시작하기

다음 주제에서는 Secure Firewall Threat Defense(이전 Firepower Threat Defense) 컨피그레이션을 시작하는 방법을 설명합니다.

가이드의 적합성 확인

이 가이드에서는 위협 방어 디바이스에 포함된 Secure Firewall Device Manager(이전 Firepower Device Manager) 웹 기반 컨피그레이션 인터페이스를 사용하여 위협 방어를 컨피그레이션하는 방법을 설명합니다.

device manager 사용을 통해 중소규모 네트워크에서 가장 흔히 사용되는 소프트웨어의 기본 기능을 구성할 수 있습니다. Firepower Device Manager는 디바이스를 하나 또는 몇 개만 포함하는 네트워크 용도로 특별히 설계되어 고성능 다중 디바이스 관리자를 사용해 여러 위협 방어 디바이스가 포함된 대규모 네트워크를 제어하기를 원하지 않을 경우에 유용합니다.

다수의 디바이스를 관리하거나 위협 방어에서 허용하는 더 복잡한 기능 및 컨피그레이션을 사용하려는 경우에는 통합형 device manager 대신 Secure Firewall Management Center(이전 Firepower Management Center)를 사용하여 디바이스를 컨피그레이션하십시오.

Device Manager/Threat Defense 버전 7.3.0의 새로운 기능

릴리스 날짜**: 2022**년 **11**월 **29**일

다음 표에는 device manager를 사용하여 구성하면 사용할 수 있는 위협 방어 7.3.0의 새로운 기능이 나와 있습니다.

기능	설명
플랫폼 기능	
Secure Firewall 3105.	Secure Firewall 3105를 도입했습니다. 최소 위협 방어: 버전 7.3.1
Secure Firewall 4100용 네트워크 모듈	Secure Firewall 4100에 대해 다음과 같은 네트워크 모듈을 도입했습니다. • 2포트 100G 네트워크 모듈(FPR-NM-2X100G)
종료를 위한 ISA 3000 시스템 LED 지원	이 기능에 대한 지원 반환 ISA 3000을 종료하면 시스템 LED가 꺼집니다. 그런 다음 디바이스에서 전원을 제거하기 전에 10초 이상 기다립니다. 이 기능은 버전 7.0.5에서 도입되었지만 버전 7.1–7.2에서 일시적으로 사용이 중단되었습니다.
지원 종료: Firepower 4110, 4120, 4140, 4150	Firepower 4110, 4120, 4140 또는 4150에서는 버전 7.3 이상을 실행할 수 없습니다.
지원 종료: Firepower 9300: SM-24, SM-36, SM-44 모듈	SM-24, SM-36 또는 SM-44 모듈이 있는 Firepower 9300에서는 버전 7.3 이상을 실행할 수 없습니다.
Firepower 1010E는 지원되지 않습니다(임시).	버전 7.2.3에서 도입된 Firepower 1010E는 버전 7.3을 지원하지 않습니다. 지원은 향후 릴리스에서 다시 제공될 예정입니다. 버전 7.2.x Firepower 1010E를 버전 7.3으로 업그레이드할 수 없으며, 버전 7.3에서도 리이미징해서는 안 됩니다. 버전 7.3을 실행하는 Firepower 1010E 디바이스가 있는 경우 지원되는 릴리스로 이미지 재설치합니다.
방화벽 및 **IPS** 기능	

기능	설명
SSL 암호 해독 정책의 TLS 1.3 지원 및 암호 해독 불가 연결에 대한 구성 가능한 동작.	업그레이드 영향. TLS 1.3 트래픽에 대한 SSL 암호 해독 규칙을 구성합니다. TLS 1.3 지원은 Snort 3을 사용하는 경우에만 사용할 수 있습니다. 해독 불가 연결에 대해 기본이 아닌 동작을 구성할 수도 있습니다. Snort 3을 사용하는 경우 업그레이드 시 모든 SSL/TLS 버전이 선택된 규칙에 대해 TLS 1.3이 자동으로 선택됩니다. 그렇지 않으면 TLS 1.3이 선택되지 않습니다. Snort 2에서 Snort 3으로 전환하는 경우에도 동일한 동작이 발생합니다. 규칙 추가/수정 대화 상자의 고급 탭에서 TLS 1.3을 옵션으로 추가했습니다. 또한 TLS 1.3 암호 해독을 활성화하고 암호 해독할 수 없는 연결 작업을 구성하는 기능을 포함하도록 SSL 암호 해독 정책 설정을 재설계했습니다. 참조: SSL 암호 해독 규칙에 대한 고급 기준 및 고급 및 암호 해독 불가 트래픽 구성
구체화된 URL 필터링 조회.	이제 URL 필터링 조회가 발생하는 방식을 명시적으로 설정할 수 있습니다. 로컬 URL 데이터베이스만 사용하거나, 로컬 데이터베이스와 클라우드 조회를 모두 사용하거나, 클라우드 조회만 사용하도록 선택할 수 있습니다. URL 필터링 시스템 설정 옵션을 보강했습니다. 참조: URL 필터링 기본 설정 구성
메모리가 적은 디바이스의 경우 VDB가 작아집니다.	VDB 363 이상의 경우 시스템은 이제 Snort 2를 실행하는 메모리가 적은 디바이스에 더 작은 VDB(*VDB lite*라고도 함)를 설치합니다. 더 작은 VDB에는 동일한 애플리케이션이 포함되어 있지만, 탐지 패턴이 더 적습니다. 더 작은 VDB를 사용하는 디바이스는 전체 VDB를 사용하는 디바이스에 비해 일부 애플리케이션 식별을 누락할 수 있습니다. 참고 더 작은 VDB를 설치하는 기능은 버전 6.4.0.17부터 제공되지만 버전 6.5, 6.6, 6.7, 7.0–7.0.5, 7.1, 7.2.0–7.2.3 및 7.3.0–7.3.1에서는 일시적으로 사용되지 않습니다. 지원되는 버전에서 지원되지 않는 버전으로 업그레이드할 경우 Snort 2를 실행하는 메모리가 적은 디바이스에 363 이상 VDB를 설치할 수 없습니다. 더 낮은 메모리 디바이스: ASA 5506-X Series, ASA-5508-X, ASA-5512-X, 5515-X, 5516-X, 5525-X, 5545-X 참조: 시스템 데이터베이스 및 피드 업데이트
인터페이스 기능	

기능	설명
가상 어플라이언스에 대한 IPv6 지원.	위협 방어 가상은 이제 다음 환경에서 IPv6를 지원합니다. • AWS • Azure • KVM • VMWare 참조: Cisco Secure Firewall Threat Defense Virtual 시작 가이드
DHCPv6 클라이언트.	이제 DHCPv6에서 IPv6 주소를 가져올 수 있습니다. 신규/수정된 화면: **Device(**디바이스**)** > **Interfaces(**인터페이스**)** > **Edit Interface(**인터페이스 편집**)** > **Advanced(**고급**)** 참조: 고급 인터페이스 옵션 구성
관리 및 트러블슈팅 기능	
CA 번들을 자동으로 업데이트합니다.	업그레이드 영향**.** 로컬 CA 번들에는 여러 Cisco 서비스에 액세스하기 위한 인증서가 포함되어 있습니다. 이제 시스템은 매일 시스템 정의 시간에 새 CA 인증서를 자동으로 쿼리합니다. 이전에는 CA 인증서를 업데이트하려면 소프트웨어를 업그레이드해야 했습니다. CLI를 사용하여 이 기능을 비활성화할 수 있습니다. 신규/수정된 CLI 명령: **configure cert-update auto-update**, **configure cert-update run-now**, **configure cert-update test**, **show cert-update** 참조: Cisco Secure Firewall Threat Defense 명령 참조
신뢰할 수 있는 인증서에 대한 인증 기관 확인을 건너뜁니다.	로컬 CA 인증서를 신뢰할 수 있는 CA 인증서로 설치해야 하는 경우 확인을 건너뛸 수 있습니다. 신뢰할 수 있는 CA 인증서를 업로드할 때 **Skip CA Certificate Check(CA** 인증서 확인 건너뛰기**)** 옵션을 추가했습니다.

기능	설명
Secure Firewall 3100용 통합 업그레이드 및 설치 패키지.	

기능	설명
	이미지 재설치 영향. 버전 7.3에서는 다음과 같이 Secure Firewall 3100에 대한 위협 방어 설치 및 업그레이드 패키지를 통합했습니다. • 버전 7.1–7.2 설치 패키지: cisco-ftd-fp3k.*version*.SPA • 버전 7.1–7.2 업그레이드 패키지: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • 버전 7.3 이상 통합 패키지: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar 문제 없이 위협 방어를 업그레이드할 수 있지만, 이전 위협 방어 및 ASA 버전에서 직접 위협 방어 버전 7.3 이상으로 이미지 재설치할 수는 없습니다. 이는 새 이미지 유형에 필요한 ROMMON 업데이트 때문입니다. 이러한 이전 버전에서 이미지를 재설치하려면 이전 ROMMON에서 지원되지만 새 ROMMON으로 업데이트되는 ASA 9.19 이상을 "처리"해야 합니다. 별도의 ROMMON 업데이터는 없습니다. 위협 방어 버전 7.3 이상을 사용하기 위한 옵션은 다음과 같습니다. • Threat Defense 버전 7.1 또는 7.2에서 업그레이드 - 일반 업그레이드 프로세스를 사용합니다. 해당 업그레이드 가이드를 참조하십시오. • Threat Defense 버전 7.1 또는 7.2에서 이미지 재설치 - 먼저 ASA 9.19 이상으로 이미지 재설치한 다음 Threat Defense 버전 7.3 이상으로 이미지 재설치. Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드에서 *Threat Defense(*위협 방어*)→ASA: Firepower 1000, 2100; Secure Firewall 3100* 및 *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode(Firepower 1000, 2100* 어플라이언스 모드*) Secure Firewall 3100*을 참조하십시오. • ASA 9.17 또는 9.18에서 이미지 재설치 - ASA 9.19 이상으로 먼저 업그레이드한 다음 Threat Defense 버전 7.3 이상으로 이미지 재설치. Cisco Secure Firewall ASA 업그레이드 가이드를 참조한 다음 Cisco Secure Firewall ASA 및 Secure Firewall Threat Defense 이미지 재설치 가이드에서 *ASA→*위협 방어*: Firepower 1000, 2100* 어플라이언스 모드*, Secure Firewall 3100*을 참조하십시오. • 위협 방어 버전 7.3 이상에서 이미지 재설치 - 일반 이미지 재

기능	설명
	설치 프로세스를 사용합니다. Firepower Threat Defense를 사용하는 Firepower 1000/2100 및 Secure Firewall 3100용 Cisco FXOS 문제 해결 가이드에서 새 소프트웨어 버전으로 시스템 이미지 재설치를 참조하십시오.
Threat Defense REST API 버전 6.4(v6).	소프트웨어 버전 7.3의 위협 방어 REST API는 버전 6.4입니다. API URL의 v6를 사용하거나 /latest/를 사용하여 디바이스에서 지원되는 가장 최신 API 버전을 사용하고 있음을 나타내는 것이 좋습니다. 6.4의 URL 버전 경로 요소는 다른 6.x과 동일한 v6입니다. 사용 중인 리소스 모델에 변경 사항이 적용되었을 수 있으므로 모든 기존 호출을 다시 평가하십시오. 리소스를 확인할 수 있는 API Explorer를 열려면 device manager에 로그인한 다음, More options(추가 옵션) 버튼( )을 클릭하고 **API Explorer**를 선택합니다. 참조: Cisco Secure Firewall Threat Defense REST API 가이드

시스템 로그인

위협 방어 디바이스에 대한 인터페이스는 다음과 같이 두 개입니다.

Device Manager 웹 인터페이스

device manager가 웹 브라우저에서 실행됩니다. 이 인터페이스를 사용하여 시스템을 구성, 관리 및 모니터링합니다.

CLI(Command Line Interface, 콘솔**)**

CLI는 트러블슈팅에 사용합니다. device manager 대신 초기 설정에 사용할 수 있습니다.

다음 주제에서는 이러한 인터페이스에 로그인하고 사용자 어카운트를 관리하는 방법을 설명합니다.

볼 수 있는 정보와 수행할 수 있는 작업을 제어하는 사용자 역할

사용자 이름에는 역할이 할당되며, 역할에 따라 device manager에서 수행할 수 있는 작업이나 볼 수 있는 정보가 결정됩니다. 로컬 정의 관리 사용자에게는 모든 권한이 있지만 다른 어카운트를 사용하여 로그인하는 경우 권한이 줄어들 수 있습니다.

device manager 창의 오른쪽 상단 모서리에 사용자 이름과 권한 레벨이 표시됩니다.

권한은 다음과 같습니다.

- **Administrator(**관리자**)** - 모든 기능을 보고 사용할 수 있습니다.

- **Read-Write User(**읽기-쓰기 사용자**)** - 읽기 전용 사용자가 수행할 수 있는 모든 작업을 수행할 수 있지만 컨피그레이션 수정 및 구축도 수행할 수 있습니다 업그레이드 설치, 백업 생성 및 복원, 감사 로그 확인, 다른 device manager 사용자의 세션 종료를 포함하는 시스템의 중요 작업만 제한됩니다.
- **Read-Only User(**읽기 전용 사용자**)** - 대시보드 및 컨피그레이션을 볼 수는 있지만 변경할 수는 없습니다. 변경을 시도하면 권한이 없음을 설명하는 오류 메시지가 표시됩니다.

이러한 권한은 CLI 사용자에게 제공되는 권한과는 관련이 없습니다.

Device Manager에 로그인

device manager을 사용하여 시스템을 구성, 관리 및 모니터링합니다. 브라우저를 통해 구성할 수 있는 기능은 CLI(Command Line Interface)를 통해서는 구성할 수 없습니다. 즉, 반드시 웹 인터페이스를 사용하여 보안 정책을 구현해야 합니다.

아래 브라우저의 최신 버전인 Firefox, Chrome, Safari, Edge를 사용하십시오.

참고 잘못된 비밀번호를 입력하고 3회 연속하여 로그인 시도에 실패할 경우, 5분 동안 어카운트가 잠깁니다. 따라서 다시 로그인을 시도하기 전에 잠시 기다려야 합니다.

시작하기 전에

처음에는 관리자 사용자 이름만 사용하여 device manager에 로그인할 수 있습니다. 그러나 첫 로그인 이후에는 Device Manager 및 Threat Defense 사용자 액세스 관리의 설명에 따라 외부 AAA 서버에 정의된 추가 사용자에 대해 인증을 구성할 수 있습니다.

