Cisco Firepower Threat Defense for Firepower 4100 빠른 시작 설명서

최초 게시일: 2016년 3월 10일

최종 업데이트: 2017년 3월 13일

1. Firepower Threat Defense 보안 서비스 정보

Cisco Firepower 4100 보안 어플라이언스는 Firepower Threat Defense 애플리케이션을 실행할 수 있는 네트워크 및 콘텐츠 보안 솔루션을 위한 독립형 보안 서비스 플랫폼입니다.

Firepower Threat Defense를 사용하여 데이터 센터에 Firepower 4100을 구축하고 스테이트풀 방화벽, 라우팅, NGIPS(Next-Generation Intrusion Prevention System), AVC(Application Visibility and Control), URL 필터링, AMP(Advanced Malware Protection)를 비롯한 차세대 방화벽 서비스를 제공할 수 있습니다. 단일 상황 모드 및 라우팅 또는 투명 모드에서 위협 방어 디바이스를 사용할 수 있습니다.

Firepower Threat Defense와 Firepower 4100의 작동 방식

Firepower 4100 보안 어플라이언스는 FXOS(Firepower eXtensible Operating System)라는 관리 프로그램에서 자체 운영 체제를 실행합니다. Firepower Chassis Manager는 단순한 GUI 기반 관리 기능을 제공합니다. Firepower Chassis Manager 웹 인터페이스 또는 CLI를 사용하여 하드웨어 인터페이스 설정, 스마트 라이선스, 관리 프로그램의 기타 기본적인 작동 매개변수를 구성할 수 있습니다.

외부 EtherChannels 설정을 비롯한 모든 물리적 인터페이스 작업은 관리 프로그램에서 담당합니다. Firepower Threat Defense를 실행하는 논리적 디바이스에 인터페이스를 할당할 수 있습니다. 세 가지 유형의 인터페이스인 Data, Management 및 Firepower Eventing이 지원됩니다. Firepower Eventing 인터페이스는 이벤트 트래픽 전송만 담당합니다. 구축 시 또는 나중에 필요한 경우 Firepower 4100 with Firepower Threat Defense에 인터페이스를 할당할 수 있습니다. 이러한 인터페이스는 관리 프로그램에서도 Firepower 4100 with Firepower Threat Defense 컨피그레이션에서와 동일한 ID를 사용합니다.

Firepower 4100 with Firepower Threat Defense를 구축하면 관리 프로그램에서는 사용자가 선택한 애플리케이션 이미지를 다운로드하고 기본 컨피그레이션을 설정합니다. Firepower 4100 with Firepower Threat Defense는 독립형 논리적 디바이스로만 구축할 수 있으며 클러스터링은 지원되지 않습니다.

Firepower Management Center 지원 및 CLI 액세스

Firepower 4100 with Firepower Threat Defense를 구축할 때 Firepower Management Center 액세스를 허용하도록 Firepower Management Center를 관리하기 위해 관리 인터페이스와 등록 정보를 지정합니다. 다른 관리되는 디바이스와 마찬가지로 Firepower Threat Defense 디바이스를 등록하고, 정책 컨피그레이션 및 구축을 수행할 수 있습니다.

내부 텔넷 연결을 사용하여 Firepower Threat Defense CLI에서 Firepower 4100 관리 프로그램 CLI에 액세스할 수도 있습니다. Firepower 4100 보안 어플라이언스 내에서 나중에 관리 인터페이스 또는 데이터 인터페이스에 대한 SSH 또는 텔넷 액세스를 구성할 수 있습니다. 6. Firepower Threat Defense CLI에 액세스, 9페이지를 참조하십시오.

관리/진단 인터페이스 및 네트워크 구축

물리적 관리 인터페이스는 논리적 관리 인터페이스와 논리적 진단 인터페이스 간에 공유됩니다.

