Cisco FXOS Firepower Chassis Manager 컨피그레이션 가이드, 1.1(2)

초판: 2015년 09월 28일

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

텍스트 부품 번호: 온라인 전용

목 차

Firepower 9300 소개 **1**

Firepower 9300 Security Appliance 정보 **1**

Firepower Chassis Manager 개요 **1**

섀시 상태 모니터링 **2**

시작하기 **5**

작업 플로우 **5**

초기 컨피그레이션 **6**

Firepower Chassis Manager 로그인 또는 로그아웃 **8**

FXOS CLI 액세스 **8**

라이센스 관리 **11**

Smart Software Licensing 정보 **11**

Firepower 9300의 보안 모듈을 위한 Smart Software Licensing **11**

Smart Software Manager 및 어카운트 **12**

가상 어카운트별로 관리되는 라이센스 및 디바이스 **12**

디바이스 등록 및 토큰 **12**

License Authority와의 정기적인 통신 **13**

규정 위반 상태 **13**

Smart Call Home 인프라 **13**

Smart Software Licensing 사전 요구 사항 **13**

Smart Software Licensing의 기본값 **14**

Smart Software Licensing 구성 **14**

(선택 사항) HTTP 프록시 구성 **14**

License Authority를 통해 Firepower 9300 등록 **15**

Smart Software Licensing 기록 **16**

사용자 관리 **17**

사용자 계정 **17**

기본 사용자 역할 **19**

로컬에서 인증된 사용자용 비밀번호 프로필 19
사용자 설정 구성 21
로컬 사용자 계정 생성 24
로컬 사용자 어카운트 삭제 26
로컬 사용자 어카운트 활성화 또는 비활성화 27
이미지 관리 29
이미지 관리 정보 29
Cisco.com에서 이미지 다운로드 30
Firepower 어플라이언스에 이미지 업로드 30
Firepower eXtensible 운영 체제 플랫폼 번들 업그레이드 31
논리적 디바이스를 위한 이미지 버전 업데이트 31
플랫폼 설정 33
날짜 및 시간 설정 33
NTP 서버를 사용하여 날짜 및 시간 설정 33
날짜 및 시간 직접 설정 34
SSH 구성 34
텔넷 구성 35
SNMP 구성 36
SNMP 소개 36
SNMP 알림 37
SNMP 보안 수준 및 권한 37
지원되는 SNMP 보안 모델과 수준 결합 37
SNMPv3 보안 기능 38
SNMP 지원 39
SNMP 활성화 및 SNMP 속성 구성 39
SNMP 트랩 생성 40
SNMP 트랩 삭제 41
SNMPv3 사용자 생성 42
SNMPv3 사용자 삭제 43
HTTPS 포트 변경 43
AAA 구성 43
AAA 정보 44

LDAP 제공자 구성 45
LDAP 제공자 속성 구성 45
LDAP 제공자 생성 46
LDAP 제공자 삭제 48
RADIUS 제공자 구성 49
RADIUS 제공자 속성 구성 49
RADIUS 제공자 생성 49
RADIUS 제공자 삭제 51
TACACS+ 제공자 구성 51
TACACS+ 제공자 속성 구성 51
TACACS+ 제공자 생성 52
TACACS+ 제공자 삭제 53
Syslog 구성 53
DNS 서버 구성 56
인터페이스 관리 57
Firepower 9300 인터페이스 정보 57
인터페이스 속성 편집 58
인터페이스의 관리 상태 변경 58
포트 채널 생성 59
분할 케이블 구성 60
논리적 디바이스 63
논리적 디바이스 정보 63
독립형 ASA 논리적 디바이스 생성 64
독립형 위협 방어 논리적 디바이스 생성 65
클러스터 구축 67
클러스터링 정보 67
마스터 및 슬레이브 유닛 역할 68
Cluster Control Link 68
관리 인터페이스 68
클러스터링 지침 69
클러스터링 기본값 69
ASA 클러스터링 구성 69

위협 방어 클러스터링 구성 71
클러스터링 기록 73
보안 모듈의 콘솔에 연결 73
논리적 디바이스 삭제 74
보안 모듈 관리 77
Firepower 9300 보안 모듈 정보 77
보안 모듈 해제/재위탁 79
보안 모듈 확인 79
보안 모듈 재설정 80
보안 모듈 다시 초기화 80
보안 모듈 켜기/끄기 80

1 장

Firepower 9300 소개

- Firepower 9300 Security Appliance 정보, 1 페이지
- Firepower Chassis Manager 개요, 1 페이지
- 섀시 상태 모니터링, 2 페이지

Firepower 9300 Security Appliance 정보

Cisco Firepower 9300 Security Appliance는 네트워크 및 콘텐츠 보안 솔루션을 위한 차세대 플랫폼입니다. Firepower 9300는 Cisco ACI(Application Centric Infrastructure) 보안 솔루션에 포함되며 확장성, 제어 일관성 및 관리 간소화를 위해 구축된 민첩한 개방형 보안 플랫폼을 제공합니다.

Firepower 9300에서 제공하는 기능은 다음과 같습니다.

- 모듈형 섀시 기반 보안 시스템 - 고성능의 유연한 입/출력 컨피그레이션 및 확장성을 제공합니다.
- Firepower Chassis Manager - 그래픽 사용자 인터페이스는 현재 섀시 상태를 간단하게 시각적으로 표시하며 간소화된 섀시 기능 컨피그레이션을 제공합니다.
- FXOS CLI - 기능 구성, 섀시 상태 모니터링 및 고급 문제 해결 기능 액세스를 위해 명령 기반 인터페이스를 제공합니다.
- FXOS REST API - 사용자는 섀시를 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 네비게이션 바를 통해 다음에 액세스할 수 있습니다.

- 개요 - 개요 페이지에서 Firepower 섀시의 상태를 간편하게 모니터링할 수 있습니다. 자세한 내용은 섀시 상태 모니터링, 2 페이지를 참고하십시오.

- 인터페이스 - 인터페이스 페이지에서 섀시에 설치된 인터페이스의 상태를 확인하고 인터페이스 속성을 편집하며 인터페이스를 활성화 또는 비활성화하고 포트 채널을 생성할 수 있습니다. 자세한 내용은 인터페이스 관리, 57 페이지를 참고하십시오.
- 논리적 디바이스 - 논리적 디바이스 페이지에서 논리적 디바이스를 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 논리적 디바이스, 63 페이지를 참고하십시오.
- 보안 모듈 - Security Modules(보안 모듈) 페이지에서 보안 모듈의 상태를 확인하고, 보안 모듈에 대해 전원 껐다 켜기, 다시 초기화, 확인 및 해제 등 다양한 기능을 수행할 수 있습니다. 자세한 내용은 보안 모듈 관리, 77 페이지를 참고하십시오.
- 플랫폼 설정 - 플랫폼 설정 페이지에서 날짜 및 시간, SSH, SNMP, HTTPS, AAA, Syslog 및 DNS 등 섀시 설정을 구성할 수 있습니다. 자세한 내용은 플랫폼 설정, 33 페이지를 참고하십시오.
- 시스템 설정 - 시스템 메뉴에서 다음 설정을 관리할 수 있습니다.
  - 라이센싱 - 라이센싱 페이지에서 Smart Call Home 설정을 구성하고 License Authority를 통해 Firepower 섀시에 등록할 수 있습니다. 자세한 내용은 라이센스 관리, 11 페이지를 참고하십시오.
  - 업데이트 - 업데이트 페이지에서 Firepower 섀시에 플랫폼 번들 및 애플리케이션 이미지를 업로드할 수 있습니다. 자세한 내용은 이미지 관리, 29 페이지를 참고하십시오.
  - 사용자 관리 - 사용자 관리 페이지에서 Firepower 어플라이언스에 대한 사용자 설정을 구성하고 사용자 어카운트를 정의할 수 있습니다. 자세한 내용은 사용자 관리, 17 페이지를 참고하십시오.

섀시 상태 모니터링

개요 페이지에서 Firepower 섀시의 상태를 쉽게 모니터링할 수 있습니다. 개요 페이지에서 다음의 정보를 제공합니다.

- 디바이스 정보 - 개요 페이지 상단에는 Firepower 섀시에 대한 다음 정보가 포함되어 있습니다.
  - 섀시 이름 - 초기 컨피그레이션 동안 섀시에 할당된 이름 표시.
  - IP 주소 - 초기 컨피그레이션 동안 섀시에 할당된 관리 IP 주소 표시.
  - 모델 - Firepower 섀시 모델 표시.
  - 버전 - 섀시에서 실행 중인 FXOS의 버전 번호 표시.
  - 모드 - 섀시의 작동 모드 표시(독립형 또는 클러스터).
  - 전체 상태 - 섀시에 대한 작동 가능 상태 표시.
  - 섀시 업타임 - 시스템이 마지막으로 재시작된 이후 경과한 시간 표시.

팁 섀시 업타임 필드 오른쪽에 있는 아이콘 위로 마우스를 가져가면 섀시에 설치된 보안 모듈에 대한 업타임을 확인할 수 있습니다.

- 시각적 상태 표시 - 디바이스 정보 섹션 아래에는 섀시를 시각적으로 볼 수 있는 설명이 나옵니다. 여기에는 섀시에 설치된 구성 요소와 그 구성 요소의 일반적인 상태를 보여줍니다. 시각적 상태 표시(Visual Status Display)에 나타난 보안 모듈 또는 포트로 마우스를 가져가면 해당 항목에 대한 추가 정보를 얻을 수 있습니다.
- 상세한 상태 정보 - 시각적 상태 표시 아래에는 섀시에 대한 상세한 상태 정보를 포함하는 표가 나와 있습니다. 상태 정보는 결함, 인터페이스, 디바이스, 라이센스 및 인벤토리의 5가지 섹션으로 나눠집니다. 각 섹션의 요약 정보를 테이블 상단에서 확인할 수 있으며 원하는 정보의 요약 영역을 클릭하여 각 섹션의 추가 정보를 확인할 수 있습니다.

  시스템은 섀시에 대해 다음의 상세한 상태 정보를 제공합니다.

  - 결함 - 시스템에서 생성된 결함을 나열합니다. 오류는 매우 중요, 주요, 사소, 경고 및 정보의 심각도별로 정렬됩니다. 나열된 각 결함의 심각도, 결함에 대한 설명, 원인, 발생 횟수 및 가장 최근에 발생한 시간을 확인할 수 있습니다. 또한 결함이 승인되었는지 여부를 확인할 수 있습니다.

    결함 중 하나를 클릭하여 결함에 대한 추가 정보를 확인하거나 결함을 승인할 수 있습니다.

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

  - 인터페이스 - 시스템에 설치된 인터페이스를 나열하고 각 인터페이스에 대해 다음 세부사항을 제공합니다. 예: 인터페이스 이름, 작동 상태, 관리 상태, 수신된 바이트 수, 전송된 바이트 수

    인터페이스 중 하나를 클릭하여 마지막 15분 동안 인터페이스에 대한 입력 및 출력 바이트 수에 대한 그래픽 표시를 확인할 수 있습니다.

  - 디바이스 - 시스템에 구성된 논리적 디바이스를 나열하고 각 논리적 디바이스에 대해 다음 세부사항을 제공합니다. 예: 디바이스 이름, 디바이스 상태, 애플리케이션 템플릿 유형, 작동 상태, 관리 상태, 이미지 버전, 관리 IP 주소 및 ASDM URL
  - 라이센스 - 스마트 라이센싱 활성화 여부를 표시하며 Firepower 라이센스의 현재 등록 상태를 제공하고 섀시의 라이센스 권한 부여 정보를 표시합니다.
  - 인벤토리 - 섀시에 설치된 구성 요소를 나열하고 해당 구성 요소와 관련된 세부사항을 제공합니다. 예: 구성 요소 이름, 코어 수, 설치 위치, 작동 상태, 동작 가능성, 용량, 전원, 열, 일련 번호, 모델 번호, 부품 번호 및 벤더

2 장

시작하기

- 작업 플로우, 5 페이지
- 초기 컨피그레이션, 6 페이지
- Firepower Chassis Manager 로그인 또는 로그아웃, 8 페이지
- FXOS CLI 액세스, 8 페이지

작업 플로우

다음 절차에서는 Firepower 어플라이언스 구성 시 완료해야 하는 기본 작업을 보여줍니다.

절차

단계 **1** Firepower 어플라이언스 하드웨어를 구성합니다(Cisco Firepower 9300 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, 33 페이지 참조).

단계 **5** DNS 서버를 구성합니다(DNS 서버 구성, 56 페이지 참조).

단계 **6** 제품 라이센스를 등록합니다(라이센스 관리, 11 페이지 참조).

단계 **7** 사용자를 구성합니다(사용자 관리, 17 페이지 참조).

단계 **8** 필요 시 소프트웨어 업데이트를 수행합니다(이미지 관리, 29 페이지 참조).

단계 **9** 추가 플랫폼 설정을 구성합니다(플랫폼 설정, 33 페이지 참조).

단계 **10** 인터페이스를 구성합니다(인터페이스 관리, 57 페이지 참조).

단계 **11** 논리적 디바이스를 생성합니다(논리적 디바이스, 63 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 어플라이언스에 액세스할 때 시스템을 구성하는 데 사용할 수 있는 설정 마법사가 나타납니다.

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

Firepower 어플라이언스의 단일 관리 포트에는 IPv4 주소, 게이트웨이 및 서브넷 마스크 하나만, 또는 IPv6 주소, 게이트웨이 및 네트워크 접두사 하나만 지정해야 합니다. 관리 포트 IP 주소에 대해 IPv4 또는 IPv6 주소를 구성할 수 있습니다.

시작하기 전에

1. Firepower 어플라이언스에서 다음의 물리적 연결을 확인합니다.
   - 콘솔 포트는 컴퓨터 터미널 또는 콘솔 서버에 물리적으로 연결됩니다.
   - 1Gbps 이더넷 관리 포트는 외부 허브, 스위치 또는 라우터에 연결됩니다.

   자세한 내용은 Cisco Firepower 9300 하드웨어 설치 가이드를 참조하십시오.
2. 콘솔 포트에 연결된 컴퓨터 터미널(또는 콘솔 서버)의 콘솔 포트 매개변수가 다음과 같은지 확인하십시오.
   - 9600보드
   - 8 데이터 비트
   - 패리티 없음
   - 1 스톱 비트

절차

단계 **1** 콘솔 포트에 연결합니다.

단계 **2** Firepower 어플라이언스의 전원을 켭니다.
Firepower 어플라이언스가 부팅할 때 자체 전원 테스트 메시지를 확인할 수 있습니다.