액티브 로그인은 한 번에 최대 5개까지 가능합니다. 여기에는 만료되지 않은 API 토큰으로 표시되는 디바이스 관리자 및 액티브 API 세션에 로그인한 사용자가 포함됩니다. 이 제한을 초과하면 가장 오래된 세션인 디바이스 관리자 로그인 또는 API 토큰이 만료되어 새 세션을 허용합니다. 이러한 제한은 SSH 세션에 적용되지 않습니다.

프로시저

단계 **1** 브라우저를 사용하여 시스템의 홈페이지(예: https://ftd.example.com)를 엽니다.

다음 주소 중 하나를 사용할 수 있습니다. IPv4 또는 IPv6 주소나 DNS 이름(구성한 경우)을 사용할 수 있습니다.

- 관리 주소. 기본적으로 대부분의 플랫폼에서 관리 인터페이스는 DHCP 클라이언트이므로 IP 주소는 DHCP 서버에 따라 달라집니다.
- HTTPS 액세스를 위해 연 데이터 인터페이스의 주소. 기본적으로 대부분의 플랫폼에서, "내부" 인터페이스는 HTTPS 액세스를 허용하므로 기본 내부 주소 192.16895.1에 연결할 수 있습니다. 모델의 내부 IP 주소에 대한 자세한 내용은 초기 설정 전의 기본 컨피그레이션, 27 페이지를 참조하십시오.

HTTPS 데이터 포트를 변경한 경우 URL에 맞춤형 포트를 포함해야 합니다. 예를 들어 포트를 4443으로 변경한 경우: https://ftd.example.com:4443과 같습니다.

팁 브라우저가 서버 인증서를 인식하도록 구성되어 있지 않으면 신뢰할 수 없는 인증서에 대한 경고가 표시됩니다. 해당 인증서를 예외적으로 수락하거나 신뢰할 수 있는 루트 인증서 저장소에 저장하십시오.

단계 **2** 디바이스용으로 정의된 사용자 이름 및 비밀번호를 입력한 다음 **Login(**로그인**)**을 클릭합니다.

미리 정의된 사용자인 관리 사용자 이름을 사용할 수 있습니다. 기본 관리자 비밀번호는 Admin123입니다. 초기 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않는 한 AWS에서 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.

비활성 상태가 30분 동안 유지되면 세션이 만료되며, 다시 로그인하라는 메시지가 표시됩니다. 페이지 오른쪽 상단에 있는 사용자 아이콘 드롭다운 메뉴에서 **Log Out(**로그아웃**)**을 선택하면 로그아웃할 수 있습니다.

CLI(Command Line Interface) 로그인

CLI(Command Line Interface)를 사용하여 시스템을 설정하고 기본적인 시스템 트러블슈팅을 수행합니다. CLI 세션을 통해 정책을 구성할 수는 없습니다.

CLI에 로그인하려면 다음 중 하나를 수행합니다.

- 디바이스에 포함된 콘솔 케이블을 사용하여 PC를 콘솔에 연결합니다(터미널 에뮬레이터 9600 보드, 8 데이터 비트, 패리티 없음, 1 정지 비트, 흐름 제어 없음). 콘솔 케이블에 대한 자세한 내용은 디바이스용 하드웨어 가이드를 참조하십시오.

참고 Firepower 및 Secure Firewall 디바이스 모델에서 콘솔 포트의 CLI는 Secure Firewall eXtensible Operating System(FXOS)입니다. 일부 디바이스 모델의 경우 **connect ftd** 명령을 사용하여 위협 방어 CLI에 액세스할 수 있습니다. Firepower 4100/9300의 경우, 애플리케이션 콘솔에 연결의 내용을 참조하십시오. FXOS CLI는 섀시 레벨 트러블슈팅에만 사용하십시오. 기본 컨피그레이션, 모니터링 및 일반 시스템 트러블슈팅 시에는 위협 방어 CLI를 사용합니다. FXOS 명령에 대한 자세한 내용은 FXOS 설명서를 참조하십시오.

- threat defense virtual의 경우에는 가상 콘솔을 엽니다.
- 관리 IP 주소에 연결하려면 SSH 클라이언트를 사용합니다. SSH 연결용 인터페이스를 여는 경우 데이터 인터페이스의 주소에 연결할 수도 있습니다(관리 액세스 목록 구성 참조). 데이터 인터페이스에 대한 SSH 액세스는 기본값으로 비활성화 상태입니다. 사용자 이름 **admin** 또는 다른 CLI

사용자 계정을 사용하여 로그인합니다. 기본 관리자 비밀번호는 Admin123입니다. AWS에서 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않은 경우 threat defense virtual에 대한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.

팁

- 로그인한 후 CLI에서 사용할 수 있는 명령에 대한 정보를 확인하려면 **help** 또는 **?**를 입력하십시오. 사용 정보는 http://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html에서 Cisco Firepower Threat Defense 명령 참조를 참조하십시오.
- **configure user add** 명령을 사용하면 CLI에 로그인할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. 그러나 이러한 사용자는 CLI에만 로그인할 수 있으며 device manager 웹 인터페이스에 로그인합니다.
- 외부 서버에서 SSH 액세스하기 위한 용도로 사용자 계정을 생성할 수 있습니다. SSH 액세스를 위한 외부 인증 컨피그레이션에 대한 내용은 Threat Defense CLI(SSH) 사용자를 위한 외부 권한 부여(AAA) 구성를 참조하십시오.

비밀번호 변경

비밀번호는 정기적으로 변경해야 합니다. 다음 절차에서는 device manager에 로그인한 상태에서 비밀번호를 변경하는 방법을 설명합니다.

참고 CLI에 로그인한 경우 **configure password** 명령을 사용하여 암호를 변경할 수 있습니다. **configure user password** *username* 명령을 사용해 다른 CLI 사용자의 암호를 변경할 수 있습니다.

시작하기 전에

이 절차는 로컬 사용자에게만 적용됩니다. 사용자 어카운트가 외부 AAA 서버에 정의되어 있는 경우에는 해당 서버를 사용하여 비밀번호를 변경해야 합니다.

프로시저

단계 **1** 메뉴 오른쪽 위에 있는 사용자 아이콘 드롭다운 목록에서 **Profile(**프로파일**)**을 선택합니다.

단계 **2** **Password(**비밀번호**)** 탭을 클릭합니다.

단계 **3** 현재 비밀번호를 입력합니다.

단계 **4** 새 비밀번호를 입력하고 확인을 위해 다시 한 번 입력합니다.

Generate(생성**)**를 클릭하여 임의의 16자 비밀번호를 생성할 수 있습니다. 마스크 해제된 비밀번호를 보려면 Show Password(비밀번호 표시) ( ) 버튼을 클릭합니다. 그런 다음 **Copy To Clipboard(**클립보드에 복사**)** 링크를 클릭하여 확인 필드에 비밀번호를 붙여넣을 수 있습니다.

이 페이지에는 비밀번호에 대한 최소 요구 사항이 나와 있습니다. 이러한 최소 요구 사항은 변경할 수 없습니다. 비밀번호는 다음 조건을 충족해야 합니다.

- 8자 ~ 128자 길이
- 소문자 및 대문자를 각각 1개 이상 포함
- 1자리 이상
- 특수 문자 1개 이상 포함
- 반복되는 문자 없음

단계 **5** **Change(**변경**)**를 클릭합니다.

사용자 프로파일 환경 설정 지정

사용자 인터페이스의 기본 설정을 설정하고 비밀번호를 변경할 수 있습니다.

프로시저

단계 **1** 메뉴 오른쪽 위에 있는 사용자 아이콘 드롭다운 목록에서 **Profile(**프로파일**)**을 선택합니다.

단계 **2** **Profile(**프로파일**)** 탭에서 다음 항목을 구성하고 **Save(**저장**)**를 클릭합니다.

- 작업 예약을 위한 시간대 - 백업 및 업데이트와 같은 작업을 예약하는 데 사용할 시간대를 선택합니다. 다른 시간대를 설정하는 경우 대시보드와 이벤트에 브라우저 시간대가 사용됩니다.
- 색 구성표 - 사용자 인터페이스에 사용할 색 구성표를 선택합니다.

단계 **3** **Password(**비밀번호**)** 탭에서 새 비밀번호를 입력하고 **Change(**변경**)**를 클릭할 수 있습니다.

시스템 설정

초기 컨피그레이션을 완료해야 네트워크에서 시스템이 정상적으로 작동합니다. 올바른 배포에는 케이블을 적절하게 연결하는 작업과 디바이스를 네트워크에 삽입하고 인터넷 또는 기타 업스트림 라우터에 연결하는 데 필요한 주소를 구성하는 작업이 포함됩니다. 다음 절차에서는 이러한 프로세스에 대해 설명합니다.

시작하기 전에

초기 설정을 시작하기 전에 디바이스에는 일부 기본 설정이 포함되어 있습니다. 자세한 내용은 초기 설정 전의 기본 컨피그레이션, 27 페이지를 참조해 주십시오.

프로시저

단계 **1** 인터페이스 연결, 12 페이지

단계 **2** 설정 마법사를 사용하여 초기 컨피그레이션 완료, 23 페이지

이 프로세스의 결과로 생성되는 컨피그레이션에 대한 자세한 내용은 초기 설정 후의 컨피그레이션, 30 페이지를 참조하십시오.

인터페이스 연결

기본 컨피그레이션에서는 특정 인터페이스가 내부 및 외부 네트워크에 사용된다고 가정합니다. 이러한 가정에 따라 인터페이스에 네트워크 케이블을 연결하면 초기 컨피그레이션을 더욱 쉽게 완료할 수 있습니다.

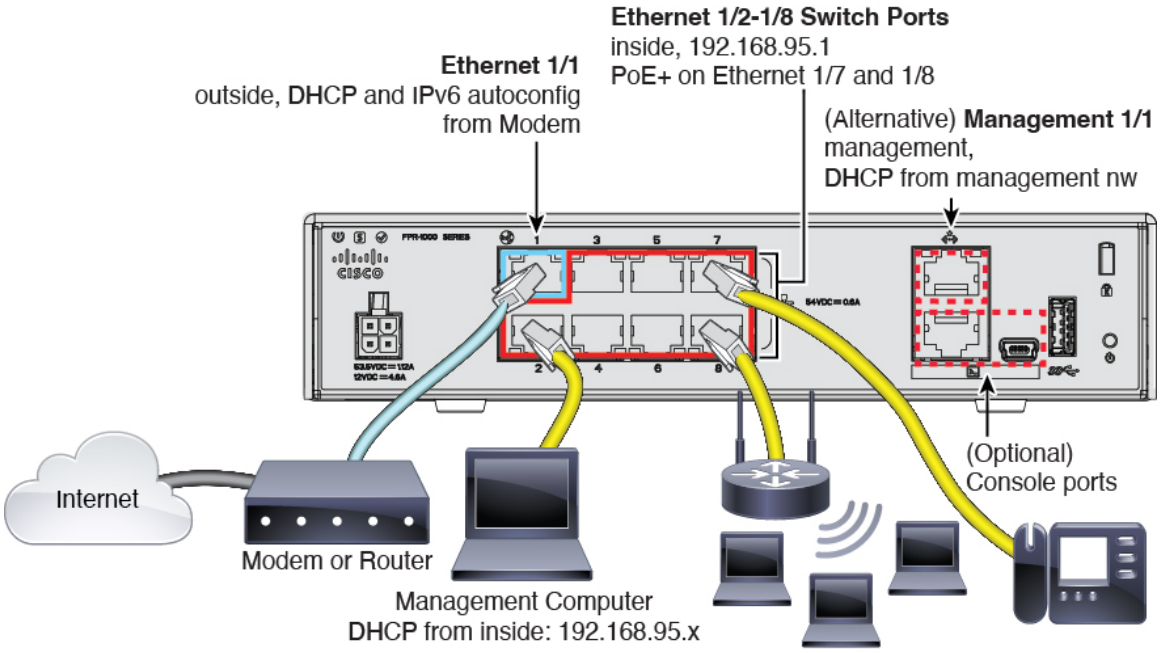
대부분 모델의 기본 컨피그레이션에서는 내부 인터페이스에 관리 컴퓨터를 연결할 수 있습니다. 워크스테이션을 관리 포트에 직접 연결할 수도 있습니다. 인터페이스는 서로 다른 네트워크에 있으므로 내부 인터페이스와 관리 포트를 같은 네트워크에 연결하지 마십시오.

활성 DHCP 서버가 있는 네트워크에 또는 내부 인터페이스를 연결하지 마십시오. 이와 같이 연결하면 내부 인터페이스에서 이미 실행 중인 DHCP 서버와 충돌하게 됩니다. 네트워크에 다른 DHCP 서버를 사용하려면 초기 설정 후 원치 않는 DHCP 서버를 비활성화하십시오.

다음 항목에서는 내부 인터페이스를 사용하여 디바이스를 구성할 때 이 토폴로지에 대해 시스템을 케이블 연결하는 방법을 설명합니다.

Firepower 1010 케이블 연결

그림 *1: Firepower 1010* 케이블 연결



- 다음 인터페이스 중 하나에 관리 컴퓨터를 연결합니다.
  - Ethernet 1/2~1/8 — 관리 컴퓨터를 내부스위치 포트(Ethernet 1/2~1/8) 중 하나에 직접 연결합니다. 내부에는 기본 IP 주소(192.168.95.1)가 있으며, DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다.
  - Management 1/1 — 관리 컴퓨터를 관리 네트워크에 연결합니다. Management 1/1 인터페이스는 DHCP에서 IP 주소를 가져오므로, 네트워크에 DHCP 서버가 포함되어 있어야 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, 22 페이지의 내용을 참조하십시오.