Firepower Threat Defense 디바이스는 Firepower Management Center 관리를 위해 설정된 IP 주소, 그리고 게이트웨이에 대한 연결된 경로를 사용합니다. 관리 IP 주소 및 경로는 디바이스에 대한 인터페이스 또는 고정 경로의 목록에서 Firepower Management Center 웹 인터페이스에 포함되어 있지 **않습니다**. 초기 설정을 수행한 후 Firepower Management Center를 사용하여 보안 및 액세스 정책, 디바이스 설정, 인터페이스 등을 구성합니다.

물리적 관리 포트를 통해 syslog 또는 SNMP 보고를 선택하는 경우, Firepower Management Center 웹 인터페이스를 사용하여 Diagnostic 0/0 또는 Diagnostic 1/1 인터페이스에 대해 별도의 IP 주소와 경로 및 외부 인증을 구성해야 합니다. 그러나 구축을 간소화하려면 보고 목적으로는 데이터 포트를 사용하는 것이 좋습니다.

관리/진단 인터페이스에 대한 자세한 내용은 *Firepower Management Center 환경 설정 가이드*의 Firepower Threat Defense 인터페이스 장을 참조하십시오.

Firepower Threat Defense의 라이선싱 요구 사항

Firepower 4100에서 실행하는 Firepower Threat Defense에는 Firepower Management Center에 대해 구성 가능한 스마트 소프트웨어 라이선싱이 필요합니다. 자세한 내용은 *Firepower Management Center 환경 설정 가이드* 또는 Firepower Management Center의 온라인 도움말을 참조하십시오.

Firepower 4100에서 실행 중인 Firepower Threat Defense의 경우 스마트 소프트웨어 라이선싱 컨피그레이션이 Firepower 4100 관리 프로그램 및 보안 모듈로 나뉩니다.

- Firepower 4100 - 관리 프로그램에 모든 스마트 소프트웨어 라이선싱 인프라를 구성하며 여기에는 License Authority와 통신하는 데 필요한 매개변수가 포함됩니다. Firepower 4100 자체는 작동하기 위한 라이선스가 필요하지 않습니다.
- Firepower Threat Defense - Firepower Management Center의 보안 서비스에 대해 모든 라이선스 엔타이틀먼트를 구성합니다.

Firepower 4100 섀시는 디바이스로서 등록되는 반면, 섀시의 보안 모듈에 있는 Firepower Threat Defense에는 고유한 라이선스가 필요합니다. Firepower 4100의 라이선스 관리에 대한 자세한 내용은 *Cisco FXOS Firepower Chassis Manager 환경 설정 가이드*를 참조하십시오.

Firepower Management Center의 라이선스 관리 방법에 대한 자세한 내용은 *Firepower Management Center 환경 설정 가이드*의 "Firepower System 라이선싱"을 참조하십시오.

Firepower Chassis Manager 웹 인터페이스에 액세스

Firepower Chassis Manager 웹 인터페이스를 사용하여 애플리케이션 이미지를 관리하고, 하드웨어 인터페이스 설정을 구성하고, 관리 프로그램의 기타 기본적인 운영 매개변수를 관리할 수 있습니다.

절차

1. Firepower Chassis Manager 웹 인터페이스에 로그인하려면 다음을 수행합니다.

   a. 지원되는 브라우저를 사용하여 주소 표시줄에 다음 URL을 입력합니다.

   `https://<chassis_mgmt_ip_address>`

   여기서 *<chassis_mgmt_ip_address>*는 초기 컨피그레이션을 설정하는 동안 입력한 Firepower 4100의 IP 주소 또는 호스트 이름입니다. 자세한 내용은 초기 컨피그레이션, 3페이지를 참조하십시오.

   b. 사용자 이름 및 비밀번호를 입력합니다.

   c. **Login(로그인)**을 클릭합니다.

   로그인하면 Firepower Chassis Manager 웹 인터페이스가 열리고 Overview(개요) 페이지가 표시됩니다.

2. Firepower Chassis Manager 웹 인터페이스에서 로그아웃하려면 **admin(관리자) > Logout(로그아웃)**을 선택합니다. Firepower Chassis Manager 웹 인터페이스에서 로그아웃되고 로그인 화면으로 돌아갑니다.