단계 **3** 구성되지 않은 시스템을 부팅할 경우, 설정 마법사에 시스템을 구성하는 데 필요한 다음 정보를 묻는 프롬프트가 표시됩니다.
- 설정 모드(전체 시스템 백업 또는 초기 설정에서 복원)
- 강력한 비밀번호 시행 정책(강력한 비밀번호 지침에 대해서는 사용자 계정, 17 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 설정 마법사를 통해 일부 설정을 변경합니다.
설정 마법사를 다시 사용하도록 선택하는 경우 이전에 입력한 값이 괄호로 나타납니다. 이전에 입력한 값을 승인하려면 **Enter**를 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

절차

단계 **1** Firepower Chassis Manager에 로그인하려면 다음과 같이 합니다.

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

이때 <*chassis_mgmt_ip_address*>는 초기 컨피그레이션을 설정하는 동안 입력한 Firepower 어플라이언스의 IP 주소 또는 호스트 이름입니다.

b) 사용자 이름과 비밀번호를 입력합니다.

c) **Login(**로그인**)**을 클릭합니다.

로그인하면 Firepower Chassis Manager가 열리고 요약 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 전원이 연결된 터미널을 사용하여 FXOS CLI에 연결할 수 있습니다. 콘솔 포트에 연결된 컴퓨터 터미널(또는 콘솔 서버)의 콘솔 포트 매개변수가 다음과 같은지 확인하십시오.

- 9600보드
- 8 데이터 비트
- 패리티 없음
- 1 스톱 비트

또한 SSH 및 텔넷을 사용하여 FXOS CLI에 연결할 수 있습니다. Firepower eXtensible 운영 체제은 최대 8개의 동시 SSH 연결을 지원합니다. SSH를 사용하여 연결하려면 Firepower 어플라이언스의 IP 주소 또는 호스트 이름을 알아야 합니다.

다음 구문 예시 중에서 하나를 사용하여 SSH, 텔넷 또는 Putty를 통해 로그인할 수 있습니다.

참고 SSH 로그인은 대/소문자를 구분합니다.

SSH를 사용하는 Linux 터미널에서 다음 구문을 사용합니다.

- **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 터미널에서 다음 구문을 사용합니다.

참고 텔넷은 기본적으로 비활성화되어 있습니다. 텔넷 활성화에 대한 지침은 텔넷 구성, 35 페이지의 내용을 참조하십시오.

