Threat Defense CDO를 이용한 구축

이 장의 설명이 유용합니까?

사용 가능한 모든 운영 체제 및 관리자를 보려면 어떤 운영 체제 및 관리자가 적합합니까? 항목을 참조하십시오. 이 장은 CDO의 온보딩 마법사 또는 LTP(Low-Touch Provisioning)를 사용하는 threat defense(CDO 포함)에 적용됩니다. LTP는 threat defense가 Cisco Cloud에 성공적으로 연결한 후 네트워크 관리자로 하여금 방화벽을 브랜치 오피스에 직접 전달하고, 방화벽을 CDO에 추가한 다음 관리할 수 있도록 하여 새 방화벽 구축을 간소화합니다.

CDO는 일관성 있는 정책 구현을 위해 고도로 분산된 환경에서 보안 정책을 쉽게 관리할 수 있는 클라우드 기반 다중 디바이스 관리자입니다. CDO에서는 불일치를 식별하고 수정 툴을 제공하여 보안 정책을 최적화하는 데 도움을 줍니다. CDO에서는 개체 및 정책을 공유하고 컨피그레이션 템플릿을 만들어 디바이스 전반에서 정책 일관성을 유지할 수 있는 방법을 제공합니다.

방화벽 정보

하드웨어는 ASA 소프트웨어 또는 threat defense 소프트웨어를 실행할 수 있습니다. ASA와 threat defense 간 전환하려면 디바이스에 이미지를 재설치해야 합니다. 현재 설치된 것과 다른 소프트웨어 버전이 필요한 경우에도 이미지를 재설치해야 합니다. Cisco ASA 또는 Firepower Threat Defense 디바이스 이미지 재설치를 참조하십시오.

방화벽은 Secure Firewall eXtensible Operating System(FXOS)라는 기본 운영 체제를 실행합니다. 방화벽은 FXOS Secure Firewall 섀시 관리자를 지원하지 않습니다. 문제 해결을 위해 제한된 CLI만 지원됩니다. 자세한 내용은 Firepower Threat Defense를 실행하는 Firepower 1000/2100 Series용 Cisco FXOS 문제 해결 가이드을 참조하십시오.

Privacy Collection Statement(개인정보 수집 선언**)**—방화벽은 개인 식별 정보를 요구하거나 적극적으로 수집하지 않습니다. 그러나 구성에서 개인 식별이 가능한 정보(예: 사용자 이름)를 사용할 수 있습니다. 이 경우 관리자는 해당 설정으로 작업하거나 SNMP를 사용할 때 이 정보를 확인할 수도 있습니다.

- 로우 터치(Low-Touch) 프로비저닝을 위한 방화벽 구축, 2 페이지
- CDO의 온보딩 마법사를 위한 방화벽 구축, 7 페이지
- CDO 관리자 온보딩 및 관리, 23 페이지

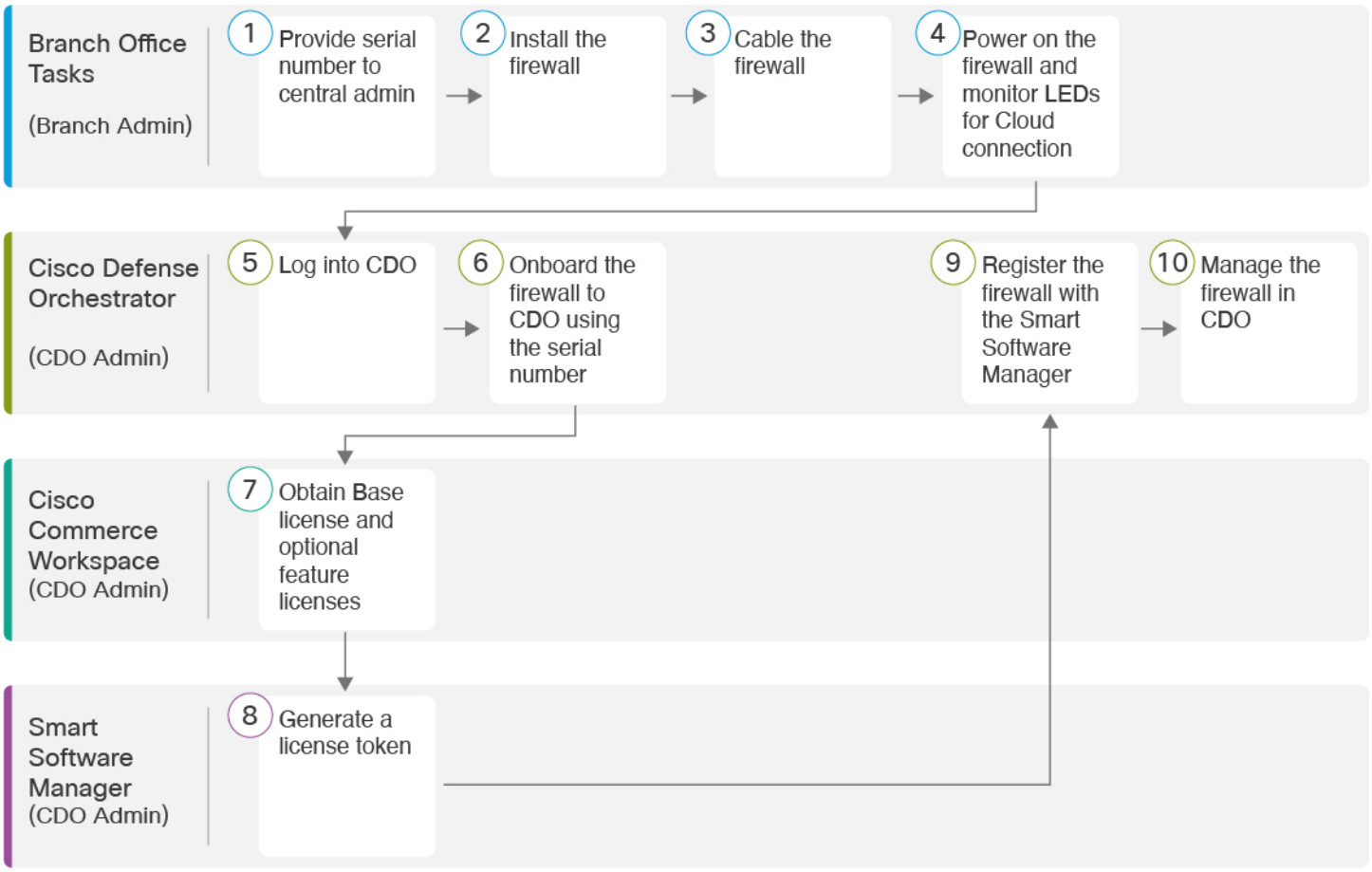
로우 터치(Low-Touch) 프로비저닝을 위한 방화벽 구축

이 섹션에서는 브랜치 오피스에서 구성을 수행할 필요 없이 방화벽을 설치하는 방법을 설명합니다. 그런 다음 CDO 관리자는 방화벽을 원격으로 온보딩할 수 있습니다.

로우 터치(Low-Touch) 프로비저닝을 위한 엔드 투 엔드 절차

새시에 CDO와 함께 threat defense을 구축하려면 다음 작업을 참조하십시오.

그림 *1:* 엔드 투 엔드 절차



1	브랜치 오피스 작업 (브랜치 관리자)	중앙 관리자에게 방화벽 일련 번호 제공, 4 페이지.
2	브랜치 오피스 작업 (브랜치 관리자)	방화벽을 설치합니다. 하드웨어 설치 가이드를 참조하십시오.

3	브랜치 오피스 작업 (브랜치 관리자)	방화벽 케이블 연결, 4 페이지.
4	브랜치 오피스 작업 (브랜치 관리자)	방화벽 켜기, 5 페이지.
5	Cisco Defense Orchestrator (CDO 관리자)	CDO 로그인, 23 페이지.
6	Cisco Defense Orchestrator (CDO 관리자)	로우 터치(Low-Touch) 프로비저닝 및 일련 번호를 사용하여 Threat Defense 온보드, 27 페이지에 전달하는 고성능 고속 어플라이언스입니다.
7	Cisco Commerce Workspace (CDO 관리자)	Base 라이선스 및 선택적 기능 라이선스를 얻습니다().라이선싱 구성, 34 페이지
8	Smart Software Manager (CDO 관리자)	라이선스 토큰을 생성합니다(라이선싱 구성, 34 페이지).
9	Cisco Defense Orchestrator (CDO 관리자)	Smart Licensing Server에 디바이스를 등록합니다(라이선싱 구성, 34 페이지).
10	Cisco Defense Orchestrator (CDO 관리자)	CDO에서 Threat Defense 구성, 39 페이지.

지사 설치

회사 IT 부서에서 threat defense을(를) 받은 후에는 방화벽의 일련 번호를 기록하고 CDO 관리자에게 전송해야 합니다. 온보딩 프로세스에 대한 커뮤니케이션 계획을 간략하게 설명합니다. 완료해야 할 주요 작업을 포함하고 각 항목에 대한 연락처를 제공합니다.

그런 다음 외부 인터페이스에서 인터넷에 액세스할 수 있도록 방화벽에 케이블을 연결하고 전원을 켜면 됩니다. 그 후에 CDO 관리자는 온보딩 프로세스를 완료할 수 있습니다.

팁 이 비디오를 시청하고 브랜치 직원이 CDO 및 로우 터치 프로비저닝을 사용하여 방화벽을 온보드 하는 방법을 확인할 수 있습니다.

중앙 관리자에게 방화벽 일련 번호 제공

방화벽을 랙에 배치하거나 배송 상자를 폐기하기 전에 하고 중앙 관리자와 조정할 수 있도록 일련 번호를 기록합니다.

프로시저

단계 **1** 섀시 및 섀시 구성 요소의 포장을 풉니다.

방화벽에 케이블 또는 전원을 연결하기 전에 방화벽 및 패키지의 인벤토리를 확인합니다. 또한 섀시 레이아웃, 구성 요소 및 LED를 숙지 해야 합니다.

단계 **2** 방화벽의 일련 번호를 기록합니다.

방화벽의 일련 번호는 배송 상자에서 확인할 수 있습니다. 방화벽 후면의 방화벽 섀시 하단에 있는 스티커

단계 **3** 방화벽 일련 번호를 IT 부서/중앙 본사의 CDO 네트워크 관리자에게 전송합니다.

네트워크 관리자는 로우 터치(low-touch) 프로비저닝을 용이하게 하고, 방화벽에 연결하고, 원격으로 구성하려면 방화벽 일련 번호가 필요합니다.

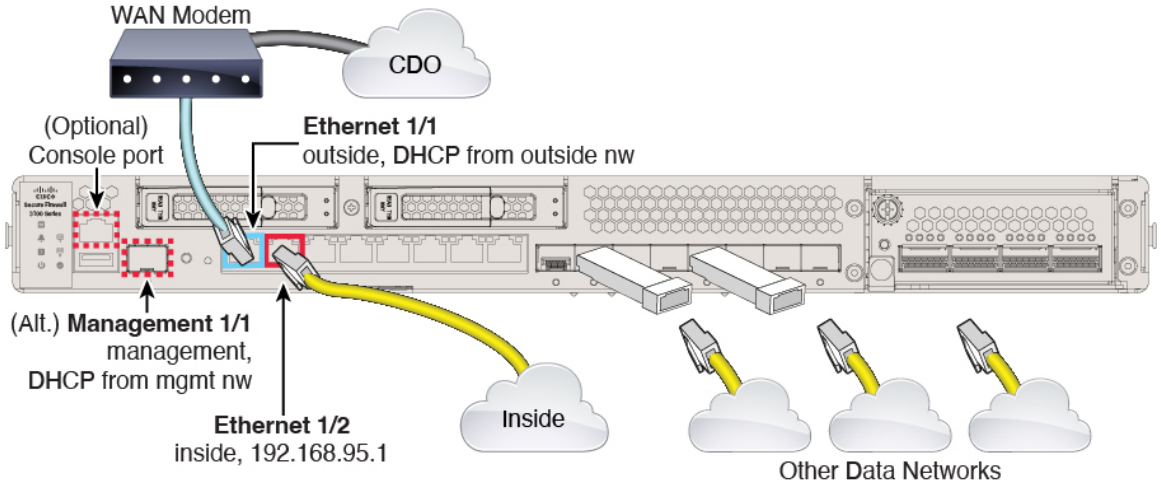
CDO 관리자와 통신하여 온보딩 타임라인을 개발합니다.

방화벽 케이블 연결

이 항목에서는 CDO 관리자가 네트워크를 원격으로 관리할 수 있도록 Secure Firewall 3100을(를) 네트워크에 연결하는 방법을 설명합니다.

브랜치 오피스에서 방화벽을 받았고 네트워크에 연결 하는 것이 직무인 경우 이 비디오를 시청하십시오. 이 비디오에서는 방화벽 및 방화벽의 상태를 나타내는 방화벽의 LED 시퀀스에 대해 설명합니다. 필요한 경우 LED를 확인하여 IT 부서와 함께 방화벽 상태를 확인할 수 있습니다.

그림 *2: Secure Firewall 3100* 케이블 연결



로우 터치(low-touch) 프로비저닝은 이더넷 1/1(외부)의 CDO에 대한 연결을 지원합니다. 또는 Management 1/1 인터페이스에서 로우 터치(low-touch) 프로비저닝을 사용할 수 있습니다.

프로시저

단계 **1** 섀시를 설치합니다. 하드웨어 설치 가이드를 참조하십시오.

단계 **2** 이더넷 1/1 인터페이스의 네트워크 케이블을 WAN(광역 네트워크) 모뎀에 연결합니다. WAN 모뎀은 인터넷에 대한 브랜치의 연결이며 인터넷에 대한 방화벽의 경로이기도 합니다.

참고 또는 방화벽의 Management 1/1 인터페이스에서 WAN으로 네트워크 케이블을 연결할 수 있습니다. 어떤 인터페이스를 사용하든 인터넷에 대한 경로가 있어야 합니다. CLI에서 IP 주소를 수동으로 설정하는 경우 관리 인터페이스는 IPv6를 지원합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 18 페이지의 내용을 참조하십시오. 외부 Ethernet 1/1 인터페이스는 로우 터치(low-touch) 프로비저닝에서만 IPv4를 지원합니다.

단계 **3** 내부 네트워크를 이더넷 1/2에 연결합니다.

단계 **4** 나머지 인터페이스에 다른 네트워크를 연결합니다.

방화벽 켜기

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

참고 처음 threat defense 부팅 시에는 초기화에 약 15~30분이 소요될 수 있습니다.

시작하기 전에

디바이스에 안정적인 전원을 제공하는 것이 중요합니다(예: UPS(Uninterruptable Power Supply) 사용). 먼저 셧다운하지 않고 전력이 손실되면 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전력이 손실되면 시스템이 정상적으로 종료되지 않습니다.

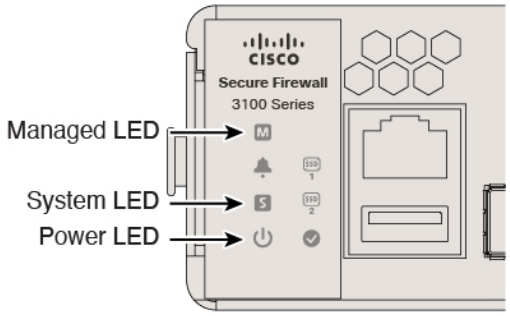
프로시저

단계 **1** 전원 케이블을 디바이스에 연결하고 전기 콘센트에 꽂습니다.

단계 **2** 전원 코드 옆 섀시 후면에 있는 표준 로커 유형 전원 켜기/끄기 스위치를 사용하여 전원을 켭니다.