2. Firepower Threat Defense를 구축합니다.

Firepower 4100에서는 두 가지 기본 이미지 유형인 플랫폼 번들 및 애플리케이션을 사용합니다. 플랫폼 번들은 관리 프로그램에 필요한 Firepower FXOS 소프트웨어 패키지를 포함합니다. 애플리케이션 이미지는 보안 엔진을 구축하기 위한 소프트웨어 이미지입니다.

Firepower Threat Defense는 Firepower 4100의 보안 엔진에서 애플리케이션 이미지로 구축됩니다. 애플리케이션 이미지는 CSP(Cisco Secure Package) 파일로 전송되고 논리적 디바이스를 생성하거나 이후 논리적 디바이스 생성에 대비하기 위해 보안 엔진에 구축될 때까지 관리 프로그램에 저장됩니다. 관리 프로그램에 동일한 애플리케이션 이미지 유형의 서로 다른 여러 버전을 둘 수 있습니다.

System(시스템) 메뉴의 **Updates(업데이트)** 페이지에서 FXOS 플랫폼 번들, Firepower Threat Defense 애플리케이션 이미지 및 Cisco.com의 최신 업데이트를 다운로드할 수 있습니다. 그런 다음 Firepower Threat Defense 이미지를 Firepower 4100에 업로드하여 논리적 디바이스를 만들거나 업데이트할 때 사용할 수 있습니다. 관리 프로그램에서 실행 중인 FXOS 버전과 호환되는 Firepower Threat Defense 이미지 버전을 사용 중인지 확인하십시오.

자세한 내용은 *Cisco FXOS Firepower Chassis Manager 환경 설정 가이드*를 참조하십시오.

작업 개요

Firepower 4100 보안 어플라이언스에서 Firepower Threat Defense 구축을 시작하기 전에 다음 지침 및 요구 사항을 검토하십시오.

- 초기 컨피그레이션, 3페이지에 설명된 대로 초기 설정 마법사를 사용하여 Firepower 4100 보안 어플라이언스의 초기 컨피그레이션을 수행합니다.
- NTP 구성, 4페이지에 설명된 대로 Firepower Chassis Manager에서 NTP를 구성합니다.
- 인터페이스 구성, 5페이지에 설명된 대로 관리 인터페이스 및 하나 이상의 데이터 인터페이스를 구성합니다.
- Firepower Threat Defense 논리적 디바이스 구축, 5페이지에 설명된 대로 Firepower Threat Defense 독립형 논리적 디바이스를 구성합니다.
- 3. Firepower Management Center 등록, 6페이지에 설명된 대로 Firepower Management Center에서 Firepower Threat Defense 유닛을 검색합니다.

Firepower Threat Defense 또는 FXOS 업그레이드인 경우 또는 다른 애플리케이션을 구축하려는 경우에는 Cisco.com에서 최신 FXOS 플랫폼 번들, 애플리케이션 이미지 및 최신 업데이트를 다운로드해야 합니다. 5. 업그레이드 고려 사항, 7페이지를 참조하십시오.

초기 컨피그레이션

Firepower Chassis Manager 또는 FXOS CLI를 사용하여 시스템을 구성 및 관리하려면 먼저 포트 콘솔을 통해 액세스할 수 있는 FXOS CLI를 사용하여 초기 컨피그레이션 작업을 수행해야 합니다. FXOS CLI를 사용하여 처음으로 FXOS 섀시에 액세스할 때 시스템을 구성하는 데 사용할 수 있는 설정 마법사가 나타납니다.

시작하기 전에

- FXOS 섀시에서 다음 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 Chassis Manager 환경 설정 가이드*를 참조하십시오.

절차

1. 콘솔 포트에서 또는 SSH를 사용하여 Firepower 4100 CLI에 연결합니다.
2. 사용자 이름 **admin** 및 비밀번호 **cisco123**으로 로그인합니다.
3. 표시되는 화면 컨피그레이션을 완료합니다.