- **telnetucs-** *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\blradmin
```

Putty 클라이언트에서 다음 구문을 사용합니다.

- 다음으로 로그인: **ucs-** *auth-domain\username*

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

참고 기본 인증이 로컬로 설정되어 있고 콘솔 인증이 LDAP로 설정된 경우, ucs-local\admin을 사용하여 Putty 클라이언트에서 패브릭 인터커넥트에 로그인할 수 있으며 이때 admin은 로컬 어카운트의 이름입니다.

3 장

라이센스 관리

Cisco Smart Software Licensing은 라이센스 풀을 중앙에서 구입하고 관리하게 해줍니다. 각 유닛의 라이센스 키를 관리할 필요 없이 손쉽게 디바이스를 구축하거나 사용 중단할 수 있습니다. Smart Software Licensing은 라이센스 사용량과 수요를 한 번에 확인하게 해줍니다.

- Smart Software Licensing 정보, 11 페이지
- Smart Software Licensing 사전 요구 사항, 13 페이지
- Smart Software Licensing의 기본값, 14 페이지
- Smart Software Licensing 구성, 14 페이지
- Smart Software Licensing 기록, 16 페이지

Smart Software Licensing 정보

이 섹션에서는 Smart Software Licensing이 적용되는 방법에 관해 설명합니다.

Firepower 9300의 보안 모듈을 위한 Smart Software Licensing

Firepower 9300의 보안 모듈의 경우, Smart Software Licensing 컨피그레이션은 Firepower 9300 관리자(Supervisor)와 보안 모듈로 나뉩니다.

- Firepower 9300 - 관리자(Supervisor)에 모든 Smart Software Licensing 인프라를 구성하며 여기에는 License Authority와 통신하는 데 필요한 매개변수가 포함됩니다. Firepower 9300 자체는 작동하기 위한 라이센스가 필요하지 않습니다.
- 보안 모듈 - 보안 모듈의 모든 라이센스 엔타이틀먼트를 구성합니다.

Smart Software Manager 및 어카운트

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

http://tools.cisco.com/rhodui/index

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, 라이센스는 마스터 어카운트 아래에서 기본 가상 어카운트에 할당됩니다. 어카운트 관리자로서, 선택적으로 추가 가상 어카운트를 생성할 수 있습니다. 예를 들어, 지역, 부서 또는 자회사에 대해 어카운트를 만들 수 있습니다. 여러 가상 어카운트를 활용하면 많은 라이센스 및 디바이스를 보다 쉽게 관리할 수 있습니다.

가상 어카운트별로 관리되는 라이센스 및 디바이스

라이센스 및 디바이스는 가상 어카운트별로 관리됩니다. 가상 어카운트의 디바이스에서만 해당 어카운트에 지정된 라이센스를 사용할 수 있습니다. 추가 라이센스가 필요한 경우, 다른 가상 어카운트에서 사용하지 않는 라이센스를 전송할 수 있습니다. 또한 가상 어카운트 간에 디바이스를 이전할 수도 있습니다.

Firepower 9300 섀시만 디바이스로 등록되는 반면, 섀시의 보안 모듈에는 고유한 라이센스가 필요합니다. 예를 들어, 보안 모듈이 3개 있는 Firepower 9300 섀시의 경우 섀시는 디바이스 1개로 간주되지만 모듈은 개별 라이센스 3개를 사용합니다.

디바이스 등록 및 토큰

각 가상 어카운트에 대해, 등록 토큰을 만들 수 있습니다. 이 토큰은 기본적으로 30일 동안 유효합니다. 각 디바이스를 구축할 때 또는 기존 디바이스를 등록할 때 이 토큰 ID와 엔타이틀먼트 레벨을 입력합니다. 기존 토큰이 만료되는 경우 새 토큰을 만들 수 있습니다.

참고 디바이스 등록은 보안 모듈이 아닌 Firepower 9300 관리자(Supervisor)에서 구성됩니다.

구축 이후 시작할 때 또는 기존 디바이스에서 이 매개변수를 수동으로 구성한 후에 디바이스가 Cisco License Authority에 등록됩니다. 디바이스를 토큰과 함께 등록하면 License Authority는 디바이스와 License Authority 간의 통신을 위해 ID 인증서를 발급합니다. 이 인증서는 6개월 마다 갱신되지만 1년 동안 유효합니다.

License Authority와의 정기적인 통신

디바이스는 30일마다 License Authority와 통신합니다. Smart Software Manager에서 변경할 경우 변경 사항이 즉시 적용되도록 디바이스에서 권한 부여를 새로 고칠 수 있습니다. 또는 디바이스에서 예정대로 통신할 때까지 기다릴 수 있습니다.

선택적으로 HTTP 프록시를 구성할 수 있습니다. 최소 90일마다 디바이스가 직접 또는 HTTP 프록시를 통해 인터넷에 연결되어야 합니다. 일반 라이센스 통신은 30일마다 이루어지지만, 유예 기간이 있으므로 디바이스는 최대 90일간 콜 홈 없이 작동할 수 있습니다. 90일이 경과하기 전에 라이센싱 기관에 문의해야 합니다.

참고 오프라인 라이센싱은 지원되지 않습니다.

규정 위반 상태

디바이스는 다음과 같은 상황에서 규정 위반이 될 수 있습니다.

- 과다 사용 - 디바이스에서 사용 불가한 라이센스를 사용할 경우
- 라이센스 만료 - 시간 기반 라이센스가 만료하는 경우
- 통신 부재 - 디바이스에서 권한 재부여를 위해 Licensing Authority에 연결하지 못한 경우

권한 재부여 시도 90일 이후에 디바이스는 애플리케이션에 따라 일부 제한됩니다.

Smart Call Home 인프라

기본적으로, Smart Call Home 프로파일은 Licensing Authority의 URL을 지정하는 컨피그레이션에 있습니다. 이 프로파일을 제거할 수 없습니다. 라이센스 프로파일에 대해 구성 가능한 옵션만이 License Authority에 대한 대상 주소 URL이 됩니다. Cisco TAC에서 지시하지 않는 한, License Authority URL을 변경해서는 안 됩니다.

Smart Software Licensing의 Smart Call Home을 비활성화할 수 없습니다.

Smart Software Licensing 사전 요구 사항

- Cisco Smart Software Manager에서 마스터 어카운트를 만듭니다.

  http://tools.cisco.com/rhodui/index

  아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager를 활용하면 조직에서 사용할 마스터 어카운트를 만들 수 있습니다.

- Cisco Software Central에서 라이센스를 하나 이상 구매합니다.

- 디바이스에서 Licensing Authority와 통신할 수 있도록 디바이스에서 인터넷 액세스 또는 HTTP 프록시 액세스를 보장합니다. 오프라인 라이센싱은 지원되지 않습니다.
- 디바이스에서 Licensing Authority 서버의 이름을 확인할 수 있도록 DNS 서버를 구성합니다. DNS 서버 구성, 56 페이지 섹션을 참조하십시오.
- 디바이스의 클록을 설정합니다. 날짜 및 시간 설정, 33 페이지 섹션을 참조하십시오.

Smart Software Licensing의 기본값

Firepower 9300 기본 컨피그레이션은 Smart Call Home 프로파일인 "SLProf"를 포함하며, 여기에서 Licensing Authority의 URL을 지정합니다.

Smart Software Licensing 구성

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

절차

단계 **1** (선택 사항) HTTP 프록시 구성, 14 페이지.

단계 **2** License Authority를 통해 Firepower 9300 등록, 15 페이지.

(선택 사항) HTTP 프록시 구성

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

절차

단계 **1** **System**(시스템) > **Licensing**(라이센싱) > **Call Home**을 선택합니다.
Call Home 페이지는 License Authority의 대상 주소 URL 구성 및 HTTP 프록시 구성을 위한 필드를 제공합니다.

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

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

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

단계 **4** **Save(**저장**)**를 클릭합니다.

License Authority를 통해 Firepower 9300 등록

Firepower 9300를 등록하면 License Authority는 Firepower 9300와 License Authority 간 통신을 위한 ID 인증서를 발급합니다. 또한 Firepower 9300를 적절한 가상 계정에 할당합니다. 일반적으로 이 절차는 1회 수행됩니다. 그러나 예를 들어 통신 문제 때문에 ID 인증서가 만료되면 나중에 Firepower 9300를 다시 등록해야 할 수 있습니다.

절차

단계 **1** Smart Software Manager에서, 이 Firepower 9300를 추가할 가상 계정에 대한 등록 토큰을 요청 및 복사합니다.

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

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

단계 **4** **Register**를 클릭합니다.
Firepower 새시에서 License Authority를 통한 등록을 시도합니다.

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

Firepower 9300의 등록을 취소하면 어카운트에서 해당 디바이스가 제거됩니다. 디바이스의 모든 라이센스 엔타이틀먼트 및 인증서가 제거됩니다. 새 Firepower 9300의 라이센스를 위해 공간을 비워두려면 등록을 취소할 수 있습니다. 또는 Smart Software Manager에서 해당 디바이스를 제거할 수 있습니다.

Smart Software Licensing 기록

기능 이름	플랫폼 릴리스	설명
Firepower 9300용 Cisco Smart Software Licensing	1.1(1)	Smart Software Licensing은 라이센스 풀을 구입하고 관리하게 해줍니다. 스마트 라이센스는 특정 일련 번호에 연결되지 않습니다. 각 유닛의 라이센스 키를 관리할 필요 없이 손쉽게 디바이스를 구축하거나 사용 중단할 수 있습니다. Smart Software Licensing은 라이센스 사용량과 수요를 한 번에 확인하게 해줍니다. Smart Software Licensing 컨피그레이션은 Firepower 9300 관리자(Supervisor)와 보안 모듈로 나뉩니다. 추가된 화면: **System(**시스템**)** > **Licensing(**라이센싱**)** > **Call Home** **System(**시스템**)** > **Licensing(**라이센싱**)** > **Smart License(**스마트 라이센스**)**

4 장

사용자 관리

- 사용자 계정, 17 페이지
- 기본 사용자 역할, 19 페이지
- 로컬에서 인증된 사용자용 비밀번호 프로필, 19 페이지
- 사용자 설정 구성, 21 페이지
- 로컬 사용자 계정 생성, 24 페이지
- 로컬 사용자 어카운트 삭제, 26 페이지
- 로컬 사용자 어카운트 활성화 또는 비활성화, 27 페이지

사용자 계정

사용자 어카운트는 시스템에 액세스하는 데 사용됩니다. 로컬 사용자 어카운트를 최대 48개 구성할 수 있습니다. 각 사용자 어카운트에는 고유한 사용자 이름 및 비밀번호가 있어야 합니다.

관리자 어카운트

관리자 어카운트는 기본 사용자 어카운트이며 수정 또는 삭제할 수 없습니다. 이 어카운트는 시스템 관리자 또는 Superuser 어카운트이며 전체 권한을 가집니다. 관리자 어카운트에 할당된 기본 비밀번호가 없습니다. 초기 시스템 설정을 하는 동안 비밀번호를 선택해야 합니다.

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

로컬로 인증된 사용자 어카운트

로컬에서 인증된 사용자 어카운트는 섀시를 통해 직접 인증되며 관리자 또는 AAA 권한을 보유한 사용자에 의해 활성화 또는 비활성화될 수 있습니다. 로컬 사용자 어카운트를 비활성화한 경우, 사용자는 로그인할 수 없습니다. 비활성화된 로컬 사용자 어카운트에 대한 컨피그레이션 세부사항은 데이터베이스에서 삭제되지 않습니다. 비활성화된 로컬 사용자 어카운트를 다시 활성화하는 경우, 어카운트는 사용자 이름 및 비밀번호를 포함한 기존 컨피그레이션으로 다시 활성화됩니다.

원격으로 인증된 사용자 어카운트

원격으로 인증된 사용자 어카운트는 LDAP, RADIUS 또는 TACACS+를 통해 인증되는 사용자 어카운트입니다.

사용자가 로컬 사용자 어카운트와 원격 사용자 어카운트를 동시에 유지 관리할 경우, 로컬 사용자 어카운트에 정의된 역할은 원격 사용자 어카운트에서 유지 관리되는 역할을 재정의합니다.

사용자 어카운트 만료

사용자 어카운트는 미리 정의된 시간에 만료되도록 구성할 수 있습니다. 만료 시간에 도달하면 사용자 어카운트는 비활성화됩니다.

기본적으로, 사용자 어카운트는 만료되지 않습니다.

만료일이 있는 사용자 계정을 구성한 후에는 이 계정을 만료되지 않도록 재구성할 수 없습니다. 단, 사용 가능한 최신 만료일의 계정을 구성할 수 있습니다.

사용자 이름에 대한 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 1자에서 32자로 다음을 포함할 수 있습니다.
  - 알파벳 문자
  - 숫자
  - _(밑줄)
  - -(대시)
  - . (점)
- 로그인 ID는 고유해야 합니다.
- 로그인 ID는 알파벳 문자로 시작해야 합니다. 숫자 또는 밑줄과 같은 특수 문자로 시작할 수 없습니다.
- 로그인 ID는 대/소문자를 구분합니다.
- 모두 숫자인 로그인 ID를 생성할 수 없습니다.
- 사용자 계정을 생성한 후, 로그인 ID를 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 생성해야 합니다.

비밀번호에 대한 지침

비밀번호는 각각의 로컬에서 인증된 사용자 어카운트에 필요합니다. 관리자 또는 AAA 권한이 있는 사용자는 사용자 비밀번호에 대한 비밀번호 보안 수준을 확인하도록 시스템을 구성할 수 있습니다. 비밀번호 보안 수준 확인이 활성화된 경우 사용자는 강력한 비밀번호를 설정해야 합니다.

각 사용자별로 강력한 비밀번호를 사용할 것을 권장합니다. 로컬에서 인증된 사용자를 위해 비밀번호 보안 수준 확인을 활성화한 경우, Firepower eXtensible 운영 체제는 다음 요건을 충족하지 않는 비밀번호를 거부합니다.

- 최소 8자 이상, 최대 80자를 포함해야 합니다.
- 다음 중 최소 3가지 이상을 포함해야 합니다.
  - 소문자
  - 대문자
  - 숫자
  - 특수 문자
- 3번 이상 연속하여 반복되는 문자(예: aaabbb)는 포함할 수 없습니다.
- 3개의 연속 숫자(예: password123)를 포함할 수 없습니다.
- 사용자 이름 또는 사용자 이름을 반대로 한 이름과 동일하지 않아야 합니다.
- 비밀번호 딕셔너리 검사를 통과해야 합니다. 예를 들어, 비밀번호는 표준 사전 단어에 기반을 둘 수 없습니다.
- 다음 기호는 포함할 수 없습니다: $(달러 기호), ? (물음표) 및 =(같음 기호)
- 로컬 사용자 및 관리자 어카운트 비밀번호는 비어 있지 않아야 합니다.

기본 사용자 역할

시스템에는 다음과 같은 기본 사용자 역할이 포함됩니다.

Administrator

전체 시스템에 대한 완전한 읽기 및 쓰기 액세스가 가능합니다. 기본 관리자 계정이 기본적으로 이 역할에 할당되며 변경할 수 없습니다.

읽기 전용

시스템 상태를 수정할 권한이 없으며 시스템 컨피그레이션에 읽기 전용으로 액세스합니다.

로컬에서 인증된 사용자용 비밀번호 프로필

비밀번호 프로필에는 로컬에서 인증된 모든 사용자에 대한 비밀번호 기록 및 비밀번호 변경 간격 속성이 포함되어 있습니다. 각각의 로컬에서 인증된 사용자에 대해 다른 비밀번호 프로필을 지정할 수 없습니다.

비밀번호 기록 수

비밀번호 기록 수를 사용하면 로컬에서 인증된 사용자가 동일한 비밀번호를 계속해서 재사용하는 것을 방지할 수 있습니다. 이 속성을 구성할 때, Firepower 섀시는 로컬에서 인증된 사용자가 이전에 사용한 비밀번호를 최대 15개까지 저장합니다. 비밀번호는 최근 항목부터 시간순으로 저장되며, 기록 수 임계값에 도달할 경우 가장 오래된 비밀번호만 재사용될 수 있습니다.

사용자는 비밀번호를 재사용할 수 있기 전에 비밀번호 기록 수에 구성되어 있는 비밀번호 수를 생성하고 사용해야 합니다. 예를 들어, 비밀번호 기록 수를 8로 설정한 경우 로컬에서 인증된 사용자는 9번째 비밀번호가 만료될 때까지 첫 번째 비밀번호를 재사용할 수 없습니다.

기본적으로 비밀번호 기록은 0으로 설정되어 있습니다. 이 값이 설정되면 기록 수를 비활성화하고 사용자가 언제든지 이전의 비밀번호를 재사용할 수 있습니다.

필요한 경우, 로컬에서 인증된 사용자에 대한 비밀번호 기록 수를 지우고 이전 비밀번호 재사용을 활성화할 수 있습니다.

비밀번호 변경 간격

비밀번호 변경 간격을 사용하면 로컬에서 인증된 사용자가 지정된 시간 이내에 변경할 수 있는 비밀번호 변경 횟수를 제한할 수 있습니다. 다음 표는 비밀번호 변경 간격의 컨피그레이션 옵션 2개를 설명합니다.

간격 컨피그레이션	설명	예
비밀번호 변경 허용 안 됨	이 옵션을 사용하면 비밀번호 변경 이후 지정된 시간 동안에는 로컬에서 인증된 사용자의 비밀번호를 변경할 수 없습니다. 변경 안 함 간격을 1~745시간으로 지정할 수 있습니다. 기본적으로, 변경 안 함 간격은 24시간입니다.	예를 들어, 로컬에서 인증된 사용자가 비밀번호를 변경한 후 48시간 이내에 비밀번호가 변경되는 것을 방지하려면 다음을 설정하십시오. • 해당 간격 동안 변경을 비활성화로 설정 • 변경 안 함 간격을 48시간으로 설정
변경 간격 동안 허용되는 비밀번호 변경	이 옵션은 로컬에서 인증된 사용자의 비밀번호를 미리 정의한 간격 이내에 변경할 수 있는 최대 횟수를 지정합니다. 변경 간격을 1~745시간으로 지정하고 비밀번호 변경 최대 횟수를 0~10으로 지정할 수 있습니다. 기본적으로, 로컬에서 인증된 사용자에게는 48시간 간격 이내에 최대 2회의 비밀번호 변경이 허용됩니다.	예를 들어, 로컬에서 인증된 사용자가 비밀번호를 변경한 후 24시간 이내에 비밀번호를 최대 한 번 변경하도록 허용하려면 다음을 설정하십시오. • 해당 간격 동안 변경을 활성화로 설정 • 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.

