빠른 시작 가이드

Cisco ASA 5500-X Series

ASA 5512-X, ASA 5515-X, ASA 5525-X, ASA 5545-X 및 ASA 5555-X

규제 준수 및 안전 정보

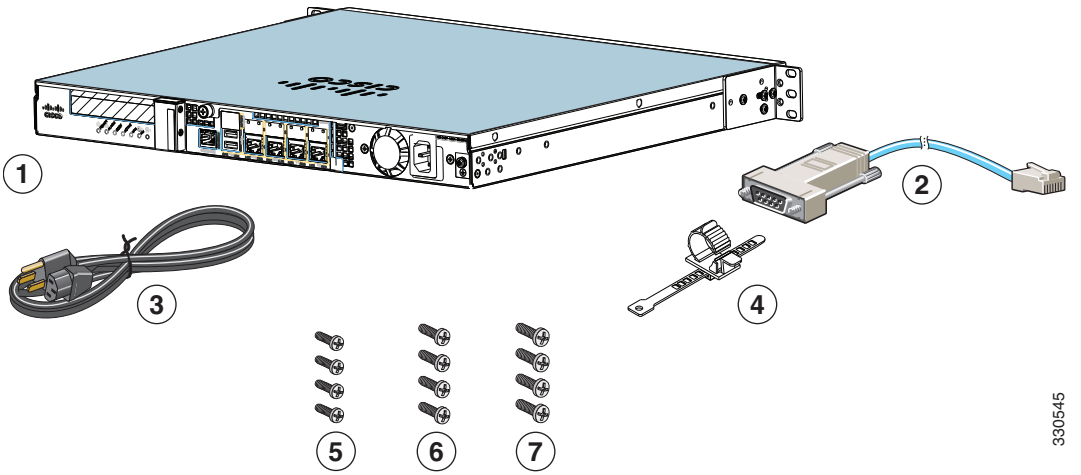
RCSI(Regulatory Compliance and Safety Information)의 안전 경고를 읽고 가이드에서 설명하고 있는 절차를 실행할 때 적절한 안전 조치를 취하도록 합니다. RCSI 및 기타 문서의 링크는 http://www.cisco.com/go/asadocs를 참고하십시오.

수정: 2014년 5월 1일

1 패키지 구성 내용

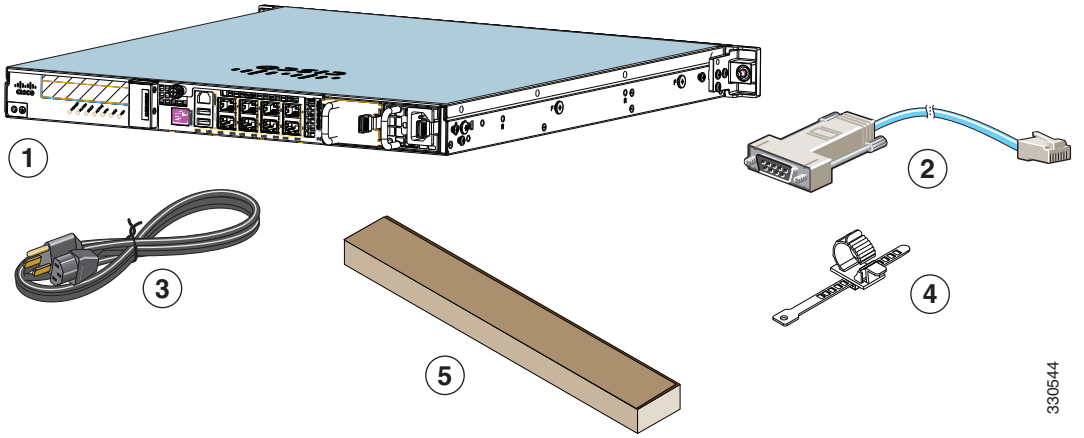
이 섹션에서는 각 섀시의 패키지 구성을 보여 줍니다. 구성 내용은 변경될 수 있으며, 정확한 구성에는 일부 항목이 추가되거나 제외될 수 있습니다.