   예를 들면 다음과 같습니다.

```
Enter the setup mode; setup newly or restore from backup. (setup/restore) ? setup
You have chosen to setup a new Security Appliance. Continue? (y/n): y
Enforce strong password? (y/n): n
Enter the password for "admin": <new password>
Confirm the password for "admin": <repeat password>
Enter the system name: FTD-SSP-4100
Physical Switch Mgmt0 IP address : 10.127.56.61
Physical Switch Mgmt0 IPv4 netmask : 255.255.255.0
IPv4 address of default gateway : 10.127.56.1
Configure the DNS Server IP address? (yes/no) [n]: n
Configure the default domain name? (yes/no) [n]: n

Following configurations will be applied:
   Switch Fabic=A
   System Name=FTD-SSP-4100
   Enforced Strong Password=no
   Physical Switch Mgmt0 IP Address=10.127.56.61
   Physical Switch Mgmt0 IP Netmask=255.255.255.0
   Default Gateway=10.127.56.1
   Ipv6 value=0

Apply and save the configuration (select 'n' if you want to re-enter)? (yes/no): yes
Applying configuration. Please wait.
```

4. Firepower Chassis Manager 웹 인터페이스를 구동하고 새로운 로그인 접속 정보를 사용하여 연결을 확인합니다.

   a. 지원되는 브라우저를 사용하여 주소 표시줄에 다음 URL을 입력합니다.

   `https://<chassis_mgmt_ip_address>`

   여기서 *<chassis_mgmt_ip_address>*는 초기 컨피그레이션을 설정하는 동안 입력한 Firepower 4100의 IP 주소 또는 호스트 이름입니다.

   b. 사용자 이름 및 비밀번호를 입력합니다.

   c. **Login(로그인)**을 클릭합니다.

   로그인하면 Firepower Chassis Manager 웹 인터페이스가 열리고 Overview(개요) 페이지가 표시됩니다.

NTP 구성

Firepower 4100에 Firepower Threat Defense를 구축하려면 Firepower Chassis Manager에서 NTP를 구성해야 합니다. Smart Licensing이 제대로 작동하고 디바이스 등록에 올바른 타임스탬프가 나타나도록 하려면 Firepower Chassis Manager에서 NTP 서버를 설정해야 합니다.

절차

1. Firepower Chassis Manager 인터페이스에서 **Platform Settings(플랫폼 설정) > NTP**를 선택합니다.
2. **Time Zone(표준 시간대)** 드롭다운 목록에서 Firepower 섀시에 적절한 표준 시간대를 선택합니다.

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.
4. **Save(저장)**를 클릭합니다.

   Firepower 섀시는 NTP 서버가 지정된 상태로 구성됩니다.

   참고: 시스템 시간을 10분 넘게 수정하는 경우 시스템에서 로그아웃되므로 Firepower Chassis Manager에 다시 로그인해야 합니다.

인터페이스 구성

Firepower 4100 Firepower Threat Defense의 구축 컨피그레이션에 포함할 수 있는 관리 프로그램의 관리 유형 인터페이스를 구성합니다. 최소 하나 이상의 데이터 유형 인터페이스도 구성해야 합니다.

절차

1. Firepower Chassis Manager 인터페이스에서 **Interface(인터페이스)**를 선택하여 Interfaces(인터페이스) 페이지를 엽니다.
2. EtherChannel을 추가하려면 다음을 수행합니다.
   a. **Add Port Channel(포트 채널 추가)**을 클릭합니다.
   b. Port Channel ID(포트 채널 ID)에 1~47 사이의 값을 입력합니다.
   c. **Enable(사용)** 확인란이 선택된 상태로 둡니다.
   d. Type(유형)으로 **Management**, **Data** 또는 **Firepower Eventing**을 선택합니다. 논리적 디바이스당 1개의 관리 인터페이스만 포함할 수 있습니다.