이름	설명
Default Authentication(기본 인증**)** 필드	사용자가 원격 로그인 중에 인증되는 기본 방법입니다. 다음 중 하나일 수 있습니다. • **Local(**로컬**)** - 사용자 어카운트가 Firepower 섀시에서 로컬로 정의되어야 합니다. • **Radius** - 사용자 어카운트가 Firepower 섀시에 지정된 RADIUS 서버에서 정의되어야 합니다. • **TACACS** - 사용자 어카운트가 Firepower 섀시에 지정된 TACACS+ 서버에서 정의되어야 합니다. • **LDAP** - 사용자 어카운트가 Firepower 섀시에 지정된 LDAP/MS-AD 서버에서 정의되어야 합니다. • **None(**없음**)** - 사용자 어카운트가 Firepower 섀시에서 로컬인 경우, 사용자가 원격으로 로그인할 때 비밀번호가 필요하지 않습니다.
원격 사용자 설정	
원격 사용자 역할 정책	사용자가 로그인을 시도하고 원격 인증 제공자가 인증 정보와 함께 사용자 역할을 제공하지 않는 경우, 발생하는 결과를 제어합니다. • **Assign Default Role(**기본 역할 할당**)** - 사용자는 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	

이름	설명
Password Strength Check(비밀번호 보안 수준 확인**)** 확인란	이 확인란을 선택한 경우, 모든 로컬 사용자 비밀번호는 다음의 비밀번호 보안 요건을 준수해야 합니다. • 최소 8자 이상, 최대 80자를 포함해야 합니다. • 다음 중 최소 3가지 이상을 포함해야 합니다. ◦ 소문자 ◦ 대문자 ◦ 숫자 ◦ 특수 문자 • 3번 이상 연속하여 반복되는 문자(예: aaabbb)는 포함할 수 없습니다. • 3개의 연속 숫자(예: password123)를 포함할 수 없습니다. • 사용자 이름 또는 사용자 이름을 반대로 한 이름과 동일하지 않아야 합니다. • 비밀번호 딕셔너리 검사를 통과해야 합니다. 예를 들어, 비밀번호는 표준 사전 단어에 기반을 둘 수 없습니다. • 다음 기호는 포함할 수 없습니다: $(달러 기호), ? (물음표) 및 =(같음 기호) • 로컬 사용자 및 관리자 계정이 공란으로 비어 있지 않아야 합니다.
History Count(기록 수**)** 필드	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 재사용될 수 있습니다. 이 값은 0~15의 모든 수가 가능합니다. **History Count(**기록 수**)** 필드를 0으로 설정하여 기록 수를 비활성화하고 사용자가 언제든지 이전에 사용한 비밀번호를 재사용하게 할 수 있습니다.

이름	설명
Change During Interval(해당 간격 동안 변경**)** 필드	로컬에서 인증된 사용자가 비밀번호를 변경할 수 있는 시기를 제어합니다. 다음을 선택할 수 있습니다. • **Enable(**활성화**)** - 로컬에서 인증된 사용자는 변경 간격 및 변경 횟수에 대한 설정을 기초로 비밀번호를 변경할 수 있습니다. • **Disable(**비활성화**)** - 로컬에서 인증된 사용자는 변경 안 함 간격에 대해 지정된 시간 간격 동안 비밀번호를 변경할 수 없습니다.
Change Interval(변경 간격**)** 필드	**Change Count(**변경 횟수**)** 필드에 지정된 비밀번호 변경 횟수가 적용되는 시간입니다. 이 값은 1~745시간으로 선택할 수 있습니다. 예를 들어, 이 필드가 48로 설정되고 **Change Count(**변경 횟수**)** 필드가 2로 설정된 경우 로컬에서 인증된 사용자는 48시간 간격 이내에 최대 2번 비밀번호를 변경할 수 있습니다.
Change Count(변경 횟수**)** 필드	로컬에서 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	로컬에서 인증된 사용자가 새로 생성된 비밀번호를 변경하기 전에 대기해야 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.

로컬 사용자 계정 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** 사용자에 대한 필수 정보를 다음 필드에 입력합니다.

이름	설명
User Name(사용자 이름**)** 필드	계정에 로그인할 때 사용되는 계정 이름입니다. 이 계정은 고유해야 하며 사용자 계정에 대한 다음 지침 및 제한사항을 충족해야 합니다. • 로그인 ID는 1자에서 32자로 다음을 포함할 수 있습니다. ◦ 알파벳 문자 ◦ 숫자 ◦ _(밑줄) ◦ -(대시) ◦ . (점) • 로그인 ID는 고유해야 합니다. • 로그인 ID는 알파벳 문자로 시작해야 합니다. 숫자 또는 밑줄과 같은 특수 문자로 시작할 수 없습니다. • 로그인 ID는 대/소문자를 구분합니다. • 모두 숫자인 로그인 ID를 생성할 수 없습니다. • 사용자 계정을 생성한 후, 로그인 ID를 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 생성해야 합니다. 사용자를 저장한 후에는 로그인 ID를 변경할 수 없습니다. 사용자 계정을 삭제하고 새로 생성해야 합니다.
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.

이름	설명
Phone Number(전화 번호**)** 필드	사용자의 전화 번호입니다.
Password(비밀번호**)** 필드	이 계정과 연관된 비밀번호입니다. 비밀번호 보안 수준 확인을 활성화한 경우, 사용자의 비밀번호가 더욱 강력해지며 Firepower eXtensible 운영 체제은 다음 요건을 충족하지 않는 비밀번호를 거부합니다. • 최소 8자 이상, 최대 80자를 포함해야 합니다. • 다음 중 최소 3가지 이상을 포함해야 합니다. ◦ 소문자 ◦ 대문자 ◦ 숫자 ◦ 특수 문자 • 3번 이상 연속하여 반복되는 문자(예: aaabbb)는 포함할 수 없습니다. • 3개의 연속 숫자(예: password123)를 포함할 수 없습니다. • 사용자 이름 또는 사용자 이름을 반대로 한 이름과 동일하지 않아야 합니다. • 비밀번호 딕셔너리 검사를 통과해야 합니다. 예를 들어, 비밀번호는 표준 사전 단어에 기반을 둘 수 없습니다. • 다음 기호는 포함할 수 없습니다: $(달러 기호), ? (물음표) 및 =(같음 기호) • 로컬 사용자 및 관리자 계정이 공란으로 비어 있지 않아야 합니다.
Confirm Password(비밀번호 확인**)** 필드	확인을 위해 비밀번호를 다시 한 번 입력합니다.
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.

이름	설명
User Role(사용자 역할**)** 드롭다운 목록	사용자 계정에 할당할 수 있는 권한에 해당하는 역할입니다. 관리 전체 시스템에 대한 완전한 읽기 및 쓰기 액세스가 가능합니다. 기본 관리자 계정이 기본적으로 이 역할에 할당되며 변경할 수 없습니다. 읽기 전용 시스템 상태를 수정할 권한이 없으며 시스템 컨피그레이션에 읽기 전용으로 액세스합니다.
Account Expires(계정 만료**)** 확인란	이 확인란을 선택한 경우, 해당 계정은 만료되며 **Expiration Date(**만료 날짜**)** 필드에 지정된 날짜 이후에 사용할 수 없습니다. 참고 만료일이 있는 사용자 계정을 구성한 후에는 이 계정을 만료되지 않도록 재구성할 수 없습니다. 단, 최신 만료일이 있는 어카운트를 구성할 수 있습니다.
Expiry Date(만료일**)** 필드	계정이 만료되는 날짜입니다. 날짜는 yyyy-mm-dd 형식이어야 합니다. 만료일을 선택하기 위해 달력을 보려면 이 필드의 마지막에 있는 달력 아이콘을 클릭합니다.

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** 삭제하려는 사용자 어카운트 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** 활성화 또는 비활성화하려는 사용자 어카운트 행에서 **Edit(**편집**)(**연필 모양 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 어카운트는 항상 활성 상태로 설정됩니다. 수정은 불가능합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

5 장

이미지 관리

- 이미지 관리 정보, 29 페이지
- Cisco.com에서 이미지 다운로드, 30 페이지
- Firepower 어플라이언스에 이미지 업로드, 30 페이지
- Firepower eXtensible 운영 체제 플랫폼 번들 업그레이드, 31 페이지
- 논리적 디바이스를 위한 이미지 버전 업데이트, 31 페이지

이미지 관리 정보

Firepower 어플라이언스는 다음의 2가지 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 관리자(Supervisor) 및 Firepower 보안 모듈에서 작동하는 여러 개별 이미지가 모여 있는 컬렉션입니다. 플랫폼 번들은 Firepower eXtensible 운영 체제 소프트웨어 패키지입니다.
- 애플리케이션 - 애플리케이션 이미지는 Firepower 어플라이언스의 보안 모듈에 구축할 소프트웨어 이미지입니다. 애플리케이션 이미지는 CSP(Cisco Secure Package) 파일로 전송되고 논리적 디바이스를 생성하거나 이후 논리적 디바이스 생성에 대비하기 위해 보안 모듈에 구축될 때까지 관리자(Supervisor)에 저장됩니다. Firepower 수퍼바이저에 저장된 동일한 애플리케이션 이미지 유형의 여러 가지 다른 버전이 있을 수 있습니다.

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 섀시에서 사용 가능한 FXOS 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.

단계 **2** 페이지 하단에서 **Download latest updates from CCO(CCO**에서 최신 업데이트 다운로드**)** 링크를 클릭합니다.
Firepower 어플라이언스에 대한 소프트웨어 다운로드 페이지가 브라우저의 새 탭에 열립니다.

단계 **3** 적절한 소프트웨어 이미지를 찾은 다음 로컬 컴퓨터에 다운로드합니다.

Firepower 어플라이언스에 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 섀시에서 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 이동하고 업로드할 이미지를 찾습니다.

단계 **4** **Upload(**업로드**)**를 클릭합니다.
선택한 이미지는 Firepower 어플라이언스에 업로드됩니다.

단계 **5** 이미지를 업로드한 후에 특정 소프트웨어 이미지에 대한 최종 사용자 라이센스 계약이 표시됩니다. 시스템 프롬프트에 따라 최종 사용자 라이센스 계약에 동의합니다.

Firepower eXtensible 운영 체제 플랫폼 번들 업그레이드

시작하기 전에

Cisco.com에서 플랫폼 번들 소프트웨어 이미지를 다운로드(Cisco.com에서 이미지 다운로드, 30 페이지 참조)한 다음 해당 이미지를 Firepower 어플라이언스에 업로드합니다(Firepower 어플라이언스에 이미지 업로드, 30 페이지 참조).

절차

단계 **1** 콘솔 포트에 연결합니다.

단계 **2** 조직 모드를 입력합니다.
Firepower-chassis# **scopeorg**

단계 **3** 기본 플랫폼 팩 모드를 입력합니다.
Firepower-chassis /org # **scopefw-platform-packdefault**

단계 **4** 설치한 버전으로 기본 플랫폼 번들을 설정합니다.
Firepower-chassis /org/fw-platform-pack # **setplatform-bundle-version** *version_number*

*version_number*는 설치 중인 FXOS 플랫폼 번들의 버전 번호입니다.

단계 **5** 변경 사항을 커밋하고 업그레이드 프로세스를 시작합니다.
commit-buffer

Firepower eXtensible 운영 체제에서는 번들의 압축을 풀고 구성 요소를 업그레이드하거나 다시 로드합니다.

단계 **6** 업그레이드 프로세스를 모니터링하려면 다음과 같이 합니다.

a) **scopefirmware**를 입력합니다.
b) **scopeauto-install**을 입력합니다.
c) **showfsmstatusexpand**를 입력합니다.

논리적 디바이스를 위한 이미지 버전 업데이트

시작하기 전에

Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드(Cisco.com에서 이미지 다운로드, 30 페이지 참고)한 다음 해당 이미지를 Firepower 어플라이언스에 업로드합니다(Firepower 어플라이언스에 이미지 업로드, 30 페이지 참고).

참고 Firepower Threat Defense 논리적 디바이스를 직접 업그레이드할 수는 없습니다. Firepower Threat Defense 논리적 디바이스를 업그레이드하려면 기존 디바이스를 삭제한 다음 업데이트된 이미지를 사용하여 새 디바이스를 생성해야 합니다.

절차

단계 **1** **Logical Devices(**논리적 디바이스**)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다. Logical Devices(논리적 디바이스) 페이지는 섀시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.

단계 **2** 업데이트하려는 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.

6 장

플랫폼 설정

- 날짜 및 시간 설정, 33 페이지
- SSH 구성, 34 페이지
- 텔넷 구성, 35 페이지
- SNMP 구성, 36 페이지
- HTTPS 포트 변경, 43 페이지
- AAA 구성, 43 페이지
- Syslog 구성, 53 페이지
- DNS 서버 구성, 56 페이지

날짜 및 시간 설정

NTP 페이지의 으로 날짜 및 시간을 수동으로 설정하거나 NTP 서버를 구성합니다. 섀시에 대해 구성된 시간 및 표준 시간대는 논리적 디바이스를 포함하여 섀시 내 다른 구성 요소와 동기화됩니다.

NTP 서버를 사용하여 날짜 및 시간 설정

NTP는 네트워크 시스템 간에 정확하게 동기화된 시간을 제공하는 계층적 서버 시스템을 구현하는 데 사용합니다. 정밀한 타임 스탬프가 포함된 CRL 검증과 같이 시간에 민감한 작업에는 이러한 정확성이 필요합니다.

절차

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

단계 **2** **Time Zone(**표준 시간대**)** 드롭다운 목록에서 Firepower 섀시에 적절한 표준 시간대를 선택합니다.

단계 **3** **Set Time Source(**시간 소스 설정**)**에서 **Use NTP Server(NTP** 서버 사용**)**를 클릭한 다음 **NTP Server(NTP** 서버**)** 필드에서 사용할 NTP 서버의 IP 주소 또는 호스트 이름을 입력합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.
Firepower 섀시는 NTP 서버가 지정된 상태로 구성됩니다.

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

날짜 및 시간 직접 설정

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

절차

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

단계 **2** **Time Zone(**표준 시간대**)** 드롭다운 목록에서 Firepower 섀시에 적절한 표준 시간대를 선택합니다.

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 통해 날짜를 설정합니다.

단계 **5** 해당하는 드롭다운 목록을 사용하여 시간을 시, 분 및 AM/PM으로 지정합니다.

팁 **Get System Time(**시스템 시간 가져오기**)**을 클릭하여 Firepower Chassis Manager 연결에 사용 중인 시스템에 구성되어 있는 날짜 및 시간과 일치하도록 날짜 및 시간을 설정할 수 있습니다.

단계 **6** **Save(**저장**)**를 클릭합니다.
Firepower 섀시는 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 섀시에 대한 SSH 액세스를 활성화하거나 비활성화하는 방법을 설명합니다. SSH는 기본적으로 활성화되어 있습니다.

절차

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

단계 **2** Firepower 섀시에 대한 SSH 액세스를 활성화하려면 **Enable SSH(SSH** 활성화**)** 확인란을 선택합니다. SSH 액세스를 비활성화하려면 **Enable SSH(SSH** 활성화**)** 확인란의 선택을 취소합니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

텔넷 구성

다음 절차에서는 Firepower 섀시에 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 입력합니다.
Firepower-chassis #**scope system**

단계 **2** 시스템 서비스 모드를 입력합니다.
Firepower-chassis /system #**scope services**

단계 **3** Firepower 섀시에 대한 텔넷 액세스를 구성하려면 다음 중 하나를 수행합니다.

- Firepower 섀시에 대한 텔넷 액세스를 허용하려면 다음 명령을 입력합니다.

  Firepower-chassis /system/services # **enable telnet-server**

- Firepower 섀시에 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 섀시에 SNMP(Simple Network Management Protocol)를 구성할 수 있습니다. 자세한 내용은 다음 항목을 참조하십시오.

SNMP 소개

SNMP(Simple Network Management Protocol)는 SNMP 관리자 및 에이전트 간 통신에 메시지 형식을 제공하는 애플리케이션 레이어 프로토콜입니다. SNMP는 네트워크에 있는 디바이스의 모니터링 및 관리에 사용되는 표준화된 프레임워크 및 공통 언어를 제공합니다.

SNMP 프레임워크는 다음 3가지 항목으로 구성됩니다.

- SNMP 관리자 - SNMP를 사용하여 네트워크 디바이스 활동을 제어하고 모니터링하는 데 사용되는 시스템입니다.
- 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. SNMP 에이전트를 활성화하고 관리자 및 에이전트 간 관계를 생성하려면 Firepower Chassis Manager 또는 FXOS CLI에서 SNMP를 활성화하고 구성합니다.
- MIB(Managed Information Base) - SNMP 에이전트에 있는 관리 객체가 모여 있는 컬렉션입니다.

