Threat Defense CDO을(를) 사용한 구축

이 장의 설명이 유용합니까?

사용 가능한 모든 애플리케이션 및 관리자를 보려면 귀하에게 적합한 애플리케이션 및 관리자는 무엇입니까?의 내용을 참조하십시오. 이 장은 Cisco Defense Orchestrator(CDO)의 클라우드 사용 Firewall Management Center를 사용하는 위협 방어에 적용됩니다.

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 Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드의 내용을 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 사용하는 Firepower 1000/2100 및 Secure Firewall 3100/4200용 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.

CDO에 의한 Threat Defense 관리 정보

관련 정보 클라우드 사용 **Firewall Management Center**

클라우드 사용 Firewall Management Center는 온프레미스 management center와 동일한 기능을 다수 제공하며 모양과 느낌이 동일합니다. CDO을 기본 관리자로 사용하는 경우, 분석만을 위해 온프레미스 management center를 사용할 수 있습니다. 온프레미스 management center는 정책 구성 또는 업그레이드를 지원하지 않습니다.

온보딩 마법사 및 CLI 등록을 사용하여 디바이스를 온보딩할 수 있습니다.

Threat Defense 관리자 액세스 인터페이스

이 가이드는 원격 지사에 대한 시나리오이므로 외부 인터페이스 액세스를 다룹니다. 관리자 액세스는 외부 인터페이스에서 발생하지만 여전히 전용 관리 인터페이스와 관련이 있습니다. 관리 인터페이스는 threat defense 데이터 인터페이스와 별도로 구성된 특수 인터페이스이며 자체 네트워크 설정이 있습니다.

- 데이터 인터페이스에서 관리자 액세스를 활성화하더라도 관리 인터페이스 네트워크 설정은 계속 사용됩니다.
- 모든 관리 트래픽은 계속해서 관리 인터페이스에서 제공되거나 관리 인터페이스로 전송됩니다.
- 데이터 인터페이스에서 관리자 액세스를 활성화하면 threat defense는 수신 인터페이스를 백플레인을 통해 관리 인터페이스로 전달합니다.
- 발신 관리 트래픽의 경우 관리 인터페이스는 백플레인을 통해 데이터 인터페이스로 트래픽을 전달합니다.

관리자 액세스 요구 사항

데이터 인터페이스에서의 관리자 액세스에는 다음과 같은 제한이 있습니다.

- 물리적 데이터 인터페이스에서만 관리자 액세스를 활성화할 수 있습니다. 하위 인터페이스 또는 EtherChannel은 사용할 수 없습니다.또한 management center를 사용하여 리던던시(redundancy)를 위해 단일 보조 인터페이스에서 관리자 액세스를 활성화할 수 있습니다.
- 이 인터페이스는 관리 전용일 수 없습니다.
- 라우팅 인터페이스를 사용하는 라우팅 방화벽 모드 전용입니다.
- PPPoE는 지원되지 않습니다. ISP에 PPPoE가 필요한 경우 threat defense와 WAN 모뎀 간에 PPPoE를 지원하는 라우터를 설치해야 합니다.
- 인터페이스는 전역 VRF에만 있어야 합니다.
- SSH는 데이터 인터페이스에 대해 기본적으로 활성화되어 있지 않으므로 나중에 management center를 사용하여 SSH를 활성화해야 합니다. 관리 인터페이스 게이트웨이가 데이터 인터페이스로 변경되므로, **configure network static-routes** 명령을 사용하여 관리 인터페이스에 대한 고정 경로를 추가하지 않는 한 원격 네트워크에서 관리 인터페이스로 SSH 연결할 수도 없습니다.

- 별도의 관리 및 이벤트 전용 인터페이스를 사용할 수 없습니다.
- 클러스터링은 지원되지 않습니다. 이 경우에는 관리 인터페이스를 사용해야 합니다.

고가용성 요구 사항

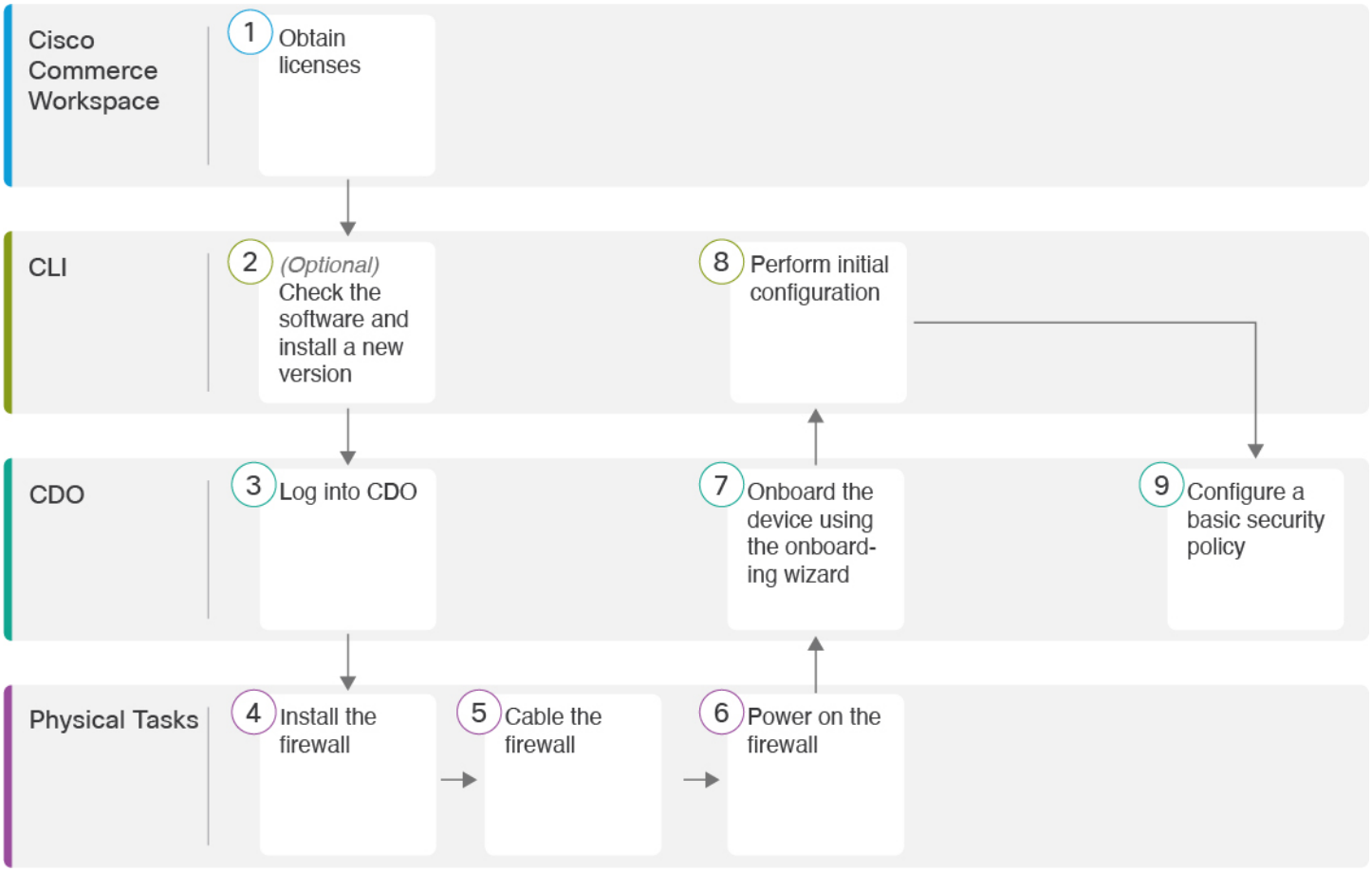
디바이스 고가용성이 있는 데이터 인터페이스를 사용하는 경우 다음 요구 사항을 참조하십시오.

- 관리자 액세스를 위해 두 디바이스에서 동일한 데이터 인터페이스를 사용합니다.
- 이중화 관리자 액세스 데이터 인터페이스는 지원되지 않습니다.
- DHCP를 사용할 수 없습니다. 정적 IP 주소만 지원됩니다. DDNS 및 로우 터치 프로비저닝을 포함하여 DHCP에 의존하는 기능은 사용할 수 없습니다.
- 동일한 서브넷에 서로 다른 고정 IP 주소가 있어야 합니다.
- IPv4 또는 IPv6을 사용하십시오. 둘 다 설정할 수 없습니다.
- 동일한 관리자 구성(**configure manager add** 명령)을 사용하여 연결이 동일한지 확인하십시오.
- 장애 조치 또는 상태 링크로 데이터 인터페이스를 사용할 수 없습니다.

엔드 투 엔드 작업

온보딩 마법사를 사용하여 새시에 CDO에 threat defense을 구축하려면 다음 작업을 참조하십시오.

그림 *1:* 엔드 투 엔드 작업



1	Cisco Commerce Workspace	라이선스 얻기, 5 페이지.
2	CLI	(선택 사항) 소프트웨어 확인 및 새 버전 설치, 7 페이지.
3	CDO	CDO 로그인, 8 페이지.
4	물리적 작업	방화벽을 설치합니다. 하드웨어 설치 가이드를 참조하십시오.
5	물리적 작업	방화벽 케이블 연결, 12 페이지.
6	물리적 작업	방화벽 켜기, 13 페이지.
7	CDO	온보딩 마법사를 사용하여 디바이스 온보딩, 14 페이지.

8	CLI	CLI를 사용한 초기 구성 수행, 17 페이지.
9	CDO	기본 보안 정책 구성, 22 페이지.

중앙 관리자 사전 구성

이 섹션에서는 방화벽용 기능 라이선스를 얻는 방법에 대해 설명합니다. 구축 전 새 소프트웨어 버전을 설치하는 방법 및 CDO에 로그인하는 방법을 제공합니다.

라이선스 얻기

모든 라이선스는 CDO를 통해 threat defense에 제공됩니다. 선택적으로 다음 기능 라이선스를 구매할 수 있습니다.

- **Essentials**—(필수) Essentials 라이선스.
- **IPS**—보안 인텔리전스 및 Next-Generation IPS
- 악성코드 방어—악성코드 방어
- **URL**—URL 필터링
- **Cisco Secure Client**—Secure Client Advantage, Secure Client Premier 또는 Secure Client VPN 전용
- **Carrier**—배율, GTP/GPRS, M3UA, SCTP

시스코 라이선싱에 대한 자세한 내용은 cisco.com/go/licensingguide를 참조하세요.

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.

