CISCO

START

Simple Secure Smart

FirePOWER 서비스를 포함한 Cisco ASA

간편 설치 가이드

이 단계별 가이드에 따라 ASA를 간편하게 설치하실 수 있습니다.

1. PC를 ASA에 연결
2. ASDM 설치
3. ASA 구성

CISCO

1 PC를 ASA에 연결

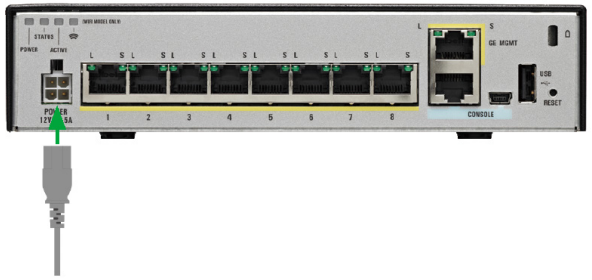
1-1 시작 전 주의사항

설치를 시작하기 앞서 아래와 같은 장비를 갖추고 있는지 확인하십시오.

- 본체
- 이더넷 케이블 3개
- AC 전원 케이블 (ASA 5506-X와 같이 제공)
- PC

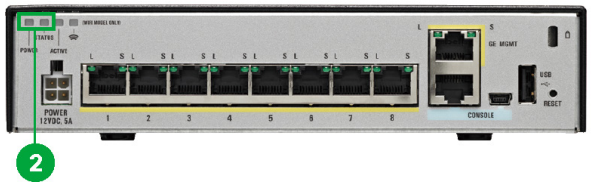
ASA에 아무 것도 연결되어 있지 않은지 확인하고 DHCP를 사용할 수 있도록 PC를 설정합니다.

1-2 PC를 ASA에 연결



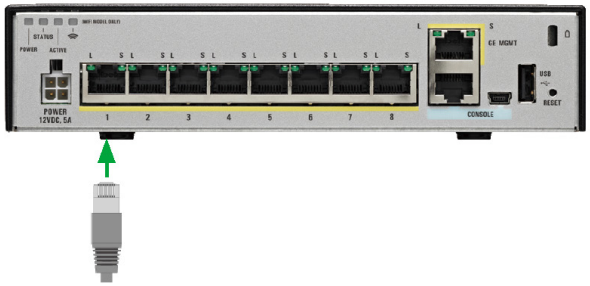
1 AC 전원 케이블을 ASA의 AC 전원 커넥터와 접지된 AC 콘센트에 연결합니다.

전원 케이블을 연결하면 자동으로 전원이 켜집니다. 전원 버튼은 따로 없습니다.



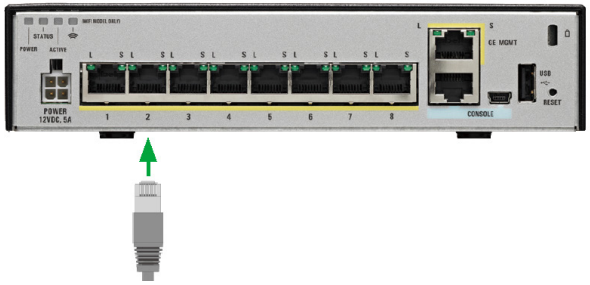
2 POWER LED와 STATUS LED가 솔리드 녹색인지 확인합니다.

POWER LED가 솔리드 녹색이 되면 장치에 전원이 들어온 것입니다. STATUS LED가 솔리드 녹색이 되면 시스템 초기 진단에 이상이 없음을 뜻합니다.



3 첫 번째 이더넷 케이블을 ASA의 이더넷 포트 1번에 연결하고, 케이블의 다른 끝은 WAN 장치의 이더넷 포트에 연결합니다.

ASA의 포트 LED와 WAN장치의 이더넷 포트 LED가 녹색이 되거나 녹색 깜박임이 나타날 때까지 기다립니다. 녹색 LED는 성공적으로 연결되었음을 의미합니다.



4 두 번째 이더넷 케이블을 ASA의 이더넷 포트 2번에 연결하고, 케이블의 다른 끝은 PC의 이더넷 포트에 연결합니다.

ASA의 포트 LED와 PC의 이더넷 포트 LED가 녹색이 되거나 녹색 깜박임이 나타날 때까지 기다립니다. 녹색 LED는 성공적으로 연결되었음을 의미합니다.

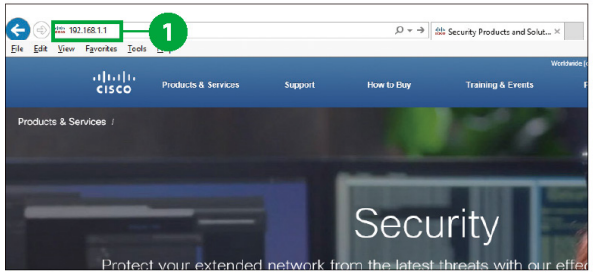
주의

❷단계에서 STATUS LED가 솔리드 녹색으로 바뀌지 않거나 황색으로 바뀐 경우에는 ASA의 시스템 초기 진단에 실패했다는 뜻이므로 AC 전원 케이블을 ASA AC 전원 커넥터와 접지된 AC 콘센트에 다시 연결하십시오. 그렇게 했는데도 STATUS LED가 솔리드 녹색으로 바뀌지 않거나 황색으로 바뀐 경우에는 시스코 담당자나 리셀러에게 연락하십시오.

❸ 및 ❹단계에서 이더넷 케이블을 연결한 ASA 포트는 RJ-45 관리 포트가 아니라 RJ-45 이더넷 포트가 되어야 합니다. RJ-45 이더넷 포트에는 번호가 매겨져 있습니다.