단계 **3** 방화벽 뒷면의 전원 LED를 확인합니다. 전원이 켜져 있으면 녹색으로 표시됩니다.

그림 ***3:*** 관리형 ***LED,*** 전원 및 시스템 ***LED***



단계 **4** 방화벽 뒷면의 시스템 LED를 확인합니다. 시스템이 전원 켜기 진단을 통과하면 녹색으로 표시됩니다.

참고 스위치가 ON(켜짐)에서 OFF(꺼짐)로 토글된 경우 시스템에서 최종적으로 전원이 꺼지는 데 몇 초 정도가 걸릴 수 있습니다. 이 시간 동안 섀시 전면에 있는 전원 LED가 녹색으로 깜박입니다. 전원 LED가 완전히 꺼질 때까지 전원을 제거하지 마십시오.

단계 **5** 방화벽 후면의 관리형 LED를 확인합니다. 방화벽이 Cisco 클라우드에 연결되면 관리형 LED가 녹색으로 천천히 깜박입니다.

문제가 있는 경우 Managed LED가 황색과 녹색으로 깜박이며 방화벽이 Cisco Cloud에 연결되지 않았음을 나타냅니다. 이 패턴이 표시되면 네트워크 케이블이 이더넷 1/1 인터페이스 및 WAN 모뎀에 연결되어 있는지 확인합니다. 네트워크 케이블을 조정한 후 약 10분이 지나도 방화벽이 Cisco 클라우드에 연결되지 않으면 IT 부서에 문의하십시오.

다음에 수행할 작업

- IT 부서와 통신하여 온보딩 타임라인 및 활동을 확인합니다. 중앙 본사의 CDO 관리자와 통신 계획을 세워야 합니다.
- 이 작업을 완료하면 CDO 관리자가 방화벽을 원격으로 구성하고 관리할 수 있습니다. 다 됐습니다.

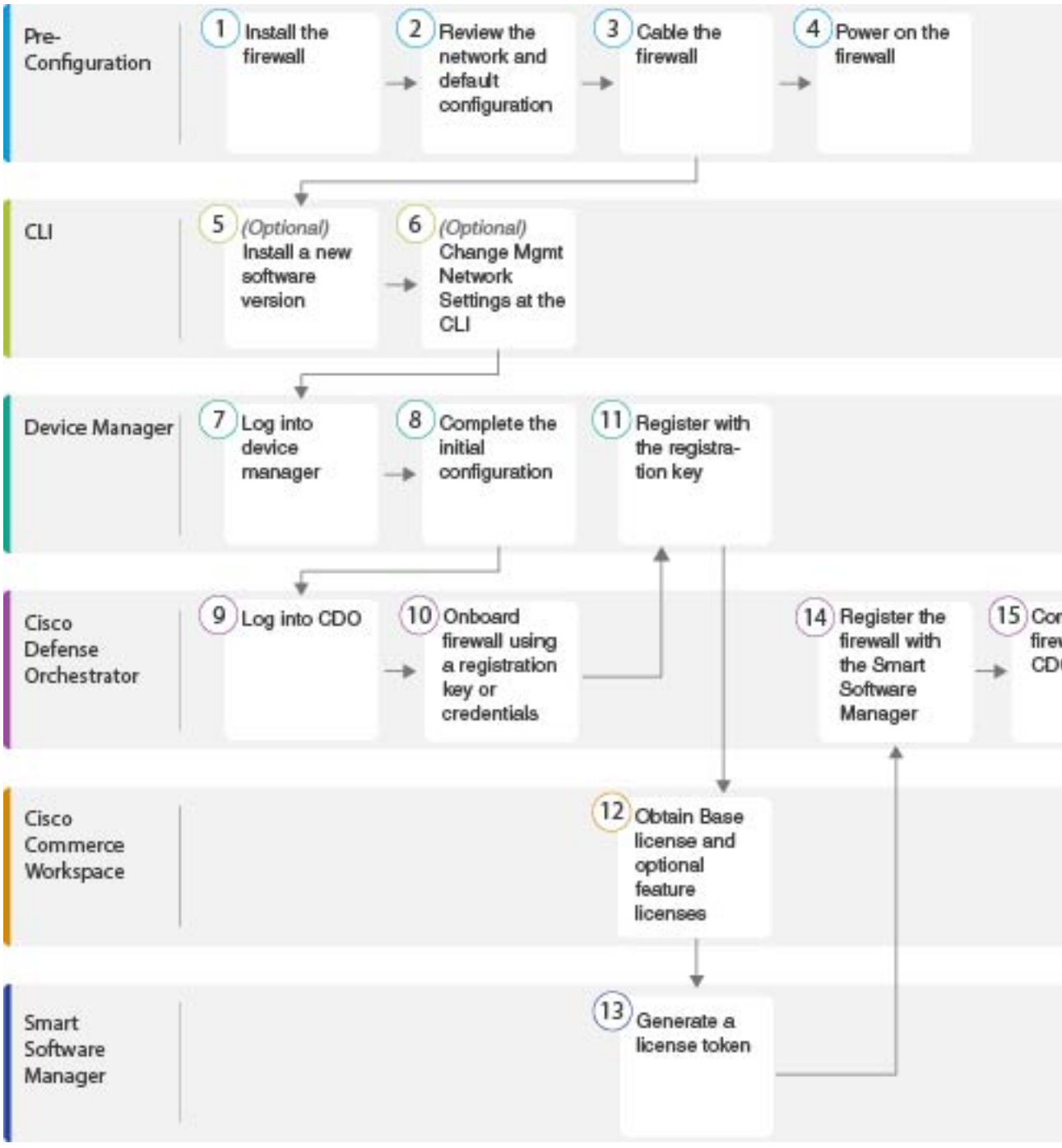
CDO의 온보딩 마법사를 위한 방화벽 구축

이 섹션에서는 CDO의 온보딩 마법사를 사용하여 온보딩을 위해 방화벽을 구성하는 방법을 설명합니다.

CDO 온보딩 마법사를 위한 엔드 투 엔드 절차

CDO 온보딩 마법사를 사용하여 새시에 CDO와 함께 threat defense을 구축하려면 다음 작업을 참조하십시오.

그림 4: 엔드 투 엔드 절차



1	사전 컨피그레이션	방화벽을 설치합니다. 하드웨어 설치 가이드
2	사전 컨피그레이션	네트워크 구축 및 기본 구성 검토, 10 페이지에 전달하는 고성능 고속 어플라이언스입니다.

3	사전 컨피그레이션	방화벽 케이블 연결, 14 페이지에 전달하는 고성능 고속 어플라이언스입니다.
4	사전 컨피그레이션	방화벽 켜기, 16 페이지에 전달하는 고성능 고속 어플라이언스입니다.
5	CLI	(선택 사항) 소프트웨어 확인 및 새 버전 설치, 17 페이지
6	CLI	(선택 사항) CLI에서 관리 네트워크 설정 변경, 18 페이지.
7	Device Manager	Device Manager에 로그인, 20 페이지.
8	Device Manager	초기 컨피그레이션 완료, 21 페이지.
9	Cisco Defense Orchestrator	Cisco Secure Sign-On을 사용하여 CDO에 로그인, 26 페이지.
10	Cisco Defense Orchestrator	등록 키 또는 크리덴셜을 사용하여 디바이스를 온보딩합니다(CDO에 Threat Defense 온보드, 27 페이지).
11	Device Manager	등록 키를 사용하여 등록합니다(CDO에 Threat Defense 온보드, 27 페이지). 자격 증명을 사용하여 온보딩하는 경우 (device manager)에 로그인할 필요가 없습니다.
12	Cisco Commerce Workspace	(선택 사항) (라이선싱 구성, 34 페이지)기능 라이선스를 가져옵니다.
13	Smart Software Manager	라이선스 토큰을 생성합니다(라이선싱 구성, 34 페이지).
14	Cisco Defense Orchestrator	Smart Licensing Server에 디바이스를 등록합니다(라이선싱 구성, 34 페이지).
15	Cisco Defense Orchestrator	CDO에서 Threat Defense 구성, 39 페이지.

CDO와 Threat Defense의 작동 방식

CDO 및 Device Manager 공동 관리

device manager에서 초기 구성을 완료하여 인터넷 연결을 설정하고 기본 네트워크 정책을 구성한 후에는 디바이스를 CDO에 온보딩할 수 있습니다. 디바이스를 CDO에 온보딩한 후에는 필요에 따라 device manager를 계속 사용할 수 있습니다. 사례별로 CDO에서 대역 외 변경 사항을 수락할지 여부를 선택할 수 있습니다.

SDC(Secure Device Connector)

CDO와 여기에서 관리하는 디바이스 간의 모든 통신은 SDC를 통과합니다.CDO 관리하는 디바이스는 직접 통신하지 않습니다.

SDC는 다음 방법을 사용하여 클라우드 또는 네트워크에 구축할 수 있습니다.

- Cloud Secure Device Connector - CDO 지원 팀은 테넌트가 생성될 때 모든 테넌트에 대해 클라우드 기반 SDC를 구축합니다.
- 온프레미스 보안 디바이스 커넥터 - 온프레미스 SDC는 네트워크에 설치된 가상 어플라이언스입니다. 자격 증명 기반 온보딩을 사용하는 경우 온프레미스 SDC를 사용하는 것이 좋습니다. 클라우드 SDC를 대신 사용하는 경우 클라우드 SDC에서 인터페이스의 HTTPS 액세스를 허용해야 하며, 이는 CDO 관리에 있습니다. 일반적인 네트워크 구축에서는 외부 인터페이스에서 HTTPS 액세스를 활성화해야 합니다. 이렇게 하면 보안 위험이 발생할 수 있으며 VPN 클라이언트 종료를 위해 외부 인터페이스를 사용할 수 없게 됩니다. threat defense

(크리덴셜 기반 온보딩의 경우) 네트워크에 대한 액세스 권한을 부여해야 할 수 있는 온프레미스 SDC 및 클라우드 SDC IP 주소를 설치하기 위한 링크를 비롯한 자세한 내용은 SDC(Security Device Connector)를 참조하십시오.

CDO 온보딩 방법

다음과 같은 방법으로 디바이스를 온보딩할 수 있습니다.

- 등록 키(권장) - 특히 디바이스가 IP 주소를 가져오기 위해 DHCP를 사용하는 경우 이 방법을 사용하는 것이 좋습니다. 해당 IP 주소가 변경되어도 디바이스는 CDO에 연결된 상태로 유지됩니다.
- 자격 증명(사용자 이름 및 비밀번호) 및 IP 주소 - 디바이스 관리자 사용자 이름 및 비밀번호와 고정 IP 주소 또는 FQDN을 사용하여 threat defense 온보딩이 가능합니다. 이 방법의 경우 내부인터페이스에 연결된 온프레미스 SDC를 사용하는 것이 좋습니다.
- 일련 번호 - device manager를 사용하여 디바이스를 사전 구성할 필요가 없는 프로비저닝의 경우 손쉬운 프로비저닝 섹션을 참조하십시오. device manager에서 디바이스 구성을 이미 시작한 경우 일련 번호를 사용하여 온보딩할 수도 있습니다. 이 방법은 이 가이드에서 다루지 않습니다. 자세한 내용은 디바이스의 일련 번호를 사용하여 FTD 온보딩을 참조하십시오.

네트워크 구축 및 기본 구성 검토

관리 1/1 인터페이스 또는 내부 인터페이스에서 device manager를 사용하여 threat defense의 초기 설정을 수행할 수 있습니다. 전용 관리 인터페이스는 트래픽의 통과를 허용하지 않으며 자체 네트워크 설정이 있는 특수 인터페이스입니다.

SDC(Secure Device Connector) 유형 및 온보딩 방법에 따라 다음과 같은 일반적인 네트워크 구축을 참조하십시오.

클라우드 **SDC** 네트워크**,** 등록 키 온보딩

다음 그림에는 클라우드 SDC를 사용한 등록 키 온보딩에 권장되는 네트워크 구축이 나와 있습니다. 등록 키 온보딩과 함께 온프레미스 SDC를 사용할 수 있지만, 이 예에서는 더 일반적인 클라우드 SDC 활용 사례를 보여줍니다. 클라우드 SDC에서 크리덴셜 기반 온보딩을 사용할 수도 있지만, 이 방법을 사용하려면 device manager에서 추가 구성이 필요하므로 바람직하지 않을 수 있습니다.

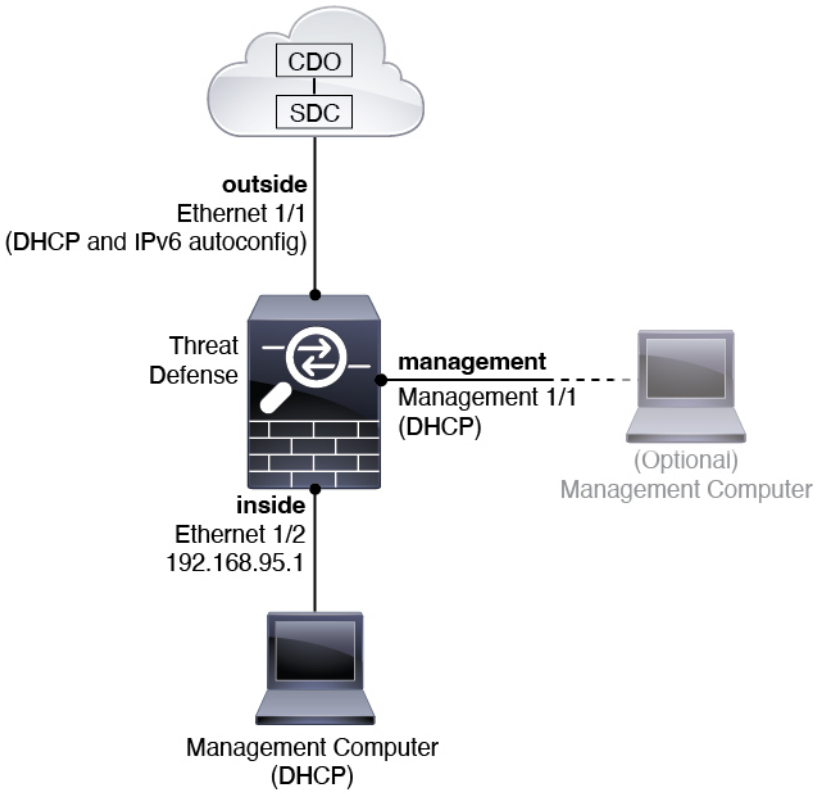
외부 인터페이스를 케이블 모뎀 또는 DSL 모뎀에 직접 연결하는 경우에는 threat defense가 내부 네트워크에 대해 모든 라우팅 및 NAT를 수행하도록 모뎀을 브리지 모드로 설정하는 것이 좋습니다.ISP에 연결하기 위해 외부 인터페이스에 대해 PPPoE를 구성해야 하는 경우 device manager 설정을 마친 뒤 수행할 수 있습니다.

참고 기본 관리 또는 IP 주소를 사용할 수 없는 경우(예: , 관리 네트워크에 DHCP 서버가 포함되지 않는 경우), 콘솔 포트에 연결하고 CLI에서 초기 설정을 수행할 수 있습니다. 이러한 설정에는 관리 IP 주소, 게이트웨이 및 기타 기본적인 네트워킹 설정이 포함됩니다.

내부 IP 주소를 변경해야 하는 경우 device manager에서 초기 설정을 완료한 후 변경할 수 있습니다. 예를 들어 다음과 같은 상황에서는 내부 IP 주소를 변경해야 할 수 있습니다.