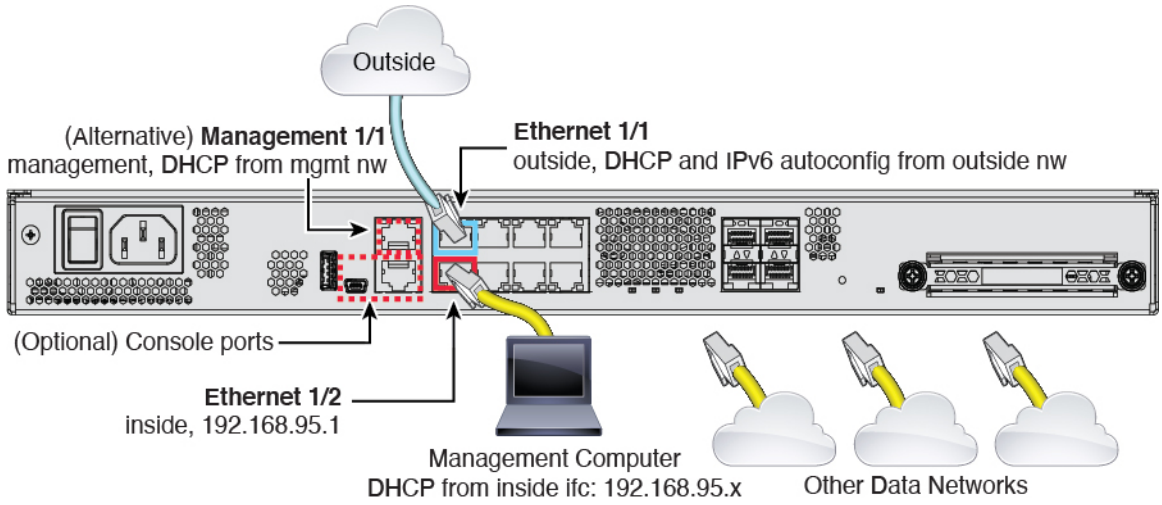
  나중에 다른 인터페이스에서 관리 액세스를 구성할 수 있습니다.
- 외부 네트워크를 Ethernet 1/1 인터페이스에 연결합니다.

  기본적으로는 IPv4 DHCP 및 IPv6 자동 설정을 사용하여 IP 주소를 가져오지만 초기 설정 중에 고정 주소를 설정할 수 있습니다.
- 나머지 스위치 포트(Ethernet 1/2~1/8)에 내부 디바이스를 연결합니다.

  Ethernet 1/7 및 1/8은 PoE+(Power over Ethernet+) 포트입니다.

Firepower 1100 케이블 연결

그림 *2: Firepower 1100* 케이블 연결



- 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. Ethernet 1/2에는 기본 IP 주소 (192.168.95.1)가 있는 Ethernet 1/2에서는 DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다.
  - Management 1/1(MGMT로 레이블이 지정됨) — 관리 컴퓨터를 관리 네트워크에 연결합니다. Management 1/1 인터페이스는 DHCP에서 IP 주소를 가져오므로, 네트워크에 DHCP 서버가 포함되어 있어야 합니다.

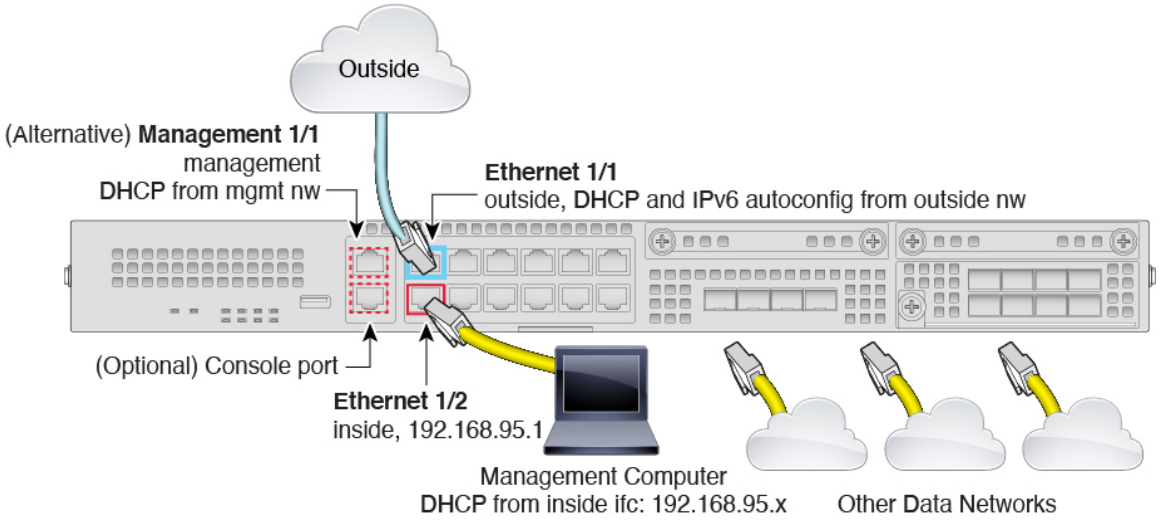
    Management 1/1 IP 주소를 기본값에서 변경하여 정적 IP 주소를 구성해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 22 페이지의 내용을 참조하십시오.

  나중에 다른 인터페이스에서 관리 액세스를 구성할 수 있습니다.
- 외부 네트워크를 Ethernet1/1 인터페이스(WAN으로 레이블이 지정됨)에 연결합니다.

  기본적으로는 IPv4 DHCP 및 IPv6 자동 설정을 사용하여 IP 주소를 가져오지만 초기 설정 중에 고정 주소를 설정할 수 있습니다.
- 나머지 인터페이스에 다른 네트워크를 연결합니다.

Firepower 2100 케이블 연결

그림 *3: Firepower 2100* 케이블 연결



- 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. Ethernet 1/2에는 기본 IP 주소 (192.168.95.1)가 있고, DHCP 서버를 실행하여 클라이언트(관리 컴퓨터 포함)에 IP 주소를 제공하므로 이러한 설정이 기존의 내부 네트워크 설정과 충돌하지 않도록 합니다.
  - Management 1/1(MGMT로 레이블이 지정됨) — 관리 컴퓨터를 관리 네트워크에 연결합니다. Management 1/1 인터페이스는 DHCP에서 IP 주소를 가져오므로, 네트워크에 DHCP 서버가 포함되어 있어야 합니다.

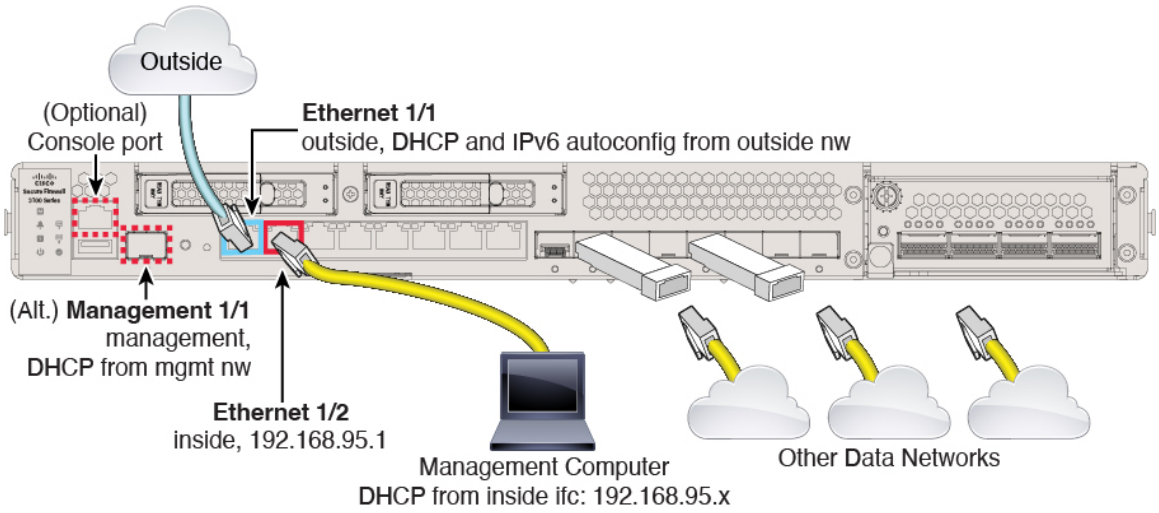
    Management 1/1 IP 주소를 기본값에서 변경하여 정적 IP 주소를 구성해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 22 페이지의 내용을 참조하십시오.

  나중에 다른 인터페이스에서 관리 액세스를 구성할 수 있습니다.
- 외부 네트워크를 Ethernet1/1 인터페이스(WAN으로 레이블이 지정됨)에 연결합니다.

  기본적으로는 IPv4 DHCP 및 IPv6 자동 설정을 사용하여 IP 주소를 가져오지만 초기 설정 중에 고정 주소를 설정할 수 있습니다.
- 나머지 인터페이스에 다른 네트워크를 연결합니다.

Secure Firewall 3100 케이블 연결

그림 *4: Secure Firewall 3100* 케이블 연결



관리 1/1 또는 이더넷 1/2에서 threat defense 디바이스를 관리합니다. 기본 구성에서는 Ethernet1/1을 외부로도 구성합니다.

- 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.
  - 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, 22 페이지의 내용을 참조하십시오.

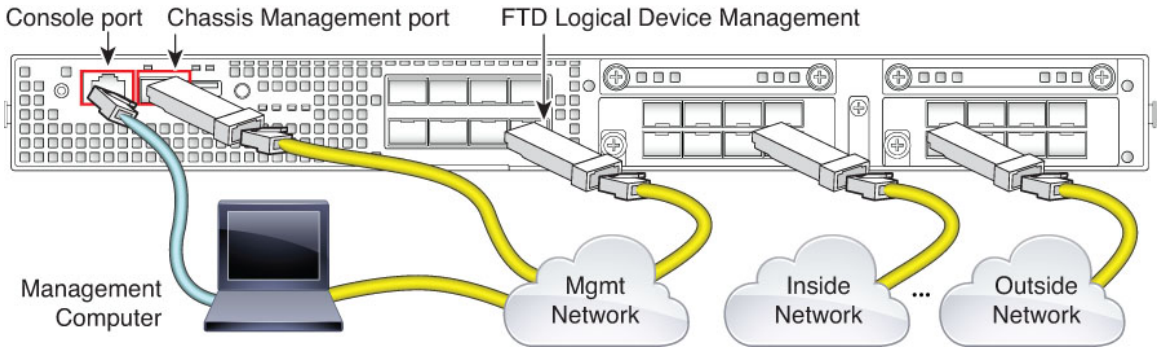
참고 관리 1/1은 SFP 모듈이 필요한 10Gb 파이버 인터페이스입니다.

- 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.

- 나머지 인터페이스에 다른 네트워크를 연결합니다.

Firepower 4100 케이블 연결



논리적 디바이스 관리 인터페이스에서 초기 위협 방어 구성을 수행합니다. 나중에 어느 데이터 인터페이스에서든지 관리를 활성화할 수 있습니다. 위협 방어 디바이스에서는 라이선싱 및 업데이트를 위해 인터넷에 액세스해야 하며, 기본 동작은 디바이스를 구축할 때 지정한 게이트웨이 IP 주소로 관리 트래픽을 라우팅하는 것입니다. 백플레인을 통해 관리 트래픽을 데이터 인터페이스로 대신 라우팅하려는 경우, 나중에 device manager에서 해당 설정을 구성할 수 있습니다.

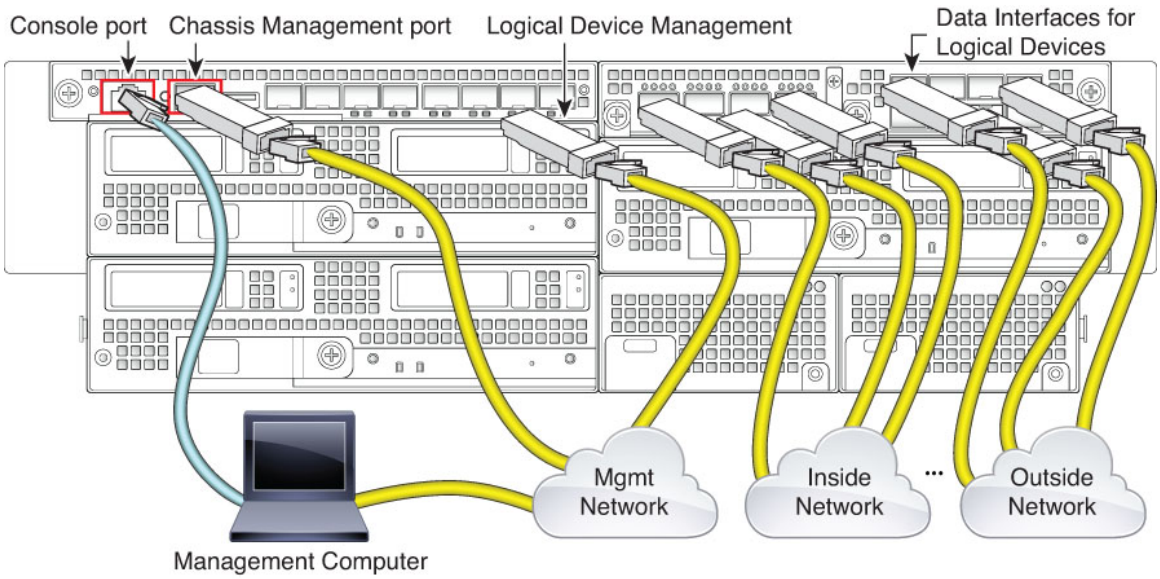
초기 섀시 설정, 지속적인 모니터링 및 논리적 디바이스 사용을 위해 다음 인터페이스에 케이블을 연결합니다.

- 콘솔 포트 — 섀시의 초기 설정을 수행하기 위해 관리 컴퓨터를 콘솔 포트에 연결합니다. Firepower 4100에는 RS-232 대 RJ-45 시리얼 콘솔 케이블이 포함되어 있습니다. 연결을 설정하려면 서드파티 시리얼-USB 케이블을 사용해야 할 수도 있습니다.
- 섀시 관리 포트 — 구성 및 지속적인 섀시 관리를 위해 섀시 관리 포트를 관리 네트워크에 연결합니다.
- Threat Defense 논리적 디바이스 관리 인터페이스 - FXOS 관리를 위해 예약된 섀시 관리 포트 이외에, 이 목적을 위해 섀시에서 어느 인터페이스든지 선택할 수 있습니다.
- 데이터 인터페이스 — 데이터 인터페이스를 논리적 디바이스 데이터 네트워크에 연결합니다. 물리적 인터페이스, EtherChannel 및 브레이크아웃 포트를 구성하여 고용량 인터페이스를 나눌 수 있습니다.

  고가용성을 위해서는 장애 조치/상태 링크에 데이터 인터페이스를 사용합니다.

참고 콘솔 포트 이외의 모든 인터페이스에는 SFP/SFP+/QSFP 트랜시버가 필요합니다. 지원되는 트랜시버에 대한 하드웨어 설치 가이드를 참조하십시오.

