅합니다.

이름	설명
Audits Admin State(감사 관리 상태**)**	감사 로깅의 활성화 여부. **Enable(**활성화**)** 체크 박스를 선택한 경우 Firepower 섀시가 모든 감사 로그 이벤트를 로깅합니다.
Events Admin State(이벤트 관리 상태**)**	시스템 이벤트 로깅의 활성화 여부. **Enable(**활성화**)** 체크 박스를 선택한 경우 Firepower 섀시가 모든 시스템 이벤트를 로깅합니다.

c) **Save(**저장**)**를 클릭합니다.

DNS: DNS 서버 구성

시스템에서 호스트 이름의 IP 주소를 확인해야 하는 경우 DNS 서버를 지정해야 합니다. 최대 4개까지 DNS 서버를 구성할 수 있습니다. 여러 DNS 서버를 구성할 경우 임의의 순서로만 서버를 검색합니다..

시작하기 전에

- DNS는 기본적으로 OpenDNS 서버인 208.67.222.222, 208.67.220.220으로 구성됩니다.

절차

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

단계 **2** **Enable DNS Server(DNS** 서버 활성화**)** 체크 박스를 선택합니다.

단계 **3** 추가하려는 각 DNS 서버에 대해 최대 4개까지 **DNS Server(DNS** 서버**)** 필드에 DNS 서버의 IP 주소를 입력하고 **Add(**추가**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** **Domain Name Configuration(**도메인 이름 컨피그레이션**)** 탭에서 Firepower 섀시에서 정규화되지 않은 이름에 접미사로 추가하려는 **Domain name(**도메인 이름**)**을 입력하고 **Add(**추가**)**를 클릭합니다. 예를 들어 도메인 이름을 "example.com"으로 설정하고 "jupiter"라는 정규화되지 않은 이름으로 syslog 서버를 지정하는 경우 Firepower 섀시는 그 이름을 "jupiter.example.com"으로 정규화합니다.

FIPS 및 공통 기준: FIPS 및 공통 기준 모드 활성화

Firepower 2100에서 FIPS 또는 CC(공통 기준) 모드를 활성화하려면 다음 단계를 수행하십시오.

또한, **fips enable** 명령을 사용하여 ASA에서 FIPS 모드를 별도로 활성화해야 합니다. ASA에는 공통 기준 모드에 대한 별도의 설정이 없으며 CC 또는 UCAPL 컴플라이언스에 대한 추가 제한 사항을 Cisco 보안 정책 문서에 따라 구성해야 합니다.

ASA에서 FIPS 모드를 먼저 설정하고 디바이스가 다시 로드될 때까지 기다린 다음 FXOS에서 FIPS 모드를 설정하는 것이 좋습니다.

절차

단계 **1** **Platform Settings(**플랫폼 설정**)** > **FIPS and Common Criteria(FIPS** 및 공통 기준**)**를 선택합니다.

단계 **2** **Enable(**활성화**)** 체크 박스를 선택하여 **FIPS**를 활성화합니다.

단계 **3** **Enable(**활성화**)** 체크 박스를 선택하여 **Common Criteria(**공통 기준**)**를 활성화합니다.
공통 기준을 활성화하는 경우 **FIPS Enable(FIPS** 활성화**)** 체크 박스가 기본적으로 활성화됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

단계 **5** 프롬프트에 따라 시스템을 리부팅합니다.

액세스 목록: 관리 액세스 구성

기본적으로 Firepower 2100을 사용하면 관리 1/1 192.168.45.0/24 네트워크에서 Firepower Chassis Manager 및 SSH 액세스에 대한 HTTPS 액세스가 가능해집니다. 다른 네트워크에서의 액세스를 허용하거나 SNMP를 허용하려는 경우 액세스 목록을 추가하거나 변경해야 합니다.

IP 주소(v4 또는 v6)의 각 블록의 경우 각 서비스에 대해 최대 25개의 서브넷을 구성할 수 있습니다.