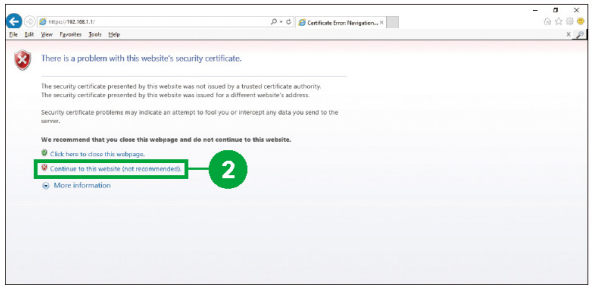
2 ASDM 설치

ASA를 구성하려면 Cisco Adaptive Security Device Manager (ASDM)을 사용하십시오. 이러한 단계들에 따라 ASA에서 Cisco ASDM을 다운로드하고 이를 PC에 설치합니다.



1 PC의 웹 브라우저를 실행하고 주소 표시줄에 IP 주소 https://192.168.1.1을 입력한 다음, Enter 키를 누릅니다.

이용자의 브라우저 환경에 따라 보안 인증서 페이지가 나타납니다.



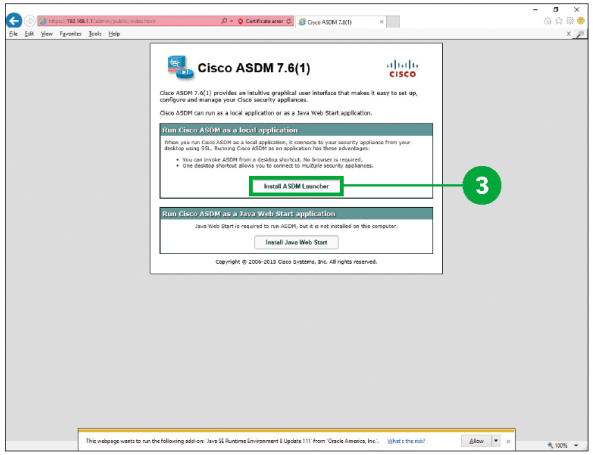
2 [Continue to this website (not recommended)]를 클릭합니다.

Cisco ASDM 웹 페이지가 나타납니다.

주의

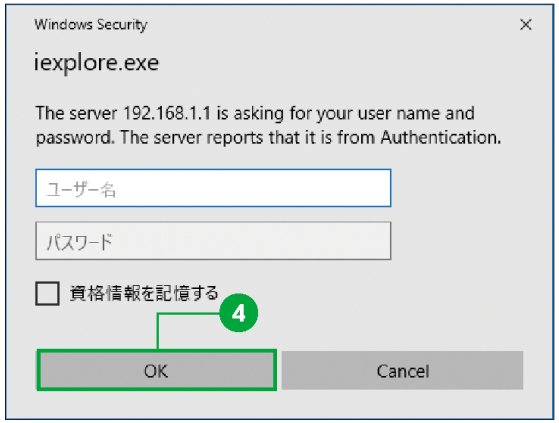
Cisco ASDM 웹 페이지가 나타나지 않으면 다음을 확인하십시오.

- POWER LED와 STATUS LED가 솔리드 녹색인지
- ASA의 이더넷 포트에 스트레이트 케이블이 연결되어 있는지
- 브라우저의 모든 팝업 차단 기능이나 프록시 설정이 비활성화되어 있는지, 그리고 PC 또는 노트북에서 모든 무선 클라이언트가 비활성화되어 있는지
- DHCP를 사용하도록 PC가 설정되어 있는지 ASA가 DHCP 서버 역할을 하고 있는지. PC에 수동으로 IP 주소가 할당되어 있는 경우에는 DHCP를 사용하도록 PC를 임시 설정합니다.



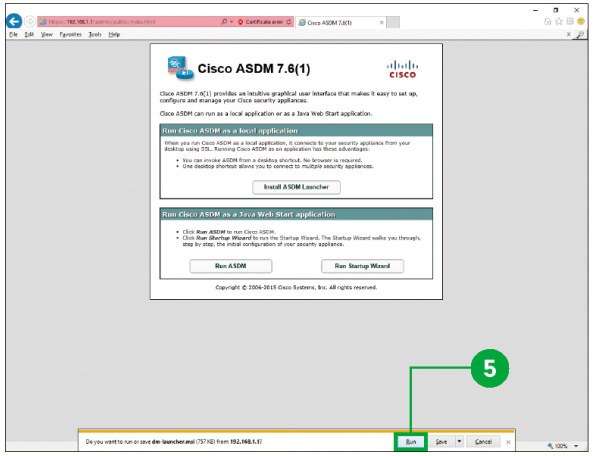
3 [Install ASDM Launcher]를 클릭합니다.

환경에 따라 인증 대화상자가 나타납니다.



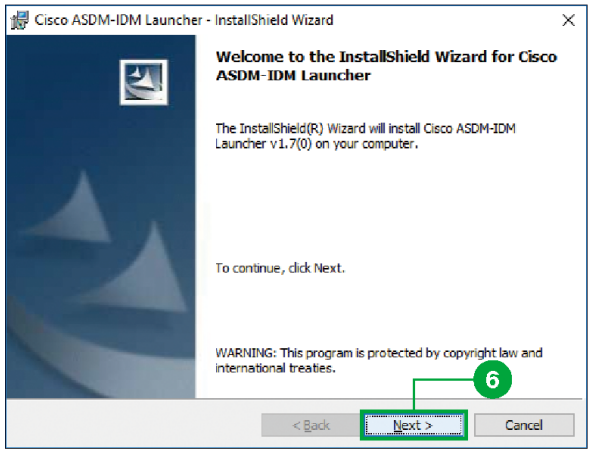
4 [OK]를 클릭합니다.

사용자 이름 및 암호 필드를 공백으로 남겨둡니다.