Firepower 9300 케이블 연결



논리적 디바이스 관리 인터페이스에서 초기 위협 방어 구성을 수행합니다. 나중에 어느 데이터 인터페이스에서든지 관리를 활성화할 수 있습니다. 위협 방어 디바이스에서는 라이선싱 및 업데이트를 위해 인터넷에 액세스해야 하며, 기본 동작은 디바이스를 구축할 때 지정한 게이트웨이 IP 주소로 관리 트래픽을 라우팅하는 것입니다. 백플레인을 통해 관리 트래픽을 데이터 인터페이스로 대신 라우팅하려는 경우, 나중에 device manager에서 해당 설정을 구성할 수 있습니다.

초기 섀시 설정, 지속적인 모니터링 및 논리적 디바이스 사용을 위해 다음 인터페이스에 케이블을 연결합니다.

- 콘솔 포트 — 섀시의 초기 설정을 수행하기 위해 관리 컴퓨터를 콘솔 포트에 연결합니다. Firepower 9300에는 RS-232 대 RJ-45 시리얼 콘솔 케이블이 포함되어 있습니다. 연결을 설정하려면 서드파티 시리얼-USB 케이블을 사용해야 할 수도 있습니다.
- 섀시 관리 포트 — 구성 및 지속적인 섀시 관리를 위해 섀시 관리 포트를 관리 네트워크에 연결합니다.
- 논리적 디바이스 관리 인터페이스 — 하나 이상의 인터페이스를 사용하여 논리적 디바이스를 관리합니다. FXOS 관리를 위해 예약된 섀시 관리 포트 이외에, 이 목적을 위해 섀시에서 어느 인터페이스든지 선택할 수 있습니다. 관리 인터페이스는 논리적 디바이스 간에 공유될 수 있습니다. 또는 논리적 디바이스마다 별도의 인터페이스를 사용할 수 있습니다. 일반적으로는 관리 인터페이스를 모든 논리적 디바이스와 공유하며, 별도의 인터페이스를 사용하는 경우에는 단일 관리 네트워크에 배치합니다. 그러나 정확한 네트워크 요구 사항은 달라질 수 있습니다.
- 데이터 인터페이스 — 데이터 인터페이스를 논리적 디바이스 데이터 네트워크에 연결합니다. 물리적 인터페이스, EtherChannel 및 브레이크아웃 포트를 구성하여 고용량 인터페이스를 나눌 수 있습니다. 네트워크 요구 사항에 따라 여러 논리적 디바이스를 동일한 네트워크 또는 서로 다른 네트워크에 케이블로 연결할 수 있습니다. 모든 트래픽은 하나의 인터페이스에서 섀시를 종료하고 다른 인터페이스로 돌아가서 다른 논리적 디바이스에 연결해야 합니다.

  고가용성을 위해서는 장애 조치/상태 링크에 데이터 인터페이스를 사용합니다.

참고 콘솔 포트 이외의 모든 인터페이스에는 SFP/SFP+/QSFP 트랜시버가 필요합니다. 지원되는 트랜시버에 대한 하드웨어 설치 가이드를 참조하십시오.

Threat Defense Virtual 가상 케이블 연결

threat defense virtual을 설치하려면 http://www.cisco.com/c/en/us/support/security/firepower-ngfw-virtual/products-installation-guides-list.html에서 사용 중인 가상 플랫폼용 빠른 시작 가이드를 참조하십시오. device manager는 가상 플랫폼인 VMware, KVM, Microsoft Azure, AWS(Amazon Web Services)에서 지원됩니다.

threat defense virtual 기본 컨피그레이션에서는 관리 인터페이스와 내부 인터페이스를 동일한 서브넷에 배치합니다. 스마트 라이선싱을 사용하고 시스템 데이터베이스로 업데이트를 가져오려면 관리 인터페이스에서 인터넷에 연결할 수 있어야 합니다.

따라서 기본 컨피그레이션은 가상 스위치의 동일한 네트워크에 Management0/0 및 GigabitEthernet0/1(내부)을 둘 다 연결할 수 있도록 설계되어 있습니다. 기본 관리 주소는 내부 IP 주소를 게이트웨이로 사용합니다. 그러므로 관리 인터페이스는 인터넷에 연결하기 위해 내부 인터페이스와 외부 인터페이스를 차례로 통과하여 라우팅합니다.

인터넷에 액세스할 수 있는 네트워크를 사용한다면 내부 인터페이스에 사용하는 것과는 다른 서브넷에 Management0/0을 연결할 수도 있습니다. 이 경우 네트워크용으로 관리 인터페이스 IP 주소 및 게이트웨이를 적절하게 구성해야 합니다.

관리 인터페이스 IP 설정은 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**에서 정의합니다. 여기서 정의하는 IP 주소는 **Device(**디바이스**)** > **Interfaces(**인터페이스**)** > **View Configuration(**설정 보기**)**에 나와 있는 Management0/0(진단) 인터페이스용 IP 주소와는 동일하지 않습니다.

VMware 네트워크 어댑터 및 인터페이스가 Threat Defense 물리적 인터페이스에 매핑되는 방식

최대 10개의 인터페이스를 VMware threat defense virtual 디바이스용으로 구성할 수 있습니다. 최소 4개의 인터페이스를 구성해야 합니다.

Management0-0 소스 네트워크가 인터넷에 액세스할 수 있는 VM 네트워크에 연결되었는지 확인하십시오. 시스템이 Cisco Smart Software Manager에 연결하고 시스템 데이터베이스 업데이트를 다운로드할 수 있으려면 이러한 연결이 필요합니다.

OVF를 설치할 때 네트워크를 할당합니다. 인터페이스를 구성하면 나중에 VMware Client를 통해 가상 네트워크를 변경할 수 있습니다. 그러나 새 인터페이스를 추가해야 하는 경우 목록 끝에 인터페이스를 추가해야 합니다. 다른 곳에서 인터페이스를 추가하거나 제거하면 하이퍼바이저에서 인터페이스의 번호를 다시 매깁니다. 그러면 구성의 인터페이스 ID가 잘못된 인터페이스에 맞춰 정렬됩니다에 설명된 것처럼 더 복잡합니다.

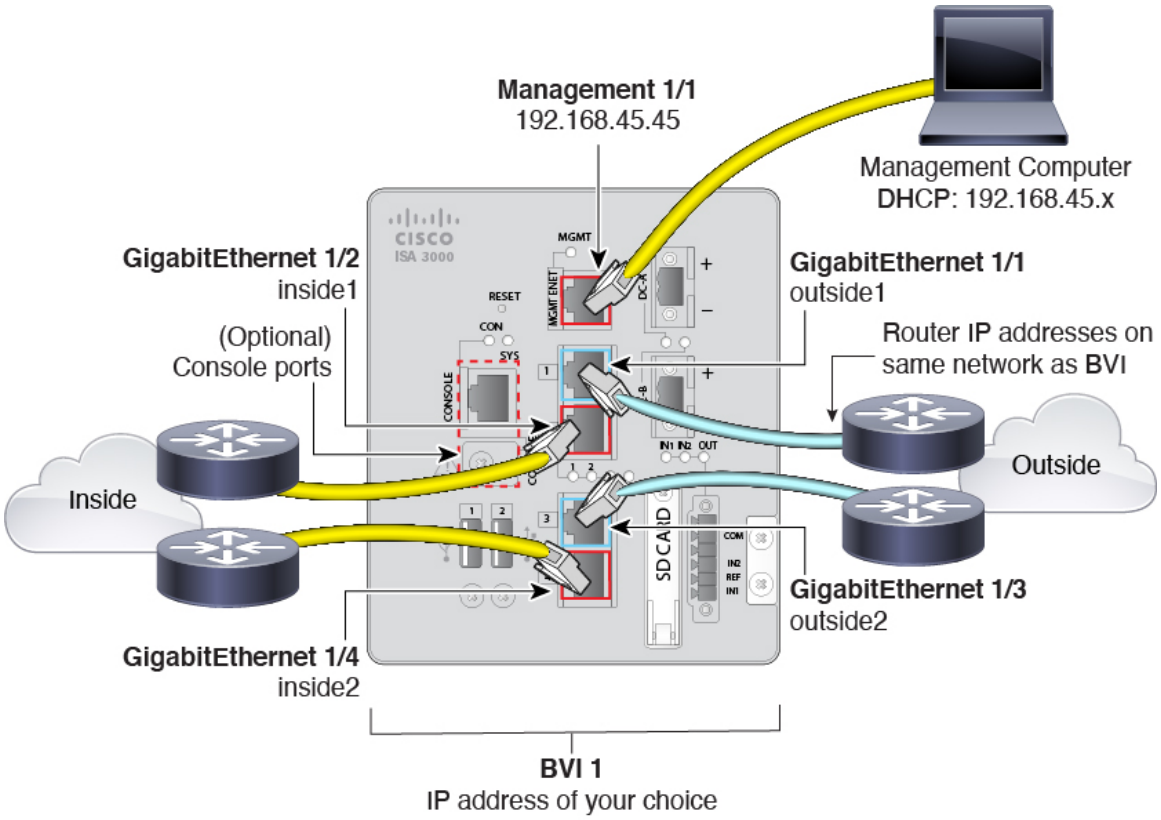
다음 표에서는 VMware 네트워크 어댑터와 소스 인터페이스가 threat defense virtual 물리적 인터페이스 이름에 매핑되는 방식을 설명합니다. 추가 인터페이스의 경우에도 같은 패턴에 따라 이름이 지정됩니다(관련 번호가 1씩 증가). 모든 추가 인터페이스는 데이터 인터페이스입니다. 가상 머신에 가상 네트워크를 할당하는 방법에 대한 자세한 내용은 VMware 온라인 도움말을 참조하십시오.

표 *1:* 소스-대상 네트워크 매핑

네트워크 어댑터	소스 네트워크	대상 네트워크(물리적 인터페이스 이름)	기능
네트워크 어댑터 1	Management0-0	Management 0/0	관리
네트워크 어댑터 2	Diagnostic0-0	Diagnostic0/0	진단
네트워크 어댑터 3	GigabitEthernet0-0	GigabitEthernet0/0	외부 데이터
네트워크 어댑터 4	GigabitEthernet0-1	GigabitEthernet0/1	내부 데이터
네트워크 어댑터 5	GigabitEthernet0-2	GigabitEthernet0/2	데이터 트래픽
네트워크 어댑터 6	GigabitEthernet0-3	GigabitEthernet0/3	데이터 트래픽
네트워크 어댑터 7	GigabitEthernet0-4	GigabitEthernet0/4	데이터 트래픽
네트워크 어댑터 8	GigabitEthernet0-5	GigabitEthernet0/5	데이터 트래픽
네트워크 어댑터 9	GigabitEthernet0-6	GigabitEthernet0/6	데이터 트래픽
네트워크 어댑터 10	GigabitEthernet0-7	GigabitEthernet0/7	데이터 트래픽

ISA 3000 케이블 연결

그림 *5: ISA 3000*



- GigabitEthernet 1/1을 외부 라우터에 연결하고 GigabitEthernet 1/2를 내부 라우터에 연결합니다.

  이러한 인터페이스에서는 하드웨어 우회 쌍을 형성합니다.

- GigabitEthernet 1/3을 이중 외부 라우터에 연결하고 GigabitEthernet 1/4를 이중 내부 라우터에 연결합니다.

  모델에 구리 포트가 있는 경우 이러한 인터페이스에서는 하드웨어 우회 쌍을 형성합니다. 파이버에서는 하드웨어 우회를 지원하지 않습니다. 이러한 인터페이스에서는 다른 쌍에 장애가 발생하는 경우 이중 네트워크 경로를 제공합니다. 이러한 데이터 인터페이스 4개는 모두 선택한 동일한 네트워크에 있습니다. BVI 1 IP 주소는 내부 및 외부 라우터와 동일한 네트워크에 있도록 구성해야 합니다.

- Management 1/1을 관리 컴퓨터(또는 네트워크)에 연결합니다.

  Management 1/1 IP 주소를 기본값에서 변경해야 할 경우, 관리 컴퓨터도 콘솔 포트에 연결해야 합니다. (선택 사항) CLI에서 관리 네트워크 설정 변경, 22 페이지의 내용을 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 구축 시 IP 주소를 수동으로 설정했으므로 Firepower 4100/9300에는 이 절차를 사용할 필요가 없습니다.

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. Cisco Secure Firewall Threat Defense 명령 참조의 내용을 참조하십시오.

프로시저

단계 **1** threat defense 콘솔 포트에 연결합니다. 자세한 내용은 CLI(Command Line Interface) 로그인, 9 페이지를 참조하십시오.

단계 **2** 사용자 이름 **admin**으로 로그인합니다.

기본 관리자 비밀번호는 Admin123입니다. AWS에서 구축 중에 사용자 데이터(**Advanced Details**(고급 세부 정보) > **User Data**(사용자 데이터))로 기본 비밀번호를 정의하지 않은 경우 threat defense virtual에 대한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다.

단계 **3** threat defense에 처음 로그인할 경우, 엔드 유저 라이선스 계약(EULA)에 동의하고 관리자 비밀번호를 변경하라는 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 게이

트웨이를 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 manager을 사용하려면 **yes**를 입력합니다. 답변이 **no**인 경우, 온프레미스 또는 클라우드 제공 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 change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
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.

설정 마법사를 사용하여 초기 컨피그레이션 완료

device manager에 처음 로그인할 때는 디바이스 설정 마법사로 이동해 초기 시스템 구성을 완료합니다.

고가용성 컨피그레이션의 디바이스를 사용하려는 경우 고가용성을 위한 두 유닛 준비의 내용을 참조하십시오.

참고 Firepower 4100/9300 및 ISA 3000에서는 설정 마법사를 지원하지 않으므로 이 절차는 이러한 모델에 적용되지 않습니다. Firepower 4100/9300의 경우, 섀시에서 논리적 디바이스를 구축할 때 모든 초기 구성이 설정됩니다. ISA 3000의 경우 배송 전에 특수한 기본 구성이 적용됩니다.

시작하기 전에

케이블 모뎀이나 라우터와 같은 게이트웨이 디바이스에 데이터 인터페이스를 연결해야 합니다. 이 디바이스는 엣지 구축의 경우 인터넷 연결 게이트웨이가 되며, 데이터 센터 구축의 경우에는 백본 라우터가 됩니다. 모델의 기본 "외부" 인터페이스를 사용합니다(인터페이스 연결, 12 페이지 및 초기 설정 전의 기본 컨피그레이션, 27 페이지 참조).

그런 다음 관리 컴퓨터를 하드웨어 모델의 "내부" 인터페이스에 연결합니다. 또는 관리 인터페이스에 연결할 수도 있습니다. threat defense virtual의 경우에는 관리 IP 주소에 연결할 수 있는지만 확인합니다.