절차

단계 **1** **Platform Settings(**플랫폼 설정**)** > **Access List(**액세스 목록**)**를 선택합니다.

단계 **2** **IPv4 Access List(IPv4** 액세스 목록**)** 영역에서 다음 작업을 수행합니다.

a) **Add(**추가**)**를 클릭합니다.

b) 다음에 대한 값을 입력합니다.

- **IP Address(IP** 주소**)** — IP 주소를 설정합니다. 모든 네트워크를 허용하려면 **0.0.0.0**을 입력합니다.
- **Prefix Length(**접두사 길이**)** — 서브넷 마스크를 설정합니다. 모든 네트워크를 허용하려면 **0**을 입력합니다.
- **Protocol(**프로토콜**)** — **HTTPS**, **SNMP** 또는 **SSH**를 선택합니다.

c) **OK(**확인**)**를 클릭합니다.

d) 서비스별로 추가 네트워크를 추가하려면 이 단계를 반복합니다.

단계 **3** **IPv6 Access List(IPv6** 액세스 목록**)** 영역에서 다음 작업을 수행합니다.

a) **Add(**추가**)**를 클릭합니다.
b) 다음에 대한 값을 입력합니다.

- **IP Address(IP** 주소**)** — IP 주소를 설정합니다. 모든 네트워크를 허용하려면 ::을 입력합니다.
- **Prefix Length(**접두사 길이**)** — 접두사 길이를 설정합니다. 모든 네트워크를 허용하려면 **0**을 입력합니다.
- **Protocol(**프로토콜**)** — **HTTPS**, **SNMP** 또는 **SSH**를 선택합니다.

c) **OK(**확인**)**를 클릭합니다.
d) 서비스별로 추가 네트워크를 추가하려면 이 단계를 반복합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

시스템 업데이트

이 작업은 독립형 ASA에 적용됩니다. 장애 조치 쌍을 업그레이드하려는 경우 Cisco ASA 업그레이드 가이드를 참조하십시오. 업그레이드 프로세스에는 일반적으로 20~30분이 소요됩니다.

ASA, ASDM 및 FXOS 이미지는 단일 패키지에 번들로 제공됩니다. 패키지 업데이트는 FXOS에 의해 관리되며 ASA 운영 체제 내에서 ASA를 업그레이드할 수 없습니다. ASA와 FXOS는 각각 별도로 업그레이드할 수 없습니다. 이 두 가지는 항상 번들로 제공됩니다.

ASDM의 예외 사항은 ASA 운영 체제 내에서 업그레이드할 수 있다는 것입니다. 따라서 번들로 제공된 ASDM 이미지만 사용할 필요는 없습니다. 수동으로 업로드하는 ASDM 이미지는 FXOS 이미지 목록에 나타나지 않습니다. ASA에서 ASDM 이미지를 관리해야 합니다.

참고 번들을 업그레이드하는 경우 번들 이미지가 동일한 이름(**asdm.bin**)을 지니고 있기 때문에 번들의 ASDM 이미지가 이전 ASDM 번들 이미지를 대체합니다. 단, 업로드한 다른 ASDM 이미지를 수동으로 선택하는 경우(예: **asdm-782.bin**) 번들 업그레이드 이후에도 계속 해당 이미지를 사용하십시오. ASDM의 호환 가능한 버전을 실행 중인지 확인하려면 번들을 업그레이드하기 전에 ASDM을 업그레이드하거나 ASA 번들을 업그레이드하기 바로 전에 번들로 제공된 ASDM 이미지(**asdm.bin**)를 사용하도록 ASA를 다시 구성해야 합니다.

시작하기 전에

업로드할 이미지를 로컬 컴퓨터에서 사용할 수 있는지 확인합니다.

절차

단계 **1** **System(**시스템**)** > **Updates(**업데이트**)**를 선택합니다.
Available Updates(사용 가능한 업데이트**)** 페이지에는 섀시에서 사용 가능한 패키지 목록이 표시됩니다.