   참고: 인터페이스 유형을 프로비저닝된 논리적 디바이스에 할당한 후에는 변경할 수 없습니다.

   e. 원하는 멤버 인터페이스를 추가합니다.
   f. **확인**을 클릭합니다.
3. 단일 인터페이스의 경우:
   a. 인터페이스 행에서 **Edit(수정)** 아이콘을 클릭하여 Edit Interface(인터페이스 수정) 대화 상자를 엽니다.
   b. **Enable(사용)** 확인란을 선택합니다.
   c. Type(유형)으로 **Management**, **Data** 또는 **Firepower Eventing**을 클릭합니다. 논리적 디바이스당 1개의 관리 인터페이스만 포함할 수 있습니다.
   d. **확인**을 클릭합니다.

Firepower Threat Defense 논리적 디바이스 구축

독립형 논리적 디바이스로 Firepower Threat Defense를 구성할 수 있습니다. 다음을 비롯한 논리적 디바이스 정보를 구성합니다.

- 디바이스 정보 및 주소 지정
- Firepower Management Center 등록 정보, 방화벽 모드, 이벤트를 비롯한 디바이스 설정
- 인터페이스 정보 및 주소 지정
- 최종 사용자 라이선스 계약

절차

1. Firepower Chassis Manager 인터페이스에서 **Logical Devices(논리적 디바이스)**를 선택하여 Logical Devices(논리적 디바이스) 페이지를 엽니다.
2. **Add Device(디바이스 추가)**를 클릭하여 Add Device(디바이스 추가) 대화 상자를 엽니다.
3. **Device Name(디바이스 이름)**에 논리적 디바이스의 이름을 제공합니다. 이 이름은 Firepower 4100 관리 프로그램이 관리 설정을 구성하고 인터페이스를 할당하는 데 사용됩니다. 이는 보안 모듈 컨피그레이션에 사용되는 디바이스 이름이 아닙니다.
4. **Template(템플릿)**에 대해 **Firepower Threat Defense**를 선택합니다.
5. **Image Version(이미지 버전)**에 대해 Firepower Threat Defense 소프트웨어 버전을 선택합니다.
6. **Device Mode(디바이스 모드)**에 대해 **Standalone(독립형)** 라디오 버튼을 클릭합니다.
7. **OK(확인)**를 클릭합니다. Provisioning - *device name*(프로비저닝 - 디바이스 이름) 창이 표시됩니다.
8. **Data Ports(데이터 포트)** 영역을 확장하고 Firepower Threat Defense에 할당할 각 인터페이스를 클릭합니다.
9. 화면 중앙의 디바이스 아이콘을 클릭합니다. 컨피그레이션 대화 상자가 나타납니다.
10. 컨피그레이션 대화 상자의 각 탭에서 구축 옵션을 구성합니다.
    a. Logical Device Information(논리적 디바이스 정보) - 이 논리적 디바이스의 관리 설정을 입력합니다.

    참고: 장치 등록 후 Firepower Management Center에서 가상 IPv4 또는 IPv6 주소를 구성할 수 있습니다. 이는 syslog를 사용하려는 경우 중요합니다.

    b. Settings(설정) - Firepower Management Center 관리를 위한 등록 키와 비밀번호 및 IP 주소를 입력합니다. 또한 방화벽 모드, Firepower Eventing 인터페이스(구성된 경우) 및 DNS 정보를 선택합니다.

    참고: 등록 키는 사용자가 생성한 일회용 키로, 37자를 초과하지 않아야 합니다. 영숫자(A~Z, a~z, 0~9)와 하이픈(-)을 사용할 수 있습니다. 장치를 Firepower Management Center에 추가할 때 이 등록 키를 기억해야 합니다.

    c. Interface Information(인터페이스 정보) - 이 논리적 디바이스의 관리 설정을 입력합니다.

    참고: 보안 모듈에는 Firepower Management Center에서 디바이스를 등록할 때 사용하는 자체 IP 주소가 필요합니다. Firepower Management Center에 모듈을 추가하려면 이 IP가 반드시 필요합니다.

    d. Agreement(계약) - EULA(end user license agreement)를 읽고 내용에 동의합니다.
11. **OK(확인)**를 클릭하여 컨피그레이션 대화 상자를 닫습니다.
12. **Save(저장)**를 클릭합니다. Firepower 4100 관리 프로그램에서 지정된 소프트웨어 버전을 다운로드하고 부트스트랩 컨피그레이션 및 관리 인터페이스 설정을 지정된 보안 모듈에 입력하여 논리적 디바이스를 구축합니다.