Firepower 섀시는 SNMPv1, SNMPv2c 및 SNMPv3를 지원합니다. SNMPv1 및 SNMPv2c는 모두 보안 커뮤니티 기반 양식을 사용합니다. SNMP는 다음에 정의되어 있습니다.

- 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 알림

SNMP의 주요 기능은 SNMP 에이전트에서 알림을 생성하는 기능입니다. 이러한 알림에는 SNMP 관리자가 요청을 전송하지 않아도 됩니다. 알림은 잘못된 사용자 인증, 재시작, 연결 종료, 네이버 라우터에 대한 연결 손실 또는 기타 중요한 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. 알림 요청을 수신하는 SNMP 관리자는 SNMP 응답 PDU(Protocol Data Unit)가 있는 메시지를 승인합니다. Firepower 섀시가 PDU를 수신하지 못하는 경우 알림 요청을 다시 전송할 수 있습니다.

SNMP 보안 수준 및 권한

SNMPv1, SNMPv2c 및 SNMPv3는 각각 다른 보안 모델을 나타냅니다. 보안 모델은 선택한 보안 수준과 결합하여 SNMP 메시지를 처리할 때 적용된 보안 메커니즘을 결정합니다.

보안 수준은 SNMP 트랩에 연결된 메시지를 표시하는 데 필요한 권한을 결정합니다. 권한 수준은 메시지가 공개되지 않도록 보호해야 하는지 또는 인증되어야 하는지를 결정합니다. 어떤 보안 모델이 구현되는지에 따라 지원되는 보안 수준이 달라집니다. SNMP 보안 수준은 다음 권한 중 하나 이상을 지원합니다.

- noAuthNoPriv - 인증 또는 암호화 없음
- authNoPriv - 인증하지만 암호화 없음
- authPriv - 인증 및 암호화

SNMPv3는 보안 모델 및 보안 수준을 모두 제공합니다. 보안 모델은 사용자 및 사용자 역할을 위해 설정된 인증 전략입니다. 보안 수준은 보안 모델 내에서 허용된 보안의 수준입니다. 보안 모델과 보안 수준을 결합하여 SNMP 패킷을 처리할 때 어떤 보안 메커니즘이 적용되는지 결정합니다.

지원되는 SNMP 보안 모델과 수준 결합

다음 표에서는 어떻게 보안 모델과 수준을 결합할 수 있는지에 대해 설명합니다.

표 *1: SNMP* 보안 모델과 수준

모델	수준기	인증	암호화	동작
v1	noAuthNoPriv	커뮤니티 문자열	아니요	인증에 커뮤니티 문자열 일치를 사용합니다.

모델	수준기	인증	암호화	동작
v2c	noAuthNoPriv	커뮤니티 문자열	아니요	인증에 커뮤니티 문자열 일치를 사용합니다.
v3	noAuthNoPriv	Username	아니요	인증에 사용자 이름 일치를 사용합니다.
v3	authNoPriv	HMAC-SHA	아니요	HMAC SHA(Secure Hash Algorithm) 기반 인증을 제공합니다.
v3	authPriv	HMAC-SHA	DES	HMAC-SHA 알고리즘 기반 인증을 제공합니다. CBC(Cipher Block Chaining) DES(DES-56) 표준 기반 인증 외에 DES(데이터 암호화 표준) 56비트 암호화를 제공합니다.

SNMPv3 보안 기능

SNMPv3는 네트워크에서 인증 및 암호화 프레임을 결합하여 디바이스에 대한 보안 액세스를 제공합니다. SNMPv3는 구성된 사용자가 수행하는 관리 작업에만 권한을 부여하고 SNMP 메시지를 암호화합니다. SNMPv3 USM(User-Based Security Model)은 SNMP 메시지 수준 보안을 참조하며 다음 서비스를 제공합니다.

- 메시지 무결성 - 메시지가 무단으로 변경 또는 손상되지 않았으며 데이터 시퀀스가 악의 없이 수행된 변경보다 적게 변경되었음을 보장합니다.
- 메시지 출처 인증 - 수신한 데이터의 출처를 대신하는 사용자의 요청된 ID가 확인되었음을 보장합니다.
- 메시지 기밀성 및 암호화 - 권한 없는 개인, 엔터티 또는 프로세스에서 정보를 사용할 수 없거나 정보를 공개하지 않았음을 보장합니다.

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 사용자의 AES 프라이버시 프로토콜

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

프라이버시 비밀번호 또는 priv 옵션은 SNMP 보안 암호화를 위해 DES 또는 128비트 AES 암호화를 제공합니다. AES-128 컨피그레이션을 활성화하고 SNMPv3 사용자에 대한 프라이버시 비밀번호가 있는 경우, Firepower 섀시는 해당 프라이버시 비밀번호를 사용하여 128비트 AES 키를 생성합니다. AES 프라이버시 비밀번호에는 최소 8자 이상을 포함할 수 있습니다. 암호가 일반 텍스트로 지정된 경우, 최대 64자를 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.

이름	설명
Admin State(관리 상태**)** 확인란	SNMP 활성화 또는 비활성화 여부. 시스템에 SNMP 서버와의 통합이 포함되는 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. 영숫자 문자열은 1자~32자로 입력합니다. @(at 기호), \(백슬래시), "(큰따옴표), ? (물음표) 또는 공백을 사용하지 마십시오. 기본값은 public입니다.

이름	설명
System Administrator Name(시스템 관리자 이름**)** 필드	SNMP 구현을 책임지는 담당자입니다. 이메일 주소 또는 이름과 전화번호로, 최대 255자의 문자열을 입력합니다.
Location(위치**)** 필드	SNMP 에이전트(서버)가 실행되는 호스트의 위치. 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 작성합니다.

이름	설명
Host Name(호스트 이름**)** 필드	Firepower 섀시가 트랩을 전송해야 하는 SNMP 호스트의 호스트 이름 또는 IP 주소입니다.
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. 이것은 SNMP 서비스를 위해 구성된 커뮤니티 또는 사용자 이름과 동일해야 합니다. 영숫자 문자열은 1자~32자로 입력합니다. @(at 기호), \(백슬래시), "(큰따옴표), ? (물음표) 또는 공백을 사용하지 마십시오.
Port(포트**)** 필드	Firepower 섀시가 트랩을 위해 SNMP 호스트와 통신하는 포트입니다. 1~65535의 정수를 입력합니다.

이름	설명
Version(버전**)** 필드	트랩에 사용되는 SNMP 버전 및 모델입니다. 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	버전을 **V3**로 선택한 경우 권한이 트랩과 연결되어 있습니다. 다음 중 하나일 수 있습니다. • **Auth** - 인증하지만 암호화 없음 • **Noauth** - 인증 또는 암호화 없음 • **Priv** - 인증 및 암호화

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 작성합니다.

이름	설명
Name(이름**)** 필드	SNMP 사용자에게 할당된 사용자 이름입니다. 최대 32개의 문자 또는 숫자를 입력합니다. 이름은 문자로 시작해야 하며 _(밑줄), . (마침표), @(at 기호) 및 -(하이픈)을 지정할 수 있습니다.
Auth Type(권한 부여 유형**)** 필드	권한 부여 유형: **SHA**.
Use AES-128(AES-128 사용**)** 확인란	이 확인란을 선택한 경우, 해당 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(비공개 비밀번호**)** 필드	이 사용자의 프라이버시 비밀번호입니다.
Confirm Privacy Password(프라이버시 비밀번호 확인**)** 필드	확인을 위해 다시 한 번 입력하는 프라이버시 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 사용자에 해당하는 테이블의 행에 있는 **Delete(**삭제**)** 아이콘을 클릭합니다.

HTTPS 포트 변경

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

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.

AAA 구성

이 섹션에서는 인증, 권한 부여 및 어카운팅에 관해 설명합니다. 자세한 내용은 다음 항목을 참조하십시오.

AAA 정보

AAA는 컴퓨터 리소스에 대한 액세스 제어를 위한 서비스 집합으로, 정책을 구현하고 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 섀시에 대한 관리 연결을 인증하도록 Firepower 어플라이언스를 구성할 수 있습니다.

- HTTPS
- SSH
- 시리얼 콘솔

승인

승인은 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.

회계

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 승인 제어, 청구, 경향 분석, 리소스 활용도 및 용량 계획 활동에 사용됩니다.

인증, 권한 검증 및 과금 간 상호 작용

인증을 단독으로 사용하거나 권한 부여 및 어카운팅과 함께 사용할 수 있습니다. 인증은 항상 사용자를 먼저 확인해야 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. 인증은 사용자가 액세스할 수 있는 리소스와 서비스를 결정하는 정책을 구현합니다. 어카운팅은 청구 및 분석을 위해 사용되는 시간과 데이터를 추적합니다.

로컬 데이터베이스 지원

Firepower 섀시는 사용자가 사용자 프로파일을 채울 수 있는 로컬 데이터베이스를 유지합니다. 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 어카운트를 생성하여 Firepower eXtensible 운영 체제와 바인딩합니다. 이 어카운트는 비밀번호가 만료되지 않는 어카운트여야 합니다.

절차

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

단계 **2** **LDAP** 탭을 클릭합니다.

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

이름	설명
Timeout(시간 초과**)** 필드	시간이 초과되기 전에 시스템이 LDAP 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다. 1~60초의 정수를 입력합니다. 기본값은 30입니다. 이 속성은 필수 항목입니다.
Attribute(특성**)** 필드	사용자 역할 및 로캘에 대한 값을 저장하는 LDAP 특성입니다. 이 속성은 항상 이름값 쌍입니다. 시스템은 이 특성 이름과 일치하는 값에 대해 사용자 레코드를 쿼리합니다.
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 문자 수로 설정될 수 있습니다. 이때 $userid는 LDAP 인증을 사용하여 Firepower 섀시에 액세스를 시도하는 원격 사용자를 식별합니다. 이 속성은 필수 항목입니다. 이 탭에서 기본 DN을 지정하지 않으면 정의하는 각 LDAP 제공자에 하나를 지정해야 합니다.

이름	설명
Filter(필터**)** 필드	LDAP 검색은 정의된 필터와 일치하는 사용자 이름으로 제한됩니다. 이 속성은 필수 항목입니다. 이 탭에서 필터를 지정하지 않으면 정의하는 각 LDAP 제공자에 하나를 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 어카운트를 생성하여 Firepower eXtensible 운영 체제와 바인딩합니다. 이 어카운트는 비밀번호가 만료되지 않는 어카운트여야 합니다.

절차

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

이름	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(Common Name)과 정확하게 일치해야 합니다.

이름	설명
Order(순서**)** 필드	Firepower eXtensible 운영 체제에서 사용자를 인증하기 위해 이 제공자를 사용하는 순서입니다. Firepower eXtensible 운영 체제에서 Firepower Chassis Manager 또는 FXOS CLI에 정의되어 있는 다른 제공자를 기반으로 사용 가능한 다음 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 고유 이름(DN)입니다. 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 문자 수로 설정될 수 있습니다. 이때 $userid는 LDAP 인증을 사용하여 Firepower Chassis Manager 또는 FXOS CLI에 액세스를 시도하는 원격 사용자를 식별합니다. 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.
SSL 사용 확인란	이 확인란을 선택한 경우, LDAP 데이터베이스와의 통신에 암호화가 필요합니다. 이 확인란이 선택되지 않은 경우, 인증 정보는 암호화되지 않은 텍스트로 전송됩니다. LDAP는 STARTTLS를 사용합니다. 이렇게 하면 포트 389를 사용한 암호화된 통신이 가능합니다.
Filter(필터**)** 필드	LDAP 검색은 정의된 필터와 일치하는 사용자 이름으로 제한됩니다. 이 값은 기본 필터가 **LDAP** 탭에 설정되지 않은 경우 필요합니다.
Attribute(특성**)** 필드	사용자 역할 및 로캘에 대한 값을 저장하는 LDAP 특성입니다. 이 속성은 항상 이름값 쌍입니다. 시스템은 이 특성 이름과 일치하는 값에 대해 사용자 레코드를 쿼리합니다. 이 값은 기본 특성이 **LDAP** 탭에 설정되지 않은 경우 필요합니다.

이름	설명
Key(키**)** 필드	**Bind DN(**바인드 **DN)** 필드에 지정된 LDAP 데이터베이스 어카운트의 비밀번호입니다. 공백, §(섹션 기호), ?(물음표) 또는 =(등호)를 제외한 모든 표준 ASCII 문자를 입력할 수 있습니다.
Confirm Key(키 확인**)** 필드	확인을 위해 반복되는 LDAP 데이터베이스 비밀번호입니다.
Timeout(시간 초과**)** 필드	시간이 초과되기 전에 시스템이 LDAP 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다. 1~60초의 정수를 입력하거나 0(숫자 0)을 입력하여 **LDAP** 탭에 지정된 전역 시간 초과 값을 사용합니다. 기본값은 30초입니다.
Vendor(벤더**)** 필드	이 선택사항으로 LDAP 제공자 또는 서버 상세 정보를 제공하는 벤더를 식별합니다. • LDAP 제공자가 Microsoft Active Directory인 경우, **MS AD**를 선택합니다. • LDAP 제공자가 Microsoft Active Directory가 아닌 경우, **Open LDAP(LDAP** 열기**)**를 선택합니다. 기본값은 **Open LDAP(LDAP** 열기**)**입니다.

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

단계 **4** **Save(**저장**)**를 클릭합니다.

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.

이름	설명
Timeout(시간 초과**)** 필드	시간이 초과되기 전에 시스템이 RADIUS 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다. 1~60초의 정수를 입력합니다. 기본값은 5초입니다. 이 속성은 필수 항목입니다.
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 체제에서는 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.

a) **RADIUS Providers(RADIUS** 제공자**)** 영역에서 **Add(**추가**)**를 클릭합니다.

b) **Add RADIUS Provider(RADIUS** 제공자 추가**)** 대화 상자에서 다음 필드를 작성합니다.

이름	설명
Hostname/FDQN (or IP Address)(호스트 이름**/FDQN(**또는 **IP** 주소**))** 필드	RADIUS 제공자가 있는 호스트 이름 또는 IP 주소입니다.
Order(순서**)** 필드	Firepower eXtensible 운영 체제에서 사용자를 인증하기 위해 이 제공자를 사용하는 순서입니다. Firepower eXtensible 운영 체제에서 Firepower Chassis Manager 또는 FXOS CLI에 정의되어 있는 다른 제공자를 기반으로 사용 가능한 다음 순서를 할당하려면 1~16의 정수를 입력하거나 lowest-available 또는 0(숫자 0)을 입력합니다.
Key(키**)** 필드	데이터베이스에 대한 SSL 암호화 키입니다.
Confirm Key(키 확인**)** 필드	확인을 위해 다시 한 번 입력하는 SSL 암호화 키입니다.
Authorization Port(권한 부여 포트**)** 필드	Firepower Chassis Manager 또는 FXOS CLI에서 RADIUS 데이터베이스와 통신할 때 사용하는 포트입니다. 범위는 1에서 65535까지입니다. 표준 포트 번호는 1700입니다.
Timeout(시간 초과**)** 필드	시간이 초과되기 전에 시스템이 RADIUS 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다. 1~60초의 정수를 입력하거나 0(숫자 0)을 입력하여 **RADIUS** 탭에 지정된 전역 시간 초과 값을 사용합니다. 기본값은 5일입니다.
Retries(재시도 횟수**)** 필드	요청에 실패한 것으로 간주하기 전에 연결을 재시도할 횟수입니다. 필요 시 0~5의 정수를 입력합니다. 값을 지정하지 않은 경우, Firepower Chassis Manager에서는 **RADIUS** 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.

이름	설명
Timeout(시간 초과**)** 필드	시간이 초과되기 전에 시스템이 TACACS+ 데이터베이스에 연결을 시도하는 데 필요한 시간(초) 길이입니다. 1~60초의 정수를 입력합니다. 기본값은 5초입니다. 이 속성은 필수 항목입니다.

단계 4 **Save(**저장**)**를 클릭합니다.

다음에 할 작업

TACACS+ 제공자를 생성합니다.

TACACS+ 제공자 생성

Firepower eXtensible 운영 체제에서는 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 작성합니다.

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

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 로깅하면 로그와 경고를 종합하는 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.

이름	설명
Console(콘솔**)** 섹션	