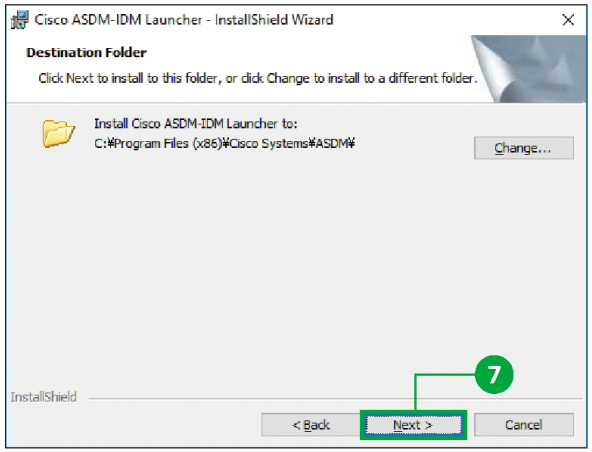


5 [Run]을 클릭합니다.

Cisco ASDM Launcher를 위한 InstallShield 마법사가 나타납니다.

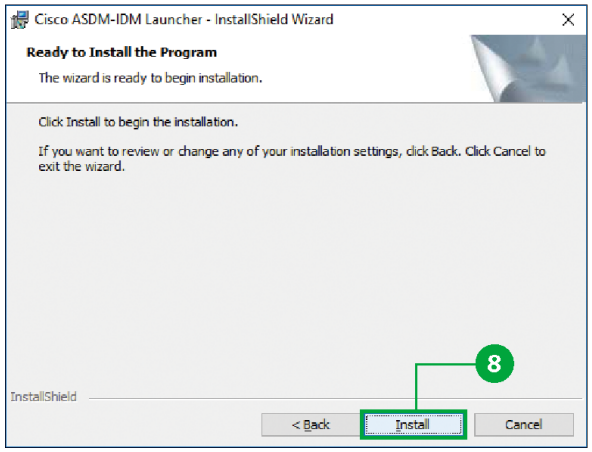


6 [Next]를 클릭합니다.

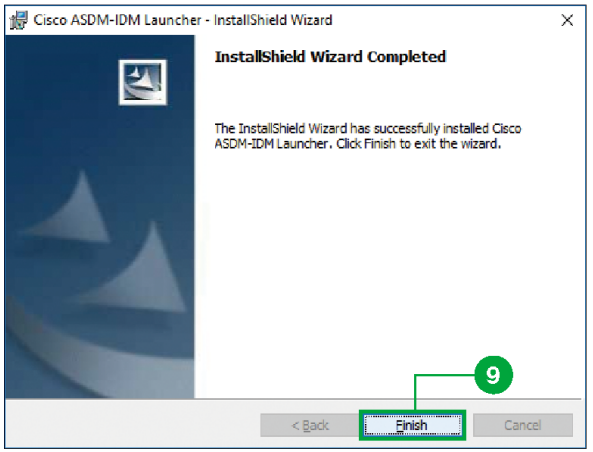


7 [Next]를 클릭합니다.

기본 설치 폴더를 변경하고 싶으면 [Change]를 클릭하고 원하는 설치 폴더를 입력하거나 선택합니다.



8 [Install]을 클릭합니다.



9 [Finish]를 클릭합니다.

Cisco ASDM Launcher가 나타납니다.

⚠ 주의

PC는 Cisco ASDM을 실행하기 위한 다음 요구사항을 충족해야 합니다.

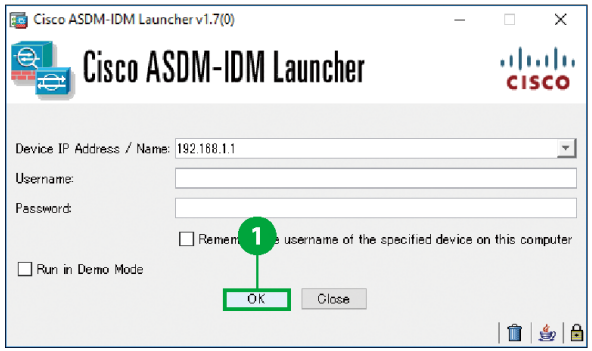
- Microsoft Windows 7, 8:
  - Microsoft Internet Explorer
  - Mozilla Firefox
  - Google Chrome
  - Java SE Plug-in 7.0 이상
- Apple OS X 10.4 이상
  - Mozilla Firefox
  - Apple Safari
  - Google Chrome (64비트 버전만)
  - Java SE Plug-in 7.0 이상

Microsoft Windows 8.1, 10을 사용할 수도 있습니다(공식 지원되는 것은 아님).

3 ASA 구성

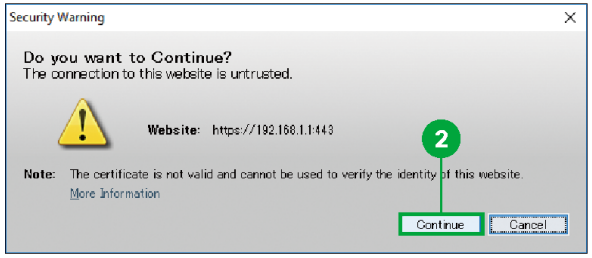
3-1 ASDM 실행

이제 Cisco ASDM Launcher를 통해 Cisco ASDM을 실행할 수 있습니다.

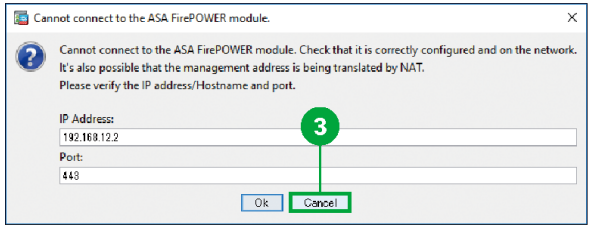


1 [OK]를 클릭합니다.

사용자 이름 및 암호 필드를 공백으로 남겨둡니다. 보안 경고가 나타납니다.



2 [Continue]를 클릭합니다.



3 [Cancel] 을 클릭합니다.