- 내부 IP 주소는 192.168.95.1입니다.
- 기존 내부 네트워크에 threat defense를 추가하는 경우 내부 IP 주소를 기존 네트워크에 있도록 변경해야 합니다.

그림 ***5:*** 제안된 네트워크 구축 클라우드 ***SDC***



온프레미스 **SDC** 네트워크**,** 자격 증명 온보딩

다음 그림에는 내부 네트워크에 연결된 온프레미스 SDC를 사용하여 자격 증명 온보딩에 권장되는 네트워크 구축이 나와 있습니다. 크리덴셜 온보딩과 함께 클라우드 SDC를 사용할 수 있지만, 이 방법을 사용하려면 device manager에서 추가 구성이 필요하므로 바람직하지 않을 수 있습니다. 이 예는 더 일반적인 온프레미스 SDC 활용 사례를 보여줍니다. 통과 트래픽을 허용 하지 않는 선택적 관리 네트워크에 SDC를 추가 하는 경우 SDC에는 인터넷에 대 한 경로가 필요 합니다 (다이어그램에 표시 되지 않음).

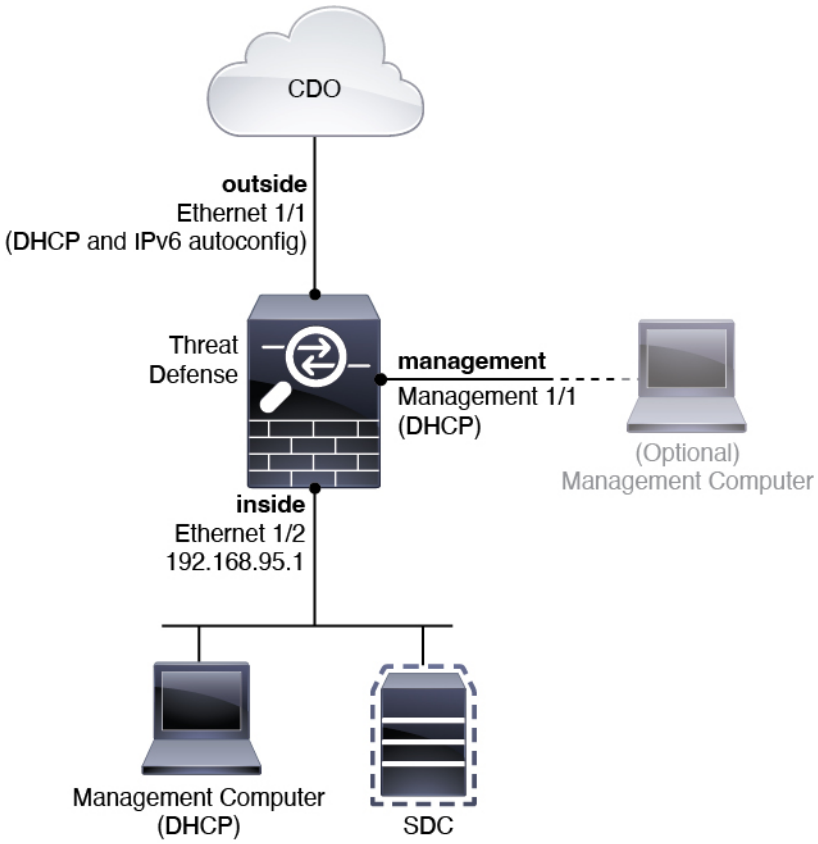
외부 인터페이스를 케이블 모뎀 또는 DSL 모뎀에 직접 연결하는 경우에는 threat defense가 내부 네트워크에 대해 모든 라우팅 및 NAT를 수행하도록 모뎀을 브리지 모드로 설정하는 것이 좋습니다.ISP에 연결하기 위해 외부 인터페이스에 대해 PPPoE를 구성해야 하는 경우 device manager 설정을 마친 뒤 수행할 수 있습니다.

참고 기본 관리 또는 IP 주소를 사용할 수 없는 경우(예: , 관리 네트워크에 DHCP 서버가 포함되지 않는 경우), 콘솔 포트에 연결하고 CLI에서 초기 설정을 수행할 수 있습니다. 이러한 설정에는 관리 IP 주소, 게이트웨이 및 기타 기본적인 네트워킹 설정이 포함됩니다.

내부 IP 주소를 변경해야 하는 경우 device manager에서 초기 설정을 완료한 후 변경할 수 있습니다. 예를 들어 다음과 같은 상황에서는 내부 IP 주소를 변경해야 할 수 있습니다.

- 내부 IP 주소는 192.168.95.1입니다.
- 기존 내부 네트워크에 threat defense를 추가하는 경우 내부 IP 주소를 기존 네트워크에 있도록 변경해야 합니다.

그림 6: 제안된 네트워크 구축 온프레미스 SDC



기본 구성

초기 설정 후 방화벽 구성에는 다음이 포함됩니다.

- 내부—이더넷 1/2, IP 주소192.168.95.1.
- 외부—이더넷 1/1, IPv4 DHCP 및 IPv6 자동 구성의 IP 주소
- 내부→외부 트래픽 흐름
- 관리—관리 1/1 (관리), DHCP에서 제공된 IP 주소

참고 관리 1/1 인터페이스는 관리, Smart Licensing 및 데이터베이스 업데이트에 사용되는 데이터 인터페이스와 분리된 특수 인터페이스입니다. 물리적 인터페이스는 두 번째 논리적 인터페이스인 진단 인터페이스와 공유됩니다. 진단은 데이터 인터페이스이지만 syslog 또는 SNMP와 같은 다른 유형의 관리 트래픽(디바이스 간 및 디바이스 내)으로 제한됩니다. 진단 인터페이스는 일반적으로 사용되지 않습니다. 자세한 내용은 Cisco Secure Firewall Device Manager 구성 가이드을 참조하십시오.

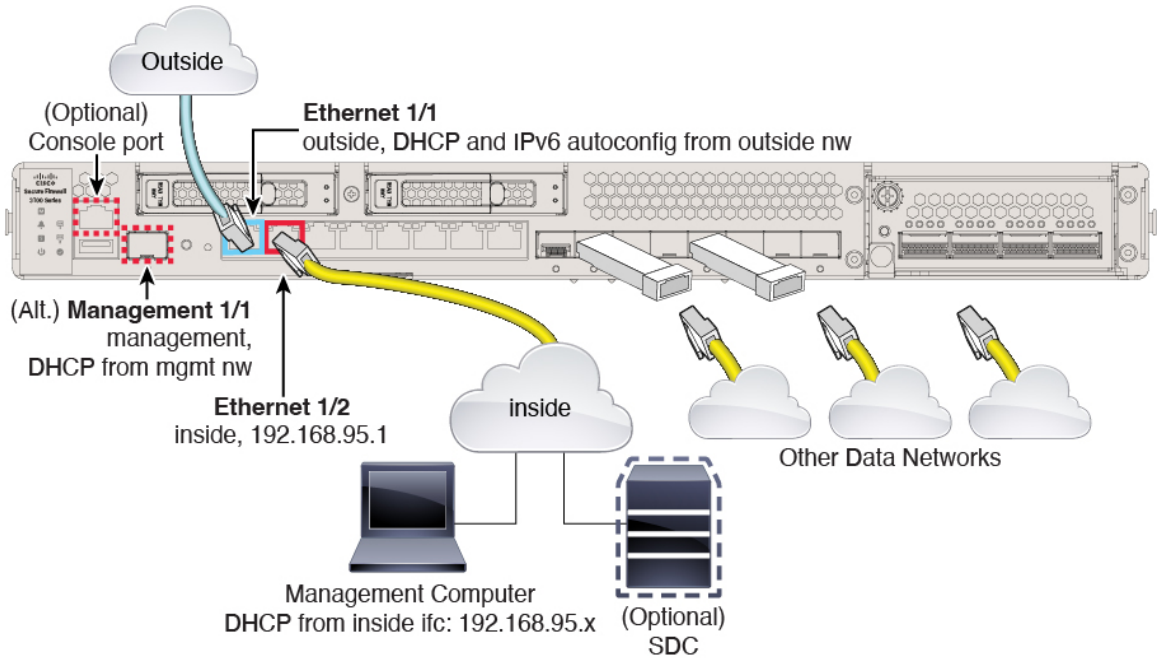
- 관리용 **DNS** 서버 - OpenDNS: (IPv4) 208.67.222.222, 208.67.220.220, (IPv6) 2620:119:35::35 또는 설정 도중 지정한 서버. DHCP에서 가져온 DNS 서버는 사용되지 않습니다.
- **NTP**—Cisco NTP 서버인 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org 또는 설정 중에 지정한 서버
- 기본 경로
  - 데이터 인터페이스—외부 DHCP에서 가져온 주소 또는 설정 중에 지정한 게이트웨이 IP 주소
  - 관리 인터페이스—관리 DHCP에서 가져온 것입니다. 게이트웨이를 수신하지 않는 경우 기본 경로는 백플레인과 데이터 인터페이스를 사용합니다.

    관리 인터페이스는 백플레인을 통해 또는 별도의 인터넷 게이트웨이를 사용하여 라이선싱 및 업데이트하도록 인터넷 액세스가 필요합니다. 관리 인터페이스에서 시작되는 트래픽만 백플레인을 통과할 수 있습니다. 그렇지 않은 경우 관리는 네트워크에서 관리로 들어가는 트래픽에 대한 트래픽 통과를 허용하지 않습니다.
- **DHCP** 서버—내부 인터페이스에서 활성화
- **Device Manager** 액세스—관리 및 내부 인터페이스에서 허용되는 모든 호스트.
- **NAT**—내부에서 외부로 가는 모든 트래픽을 위한 인터페이스 PAT

방화벽 케이블 연결

이 항목에서는 CDO 관리자가 네트워크를 원격으로 관리할 수 있도록 Secure Firewall 3100을(를) 네트워크에 연결하는 방법을 설명합니다.

그림 *7: Secure Firewall 3100* 케이블 연결



관리 1/1 또는 이더넷 1/2에서 Secure Firewall 3100를 관리합니다. 기본 구성에서는 Ethernet1/1을 외부로도 구성합니다.

프로시저

단계 **1** 섀시를 설치합니다. 하드웨어 설치 가이드를 참조하십시오.

단계 **2** 다음 인터페이스 중 하나에 관리 컴퓨터를 연결합니다.

- Ethernet 1/2 — 관리 컴퓨터를 초기 컨피그레이션용 Ethernet 1/2에 직접 연결하거나, Ethernet 1/2를 내부 네트워크에 연결합니다. 기본 IP 주소(192.168.95.1)가 있는 이더넷 1/2에서는 DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로, 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다(기본 구성, 13 페이지 참조).
- 관리 1/1—관리 1/1을 관리 네트워크에 연결하고 관리 컴퓨터가 켜져 있는지, 또는 관리 네트워크에 대한 액세스 권한이 있는지 확인합니다. 관리 1/1은 관리 네트워크의 DHCP 서버에서 IP 주소를 가져옵니다. 이 인터페이스를 사용하는 경우 관리 컴퓨터에서 해당 IP 주소에 연결할 수 있도록 방화벽에 할당된 IP 주소를 확인해야 합니다.

  Management 1/1 IP 주소를 기본값에서 변경하여 정적 IP 주소를 구성해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 18 페이지의 내용을 참조하십시오.

  참고 관리 1/1은 SFP 모듈이 필요한 10Gb 파이버 인터페이스입니다.

나중에 다른 인터페이스에서 device manager 관리 액세스를 구성할 수 있습니다. FDM 일반 운영 구성 가이드를 참조하십시오.

단계 **3** 선택 사항인 온프레미스 SDC(Secure Device Connector)를 내부 네트워크에 연결합니다.

단계 **4** Ethernet1/1 인터페이스에 외부 네트워크를 연결합니다.

기본적으로는 IPv4 DHCP 및 IPv6 자동 설정을 사용하여 IP 주소를 가져오지만 초기 설정 중에 고정 주소를 설정할 수 있습니다.

단계 **5** 나머지 인터페이스에 다른 네트워크를 연결합니다.

방화벽 켜기

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

참고 처음 threat defense 부팅 시에는 초기화에 약 15~30분이 소요될 수 있습니다.

시작하기 전에

디바이스에 안정적인 전원을 제공하는 것이 중요합니다(예: UPS(Uninterruptable Power Supply) 사용). 먼저 셧다운하지 않고 전력이 손실되면 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전력이 손실되면 시스템이 정상적으로 종료되지 않습니다.

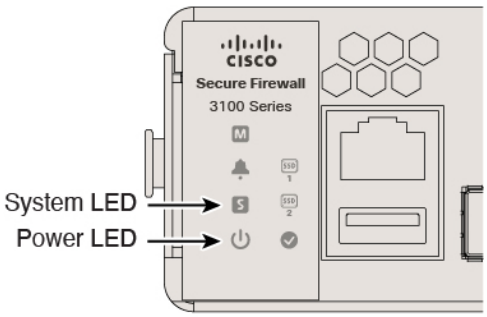
프로시저

단계 **1** 전원 케이블을 디바이스에 연결하고 전기 콘센트에 꽂습니다.

단계 **2** 전원 코드 옆 섀시 후면에 있는 표준 로커 유형 전원 켜기/끄기 스위치를 사용하여 전원을 켭니다.

단계 **3** 방화벽 뒷면의 전원 LED를 확인합니다. 전원이 켜져 있으면 녹색으로 표시됩니다.

그림 ***8:*** 시스템 및 전원 ***LED***



단계 **4** 방화벽 뒷면의 시스템 LED를 확인합니다. 시스템이 전원 켜기 진단을 통과하면 녹색으로 표시됩니다.

참고 스위치가 ON(켜짐)에서 OFF(꺼짐)로 토글된 경우 시스템에서 최종적으로 전원이 꺼지는 데 몇 초 정도가 걸릴 수 있습니다. 이 시간 동안 섀시 전면에 있는 전원 LED가 녹색으로 깜박입니다. 전원 LED가 완전히 꺼질 때까지 전원을 제거하지 마십시오.

(선택 사항) 소프트웨어 확인 및 새 버전 설치

소프트웨어 버전을 확인하고 필요한 경우 다른 버전을 설치하려면 다음 단계를 수행합니다. 방화벽을 구성하기 전에 대상 버전을 설치하는 것이 좋습니다. 또는 가동을 시작한 후 업그레이드를 수행할 수 있지만, 구성을 유지하는 업그레이드는 이 절차를 사용하는 것보다 시간이 더 오래 걸릴 수 있습니다.

어떤 버전을 실행해야 합니까**?**

Cisco는 소프트웨어 다운로드 페이지에서 릴리스 번호 옆에 금색 별표로 표시된 Gold Star 릴리스를 실행할 것을 권장합니다. https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html에 설명된 릴리스 전략을 참조할 수도 있습니다. 예를 들어, 이 게시판에서는 단기 릴리스 번호 지정(최신 기능 포함), 장기 릴리스 번호 지정(장기간 유지 보수 릴리스 및 패치) 또는 추가 장기 릴리스 번호 지정(가장 긴 기간, 정부 인증) 등이 있습니다.

프로시저

단계 **1** CLI에 연결합니다. 자세한 내용은 Threat Defense 및 FXOS CLI 액세스, 43 페이지를 참조하십시오. 이 절차에서는 콘솔 포트를 사용하는 방법을 보여 주지만 SSH를 대신 사용할 수 있습니다.

관리자 사용자(비밀번호: **Admin123**)로 로그인합니다.

FXOS CLI에 연결합니다. 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 threat defense 로그인에도 사용됩니다.

참고 비밀번호가 이미 변경된 경우 모르는 경우, 비밀번호를 기본값으로 재설정하려면 디바이스를 재 이미지화해야합니다. 이미지 재설치 절차는 FXOS 문제 해결 설명서를 참조하십시오.