(관리 IP 주소에서 인터넷 연결이 필요한 threat defense virtual 제외) 관리 인터페이스는 네트워크에 연결하지 않아도 됩니다. 기본적으로 시스템은 인터넷에 연결하는 데이터 인터페이스(대개 외부 인터페이스)를 통해 시스템 라이선싱 및 데이터베이스 업데이트와 기타 업데이트를 가져옵니다. 별도의 관리 네트워크를 대신 사용하려는 경우에는 관리 인터페이스를 네트워크에 연결하고 초기 설정을 완료한 후에 별도의 관리 게이트웨이를 구성하면 됩니다.

기본 IP 주소에 액세스할 수 없는 경우 관리 인터페이스 네트워크 설정을 변경하려면 (선택 사항) CLI에서 관리 네트워크 설정 변경, 22 페이지를 참조하십시오.

프로시저

단계 **1** device manager에 로그인합니다.

a) CLI에서 초기 구성을 수행하지 않았다고 가정하겠습니다. **https://***ip-address*에서 device manager를 엽니다. 여기서 주소는 다음 중 하나입니다.

- 내부 인터페이스에 연결된 경우: **https://192.168.95.1**.
- () 관리 인터페이스에 연결되어 있는 경우: **https://192.168.45.45**.
- (모든 기타 모델) 관리 인터페이스에 연결되어 있는 경우: **https://***dhcp_client_ip*

b) 사용자 이름 **admin**으로 로그인합니다. 기본 관리자 비밀번호는 Admin123입니다. AWS에서 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않은 경우 threat defense virtual에 대한 기본 관리자 비밀번호는 AWS 인스턴스 ID입니다..

단계 **2** 시스템에 처음으로 로그인하며 CLI 설정 마법사를 사용하지 않은 경우에는 엔드 유저 라이선스 계약을 확인 및 동의하고 관리자 비밀번호를 변경하라는 메시지가 표시됩니다.

계속하려면 이러한 단계를 완료해야 합니다.

단계 **3** 외부 및 관리 인터페이스에 대해 다음 옵션을 구성하고 **Next(**다음**)**를 클릭합니다.

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

외부 인터페이스

- **IPv4** 구성 - 외부 인터페이스의 IPv4 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 서브넷 마스크 및 게이트웨이를 입력할 수 있습니다. 끄기를 선택하여 IPv4 주소를 구성하지 않을 수도 있습니다. 기본 내부 주소와 동일한 서브넷에서 정적으로 또는 DHCP를 통해 IP 주소를 구성하지 마십시오(초기 설정 전의 기본 컨피그레이션, 27 페이지 참조). 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. 실제 인터페이스 구성의 내용을 참조하십시오.
- **IPv6** 구성 - 외부 인터페이스의 IPv6 주소를 구성합니다. DHCP를 사용하거나 수동으로 고정 IP 주소, 접두사 및 게이트웨이를 입력할 수 있습니다. 끄기를 선택하여 IPv6 주소를 구성하지 않을 수도 있습니다.

관리 인터페이스

- **DNS** 서버 - 시스템 관리 주소용 DNS 서버를 지정합니다. 이름 확인을 위해 DNS 서버의 주소를 하나 이상 입력합니다. 기본값은 OpenDNS 공용 DNS 서버 또는 DHCP 서버에서 가져오는 DNS 서버입니다. 필드를 수정하여 기본값으로 되돌리려면 **OpenDNS(OpenDNS** 사용**)**를 클릭하여 적절한 IP 주소를 필드에 다시 로드합니다. 사용 중인 ISP에 따라서는 특정 DNS 서버를 사용해야 할 수도 있습니다. 마법사를 완료한 후 DNS 확인이 작동하지 않으면 관리 인터페이스용 DNS 문제 해결의 내용을 참조하십시오.
- 방화벽 호스트 이름 - 시스템 관리 주소용 호스트 이름을 지정합니다.

단계 **4** 시스템 시간 설정을 구성하고 **Next(**다음**)**를 클릭합니다.

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

단계 **5** 시스템에 대한 스마트 라이선스를 구성합니다.

시스템에 필요한 라이선스를 가져오고 적용하려면 스마트 라이선스 어카운트가 있어야 합니다. 처음에는 90일 평가 라이선스를 사용하고 나중에 스마트 라이선싱을 설정할 수 있습니다.

디바이스를 바로 등록하려면 디바이스를 등록하는 옵션을 선택하고 링크를 클릭하여 Smart Software Manager 어카운트에 로그인한 다음, 새 토큰을 생성하여 수정 상자에 복사합니다. 또한 서비스 지역을 선택하고 Cisco Success Network에 사용량 데이터를 전송할지 결정해야 합니다. 화면 텍스트로 이러한 설정이 자세히 설명됩니다.

디바이스를 아직 등록하지 않으려면 평가 모드 옵션을 선택합니다. 평가 기간은 최대 90일입니다. 나중에 디바이스를 등록하고 스마트 라이선스를 가져오려면 디바이스를 클릭한 다음, **Smart Licenses(**스마트 라이선스**)** 그룹에서 링크를 클릭하십시오.

단계 **6** **Finish(**마침**)**를 클릭합니다.

다음에 수행할 작업

- 범주 기반 URL 필터링, 침입 검사, 악성코드 방지 등 선택 가능한 라이선스에 포함되는 기능을 사용하려면 필요한 라이선스를 활성화합니다. 선택 가능한 라이선스 활성화 또는 비활성화의 내용을 참조하십시오.
- 다른 데이터 인터페이스를 고유 네트워크에 연결한 다음 인터페이스를 구성합니다. 인터페이스 구성에 대한 자세한 내용은 서브넷을 추가하는 방법 및 인터페이스를 참조하십시오.
- 내부 인터페이스를 통해 디바이스를 관리하는 경우 내부 인터페이스를 통해 CLI 세션을 열려면 SSH 연결에 대해 내부 인터페이스를 엽니다. 관리 액세스 목록 구성의 내용을 참조하십시오.
- 제품 사용 방법을 파악하려면 활용 사례를 확인하십시오. 모범 사례: Threat Defense의 사용 사례의 내용을 참조하십시오.

외부 인터페이스의 IP 주소를 획득하지 못하는 경우 해야 할 작업

기본 디바이스 컨피그레이션에는 내부 인터페이스에 대한 고정 IPv4 주소가 포함됩니다. 초기 디바이스 설치 마법사를 통해 이 주소를 변경할 수는 없지만, 나중에는 이 주소를 변경할 수 있습니다.

기본 내부 IP 주소는 디바이스에 연결되어 있는 다른 네트워크와 충돌할 수 있습니다. 특히, DHCP를 사용하여 ISP(Internet Service Provider)로부터 주소를 얻으려는 경우 그렇게 될 수 있습니다. 일부 ISP는 내부 네트워크와 동일한 서브넷을 주소 풀로 사용합니다. 동일한 서브넷의 주소를 사용하는 두 개의 데이터 인터페이스를 지닐 수 없으므로 ISP의 충돌하는 주소는 외부 인터페이스에 구성할 수 없습니다.

내부 고정 IP 주소와 외부 인터페이스의 DHCP 제공 주소 간에 충돌이 발생하는 경우, 연결 다이어그램에는 IPv4 주소 없이 관리자가 외부 인터페이스를 가동 중인 상태로 표시됩니다.

이 경우, 설치 마법사가 성공적으로 완료되고 모든 기본 NAT, 액세스 및 기타 정책 및 설정이 구성됩니다. 충돌을 제거하려면 다음 절차를 따르면 됩니다.

시작하기 전에

ISP에 정상적으로 연결되었는지 확인합니다. 서브넷 충돌이 발생하면 외부 인터페이스의 주소를 가져올 수 없게 되지만, 단순히 ISP에 대한 링크가 없는 경우에도 주소를 가져올 수 없게 됩니다.

프로시저

단계 **1** **Device(**디바이스**)**를 클릭한 다음 **Interfaces(**인터페이스**)** 요약의 링크를 클릭합니다.

단계 **2** 내부 인터페이스의 **Actions(**작업**)** 열 위로 마우스를 가져가 수정 아이콘( )을 클릭합니다.

단계 **3** **IPv4 Address(IPv4** 주소**)** 탭에서 고유한 서브넷에 고정 주소를 입력합니다(예: 192.168.2.1/24 또는 192.168.46.1/24). 기본 관리 주소가 192.168.45.45/24인 경우 해당 서브넷을 사용하지 마십시오.

또한 이미 내부 네트워크에서 실행 중인 DHCP 서버가 있는 경우, 주소를 가져오기 위해 DHCP를 사용할 수도 있습니다. 그러나 인터페이스에서 DHCP 서버를 제거하려면 먼저 **DHCP SERVER IS DEFINED FOR THIS INTERFACE(DHCP** 서버가 이 인터페이스에 대해 정의되어 있음**)** 그룹에서 **Delete(**삭제**)**를 클릭해야 합니다.

단계 **4** **DHCP SERVER IS DEFINED FOR THIS INTERFACE(DHCP** 서버가 이 인터페이스에 대해 정의되어 있음**)** 영역에서 **Edit(**편집**)**을 클릭하고 DHCP 풀을 새로운 서브넷에 대한 범위로 변경합니다(예: 192.168.2.5-192.168.2.254).

단계 **5** **OK(**확인**)**를 클릭하여 인터페이스 변경 사항을 저장합니다.

단계 **6** 메뉴에서 **Deploy(**구축**)** 버튼을 클릭하여 변경 사항을 구축합니다.

단계 **7** **Deploy Now(**지금 구축**)**를 클릭합니다.

구축을 완료하고 나면 연결 그래픽에는 외부 인터페이스에 이제 IP 주소가 있는 것으로 표시됩니다. 내부 네트워크에서 클라이언트를 사용하여 인터넷 또는 다른 업스트림 네트워크에 연결되었는지 확인합니다.

초기 설정 전의 기본 컨피그레이션

로컬 관리자(device manager)를 사용하여 위협 방어 디바이스를 처음으로 구성하기 전에 디바이스에는 다음과 같은 기본 컨피그레이션이 포함되어 있습니다.

많은 모델의 경우, 이 구성에서는 대개 인터페이스에 컴퓨터를 직접 연결하는 방식을 사용하여 내부 인터페이스를 통해 디바이스 관리자를 열며, 내부 인터페이스에 정의된 DHCP 서버를 사용하여 컴퓨터에 IP 주소를 제공한다고 가정합니다. 또는, 컴퓨터를 관리 인터페이스에 연결한 다음, DHCP를 사용하여 주소를 얻을 수도 있습니다. 그러나 일부 모델의 경우 기본 구성 및 관리 요구 사항이 다릅니다. 자세한 내용은 아래 표를 참조하십시오.

참고 마법사를 사용하여 설치를 수행하기 전에 우선 CLI 설정((선택 사항) CLI에서 관리 네트워크 설정 변경, 22 페이지)을 사용하여 이러한 여러 설정을 사전 구성할 수 있습니다.

기본 컨피그레이션 설정

설정	기본	초기 컨피그레이션 중 변경 가능 여부
관리자 사용자의 비밀번호	Admin123 Firepower 4100/9300: 논리적 디바이스를 구축할 때 비밀번호를 설정합니다. AWS: 초기 구축 중에 사용자 데이터(**Advanced Details(**고급 세부 정보**)** > **User Data(**사용자 데이터**)**)로 기본 비밀번호를 정의하지 않는 한 기본값은 AWS 인스턴스 ID입니다.	예. 기본 비밀번호를 변경해야 합니다.
관리 IP 주소	DHCP를 통해 얻습니다. Threat Defense Virtual192.168.45.45 Firepower 4100/9300: 논리적 디바이스를 구축할 때 관리 IP 주소를 설정합니다.	아니요. Firepower 4100/9300의 경우: 예.
관리 게이트웨이	디바이스의 데이터 인터페이스. 일반적으로 외부 인터페이스는 인터넷의 경로가 됩니다. 이 게이트웨이는 디바이스에서 시작되는 트래픽에 대해서만 작동합니다. 디바이스가 DHCP 서버에서 기본 게이트웨이를 수신하는 경우 해당 게이트웨이가 사용됩니다. Firepower 4100/9300: 논리적 디바이스를 구축할 때 게이트웨이 IP 주소를 설정합니다. ISA 3000: 192.168.45.1. Threat Defense Virtual: 192.168.45.1	아니요. Firepower 4100/9300의 경우: 예.
관리 인터페이스의 DNS 서버	OpenDNS 공용 DNS 서버, IPv4: 208.67.220.220 및 208.67.222.222, IPv6: 2620:119:35::35. DHCP에서 가져온 DNS 서버는 사용되지 않습니다. Firepower 4100/9300: 논리적 디바이스를 구축할 때 DNS 서버를 설정합니다.	예.

설정	기본	초기 컨피그레이션 중 변경 가능 여부
내부 인터페이스 IP 주소	192.168.95.1/24 Firepower 4100/9300: 데이터 인터페이스가 사전 구성되어 있지 않습니다. ISA 3000: BVI1 IP 주소가 사전 구성되어 있지 않습니다. BVI1에는 모든 내부 및 외부 인터페이스가 포함되어 있습니다. Threat Defense Virtual: 192.168.45.1/24	아니요.
내부 클라이언트에 대한 DHCP 서버	주소 풀 192.168.95.5-192.168.95.254를 포함하는 내부 인터페이스에서 실행됩니다. Firepower 4100/9300: 활성화된 DHCP 서버가 없습니다. ISA 3000: 활성화된 DHCP 서버가 없습니다. Threat Defense Virtual: 내부 인터페이스의 주소 풀은 192.168.45.46 - 192.168.45.254입니다.	아니요.
내부 클라이언트에 대한 DHCP 자동 컨피그레이션 (자동 컨피그레이션은 클라이언트에 WINS 및 DNS 서버용 주소를 제공)	외부 인터페이스에서 활성화됩니다.	예(간접적). 외부 인터페이스에 대해 고정 IPv4 주소를 구성하는 경우 DHCP 서버 자동 컨피그레이션은 비활성화됩니다.
외부 인터페이스 IP 주소	IPv4: ISP(Internet Service Provider) 또는 업스트림 라우터에서 DHCP를 통해 가져옵니다. IPv6: 자동 설정. Firepower 4100/9300: 데이터 인터페이스가 사전 구성되어 있지 않습니다. ISA 3000: BVI1 IP 주소가 사전 구성되어 있지 않습니다. BVI1에는 모든 내부 및 외부 인터페이스가 포함되어 있습니다.	예.