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

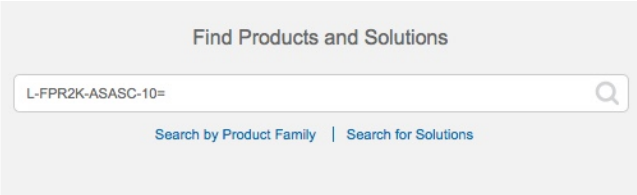
프로시저

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 *2:* 라이선스 검색



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

- Essentials 라이선스:
  - L-FPR4215-BSE=
  - L-FPR4225-BSE=
  - L-FPR4245-BSE=
- IPS, 악성코드 방어 및 URL 라이선스 조합:
  - L-FPR4215T-TMC =
  - L-FPR4225T-TMC =
  - L-FPR4245T-TMC =

  위의 PID 중 하나를 주문에 추가하면 다음 PID 중 하나에 해당하는 기간별 서브스크립션을 선택할 수 있습니다.
  - L-FPR4215T-TMC-1Y
  - L-FPR4215T-TMC-3Y
  - L-FPR4215T-TMC-5Y
  - L-FPR4225T-TMC-1Y
  - L-FPR4225T-TMC-3Y
  - L-FPR4225T-TMC-5Y
  - L-FPR4245T-TMC-1Y
  - L-FPR4245T-TMC-3Y
  - L-FPR4245T-TMC-5Y
- 통신 사업자 라이선스:
  - L-FPR4200-FTD-CAR=

- Cisco Secure Client— Cisco Secure Client 주문 가이드를 참고하십시오.

단계 **2** 아직 등록하지 않은 경우 CDO를 Smart Software Manager에 등록합니다.

등록하려면 Smart Software Manager에서 등록 토큰을 생성해야 합니다. 자세한 지침은 CDO 설명서를 참조하십시오.

(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** 방화벽의 전원을 켜고 콘솔 포트에 연결합니다. 자세한 내용은 방화벽 켜기, 13 페이지 및 Threat Defense 및 FXOS CLI 액세스, 36 페이지를 참고하십시오.

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 변경되었고 모르는 경우, 비밀번호를 기본값으로 재설정하려면 공장 설정 초기화를 수행해야 합니다. 공장 설정 초기화 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               7.4.0.65        7.4.0.65
        Not Applicable
```

단계 **3** 새 버전을 설치하려면 다음 단계를 수행합니다.

a) 관리 인터페이스에 대한 고정 IP 주소를 설정해야 하는 경우 CLI를 사용한 초기 구성 수행, 17 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.

방화벽이 재부팅된 후 FXOS CLI에 다시 연결됩니다.

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, 11 페이지 단계로 건너뜁니다.
- Cisco Secure Sign-On 어카운트가 없는 경우 새 Cisco Secure Sign-On 계정생성, 9 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.

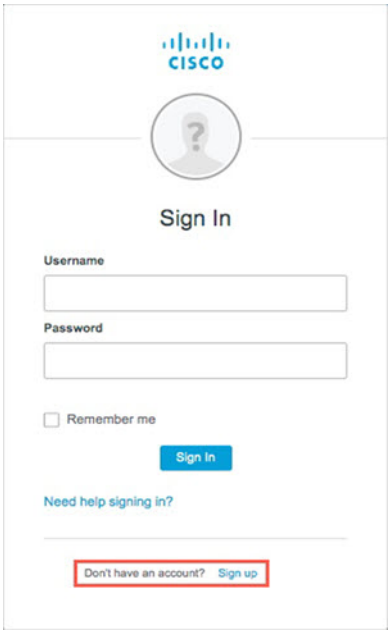
프로시저

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

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

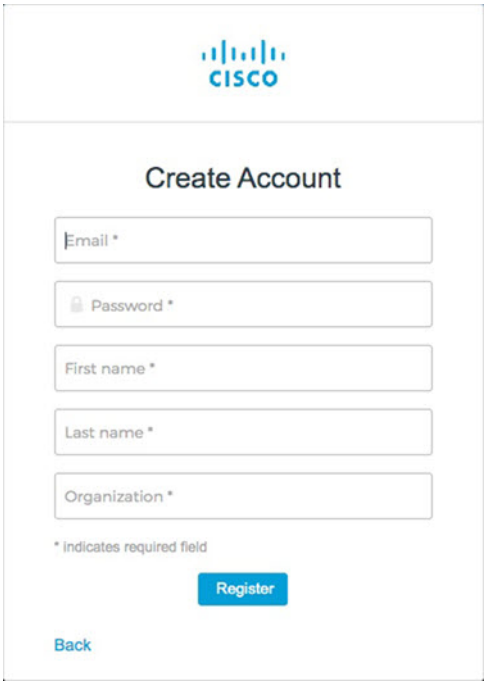
b) Sign In(로그인) 화면 하단에서 **Sign up(**등록**)**를 클릭합니다.

그림 ***3: Cisco SSO*** 등록



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

그림 4: 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 참조하십시오. 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**)**를 클릭합니다.

d) 2단계 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 복원 전화번호를 선택합니다.

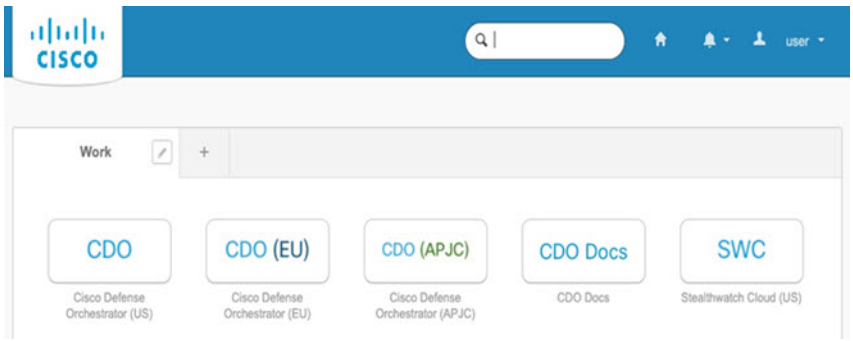
c) 보안 이미지를 선택합니다.

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 ***5: Cisco ISE*** 대시보드



Cisco Secure Sign-On을 사용하여 CDO에 로그인

장치를 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, 9 페이지 참조.
- 최신 버전의 Firefox 또는 Chrome을 사용합니다.

프로시저

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

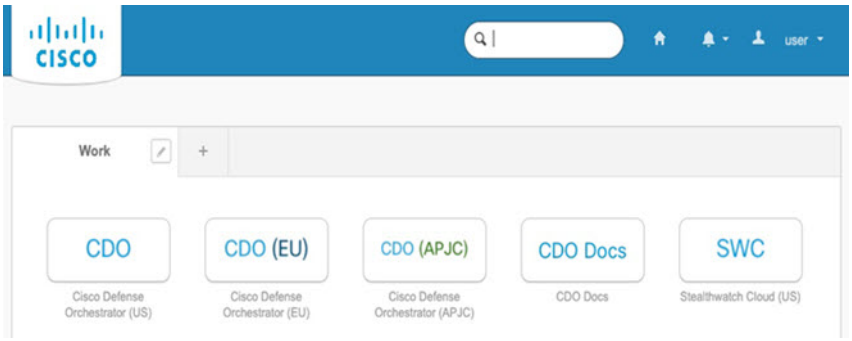
단계 **2** 사용자 이름 및 비밀번호를 입력합니다.

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 *6: 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.

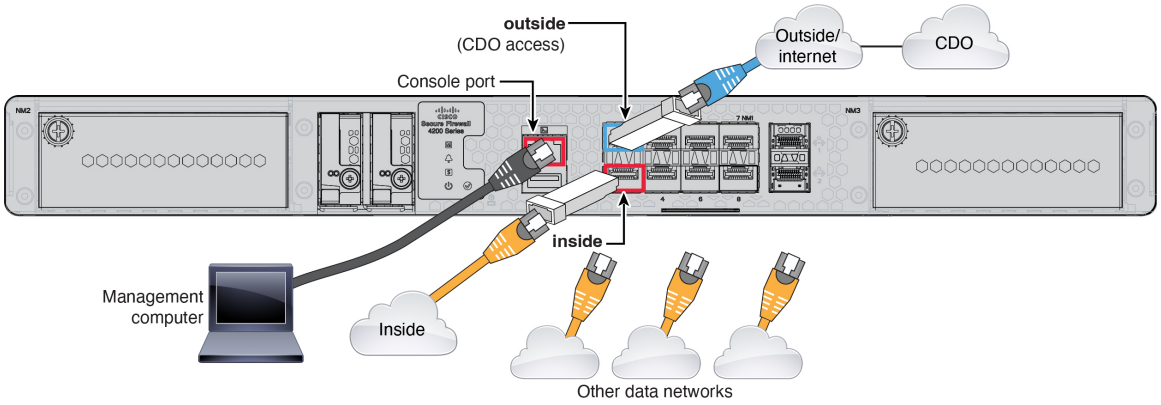
온보딩 마법사를 사용하여 방화벽 구축

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

방화벽 케이블 연결

이 항목에서는 CDO가 네트워크를 관리할 수 있도록 Secure Firewall 4200을 네트워크에 연결하는 방법을 설명합니다.

그림 *7: Secure Firewall 4200* 케이블 연결



시작하기 전에

- 데이터 인터페이스 포트에 SFP 설치 - 기본 제공 포트는 SFP 모듈이 필요한 1/10/25-Gb SFP 포트입니다.
- 콘솔 케이블 얻기 - 방화벽은 기본적으로 콘솔 케이블과 함께 제공되지 않으므로 예를 들어 서드파티 USB-RJ-45 직렬 케이블을 구매해야 합니다.

프로시저

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

단계 **2** 외부 인터페이스(예: Ethernet 1/1)를 외부 라우터에 연결합니다.

단계 **3** 내부 인터페이스(예: Ethernet 1/2)를 내부 스위치 또는 라우터에 연결합니다.

단계 **4** 나머지 인터페이스에 다른 네트워크를 연결합니다.

단계 **5** 관리 컴퓨터를 콘솔 포트에 연결합니다.

CLI를 사용하여 초기 설정을 수행해야 합니다. 콘솔 포트는 문제 해결을 위해서도 필요할 수 있습니다.

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.

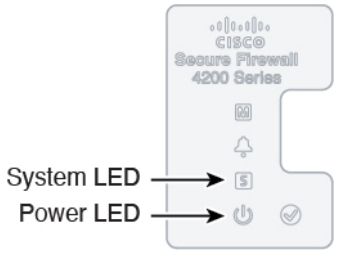
프로시저

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.

온보딩 마법사를 사용하여 디바이스 온보딩

CLI 등록 키를 사용하는 CDO의 온보딩 마법사를 사용하여 threat defense을(를) 온보딩합니다.

프로시저

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

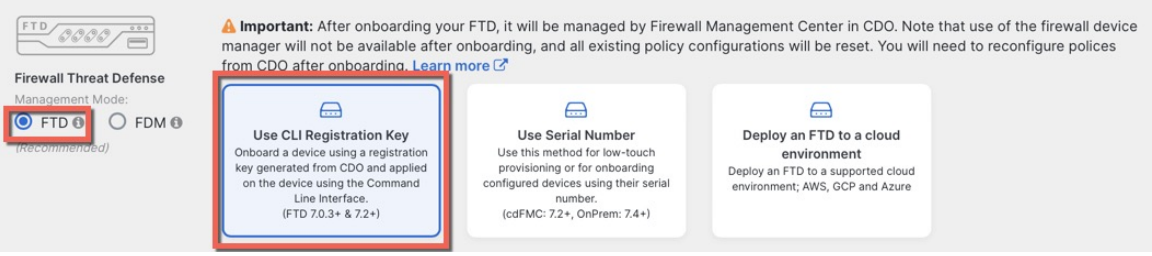
단계 **2** **FTD** 타일을 선택합니다.

단계 **3** **Management Mode(**관리 모드**)**에서 **FTD**가 선택되어 있는지 확인합니다.

FTD를 관리 모드로 선택한 후 언제든지 **Manage Smart License(**스마트 라이선스 관리**)**를 클릭하여 디바이스에 사용 가능한 기존 스마트 라이선스를 등록하거나 수정할 수 있습니다. 어떤 라이선스를 사용할 수 있는지 확인하려면 라이선스 얻기, 5 페이지의 내용을 참조하십시오.

단계 **4** 온보딩 방법으로 **Use CLI Registration Key(CLI** 등록 키 사용**)**를 선택합니다.

그림 ***9: CLI*** 등록 키 사용

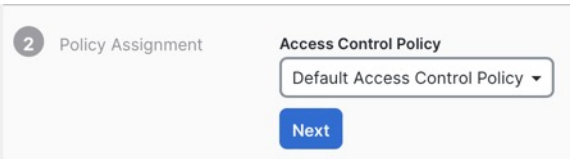


단계 **5** **Device Name(**디바이스 이름**)**을 입력하고 **Next(**다음**)**를 클릭합니다.

그림 ***10: Device Name(***디바이스 이름***)***

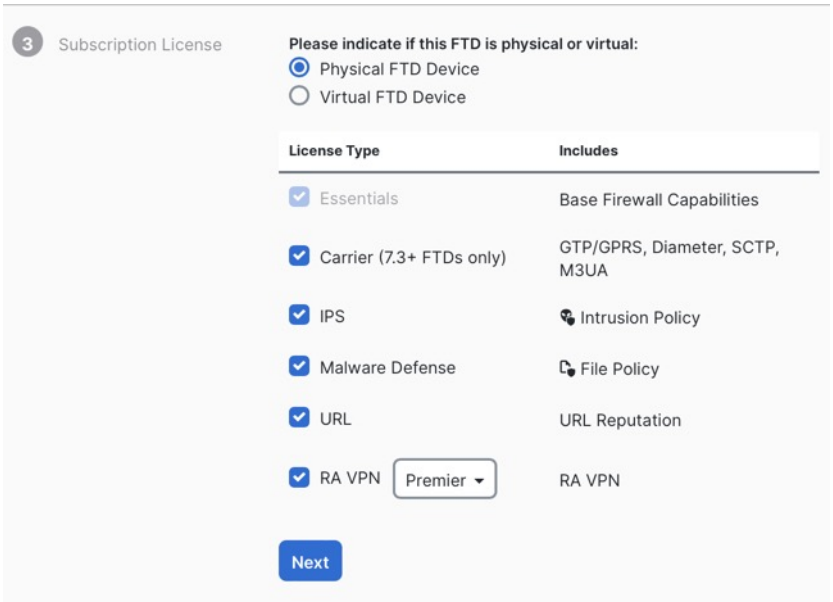
단계 **6** **Policy Assignment(**정책 할당**)**에서 드롭다운 메뉴를 사용하여 디바이스에 대한 액세스 제어 정책을 선택합니다. 구성된 정책이 없는 경우 **Default Access Control Policy(**기본 액세스 제어 정책**)**를 선택합니다.

그림 ***11:*** 액세스 제어 정책



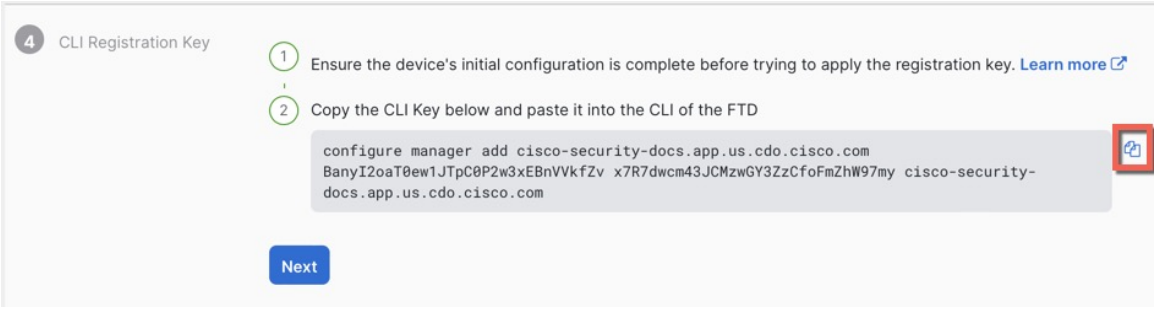
단계 **7** 구독 라이선스의 경우, **Physical FTD Device(**물리적 **FTD** 디바이스**)** 라디오 버튼을 클릭한 다음 활성화하려는 각 기능 라이선스를 선택합니다. **Next(**다음**)**를 클릭합니다.

그림 *12:* 구독 라이선스



단계 **8** **CLI** 등록 키의 경우 CDO는 등록 키 및 기타 매개 변수를 사용하여 명령을 생성합니다. 이 명령을 복사하여 threat defense의 초기 구성에서 사용해야 합니다.

그림 *13: CLI* 등록 키



configure manager add *cdo_hostname registration_key nat_id display_name*

시작 스크립트를 완료한 후 threat defense CLI에서 이 명령을 복사합니다. CLI를 사용한 초기 구성 수행, 17 페이지의 내용을 참조하십시오.

예제:

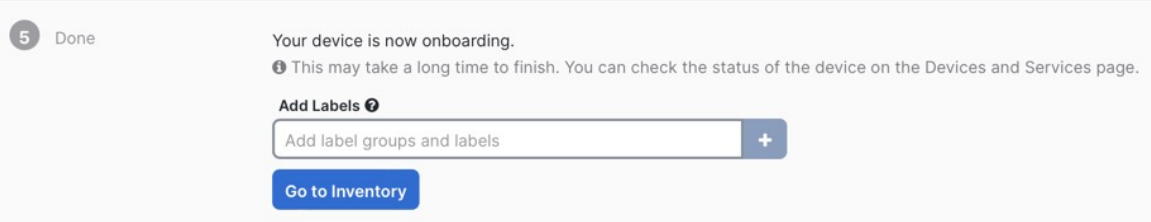
CLI 설정을 위한 샘플 명령:

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

단계 **9** 온보딩 마법사에서 **Next(**다음**)**를 클릭하여 디바이스 등록을 시작합니다.

단계 **10** (선택 사항) **Inventory(**재고 목록**)** 페이지를 정렬하고 필터링하는 데 도움이 되도록 디바이스에 레이블을 추가합니다. 레이블을 입력하고 파란색 더하기 버튼( )을 선택합니다. 레이블은 CDO에 온보딩된 후 디바이스에 적용됩니다.

그림 ***14:*** 완료



다음에 수행할 작업

Inventory(재고 목록**)** 페이지에서 방금 온보딩한 디바이스를 선택하고 오른쪽에 있는 **Management(**관리**)** 창 아래에 나열된 옵션 중 하나를 선택합니다.

CLI를 사용한 초기 구성 수행

초기 설정을 수행하려면 threat defense CLI에 연결합니다.

Procedure

단계 **1** SSH 또는 콘솔 포트를 사용하여 threat defense CLI에 연결합니다.

콘솔 포트는 FXOS CLI에 연결됩니다.

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

FXOS에 처음 로그인하면 비밀번호를 변경하라는 메시지가 표시됩니다. 이 비밀번호는 SSH의 threat defense 로그인에도 사용됩니다.

Note 비밀번호가 이미 변경되었거나 비밀번호를 모르는 경우 비밀번호를 기본값으로 재설정하려면 디바이스의 이미지를 재설치해야 합니다. 이미지 재설치 절차는 FXOS 문제 해결 설명서를 참조하십시오.

Example:

```
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 **3** threat defense CLI에 연결합니다.

connect ftd

Example:

```
firepower# connect ftd
>
```

단계 **4** threat defense에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하라는 메시지가 표시됩니다. 그러면 관리 인터페이스 설정에 대한 CLI 설정 스크립트가 표시됩니다.

데이터 인터페이스에서 관리자 액세스를 활성화하더라도 관리 인터페이스 네트워크 설정은 계속 사용됩니다.

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

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

다음 지침을 참조하십시오.

- **Do you want to configure IPv4?(IPv4**를 구성하시겠습니까**?)** 및/또는 **Do you want to configure IPv6?(IPv6**를 구성하시겠습니까**?)** - 이러한 주소 유형 중 하나 이상에 **y**를 입력합니다. 관리 인터페이스를 사용할 계획은 없지만 IP 주소(예: 개인 주소)를 설정해야 합니다.
- **Configure IPv4 via DHCP or manually?(DHCP**를 통해 또는 수동으로 **IPv4**를 구성하시겠습니까**)?** 및/또는 **Configure IPv6 via DHCP, router, or manually?(DHCP,** 라우터를 통해 또는 수동으로 **IPv6**를 설정하시겠습니까**?)- manual(**수동**)**을 선택합니다. 관리 인터페이스가 DHCP로 설정된 경우 관리를 위해 데이터 인터페이스를 설정할 수 없습니다. 데이터 인터페이스**(**데이터 인터페이스**)**여야 하는 기본 경로(다음 글머리 기호 참조)가 DHCP 서버에서 수신한 기본 경로를 덮어쓸 수 있기 때문입니다.
- **Enter the IPv4 default gateway for the management interface(**관리 인터페이스의 **IPv4** 기본 게이트웨이 입력**)** 및/또는 **Enter the IPv6 gateway for the management interface(**관리 인터페이스에 대한 **IPv6** 게이트웨이 입력**)**— 게이트웨이를 **data-interfaces**로 설정합니다. 이 설정은 관리 트래픽을 백플레인을 통해 전달하므로 관리자 액세스 데이터 인터페이스를 통해 라우팅될 수 있습니다.
- **Configure firewall mode?(**방화벽 모드를 구성하시겠습니까**?)**—**routed(**라우팅**)**를 입력합니다. 외부 관리자 액세스는 라우팅 방화벽 모드에서만 지원됩니다.

Example:

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

System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
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]:
Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none'
[208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com
Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: data on management0
Updating routing tables, please wait...
All configurations applied to the system. Took 3 Seconds.
Saving a copy of running network configuration to local disk.
For HTTP Proxy configuration, run 'configure network http-proxy'


DHCP server is already disabled
DHCP Server Disabled
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...