ASA 5512-X, ASA 5515-X 또는 ASA 5525-X



1	ASA 5512-X, ASA 5515-X 또는 ASA 5525-X 섀시	**2**	파란색 콘솔 케이블 및 시리얼 PC 터미널 어댑터 (DB-9 to RJ-45)
3	전원 코드	**4**	전원 코드 리테이너
5	랙 마운팅용 10-32 Philips 나사 4 개	**6**	랙 마운팅용 12-24 Philips 나사 4 개
7	랙 마운팅용 M6 Philips 나사 4 개		

ASA 5545-X 및 ASA 5555-X



1	ASA 5545-X 또는 ASA 5555-X 섀시 (표시된 전원 공급 장치 1 개)	**2**	파란색 콘솔 케이블 및 시리얼 PC 터미널 어댑터 (DB-9 to RJ-45)
3	전원 코드	**4**	전원 코드 리테이너
5	슬라이드 레일 키트		

2 ASA 전원 켜기

1단계 전원 케이블을 ASA에 연결하고 전기 콘센트에 꽂습니다.

전원 케이블을 꽂으면 전원이 자동으로 켜지므로 전면 패널의 전원 버튼을 누르지 마십시오. (구형 모델에서는 전원이 자동으로 켜지지 않습니다. 자세한 내용은 하드웨어 설치 가이드를 확인하십시오.)

2단계 ASA 전면의 전원 LED를 확인합니다. 장치의 전원이 켜져 있으면 녹색으로 표시됩니다.

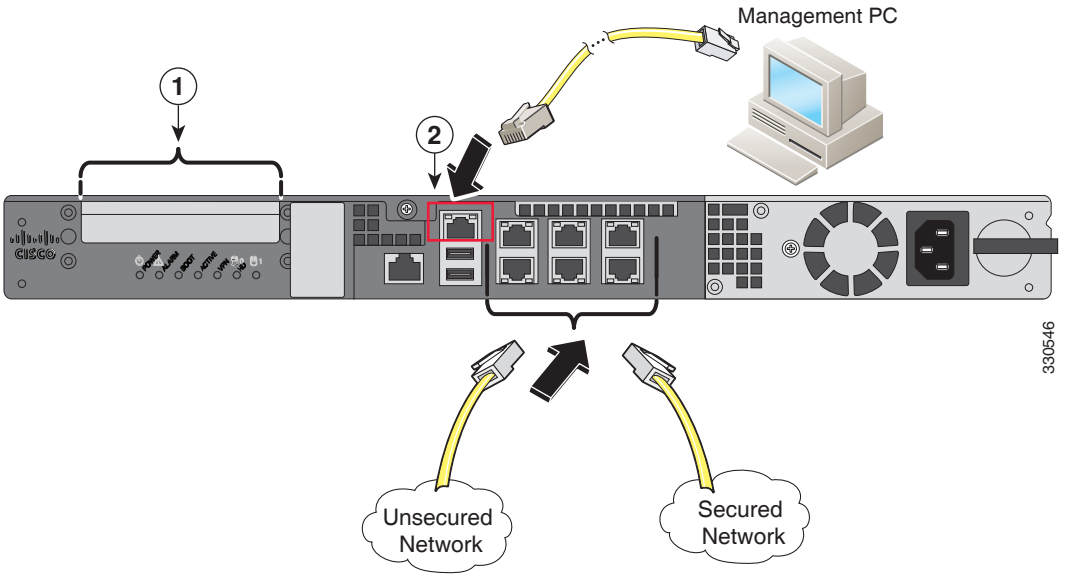
3단계 ASA 전면의 상태 LED를 확인합니다. 시스템이 전원 켜기 진단을 통과하면 녹색으로 표시됩니다.