예제**:**

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]
```

```
firepower#
```

단계 **2** FXOS CLI에서 실행 중인 버전을 표시합니다.

scope ssa

show app-instance

예제:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.1.0.65        7.1.0.65
        Not Applicable
```

단계 **3** 새 버전을 설치하려면 다음 단계를 수행합니다.

a) 관리 인터페이스에 대한 고정 IP 주소를 설정해야 하는 경우 (선택 사항) CLI에서 관리 네트워크 설정 변경, 18 페이지를 참조하십시오. 기본적으로 관리 인터페이스는 DHCP를 사용합니다.

관리 인터페이스에서 액세스할 수 있는 서버에서 새 이미지를 다운로드해야 합니다.

b) 이미지 재설치 절차는 FXOS 문제 해결 설명서를 참조하십시오.

(선택 사항) CLI에서 관리 네트워크 설정 변경

기본 관리 IP 주소를 사용할 수 없는 경우 콘솔 포트에 연결하고 CLI에서 관리 IP 주소, 게이트웨이 및 기타 기본적인 네트워킹 설정을 비롯한 초기 설정을 수행할 수 있습니다. 관리 인터페이스 설정만 구성할 수 있습니다. 내부 또는 외부 인터페이스는 구성할 수 없으며 나중에 GUI에서 구성할 수 있습니다.

참고 이미지 재설치 등을 통해 컨피그레이션을 지우지 않으면 CLI 설정 스크립트를 반복할 수 없습니다. 그러나 이러한 모든 설정은 **configure network**(네트워크 구성) 명령을 사용하여 CLI에서 나중에 변경할 수 있습니다. Secure Firewall Threat Defense 명령 참조의 내용을 참조하십시오.

프로시저

단계 **1** threat defense 콘솔 포트에 연결합니다. 자세한 내용은 Threat Defense 및 FXOS CLI 액세스, 43 페이지를 참조하십시오.

관리자 사용자(비밀번호: **Admin123**)로 로그인합니다.

FXOS CLI에 연결합니다. 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 threat defense 로그인에도 사용됩니다.

참고 비밀번호가 이미 변경된 경우 모르는 경우, 비밀번호를 기본값으로 재설정하려면 디바이스를 재 이미지화해야합니다. 이미지 재설치 절차는 FXOS 문제 해결 설명서를 참조하십시오.

예제:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

단계 **2** threat defense CLI에 연결합니다.

connect ftd

예제:

```
firepower# connect ftd
>
```

단계 **3** threat defense에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하고 하라는 메시지가 표시됩니다. 그 다음에는 CLI 설정 스크립트가 표시됩니다.

기본값 또는 이전에 입력한 값이 괄호 안에 표시됩니다. 이전에 입력한 값을 승인하려면 **Enter**를 누릅니다.

다음 지침을 참조하십시오.

- **Enter the IPv4 default gateway for the management interface(**관리 인터페이스의 **IPv4** 기본 게이트웨이 입력**)** — 수동 IP 주소를 설정하는 경우 **data-interfaces** 또는 게이트웨이 라우터의 IP 주소를 입력합니다. **data-interfaces** 설정은 백플레인을 통해 아웃바운드 관리 트래픽을 전송하여 데이터 인터페이스를 종료합니다. 이 설정은 인터넷에 액세스할 수 있는 별도의 관리 네트워크가 없는 경우에 유용합니다. 관리 인터페이스에서 발생하는 트래픽에는 인터넷 액세스가 필요한 라이선스 등록 및 데이터베이스 업데이트가 포함되어 있습니다. **data-interfaces**를 사용하면 관리 네트워크에 직접 연결된 경우 관리 인터페이스에서 device manager(또는 SSH)을 계속 사용할 수 있지만 특정 네트워크 또는 호스트에 대한 원격 관리의 경우 **configure network static-routes** 명령을 사용하여 정적 경로를 추가해야 합니다. 데이터 인터페이스에 대한 device manager 관리는 이 설정의 영향을 받지 않습니다. DHCP를 사용하는 경우 시스템은 DHCP에서 제공하는 게이트웨이를 사용하며, DHCP가 게이트웨이를 제공하지 않는 경우 **data-interfaces**를 대체 방법으로 사용합니다.

- **If your networking information has changed, you will need to reconnect(**네트워킹 정보가 변경된 경우 다시 연결해야 합니다**)** — SSH를 통해 기본 IP 주소에 연결되어 있지만 최초 설정에서 IP 주소를 변경한 경우 연결이 끊깁니다. 새 IP 주소 및 비밀번호를 사용하여 다시 연결합니다. 콘솔 연결에는 영향을 미치지 않습니다.
- **Manage the device locally?(**디바이스를 로컬로 관리하시겠습니까**?)**—device manager 또는 CDO을(를) 사용하려면 **yes**를 입력합니다. 답변이 **no**인 경우, management center를 사용하여 디바이스를 관리함을 의미합니다.

예제**:**

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

단계 **4** 새 관리 IP 주소에서 device manager에 로그인합니다.

다음에 수행할 작업

CLI를 사용하여 관리 네트워크 설정을 변경하려면 EULA에 동의하고 IP 주소를 변경하며 비밀번호를 변경해야 합니다. 초기 구성을 완료합니다(초기 컨피그레이션 완료, 21 페이지 참고).

Device Manager에 로그인

threat defense를 구성하려면 device manager에 로그인합니다. device manager 설정 마법사를 사용하여 디바이스를 CDO에 온보딩하기 전에 초기 구성을 완료합니다.

시작하기 전에

- 최신 버전의 Firefox 또는 Chrome을 사용합니다.

프로시저

단계 **1** 브라우저에 다음 URL을 입력합니다.

- 내부(이더넷 1/2)—**https://192.168.95.1**.
- 관리—**https://***management_ip*. 기본적으로 대부분의 플랫폼에서 관리 인터페이스는 DHCP 클라이언트이므로 IP 주소는 DHCP 서버에 따라 달라집니다. CLI 설정에서 관리 IP 주소를 변경한 경우 해당 주소를 입력합니다.

단계 **2** 사용자 이름 **admin** 및 기본 비밀번호 **Admin123**으로 로그인합니다.

다음에 수행할 작업

- device manager 설정 마법사를 통해 실행합니다. 초기 컨피그레이션 완료, 21 페이지를 참조하십시오.

초기 컨피그레이션 완료

초기 설정을 완료하기 전에 처음으로 device manager에 로그인할 때 설정 마법사를 사용합니다. 설치 마법사를 완료하고 나면 작동 중인 디바이스에 몇 가지 기본 정책이 갖추어져 있어야 합니다.

- 외부(Ethernet1/1) 및 내부 인터페이스 (Ethernet1/2).
- 내부 및 외부 인터페이스용 보안 영역
- 내부에서 외부로 이동하는 모든 트래픽을 신뢰하는 액세스 규칙
- 내부에서 외부로 이동하는 모든 트래픽을 외부 인터페이스의 IP 주소에 있는 고유한 포트로 변환하는 인터페이스 NAT 규칙입니다.
- 내부 인터페이스에서 실행 중인 DHCP 서버입니다.

참고 (선택 사항) CLI에서 관리 네트워크 설정 변경, 18 페이지 절차를 수행한 경우 이러한 작업 중 일부, 특히 관리자 비밀번호를 변경하고 외부 및 관리 인터페이스를 구성하는 작업이 이미 완료되었을 것입니다.

프로시저

단계 **1** 최종 사용자 라이선스 계약(EULA)에 동의하고 관리자 비밀번호를 변경하라는 메시지가 표시됩니다.

계속하려면 이러한 단계를 완료해야 합니다.

단계 **2** 외부 및 관리 인터페이스에 대해 다음 옵션을 구성하고 **Next(**다음**)**를 클릭합니다.

참고 **Next(**다음**)**를 클릭하면 설정이 디바이스에 구축됩니다. 인터페이스는 이름이 "외부"로 지정되어 "outside_zone" 보안 영역에 추가됩니다. 설정이 올바른지 확인합니다.

a) **Outside Interface(**외부 인터페이스**)**—게이트웨이 라우터에 연결한 데이터 포트입니다. 초기 디바이스 설정 중에는 대체 외부 인터페이스를 선택할 수 없습니다. 첫 번째 데이터 인터페이스가 기본 외부 인터페이스입니다.

IPv4 구성 - 외부 인터페이스의 IPv4 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 서브넷 마스크 및 게이트웨이를 입력할 수 있습니다. *끄기*를 선택하여 IPv4 주소를 구성하지 않을 수도 있습니다. 설정 마법사를 사용하여 PPPoE를 구성할 수 없습니다. 인터페이스가 DSL 모뎀이나 케이블 모뎀에 연결되어 있거나 기타 ISP 연결을 사용하고 ISP에서 PPPoE를 사용하여 IP 주소를 제공하는 경우, PPPoE가 필요할 수 있습니다. 마법사를 완료한 후 PPPoE를 구성할 수 있습니다.

IPv6 구성 - 외부 인터페이스의 IPv6 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 접두사 및 게이트웨이를 입력할 수 있습니다. *끄기*를 선택하여 IPv6 주소를 구성하지 않을 수도 있습니다.

b) 관리 인터페이스

DNS 서버 - 시스템 관리 주소용 DNS 서버를 지정합니다. 이름 확인을 위해 DNS 서버의 주소를 하나 이상 입력합니다. 기본값은 OpenDNS 공개 DNS 서버입니다. 필드를 수정하여 기본값으로 되돌리려면 **OpenDNS(OpenDNS** 사용**)**를 클릭하여 적절한 IP 주소를 필드에 다시 로드합니다.

방화벽 호스트 이름 - 시스템 관리 주소용 호스트 이름을 지정합니다.

단계 **3** 시스템 시간 설정을 구성하고 **Next(**다음**)**를 클릭합니다.

a) 표준 시간대 - 시스템의 표준 시간대를 선택합니다.
b) **NTP** 시간 서버 - 기본 NTP 서버를 사용할지 아니면 NTP 서버의 주소를 수동으로 입력할지를 선택합니다. 백업을 제공하기 위해 여러 서버를 추가할 수 있습니다.

단계 **4** 등록 없이 **90**일 평가 기간 시작을 선택하십시오.

참고 Smart Software Manager 어카운트 및 사용 가능한 라이선스가 있더라도 90일 평가판 라이선스를 사용하려면 선택합니다. threat defense에 온보딩한 후 라이선싱을 수행할 수 있습니다. 이 옵션을 선택하면 라이선스를 등록 취소하고 다시 등록할 필요가 없습니다.

threat defense 디바이스 구매 시 기본 라이선스가 자동으로 포함됩니다. 모든 추가 라이선스는 선택 사항입니다.

단계 **5** 마침을 클릭합니다.

다음에 수행할 작업

- CDO 로그인, 23 페이지로 이동하여 온보딩 프로세스를 시작합니다.

CDO 관리자 온보딩 및 관리

로우 터치**(Low-touch)** 프로비저닝

원격 브랜치 관리자가 일련 번호 정보를 중앙 본사로 전송한 후 CDO 관리자는 threat defense를 CDO에 온보딩합니다. 일련 번호를 사용하여 CDO에서 방화벽을 온보딩하는 경우 방화벽은 Cisco 클라우드의 CDO 테넌트와 연결됩니다.

브랜치 오피스 관리자가 방화벽을 연결하고 전원을 켜면 방화벽이 Cisco 클라우드에 연결되고 CDO에 방화벽의 컨피그레이션이 자동으로 동기화됩니다.

그런 다음 방화벽에 라이선스를 부여하고 CDO를 사용하여 방화벽을 구성 및 관리할 수 있습니다.

온보딩 마법사

방화벽의 초기 구성을 수행한 후 CDO에 로그인하여 방화벽을 온보딩할 수 있습니다.

그런 다음 방화벽에 라이선스를 부여하고 CDO를 사용하여 방화벽을 구성 및 관리할 수 있습니다.

CDO 로그인

CDO는 Cisco Secure Sign-On을 ID 제공자로 사용하며, MFA(multi-factor authentication)에는 Duo Security를 사용합니다. CDO에는 사용자 ID를 보호하기 위해 추가 보안 레이어를 제공하는 MFA가 필요합니다. MFA 유형인 이중 인증에서는 CDO에 로그인하는 사용자의 ID를 확인하기 위해 두 가지 구성 요소 또는 요소가 필요합니다.

첫 번째 요소는 사용자 이름과 비밀번호이고, 두 번째 요소는 Duo Security에서 요청 시 생성되는 일회용 비밀번호(OTP)입니다.

Cisco Secure Sign-On 크리덴셜을 설정한 후에는 Cisco Secure Sign-On 대시보드에서 CDO에 로그인할 수 있습니다. Cisco Secure Sign-On 대시보드에서 지원되는 다른 Cisco 제품에도 로그인할 수 있습니다.

- Cisco Secure Sign-On 어카운트가 있는 경우 Cisco Secure Sign-On을 사용하여 CDO에 로그인, 26 페이지 단계로 건너뜁니다.
- Cisco Secure Sign-On 어카운트가 없는 경우 새 Cisco Secure Sign-On 계정생성, 23 페이지 단계로 계속 진행합니다.

새 Cisco Secure Sign-On 계정생성

초기 로그인 워크플로우는 4단계 프로세스입니다. 4단계를 모두 완료해야 합니다.

시작하기 전에

- **DUO Security** 설치 —휴대전화에 Duo Security 앱을 설치하는 것이 좋습니다. Duo 설치에 대한 질문은 Duo 이중 인증 가이드: 등록 가이드를 참고하십시오.

- 시간 동기화—모바일 디바이스를 사용하여 일회용 비밀번호를 생성하려고 합니다. OTP는 시간을 기반으로 하므로 디바이스 시계를 실시간으로 동기화하는 것이 중요합니다. 디바이스 시계가 올바른 시간으로 설정되어 있는지 확인합니다.
- 최신 버전의 Firefox 또는 Chrome을 사용합니다.

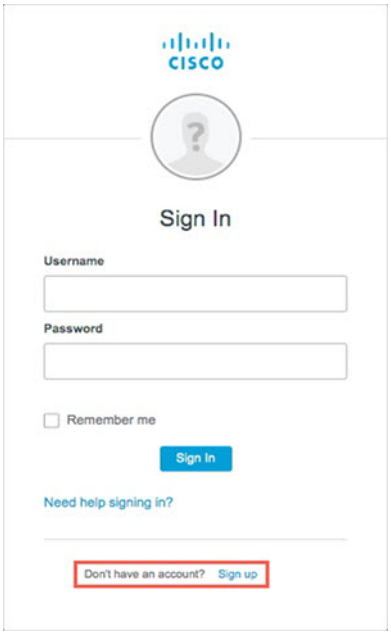
프로시저

단계 **1** 새 **Cisco Secure Sign-On** 계정을 등록**.**

a) https://sign-on.security.cisco.com으로 이동합니다.

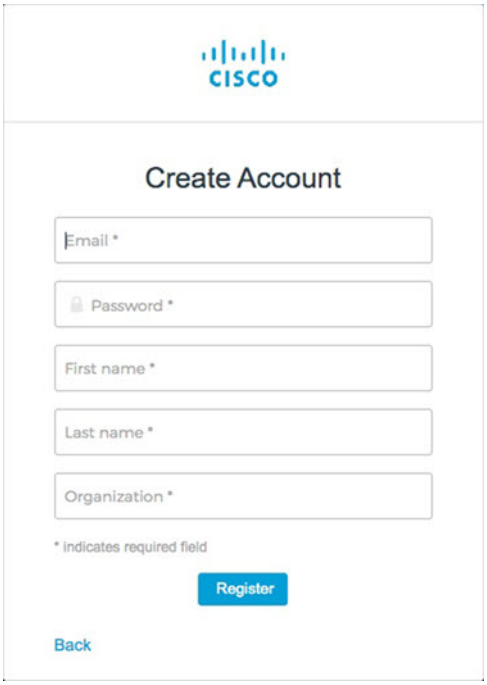
b) Sign In(로그인) 화면 하단에서 **Sign up(**등록**)**을 클릭합니다.