디바이스 모델별 기본 인터페이스

초기 컨피그레이션 중에는 다른 내부 및 외부 인터페이스를 선택할 수 없습니다. 컨피그레이션 후에 인터페이스 할당을 변경하려면 인터페이스 및 DHCP 설정을 수정합니다. 브리지 그룹에서 인터페이스를 제거해야 해당 인터페이스를 비스위치 인터페이스로 구성할 수 있습니다.

Threat Defense 디바이스	외부 인터페이스	내부 인터페이스
Firepower 1010	Ethernet1/1	VLAN1에는 물리적 방화벽 인터페이스인 외부 인터페이스를 제외한 다른 모든 스위치 포트가 포함되어 있습니다.
Firepower 1120, 1140, 1150	Ethernet1/1	Ethernet1/2
Firepower 2100 Series	Ethernet1/1	Ethernet1/2
Secure Firewall 3100 Series	Ethernet1/1	Ethernet1/2
Firepower 4100 Series	데이터 인터페이스가 사전 구성되어 있지 않습니다.	데이터 인터페이스가 사전 구성되어 있지 않습니다.
Firepower 9300 Appliance	데이터 인터페이스가 사전 구성되어 있지 않습니다.	데이터 인터페이스가 사전 구성되어 있지 않습니다.
Threat Defense Virtual	GigabitEthernet0/0	GigabitEthernet0/1
ISA 3000	GigabitEthernet1/1 및 GigabitEthernet1/3 GigabitEthernet1/1(outside1) 및 1/2(inside1), GigabitEthernet1/3(outside2) 및 1/4(inside2)(비파이버 모델만 해당)는 하드웨어 우회 쌍으로 구성됩니다. 모든 내부 및 외부 인터페이스는 BVI1의 일부입니다.	GigabitEthernet1/2 및 GigabitEthernet1/4

초기 설정 후의 컨피그레이션

설정 마법사를 완료한 후의 디바이스 컨피그레이션에는 다음 설정이 포함됩니다. 아래 표에는 특정 설정이 명시적으로 선택한 것인지 아니면 다른 선택 항목을 기준으로 하여 정의된 것인지가 나와 있습니다. "암시적" 컨피그레이션을 검증한 후 필요한 사항에 맞지 않으면 수정합니다.

참고 Firepower 4100/9300 및 ISA 3000에서는 설정 마법사를 지원하지 않습니다. Firepower 4100/9300의 경우, 섀시에서 논리적 디바이스를 구축할 때 모든 초기 구성이 설정됩니다. ISA 3000의 경우 배송 전에 특수한 기본 구성이 적용됩니다.

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
관리자 사용자의 비밀번호	입력한 내용	명시적
관리 IP 주소	DHCP를 통해 얻습니다. Threat Defense Virtual: 192.168.45.45 Firepower 4100/9300: 논리적 디바이스를 구축할 때 설정한 관리 IP 주소입니다.	기본
관리 게이트웨이	디바이스의 데이터 인터페이스. 일반적으로 외부 인터페이스는 인터넷의 경로가 됩니다. 관리 게이트웨이는 디바이스에서 시작되는 트래픽에 대해서만 작동합니다. 디바이스가 DHCP 서버에서 기본 게이트웨이를 수신하는 경우 해당 게이트웨이가 사용됩니다. Firepower 4100/9300: 논리적 디바이스를 구축할 때 설정한 게이트웨이 IP 주소입니다. ISA 3000: 192.168.45.1 Threat Defense Virtual: 192.168.45.1	기본
관리 인터페이스의 DNS 서버	OpenDNS 공용 DNS 서버, IPv4: 208.67.220.220, 208.67.222.222, IPv6: 2620:119:35::35, 또는 입력한 모든 값. DHCP에서 가져온 DNS 서버는 사용되지 않습니다. Firepower 4100/9300: 논리적 디바이스를 구축할 때 설정한 DNS 서버입니다.	명시적
관리 호스트 이름	**firepower** 또는 입력한 내용 Firepower 4100/9300: 논리적 디바이스를 구축할 때 설정한 호스트 이름입니다.	명시적
데이터 인터페이스를 통한 관리 액세스	데이터 인터페이스 관리 액세스 목록 규칙을 사용하면 내부 인터페이스를 통한 HTTPS 액세스가 허용됩니다. SSH 연결은 허용되지 않습니다. IPv4 및 IPv6 연결은 모두 허용됩니다. Firepower 4100/9300: 데이터 인터페이스에 기본 관리 액세스 규칙이 없습니다. ISA 3000: 데이터 인터페이스에 기본 관리 액세스 규칙이 없습니다. Threat Defense Virtual: 데이터 인터페이스에 기본 관리 액세스 규칙이 없습니다.	암시적

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
시스템 시간	선택한 표준 시간대 및 NTP 서버 Firepower 4100/9300: 시스템 시간이 섀시에서 상속됩니다. ISA 3000: Cisco NTP 서버: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org	명시적
스마트 라이선스	기본 라이선스를 사용하여 등록된 라이선스 또는 사용 설정된 평가 기간 중 선택하는 항목. 서브스크립션 라이선스는 활성화하지 않습니다. 서브스크립션 라이선스를 활성화하려면 스마트 라이선싱 페이지로 이동합니다.	명시적
내부 인터페이스 IP 주소	192.168.95.1/24 Firepower 4100/9300: 데이터 인터페이스가 사전 구성되어 있지 않습니다. ISA 3000: 없음. BVI1 IP 주소를 수동으로 설정해야 합니다. Threat Defense Virtual: 192.168.45.1/24	기본
내부 클라이언트에 대한 DHCP 서버	주소 풀 192.168.95.5-192.168.95.254를 포함하는 내부 인터페이스에서 실행됩니다. Firepower 4100/9300: 활성화된 DHCP 서버가 없습니다. ISA 3000: 활성화된 DHCP 서버가 없습니다. Threat Defense Virtual: 내부 인터페이스의 주소 풀은 192.168.45.46 - 192.168.45.254입니다.	기본
내부 클라이언트에 대한 DHCP 자동 컨피그레이션 (자동 컨피그레이션은 클라이언트에 WINS 및 DNS 서버용 주소를 제공)	DHCP를 사용하여 외부 인터페이스 IPv4 주소를 가져오는 경우 외부 인터페이스에서 활성화하는 것으로 설정됩니다. 고정 주소를 사용하는 경우에는 DHCP 자동 컨피그레이션이 비활성화됩니다.	명시적(간접적)

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
데이터 인터페이스 컨피그레이션	• Firepower 1010 - 외부 인터페이스(Ethernet1/1)가 물리적 방화벽 인터페이스입니다. 기타 모든 인터페이스는 활성화된 스위치 포트이며, 내부 인터페이스인 VLAN1에 포함됩니다. 엔드포인트 또는 스위치를 이러한 포트에 연결하고 내부 인터페이스용으로 DHCP 서버에서 주소를 가져올 수 있습니다. • Firepower 4100/9300- 모든 데이터 인터페이스가 비활성화되어 있습니다. • ISA 3000 - 모든 데이터 인터페이스가 활성화되어 있으며 동일한 브리지 그룹인 BVI1에 포함됩니다. GigabitEthernet1/1 및 1/3은 외부 인터페이스이고 GigabitEthernet1/2 및 1/4는 내부 인터페이스입니다. GigabitEthernet1/1(outside1) 및 1/2(inside1), GigabitEthernet1/3(outside2) 및 1/4(inside2)(비파이버 모델만 해당)는 하드웨어 우회 쌍으로 구성됩니다. • 다른 모든 모델 - 외부 및 내부 인터페이스만 구성 및 활성화됩니다. 다른 모든 데이터 인터페이스는 비활성화됩니다.	기본
외부 실제 인터페이스 및 IP 주소	디바이스 모델에 따른 기본 외부 포트. 초기 설정 전의 기본 컨피그레이션, 27 페이지를 참조하십시오. IP 주소는 DHCP 및 IPv6 자동 설정에서 가져온 주소이거나 입력한 고정 주소(IPv4, IPv6 또는 둘 다)입니다. Firepower 4100/9300: 데이터 인터페이스가 사전 구성되어 있지 않습니다. ISA 3000: 없음. BVI1 IP 주소를 수동으로 설정해야 합니다.	인터페이스: 기본 주소 지정: 명시적
정적 경로	외부 인터페이스에 대해 고정 IPv4 또는 IPv6 주소를 구성하는 경우 정적 기본 경로가 IPv4/IPv6에 대해 적절하게 구성되어 해당 주소 유형에 대해 정의한 게이트웨이를 가리킵니다. DHCP를 선택하는 경우 DHCP 서버에서 기본 경로를 가져옵니다. 게이트웨이 및 "임의" 주소에 대한 네트워크 개체도 생성됩니다(IPv4의 경우 0.0.0.0/0, IPv6의 경우 ::/0).	암시적

설정	컨피그레이션	명시적, 암시적 또는 기본 컨피그레이션
보안 영역	**inside_zone**에는 내부 인터페이스가 포함되어 있습니다. Firepower 4100/9300의 경우 이 보안 영역에 인터페이스를 수동으로 추가해야 합니다. **outside_zone**에는 내부 인터페이스가 포함되어 있습니다. Firepower 4100/9300의 경우 이 영역에 인터페이스를 수동으로 추가해야 합니다. 이러한 영역을 수정하여 다른 인터페이스를 추가하거나 영역을 직접 생성할 수 있습니다.	암시적
액세스 제어 정책	inside_zone에서 outside_zone으로 전송되는 모든 트래픽을 신뢰하는 규칙입니다. 이 규칙을 사용하면 네트워크 내의 사용자가 외부로 전송하는 모든 트래픽 및 해당 연결에 대한 모든 반환 트래픽이 검사 없이 허용됩니다. 기타 모든 트래픽에 대한 기본 작업은 차단입니다. 즉, 외부에서 시작되어 네트워크로 진입하는 모든 트래픽은 차단됩니다. Firepower 4100/9300: 사전 구성된 액세스 규칙이 없습니다. ISA 3000: inside_zone에서 outside_zone으로의 모든 트래픽을 신뢰하는 규칙, outside_zone에서 inside_zone으로의 모든 트래픽을 신뢰하는 규칙이 있습니다. 트래픽은 차단되지 않습니다. 또한 디바이스에는 inside_zone과 outside_zone의 인터페이스 간의 모든 트래픽을 신뢰하는 규칙도 있습니다. 그러므로 내부 사용자와 외부 사용자 간의 모든 트래픽을 검사하지 않아도 됩니다.	암시적
NAT	인터페이스 동적 PAT 규칙이 외부 인터페이스로 전송되는 IPv4 트래픽의 소스 주소를 외부 인터페이스 IP 주소의 고유 포트로 변환합니다. 관리 주소의 데이터 인터페이스를 통한 라우팅과 내부 인터페이스를 통한 HTTPS 액세스를 활성화하는 숨겨진 추가 PAT 규칙도 있습니다. 이러한 규칙은 NAT 테이블에는 표시되지 않지만, CLI에서 **show nat** 명령을 사용해 확인할 수 있습니다. Firepower 4100/9300: NAT가 사전 구성되어 있지 않습니다. ISA 3000: NAT가 사전 구성되어 있지 않습니다.	암시적

컨피그레이션 기본 사항

다음 항목에서는 디바이스 구성을 위한 기본 방법을 설명합니다.

디바이스 구성

device manager에 처음 로그인할 때는 기본 설정을 구성할 수 있도록 설정 마법사로 이동하게 됩니다. 마법사를 완료한 후에 다음 방법을 사용하여 다른 기능을 구성하고 디바이스 컨피그레이션을 관리합니다.

항목을 시각적으로 구분하기가 어려운 경우 사용자 프로파일에서 다른 색 구성표를 선택합니다. 페이지 오른쪽 상단에 있는 사용자 아이콘 드롭다운 메뉴에서 **Profile(**프로파일**)**을 선택합니다.

프로시저

단계 **1** 디바이스를 클릭하여 **Device Summary(**디바이스 요약**)**로 이동합니다.

대시보드에는 키 설정이 구성되어 있는지(녹색으로 표시됨) 아니면 구성해야 하는지에 대한 정보 및 활성화된 인터페이스를 비롯하여 디바이스의 시각적 상태가 표시됩니다. 자세한 내용은 인터페이스 및 관리 상태 보기, 41 페이지를 참고하십시오.

상태 이미지 위에는 디바이스 모델, 소프트웨어 버전, 시스템 및 VDB(Vulnerability Database) 버전, 침입 규칙을 마지막으로 업데이트한 시간의 요약이 표시됩니다. 이 영역에서는 기능을 컨피그레이션할 수 있는 링크를 포함한 고가용성 상태도 표시합니다. 고가용성(페일오버)를 참조하십시오. 또한 클라우드 관리 상태를 표시합니다. 클라우드 관리를 사용하는 경우 디바이스가 등록된 어카운트가 여기에 표시됩니다. 클라우드 서비스 구성를 참조하십시오.

이미지 아래에는 구성 가능한 여러 기능의 그룹이 있으며 각 그룹의 컨피그레이션 요약과 시스템 컨피그레이션을 관리하기 위해 수행할 수 있는 작업이 표시됩니다.

단계 **2** 각 그룹의 링크를 클릭하여 설정을 구성하거나 작업을 수행합니다.

아래에는 그룹에 대한 설정이 요약되어 있습니다.

- **Interface(**인터페이스**)** — 관리 인터페이스 이외에 둘 이상의 데이터 인터페이스가 구성되어 있어야 합니다. 인터페이스의 내용을 참조하십시오.
- **Routing(**라우팅**)** — 라우팅 컨피그레이션입니다. 기본 경로를 정의해야 합니다. 컨피그레이션에 따라서는 다른 경로가 필요할 수 있습니다. 라우팅의 내용을 참조하십시오.
- **Updates(**업데이트**)** — 지리위치, 침입 규칙, 취약점 데이터베이스 업데이트 및 시스템 소프트웨어 업그레이드가 표시됩니다. 이러한 기능을 사용하려는 경우 최신 데이터베이스 업데이트를 받을 수 있도록 정기 업데이트 일정을 설정하십시오. 정기 일정에 따른 업데이트가 수행되기 전에 업데이트를 다운로드해야 하는 경우에도 이 페이지로 이동할 수 있습니다. 시스템 데이터베이스 및 피드 업데이트의 내용을 참조하십시오.