3 인터페이스 케이블 연결 및 연결 확인

1단계 ASDM(Adaptive Security Device Manager)용 관리 0/0 인터페이스에 관리 PC를 연결합니다. 이더넷 케이블을 사용하여 PC를 직접 연결하거나, PC와 ASA를 동일한 관리 네트워크에 연결할 수 있습니다. PC가 DHCP를 사용하여 IP 주소를 가져오도록 구성되어 있는지 확인하십시오.

CLI를 사용하려면 PC를 콘솔 포트에 연결하고 CLI 컨피그레이션 가이드에서 자세한 내용을 참고하십시오.

2단계 네트워크를 적절한 포트에 연결합니다.



1	(선택 사항) I/O 카드 파이버 I/O 카드가 있는 경우 SFP 모듈 (포함되지 않음) 을 사용해야 합니다 . 자세한 내용은 하드웨어 설치 가이드를 참고하십시오 .	**2**	관리 0/0 인터페이스 (RJ-45)

3단계 LINK/ACT 표시기에서 인터페이스 연결을 확인합니다.

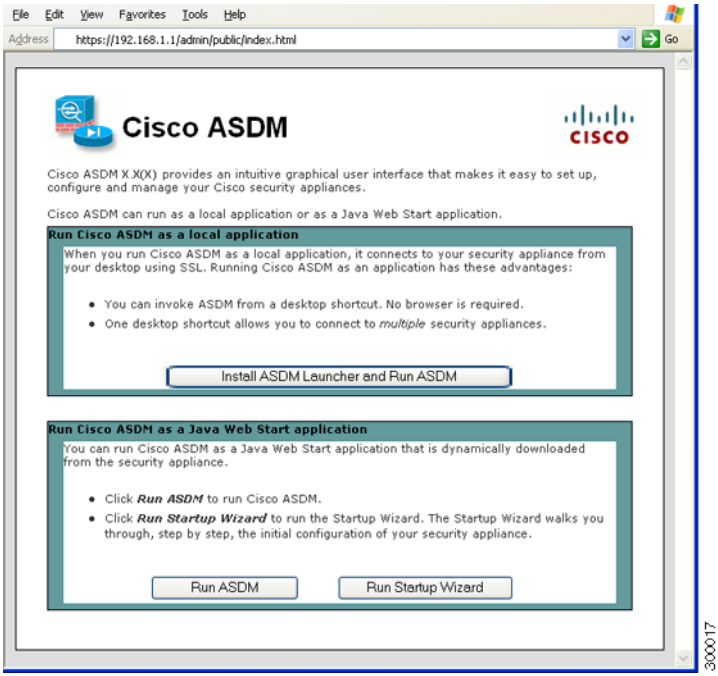
4 ASDM 실행

ASA는 기본적으로 ASDM과 관리 0/0 인터페이스의 연결을 활성화하는 구성으로 제공됩니다. ASDM을 사용하면 마법사를 통해 기본 및 고급 기능을 구성할 수 있습니다. ASDM은 웹 브라우저를 사용하여 어디에서든 ASA를 관리할 수 있도록 해주는 그래픽 사용자 인터페이스(GUI)입니다.

ASDM을 실행하기 위한 요구 사항은 Cisco.com에서 ASDM 릴리스 노트를 참고하십시오.

1단계 ASA에 연결된 PC에서 웹 브라우저를 실행합니다.

2단계 주소 필드에 URL **https://192.168.1.1/admin**을 입력합니다. Cisco ASDM 웹 페이지가 나타납니다.



3단계 **Run Startup Wizard(상태 마법사 실행)**를 클릭합니다.