3. Firepower Management Center 등록

시작하기 전에

- 등록하려는 Firepower Threat Defense 보안 모듈에 대해 Firepower Chassis Manager에서 설정을 확인합니다.
- Firepower 4100에서 실행하는 Firepower Threat Defense에는 Firepower Management Center에 대해 구성 가능한 스마트 소프트웨어 라이선싱이 필요합니다.

절차

1. 브라우저에서 HTTPS를 사용하고, Firepower Management Center에 구성된 호스트 이름 또는 주소를 사용하여 Firepower Management Center에 로그인합니다. 예: https://MC.example.com.
2. Management Center에 대한 웹 인터페이스에서 **Devices(디바이스)** > **Device Management(디바이스 관리)**를 선택합니다.

3. **Add** 드롭다운 메뉴에서 **Add Device**를 클릭합니다.
4. 추가할 Firepower Threat Defense 디바이스의 IP 주소 또는 호스트 이름을 **Host(호스트)** 필드에 입력합니다.
5. Management Center에 표시할 Firepower Threat Defense 디바이스의 이름을 **Display Name(표시 이름)** 필드에 입력합니다.
6. Firepower Chassis Manager에서 Firepower Threat Defense 디바이스를 구성할 때 사용한 것과 동일한 등록 키를 **Registration Key(등록 키)** 필드에 입력합니다.
7. 다중 도메인 환경에서 디바이스를 추가하는 경우 **Domain(도메인)** 드롭다운 목록에서 값을 선택하여 디바이스를 리프 도메인에 할당합니다.
8. **Access Control Policy(액세스 제어 정책)** 드롭다운 목록에서 보안 모듈에 구축할 초기 정책을 선택합니다.
   - **Default Access Control** 정책은 네트워크에 들어오는 모든 트래픽을 차단합니다.
   - **Default Intrusion Prevention** 정책은 Balanced Security and Connectivity 침입 정책을 통과한 모든 트래픽을 허용합니다.
   - **Default Network Discovery** 정책은 네트워크 검색만으로 검사되는 모든 트래픽을 허용합니다.
   - 기존의 사용자 정의 액세스 제어 정책을 선택할 수 있습니다. 자세한 내용은 *Firepower Management Center 환경 설정 가이드*의 "액세스 제어 정책 관리"를 참조하십시오.
9. 디바이스에 적용할 라이선스를 선택합니다. 다음을 참고하십시오.
   - Control, Malware 및 URL Filtering 라이선스에는 Protection 라이선스가 필요합니다.
10. **Register(등록)**를 클릭하여 성공적인 등록을 확인합니다.

4. 정책 및 디바이스 설정 구성

Firepower Threat Defense를 설치하고 Management Center에 디바이스를 추가한 후 Firepower Management Center 사용자 인터페이스를 사용하여, Firepower 4100에서 실행 중인 Firepower Threat Defense의 디바이스 관리 설정을 구성하고 Firepower Threat Defense 보안 모듈을 사용하여 트래픽을 관리하기 위한 액세스 제어 정책 및 기타 관련 정책을 구성할 수 있습니다.

보안 정책은 Firepower Threat Defense에서 제공하는 Next Generation IPS 필터링 및 애플리케이션 필터링 등의 서비스를 제어합니다. Firepower Management Center를 사용하여 Firepower Threat Defense에서 보안 정책을 구성할 수 있습니다. 보안 정책 구성 방법에 대한 자세한 내용은 *Cisco Firepower 환경 설정 가이드* 또는 Firepower Management Center의 온라인 도움말을 참조하십시오.

5. 업그레이드 고려 사항

Firepower Threat Defense 또는 Firepower 관리 프로그램을 업그레이드하려는 경우, 또는 다른 애플리케이션을 구축하려는 경우에는 Cisco.com에서 최신 FXOS 플랫폼 번들, 애플리케이션 이미지 및 최신 업데이트를 가져와야 합니다.