Device is in OffBox mode - disabling/removing port 443 from iptables.
Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
```

```
this sensor to the Firepower Management Center.
>
```

단계 **5** 관리자 액세스를 위한 외부 인터페이스를 구성합니다.

configure network management-data-interface

그러면 외부 인터페이스에 대한 기본 네트워크 설정을 구성하라는 메시지가 표시됩니다. 이 명령 사용에 대한 자세한 내용은 다음을 참조하십시오.

- 관리에 데이터 인터페이스를 사용하려는 경우 관리 인터페이스에서 DHCP를 사용할 수 없습니다. 초기 설정 중에 IP 주소를 수동으로 설정하지 않은 경우 지금 **configure network** {**ipv4** | **ipv6**} **manual** 명령을 사용하여 설정할 수 있습니다. 관리 인터페이스 게이트웨이를 아직 **data-interfaces**로 설정하지 않은 경우, 이 명령이 이제 설정합니다.
- CDO에 threat defense를 추가하면 CDO는 인터페이스 이름 및 IP 주소, 게이트웨이에 대한 고정 경로, DNS 서버 및 DDNS 서버를 포함한 인터페이스 컨피그레이션을 검색하고 유지 관리합니다. DNS 서버 설정에 관한 자세한 내용은 아래를 참조하십시오. CDO에서 나중에 관리자 액세스 인터페이스 구성을 변경할 수 있지만, threat defense 또는 CDO가 관리 연결을 재설정하지 못하게 할 수 있는 변경은 수행하지 않아야 합니다. 관리 연결이 중단되면 threat defense에 이전 구축을 복구하는 **configure policy rollback** 명령이 포함됩니다.
- DDNS 서버 업데이트 URL을 설정하는 경우 threat defense가 HTTPS 연결을 위해 DDNS 서버 인증서를 검증할 수 있도록 threat defense가 Cisco Trusted Root CA 번들에서 모든 주요 CA에 대한 인증서를 자동으로 추가합니다. threat defense는 DynDNS 원격 API 사양 (https://help.dyn.com/remote-access-api/)을 사용하는 모든 DDNS 서버를 지원합니다.
- 이 명령은 데이터 인터페이스 DNS 서버를 설정합니다. 설정 스크립트로 설정하거나 **configure network dns servers** 명령을 사용하여 설정한 관리 DNS 서버는 관리 트래픽에 사용됩니다. 데이터 DNS 서버는 DDNS(설정된 경우) 또는 이 인터페이스에 적용된 보안 정책에 사용됩니다.

  CDO에서 이 threat defense에 할당하는 플랫폼 설정 정책에서 데이터 인터페이스 DNS 서버가 설정됩니다. CDO 에 threat defense를 추가하면 로컬 설정이 유지되고 DNS 서버가 플랫폼 설정 정책에 추가되지 않습니다. 그러나 나중에 DNS 컨피그레이션을 포함하는 threat defense에 플랫폼 설정 정책을 할당하면 해당 컨피그레이션이 로컬 설정을 덮어씁니다. CDO와 threat defense를 동기화하려면 이 설정과 일치하도록 DNS 플랫폼 설정을 적극적으로 구성하는 것이 좋습니다.

  또한 로컬 DNS 서버는 초기 등록시 DNS 서버가 검색된 경우에만 CDO에 의해 유지됩니다. 예를 들어 관리 인터페이스를 사용하여 디바이스를 등록한 다음 나중에 **configure network management-data-interface** 명령을 사용하여 데이터 인터페이스를 구성하는 경우 threat defense 구성과 일치하도록 DNS 서버를 포함하여 CDO에서 이러한 모든 설정을 수동으로 구성해야 합니다.
- threat defense를 CDO에 등록한 후 관리 인터페이스를 관리 인터페이스 또는 다른 데이터 인터페이스로 변경할 수 있습니다.
- 설정 마법사에서 설정한 FQDN이 이 인터페이스에 사용됩니다.
- 명령의 일부로 전체 디바이스 구성을 지울 수 있습니다. 복구 시나리오에서는 이 옵션을 사용할 수 있지만 초기 설정 또는 정상 작동에는 이 옵션을 사용하지 않는 것이 좋습니다.

- 데이터 관리를 비활성화하려면 **configure network management-data-interface disable** 명령을 입력합니다.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

단계 **6** CDO에서 생성한 **configure manager add** 명령을 사용하여 이 threat defense을 관리할 CDO를 식별합니다. 명령을 생성하려면 온보딩 마법사를 사용하여 디바이스 온보딩, on page 14의 내용을 참조하십시오.

Example:

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

기본 보안 정책 구성

이 섹션에서는 다음 설정을 사용해 기본 보안 정책을 구성하는 방법에 대해 설명합니다.

- 내부 및 외부 인터페이스 - 내부 인터페이스에 고정 IP 주소를 할당합니다. 관리자 액세스 설정의 일부로 외부 인터페이스의 기본 설정을 구성했지만 보안 영역에 할당해야 합니다.
- DHCP Server(DHCP 서버) - 클라이언트용 내부 인터페이스에서 DHCP 서버를 사용합니다.
- NAT - 외부 인터페이스에서 인터페이스 PAT를 사용합니다.
- Access control(액세스 제어) - 내부에서 외부로 향하는 트래픽을 허용합니다.
- SSH - 관리자 액세스 인터페이스에서 SSH를 활성화합니다.

인터페이스 구성

threat defense 인터페이스를 활성화하고, 보안 영역에 이를 할당하며, IP 주소를 설정합니다. 또한 분할 인터페이스를 설정합니다. 일반적으로 시스템이 의미 있는 트래픽을 전달하도록 최소 2개 이상의 인터페이스를 구성해야 합니다. 일반적으로 업스트림 라우터 또는 인터넷과 만나는 외부 인터페이스와 조직 네트워크에서 사용하는 하나 이상의 내부 인터페이스를 사용합니다. 이런 인터페이스의 일부는 웹 서버와 같이 공개적으로 액세스할 수 있는 에셋을 배치하는 '비무장지대(DMZ)'로 사용하게 됩니다.