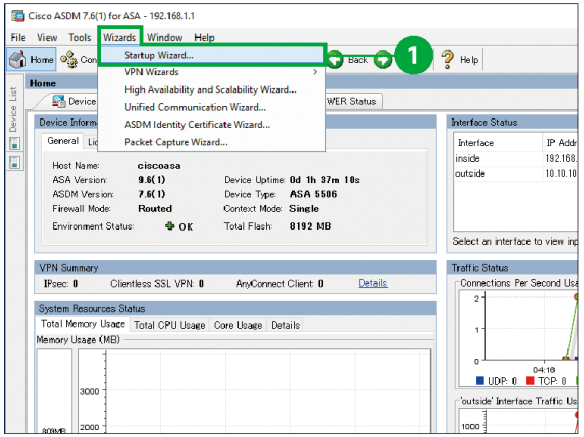
메인 ASDM 창이 나타납니다.

메모

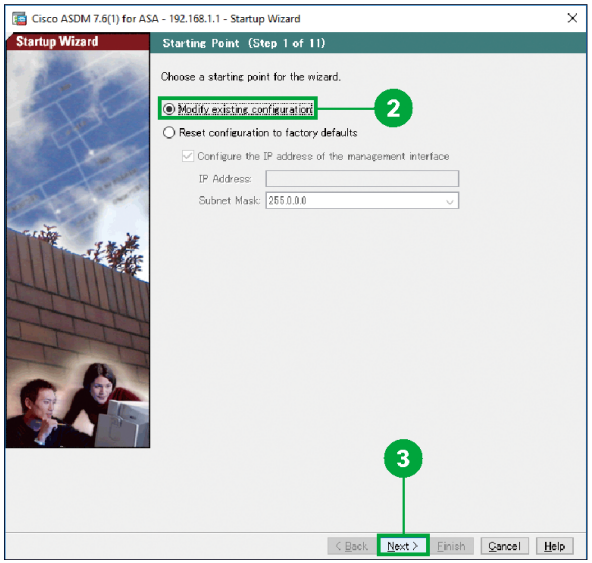
❸단계에서 ASA FirePOWER 모듈의 IP 주소를 입력하라는 메시지가 나타날 것입니다. 나중에 시작 마법사를 통해 FirePOWER 모듈의 IP주소를 변경할 수 있습니다.

3-2 시작 마법사 실행

ASDM를 실행한 이후에 시작 마법사를 이용해 초기 구성을 수행합니다.

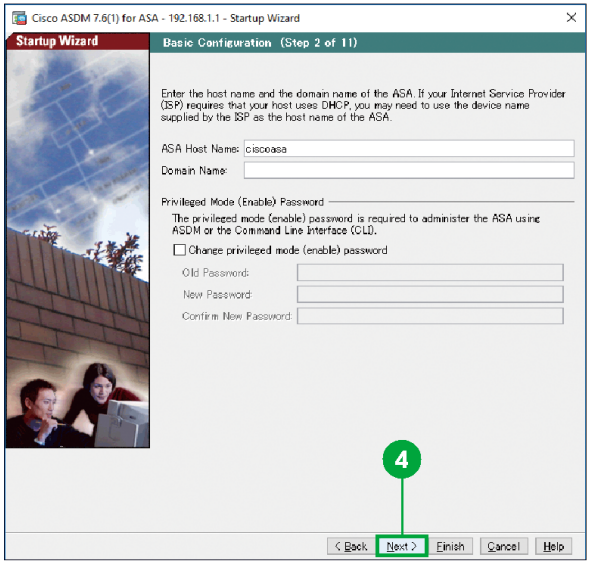


1 [Wizards] 메뉴 표시줄에서 [Startup Wizard]를 클릭합니다.



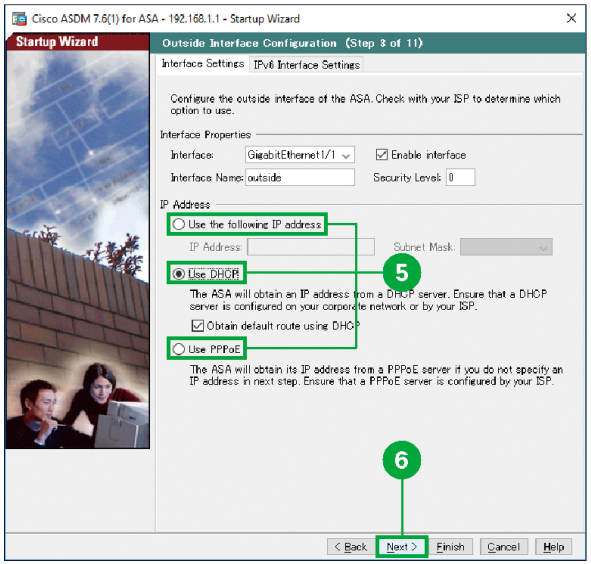
2 [Modify existing configuration]를 클릭합니다.

3 [Next]를 클릭합니다.



4 [Next]를 클릭합니다.

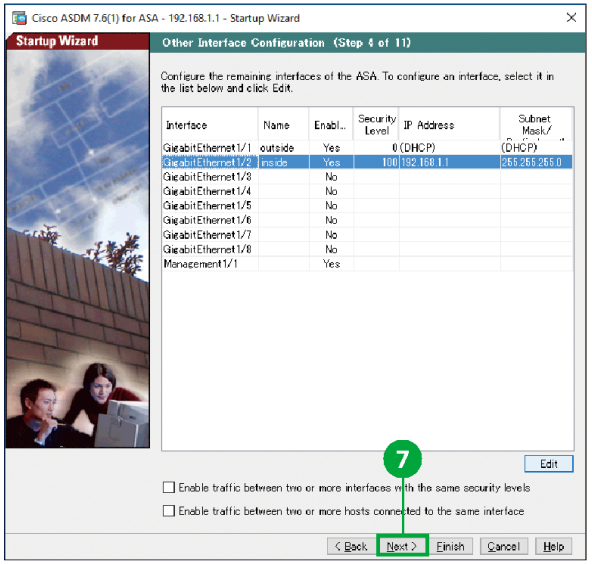
호스트 이름과 ASA의 도메인 이름을 입력할 수 있습니다.