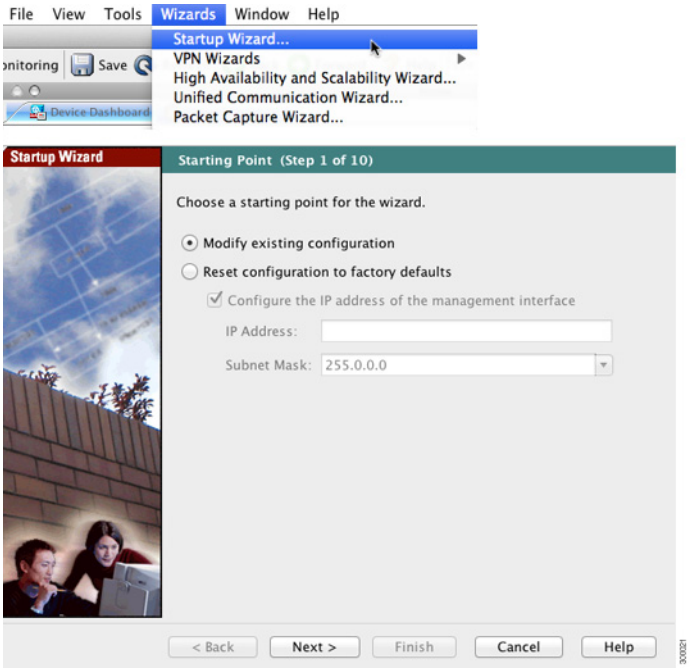
4단계 표시되는 대화 상자에 따라 모든 인증서를 적용합니다. Cisco ASDM-IDM Launcher(Cisco ASDM-IDM 시작 관리자)가 나타납니다.

5단계 사용자 이름 및 비밀번호 필드를 비어 있는 상태로 두고 **OK(확인)**를 클릭합니다. 기본 ASDM 창이 나타나고 Startup Wizard(시작 마법사)가 열립니다.

5 Startup Wizard(시작 마법사) 실행

배포에 맞게 보안 정책을 사용자 지정할 수 있도록 기본 구성을 수정하려면 **Startup Wizard(시작 마법사)**를 실행합니다. Startup Wizard(시작 마법사)를 사용하여 다음을 설정할 수 있습니다.

- 호스트 이름
- 도메인 이름
- 관리 비밀번호
- 인터페이스
- IP 주소
- 정적 경로
- DHCP 서버
- 네트워크 주소 변환 규칙
- 기타



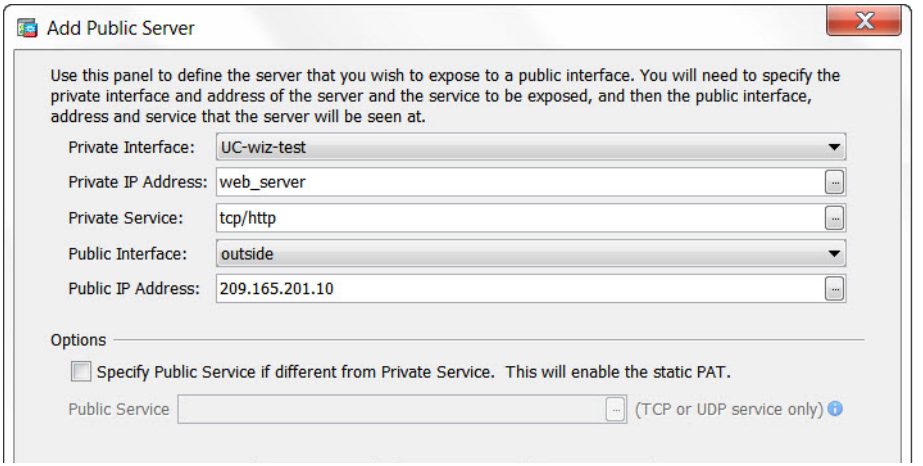
1단계 마법사를 아직 실행하지 않은 경우 기본 ASDM 창에서 **Wizards(마법사) > Startup Wizard(시작 마법사)**를 선택합니다.

2단계 Startup Wizard(시작 마법사)의 지침에 따라 ASA를 구성합니다.