그림 ***9: Cisco SSO*** 등록



c) **Create Account(**어카운트 생성**)** 대화 상자의 필드를 입력하고 **Register(**등록**)**를 클릭합니다.

그림 *10:* 어카운트 만들기



팁 CDO에 로그인하는 데 사용할 이메일 주소를 입력하고 회사를 나타내는 조직 이름을 추가합니다.

d) **Register(**등록**)**를 클릭하면 Cisco에서 등록한 주소로 확인 이메일을 보냅니다. 이메일을 열고 어카운트 활성화를 클릭합니다.

단계 **2** **Duo**를 통한 다단계 인증 설정**.**

a) **Set up multi-factor authentication(**다단계 인증 설정**)** 화면에서 **Configure(**구성**)**를 클릭합니다.

b) **Start setup(**설정 시작**)**을 클릭하고 프롬프트에 따라 디바이스를 선택하고 해당 디바이스와 어카운트의 페어링을 확인합니다.

자세한 내용은 Duo Guide to Two Factor Authentication: Enrollment Guide를 참고하십시오. 디바이스에 이미 Duo 앱이 있는 경우 이 어카운트에 대한 활성화 코드를 받게 됩니다. Duo는 하나의 디바이스에서 여러 계정을 지원합니다.

c) 마법사가 끝나면 **Continue to Login(**계속 로그인**)**을 클릭합니다.

d) 이중 인증을 사용하여 Cisco Secure Sign-On에 로그인합니다.

단계 **3** (선택 사항) **Google OTP**를 추가 인증자로 설정**.**

a) Google Authenticator와 페어링할 모바일 디바이스를 선택하고 **Next(**다음**)**를 클릭합니다.

b) 설정 마법사의 프롬프트에 따라 Google 인증기를 설정합니다.

단계 **4** **Cisco Secure Sign-On** 어카운트에 대한 어카운트 복구 옵션 구성**.**

a) "비밀번호 분실" 질문 및 답변을 선택합니다.

b) SMS를 사용하여 계정을 재설정하려면 복구 전화번호를 선택합니다.

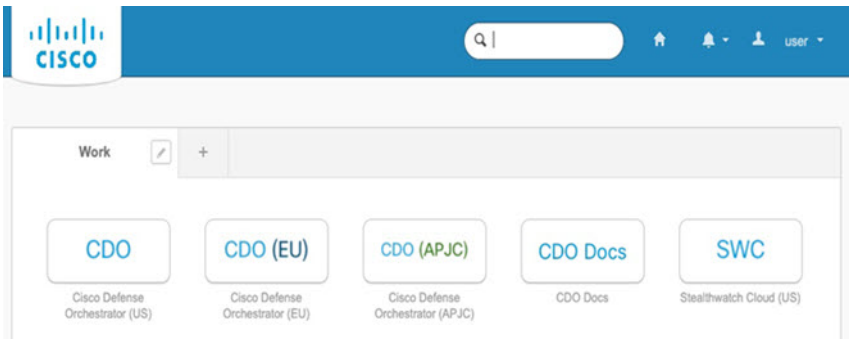
c) 보안 이미지를 선택합니다.

d) **Create My Account(**내 계정 생성**)**를 클릭합니다.

이제 CDO 앱 타일이 있는 Cisco Security Sign-On 대시보드가 표시됩니다. 다른 앱 타일도 표시될 수 있습니다.

팁 대시보드에서 타일을 끌어 원하는 대로 정렬하고, 탭을 생성하여 타일을 그룹화하고, 탭의 이름을 바꿀 수 있습니다.

그림 ***11: Cisco ISE*** 대시보드



Cisco Secure Sign-On을 사용하여 CDO에 로그인

threat defense 온보딩 및 관리를 하려면 CDO에 로그인합니다.

시작하기 전에

CDO(Cisco Defense Orchestrator)는 MFA(multi-factor authentication)를 위해 Cisco Secure Sign-On을 ID 제공자 및 Duo Security로 사용합니다.

- CDO에 로그인하려면 먼저 Cisco Secure Sign-On에서 계정을 생성하고 Duo를 사용하여 MFA를 구성해야 합니다. 새 Cisco Secure Sign-On 계정생성, 23 페이지 참조.
- 최신 버전의 Firefox 또는 Chrome을 사용합니다.

프로시저

단계 **1** 웹 브라우저에서 https://sign-on.security.cisco.com/ 페이지로 이동합니다.

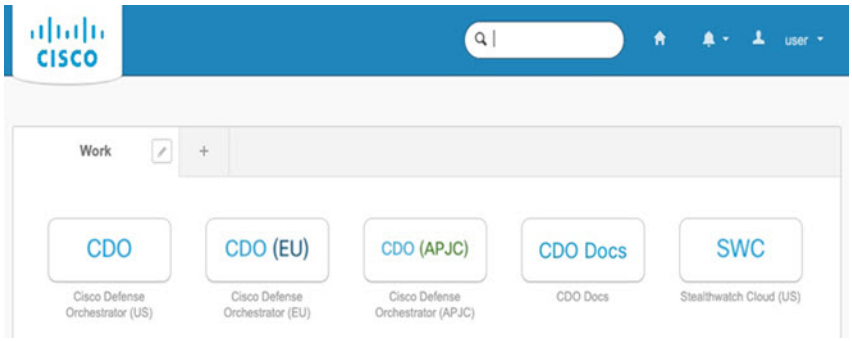
단계 **2** 사용자 이름 및 비밀번호를 입력합니다.

단계 **3** **Log In(**로그인**)**을 클릭합니다.

단계 **4** Duo Security를 사용하여 다른 인증 요소를 수신하고 로그인을 확인합니다. 시스템에서 로그인을 확인하고 Cisco Secure Sign-On 대시보드를 표시합니다.

단계 **5** Cisco Secure Sign-on 대시보드에서 적절한 CDO 타일을 클릭합니다. **CDO** 타일은 https://defenseorchestrator.com으로, **CDO(EU)** 타일은 https://defenseorchestrator.eu, **CDO(APJC)** 타일은 https://www.apj.cdo.cisco.com 쪽으로 안내합니다.

그림 *12: Cisco ISE* 대시보드



단계 **6** 두 인증자를 모두 설정한 경우 인증자 로고를 클릭하여 **Duo Security** 또는 **Google Authenticator**를 선택합니다.

- 기존 테넌트에 사용자 레코드가 이미 있는 경우 해당 테넌트에 로그인됩니다.
- 여러 테넌트에 대한 사용자 레코드가 이미 있는 경우 연결할 CDO 테넌트를 선택할 수 있습니다.
- 기존 테넌트에 대한 사용자 레코드가 아직 없는 경우 CDO에 대해 자세히 알아보거나 평가판 계정을 요청할 수 있습니다.

CDO에 Threat Defense 온보드

방화벽을 CDO에 온보딩합니다.

로우 터치(Low-Touch) 프로비저닝 및 일련 번호를 사용하여 Threat Defense 온보드

로우 터치(low-touch) 프로비저닝을 사용하면 공장에서 배송된 새 디바이스를 자동으로 프로비저닝하고 구성할 수 있으므로 디바이스를 CDO에 온보딩하는 것과 관련된 수동 작업을 많이 수행할 필요가 없습니다. 로우 터치(low-touch) 프로비저닝을 사용하여 CDO에 디바이스를 온보딩하려면 이 절차를 완료하고 인터넷에 연결할 수 있는 네트워크에 디바이스를 연결한 다음 디바이스의 전원을 켭니다.

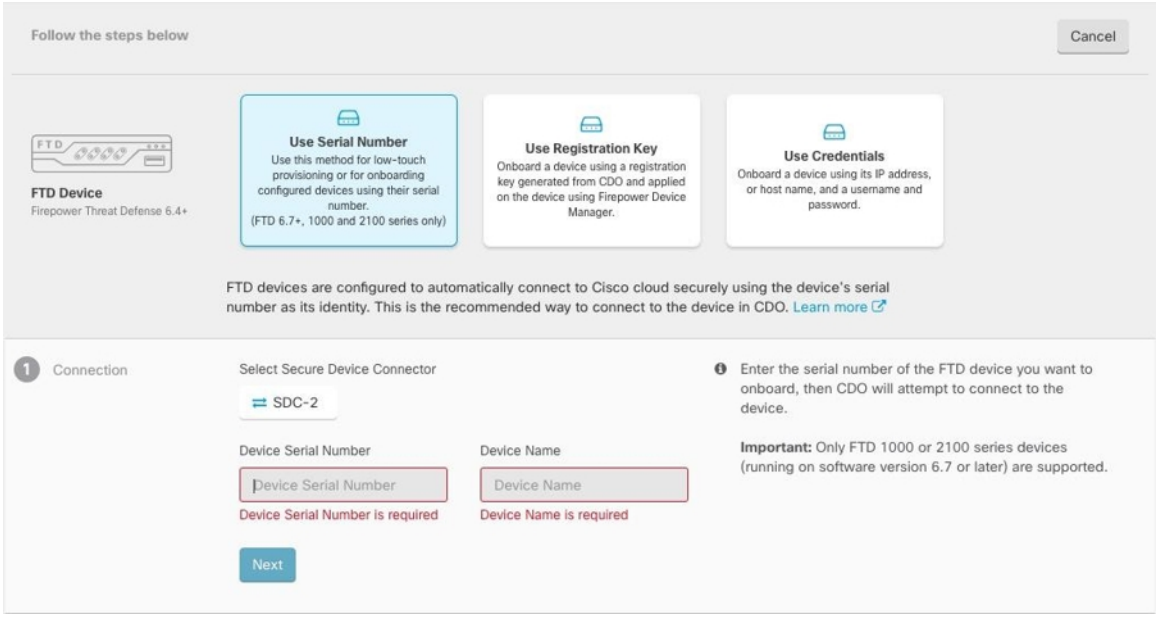
프로시저

단계 **1** CDO 탐색창에서 **Inventory(**인벤토리**)**를 클릭한 다음 파란색 더하기 버튼()을 클릭하여 디바이스를 온보딩합니다.

단계 **2** **FTD** 카드를 클릭합니다.

단계 **3** 일련 번호 사용을 클릭합니다.

단계 **4** Connection(연결) 단계에서 다음 세부 정보를 제공합니다.



a) 이 디바이스가 통신할 보안 디바이스 커넥터를 선택합니다. 기본 SDC가 표시되지만 SDC 이름을 클릭하여 변경할 수 있습니다.
b) 디바이스 일련 번호 — 온보딩할 디바이스의 일련 번호 또는 PCA 번호를 입력합니다.
c) 디바이스 이름 — 논리적 디바이스의 이름을 입력합니다.
d) **Next(**다음**)**를 클릭합니다.

단계 **5** **Password Reset(**비밀번호 재설정**)** 단계에서 **Default Password Not Changed(**기본 비밀번호가 변경되지 않음**)**를 클릭하고 **New Password(**새 비밀번호**)** 및 **Confirm Password(**비밀번호 확인**)**를 입력한 후 **Next(**다음**)**를 클릭합니다.

새 비밀번호가 화면에 나와 있는 요구 사항을 충족하는지 확인합니다.

단계 **6** 스마트 라이선스 단계에서 다음 옵션 중 하나를 선택합니다.

- **Apply Smart License(**스마트 라이선스 적용**)** — 디바이스에 스마트 라이선스가 아직 없는 경우 이 옵션을 선택합니다. Cisco Smart Software Manager를 사용하여 토큰을 생성하고 이 필드에 복사해야 합니다.
- 디바이스에 이미 라이선스 부여 — 디바이스에 이미 라이선스가 부여된 경우 이 옵션을 선택합니다.
- **90**일 평가 라이선스 사용 — 90일 평가 라이선스를 적용합니다.

단계 **7** **Subscription Licenses(**구독 라이선스**)** 단계에서 다음을 수행합니다.

- 스마트 라이선스가 적용된 경우 원하는 추가 라이선스를 활성화하고 **Next(**다음**)**를 클릭할 수 있습니다.
- 평가판 라이선스가 활성화된 경우 RA VPN 라이선스를 제외한 다른 모든 라이선스를 사용할 수 있습니다. 원하는 라이선스를 선택하고 **Next(**다음**)**를 클릭하여 계속합니다.

- 기본 라이센스로만 계속 진행할 수 있습니다.

참고 스마트 라이선스 단계에서 디바이스가 이미 라이선스됨을 선택한 경우 여기에서 선택을 수행할 수 없습니다. CDO에 **Keep Existing Subscription(**기존 구독 유지**)**이 표시되고 **Labels(**레이블**)** 단계로 이동합니다.

단계 **8** (선택 사항) 필요한 경우 **Labels(**레이블**)** 단계에서 레이블 이름을 입력할 수 있습니다.

단계 **9** **Go to Inventory(**인벤토리로 이동**)**를 클릭합니다.

CDO가 디바이스 클레임을 시작하고 오른쪽에 **Claiming(**클레임**)** 메시지가 표시됩니다. CDO는 1시간 동안 지속적으로 폴링하여 디바이스가 온라인 상태이고 클라우드에 등록되어 있는지 확인합니다. 클라우드에 등록되면 CDO가 초기 프로비저닝을 시작하고 디바이스를 성공적으로 온보딩합니다. 디바이스에서 LED 상태가 녹색으로 깜박이면 디바이스 등록을 확인할 수 있습니다. 디바이스가 Cisco 클라우드에 연결할 수 없거나 연결 후 연결이 끊어지면 M LED가 녹색과 황색으로 번갈아 깜박이는 것을 확인할 수 있습니다.

디바이스가 처음 1시간 이내에 클라우드에 등록되지 않으면 시간 초과가 발생하며, 이제 CDO는 10분마다 주기적으로 폴링하여 디바이스 상태를 확인하고 클레임 상태를 유지합니다. 디바이스가 켜져 있고 클라우드에 연결되어 있으면 온보딩 상태를 확인하기 위해 10분 동안 기다릴 필요가 없습니다. 언제든지 **Check Status(**상태 확인**)** 링크를 클릭하여 상태를 확인할 수 있습니다. CDO가 초기 프로비저닝을 시작하고 디바이스를 성공적으로 온보딩합니다.

Threat Defense 등록 키로 온보드

등록 키를 사용하여 threat defense 디바이스를 온보딩하는 것이 좋습니다. DHCP를 사용하여 threat defense에 IP 주소가 할당되고 어떤 이유로 주소가 변경된 경우 threat defense는 CDO에 연결된 상태를 유지합니다. 또한 threat defense에는 공용 IP 주소가 없어도 되며, 디바이스가 외부 네트워크에 액세스할 수 있는 한 이 방법을 사용하여 CDO에 온보딩할 수 있습니다.

참고 SecureX 또는 Cisco Threat Response(CTR) 계정이 있는 경우, 디바이스를 SecureX에 등록하려면 CDO 계정과 SecureX/CTR 계정을 병합해야 합니다. 어카운트가 병합될 때까지 SecureX에서 디바이스의 이벤트를 보거나 다른 SecureX 기능을 활용할 수 없습니다. SecureX에서 CDO 모듈을 생성하기 전에 계정을 병합하는 것이 좋습니다. SecureX 포털을 통해 어카운트를 병합할 수 있습니다. 자세한 내용은 어카운트 병합을 참조하십시오.