- **System Settings(**시스템 설정**)** — 이 그룹에는 여러 설정이 포함되어 있습니다. 그 중 일부 설정은 디바이스를 초기 설정할 때 구성하며 거의 변경하지 않는 기본 설정입니다. 시스템 설정의 내용을 참조하십시오.
- **Smart License(**스마트 라이선스**)** — 시스템 라이선스의 현재 상태가 표시됩니다. 시스템을 사용하려면 적절한 라이선스를 설치해야 합니다. 일부 기능의 경우 추가 라이선스가 필요합니다. 시스템 라이선싱의 내용을 참조하십시오.
- **Backup and Restore(**백업 및 복원**)** — 시스템 컨피그레이션을 백업하거나 이전 백업을 복원합니다. 시스템 백업 및 복원의 내용을 참조하십시오.
- **Troubleshoot(**트러블슈팅**)** — Cisco Technical Assistance Center에서 요청하는 경우 트러블슈팅 파일을 생성합니다. 트러블슈팅 파일 생성의 내용을 참조하십시오.
- **Site-to-Site VPN(**사이트 대 사이트 **VPN)** — 이 디바이스와 원격 디바이스 간의 사이트 대 사이트 VPN(Virtual Private Network) 연결이 표시됩니다. 사이트 대 사이트 VPN 관리의 내용을 참조하십시오.
- **Remote Access VPN(**원격 액세스 **VPN)** — 외부 클라이언트가 내부 네트워크에 연결하도록 허용하는 원격 액세스 VPN(Virtual Private Network) 컨피그레이션입니다. 원격 액세스 VPN 구성의 내용을 참조하십시오.
- **Advanced Configuration(**고급 컨피그레이션**)** — device manager를 사용해서는 구성할 수 없는 기능을 FlexConfig 및 스마트 CLI를 사용하여 구성합니다. 고급 컨피그레이션의 내용을 참조하십시오.
- **Device Administration(**디바이스 관리**)** — 감사 로그를 확인하거나 컨피그레이션 복사본을 내보냅니다. 감사 및 변경 관리의 내용을 참조하십시오.

단계 **3** 메뉴에서 **Deploy(**구축**)** 버튼을 클릭하여 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다. 변경 사항 구축, 38 페이지의 내용을 참조하십시오.

다음에 수행할 작업

주 메뉴에서 **Policies(**정책**)**를 클릭하여 시스템의 보안 정책을 구성합니다. **Objects(**개체**)**를 클릭하여 해당 정책에 필요한 개체를 구성할 수도 있습니다.

보안 정책 구성

보안 정책을 사용하여 조직의 사용 제한 정책을 구현하고 침입 및 기타 위협으로부터 네트워크를 보호합니다.

프로시저

단계 **1** **Policies(**정책**)**를 클릭합니다.

Security Policies(보안 정책) 페이지에는 시스템 전체의 일반적인 연결 플로우와 보안 정책이 적용되는 순서가 표시됩니다.

단계 **2** 정책 이름을 클릭하여 정책을 구성합니다.

항상 액세스 제어 정책을 적용해야 하더라도 각 정책 유형을 반드시 구성할 필요는 없을 수 있습니다. 정책 요약은 다음과 같습니다.

- **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. SSL 암호 해독 정책 구성를 참조하십시오.
- **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. ID 정책 구성를 참조하십시오.
- **Security Intelligence(**보안 인텔리전스**)** — 보안 인텔리전스 정책을 사용하여 선택된 IP 주소 또는 URL을 오가는 연결을 신속하게 삭제합니다. 알려진 유해 사이트를 차단하면 해당 사이트를 액세스 제어 정책에서 고려할 필요가 없습니다. Cisco에서는 알려진 유해 주소 및 URL에 대해 정기적으로 업데이트된 피드를 제공하므로 보안 인텔리전스 차단 목록이 동적으로 업데이트됩니다. 피드를 사용하는 경우에는 차단 목록에서 항목을 추가하거나 제거하기 위해 정책을 수정할 필요가 없습니다. 보안 인텔리전스 구성를 참조하십시오.
- **NAT**(Network Address Translation) — NAT 정책을 사용하여 내부 IP 주소를 외부에서 라우팅 가능한 주소로 변환합니다. NAT 구성를 참조하십시오.
- **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. 액세스 제어 정책 구성를 참조하십시오.
- **Intrusion(**침입**)** — 침입 정책을 사용하여 알려진 위협을 검사합니다. 액세스 제어 규칙을 사용하여 침입 정책을 적용하는 경우에도 침입 정책을 편집하여 특정 침입 규칙을 선택적으로 활성화 또는 비활성화할 수 있습니다. 침입 정책의 내용을 참조하십시오.

단계 **3** 메뉴에서 **Deploy(**구축**)** 버튼을 클릭하여 변경 사항을 구축합니다.

변경 사항은 구축할 때까지 디바이스에서 활성화되지 않습니다. 변경 사항 구축, 38 페이지의 내용을 참조하십시오.

규칙 또는 개체 검색

정책 규칙 또는 개체 목록에서 전체 텍스트 검색을 사용하면 수정하려는 항목을 찾는 데 도움이 됩니다. 이 기능은 수백 개의 규칙 또는 긴 개체 목록이 있는 정책을 처리할 때 특히 유용합니다.

규칙 및 개체에서 검색 기능을 사용하는 방법은 침입 정책을 제외한 모든 유형의 정책에서 동일합니다. 즉 **Search(**검색**)** 필드에서 검색할 문자열을 입력하고 Enter를 누릅니다.

이 문자열은 규칙 또는 개체의 어느 부분에도 있을 수 있으며, 부분 문자열일 수 있습니다. 별표(*)를 0개 이상의 문자와 일치하는 와일드카드로 사용할 수 있습니다. ?~!{}<>:% 문자는 검색 문자열의 일부로 지원하지 않으므로 포함하지 마십시오. ;#& 문자는 무시됩니다.

문자열은 그룹에 있는 개체 안에 표시될 수 있습니다. 예를 들어 IP 주소를 입력하고 해당 주소를 지정하는 네트워크 개체 또는 그룹을 검색할 수 있습니다.

완료했으면 검색 상자 오른쪽의 **x**를 클릭하여 필터를 지웁니다.

변경 사항 구축

정책 또는 설정을 업데이트할 때 변경 사항은 디바이스에 즉시 적용되지 않습니다. 다음과 같은 2단계 프로세스를 통해 컨피그레이션을 변경합니다.

1. 변경 사항을 적용합니다.
2. 변경 사항을 배포합니다.

이 프로세스에서는 "부분 구성" 방식으로 디바이스를 실행할 필요 없이 관련 변경 사항 그룹을 적용할 수 있습니다. 대부분의 경우, 구축에는 변경 사항만 포함되어 있습니다. 그러나 필요한 경우, 시스템에서는 네트워크를 중단시킬 수 있는 전체 컨피그레이션을 다시 적용합니다. 뿐만 아니라 일부 변경 사항에서는 검사 엔진을 재시작해야 하는데, 재시작하는 동안 트래픽 속도가 느려집니다. 따라서 잠재적 중단으로 인한 영향이 가장 적을 때 변경 사항을 구축하는 것이 좋습니다.

참고 구축 작업에 실패할 경우, 시스템에서는 이전 컨피그레이션의 부분적인 변경 사항을 롤백해야 합니다. 롤백에는 데이터 평면 컨피그레이션을 지우고 이전 버전을 다시 구축하는 작업이 포함됩니다. 이 작업을 수행하면 롤백이 완료될 때까지 트래픽이 중단됩니다.

수행하려는 변경을 완료한 후에는 다음 절차에 따라 디바이스에 변경 사항을 배포합니다.

주의 threat defense 디바이스는 소프트웨어 리소스 문제가 있어 검사 엔진이 사용 중이거나, 컨피그레이션 배포 중에 특정 컨피그레이션으로 인해 엔진을 재시작해야 하여 엔진이 다운되면 트래픽을 삭제합니다. 재시작이 필요한 변경에 대한 자세한 내용은 검사 엔진을 재시작하는 컨피그레이션 변경, 40 페이지를 참조하십시오.

프로시저

단계 **1** 웹 페이지의 오른쪽 상단에 있는 **Deploy Changes(**변경 사항 구축**)** 아이콘을 클릭합니다.

배포되지 않은 변경 사항이 있으면 아이콘이 점으로 강조 표시됩니다.

Pending Changes(보류 중인 변경 사항) 창에는 컨피그레이션의 구축된 버전과 보류 중인 변경 사항을 비교한 내용이 표시됩니다. 이러한 변경 사항은 제거, 추가 또는 수정된 요소를 나타내기 위해 색상 코드가 지정됩니다. 색상의 설명은 창의 범례를 참조하십시오.

구축 시 검사 엔진을 재시작해야 하는 경우, 페이지에는 재시작이 필요한 변경 사항에 대한 세부 정보를 제공하는 메시지가 포함되어 있습니다. 현재 일시적인 트래픽 손실을 허용할 수 없는 경우, 대화 상자를 닫고 변경 내용을 구축하기에 더 좋은 시기를 기다립니다.

아이콘이 강조 표시되지 않아도 아이콘을 클릭하면 마지막으로 성공한 구축 작업의 날짜와 시간을 확인할 수 있습니다. 구축 기록을 표시하는 링크도 있습니다. 이 링크를 클릭하면 구축 작업만 표시하도록 필터링된 감사 페이지로 이동합니다.

단계 **2** 변경 사항에 만족하는 경우 **Deploy Now(**지금 구축**)**를 클릭하여 작업을 즉시 시작할 수 있습니다.

창에는 배포이 진행 중임이 표시됩니다. 창을 닫을 수도 있고 구축이 완료될 때까지 기다릴 수도 있습니다. 구축이 진행 중인 동안 창을 닫아도 작업은 중지되지 않습니다. 작업 목록이나 감사 로그에서 결과를 확인할 수 있습니다. 창을 열어 두는 경우 결과를 확인하려면 **Deployment History(**구축 기록**)** 링크를 클릭합니다.

선택적으로 다음을 수행할 수 있습니다.

- **Name the Job(**작업 이름 지정**)** — 구축 작업의 이름을 지정하려면 **Deploy Now(**지금 구축**)** 버튼의 드롭다운 화살표를 클릭하고 **Name the Deployment Job(**구축 작업 이름 지정**)**을 선택합니다. 그런 다음 이름을 입력하고 **Deploy(**구축**)**를 클릭합니다. 그러면 이름이 작업의 일부분으로 감사 및 구축 기록에 표시되므로 작업을 더 쉽게 찾을 수 있습니다.

  예를 들어 작업 이름을 "DMZ Interface Configuration(DMZ 인터페이스 컨피그레이션)"으로 지정하는 경우 성공한 구축 이름은 "Deployment Completed: DMZ Interface Configuration(구축 완료: DMZ 인터페이스 컨피그레이션)"으로 지정됩니다. 또한, 이 이름은 구축 작업과 관련된 Task Started(작업 시작됨) 및 Task Completed(작업 완료됨) 이벤트에서도 Event Name(이벤트 이름)으로 사용됩니다.

- **Force a full deployment(**전체 구축 강제**)** - 문제가 발생하여 시스템에서 변경 사항만이 아니라 전체 구성을 강제로 구축하도록 하려면 **Deploy Now(**지금 구축**)** 버튼의 드롭다운 화살표를 클릭하고 **Apply Full Deployment(**전체 구축 적용**)**를 선택합니다. 전체 구축에서는 트래픽이 중단되므로 이 작업을 수행할 것임을 확인해야 **Deploy(**구축**)**를 클릭할 수 있습니다.

- **Discard Changes(**변경 사항 취소**)** — 보류 중인 변경 사항을 모두 취소하려면 **More Options(**기타 옵션**)** > **Discard All(**모두 취소**)**을 클릭합니다. 그러면 취소를 확인하라는 메시지가 표시됩니다.
- **Copy Changes(**변경 사항 복사**)** — 변경 사항 목록을 클립보드에 복사하려면 **More Options(**기타 옵션**)** > **Copy to Clipboard(**클립보드에 복사**)**를 클릭합니다. 이 옵션은 변경 사항 수가 500개 미만일 때만 작동합니다.
- **Download Changes(**변경 사항 다운로드**)** — 변경 사항 목록을 파일로 다운로드하려면 **More Options(**기타 옵션**)** > **Download as Text(**텍스트로 다운로드**)**를 클릭합니다. 그러면 파일을 워크스테이션에 저장하라는 메시지가 표시됩니다. 파일은 YAML 형식입니다. YAML 형식을 구체적으로 지원하는 편집기가 없으면 텍스트 편집기에서 해당 파일을 볼 수 있습니다.

검사 엔진을 재시작하는 컨피그레이션 변경

다음 컨피그레이션 또는 작업 중 하나를 수행하면 컨피그레이션 변경 사항을 구축할 때 검사 엔진이 재시작됩니다.

⚠

주의 구축 시에는 리소스 요구사항으로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한, 일부 컨피그레이션을 구축하려면 검사 엔진을 재시작해야 하므로 트래픽 검사가 중단되고 트래픽이 삭제됩니다.

구축

일부 사항을 변경하려면 검사 엔진을 재시작해야 하며 이로 인해 일시적인 트래픽 손실이 발생합니다. 다음은 검사 엔진 재시작이 필요한 변경 사항입니다.

- SSL 암호 해독 정책이 활성화 또는 비활성화된 경우
- 하나 이상의 물리적 인터페이스(하위 인터페이스 제외)에서 MTU가 변경된 경우
- 액세스 제어 규칙에서 파일 정책을 추가하거나 제거하는 경우
- VDB가 업데이트된 경우
- 고가용성 컨피그레이션을 생성 또는 해제한 경우

또한 Snort 프로세스가 CPU 사용률이 60%를 초과한 상태로 사용 중인 경우 구축 중에 일부 패킷이 삭제될 수 있습니다. **show asp inspect-dp snort** 명령을 사용하면 Snort의 현재 CPU 사용률을 확인할 수 있습니다.

시스템 데이터베이스 업데이트

규칙 데이터베이스 또는 VDB에 업데이트를 다운로드하는 경우, 이를 활성화하려면 업데이트를 구축해야 합니다. 이 구축 작업 시 검사 엔진이 재시작될 수 있습니다. 수동으로 업데이트를 다운로드하거나 업데이트 일정을 정하는 경우, 다운로드 완료 후에 시스템이 변경 사항을 자동으로 구축해야

하는지를 설정할 수 있습니다. 시스템이 업데이트를 자동으로 구축하도록 설정하지 않은 경우, 업데이트는 다음에 변경 사항을 구축할 때 적용되며 이때 검사 엔진이 재시작될 수 있습니다.