3단계 마법사를 실행하는 동안 기본 설정을 적용하거나 필요에 따라 변경할 수 있습니다. 마법사 필드에 대한 자세한 내용을 보려면 **Help(도움말)**를 클릭하십시오.

6 (선택 사항) ASA 뒤에 있는 공용 서버에 대한 액세스 허용

Public Server(공용 서버) 창에서는 인터넷을 통해 내부 서버에 액세스할 수 있도록 하는 보안 정책을 자동으로 구성합니다. 비즈니스 소유자는 웹 및 FTP 서버 등 외부 사용자가 사용할 수 있도록 해야 하는 내부 네트워크 서비스를 운영할 수 있습니다. 이러한 서비스를 ASA 뒤에 있는 DMZ(Demilitarized Zone)라는 별도의 네트워크에 둘 수 있습니다. 공용 서버를 DMZ에 두면 공용 서버에 대해 실행된 어떤 공격도 내부 네트워크에 영향을 주지 않습니다.



1단계 기본 ASDM 창에서 **Configuration(구성) > Firewall(방화벽) > Public Servers(공용 서버)**를 선택합니다. Public Server(공용 서버) 창이 나타납니다.

2단계 **Add(추가)**를 클릭한 다음 Add Public Server(공용 서버 추가) 대화 상자에서 공용 서버 설정을 입력합니다. 필드에 대한 자세한 내용을 보려면 **Help(도움말)**를 클릭하십시오.

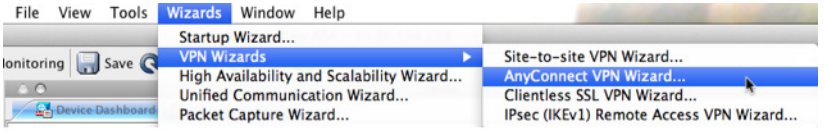
3단계 **OK(확인)**를 클릭합니다. 서버가 목록에 표시됩니다.

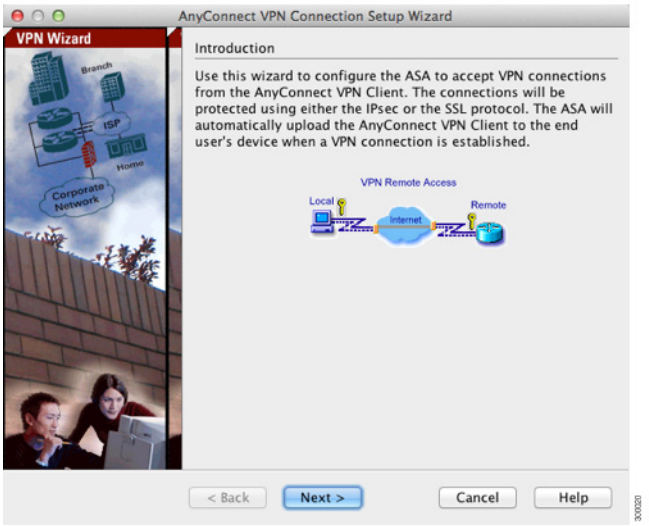
4단계 **Apply(적용)**를 클릭하여 ASA로 구성을 전송합니다.

7 (선택 사항) VPN 마법사 실행

다음 마법사를 사용하여 VPN을 구성할 수 있습니다.