일반적인 에지 라우팅 상황의 경우, 내부 인터페이스에서 정적 주소를 정의하는 반면 ISP에서 온 DHCP를 통해 외부 인터페이스 주소를 가져옵니다.

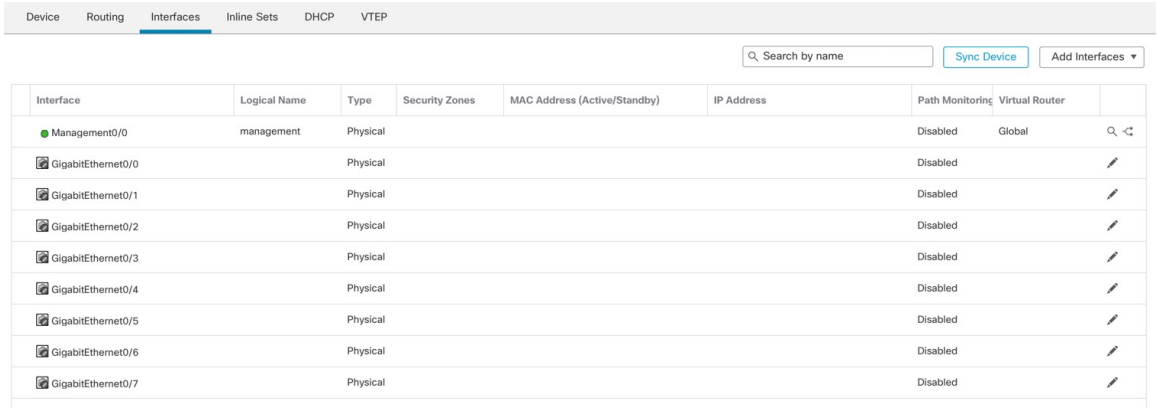
다음 예에서는 DHCP를 사용하는 외부 인터페이스에서 고정 주소 및 라우팅 모드를 사용하여 인터페이스 내부에 라우팅 모드를 구성합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 방화벽에 대해 수정( )를 클릭합니다.

단계 **2** **Interfaces(**인터페이스**)**를 클릭합니다.

그림 ***15: Interfaces***



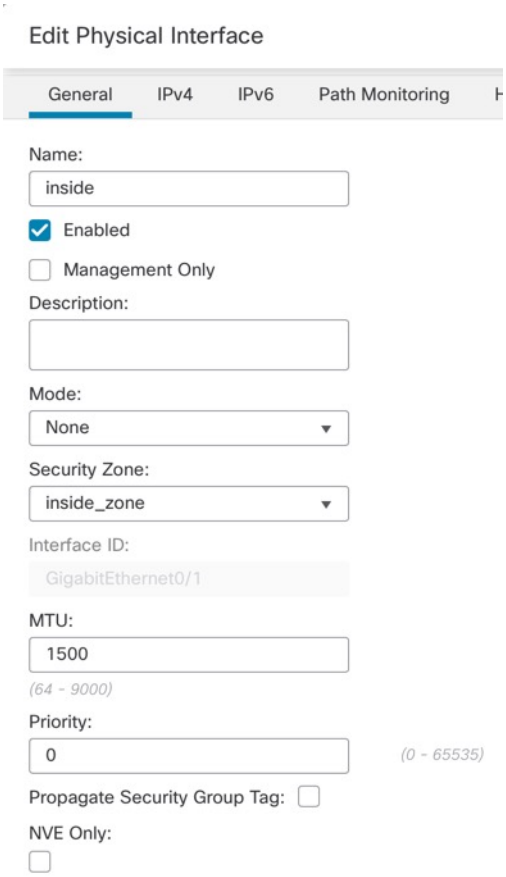
단계 **3** 40Gb 인터페이스(일부 모델에서 사용 가능)에서 10Gb 분할 인터페이스 4개를 생성하려면 인터페이스의 분할 아이콘을 클릭합니다.

구성에서 이미 40Gb 인터페이스를 사용한 경우 분할을 계속 진행하기 전에 구성을 제거해야 합니다.

단계 **4** 내부에 사용할 인터페이스의 수정( )를 클릭합니다.

General(일반**)** 탭이 표시됩니다.

그림 *16:* 일반 탭



a) **Name(**이름**)** 필드에 이름을 48자 이내로 입력합니다.

   예를 들어 인터페이스에 **inside**라는 이름을 지정합니다.

b) **Enable(**활성화**)** 확인란을 선택합니다.

c) **Mode(**모드**)**는 **None(**없음**)** 상태로 남겨둡니다.

d) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 내부 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

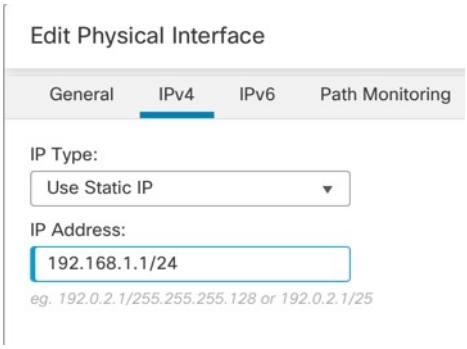
   예를 들어 **inside_zone**이라는 영역을 추가합니다. 각 인터페이스는 보안 영역 및/또는 인터페이스 그룹에 할당되어야 합니다. 인터페이스는 하나의 보안 영역에만 속할 수 있지만, 여러 인터페이스 그룹에 속할 수도 있습니다. 영역 또는 그룹을 기준으로 보안 정책을 적용합니다. 예를 들어 내부 인터페이스는 내부 영역에, 외부 인터페이스는 외부 영역에 할당할 수 있습니다. 트래픽이 내부에서 외부로는 이동하지만 외부에서 내부로는 이동할 수 없도록 액세스 제어 정책을 구성할 수 있습니다. 대부분의 정책은 보안 영역만 지원합니다. NAT 정책, 사전 필터 정책, QoS 정책에서 영역이나 인터페이스 그룹을 사용할 수 있습니다.

e) **IPv4** 및/또는 **IPv6** 탭을 클릭 합니다.

   - **IPv4** - 드롭다운 목록에서 **Use Static IP(**고정 **IP** 사용**)**를 선택하고 슬래시(/) 표기로 IP 주소와 서브넷 마스크를 입력합니다.

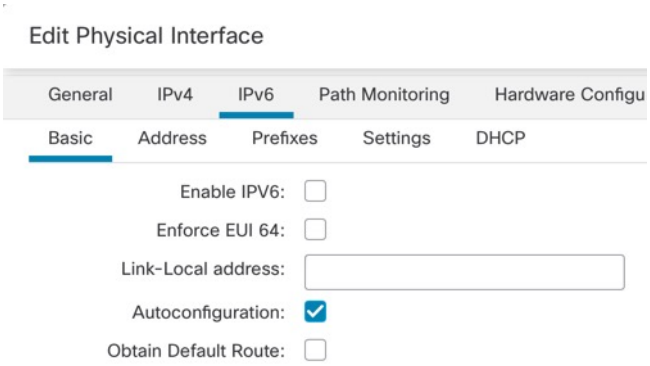
예를 들어 **192.168.1.1/24** 를 입력합니다.

그림 ***17: IPv4*** 탭



- **IPv6 -** 상태 비저장 자동 구성을 하려면 **Autoconfiguration(**자동 구성**)** 확인란을 선택합니다.

그림 ***18: IPv6*** 탭

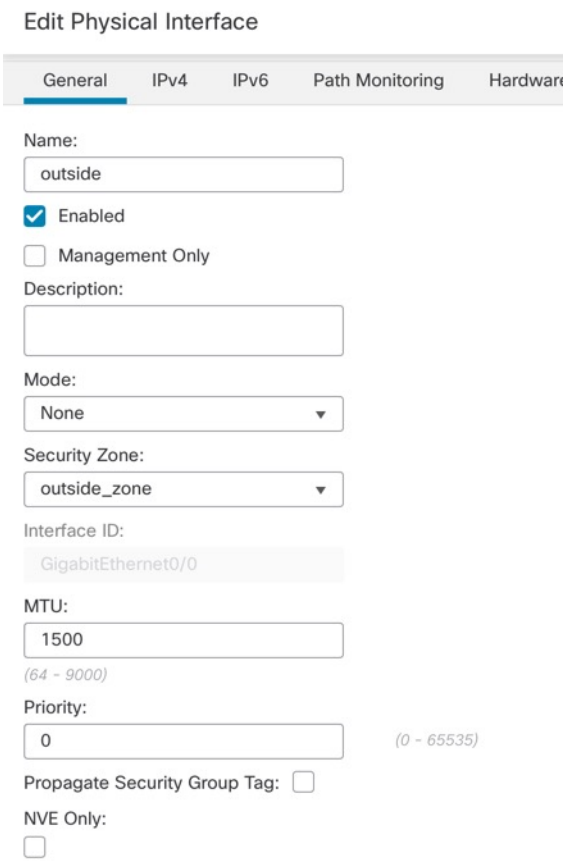


f) **OK(**확인**)**를 클릭합니다.

단계 **5** 외부에서 사용하려는 인터페이스의 수정( )를 클릭합니다.

General(일반**)** 탭이 표시됩니다.

그림 ***19:*** 일반 탭



관리자 액세스를 위해 이 인터페이스를 미리 구성했으므로 인터페이스의 이름이 이미 지정되고 활성화되어 있으며 주소가 지정됩니다. 이러한 기본 설정을 변경하면 management center 관리 연결이 중단되므로 이 설정을 변경하면 안됩니다. 트래픽 정책을 통해 이 화면에서 보안 영역을 구성해야 합니다.

a) **Security Zone(**보안 영역**)** 드롭다운 목록에서 기존의 외부 보안 영역을 선택하거나 **New(**새로 만들기**)**를 클릭하여 새 보안 영역을 추가합니다.

   예를 들어 **outside_zone**이라는 영역을 추가합니다.

b) **OK(**확인**)**를 클릭합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

DHCP 서버 구성

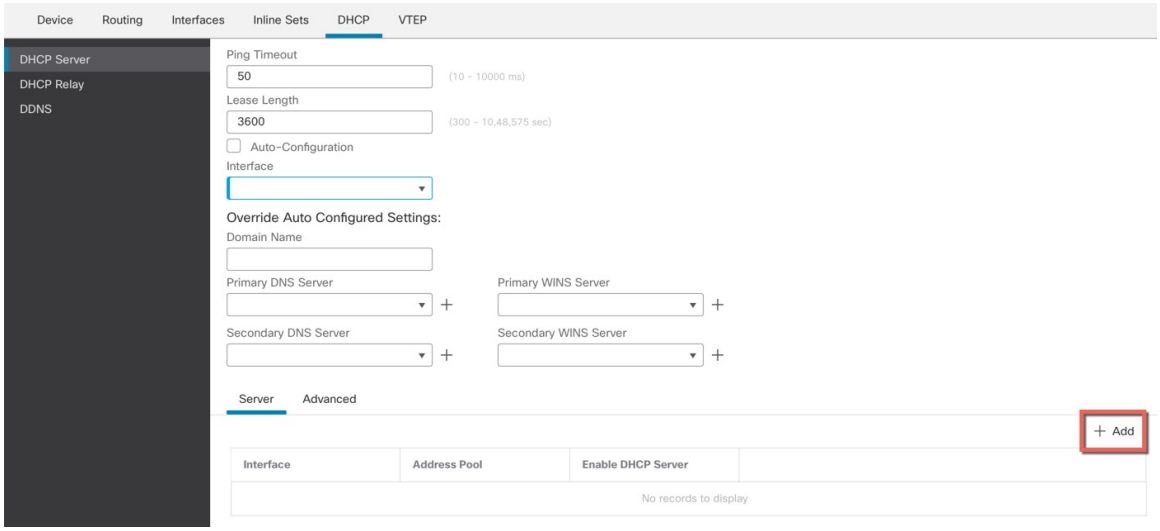
클라이언트가 DHCP를 사용하여 위협 방어에서 IP 주소를 가져오게 하려면 DHCP 서버를 활성화합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택하고 디바이스의 수정( )을 클릭합니다.

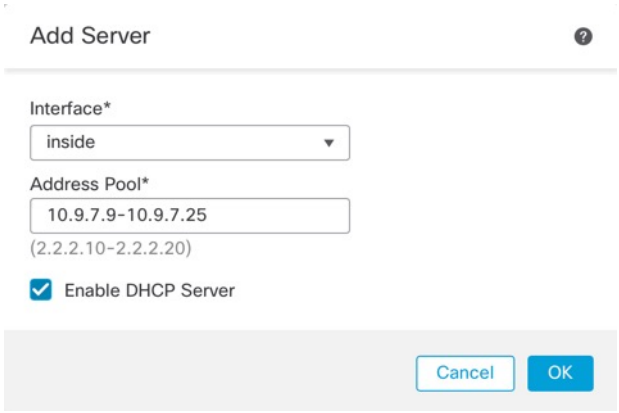
단계 **2** **DHCP** > **DHCP Server(DHCP** 서버**)**를 선택합니다.

그림 ***20: DHCP*** 서버



단계 **3** 서버 페이지에서 **Add(**추가**)**를 클릭하고 다음 옵션을 설정합니다.

그림 ***21:*** 서버 추가



- 인터페이스 - 드롭다운 목록에서 인터페이스를 선택합니다.
- **Address Pool(**주소 풀**)** - DHCP 서버에서 사용되는 최소 및 최대 IP 주소 범위를 설정합니다. 이 IP 주소 범위는 선택된 인터페이스와 동일한 서브넷에 있어야 하며, 인터페이스 자체의 IP 주소는 포함할 수 없습니다.
- **Enable DHCP Server(DHCP** 서버 활성화**)** - 선택한 인터페이스에서 DHCP 서버를 활성화합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

NAT 구성

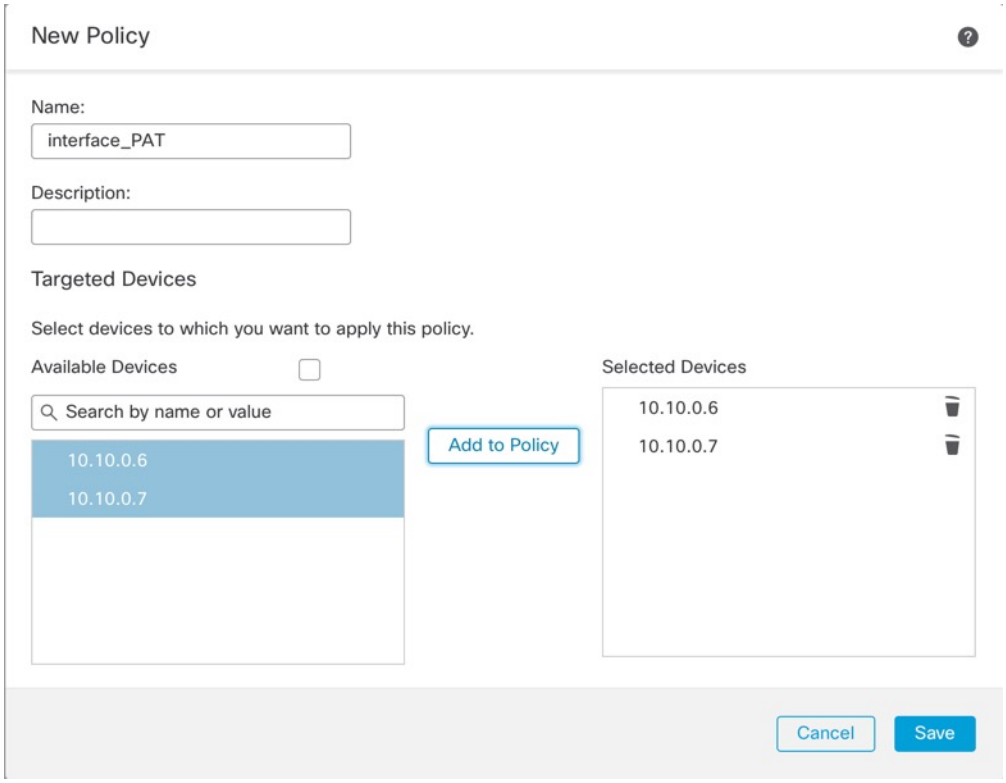