참고: Firepower Threat Defense 논리적 디바이스를 업그레이드하려면 Firepower Management Center를 사용해야 합니다. Firepower Chassis Manager 또는 FXOS CLI를 사용하여 Firepower Threat Defense 논리적 디바이스를 업그레이드하지 마십시오. 자세한 내용은 Firepower System 릴리스 노트를 참조하십시오.

다음 절차에서는 **System(시스템)** 메뉴의 **Updates(업데이트)** 페이지를 사용하여 Cisco.com에서 FXOS 플랫폼 번들, 애플리케이션 이미지(예: Firepower Threat Defense 또는 기타 애플리케이션) 및 최신 업데이트를 다운로드하는 방법, 그리고 이미지를 업로드하고 관리 프로그램을 업그레이드하는 방법을 설명합니다.

- 필요한 FXOS 소프트웨어 패키지 및 애플리케이션 이미지를 다운로드하려면 Cisco.com에서 소프트웨어 이미지 다운로드, 8페이지를 참조하십시오.
- 애플리케이션 또는 플랫폼 번들을 업로드하려면 Firepower 4100에 소프트웨어 이미지 업로드, 8페이지를 참조하십시오.
- 기존의 논리적 디바이스 또는 컨피그레이션을 삭제하려면 기존의 논리적 디바이스 및 애플리케이션 컨피그레이션 삭제, 9페이지를 참조하십시오.
- 관리 프로그램 소프트웨어 번들을 업그레이드하려면 Firepower 관리 프로그램 플랫폼 업그레이드, 9페이지를 참조하십시오.

Cisco.com에서 소프트웨어 이미지 다운로드

시작하기 전에

- Cisco.com 어카운트가 있어야 합니다.
- 설치에 필요한 호환되는 플랫폼 번들 및 Firepower Threat Defense 애플리케이션 이미지 버전을 잘 알고 있어야 합니다.
- 인터넷 액세스가 가능해야 합니다.

절차

1. Firepower Chassis Manager 인터페이스에서 **System(시스템) > Updates(업데이트)**를 선택합니다. Available Updates(사용 가능한 업데이트) 페이지는 섀시에서 사용 가능한 Firepower 4100 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.
2. 페이지 하단에서 **Download latest updates from CCO(CCO에서 최신 업데이트 다운로드)** 링크를 클릭합니다. Firepower 4100에 대한 소프트웨어 다운로드 페이지가 브라우저의 새 탭에 열립니다.
3. 적절한 소프트웨어 이미지를 찾아 로컬 컴퓨터에 다운로드합니다.

Firepower 4100에 소프트웨어 이미지 업로드

시작하기 전에

- 업로드하려는 이미지가 로컬 컴퓨터에서 사용 가능한지 확인합니다.

절차

1. Firepower Chassis Manager 인터페이스에서 **System(시스템) > Updates(업데이트)**를 선택합니다. Available Updates(사용 가능한 업데이트) 페이지는 섀시에서 사용 가능한 Firepower 4100 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.
2. **Upload Image(이미지 업로드)**를 클릭하여 Upload Image(이미지 업로드) 대화 상자를 엽니다.
3. **Browse(찾아보기)**를 클릭하고 업로드할 이미지를 찾아서 선택합니다.
4. **Upload(업로드)**를 클릭합니다. 선택한 이미지는 Firepower 4100에 업로드됩니다.
5. 계속하려면 화면의 지침에 따라 최종 사용자 라이선스 계약에 동의합니다.

기존의 논리적 디바이스 및 애플리케이션 컨피그레이션 삭제

Firepower Threat Defense 논리적 디바이스를 업그레이드하거나 다른 논리적 디바이스를 구축하려면 기존 디바이스를 삭제한 다음 업데이트된 이미지를 사용하여 새 디바이스를 생성해야 합니다. FXOS 플랫폼 번들 이미지와 애플리케이션을 모두 업그레이드하려면 먼저 FXOS 플랫폼 번들을 업그레이드해야 합니다.