단계 **2** **Upload Image(**이미지 업로드**)**를 클릭합니다.

단계 **3** **Browse(**찾아보기**)**를 클릭하여 이동하고 업로드할 이미지를 찾습니다.

단계 **4** **Upload(**업로드**)**를 클릭합니다.
선택한 이미지가 섀시에 업로드됩니다. 이미지 무결성은 새로운 이미지가 섀시에 추가될 때 자동으로 확인됩니다. 수동으로 확인하려는 경우 **Verify(**확인**)**(체크 마크 아이콘)를 클릭합니다.

단계 **5** 업그레이드하려는 ASA 패키지를 선택하고 **Upgrade(**업그레이드**)**를 클릭합니다.

단계 **6** **Yes(**예**)**를 클릭하여 설치를 계속할지 확인하거나 **No(**아니요**)**를 클릭하여 설치를 취소합니다.
업그레이드하는 동안 Firepower Chassis Manager에서 로그아웃됩니다.

사용자 관리

사용자 계정은 Firepower 2100 섀시에 액세스하는 데 사용됩니다. 이러한 계정은 Firepower Chassis Manager 및 SSH 액세스를 위해 사용됩니다. ASA에는 별도의 사용자 계정 및 인증 기능이 있습니다.

사용자 계정 정보

최대 48개의 로컬 사용자 계정을 구성할 수 있습니다. 각 사용자 계정에는 고유한 사용자 이름 및 비밀번호가 있어야 합니다.

계정 유형

관리자 계정

관리자 계정은 기본 사용자 계정이며 수정하거나 삭제할 수 없습니다. 이 계정은 시스템 관리자 또는 슈퍼 사용자(superuser) 계정이며 전체 권한을 갖습니다. 기본 비밀번호는 **Admin123**입니다.

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

로컬 인증 사용자 계정

로컬 인증 사용자 계정은 섀시를 통해 직접 인증되며 관리자 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 계정을 다시 활성화하는 경우, 해당 계정은 사용자 이름 및 비밀번호를 포함한 기존 컨피그레이션으로 다시 활성화됩니다.

사용자 역할

시스템에는 다음과 같은 사용자 역할이 포함됩니다.

관리자

전체 시스템에 대한 완전한 읽기 및 쓰기 액세스. 기본 관리자 계정은 기본적으로 이 역할을 지정받으며 변경할 수 없습니다.

읽기 전용

시스템 상태를 수정할 권한이 없는, 시스템 컨피그레이션에 대한 읽기 전용 액세스.

사용자 계정 만료

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

기본적으로 사용자 계정은 만료되지 않습니다.

사용자 계정에 만료일을 구성하면, 해당 계정을 만료하도록 재구성할 수 없습니다. 그러나 계정에 최신 만료일을 사용할 수 있도록 구성할 수는 있습니다.

사용자 계정에 대한 지침

사용자 이름

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

- 로그인 ID는 1자 ~ 32자이며 다음을 포함할 수 있습니다.
  - 모든 영문자
  - 모든 숫자
  - _(밑줄)
  - -(대시)
  - . (점)
- 로그인 ID는 고유해야 합니다.
- 로그인 ID는 영문자로 시작해야 합니다. 숫자 또는 특수 문자(예: 밑줄)로 시작할 수 없습니다.
- 로그인 ID는 대/소문자를 구분합니다.
- 전부 숫자로 된 로그인 ID를 만들 수 없습니다.
- 사용자 계정을 만든 후에는 로그인 ID를 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 만들어야 합니다.

비밀번호

로컬에서 인증되는 각 사용자 계정에는 비밀번호가 필요합니다. 관리자 또는 AAA 권한이 있는 사용자는 사용자 비밀번호에 대한 비밀번호 보안 수준을 확인하도록 시스템을 구성할 수 있습니다. 비밀번호 길이 검사를 활성화하면 각 사용자는 강력한 비밀번호를 사용해야 합니다.