5 적절한 옵션을 선택합니다.

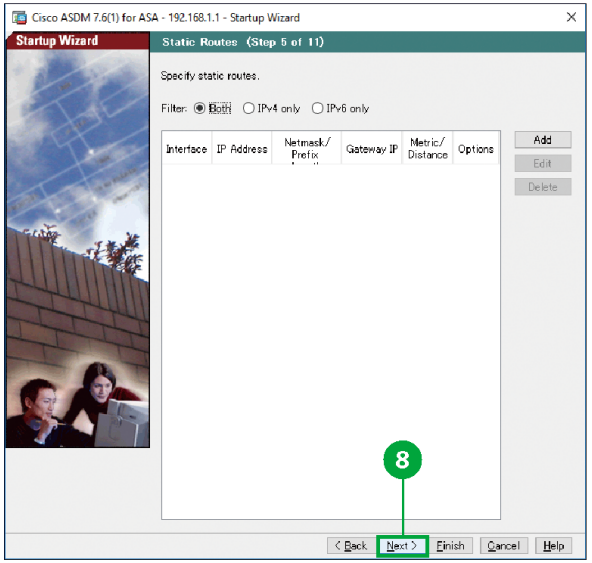
ASA의 외부 인터페이스를 구성합니다. 네트워크 구성상 기존 라우터 뒤쪽에 ASA가 위치하는 경우는 대부분 [Use DHCP]를 선택합니다. 기존 라우터 대신에 ASA가 들어가는 경우는 라우터 구성 절차를 따릅니다.

6 [Next]를 클릭합니다.



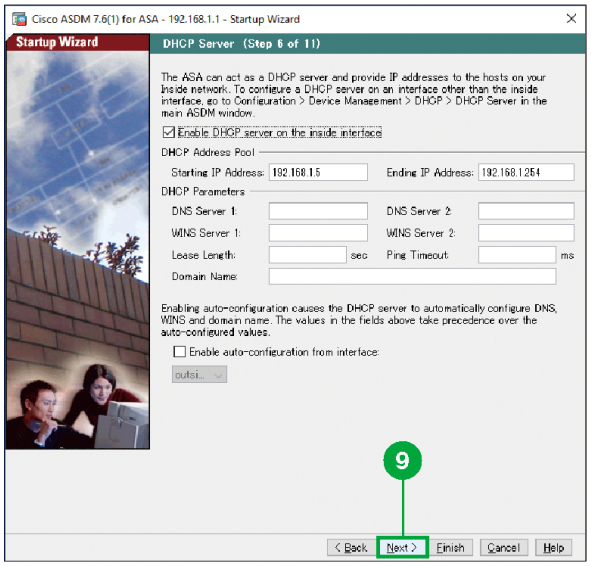
7 [Next]를 클릭합니다.

> **⚠ 주의**
> 내부 인터페이스는 외부 인터페이스에 할당된 IP 주소 범위와 다른 범위를 할당해야 합니다. 예를 들어 외부 범위가 192.168.1.x라면 내부 범위는 192.168.10.x 같이 달라야 합니다. 인터페이스를 선택하고 [Edit]를 클릭해서 범위를 변경할 수 있습니다.



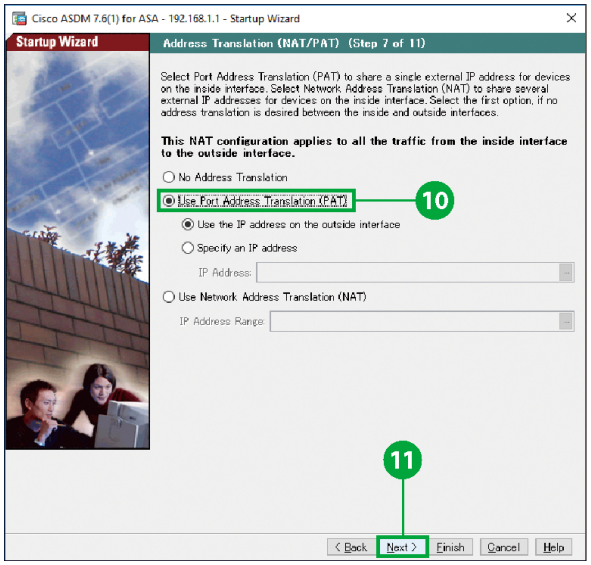
8 [Next]를 클릭합니다.

네트워크 상에 여러 대의 라우터가 있는 경우에는 정적 경로(Static routes)를 지정할 수 있습니다.



9 [Next]를 클릭합니다.

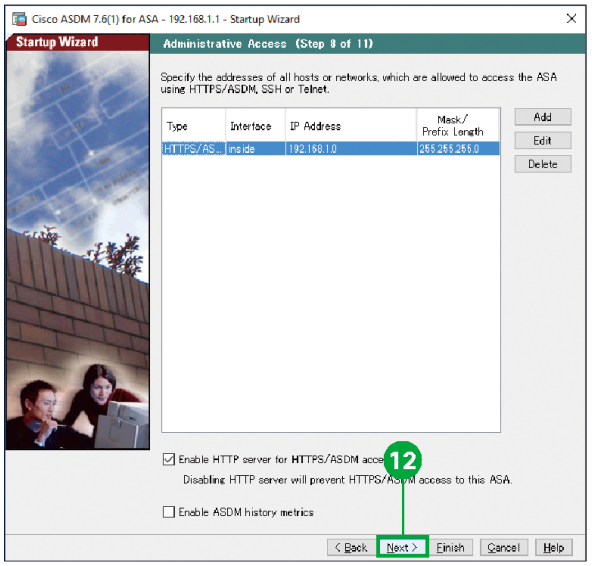
ASA가 DHCP 서버로 동작하게 하여 내부 네트워크의 호스트에 IP주소를 제공할 수 있습니다.



10 [Use Port Address Translation (PAT)]를 클릭합니다.