- Site-to-Site VPN Wizard(사이트 대 사이트 VPN 마법사) - 두 ASA 사이에 IPsec Site-to-Site 터널을 만듭니다.
- AnyConnect VPN Wizard(AnyConnect VPN 마법사) - Cisco AnyConnect VPN 클라이언트에 대한 SSL VPN 원격 액세스를 구성합니다. AnyConnect는 회사 리소스에 대한 완전한 VPN 터널링을 통해 원격 사용자에게 ASA에 대한 보안 SSL 연결을 제공합니다. 원격 사용자가 브라우저를 통해 처음 연결할 때 AnyConnect 클라이언트를 다운로드하도록 ASA 정책을 구성할 수 있습니다. AnyConnect 3.0 이상을 사용하면 클라이언트에서 SSL 또는 IPsec IKEv2 VPN 프로토콜을 실행할 수 있습니다.
- Clientless SSL VPN Wizard(클라이언트리스 SSL VPN 마법사) - 브라우저에 대한 클라이언트 없는 SSL VPN 원격 액세스를 구성합니다. 클라이언트 없는 브라우저 기반 SSL VPN은 사용자가 웹 브라우저를 사용하여 ASA에 대한 보안 원격 액세스 VPN 터널을 설정할 수 있도록 해줍니다. 사용자는 인증 후 포털 페이지에 액세스하여 지원되는 특정 내부 리소스에 액세스할 수 있습니다. 네트워크 관리자는 사용자 그룹별로 리소스에 대한 액세스를 제공합니다. ACL을 적용하여 특정 회사 리소스에 대한 액세스를 제한하거나 허용할 수 있습니다.
- IPsec (IKEv1) Remote Access VPN Wizard(IPsec(IKEv1) 원격 액세스 VPN 마법사) - Cisco IPsec 클라이언트에 대한 IPsec VPN 원격 액세스를 구성합니다.





1단계 기본 ASDM 창에서 **Wizards(마법사) > VPN Wizards(VPN 마법사)**를 선택한 후 다음 중 하나를 선택합니다.

- **Site-to-Site VPN Wizard(사이트 대 사이트 VPN 마법사)**
- **AnyConnect VPN Wizard(AnyConnect VPN 마법사)**
- **Clientless VPN Wizard(클라이언트 없는 VPN 마법사)**
- **IPsec (IKEv1) Remote Access VPN Wizard(IPsec(IKEv1) 원격 액세스 VPN 마법사)**

2단계 마법사의 지침을 따릅니다. 마법사 필드에 대한 자세한 내용을 보려면 **Help(도움말)**를 클릭하십시오.

8 (선택 사항) ASDM에서 다른 마법사 실행

ASDM에서 다음 추가 마법사를 선택적으로 실행할 수 있습니다.

- High Availability and Scalability Wizard(고가용성 및 확장성 마법사)

  활성/활성 또는 활성/대기 장애 조치나 VPN 클러스터 부하 균형을 구성합니다.
- Unified Communications Wizard(유니파이드 커뮤니케이션 마법사)

  ASA에서 원격 액세스 또는 B2B(Business-to-Business) 통신용 프록시를 구성합니다. 특정 라이센스가 적용될 수 있습니다. ASA 라이센스에 대한 자세한 내용은 CLI 컨피그레이션 가이드를 참고하십시오.
- Packet Capture Wizard(패킷 캡처 마법사)

  패킷 캡처를 구성하고 실행합니다. 이 마법사는 인그레스(ingress) 및 이그레스(egress) 인터페이스 각각에서 하나의 패킷 캡처를 실행합니다. 패킷 캡처가 완료되면 패킷 분석기에서 검사하고 재생하기 위해 패킷 캡처를 PC에 저장할 수 있습니다.

9 고급 구성

ASA 구성을 계속하려면 http://www.cisco.com/go/asadocs에서 사용 중인 소프트웨어 버전에 대해 제공되는 문서를 참고하십시오.

미주 지역 본부
Cisco Systems, Inc.
San Jose, CA

아시아 태평양 지역 본부
Cisco Systems (USA) Pte. Ltd.
싱가포르

유럽 지역 본부
Cisco Systems International BV Amsterdam,
네덜란드

Cisco 는 전 세계에 200 여 개 이상의 지사가 있습니다 . 주소 , 전화 번호 및 팩스 번호는 Cisco 웹사이트 **www.cisco.com/go/offices** 에서 확인하십시오 .

78-20618-02