등록 키를 사용하여 threat defense 디바이스를 온보딩하려면 다음 절차를 수행합니다.

시작하기 전에

- 이 방법을 사용하여 디바이스를 미국, EU 또는 APJ 지역으로 온보딩할 수 있습니다.
- 디바이스는 device manager에서 관리해야 합니다. 디바이스에서 대기 중인 변경 사항이 없는지 확인합니다.

- 디바이스는 90일 평가 라이선스를 사용하거나 스마트 라이선스를 사용할 수 있습니다. Cisco Smart Software Manager에서 디바이스에 설치된 라이선스를 등록 취소할 필요가 없습니다.
- DNS가 threat defense 디바이스에 올바르게 구성되어 있는지 확인합니다.
- threat defense 디바이스에서 시간 서비스가 올바르게 구성되었는지 확인합니다. threat defense 디바이스에 올바른 날짜 및 시간이 표시되는지 확인합니다. 그렇지 않으면 온보딩이 실패합니다.

프로시저

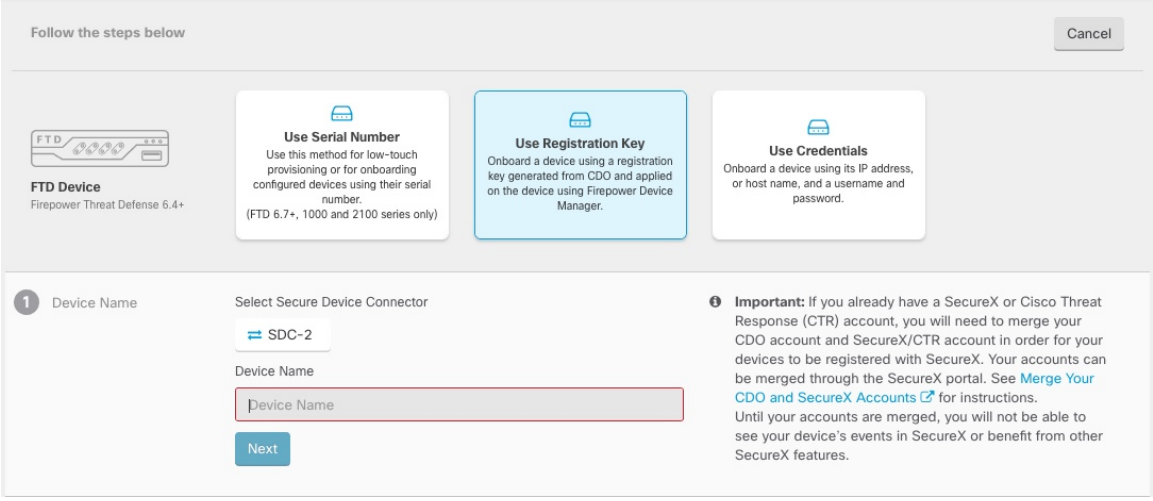
단계 **1** CDO 탐색창에서 **Inventory(**인벤토리**)**를 클릭한 다음 파란색 더하기 버튼(+)을 클릭하여 디바이스를 온보딩합니다.

단계 **2** **FTD** 카드를 클릭합니다.

단계 **3** 등록 키 사용을 클릭합니다.

단계 **4** **Device Name(**디바이스 이름**)** 영역 필드를 작성합니다.

그림 ***13: Device Name(***디바이스 이름***)***



a) 이 디바이스가 통신할 보안 디바이스 커넥터를 선택합니다. 기본 SDC가 표시되지만 SDC 이름을 클릭하여 변경할 수 있습니다.

b) **Device Name(**디바이스 이름**)** 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.

c) **Next(**다음**)**를 클릭합니다.

단계 **5** **Database Updates(**데이터베이스 업데이트**)** 영역에서 즉시 보안 업데이트를 수행하고 반복 업데이트를 선택하거나 선택 취소하고 **Next(**다음**)**를 클릭합니다.

이 옵션은 보안 업데이트를 즉시 트리거할 뿐 아니라 매주 월요일 오전 2시에 추가 업데이트를 확인하도록 디바이스를 자동으로 예약합니다. 자세한 내용은 FTD 보안 데이터베이스 업데이트 및 보안 데이터베이스 업데이트 예약을 참조하십시오.

참고 이 옵션을 비활성화해도 device manager를 통해 구성했을 수 있는 이전에 예약된 업데이트에는 영향을 주지 않습니다.

단계 **6** **Create Registration Key(**등록 키 생성**)** 영역에서 CDO가 등록 키를 생성합니다.

참고 키가 생성된 후 디바이스가 완전히 온보딩되기 전에 온보딩 화면에서 나갈 경우, 온보딩 화면으로 돌아갈 수 없습니다. 그러나 CDO는 **Device & Services(**디바이스 및 서비스**)** 페이지에서 해당 디바이스에 대한 자리 표시자를 생성합니다. 디바이스 자리 표시자를 선택하여 해당 디바이스의 키를 확인합니다.

단계 **7** **Copy(**복사**)** 아이콘()을 클릭하여 등록 키를 복사하고 **Next(**다음**)**를 클릭합니다.

참고 등록 키 복사를 건너뛰고 **Next(**다음**)**를 클릭하여 디바이스에 대한 자리 표시자 항목을 완료한 다음 나중에 디바이스를 등록할 수 있습니다. 이 옵션은 디바이스를 먼저 생성하고 나중에 디바이스를 등록하려는 경우 또는 고객 네트워크에 POV(Proof of Value) 디바이스를 설치하는 Cisco 파트너인 경우 유용합니다.

이제 디바이스가 연결 상태인 "프로비저닝되지 않음"이 됩니다. **Unprovisioned(**프로비저닝되지 않음**)** 아래에 표시되는 등록 키를 device manager에 복사하여 온보딩 프로세스를 완료합니다.

단계 **8** CDO에 온보딩할 디바이스의 device manager에 로그인합니다.

a) **System Settings(**시스템 설정**)**에서 **Cloud Services(**클라우드 서비스**)**를 클릭합니다.

b) Cisco Smart Licensing에 디바이스를 이미 등록했으며 이 페이지에 이미 클라우드에 등록되어 있는 것으로 표시되는 경우 기어 메뉴를 클릭하고 **Unregister Cloud Services(**클라우드 서비스 등록 취소**)**를 선택합니다. 등록되지 않은 옵션을 보려면 페이지를 다시 로드하십시오.

c) **Enrollment Type(**등록 유형**)** 영역에서 **Security/CDO Account(**보안/**CDO** 계정**)**를 클릭합니다.

d) isco Defense Orchestrator에서 **Auto-enroll with Tenancy(**테넌시 자동 등록**)**를 선택하지 마십시오.

일련 번호를 사용한 자동 등록에 대한 자세한 내용은 Cisco Secure Firewall Device Manager 구성 가이드 섹션을 참조하십시오.

e) **Region(**지역**)** 필드에서 테넌트가 할당된 Cisco 클라우드 지역을 선택합니다.

- *defenseorchestrator.com*에 로그인하는 경우 **US**를 선택합니다.
- *defenseorchestrator.eu*에 로그인하는 경우 **EU**를 선택합니다.
- *apj.cdo.cisco.com*에 로그인하는 경우 **APJ**를 선택합니다.

f) CDO에서 생성한 등록 키를 **Registration Key(**등록 키**)**필드에 붙여넣습니다.

g) (6.7 이상) Service Enrollment(서비스 등록) 영역에서 Enable Cisco Defense Orchestrator(Cisco Defense Orchestrator 활성화)를 선택합니다.

h) Cisco Success Network에 대한 정보를 검토합니다. 참여하지 않으려면 **Enroll Cisco Success Network(Cisco Success Network** 등록**)**의 선택을 취소합니다.

i) **Register(**등록**)**를 클릭한 다음, **Accept** Cisco Disclosure(Cisco 공개 동의)를 클릭합니다. device manager에서 CDO에 등록 요청을 전송합니다.

j) 클라우드 서비스 페이지를 새로 고칩니다. 디바이스가 Cisco 클라우드에 성공적으로 등록된 경우 **Cisco Defense Orchestrator** 타일에서 **Enable(**활성화**)**을 클릭합니다.

단계 **9** CDO로 돌아갑니다. **Smart License(**스마트 라이선스**)** 영역에서 threat defense 디바이스에 스마트 라이선스를 적용하고 **Next(**다음**)**를 클릭합니다.

자세한 내용은 라이선싱 구성, 34 페이지를 참고하십시오. **Skip(**건너뛰기**)**을 클릭하여 90일 평가 라이선스로 온보딩을 계속합니다.

단계 **10** **Done(**완료**)** 영역에서 **Go to Inventory(**인벤토리로 이동**)**를 클릭하여 온보딩된 디바이스를 확인합니다.

단계 **11** 인벤토리에서 디바이스 상태가 "프로비저닝되지 않음"에서 "찾는 중", "동기화 중"에서 "동기화됨"으로 진행되는지 확인합니다.

자격 증명 및 IP 주소를 사용하여 Threat Defense 온보딩

로그인 자격 증명(사용자 이름 및 비밀번호) 및 IP 주소 또는 threat defense을 사용하여 를 온보딩할 수 있습니다. 그러나 고정 IP 주소에 의존하지 않고 온프레미스 SDC가 필요하지 않으므로 등록 키로 디바이스를 온보딩하는 것이 좋습니다. Threat Defense 등록 키로 온보드, 29 페이지 참조.

시작하기 전에

- 이 방법을 사용하여 디바이스를 미국, EU 또는 APJ 지역으로 온보딩할 수 있습니다.
- 디바이스는 device manager에서 관리해야 합니다. 디바이스에서 대기 중인 변경 사항이 없는지 확인합니다.
- 디바이스는 90일 평가 라이선스를 사용하거나 스마트 라이선스를 사용할 수 있습니다. Cisco Smart Software Manager에서 디바이스에 설치된 라이선스를 등록 취소할 필요가 없습니다.
- 내부 인터페이스에 연결된 온프레미스 SDC(Secure Device Connector)를 구축하는 것이 좋습니다. 또는 외부 인터페이스를 통해 클라우드 SDC를 사용하려는 경우 외부에서 HTTPS 액세스(device manager 시스템 설정 > 관리 액세스)를 허용해야 합니다. 이는 보안상의 이유로 권장되지 않습니다. SDC에 대한 자세한 내용은 CDO와 Threat Defense의 작동 방식, 9 페이지 섹션을 참조하십시오.
- CDO 관리/SDC 통신에 사용되는 인터페이스를 고정 IP 주소로 구성하거나 DDNS(동적 DNS)를 사용하여 일관된 FQDN을 유지합니다. device manager에서 DDNS를 구성할 수 있습니다.

프로시저

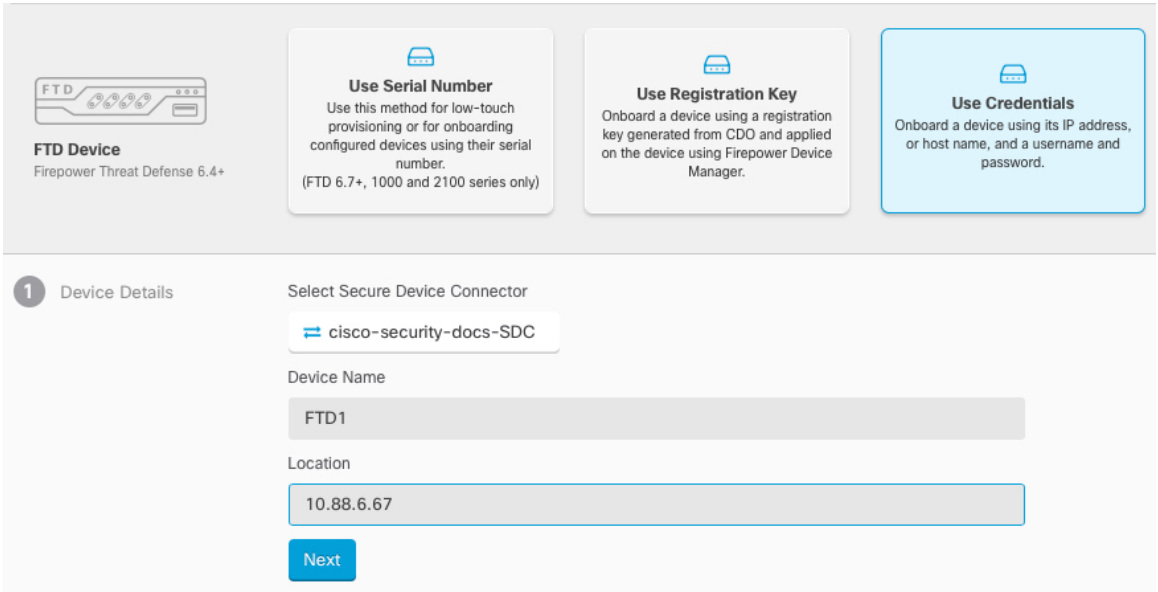
단계 **1** CDO 탐색창에서 **Inventory(**인벤토리**)**를 클릭한 다음 파란색 더하기 버튼( )을 클릭하여 디바이스를 온보딩합니다.

단계 **2** **FTD** 카드를 클릭합니다.

단계 **3** **Use Credentials(**크리덴셜 사용**)**를 클릭합니다.

단계 **4** **Device Name(**디바이스 이름**)** 영역 필드를 작성합니다.

그림 ***14: Device Name(***디바이스 이름***)***



a) 이 디바이스가 통신할 보안 디바이스 커넥터를 선택합니다. 기본 SDC가 표시되지만 SDC 이름을 클릭하여 변경할 수 있습니다.

b) **Device Name(**디바이스 이름**)** 필드에 디바이스 이름을 입력합니다. 디바이스의 호스트 이름 또는 선택한 다른 이름일 수 있습니다.

c) **Location(**위치**)**에 IP 주소, 호스트 이름 또는 FQDN을 입력합니다.

기본 포트는 443입니다. 디바이스의 컨피그레이션을 반영하도록 포트 번호를 변경할 수 있습니다.

d) **Next(**다음**)**를 클릭합니다.

단계 **5** **Database Updates(**데이터베이스 업데이트**)** 영역에서 즉시 보안 업데이트를 수행하고 반복 업데이트를 선택하거나 선택 취소하고 **Next(**다음**)**를 클릭합니다.

이 옵션은 보안 업데이트를 즉시 트리거할 뿐 아니라 매주 월요일 오전 2시에 추가 업데이트를 확인하도록 디바이스를 자동으로 예약합니다. 자세한 내용은 FTD 보안 데이터베이스 업데이트 및 보안 데이터베이스 업데이트 예약을 참조하십시오.

참고 이 옵션을 비활성화해도 device manager를 통해 구성했을 수 있는 이전에 예약된 업데이트에는 영향을 주지 않습니다.

단계 **6** **Credentials(**크리덴셜**)** 영역에 사용자 이름을 **admin**으로 입력하고 초기 설정 중에 설정한 비밀번호를 입력합니다. 그 다음, **Next(**다음**)**를 클릭합니다.

CDO는 연결을 테스트하고 디바이스에 연결할 수 있는지 확인합니다. 성공하면 **Credentials(**크리덴셜**)** 영역에 **Connected(**연결됨**)**가 표시되고 **Onboarding Checks(**온보딩 확인**)** 영역에 **Done(**완료**)**이 표시됩니다.

단계 **7** **Done(**완료**)** 영역에서 **Go to Inventory(**인벤토리로 이동**)**를 클릭하여 온보딩된 디바이스를 확인합니다.