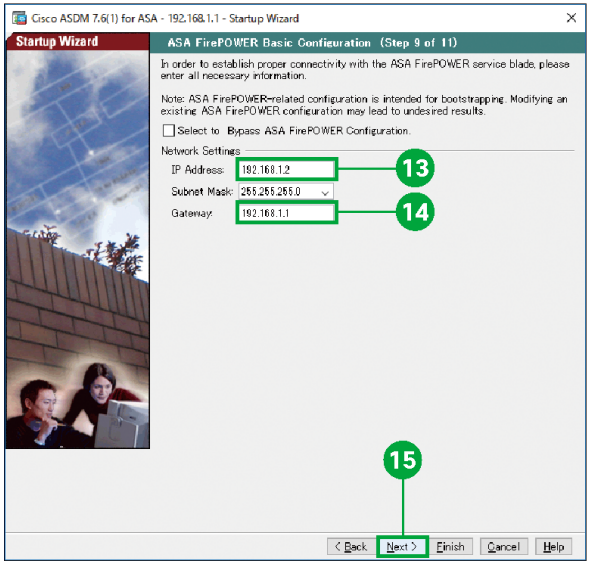
다수의 내부 네트워크 디바이스들에 대해 외부 인터페이스의 단일 IP 주소를 공유하도록 하는 경우는 [Use Port Address Translation (PAT)]를 선택합니다. 내부 인터페이스를 통해 연결된 다수의 네트워크 디바이스들에 대해 여러 개의 외부 IP주소를 공유하고 싶으면 [Use Network Address Translation (NAT)]를 선택합니다.

11 [Next]를 클릭합니다.



12 [Next]를 클릭합니다.

HTTPS/ASDM, SSH 또는 Telnet을 통해 ASA로 접속을 허용할 호스트 또는 네트워크를 지정할 수 있습니다.



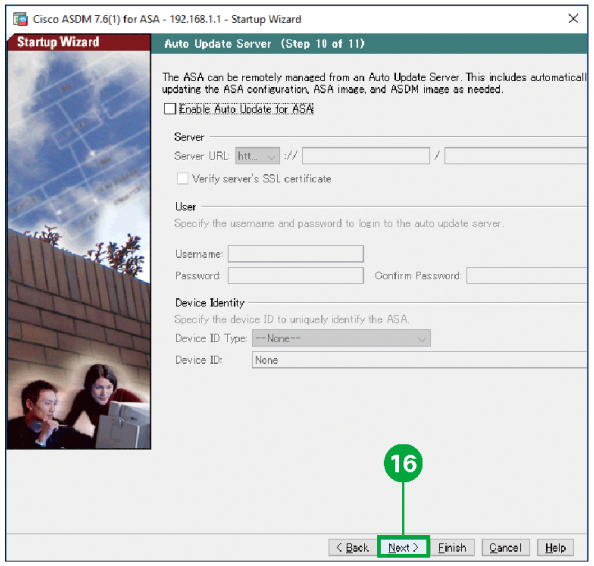
13 ASA FirePOWER 모듈에 대한 IP 주소를 입력합니다.

예를 들어 기본 구성에는 “192.168.1.2”이 설정되어 있습니다.

14 기본 게이트웨이의 IP 주소를 입력합니다.

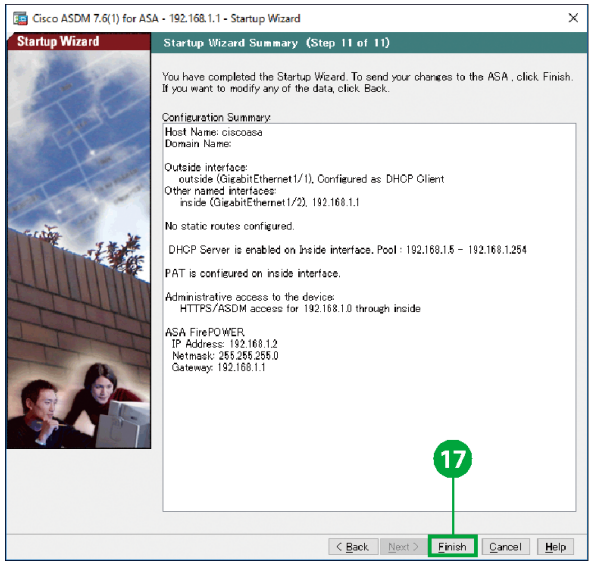
예를 들어 기본 구성에는 “192.168.1.1”이 설정되어 있습니다.

15 [Next]를 클릭합니다.



16 [Next]를 클릭합니다.

자동 업데이트 서버를 통해 ASA를 원격으로 관리할 수 있습니다. ASA설정, ASA이미지, ASDM이미지를 자동으로 업데이트 할 수 있는 구성이 포함되어 있습니다.