일반적인 NAT 규칙은 내부 주소를 외부 인터페이스 IP 주소의 포트로 변환합니다. 이러한 유형의 NAT 규칙을 인터페이스 포트 주소 변환*(PAT)*이라고 합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **NAT**를 선택하고, **New Policy(**새 정책**)** > **Threat Defense NAT**를 클릭합니다.

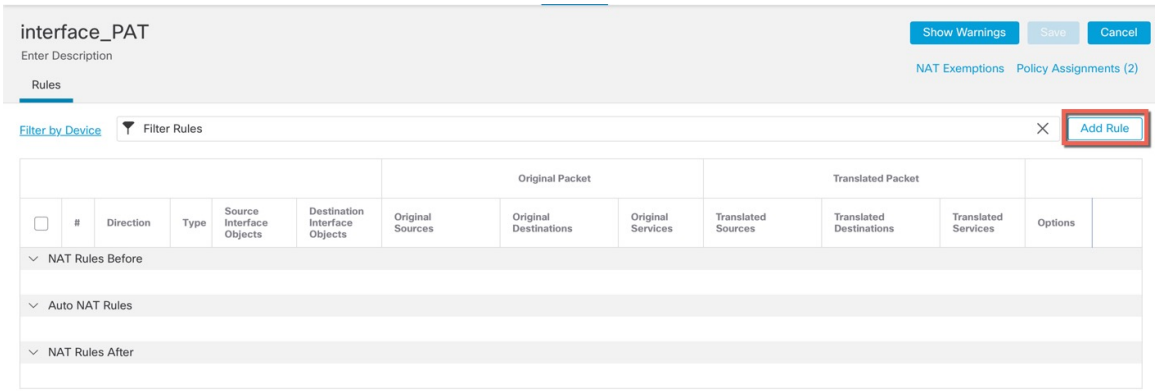
단계 **2** 정책 이름을 지정하고, 정책을 사용할 디바이스를 선택한 뒤 **Save(**저장**)**를 클릭합니다.

그림 ***22: New Policy***



정책이 management center을 추가합니다. 계속해서 정책에 규칙을 추가해야 합니다.

그림 *23: NAT* 정책

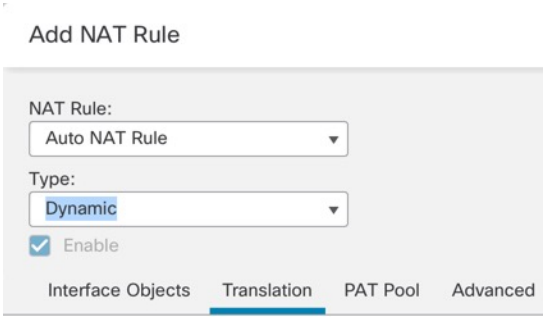


단계 **3** **Add Rule(**규칙 추가**)**을 클릭합니다.

Add NAT Rule(NAT 규칙 추가**)** 대화 상자가 나타납니다.

단계 **4** 기본 규칙 옵션을 구성합니다.

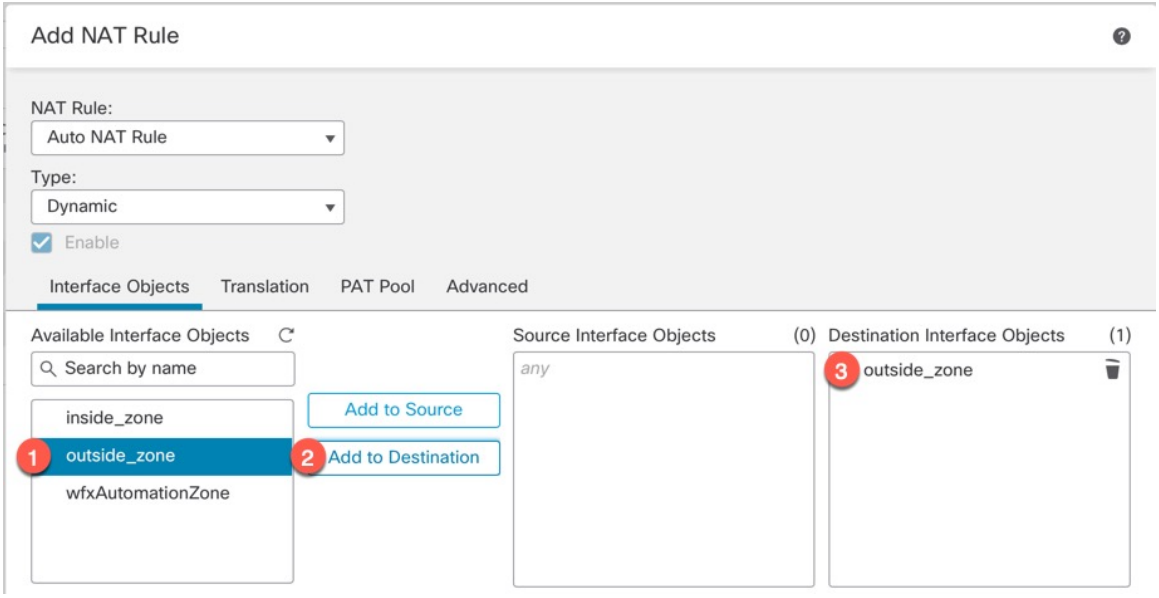
그림 *24:* 기본 규칙 옵션



- **NAT Rule(NAT** 규칙**) - Auto NAT Rule(**자동 **NAT** 규칙**)**을 선택합니다.
- **Type(**유형**) - Dynamic(**동적**)**을 선택합니다.

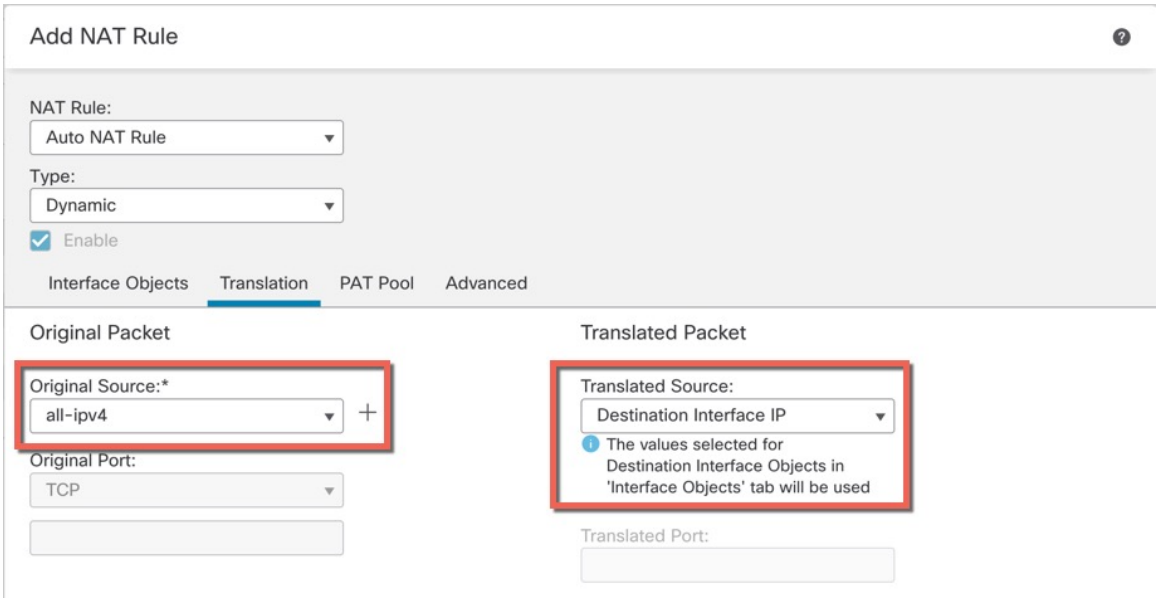
단계 **5** **Interface Objects(**인터페이스 개체**)** 페이지에서 **Available Interface Objects(**사용 가능한 인터페이스 개체**)** 영역의 외부 영역을 **Destination Interface objects(**대상 인터페이스 개체**)** 영역에 추가합니다.

그림 *25:* 인터페이스 객체



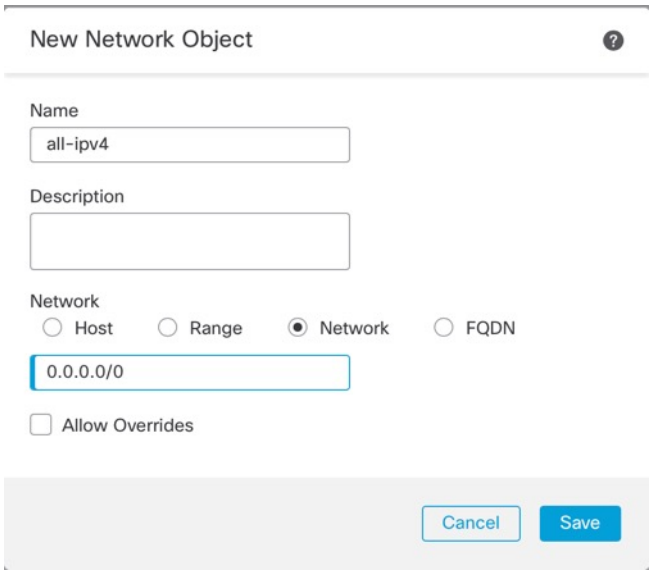
단계 **6** **Translation(**변환**)** 페이지에서 다음 옵션을 설정합니다.

그림 *26:* 변환



- **Original Source(**원본 소스**)**- 모든 IPv4 트래픽**(0.0.0.0/0)**에 대한 네트워크 개체를 추가하려면 추가(+)를 클릭합니다.

그림 *27:* 새 네트워크 개체



참고 자동 NAT 규칙은 개체 정의의 일부로 NAT를 추가하고 시스템 정의 개체를 수정할 수 없기 때문에 시스템에서 정의된 **any-ipv4** 개체를 사용할 수 없습니다.

- **Translated Source(**변환된 소스**) - Destination Interface IP(**대상 인터페이스 **IP)**를 선택합니다.

단계 **7** **Save(**저장**)**를 클릭하여 규칙을 저장하십시오.

규칙이 **Rules(**규칙**)** 테이블에 저장됩니다.

단계 **8** 변경 사항을 저장하려면 **NAT** 페이지에서 **Save(**저장**)**를 클릭합니다.

내부에서 외부로 트래픽을 허용합니다.

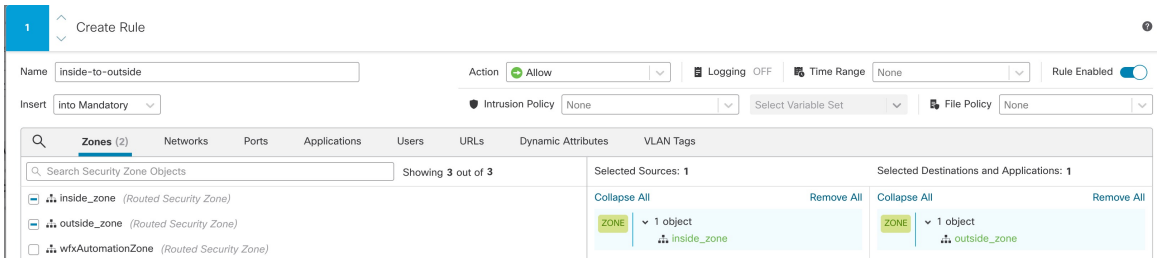
위협 방어를 등록할 때 기본 액세스 컨트롤 정책인 **Block all traffic(**모든 트래픽 차단**)**을 생성했다면, 디바이스에 트래픽을 허용하기 위해 정책에 규칙을 추가해야 합니다. 다음 절차에서는 내부 영역에서 외부 영역으로 향하는 트래픽을 허용하는 규칙을 추가합니다. 다른 영역이 있는 경우에는 적절한 네트워크에 대한 트래픽을 허용하는 규칙을 추가해야 합니다.

프로시저

단계 **1** **Policy(**정책**) > Access Policy(**액세스 정책**) > Access Policy(**액세스 정책**)**을 선택하고 위협 방어에 할당된 액세스 컨트롤 정책에 대해 수정( )를 클릭합니다.

단계 **2** **Add Rule(**규칙 추가**)**을 클릭하고 다음 매개변수를 설정합니다.

그림 *28:* 규칙 추가



- **Name (**이름**)** - 예를 들어 이 규칙의 이름을 **inside-to-outside**로 지정합니다.
- **Selected Sources(**선택한 원본**)**—**Zones(**영역**)**에서 내부 영역을 선택하고 **Add Source Zone(**원본 영역 추가**)**을 클릭합니다.
- **Selected Destinations and Applications(**선택한 대상 및 애플리케이션**)**—**Zones(**영역**)**에서 외부 영역을 선택하고 **Add Destination Zone(**대상 영역 추가**)**을 클릭합니다.

기타 설정은 변경하지 않습니다.

단계 **3** **Apply(**적용**)**를 클릭합니다.

규칙이 **Rules(**규칙**)** 테이블에 추가됩니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

관리자 액세스 데이터 인터페이스에서 SSH 구성

외부와 같은 데이터 인터페이스에서 management center 액세스를 활성화한 경우 이 절차를 사용하여 해당 인터페이스에서 SSH를 활성화해야 합니다. 이 섹션에서는 threat defense에서 하나 이상의 데이터 또는 진단 인터페이스에 대한 SSH 연결을 활성화하는 방법을 설명합니다.

참고 SSH는 관리 인터페이스에서 기본적으로 활성화됩니다. 하지만 이 화면은 관리 SSH 액세스에 영향을 미치지 않습니다.

관리 인터페이스는 디바이스에 있는 다른 인터페이스와 분리되어 있습니다. 이 인터페이스는 디바이스를 management center에 설치하고 등록하는 데 사용됩니다. 데이터 인터페이스용 SSH는 관리 인터페이스용 SSH로 내부 및 외부 사용자 목록을 공유합니다. 다른 설정은 별도로 구성됩니다. 데이터 인터페이스의 경우 이 화면을 사용하여 SSH 및 액세스 목록을 활성화합니다. 데이터 인터페이스용 SSH 트래픽은 일반 라우팅 구성을 사용하며 설치 또는 CLI에서 구성된 정적 경로는 사용하지 않습니다.