라이선싱 구성

threat defense는 중앙 집중식으로 라이선스 풀을 구매하여 관리할 수 있는 Cisco Smart Software Licensing을 사용합니다.

섀시를 등록할 때 라이선스 기관에서 섀시와 라이선스 기관 간 통신을 위한 ID 인증서를 발급합니다. 또한 섀시를 적절한 가상 어카운트에 할당합니다.

기본 라이선스는 자동으로 포함됩니다. Smart Licensing을 사용하는 경우에는 아직 구매하지 않은 제품 기능도 사용할 수 있습니다. Cisco Smart Software Manager에 등록만 되어 있으면 라이선스 사용을 즉시 시작할 수 있으며 나중에 라이선스를 구매할 수 있습니다. 따라서 기능을 구축 및 사용할 수 있으며 구매 발주서 승인 대기로 인한 지연을 방지할 수 있습니다. 다음 라이선스를 참조하십시오.

- **Threat**—보안 인텔리전스 및 Cisco Firepower Next-Generation IPS
- **Malware**—네트워크용 Advanced Malware Protection(AMP)
- **URL**—URL 필터링
- **RA VPN**—AnyConnect Plus, AnyConnect Apex 또는 AnyConnect VPN 전용입니다.

시스템 라이선싱에 대한 전체적인 내용은 Cisco Secure Firewall Device Manager 구성 가이드를 참조하십시오.

주의 디바이스를 CDO에 온보딩할 때까지 평가판 라이선스를 사용합니다. Smart Software Manager에 등록하는 모든 추가 라이선스는 CDO에 온보딩한 다음 다시 등록하기 전에 등록을 취소해야 합니다. 스마트 라이선스 Threat Defense 등록 취소 참조.

시작하기 전에

- Cisco Smart Software Manager에서 마스터 계정을 만듭니다.

  아직 어카운트가 없는 경우 새 어카운트 설정 링크를 클릭합니다. Smart Software Manager에서 조직의 마스터 계정을 만들 수 있습니다.

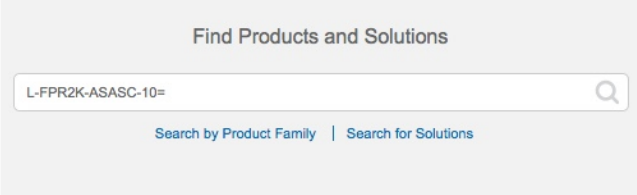
- Cisco Smart Software Licensing 계정은 일부 기능(export-compliance 플래그를 사용하여 활성화됨)을 사용하려면 강력한 암호화(3DES/AES) 라이선스 자격을 얻어야 합니다.

프로시저

단계 **1** Smart Licensing 계정에서 필요한 라이선스가 사용 가능한지 확인합니다.

Cisco 또는 리셀러에서 디바이스를 구매한 경우 라이선스는 Smart Software License 계정에 연결되어 있어야 합니다. 그러나 라이선스를 직접 추가해야 하는 경우 Cisco Commerce Workspace에서 **Find Products and Solutions(**제품 및 솔루션 찾기**)** 검색 필드를 사용합니다. 다음 라이선스 PID를 검색합니다.

그림 ***15:*** 라이선스 검색



참고 PID를 찾을 수 없는 경우 주문에 수동으로 PID를 추가할 수 있습니다.

- Threat, Malware, URL 라이선스 조합:

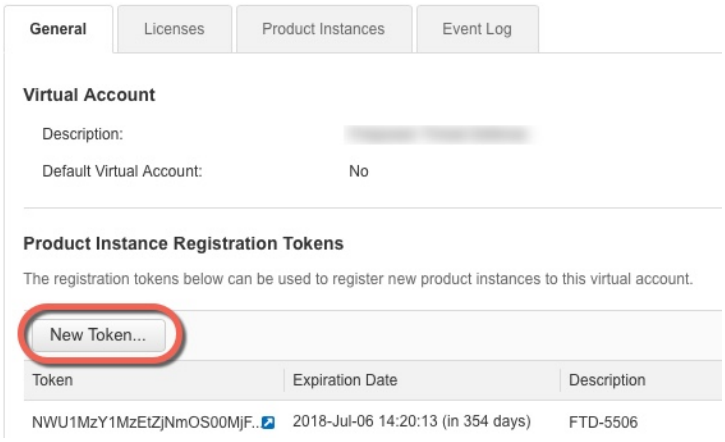
  위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.

- RA VPN—Cisco AnyConnect 주문 가이드를 참조하십시오.

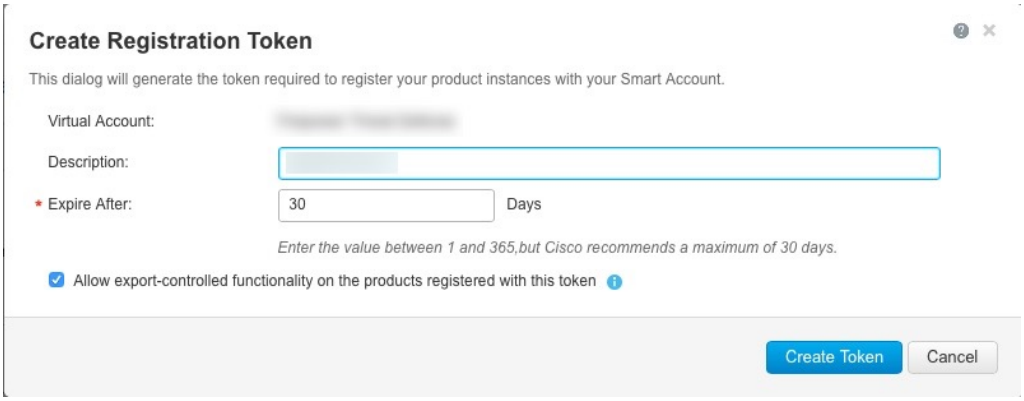
단계 **2** Cisco Smart Software Manager에서 이 디바이스를 추가할 가상 어카운트에 대한 등록 토큰을 요청 및 복사합니다.

a) **Inventory(**인벤토리**)**를 클릭합니다.

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



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



- 설명
- **Expire After(**다음 이후에 만료**)** — 30일로 설정하는 것이 좋습니다.
- **Allow export-controlled functionaility on the products registered with this token(**이 토큰을 사용하여 등록한 제품에서 내보내기 제어 기능 허용**)**—강력한 암호화를 허용하는 국가에 있는 경우 내보내기-규정 준수 플래그를 활성화합니다.

토큰이 인벤토리에 추가됩니다.

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

그림 *16:* 토큰 보기

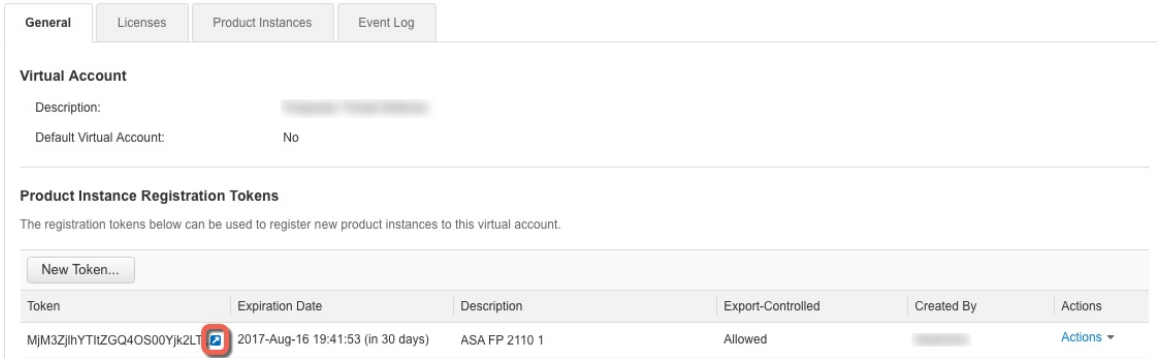
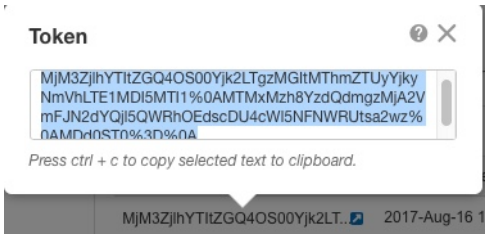


그림 *17:* 토큰 복사



단계 **3** CDO에서 **Inventory(**인벤토리**)**를 클릭한 다음 라이선스를 부여할 threat defense 디바이스를 선택합니다.

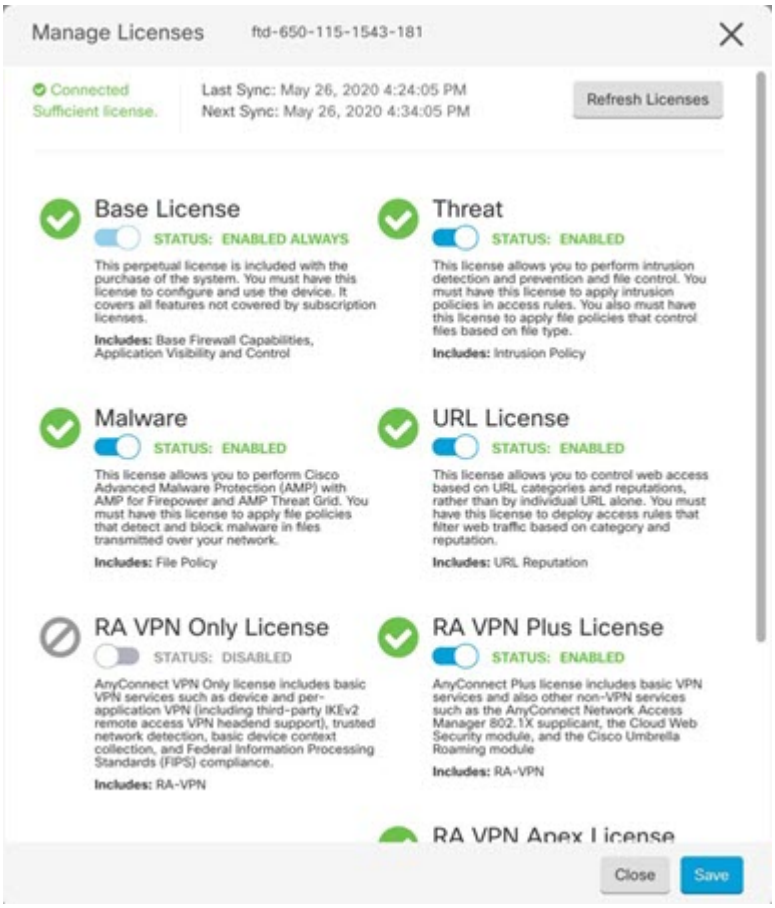
단계 **4** **Device Actions(**디바이스 작업**)** 창에서 **Manage Licenses(**라이선스 관리**)**를 클릭하고 화면의 지침에 따라 Smart Software Manager에서 생성된 스마트 라이선스를 입력합니다.

단계 **5** **Register Device(**디바이스 등록**)**를 클릭합니다. 디바이스와 동기화되면 연결 상태가 'Online(온라인)'으로 변경됩니다.

Manage License(라이선스 관리**)** 페이지로 돌아갑니다. 디바이스가 등록되는 동안 다음 메시지가 표시됩니다.

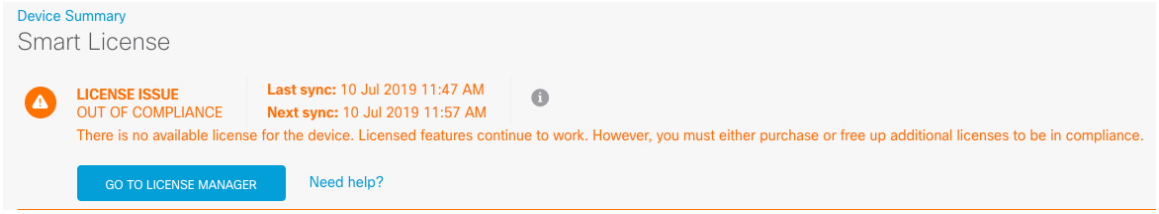
Registration request sent on 10 Jul 2019. Please wait. Normally, it takes about one minute to complete the registration. You can check the task status in Task List. Refresh this page to see the updated status.

단계 **6** 스마트 라이선스를threat defense 디바이스에 성공적으로 적용하면 디바이스 상태에 **Connected, Sufficient License(**연결됨**,** 라이선스가 충분함**)**가 표시됩니다. 선택 가능한 각 라이선스에 대해 **Enable(**활성화**)/Disable(**비활성화**)** 컨트롤을 필요한 대로 클릭합니다.



- **Enable(**활성화**)** - Cisco Smart Software Manager 어카운트에 라이선스를 등록하고 제어되는 기능을 활성화합니다. 이제 라이선스를 통해 제어되는 정책을 구성하고 구축할 수 있습니다.
- **Disable(**비활성화**)** - Cisco Smart Software Manager 어카운트에서 라이선스를 등록 취소하고 제어되는 기능을 비활성화합니다. 이렇게 하면 새 정책에서 기능을 구성할 수 없으며 해당 기능을 사용하는 정책을 구축할 수도 없습니다.
- **RA VPN** 라이선스를 활성화한 경우 **Plus**, **Apex**, **VPN** 전용, **Plus** 및 **Apex** 중 사용할 라이선스 유형을 선택합니다.

기능을 활성화한 뒤 사용자 계정에 라이선스가 없는 경우 페이지를 새로 고친 후에 다음과 같은 비컴플라이언스 메시지가 표시됩니다. 라이선스 문제**,** 컴플라이언스 위반:



단계 **7** Smart Software Manager와 라이선스 정보를 동기화하려면 **Refresh Licenses(**라이선스 새로 고침**)**를 선택합니다.

CDO에서 Threat Defense 구성

다음 단계에서는 구성하려는 추가적인 기능에 대한 개요가 제공됩니다. 각 단계에 대한 자세한 내용을 보려면 페이지에서 도움말 버튼**(?)**을 클릭하십시오.

프로시저

단계 **1** CDO 포털에 로그인하고 CDO 메뉴에서 **Devices & Services(**디바이스 및 서비스**)**를 선택한 다음 방금 온보딩한 디바이스를 선택합니다.

단계 **2** 관리 > 인터페이스를 선택하고 구성할 물리적 인터페이스를 선택합니다.

단계 **3** 구성하려는 각 인터페이스의 편집 아이콘( )을 클릭하고 인터페이스에 **Logical Name(**논리적 이름**)**을 지정하고 필요에 따라 **Description(**설명**)**을 지정합니다.

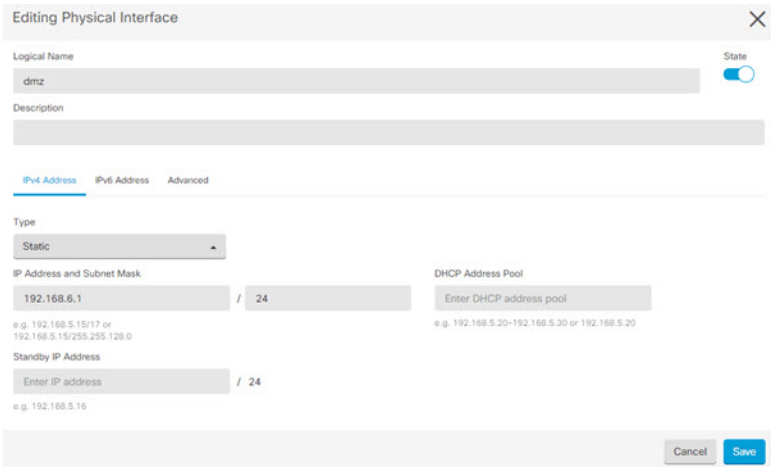
하위 인터페이스를 구성하는 경우가 아니면 인터페이스에는 이름이 있어야 합니다.