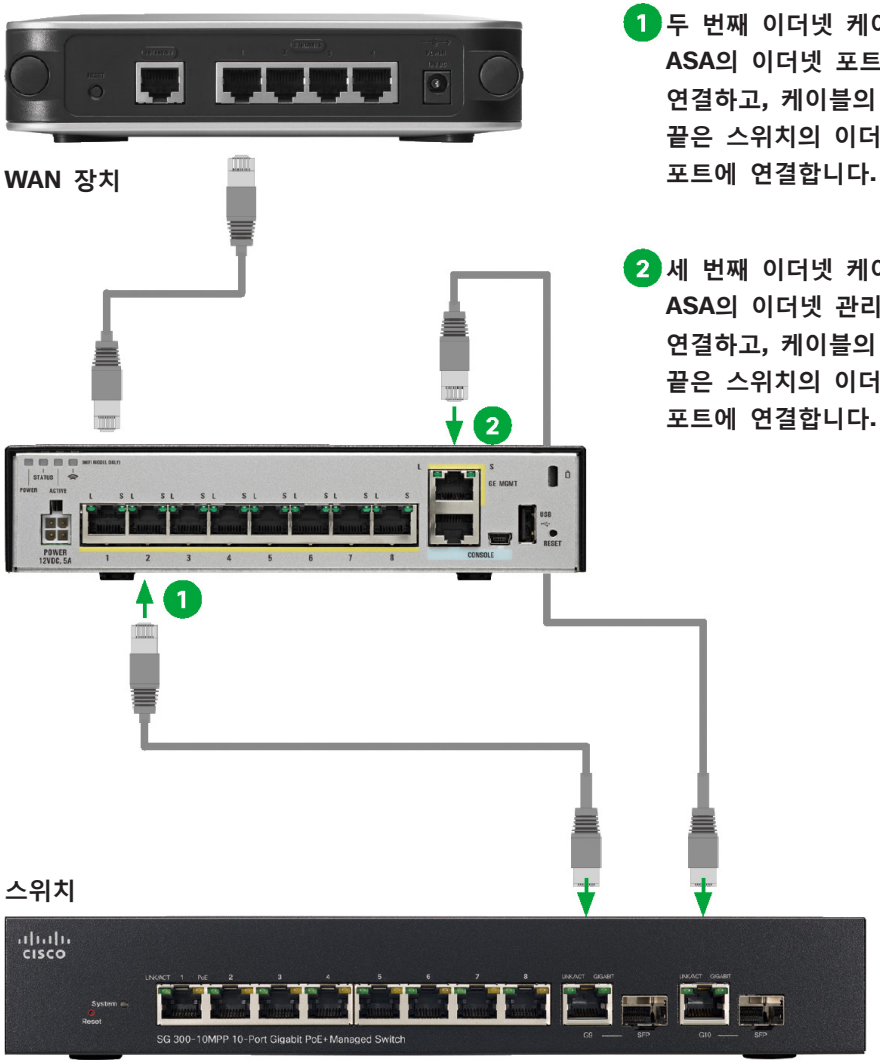


17 [Finish]를 클릭합니다.

시작 마법사를 완료하셨습니다. 변경한 내용으로 설정을 완료하는 경우 [Finish]를 클릭합니다. 데이터를 수정하고 싶으면 [Back]을 클릭합니다.

3-3 스위치를 ASA에 연결

시작 마법사를 완료했으면 ASDM을 종료하고 PC에서 이더넷 케이블을 분리합니다. 그런 다음, 아래 단계들에 따라 ASA에 스위치를 연결합니다. 스위치에 아무 것도 연결되어 있지 않은지, DHCP를 사용할 수 있도록 설정이 되어 있는지, 첫 번째 이더넷 케이블이 ASA와 WAN 장치 사이에 여전히 연결이 되어 있는지 확인합니다.

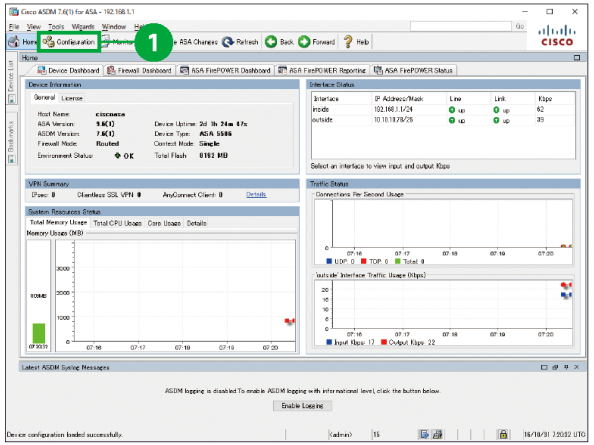


1 두 번째 이더넷 케이블을 ASA의 이더넷 포트 2번에 연결하고, 케이블의 다른 끝은 스위치의 이더넷 포트에 연결합니다.

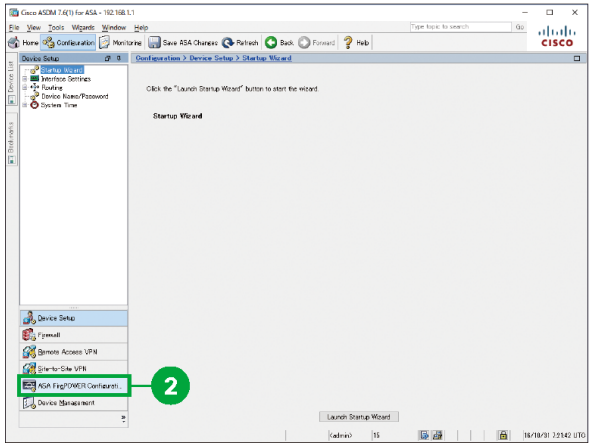
2 세 번째 이더넷 케이블을 ASA의 이더넷 관리 포트에 연결하고, 케이블의 다른 끝은 스위치의 이더넷 포트에 연결합니다.

3-4 라이센스 설치

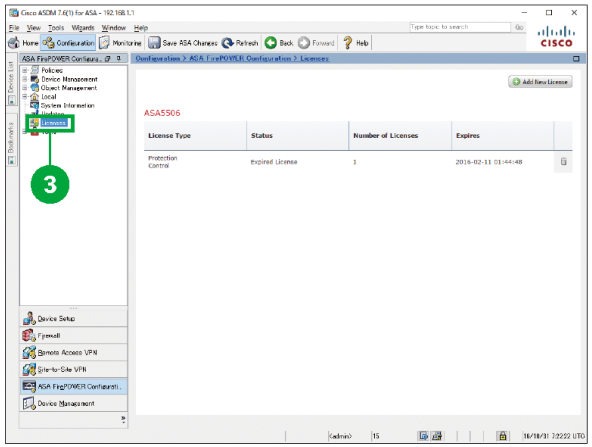
이제 Cisco ASDM에서 ASA FirePOWER 모듈에 액세스할 수 있게 되었습니다. Cisco ASDM을 재실행해서 라이센스를 설치합니다. 제어(AVC, Application Visibility and Control) 라이센스가 기본적으로 제공되며, 상자의 인쇄에 PAK(Product Authorization Key)가 포함됩니다. 추가 라이센스를 주문했다면 이메일에 이러한 라이센스에 대한 PAK가 포함될 것입니다.