관리 인터페이스의 경우 SSH 액세스 목록을 구성하려면 Cisco Secure Firewall Threat Defense 명령 참조의 **configure ssh-access-list** 명령을 참조하십시오. 정적 경로를 구성하려면 **configure network static-routes** 명령을 참조하십시오. 기본적으로 초기 설정 시 관리 인터페이스를 통해 기본 경로를 구성합니다.

SSH를 사용하려면 호스트 IP 주소를 허용하는 액세스 규칙은 필요하지 않습니다. 이 섹션에 따라 SSH 액세스를 구성하면 됩니다.

연결할 수 있는 인터페이스에만 SSH를 사용할 수 있습니다. SSH 호스트가 외부 인터페이스에 있을 경우 외부 인터페이스와의 직접적인 관리 연결만 시작할 수 있습니다.

SSH는 다음과 같은 암호 및 키 교환을 지원합니다.

- 암호화—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- 무결성—hmac-sha2-256
- 키 교환 — dh-group14-sha256

참고 3회 연속 SSH를 사용한 CLI 로그인에 실패한 경우, 디바이스가 SSH 연결을 종료합니다.

Threat DefenseFeature History(기능 기록**)**

- 7.4—SSH에 대한 루프백 인터페이스 지원.

시작하기 전에

- **configure user add** 명령을 사용해 CLI에서 SSH 내부 사용자를 설정할 수 있습니다.의 내용을 참조하십시오. 기본적으로 초기 설정 중에 비밀번호를 구성한 관리자 사용자가 있습니다. 플랫폼 설정에서 **External Authentication(**외부 인증**)**을 구성하여 LDAP 또는 RADIUS에서 외부 사용자를 구성할 수도 있습니다.
- 디바이스에 SSH 연결을 허용할 호스트 또는 네트워크를 정의하는 네트워크 개체가 필요합니다. 이 절차의 일부로 개체를 추가할 수 있지만 개체 그룹을 사용하여 IP 주소 그룹을 식별하려면 규칙에 필요한 그룹이 이미 있는지 확인합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**를 선택하여 개체를 설정합니다.

참고 시스템에서 제공하는 **any** 네트워크 개체를 사용할 수 없습니다. 대신 **any-ipv4** 또는 **any-ipv6**를 사용합니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Platform Settings(**플랫폼 설정**)**를 선택하고 threat defense 정책을 생성하거나 편집합니다.

단계 **2** **SSH Access(SSH** 액세스**)**를 선택합니다.

단계 **3** SSH 연결을 허용하는 인터페이스와 IP 주소를 확인합니다.

이 테이블을 사용하여 SSH 연결을 허용할 인터페이스와 이러한 연결을 허용할 수 있는 클라이언트의 IP 주소를 제한합니다. 개별 IP 주소가 아닌 네트워크 주소를 사용할 수 있습니다.

a) **Add(**추가**)**를 클릭해 새 규칙을 추가하거나, **Edit(**편집**)**을 클릭해 기존 규칙을 편집합니다.
b) 규칙 속성을 구성합니다.

- **IP Address(IP** 주소**)** - SSH 연결을 허용하는 호스트 또는 네트워크를 식별하는 네트워크 개체 또는 그룹입니다. 드롭다운 메뉴에서 개체를 선택하거나 +를 클릭하여 새 네트워크 개체를 추가합니다.
- **Available Zones/Interfaces(**사용 가능한 영역/인터페이스**)** - SSH 연결을 허용할 인터페이스가 포함된 영역을 추가합니다. 영역에 없는 인터페이스의 경우 **Selected Zones/Interface(**선택한 영역/인터페이스**)** 목록 아래의 필드에 인터페이스 이름을 입력하고 **Add(**추가**)**를 클릭할 수 있습니다. 루프백 인터페이스 및 가상 라우터 인식 인터페이스를 추가할 수도 있습니다. 이 규칙은 디바이스에 선택한 인터페이스 또는 영역이 포함되어 있는 경우에만 디바이스에 적용됩니다.

c) **OK(**확인**)**를 클릭합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

이제 **Deploy(**구축**)** > **Deployment(**구축**)**로 이동하여 할당된 디바이스에 정책을 구축할 수 있습니다. 변경사항은 구축할 때까지 활성화되지 않습니다.

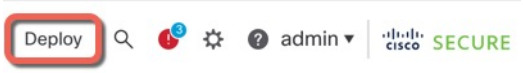
구성 구축

위협 방어에 설정 변경 사항을 구축합니다. 구축하기 전에는 디바이스에서 변경 사항이 활성 상태가 아닙니다.

프로시저

단계 **1** 우측 상단에서 **Deploy(**구축**)**를 클릭합니다.

그림 ***29:*** 구축



단계 **2** **Deploy All(**모두 구축**)**을 클릭하여 모든 디바이스에 구축하거나 **Advanced Deploy(**고급 구축**)**를 클릭하여 선택한 디바이스에 구축합니다.

그림 *30:* 모두 구축

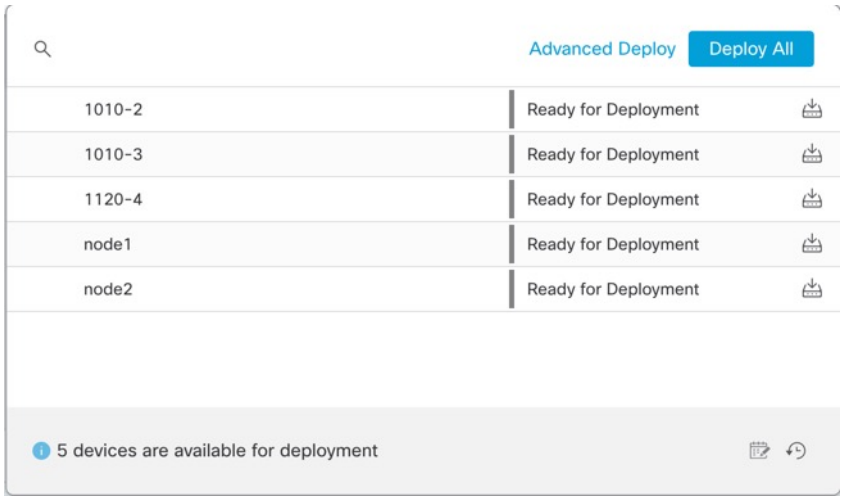
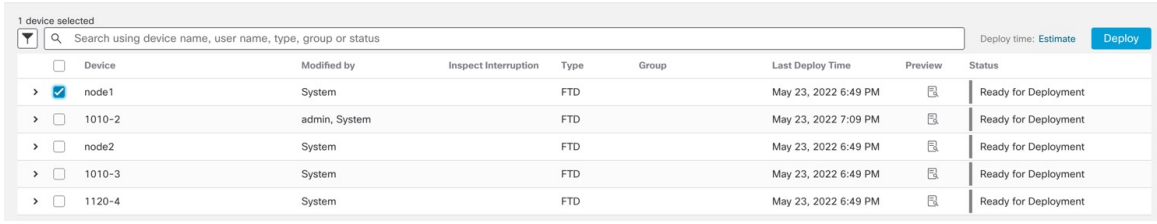
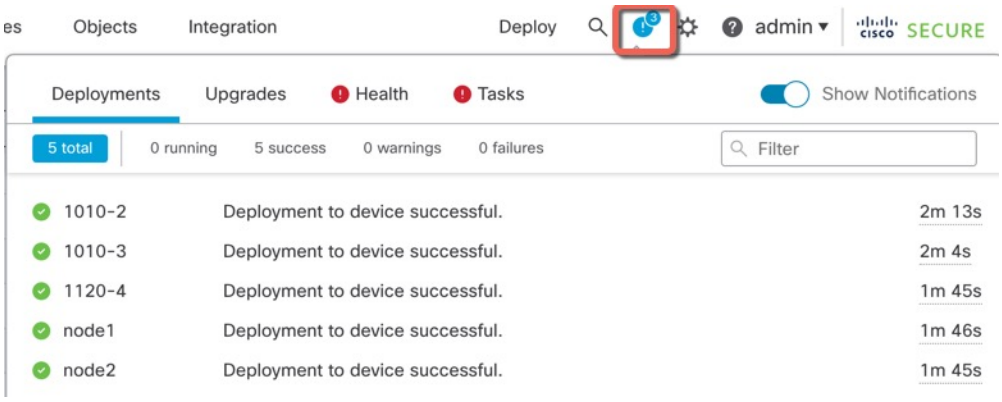


그림 *31:* 고급 구축



단계 **3** 구축이 성공하는지 확인합니다. 메뉴 모음의 **Deploy(구축)** 버튼 오른쪽에 있는 아이콘을 클릭하여 구축 상태를 확인합니다.

그림 *32:* 구축 상태



문제 해결 및 유지 보수

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 4200은 기본적으로 콘솔 케이블과 함께 제공되지 않으므로, 예를 들어 서드파티 USB-RJ-45 직렬 케이블을 구매해야 합니다. 운영 체제에 필요한 모든 USB 시리얼 드라이버를 설치해야 합니다. 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 Cisco 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#
```