참고 이름을 변경하는 경우 보안 영역, syslog 서버 개체, DHCP 서버 정의 등 이전 이름을 사용했던 모든 위치에서 변경 사항이 자동으로 반영됩니다. 그러나 해당 이름을 사용하는 모든 컨피그레이션을 먼저 제거해야 이름을 제거할 수 있습니다. 일반적으로는 정책이나 설정에 대해 이름이 없는 인터페이스를 사용할 수 없기 때문입니다.

단계 **4** **Type(**유형**)**을 설정하고 IP 주소 및 기타 설정을 정의합니다.

다음 예에서는 인터페이스를 웹 서버와 같이 공개적으로 액세스할 수 있는 자산을 배치하는 DMZ("Demilitarized Zone(비무장지대)")로 사용하도록 구성합니다. 완료되면 **Save(**저장**)**를 클릭합니다.

그림 ***18:*** 인터페이스 수정

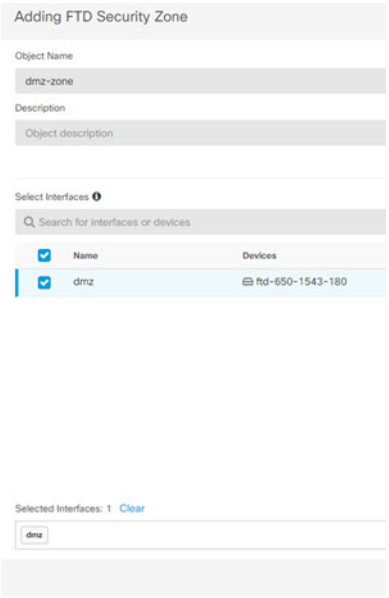


단계 **5** 새 인터페이스를 구성한 경우 관리 > 개체를 선택합니다.

새로운 보안 영역을 적절히 편집하거나 생성합니다. 정책은 인터페이스가 아니라 보안 영역을 기반으로 구성하기 때문에 각 인터페이스는 하나의 영역에 속해 있어야 합니다. 인터페이스를 구성할 때는 영역에 인터페이스를 배치할 수 없으므로 새 인터페이스를 생성하거나 기존 인터페이스의 용도를 변경한 후에는 항상 영역 개체를 편집해야 합니다.

다음 예에는 dmz 인터페이스에서 새 dmz-zone을 생성하는 방법이 나와 있습니다.

그림 ***19:*** 보안 영역 개체



단계 **6** 내부 클라이언트가 DHCP를 사용해 디바이스에서 IP 주소를 가져오도록 하려면 **Management(**관리**)** > **Settings(**설정**)** > **DHCP Server(DHCP** 서버**)**을 선택하고 **DHCP Servers(DHCP** 서버**)** 섹션을 검토합니다.

내부 인터페이스에 이미 DHCP 서버가 구성되어 있지만 주소 풀을 편집하거나 삭제할 수도 있습니다. 다른 내부 인터페이스를 구성한 경우, 이러한 인터페이스에서 DHCP 서버를 설정하는 것은 매우 일반적입니다. +를 클릭하여 각 내부 인터페이스에 서버 및 주소 풀을 구성합니다.

DNS Server(DNS 서버**)** 탭에서 클라이언트에 제공된 DNS 설정을 검토할 수도 있습니다. 다음 예에는 주소 풀이 192.168.45.46-192.168.45.254인 inside2 인터페이스에서 DHCP 서버를 설정하는 방법이 나와 있습니다.

그림 ***20: DHCP*** 서버

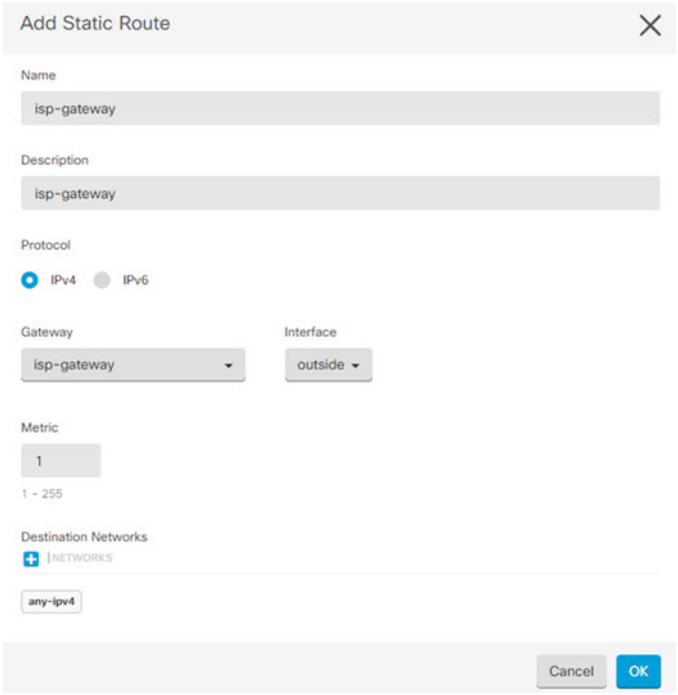
단계 **7** **Management(**관리**)** > **Routing(**라우팅**)**을 선택한 다음 Add(추가) 아이콘을 클릭하여 기본 경로를 구성합니다.

기본 경로는 일반적으로 외부 인터페이스 외에 있는 업스트림 또는 ISP 라우터를 가리킵니다. 기본 IPv4 경로는 any-ipv4(0.0.0.0/0)용인 반면, 기본 IPv6 경로는 any-ipv6(::0/0)용입니다. 사용하는 각 IP 버전에 대해 경로를 생성합니다. DHCP를 사용하여 외부 인터페이스에 대한 주소를 얻으려는 경우, 필요한 기본 경로가 이미 있을 수도 있습니다.

참고 이 페이지에서 정의하는 경로는 데이터 인터페이스 전용입니다. 이러한 경로는 관리 인터페이스에 영향을 주지 않습니다. **Management(**관리**)** > **Settings(**설정**)** > **Management Access(**관리 액세스**)**에서 관리 게이트웨이를 설정합니다.

다음 예에는 IPv4의 기본 경로가 나와 있습니다. 이 예에서 isp-gateway는 ISP 게이트웨이의 IP 주소(ISP에서 주소를 획득해야 함)를 식별하는 네트워크 개체입니다. 이 개체는 **Gateway(**게이트웨이**)** 드롭다운 목록의 아래쪽에서 **Create New Object(**새 개체 생성**)**를 클릭하여 생성할 수 있습니다.

그림 *21:* 기본 라우터



단계 **8** **Management(관리)** > **Policies(정책)**를 선택하고 네트워크의 보안 정책을 구성합니다.

초기 설정을 사용하면 외부 인터페이스로 이동할 때 모든 인터페이스에 대한 inside-zone, outside-zone 및 인터페이스 NAT 간의 트래픽 플로우가 가능합니다. 새 인터페이스를 구성하는 경우에도 inside-zone 개체에 이러한 인터페이스를 추가하면 이러한 인터페이스에 액세스 제어 규칙이 자동으로 적용됩니다.

그러나 내부 인터페이스가 여러 개 있는 경우, inside-zone 간의 트래픽 플로우를 허용하기 위해 액세스 제어 규칙이 필요합니다. 다른 보안 영역을 추가하는 경우, 이러한 영역을 오고 가는 트래픽을 허용하는 규칙이 필요합니다. 이렇게 해야 변경 사항이 가장 적습니다.

또한, 다른 정책을 구성하여 추가 서비스를 제공할 수 있으며 NAT 및 액세스 규칙을 조정하여 조직에 필요한 결과를 얻을 수 있습니다. 다음과 같은 정책을 구성할 수 있습니다.

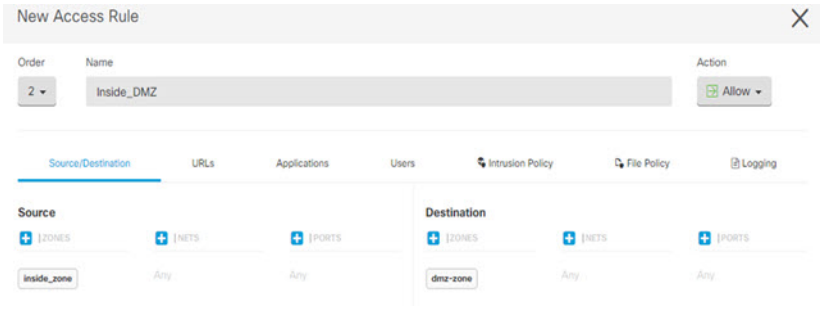
- **SSL Decryption(SSL** 암호 해독**)** — 침입, 악성코드 등에 대한 암호화된 연결(예: HTTPS)을 검사하려는 경우, 연결을 암호 해독해야 합니다. SSL 암호 해독 정책을 사용하여 어떤 연결을 암호 해독해야 할지 확인합니다. 시스템은 검사를 수행한 후에 연결을 다시 암호화합니다.
- **Identity(ID)** — 네트워크 활동과 개인 사용자의 상관관계를 분석하거나 사용자 또는 사용자 그룹 멤버십을 기반으로 네트워크 액세스를 제어하려면 ID 정책을 사용하여 지정된 소스 IP 주소와 연결된 사용자를 확인합니다.
- **Security Intelligence(**보안 인텔리전스**)** — 보안 인텔리전스 정책을 사용하여 블랙리스트에 추가된 IP 주소 또는 URL를 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 블랙리스트에 추가함으로써 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. Cisco는 알려진 유해 주소 및 URL에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 블랙리

스트가 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 블랙리스트에서 항목을 추가하거나 제거하기 위해 정책을 편집할 필요가 없습니다.

- **Access Control(**액세스 제어**)** — 액세스 제어 정책을 사용하여 네트워크에서 어떤 연결이 허용되는지 확인합니다. 보안 영역, IP 주소, 프로토콜, 포트, 애플리케이션, URL, 사용자 또는 사용자 그룹을 기준으로 필터링할 수 있습니다. 액세스 제어 규칙을 사용하여 침입 및 파일(악성코드) 정책을 적용할 수도 있습니다. 이 정책을 사용하여 URL 필터링을 구현할 수 있습니다.

다음 예에는 액세스 제어 정책에서 inside-zone 및 dmz-zone 간의 트래픽을 허용하는 방법이 나와 있습니다. 이 예에서는 **Logging(**로깅**)(At End of Connection(**연결 종료 시**)**이 선택된 경우)을 제외하고는 다른 어떤 탭에도 옵션이 설정되어 있지 않습니다.

그림 ***22:*** 액세스 제어 정책



단계 **9** **Security Database Updates(**보안 데이터베이스 업데이트**)** 섹션을 찾아 threat defense 디바이스의 보안 데이터베이스를 확인하고 업데이트하는 예약된 작업을 생성합니다.

threat defense 디바이스를 CDO에 온보딩할 때 온보딩 프로세스의 일부를 통해 데이터베이스에 대해 예약된 반복 업데이트를 활성화할 수 있습니다. 이 옵션은 기본적으로 선택되어 있습니다. 활성화되면 CDO는 보안 업데이트를 즉시 확인하고 적용할 뿐 아니라 디바이스에서 추가 업데이트를 확인하도록 자동으로 예약합니다. 디바이스가 온보딩된 후 예약된 작업의 날짜 및 시간을 수정할 수 있습니다.

침입 정책을 사용하는 경우 규칙 및 VDB 데이터베이스에 대한 정기 업데이트를 설정합니다. 보안 인텔리전스 피드를 사용하는 경우 피드의 업데이트 일정을 설정합니다. 모든 보안 정책의 일치 기준으로 지리적 위치를 사용하는 경우 해당 데이터베이스에 대한 업데이트 일정을 설정합니다.

단계 **10** 메뉴에서 **Preview and Deploy(**미리보기 및 구축**)** 버튼을 클릭한 다음 **Deploy Now(**지금 구축**)**를 클릭하여 디바이스에 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다.

Threat Defense 및 FXOS CLI 액세스

CLI(Command Line Interface)를 사용하여 시스템을 설정하고 기본적인 시스템 트러블슈팅을 수행합니다. CLI 세션을 통해 정책을 구성할 수는 없습니다. 콘솔 포트에 연결하여 CLI에 액세스할 수 있습니다.

문제 해결을 위해 FXOS CLI에 액세스할 수 있습니다.

참고 아니면 SSH를 threat defense 디바이스의 관리 인터페이스로 할 수 있습니다. 콘솔 세션과 달리 SSH 세션은 기본적으로 threat defense CLI를 사용하며, **connect fxos** 명령을 사용하여 FXOS CLI에 연결할 수 있습니다. 이후 SSH 연결용 인터페이스를 여는 경우 데이터 인터페이스에 있는 주소에 연결할 수도 있습니다. 데이터 인터페이스에 대한 SSH 액세스는 기본값으로 사용 해제 상태입니다. 이 절차에서는 기본값이 FXOS CLI인 콘솔 포트 액세스에 대해 설명합니다.

프로시저

단계 **1** CLI에 로그인하려면 관리 컴퓨터를 콘솔 포트에 연결합니다. Secure Firewall 3100은 DB-9~RJ-45 시리얼 케이블과 함께 제공되므로 연결을 설정하려면 서드파티 시리얼-USB 케이블이 필요합니다. 운영 체제에 필요한 USB 시리얼 드라이버를 설치해야 합니다 (Secure Firewall 3100 하드웨어 가이드 참조). 콘솔 포트의 기본값은 FXOS CLI입니다. 다음 시리얼 설정을 사용하십시오.

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

FXOS CLI에 연결합니다. 초기 설정 시 설정한 관리자 사용자 이름 및 비밀번호(기본값은 **Admin123**)를 사용하여 CLI에 로그인합니다.

예제:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

단계 **2** threat defense CLI에 액세스합니다.

connect ftd

예제:

```
firepower# connect ftd
>
```

로그인한 후 CLI에서 사용할 수 있는 명령에 대한 정보를 확인하려면 **help** 또는 **?**를 입력하십시오. 사용 정보는 Secure Firewall Threat Defense 명령 참조에서 참조하십시오.

단계 **3** threat defenseCLI를 종료하려면 **exit** 또는 **logout** 명령을 입력합니다.

그러면 FXOS CLI 프롬프트로 돌아갑니다. FXOS CLI에서 사용할 수 있는 명령에 대한 정보를 확인하려면 **?**를 입력하십시오.

예제**:**

```
> exit
firepower#
```

Device Manager을 사용하여 방화벽 전원 끄기

device manager를 사용하여 시스템을 올바르게 종료할 수 있습니다.

프로시저

단계 **1** device manager를 사용하여 방화벽을 종료합니다.

a) 디바이스를 클릭한 다음, **System Settings(**시스템 설정**)** > **Reboot/Shutdown(**리부팅/종료**)** > 링크를 클릭합니다.

b) **Shut Down(**종료**)**을 클릭합니다.

단계 **2** 방화벽에 대한 콘솔 연결이 있는 경우 방화벽이 종료될 때 시스템 프롬프트를 모니터링합니다. 다음 프롬프트가 표시됩니다.

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

콘솔에 연결되지 않은 경우 시스템이 종료될 때까지 약 3분 동안 기다리십시오.

단계 **3** 섀시가 성공적으로 꺼진 후에 필요한 경우 섀시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

다음 단계

CDO사용을 통해 threat defense 구성을 계속하려면 CDO 구성 가이드를 참조하십시오.

CDO 사용과 관련된 자세한 내용은 Cisco Defense Orchestrator 홈 페이지를 참조하십시오.