절차

1. Firepower Chassis Manager 인터페이스에서 **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.
2. 각 논리적 디바이스와 연결된 **Delete(삭제)** 아이콘을 클릭합니다.
3. 논리적 디바이스를 삭제할지 묻는 메시지가 표시되면 **Yes(예)**를 클릭합니다.
4. 애플리케이션 컨피그레이션을 삭제할지 묻는 메시지가 표시되면 **Yes(예)**를 클릭합니다. Firepower Threat Defense를 성공적으로 설치하려면 이 마지막 단계가 필요합니다.

향후 작업

- 섀시에서 실행 중인 Firepower FXOS 소프트웨어의 버전을 확인하여 보안 엔진에서 Firepower Threat Defense 또는 기타 애플리케이션 실행을 지원하기 위해 업그레이드가 필요한지를 알아봅니다.

Firepower 관리 프로그램 플랫폼 업그레이드

Firepower Chassis Manager 웹 인터페이스의 **Overview(개요)** 페이지 상단에 FXOS의 실행 버전이 표시됩니다. 섀시에서 실행 중인 FXOS의 현재 버전이 보안 엔진에서 애플리케이션 실행을 지원하기에 충분한지 확인해야 합니다. **System(시스템)** 메뉴의 **Updates(업데이트)** 페이지에서 FXOS 플랫폼 번들을 업그레이드합니다.

절차

1. Firepower Chassis Manager 인터페이스에서 **System(시스템) > Updates(업데이트)**를 선택합니다. Available Updates(사용 가능한 업데이트) 페이지는 섀시에서 사용 가능한 Firepower 4100 플랫폼 번들 이미지와 애플리케이션 이미지 목록을 보여줍니다.
2. **Image Name(이미지 이름)** 열로 이동하여 로드해야 할 FXOS 플랫폼 번들을 찾습니다.
3. 업로드해야 할 FXOS 플랫폼 번들과 연결된 업로드/다운로드 아이콘을 클릭합니다.
4. 선택한 버전의 **Update Bundle Image(번들 이미지 업데이트)** 대화 상자에서 Yes(예)를 클릭합니다. Yes(예)를 클릭하면 선택한 버전이 설치되고 디바이스가 리부팅됩니다.

6. Firepower Threat Defense CLI에 액세스

초기 컨피그레이션을 수행하거나 문제를 해결하려면 Firepower 4100 FXOS 관리 프로그램 CLI에서 Firepower Threat Defense CLI에 액세스할 수 있습니다.

절차

1. 콘솔 포트에서 또는 SSH를 사용하여 관리 프로그램 CLI에 연결합니다.
2. 보안 모듈 중 하나에 연결합니다.

connect module *slot* **console**

예:

```
cisco-ssp-A# connect module 1 console
firepower>
```

3. 모듈에 처음 연결하는 경우 firepower 프롬프트에서 FirePOWER Chassis Manager CLI로 들어갑니다. 그런 다음 Firepower Threat Defense CLI에 연결해야 합니다.

   connect ftd

   예:

   ```
   firepower> connect ftd
   >
   ```

   다음에 연결하면 Firepower Threat Defense CLI로 직접 이동합니다.

4. Firepower Threat Defense 연결을 종료하려면 **exit**를 입력합니다.

   예:

   ```
   > exit
   firepower>
   ```

5. 시스템 진단에 액세스하려면 **system support diagnostic-cli**를 입력합니다.

   예:

   ```
   firepower> system support diagnostic-cli
   ```

6. 콘솔 연결을 종료하려면 **~**를 입력합니다. 텔넷 애플리케이션을 종료합니다. **quit**를 입력하여 관리 프로그램 CLI를 종료합니다.

   예:

   ```
   firepower> ~
   telnet> quit
   cisco-ssp-A#
   ```

7. 다음으로 살펴볼 내용

- Firepower 4100 설명서에서 모든 Firepower 4100 설명서 링크를 찾을 수 있습니다.