시스템 업데이트

시스템을 재부팅하지 않으며 이진 변경을 포함하는 시스템 업데이트나 패치를 설치할 때는 검사 엔진을 재시작해야 합니다. 이진 변경에는 검사 엔진, 전처리기, VDB(Vulnerability Database) 또는 공유 개체 규칙 변경이 포함될 수 있습니다. 이진 변경을 포함하지 않는 패치 시에도 Snort를 재시작해야 할 수 있습니다.

전체 구축을 강제하는 컨피그레이션 변경

대부분의 경우, 구축에는 변경 사항만 포함되어 있습니다. 그러나 필요한 경우, 시스템에서는 네트워크를 중단시킬 수 있는 전체 컨피그레이션을 다시 적용합니다. 다음은 전체 구축을 적용하는 몇 가지 변경 사항입니다.

- 보안 인텔리전스 또는 ID 정책은 초기에 활성화되어 있습니다.
- 보안 인텔리전스 및 ID 정책이 모두 비활성화됩니다.
- 데이터 재사용 시 EtherChannel을 생성합니다.
- EtherChannel 삭제.
- EtherChannel의 멤버 인터페이스 연결을 수정합니다.
- 구성에 사용된 모든 인터페이스를 삭제합니다. 예를 들어 액세스 제어 규칙에 사용되는 보안 영역의 일부인 하위 인터페이스를 삭제하는 경우를 예로 들 수 있습니다.
- FlexConfig 정책의 일부인 FlexConfig 개체를 변경하거나 정책에서 개체를 삭제하는 경우(개체에 부정 표기법이 포함되어 있지 않음) FlexConfig 개체에 의해 생성된 구성을 제거하는 특별한 방법이 없으므로 무효화 줄을 생략하면 시스템이 전체 구축을 강제로 수행합니다. 각 FlexConfig 개체에 항상 적절한 무효화 행을 포함하면 이 문제를 방지할 수 있습니다.

인터페이스 및 관리 상태 보기

디바이스 요약에는 디바이스의 그래픽 보기와 관리 주소에 대한 일부 설정이 포함됩니다. Device Summary(디바이스 요약)를 열려면 **Device(**디바이스**)**를 클릭합니다.

이 그래픽의 요소는 요소 상태에 따라 색이 변경됩니다. 요소 위에 마우스를 놓으면 추가 정보가 제공되는 경우도 있습니다. 이 그래픽을 통해 다음 항목을 모니터링할 수 있습니다.

참고 인터페이스 상태 정보를 비롯한 그래픽의 인터페이스 부분은 **Interfaces(**인터페이스**)** 페이지와 **Monitoring(**모니터링**)** > **System(**시스템**)** 대시보드에서도 제공됩니다.

인터페이스 상태

포트 위에 마우스를 놓으면 해당 IP 주소와 활성화 상태 및 링크 상태가 표시됩니다. IP 주소는 정적으로 할당할 수도 있고 DHCP를 사용하여 가져올 수도 있습니다. BVI(Bridge Virtual Interface) 위에 마우스를 놓으면 멤버 인터페이스의 목록도 표시됩니다.

인터페이스 포트는 다음 색 코드를 사용합니다.

- 녹색 — 인터페이스가 구성되어 있고 활성화된 상태이며 링크가 작동합니다.
- 회색 — 인터페이스를 활성화하지 않습니다.
- 주황색/빨간색 — 인터페이스가 구성되어 있고 활성화된 상태이지만 링크가 작동하지 않습니다. 유선 인터페이스의 경우 이 색은 수정해야 하는 오류 상태를 나타냅니다. 유선 인터페이스가 아닌 경우에는 이 색이 표시되는 것이 정상입니다.

내부, 외부 네트워크 연결

그래픽에는 다음 조건에 따라 외부(또는 업스트림) 및 내부 네트워크에 연결된 포트가 표시됩니다.

- 내부 네트워크 — 내부 네트워크의 포트는 이름이 "내부"인 인터페이스에 대해서만 표시됩니다. 추가 내부 네트워크는 있더라도 표시되지 않습니다. 이름을 "내부"로 지정한 인터페이스가 없으면 어떤 포트도 내부 포트로 표시되지 않습니다.
- 외부 네트워크 — 외부 네트워크의 포트는 이름이 "외부"인 인터페이스에 대해서만 표시됩니다. 내부 네트워크와 마찬가지로 이 이름은 필수 항목입니다. 이름을 지정하지 않으면 어떤 포트도 외부 포트로 표시되지 않습니다.

관리 설정 상태

그래픽에는 관리 주소에 대해 게이트웨이, DNS 서버, NTP 서버 및 스마트 라이선싱이 구성되어 있는지와 해당 설정이 올바르게 작동하고 있는지가 표시됩니다.

녹색은 기능이 구성되어 있고 정상적으로 작동함을 나타내며, 회색은 기능이 구성되어 있지 않거나 정상적으로 작동하지 않음을 나타냅니다. 예를 들어 서버에 연결할 수 없으면 DNS 상자가 회색으로 표시됩니다. 요소 위에 마우스를 올려놓으면 추가 정보가 표시됩니다.

문제가 확인되면 다음과 같이 수정하십시오.

- 관리 포트 및 게이트웨이 — **System Settings(**시스템 설정**)** > **Management Interface(**관리 인터페이스**)**를 선택합니다.
- DNS 서버 — **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**를 선택합니다.
- NTP 서버 — **System Settings(**시스템 설정**)** > **NTP**를 선택합니다. NTP 트러블슈팅도 참조하십시오.
- 스마트 라이선스 — 스마트 라이선스 그룹에서 **View Configuration(**컨피그레이션 보기**)** 링크를 클릭합니다.

시스템 작업 상태 보기

시스템 작업에는 다양한 데이터베이스 업데이트 검색/적용 등 사용자가 직접 개입하지 않아도 수행되는 작업이 포함됩니다. 이러한 작업 및 해당 상태의 목록을 통해 이러한 시스템 작업이 성공적으로 완료됨을 확인할 수 있습니다.

작업 목록에는 시스템 작업 및 구축 작업의 통합된 상태가 표시됩니다. 감사 로그에는 더 자세한 정보가 포함되어 있는데, 이러한 감사 로그는 **Device(**디바이스**)** > **Device Administration(**디바이스 관리**)** > **Audit Log(**감사 로그**)**에서 얻을 수 있습니다. 예를 들어 감사 로그에는 작업 시작과 작업 종료에 대해 각기 별도의 이벤트가 표시되는 반면 작업 목록에서는 이러한 이벤트가 단일 항목으로 병합됩니다. 그리고 구축에 대한 감사 로그 항목에는 구축된 변경 사항과 관련된 세부 정보가 포함됩니다.

프로시저

단계 **1** 주 메뉴에서 **Task List(**작업 목록**)** 버튼을 클릭합니다.

작업 목록이 열리고 시스템 작업의 상태와 세부정보가 표시됩니다.

단계 **2** 작업 상태를 평가합니다.

지속적으로 발생하는 문제가 있으면 디바이스 컨피그레이션을 수정해야 할 수 있습니다. 예를 들어 데이터베이스 업데이트를 가져올 때 지속적으로 장애가 발생하면 인터넷으로 이동하는 디바이스 관리 IP 주소용 경로가 없는 것일 수 있습니다. 일부 문제의 경우 작업 설명에 나와 있는 대로 Cisco TAC(Technical Assistance Center)에 문의해야 할 수 있습니다.

작업 목록을 사용하여 다음 작업을 수행할 수 있습니다.

- **Success(**성공**)** 또는 **Failures(**실패**)** 버튼을 클릭하여 이러한 상태를 기준으로 목록을 필터링합니다.
- 작업의 삭제 아이콘( )을 클릭하여 목록에서 제거합니다.
- **Remove All Completed Tasks(**완료된 모든 작업 제거**)**를 클릭하여 진행 중이지 않은 모든 작업의 목록을 비웁니다.

CLI 콘솔을 사용하여 컨피그레이션 모니터링 및 테스트

Threat Defense 디바이스에는 모니터링 및 문제해결에 사용할 수 있는 CLI(Command Line Interface)가 포함되어 있습니다. SSH 세션을 열어 모든 시스템 명령에 대한 액세스 권한을 얻을 수 있지만, device manager에서 CLI 콘솔을 열어 읽기 전용 명령(예: 다양한 **show** 명령 및 **ping**, **traceroute**, **packet-tracer**)을 사용할 수도 있습니다. 관리자 권한을 보유한 경우, **failover**, **reboot**, **shutdown** 명령을 입력할 수도 있습니다.

페이지 간을 이동하고 기능을 구성 및 구축할 때 CLI 콘솔을 열어 둘 수 있습니다. 예를 들어 새 정적 경로를 구축한 후에 CLI 콘솔에서 **ping**을 사용하여 대상 네트워크에 연결할 수 있는지 확인할 수 있습니다.

CLI 콘솔에서는 기본 위협 방어 CLI를 사용합니다. CLI 콘솔을 사용하여 진단 CLI, 전문가 모드 또는 FXOS CLI(FXOS를 사용하는 모델)를 시작할 수는 없습니다. 기타 CLI 모드를 시작해야 하는 경우에는 SSH를 사용합니다.

명령에 대한 세부 정보는 Cisco Firepower Threat Defense 명령 참조, https://www.cisco.com/c/en/us/td/docs/security/firepower/command_ref/b_Command_Reference_for_Firepower_Threat_Defense.html을 참조 하십시오.

참고**:**

- **ping**은 CLI 콘솔에서 지원하지만 **ping system** 명령은 지원하지 않습니다.
- 시스템은 동시 명령을 2개까지만 처리할 수 있습니다. 따라서 다른 사용자가 REST API 등을 사용하여 명령을 실행 중이라면 명령을 입력하기 전에 다른 명령이 완료될 때까지 기다려야 할 수 있습니다. 문제가 지속되면 CLI 콘솔 대신 SSH 세션을 사용하십시오.
- 명령은 구축된 컨피그레이션을 기반으로 정보를 반환합니다. device manager에서 컨피그레이션을 변경하되 이를 구축하지 않을 경우, 명령 출력에 변경 결과가 표시되지 않습니다. 예를 들어 새 정적 경로를 생성하지만 이를 구축하지 않을 경우, 해당 경로는 **show route** 출력에 표시되지 않습니다.

프로시저

단계 **1** 웹 페이지의 오른쪽 상단에 있는 **CLI Console(CLI** 콘솔**)** 버튼을 클릭합니다.

단계 **2** 프롬프트에서 명령을 입력하고 **Enter** 키를 누릅니다.

일부 명령은 다른 명령보다 출력을 생성하는 데 오래 걸릴 수 있으니 기다려 주십시오. 명령 실행 시간 제한이 초과되었다는 메시지를 받으면 다시 시도하십시오. 또한 **show perfstats**와 같은 대화형 응답이 필요한 명령을 입력하는 경우, 타임 아웃 오류가 발생합니다. 문제가 지속되면 CLI 콘솔 대신 SSH 클라이언트를 사용해야 할 수 있습니다.

창을 사용하는 방법에 몇 가지 팁은 다음과 같습니다.

- 명령의 일부만 입력하면 자동으로 전체 명령이 입력되도록 하려면 **Tab** 키를 누릅니다. 또한, Tab 키를 누르면 명령에서 해당 시점에 사용할 수 있는 파라미터가 나열됩니다. Tab 키는 키워드의 세 가지 레벨에서 작동합니다. 세 가지 레벨 이후 자세한 내용을 확인하려면 명령 참조를 사용해야 합니다.
- Ctrl+C를 눌러 명령 실행을 중지할 수 있습니다.
- 창을 이동하려면 헤더의 아무 곳이나 클릭하여 누른 상태에서 원하는 위치로 창을 끌어옵니다.

- 창을 더 크게 또는 더 작게 조정하려면 **Expand(**확장**)(**  **)** 또는 **Collapse(**축소**)(****)** 버튼을 클릭합니다.
- 웹 페이지에서 창을 분리하여 사용 중인 브라우저 창에 도킹하려면 **Undock Into Separate Window(**분리하여 별도의 창에 도킹**)(**  **)** 버튼을 클릭합니다. 다시 도킹하려면 **Dock to Main Window(**기본 창에 도킹**)(**  **)** 버튼을 클릭합니다.
- 클릭하고 끌어 텍스트를 강조 표시한 다음 Ctrl+C를 눌러 출력을 클립보드에 복사합니다.
- 모든 출력을 지우려면 **Clear CLI(CLI** 지우기**)(**  **)** 버튼을 클릭합니다.
- 입력한 마지막 명령의 출력을 클립보드에 복사하려면 **Copy Last Output(**마지막 출력 복사**)(**  **)** 버튼을 클릭합니다.

단계 **3** 작업을 마치면 콘솔 창을 닫습니다. **exit** 명령은 사용하지 마십시오.

device manager에 로그인할 때 사용하는 크리덴셜은 CLI에 대한 액세스를 검증하지만, 콘솔을 사용할 때는 CLI에 실제로 로그인하지 않습니다.

Device Manager 및 REST API 함께 사용

로컬 관리 모드로 디바이스를 설정할 때는 device manager와 위협 방어 REST API를 사용하여 디바이스를 구성할 수 있습니다. 실제로 device manager는 REST API를 사용하여 디바이스를 구성합니다.

그러나 REST API는 device manager를 통해 제공되는 기능 이외의 추가 기능을 제공할 수 있습니다. 따라서 특정 기능에 대해 device manager를 통해 컨피그레이션을 확인할 때는 표시할 수 없는 설정을 REST API를 통해서는 구성할 수도 있습니다.

REST API에서는 제공되지만 device manager에서는 제공되지 않는 기능 설정을 구성한 다음 device manager를 사용하여 원격 액세스 VPN 등의 전체 기능을 변경하는 경우에는 해당 설정이 실행 취소될 수 있습니다. API 전용 설정이 유지되는지 여부는 달라질 수 있으며, 많은 경우 device manager에서 사용할 수 없는 설정에 대한 API 변경 사항은 device manager 수정을 통해 유지됩니다. 특정 기능의 경우 변경 사항이 유지되는지 여부를 확인해야 합니다.

일반적으로, 특정 기능에 대해 device manager와 REST API를 동시에 사용해서는 안 됩니다. 대신 기능별로 한 가지 방법을 선택해 디바이스를 구성하십시오.

API Explorer를 사용하여 API 메서드를 확인하고 시도할 수 있습니다. More options(추가 옵션) 버튼(⋮)을 클릭하고 **API Explorer**를 선택합니다.