각 사용자가 강력한 비밀번호를 사용하는 것이 좋습니다. 로컬로 인증된 사용자에 대해 비밀번호 길이 검사를 활성화하는 경우 FXOS에서는 다음 요건을 충족하지 않는 비밀번호를 거부합니다.

- 8자 이상, 80자 이하여야 합니다.

참고 Common Criteria 요구 사항을 준수하기 위해 시스템에서 최소 15자 비밀번호 길이를 선택적으로 구성할 수 있습니다. 자세한 내용은 사용자 설정 구성, 45 페이지를 참조하십시오.

- 하나 이상의 알파벳 대문자를 포함해야 합니다.
- 하나 이상의 알파벳 소문자를 포함해야 합니다.
- 하나 이상의 영숫자 외 문자(특수 문자)를 포함해야 합니다.
- aaabbb와 같이 한 문자가 3번 이상 연속적으로 나와서는 안 됩니다.
- 어떤 순서로든 3개의 연속 숫자 또는 문자를 포함해서는 안 됩니다(예: passwordABC 또는 password321).
- 사용자 이름 또는 사용자 이름의 역순과 같아서는 안 됩니다.
- 비밀번호 사전 검사를 통과해야 합니다. 예를 들어 비밀번호가 표준 사전 단어를 기반으로 해서는 안 됩니다.
- $(달러 기호), ?(물음표), =(등호) 기호를 포함해서는 안 됩니다.
- 로컬 사용자 및 관리자 계정 비밀번호는 비어 있지 않아야 합니다.

사용자 추가

Firepower Chassis Manager 및 FXOS CLI 액세스를 위해 로컬 사용자를 추가합니다.

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** 사용자에 대한 필수 정보로 다음 필드를 완성합니다.

이름	설명
User Name(사용자 이름) 필드	계정 로그인에 사용하는 계정 이름. 이름은 고유해야 하며 사용자 계정 이름에 대한 지침 및 제한 사항을 따라야 합니다(사용자 계정에 대한 지침, 42 페이지 참조). 사용자를 저장하면 로그인 ID는 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 만들어야 합니다.
First Name(이름) 필드	사용자의 이름입니다. 최대 32자입니다.
Last Name(성) 필드	사용자의 성입니다. 최대 32자입니다.
Email(이메일) 필드	사용자의 이메일 주소입니다.
Phone Number(전화 번호) 필드	사용자의 전화 번호.
Password(비밀번호) 필드	이 계정의 비밀번호. 비밀번호 길이 검사를 활성화한 경우 사용자의 비밀번호가 더욱 강력해지며 FXOS는 길이 검사 요건을 충족하지 않는 비밀번호를 거부합니다(사용자 계정에 대한 지침, 42 페이지 참조).
Confirm Password(비밀번호 확인) 필드	확인을 위해 두 번째로 입력하는 비밀번호.
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	사용자 계정에 할당할 수 있는 권한에 해당하는 역할입니다(사용자 역할, 41 페이지 참조). 모든 사용자에게 기본적으로 읽기 전용 역할이 할당되며 이 역할은 선택 취소할 수 없습니다. 여러 역할을 할당하려면 Ctrl 키를 누른 상태에서 원하는 역할을 클릭합니다. 참고 사용자 역할 및 권한의 변경은 사용자가 다음에 로그인할 때 적용됩니다. 사용자가 로그인할 때 새 역할을 지정하거나 사용자 계정의 기존 역할을 삭제할 경우 활성 세션에서는 기존의 역할 및 권한을 유지합니다.
Account Expires(계정 만료) 체크 박스	이 체크 박스를 선택한 경우, 해당 계정은 만료되며 **Expiration Date**(만료일) 필드에 지정된 날짜 이후에 사용할 수 없습니다. 참고 사용자 계정에 만료일을 구성하면, 해당 계정을 만료하도록 재구성할 수 없습니다. 그러나 계정에 최신 만료일을 사용할 수 있도록 구성할 수는 있습니다.