Admin State(관리 상태**)** 필드	Firepower 새시가 콘솔에 syslog 메시지를 표시하는지 여부. 콘솔에 syslog 메시지를 표시하고 로그에 추가하려는 경우 **Enable(**활성화**)** 확인란을 선택합니다. **Enable(**활성화**)** 확인란이 선택되지 않은 경우, syslog 메시지는 로그에 추가되지만 콘솔에 표시되지 않습니다.

이름	설명
Level(수준**)** 필드	**Console - Admin State(**콘솔 **-** 관리 상태**)**의 **Enable(**활성화**)** 확인란을 선택한 경우, 콘솔에 표시할 가장 낮은 메시지 수준을 선택합니다. Firepower 섀시는 콘솔에 해당 수준 이상의 메시지를 표시합니다. 다음 중 하나일 수 있습니다. • 긴급 상황 • **Alerts(**경고문**)** • 중대
Monitor(모니터**)** 섹션	
Admin State(관리 상태**)** 필드	Firepower 섀시가 모니터에 syslog 메시지를 표시하는지 여부. 모니터에 syslog 메시지를 표시하고 로그에 추가하려는 경우 **Enable(**활성화**)** 확인란을 선택합니다. **Enable(**활성화**)** 확인란이 선택되지 않은 경우, syslog 메시지는 로그에 추가되지만 모니터에 표시되지 않습니다.
Level(수준**)** 드롭다운 목록	**Monitor - Admin State(**모니터 **-** 관리 상태**)**의 **Enable(**활성화**)** 확인란을 선택한 경우, 모니터에 표시할 가장 낮은 메시지 수준을 선택합니다. Firepower 섀시는 모니터에 해당 수준 이상의 메시지를 표시합니다. 다음 중 하나일 수 있습니다. • **Emergencies(**긴급 상황**)** • **Alerts(**경고문**)** • **Critical(**중대**)** • **Errors(**오류**)** • **Warnings(**경고**)** • **Notifications(**알림**)** • **Information(**정보**)** • **Debugging(**디버깅**)**

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
Admin State(관리 상태**)** 필드	원격 로그 파일에 syslog 메시지를 저장하려는 경우 **Enable(**활성화**)** 확인란을 선택합니다.
Level(수준**)** 드롭다운 목록	시스템에서 저장할 가장 낮은 메시지 수준을 선택합니다. 시스템은 원격 파일에 해당 수준 이상의 메시지를 저장합니다. 다음 중 하나일 수 있습니다. • **Emergencies(**긴급 상황**)** • **Alerts(**경고문**)** • **Critical(**중대**)** • **Errors(**오류**)** • **Warnings(**경고**)** • **Notifications(**알림**)** • **Information(**정보**)** • **Debugging(**디버깅**)**
Hostname/IP Address(호스트 이름**/IP** 주소**)** 필드	원격 로그 파일이 있는 호스트 이름 또는 IP 주소입니다. 참고 IP 주소 대신 호스트 이름을 사용하는 경우 DNS 서버를 구성해야 합니다.
Facility(기능**)** 드롭다운 목록	파일 메시지의 기반으로 사용할 syslog 서버에 대한 시스템 로그를 선택합니다. 다음 중 하나일 수 있습니다. • **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) **Local Sources(**로컬 소스**)** 탭에서 다음 필드를 입력합니다.

이름	설명
Faults Admin State(결함 관리 상태**)** 필드	시스템 결함 로깅의 활성화 여부. **Enable(**활성화**)** 확인란을 선택한 경우 Firepower 섀시가 모든 시스템 결함을 로깅합니다.
Audits Admin State(감사 관리 상태**)** 필드	감사 로깅의 활성화 여부. **Enable(**활성화**)** 확인란을 선택한 경우 Firepower 섀시가 모든 감사 로그 이벤트를 로깅합니다.
Events Admin State(이벤트 관리 상태**)** 필드	시스템 이벤트 로깅의 활성화 여부. **Enable(**활성화**)** 확인란을 선택한 경우 Firepower 섀시가 모든 시스템 이벤트를 로깅합니다.

c) **Save(**저장**)**를 클릭합니다.

DNS 서버 구성

시스템에서 호스트가 IP 주소로 분석 해야하는 경우 DNS 서버를 지정해야 합니다. 예를 들어 DNS 서버를 구성하지 않으면 Firepower 섀시에서 설정을 구성할 때 www.cisco.com 등의 이름을 사용할 수 없습니다. IPv4 또는 IPv6 주소 중 하나로 서버의 IP 주소를 사용해야 합니다. 최대 4개까지 DNS 서버를 구성할 수 있습니다.

참고 여러 DNS 서버를 구성할 때 시스템은 임의 순서로 해당 서버만 검색합니다. 로컬 관리 명령에 DNS 서버 조회가 필요한 경우, 임의 순서로 DNS 서버 3개만 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** 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.

7 장

인터페이스 관리

- Firepower 9300 인터페이스 정보, 57 페이지
- 인터페이스 속성 편집, 58 페이지
- 인터페이스의 관리 상태 변경, 58 페이지
- 포트 채널 생성, 59 페이지
- 분할 케이블 구성, 60 페이지

Firepower 9300 인터페이스 정보

Firepower Chassis Manager의 인터페이스 페이지에서 섀시에 설치된 인터페이스의 상태를 확인하고 인터페이스 속성을 편집하며 인터페이스를 활성화 또는 비활성화하고 포트 채널을 생성할 수 있습니다.

인터페이스 페이지는 다음의 두 가지 섹션으로 구성됩니다.

- 상위 섹션에서는 Firepower 섀시에 설치된 인터페이스를 시각적으로 표시합니다. 인터페이스에 마우스 커서를 대면 해당 인터페이스에 대한 자세한 정보를 얻을 수 있습니다.

  인터페이스에는 현재 상태를 표시하는 다음과 같은 색상 코드가 지정됩니다.

  - 녹색 - 인터페이스가 설치 및 활성화된 상태입니다.
  - 어두운 회색 - 인터페이스가 설치되었지만 비활성화된 상태입니다.
  - 노란색 - 인터페이스의 작동 상태에 문제가 있습니다.
  - 밝은 회색 - 인터페이스가 설치되지 않았습니다.

- 하위 섹션에는 Firepower 섀시에 설치된 인터페이스 테이블이 있습니다. 인터페이스마다 활성화하거나 비활성화할 수 있습니다. 또한 **Edit(**편집**)**을 클릭하면 속도 및 인터페이스 유형 등 인터페이스 속성을 편집할 수 있습니다.

Firepower 9300는 단일 인터페이스뿐만 아니라 EtherChannel(port-channel) 인터페이스도 지원합니다. EtherChannel 인터페이스는 동일한 유형의 멤버 인터페이스를 최대 16개까지 포함할 수 있습니다.

각 인터페이스는 다음 유형 중 하나일 수 있습니다.

- 데이터(기본값) -- 데이터 인터페이스는 보안 모듈 간에 공유할 수 없습니다.
- 관리 -- 보안 모듈 간에 관리 인터페이스를 공유할 수 있습니다. 논리적 디바이스당 관리 인터페이스 1개만 할당할 수 있습니다.
- 클러스터 -- 클러스터된 논리적 디바이스에 사용되는 특수 인터페이스 유형입니다. 이 유형은 유닛 클러스터 간 통신을 지원하는 클러스터 제어 링크에 자동으로 할당됩니다. 기본적으로 클러스터 제어 링크는 Port-channel 48에서 자동으로 생성됩니다. 클러스터 제어 링크에 다른 포트 채널을 사용하려는 경우, 클러스터를 구축하기 전에 클러스터 유형을 다른 포트 채널에 할당할 수 있습니다.

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

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

단계 **4** (선택 사항) 이 인터페이스를 데이터 인터페이스로 구성하려면 **Data(**데이터**)** 라디오 버튼을 클릭하고, 관리 인터페이스로 구성하려면 **Management(**관리**)** 라디오 버튼을 클릭합니다.

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

  인터페이스의 관리 상태가 활성화로 변경됩니다. 해당 인터페이스의 시각적 표시가 회색에서 녹색으로 변경됩니다.

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

  인터페이스의 관리 상태가 비활성화로 변경됩니다. 해당 인터페이스의 시각적 표시가 녹색에서 회색으로 변경됩니다.

포트 채널 생성

EtherChannel(port-channel)은 동일한 유형의 멤버 인터페이스를 최대 16개까지 포함할 수 있습니다.

시작하기 전에

Firepower 어플라이언스에서는 활성 LACP(Link Aggregation Control Protocol) 모드에서 EtherChannel만 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.
Port-channel 48은 클러스터된 논리적 디바이스를 구축할 때 클러스터 제어 링크로 예약됩니다. 클러스터 제어 링크에 Port-channel 48을 사용하지 않으려면 다른 ID로 EtherChannel을 구성하고 인터페이스의 클러스터 유형을 선택할 수 있습니다. 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** 인터페이스를 포트 채널에 추가하려면 **Available Interface(**사용 가능한 인터페이스**)** 목록에서 인터페이스를 선택하고 **Add Interface(**인터페이스 추가**)**를 클릭하여 Member ID(멤버 ID) 목록으로 해당 인터페이스를 이동합니다. 동일한 유형과 속도를 가진 인터페이스는 최대 16개까지 추가할 수 있습니다.

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 **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.

분할 케이블 구성

다음 절차에서는 Firepower 섀시에서 사용할 분할 케이블을 구성하는 방법을 보여줍니다. 분할 케이블을 사용하여 40Gbps 포트 1개 대신 10Gbps 포트 4개를 제공할 수 있습니다.

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.

분할 케이블을 지원할 수 있지만 현재 구성되어 있지 않은 인터페이스는 해당 인터페이스 행에 분할 포트 아이콘으로 표시되어 있습니다. 분할 케이블을 사용하도록 구성된 인터페이스의 경우, 개별 분할 인터페이스가 별도로 나열되어 있습니다(예: Ethernet 2/1/1, 2/1/2, 2/1/3 및 2/1/4).

단계 **2** 40Gbps 인터페이스 1개를 10Gbps 인터페이스 4개로 변환하려면 다음과 같이 합니다.

a) 변환할 인터페이스의 **Breakout Port(**분할 포트**)** 아이콘을 클릭합니다.
Breakout Port Creation(분할 포트 생성) 대화 상자가 열리면서 계속 진행할 것인지 확인을 요청하고 섀시가 재부팅된다고 경고합니다.

b) 확인하려면 **Yes(**예**)**를 클릭합니다.
Firepower 섀시가 재부팅되고 지정된 인터페이스가 10Gbps 인터페이스 4개로 변환됩니다.

단계 **3** 10Gbps 분할 인터페이스 4개를 40Gbps 인터페이스 1개로 다시 변환하려면 다음과 같이 합니다.

a) 분할 인터페이스 중 하나에 대해 **Delete(**삭제**)**를 클릭합니다.
확인 대화 상자가 열리면서 계속 진행할 것인지 확인을 요청하고 분할 인터페이스 4개가 모두 삭제되며 섀시가 재부팅된다고 경고합니다.

b) 확인하려면 **Yes(**예**)**를 클릭합니다.
Firepower 섀시가 재부팅되고 지정된 인터페이스가 40Gbps 인터페이스 1개로 변환됩니다.

8 장

논리적 디바이스

- 논리적 디바이스 정보, 63 페이지
- 독립형 ASA 논리적 디바이스 생성, 64 페이지
- 독립형 위협 방어 논리적 디바이스 생성, 65 페이지
- 클러스터 구축, 67 페이지
- 보안 모듈의 콘솔에 연결, 73 페이지
- 논리적 디바이스 삭제, 74 페이지

논리적 디바이스 정보

논리적 디바이스를 생성, 편집 및 삭제하려면 Firepower Chassis Manager의 논리적 디바이스 페이지를 사용합니다.

논리적 디바이스를 생성할 때 Firepower 어플라이언스 관리자(Supervisor)는 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈에 푸시하여 논리적 디바이스를 구축합니다. 또는 클러스터의 경우, Firepower 섀시에 설치된 모든 보안 모듈에 적용합니다.

다음 2가지 유형의 논리적 디바이스 중 하나를 생성할 수 있습니다.

참고 논리적 디바이스의 한 가지 유형만 또는 다른 유형만 만들 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.

- 독립형 - Firepower 섀시에 설치된 각각의 보안 모듈에 독립형 논리적 디바이스를 생성할 수 있습니다.

참고 독립형 논리적 디바이스를 구성 중인 경우, 섀시에 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.

- 클러스터 - Firepower 섀시에 설치된 모든 보안 모듈이 단일 논리적 디바이스로서 그룹화되는 클러스터를 만들 수 있습니다. 클러스터는 처리량 증대 및 여러 디바이스의 이중화라는 목표를 달성하는 동시에 단일 디바이스(관리, 네트워크에 통합)의 모든 편의성을 제공합니다.

독립형 **ASA** 논리적 디바이스 생성

클러스터를 구성하지 않은 경우 Firepower 섀시에 설치된 각각의 보안 모듈에 독립형 논리적 디바이스를 생성할 수 있습니다. 클러스터를 구성한 경우 독립형 디바이스를 구성하려면 먼저 클러스터를 삭제해야 합니다.

참고 하나의 섀시 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 디바이스가 이미 구성되어 있는 보안 모듈을 논리적 디바이스에 사용하려는 경우, 기존의 논리적 디바이스를 먼저 삭제해야 합니다(논리적 디바이스 삭제, 74 페이지 참조).
- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드(Cisco.com에서 이미지 다운로드, 30 페이지 참고)한 다음 해당 이미지를 Firepower 어플라이언스에 업로드합니다(Firepower 어플라이언스에 이미지 업로드, 30 페이지 참고).
- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다.

절차

단계 **1** **Logical Devices**(논리적 디바이스)를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다. Logical Devices(논리적 디바이스) 페이지는 섀시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 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 Appliance**를 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** **Management Interface(**관리 인터페이스**)** 드롭다운 목록에서 논리적 디바이스에 사용할 관리 인터페이스를 선택합니다.

단계 **11** IPv4 및/또는 IPv6 영역에서 관리 IP 주소 정보를 구성합니다.
이 정보는 보안 모듈 컨피그레이션의 관리 인터페이스를 구성하는 데 사용됩니다. 이 관리 IP 주소는 ASDM에 연결하는 데 사용할 IP 주소입니다.

a) **Management IP(**관리 **IP)** 필드에서 로컬 IP 주소를 구성합니다.
b) **Network Mask(**네트워크 마스크**)** 또는 **Prefix Length(**접두사 길이**)**를 입력합니다.
c) **Network Gateway(**네트워크 게이트웨이**)** 주소를 입력합니다.

단계 **12** **Password(**비밀번호**)**에 "admin" 사용자의 비밀번호를 입력합니다.

단계 **13** Select Security Module(보안 모듈 선택) 아래에서 이 논리적 디바이스에 사용할 보안 모듈을 클릭하여 선택합니다.

단계 **14** **OK(**확인**)**를 클릭하여 ASA Configuration(ASA 컨피그레이션) 대화 상자를 닫습니다.

단계 **15** **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.

독립형 위협 방어 논리적 디바이스 생성

클러스터를 구성하지 않은 경우 Firepower 섀시에 설치된 각각의 보안 모듈에 독립형 논리적 디바이스를 생성할 수 있습니다. 클러스터를 구성한 경우 독립형 디바이스를 구성하려면 먼저 클러스터를 삭제해야 합니다.

참고 하나의 섀시 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 디바이스가 이미 구성되어 있는 보안 모듈을 논리적 디바이스에 사용하려는 경우, 기존의 논리적 디바이스를 먼저 삭제해야 합니다(논리적 디바이스 삭제, 74 페이지 참조).
- Cisco.com에서 논리적 디바이스에 사용할 애플리케이션 이미지를 다운로드(Cisco.com에서 이미지 다운로드, 30 페이지 참고)한 다음 해당 이미지를 Firepower 어플라이언스에 업로드합니다(Firepower 어플라이언스에 이미지 업로드, 30 페이지 참고).
- 논리적 디바이스에 사용할 관리 인터페이스를 구성합니다. 최소 하나 이상의 데이터 유형 인터페이스도 구성해야 합니다.

절차

단계 **1** **Logical Devices**(논리적 디바이스)를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.
Logical Devices(논리적 디바이스) 페이지는 섀시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 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 9300 관리 프로그램이 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 보안 모듈 컨피그레이션에 사용되는 디바이스 이름이 아닙니다.

단계 **4** **Template**(템플릿)에서 **Cisco Firepower Threat Defense**를 선택합니다.

단계 **5** **Image Version**(이미지 버전)에서 위협 방어 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.
컨피그레이션 대화 상자가 나타납니다.

단계 **10** **General Information**(일반 정보) 탭에서 다음 작업을 수행합니다.

a) Security Module Selection(보안 모듈 선택) 아래에서 이 논리적 디바이스에 사용할 보안 모듈을 클릭하여 선택합니다.

b) **Management Interface**(관리 인터페이스) 드롭다운 목록에서 논리적 디바이스에 사용할 관리 인터페이스를 선택합니다.