데이터 인터페이스에서 관리 연결성 문제 해결

전용 관리 인터페이스를 사용하는 대신 관리자 데이터 인터페이스를 사용하는 경우, CDO에서 threat defense에 대한 인터페이스 및 네트워크 설정을 변경할 때 연결이 중단되지 않도록 주의해야 합니다. CDO에 threat defense를 추가한 후 관리 인터페이스 유형을 데이터에서 관리로 또는 관리에서 데이터로 변경하는 경우, 인터페이스 및 네트워크 설정이 올바르게 설정되지 않으면 관리 연결이 끊어질 수 있습니다.

이 주제는 관리 연결 끊김 문제를 해결하는 데 도움이 됩니다.

관리 연결 상태 보기

CDO의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Manager Access - Configuration Details(**관리자 액세스 - 구성 세부 사항**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

threat defense CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다. **sftunnel-status** 명령을 사용하여 전체 정보를 볼 수도 있습니다.

작동 중지된 연결에 대해서는 다음 샘플 출력을 참조하십시오. 다음과 같은 피어 채널이나 하트비트 정보가 "연결"되지 않았습니다.

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

피어 채널 및 하트비트 정보가 표시되는 작동 중인 연결에 대한 다음 샘플 출력을 참조하십시오.

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

threat defense 네트워크 정보 보기

threat defense CLI에서 관리 및 FMC 액세스 데이터 인터페이스 네트워크 설정을 확인합니다.

show network

```
> show network
===============[ System Information ]===============
Hostname                : ftd-1
DNS Servers             : 208.67.220.220,208.67.222.222
Management port         : 8305
IPv4 Default route
  Gateway               : data-interfaces
IPv6 Default route
  Gateway               : data-interfaces

=====================[ management0 ]=====================
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration           : Manual
Address                 : 10.99.10.4
Netmask                 : 255.255.255.0
Gateway                 : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration           : Disabled

===============[ Proxy Information ]================
State                   : Disabled
Authentication          : Disabled

======[ System Information - Data Interfaces ]======
DNS Servers             :
Interfaces              : Ethernet1/1

===============[ Ethernet1/1 ]===============
State                   : Enabled
Link                    : Up
Name                    : outside
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration           : Manual
Address                 : 10.89.5.29
```

```
Netmask                  : 255.255.255.192
Gateway                  : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration            : Disabled
```

threat defense가 **CDO**에 등록되었는지 확인합니다**.**

threat defense CLI에서 CDO 등록이 완료되었는지 확인합니다. 이 명령은 관리 연결의 현재 상태를 표시하지 않습니다.

show managers

```
> show managers
Type                     : Manager
Host                     : account1.app.us.cdo.cisco.com
Display name             : account1.app.us.cdo.cisco.com
Identifier               : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration             : Completed
Management type          : Configuration
```

CDO ping

FTD CLI에서 threat defense 다음 명령을 사용하여 데이터 인터페이스에서 CDO를 ping합니다.

ping *cdo_hostname*

threat defenseCLI에서 다음 명령을 사용하여 관리 인터페이스에서 CDO를 ping합니다. 이 인터페이스는 백플레인을 통해 데이터 인터페이스로 라우팅되어야 합니다.

ping system *cdo_hostname*

threat defense 내부 인터페이스에서 패킷 캡처

threat defense CLI에서 내부 백플레인 인터페이스(nlp_int_tap)의 패킷을 캡처하여 관리 패킷이 전송되는지 확인합니다.

capture *name* **interface nlp_int_tap trace detail match ip any any**

show capture *name* **trace detail**

내부 인터페이스 상태**,** 통계 및 패킷 수 확인

threat defense CLI에서 내부 백플레인 인터페이스, nlp_int_tap에 대한 정보를 참조하십시오.

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
```

```
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

라우팅 및 **NAT** 확인

threat defense CLI에서 기본 경로(S *)가 추가되었고 관리 인터페이스(nlp_int_tap)에 대한 내부 NAT 규칙이 있는지 확인합니다.

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
```

```
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

다른 설정 확인

다른 모든 설정이 있는지 확인하려면 다음 명령을 참조하십시오. CDO의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Manager Access - Configuration Details(**관리자 액세스 구성 디테일**)** > **CLI Output(CLI** 출력**)** 페이지에서 이러한 명령을 많이 볼 수 있습니다.

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *fmc_ip*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

성공적인 **DDNS** 업데이트 확인

threat defense CLI에서 DDNS 업데이트에 성공했는지 확인합니다.

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

업데이트가 실패하면 **debug http** 및 **debug ssl** 명령을 사용합니다. 인증서 검증에 실패한 경우, 다음을 통해 루트 인증서가 디바이스에 설치되어 있는지 확인합니다.

show crypto ca certificates *trustpoint_name*

DDNS 작업을 확인하려면 다음 명령을 사용하십시오.

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside
```

```
Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

CDO 로그 파일 확인

https://cisco.com/go/fmc-reg-error를 참조하십시오.

CDO가 연결을 상실할 경우 구성을 롤백

threat defense 관리를 위해 FTD에서 데이터 인터페이스를 사용하고 네트워크 연결에 영향을 주는 CDO 구성 변경 사항을 배포하는 경우 관리 연결을 복원할 수 있도록 threat defense의 구성을 마지막으로 배포된 구성으로 롤백할 수 있습니다. 그런 다음 네트워크 연결이 유지되도록 CDO에서 구성 설정을 조정하고 다시 배포할 수 있습니다. 연결이 끊기지 않아도 롤백 기능을 사용할 수 있습니다. 이는 이 문제 해결 상황으로 제한되지 않습니다.

다음 지침을 참조하십시오.

- 이전 배포만 threat defense에서 로컬로 사용할 수 있습니다. 이전 배포으로 롤백할 수 없습니다.
- 롤백은 CDO에서 설정할 수 있는 구성에만 영향을 미칩니다. 예를 들어 롤백은 threat defense CLI에서만 구성할 수 있는 전용 관리 인터페이스와 관련된 로컬 구성에 영향을주지 않습니다. **configure network management-data-interface** 명령을 사용하여 마지막 CDO 배포 후 데이터 인터페이스 설정을 변경한 다음 롤백 명령을 사용하면 해당 설정이 유지되지 않습니다. 마지막으로 배포된 CDO 설정으로 롤백됩니다.
- 이전 배포 중에 업데이트된 OOB(Out of Band) SCEP 인증서 데이터는 롤백할 수 없습니다.
- 롤백 중에는 현재 구성이 지워지므로 연결이 삭제됩니다.

프로시저

단계 **1** threat defense CLI에서 이전 구성으로 롤백합니다.

configure policy rollback

롤백 후 threat defense는 롤백이 성공적으로 완료되었음을 CDO에 알립니다. CDO에서 배포 화면에는 구성이 롤백되었음을 알리는 배너가 표시됩니다.

참고 롤백에 실패하고 CDO 관리가 복원된 경우, 일반적인 배포 문제에 대한 https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html을 참조하십시오. 경우에 따라 CDO 관리 액세스가 복원된 후 롤백이 실패할 수 있습니다. 이 경우 CDO 구성 문제를 해결하고 CDO에서 다시 배포할 수 있습니다.

예제:

관리자 액세스를 위해 데이터 인터페이스를 사용하는 threat defense의 경우:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

단계 **2** 관리 연결이 재설정되었는지 확인합니다.

CDO의 **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)** > **Device(**디바이스**)** > **Management(**관리**)** > **Manager Access - Configuration Details(**관리자 액세스 - 구성 세부 사항**)** > **Connection Status(**연결 상태**)** 페이지에서 관리 연결 상태를 확인합니다.

threat defense CLI에서 관리 연결 상태를 확인하는 **sftunnel-status-brief** 명령을 입력합니다.

연결을 다시 설정하는 데 10분 이상 걸릴 경우, 연결 문제를 해결해야 합니다. 데이터 인터페이스에서 관리 연결성 문제 해결, 37 페이지의 내용을 참조하십시오.

CDO를 사용하여 방화벽 전원 끄기

시스템을 올바르게 종료하는 것이 중요합니다. 단순히 전원을 분리하거나 전원 스위치를 누르는 경우 파일 시스템이 심각하게 손상될 수 있습니다. 항상 백그라운드에서 많은 프로세스가 실행되므로 전원을 분리하거나 종료하면 방화벽이 정상적으로 종료되지 않는다는 점에 유의하십시오.

management center를 사용하여 시스템을 올바르게 종료할 수 있습니다.

프로시저

단계 **1** **Devices(**디바이스**)** > **Device Management(**디바이스 관리**)**를 선택합니다.

단계 **2** 다시 시작할 디바이스 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **3** **Device(**디바이스**)** 탭을 클릭합니다.

단계 **4** **System(**시스템**)** 섹션에서 **Shut Down Device(**디바이스 종료**)**( )을 클릭합니다.

단계 **5** 메시지가 표시되면 디바이스 종료를 확인합니다.

단계 **6** 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 **7** 섀시가 성공적으로 꺼진 후에 필요한 경우 섀시에서 전원을 분리하여 물리적으로 제거할 수 있습니다.

다음 단계

threat defense를 사용하여 CDO를 계속 구성하려면 Cisco Defense Orchestrator 홈 페이지를 참조하십시오.