이름	설명
Expiry Date(만료일**)** 필드	계정이 만료되는 날. yyyy-mm-dd 형식이어야 합니다. 만료일을 선택하기 위해 달력을 보려면 이 필드의 마지막에 있는 달력 아이콘을 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** 사용자를 비활성화합니다.

a) 비활성화하려는 사용자에 대해 **Edit(**편집**)(**연필 아이콘**)**을 클릭합니다.
관리자 사용자 계정은 항상 활성으로 설정됩니다. 이는 수정할 수 없습니다.

b) **Account Status(**계정 상태**)** 필드의 **Inactive(**비활성**)** 라디오 버튼을 클릭합니다.

c) **Save(**저장**)**를 클릭합니다.

사용자 설정 구성

모든 사용자에 대해 글로벌 설정을 구성할 수 있습니다.

절차

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

단계 **2** **Settings(**설정**)** 탭을 클릭합니다.

단계 **3** 다음 필드에 필수 정보를 입력합니다.

이름	설명
Default Authentication(기본 인증**)** 필드	원격 로그인 과정에서 사용자가 인증되는 기본 방법. 다음 중 하나일 수 있습니다. • **Local(**로컬**)** — 사용자 계정이 Firepower 섀시에서 로컬로 정의되어야 합니다. • **None(**없음**)** — 사용자 계정이 Firepower 섀시에서 로컬인 경우, 사용자가 원격으로 로그인할 때 비밀번호가 필요하지 않습니다.
로컬 사용자 설정	
Password Strength Check(비밀번호 길이 검사**)** 체크 박스	이 옵션을 선택하면 모든 로컬 사용자 비밀번호가 강력한 비밀번호의 지침을 따라야 합니다(사용자 계정에 대한 지침, 42페이지 참조).

이름	설명
History Count(기록 수**)** 필드	사용자가 이전에 사용했던 비밀번호를 재사용하기 전에 생성해야 할 고유한 비밀번호의 수. 기록 수는 최근 항목부터 시간순으로 저장되며, 기록 수 임계값에 도달할 경우 가장 오래된 비밀번호만 재사용될 수 있습니다. 0 ~ 15의 어떤 값이든 가능합니다. **History Count(**기록 수**)** 필드를 0으로 설정하여 기록 수를 비활성화하고 사용자가 언제든지 이전에 사용한 비밀번호를 재사용하게 할 수 있습니다.
Change During Interval(사이에 변경**)** 필드	로컬로 인증된 사용자가 비밀번호를 변경할 수 있는 시기를 제어합니다. 가능한 값은 다음과 같습니다. • **Enable(**활성화**)** — 로컬로 인증된 사용자는 변경 간격 및 변경 횟수에 대한 설정을 기초로 비밀번호를 변경할 수 있습니다. • **Disable(**비활성화**)** — 로컬로 인증된 사용자는 변경 안 함 간격 동안 지정된 시간 간격에 비밀번호를 변경할 수 없습니다.
Change Interval(변경 간격**)** 필드	**Change Count(**변경 횟수**)** 필드에 지정된 비밀번호 변경 횟수가 적용되는 시간입니다. 1시간 ~ 745시간의 어떤 값이든 가능합니다. 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.
Change Count(변경 수**)** 필드	로컬로 인증된 사용자가 변경 간격 동안 비밀번호를 변경할 수 있는 최대 횟수입니다. 0 ~ 10의 어떤 값이든 가능합니다.
No Change Interval(변경 불가 간격**)** 필드	로컬로 인증된 사용자가 새로 생성된 비밀번호를 변경하기 전에 기다려야 하는 최소 시간입니다. 1시간 ~ 745시간의 어떤 값이든 가능합니다. 이 간격은 **Change During Interval(**사이에 변경**)** 속성이 **Disable(**비활성**)**로 설정되지 않은 경우 무시됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.