c) Default and Firepower(기본값 및 Firepower) 아래에서 관리 인터페이스를 구성합니다.
기본 관리 트래픽 채널은 모든 내부 트래픽(예: 어플라이언스 및 시스템의 관리에 한정된 디바이스 간 트래픽)을 전달하고, Firepower 트래픽 채널은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달합니다.

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) **Registration Key(**등록 키**)** 필드에 등록하는 동안 Firepower Management Center와 디바이스 간에 공유할 키를 입력합니다.
b) 디바이스의 비밀번호를 입력합니다.
c) **Firepower Management Center IP** 필드에 Firepower Management Center를 관리하기 위한 IP 주소를 입력합니다.
d) 방화벽 모드를 선택합니다.
e) Firepower 이벤트를 전송해야 할 인터페이스를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다.

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 모듈에 입력하여 논리적 디바이스를 구축합니다.

클러스터 구축

클러스터링을 사용하면 섀시에 있는 모든 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.

참고 Firepower 9300은 여러 섀시 전반에(섀시 간) 클러스터를 지원하지 않으며 인트라 섀시 클러스터링(intra-chassis clustering)만 지원됩니다.

클러스터링 정보

클러스터는 단일 유닛으로 작동하는 여러 개의 보안 모듈로 구성됩니다. Firepower 9300에서 클러스터를 구축하려면 다음 작업을 수행합니다.

- 보안 모듈 대 보안 모듈 통신용 클러스터 제어 링크를 생성합니다. 이 링크는 클러스터 통신에 Firepower 9300 백플레인을 사용합니다.
- 모든 보안 모듈에서 애플리케이션 내부에 클러스터 부트스트랩 컨피그레이션을 생성합니다.

클러스터를 구축할 때, Firepower 9300 관리자(Supervisor)는 클러스터 이름, 클러스터 제어 링크 인터페이스 및 기타 클러스터 설정을 포함하는 각 보안 모듈에 최소한의 부트스트랩 컨피그레이션을 푸시합니다. 클러스터링 환경을 사용자 정의하려는 경우, 사용자가 일부 부트스트랩 컨피그레이션을 보안 모듈 내부에 구성할 수 있습니다.

- 데이터 인터페이스를 *Spanned* EtherChannel로 클러스터에 할당합니다.

  Firepower 9300 관리자(Supervisor)는 모든 보안 모듈의 Spanned EtherChannel에서 트래픽을 로드 밸런싱합니다.

  참고 개별 인터페이스는 관리 인터페이스를 제외하고 지원되지 않습니다.

- 모든 보안 모듈에서 공유되는 별도의 관리 인터페이스를 할당합니다.

클러스터링 및 클러스터링이 보안 모듈 레벨에서 작동하는 방식에 대한 자세한 내용은 보안 모듈 애플리케이션에 대한 클러스터링 장을 참조하십시오. 다음 섹션에서는 클러스터링 개념 및 구현에 대한 자세한 정보를 제공합니다.

마스터 및 슬레이브 유닛 역할

클러스터의 멤버 1개는 마스터 유닛입니다. 마스터 유닛은 자동으로 결정됩니다. 기타 모든 멤버는 슬레이브 유닛입니다.

모든 컨피그레이션은 마스터 유닛에서만 수행해야 하며, 이후 컨피그레이션이 슬레이브 유닛에 복제됩니다.

Cluster Control Link

클러스터 제어 링크는 멤버 인터페이스 없이 Port-channel 48 인터페이스를 사용하여 자동으로 생성됩니다. 이 클러스터 유형 EtherChannel은 인트라 섀시 클러스터링(intra-chassis clustering)을 위한 클러스터 통신에 Firepower 9300 백플레인을 활용합니다. 나중에 섀시 간 클러스터링이 지원되면, 외부 연결을 위한 이 EtherChannel에 멤버 인터페이스를 추가할 수 있습니다. Port-channel 48 인터페이스를 사용하지 않으려는 경우, 대신 원하는 클러스터 유형의 EtherChannel을 미리 구성할 수 있습니다. 그러면 이것이 클러스터 제어 링크로 사용됩니다.

클러스터 제어 링크 트래픽에는 제어 및 데이터 트래픽이 모두 포함됩니다.

관리 인터페이스

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

기본 클러스터 IP 주소는 현재 마스터 유닛에 항상 속해 있는 클러스터의 고정 주소입니다. 주소의 범위를 구성하여 현재 마스터를 비롯한 각 유닛에서 해당 범위의 로컬 주소를 사용할 수 있도록 합니다. 기본 클러스터 IP 주소에서는 주소에 대한 일관된 관리 액세스를 제공합니다. 마스터 유닛이 변경될

경우 주요 클러스터 IP 주소는 새 마스터 유닛으로 이동되므로 클러스터는 지속적으로 원활하게 관리됩니다. 로컬 IP 주소는 라우팅에 사용되며 문제 해결에도 도움이 됩니다.

예를 들어, 현재 마스터 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 마스터 유닛을 비롯한 각 유닛에서는 로컬 IP 주소를 사용하여 서버에 연결합니다.

클러스터링 지침

- 이중화를 위해 EtherChannel을 VSS 또는 vPC에 연결할 것을 권장합니다.
- 일부 섀시 보안 모듈을 클러스터하고 독립형 모드에서 다른 보안 모듈을 실행할 수 없습니다. 클러스터에 모든 보안 모듈을 포함해야 합니다.

클러스터링 기본값

다른 클러스터 유형 인터페이스를 정의하지 않은 경우 클러스터 제어 링크는 Port-channel 48을 사용합니다.

ASA 클러스터링 구성

Firepower 9300 관리자(Supervisor)에서 손쉽게 클러스터를 구축할 수 있습니다. 모든 초기 컨피그레이션은 유닛마다 자동으로 생성됩니다.

절차

단계 **1** 클러스터를 구축하기 전에 데이터 유형 인터페이스 또는 EtherChannel(port-channel)을 최소 1개 추가합니다. 포트 채널 생성, 59 페이지 또는 인터페이스 속성 편집, 58 페이지를 참조하십시오.
또한 데이터 인터페이스를 구축한 후에 클러스터에 추가할 수 있습니다.

단계 **2** 관리 유형 인터페이스 또는 EtherChannel을 추가합니다. 포트 채널 생성, 59 페이지 또는 인터페이스 속성 편집, 58 페이지를 참조하십시오.

단계 **3** **Logical Devices(**논리적 디바이스**)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.
Logical Devices(논리적 디바이스) 페이지는 섀시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.

단계 **4** **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 **5** **Device Name(**디바이스 이름**)**에 논리적 디바이스의 이름을 제공합니다. 이 이름은 Firepower 9300 관리자(Supervisor)가 클러스터링 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 보안 모듈 컨피그레이션에 사용되는 클러스터 이름이 아닙니다.

단계 **6** **Template(**템플릿**)**에서 **Cisco Adaptive Security Appliance**를 선택합니다.

단계 **7** **Image Version(**이미지 버전**)**은 ASA 소프트웨어 버전을 선택합니다.

단계 **8** **Device Mode(**디바이스 모드**)**에서 **Cluster(**클러스터**)** 라디오 버튼을 클릭합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.
독립형 디바이스가 구성되어 있는 경우, 이 디바이스를 새 클러스터로 교체하라는 프롬프트가 표시됩니다. Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 **10** 기본적으로 모든 인터페이스는 클러스터에 할당됩니다. **Data Ports(**데이터 포트**)** 영역을 확장하고 클러스터에서 할당 취소할 각 인터페이스를 클릭합니다.

단계 **11** 화면 중앙의 디바이스 아이콘을 클릭합니다.
ASA Configuration(ASA 컨피그레이션) 대화 상자가 나타납니다.

단계 **12** **Management Interface(**관리 인터페이스**)**를 클릭하고 이전에 생성한 관리 인터페이스를 선택합니다.

단계 **13** **Cluster Information(**클러스터 정보**)** 영역에서 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 **14** **Cluster Group Name(**클러스터 그룹 이름**)**(보안 모듈 컨피그레이션의 클러스터 그룹 이름)을 설정합니다.
이름은 1~38자로 된 ASCII 문자열이어야 합니다.

단계 **15** **IPv4** 및/또는 **IPv6** 영역에서 관리 IP 주소 정보를 구성합니다.
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. 클러스터를 확장하려는 경우, 추가 주소를 포함하십시오. 현재 마스터 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.

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 **16** **Password(**비밀번호**)**에 "admin" 사용자의 비밀번호를 입력합니다.

단계 **17** **OK(**확인**)**를 클릭하여 ASA Configuration(ASA 컨피그레이션) 대화 상자를 닫습니다.

단계 **18** **Save(**저장**)**를 클릭합니다.

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

단계 **19** 클러스터링 컨피그레이션을 사용자 정의하려면 보안 모듈에 연결합니다.

위협 방어 클러스터링 구성

Firepower 9300 관리자(Supervisor)에서 손쉽게 클러스터를 구축할 수 있습니다. 모든 초기 컨피그레이션은 유닛마다 자동으로 생성됩니다.

절차

단계 **1** 클러스터를 구축하기 전에 데이터 유형 인터페이스 또는 EtherChannel(port-channel)을 최소 1개 추가합니다. 포트 채널 생성, 59 페이지 또는 인터페이스 속성 편집, 58 페이지를 참조하십시오.
또한 데이터 인터페이스를 구축한 후에 클러스터에 추가할 수 있습니다.

단계 **2** 관리 유형 인터페이스 또는 EtherChannel을 추가합니다. 포트 채널 생성, 59 페이지 또는 인터페이스 속성 편집, 58 페이지를 참조하십시오.

단계 **3** **Logical Devices(**논리적 디바이스**)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.
Logical Devices(논리적 디바이스) 페이지는 섀시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 논리적 디바이스가 구성되어 있지 않은 경우, 대신 이를 알리는 메시지가 표시됩니다.

단계 **4** **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 **5** **Device Name(**디바이스 이름**)**에 논리적 디바이스의 이름을 제공합니다. 이 이름은 Firepower 9300 관리자(Supervisor)가 클러스터링/관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 보안 모듈 컨피그레이션에 사용되는 클러스터 이름이 아닙니다.

단계 **6** **Template(**템플릿**)**에서 **Cisco Firepower Threat Defense**를 선택합니다.

단계 **7** **Image Version(**이미지 버전**)**에서 위협 방어 소프트웨어 버전을 선택합니다.

단계 **8** **Device Mode(**디바이스 모드**)**에서 **Cluster(**클러스터**)** 라디오 버튼을 클릭합니다.

단계 **9** **OK(**확인**)**를 클릭합니다.
독립형 디바이스가 구성되어 있는 경우, 이 디바이스를 새 클러스터로 교체하라는 프롬프트가 표시됩니다. Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.

단계 **10** 기본적으로 모든 인터페이스는 클러스터에 할당됩니다. 데이터 인터페이스의 할당을 취소하려면 **Data Ports(**데이터 포트**)** 영역을 확장하고 클러스터에서 할당 취소할 각 인터페이스를 클릭합니다.

단계 **11** 화면 중앙의 디바이스 아이콘을 클릭합니다.
Cisco Firepower Threat Defense Configuration(Cisco Firepower Threat Defense 컨피그레이션) 대화 상자가 나타납니다.

단계 **12** **Cluster Information(**클러스터 정보**)** 탭에서 다음 작업을 수행합니다.

a) **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.

b) **Cluster Group Name(**클러스터 그룹 이름**)(**보안 모듈 컨피그레이션의 클러스터 그룹 이름**)**을 설정합니다.
이름은 1~38자로 된 ASCII 문자열이어야 합니다.

c) **Management Interface(**관리 인터페이스**)** 드롭다운 목록에서 논리적 디바이스에 사용할 관리 인터페이스를 선택합니다.

d) Default(기본값)에서 기본 관리 인터페이스를 구성합니다.
기본 관리 트래픽 채널은 모든 내부 트래픽(예: 어플라이언스 및 시스템의 관리에 한정된 디바이스 간 트래픽)을 전달합니다.

1 **Address Type(**주소 유형**)** 드롭다운 목록에서 주소 유형을 선택합니다.

2 **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. 클러스터를 확장하려는 경우, 추가 주소를 포함하십시오. 현재 마스터 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.

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

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

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

5 **Network Gateway(**네트워크 게이트웨이**)** 주소를 입력합니다.

단계 **13** **Settings(**설정**)** 탭에서 다음 작업을 수행합니다.

a) **Registration Key(**등록 키**)** 필드에 등록하는 동안 Firepower Management Center와 디바이스 간에 공유할 키를 입력합니다.

b) 디바이스의 비밀번호를 입력합니다.

c) **Firepower Management Center IP** 필드에 Firepower Management Center를 관리하기 위한 IP 주소를 입력합니다.

d) 방화벽 모드를 선택합니다.

e) Firepower 이벤트를 전송해야 할 인터페이스를 선택합니다. 인터페이스가 지정되지 않은 경우, 관리 인터페이스가 사용됩니다.

단계 **14** **Interface Information(**인터페이스 정보**)** 탭에서 클러스터의 각 보안 모듈의 관리 인터페이스를 구성합니다. 이것은 모든 이벤트 트래픽(예: 웹 이벤트)을 전달하는 Firepower 이벤트 트래픽 채널에 사용되는 인터페이스입니다. **Address Type(**주소 유형**)** 드롭다운 목록에서 주소 유형을 선택한 다음 각 보안 모듈에 대해 다음 작업을 수행합니다.

a) **Management IP(**관리 **IP)** 필드에서 로컬 IP 주소를 구성합니다.
b) **Network Mask(**네트워크 마스크**)** 또는 **Prefix Length(**접두사 길이**)**를 입력합니다.
c) **Network Gateway(**네트워크 게이트웨이**)** 주소를 입력합니다.

단계 **15** **Agreement(**계약**)** 탭에서 EULA(End User License Agreement)를 읽고 내용에 동의해야 합니다.

단계 **16** **OK(**확인**)**를 클릭하여 Cisco Firepower Threat Defense Configuration(Cisco Firepower Threat Defense 컨피그레이션) 대화 상자를 닫습니다.

단계 **17** **Save(**저장**)**를 클릭합니다.
Firepower 9300 관리자(Supervisor)는 지정된 소프트웨어 버전을 다운로드하고 클러스터 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 각 보안 모듈에 입력하여 클러스터를 구축합니다.

단계 **18** 클러스터링 컨피그레이션을 사용자 정의하려면 보안 모듈에 연결합니다.

클러스터링 기록

기능 이름	플랫폼 릴리스	기능 정보
Cisco ASA를 위한 섀시 클러스터링	1.1(1)	Firepower 9300 섀시 내부에서 모든 ASA 보안 모듈을 클러스터링할 수 있습니다. 추가된 화면: **Logical Devices(**논리적 디바이스**)** > **Configuration(**컨피그레이션**)**
Cisco Firepower Threat Defense를 위한 인트라-섀시 클러스터링	1.1(2)	Firepower 9300 섀시 내부에서 모든 Threat Defense 보안 모듈을 클러스터링할 수 있습니다.

보안 모듈의 콘솔에 연결

다음 절차를 수행하여 보안 모듈의 콘솔에 연결합니다.

참고 콘솔 액세스 시 문제가 발생한 경우, 다른 SSH 클라이언트를 시도하거나 SSH 클라이언트를 새 버전으로 업그레이드할 것을 권장합니다.

절차

단계 **1** 보안 모듈의 콘솔에 연결하려면 다음과 같이 합니다.

a) FXOS CLI에서 보안 모듈에 연결합니다.
Firepower-chassis # **connectmodule** *slot_number***console**

보안 모듈에 처음 연결할 때, FXOS 모듈 CLI에 액세스합니다.

b) 모듈 OS에 연결하려면 디바이스에 적절한 명령을 입력합니다.
Firepower-module1>**connect asa**

Firepower-module1>**connect ftd**

FXOS CLI의 관리자(Supervisor) 수준에서 보안 모듈에 대한 후속 연결은 모듈 OS에 직접 액세스 됩니다.

단계 **2** (선택 사항) FXOS 모듈 CLI에 대한 모듈 OS 콘솔은 **Ctrl-A-D**를 입력하여 종료합니다.
문제 해결을 위해 FXOS 모듈 CLI에 액세스할 수 있습니다.

단계 **3** FXOS CLI의 관리자(Supervisor) 수준으로 돌아갑니다.

a) 보안 모듈 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 FXOS CLI의 관리자(Supervisor) 수준으로 다시 종료합니다.

```
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) 페이지는 섀시에 구성되어 있는 논리적 디바이스 목록을 보여줍니다. 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 것임을 확인합니다.

단계 **4** **Yes(**예**)**를 클릭하여 애플리케이션 컨피그레이션을 삭제할 것임을 확인합니다.

9 장

보안 모듈 관리

- Firepower 9300 보안 모듈 정보, 77 페이지
- 보안 모듈 해제/재위탁, 79 페이지
- 보안 모듈 확인, 79 페이지
- 보안 모듈 재설정, 80 페이지
- 보안 모듈 다시 초기화, 80 페이지
- 보안 모듈 켜기/끄기, 80 페이지

Firepower 9300 보안 모듈 정보

Firepower Chassis Manager의 Security Modules(보안 모듈) 페이지에서 섀시에 설치된 보안 모듈의 상태를 볼 수 있으며, 보안 모듈에서 다음 기능을 수행할 수 있습니다.

- Decommission/Recommission(해제/재위탁) - 보안 모듈을 해제하면 보안 모듈이 유지 관리 모드로 들어갑니다. 또한 특정 장애 상태를 수정하려면 모듈을 해제한 후 재위탁할 수 있습니다. 보안 모듈 해제/재위탁, 79 페이지를 참조하십시오.
- Acknowledge(확인) - 새로 설치된 보안 모듈을 온라인 상태로 전환합니다. 보안 모듈 확인, 79 페이지를 참조하십시오.
- Power Cycle(전원 껐다 켜기) - 보안 모듈을 다시 시작합니다. 보안 모듈 재설정, 80 페이지를 참조하십시오.
- Reinitialize(다시 초기화) - 보안 모듈 하드 디스크를 다시 포맷하여 모든 구축된 애플리케이션과 컨피그레이션을 보안 모듈에서 제거한 다음 시스템을 다시 시작합니다. 다시 초기화를 완료한 후, 보안 모듈에 대해 논리적 디바이스가 구성되어 있으면 Firepower eXtensible 운영 체제에서는 애플리케이션 소프트웨어를 다시 설치하고, 논리적 디바이스를 재구축하고, 애플리케이션을 자동으로 시작합니다. 보안 모듈 다시 초기화, 80 페이지를 참조하십시오.

  보안 모듈의 모든 애플리케이션 데이터는 다시 초기화하는 동안 삭제됩니다. 보안 모듈을 다시 초기화하기 전에 모든 애플리케이션 데이터를 백업하십시오.

- 전원 끄기/켜기 - 보안 모듈의 전원 상태를 전환합니다. 보안 모듈 켜기/끄기, 80 페이지를 참조하십시오.

Security Modules(보안 모듈) 페이지에서는 다음 정보를 제공합니다.

- Hardware State(하드웨어 상태) - 보안 모듈 하드웨어의 상태를 보여줍니다.
  - Up(가동) - 보안 모듈 전원이 성공적으로 켜졌고 하드웨어 장애가 보이지 않습니다.
  - Booting Up(부팅 중) - 보안 모듈의 전원을 켜는 중입니다.
  - Down(중단) - 보안 모듈의 전원이 켜지지 않았거나, 하드웨어 장애 때문에 보안 모듈을 성공적으로 시작할 수 없습니다.
  - Unassociated(연결되지 않음) - 보안 모듈에 논리적 디바이스가 연결되어 있지 않습니다.
  - Mismatch(불일치) - 보안 모듈이 해제되었거나 슬롯에 새 보안 모듈이 설치되었습니다. 보안 모듈을 작동 상태로 전환하려면 Recommission(재위탁) 또는 Acknowledge(확인) 기능을 사용합니다.
- Service State(서비스 상태) - 서비스 모듈에서 소프트웨어의 상태를 보여줍니다.
  - Not-available(사용 불가) - 보안 모듈이 섀시 슬롯에서 제거되었습니다. 보안 모듈을 정상적인 작동 상태로 전환하려면 다시 설치합니다.
  - Offline(오프라인) - 보안 모듈이 설치되었지만 해제되었거나, 전원이 꺼졌거나, 아직도 전원을 켜는 중입니다.
  - Online(온라인) - 보안 모듈이 설치되었고 정상 작동 모드에 있습니다.
  - Not Responding(응답 없음) - 보안 모듈이 응답하지 않습니다.
  - Fault(장애) - 보안 모듈이 장애 상태에 있습니다. 오류 상태를 일으킬 수 있는 것에 대해 자세히 알아보려면 시스템 결함 목록을 검토하십시오.
  - Token Mismatch(토큰 불일치) - 전에 구성된 것이 아닌 보안 모듈이 섀시 슬롯에 설치되었음을 나타냅니다. 또한 소프트웨어 설치 오류로 인해 발생할 수도 있습니다. 보안 모듈을 작동 상태로 전환하려면 Reinitialize(다시 초기화) 기능을 사용합니다.
- Power(전원) - 보안 모듈의 전원 상태를 보여줍니다.
  - On(켜짐) - 보안 모듈의 전원 상태를 전환하려면 전원 끄기/켜기 기능을 사용합니다.
  - Off(꺼짐) - 보안 모듈의 전원 상태를 전환하려면 전원 끄기/켜기 기능을 사용합니다.
- Application(애플리케이션) - 보안 모듈에 설치된 논리적 디바이스 유형을 보여줍니다.

보안 모듈 해제/재위탁

보안 모듈을 해제하면, 보안 모듈 객체가 컨피그레이션에서 삭제되고 보안 모듈은 관리되지 않는 상태가 됩니다. 보안 모듈에서 실행되는 모든 논리적 디바이스 또는 소프트웨어는 비활성 상태가 됩니다.

보안 모듈의 사용을 일시적으로 중단하려는 경우 보안 모듈을 해제할 수 있습니다. 또한 보안 모듈을 다시 시작해도 오류 상태가 해결되지 않는 경우, 보안 모듈을 다시 초기화하지 않은 채 보안 모듈을 해제한 후 재위탁하여 오류 상태가 해결되는지 확인할 수 있습니다.

절차

단계 **1** **Security Modules(**보안 모듈**)**를 선택하여 Security Modules(보안 모듈) 페이지를 엽니다.

단계 **2** 보안 모듈을 해제하려면 해당 보안 모듈에 대해 **Decommission(**해제**)**을 클릭합니다.
보안 모듈을 재위탁하려면 해당 보안 모듈에 대해 **Recommission(**재위탁**)**을 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭하여 지정된 보안 모듈의 해제 또는 재위탁을 확인합니다.

보안 모듈 확인

새로운 보안 모듈을 섀시에 설치할 경우 먼저 보안 모듈을 확인해야만 사용할 수 있습니다.

보안 모듈의 상태가 "불일치" 또는 "토큰 불일치"로 나타나면, 슬롯에 새로 설치한 보안 모듈에 전에 설치했던 것과 일치하지 않는 데이터가 있음을 나타내는 것입니다. 보안 모듈에 기존의 데이터가 있고 이것을 새 슬롯에서 사용하려는 경우(다시 말하면, 보안 모듈을 실수로 잘못된 슬롯에 설치한 것이 아닌 경우), 여기에 논리적 디바이스를 구축하려면 먼저 보안 모듈을 다시 초기화해야 합니다.

절차

단계 **1** **Security Modules(**보안 모듈**)**를 선택하여 Security Modules(보안 모듈) 페이지를 엽니다.

단계 **2** 확인할 보안 모듈에 대해 **Acknowledge(**확인**)**를 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭하여 지정된 보안 모듈을 확인합니다.

보안 모듈 재설정

절차

단계 **1** **Security Modules(**보안 모듈**)**를 선택하여 Security Modules(보안 모듈) 페이지를 엽니다.

단계 **2** 재설정할 보안 모듈에 대해 **Power Cycle(**전원 껐다 켜기**)**을 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭하여 지정된 보안 모듈의 재설정을 확인합니다.

보안 모듈 다시 초기화

보안 모듈을 다시 초기화하면 보안 모듈 하드 디스크가 포맷되고 설치된 모든 애플리케이션 인스턴스 및 컨피그레이션이 제거됩니다. 다시 초기화를 완료한 후, 보안 모듈에 대해 논리적 디바이스가 구성되어 있으면 Firepower eXtensible 운영 체제에서는 애플리케이션 소프트웨어를 다시 설치하고, 논리적 디바이스를 재구축하고, 애플리케이션을 자동으로 시작합니다.

보안 모듈의 모든 애플리케이션 데이터는 다시 초기화하는 동안 삭제됩니다. 보안 모듈을 다시 초기화하기 전에 모든 애플리케이션 데이터를 백업하십시오.

절차

단계 **1** **Security Modules(**보안 모듈**)**를 선택하여 Security Modules(보안 모듈) 페이지를 엽니다.

단계 **2** 다시 초기화할 보안 모듈에 대해 **Reinitialize(**다시 초기화**)**를 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭하여 지정된 보안 모듈의 다시 초기화를 확인합니다.
보안 모듈이 다시 시작되고 보안 모듈의 모든 데이터가 삭제됩니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.

보안 모듈 켜기/끄기

절차

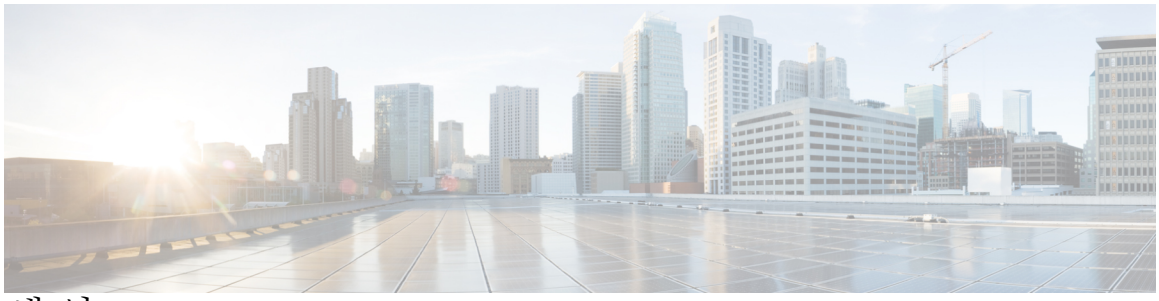
단계 **1** **Security Modules(**보안 모듈**)**를 선택하여 Security Modules(보안 모듈) 페이지를 엽니다.

단계 **2** 다음 중 하나를 수행합니다.

a) 보안 모듈을 켜려면 해당 보안 모듈에 대해 **Power on(**전원 켜기**)**을 클릭합니다.

b) 보안 모듈을 끄려면 해당 보안 모듈에 대해 **Power off(**전원 끄기**)**를 클릭합니다.

단계 **3** **Yes(**예**)**를 클릭하여 지정된 보안 모듈의 전원 켜기 또는 끄기를 확인합니다.



색 인

A

계정 19
  로컬에서 인증 19
기록, 비밀번호 20

B

날짜 및 시간 33
  구성 33
논리적 디바이스 31, 63, 64, 65, 69, 71, 73, 74
  독립형 생성 64, 65
  삭제 74
  연결 73
  연결 종료 73
  이미지 버전 업데이트 31
  이해 63
  클러스터 생성 69, 71
논리적 디바이스 연결 종료 73
논리적 디바이스에 연결 73
높은 수준의 작업 목록 5

D

date 34
  수동으로 설정 34
DNS 56

F

보안 모듈 79, 80
  다시 초기화 80
  리셋 80
  전원 끄기 80
  전원 켜기 80
보안 모듈 (계속)
  해제 79
  확인 79
보안 모듈 다시 초기화 80
보안 모듈 재설정 80
보안 모듈 켜기/끄기 80
보안 모듈 해제 79
보안 모듈 확인 79
분할 케이블 60
  구성 60
분할 포트 60
비밀번호 20, 21
  기록 수 20
  변경 간격 20
  보안 수준 확인 21
비밀번호 프로필 19
  정보 19

G

사용 39
  SNMP 39
사용자 계정 19
  비밀번호 프로필 19
사용자 인터페이스 1
  overview 1
섀시 관리자 1
  사용자 인터페이스 개요 1
섀시 상태 모니터링 2

H

위협 방어 65, 69, 71, 73, 74
  논리적 디바이스 삭제 74
  독립형 위협 방어 논리적 디바이스 생성 65
  연결 73

위협 방어 *(계속)*
연결 종료 **73**
클러스터 생성 **69, 71**
이미지 **29, 30, 31**
Cisco.com에서 다운로드 **30**
Firepower 9300 업로드 **30**
Firepower eXtensible 운영 체제 플랫폼 번들 업그레이드 **31**
관리 **29**
이미지 버전 **31**
업데이트 **31**

I

작업 플로우 **5**

J

초기 컨피그레이션 **6**

K

커뮤니티, SNMP **39**
클러스터 **67, 69, 71**
생성 **69, 71**
생성 시 기본값 **69**
정보 **67**

L

텔넷 **35**
구성 **35**
통신 서비스 **39**
SNMP **39**
트랩 **40, 41**
삭제 **41**
생성 **40**

M

포트 채널 **59**
구성 **59**
표준 시간대 **33, 34**
setting **33, 34**
프로파일 **19**
password **19**
플랫폼 번들 **29, 30, 31**
Cisco.com에서 다운로드 **30**
Firepower 9300 업로드 **30**
업그레이드 **31**
정보 **29**

R

RADIUS **49, 51**
RADIUS 제공자 **49, 51**
삭제 **51**
생성 **49**

S

Smart Call Home **14**
HTTP 프록시 구성 **14**
SNMP **36, 37, 38, 39, 40, 41, 42, 43**
community **39**
notifications **37**
users **42, 43**
삭제 **43**
생성 **42**
권한 **37**
버전 3 보안 기능 **38**
보안 수준 **37**
사용 **39**
정보 **36**
지원 **36, 39**
트랩 **40, 41**
삭제 **41**
생성 **40**
SNMPv3 **38**
보안 기능 **38**
SSH **34**
구성 **34**
syslog **53**
로컬 대상 구성 **53**
로컬 소스 구성 **53**
원격 대상 구성 **53**
system **6**
초기 컨피그레이션 **6**

T

TACACS+ 51, 52, 53
TACACS+ 제공자 52, 53
    삭제 53
    생성 52
time 34
    수동으로 설정 34
traps 37
    정보 37

U

users 17, 19, 21, 24, 26, 27, 42, 43
    SNMP 42, 43
    관리 17
    기본 역할 19
    기본 인증 21
users *(계속)*
    로컬에서 인증 19
    비활성화 27
    삭제 26
    생성 24
    설정 21
    활성화 27

W

라이센스 15
    등록 15
라이센스 등록 15
로그인 또는 로그아웃 8
로컬에서 인증된 사용자 19
    비밀번호 프로필 19