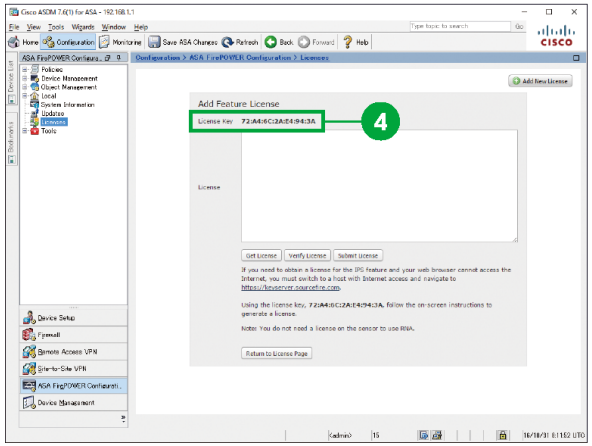
1 ASDM을 실행하고 [Configuration]을 클릭합니다.



2 [ASA FirePOWER Configuration]을 클릭합니다.



3 [Licenses]를 클릭합니다.



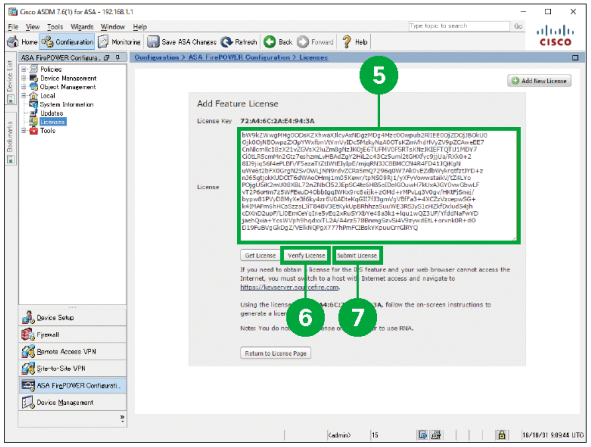
4 [License Key] 텍스트를 복사해서 라이센싱 포털에서 라이센스를 획득합니다(아래 메모 확인).

본 가이드에서 사용하는 샘플 라이센스 키는 72:78:DA:6E:D9:93:35입니다.

메모

라이센싱 포털에서 라이센스(라이센스 활성화 키)를 획득할 수 있습니다.

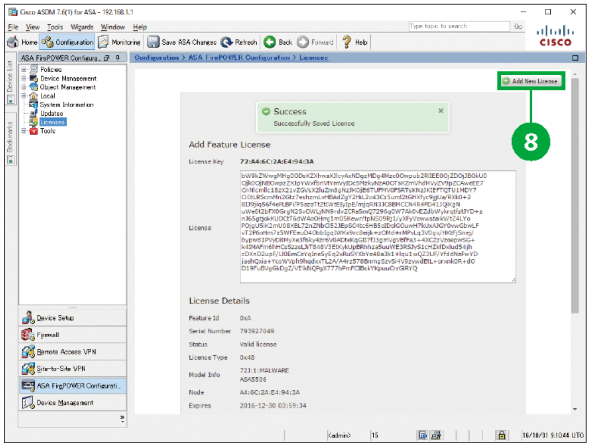
1. http://www.cisco.com/go/license로 갑니다.
2. [Get New Licenses] 필드에서 콤마로 구분된 PAK를 입력하고 [Fulfill]을 클릭합니다.
3. 다른 필드에 라이센스 키와 이메일 주소를 입력하라는 메시지가 나타날 것입니다.
4. 웹 사이트 화면이나 시스템에서 자동으로 제공되는 라이센싱 이메일에 첨부된 zip 파일에서 획득한 라이센스 활성화 키를 복사합니다.



5 **[License] 상자에 라이센스 활성화 키를 붙여 넣습니다.**

6 **[Verify License]를 클릭합니다.**

7 **[Submit License]를 클릭합니다.**



8 **추가 라이센스가 있다면 [Add New License]를 클릭하고 5 ~ 7단계를 반복합니다.**

부록 마이그레이션 가이드

대부분의 NGFW(Next-Generation Firewall)은 애플리케이션 및 사용자에 대한 액세스 제어를 제공하여 위험을 줄여줍니다. 그러나 공격자는 그 외에 개방된 웹 환경 및 승인된 어플리케이션을 통하여 여전히 공격을 할 수 있기 때문에 보안에 대한 위협 자체가 완전히 사라진 것은 아닙니다. 따라서 보다 뛰어난 보안성을 위해 NGFW은 네트워크 전반에 대한 심층적인 가시성을 제공하고, 위협을 파악하기 위한 지능적인 자동화 기법을 적용하며, 동적 네트워크 환경에 최적화된 보호 기능 제공하고 발 빠르게 공격을 파악하여 대처함으로써 위협을 최소화할 수 있어야 합니다. 시스코 ASA with FirePOWER 서비스는 고객의 소중한 디지털 자산을 보호할 수 있도록 이러한 기능들을 모두 제공합니다.

기능	일반 NGFW	FirePOWER 서비스를 포함한 Cisco ASA
NSS 유출 탐지 및 NGIPS 리더쉽 포지션 보고서	일부 또는 불가	뛰어남
평판 기반의 선처리 방어	불가	뛰어남
지능적 보안 자동화	불가	뛰어남
파일 평판, 파일 궤적, 파일 회귀 분석	불가	뛰어남
AVC(Application Visibility and Control)	가용	뛰어남
AMP 및 NGIPS 단일 장비 통합	제한적	뛰어남
실시간 위협 탐지 기능을 제공하기 위해 보안 인텔리전스로부터 위협 피드가 매일 업데이트	제한적	뛰어남

기존 모델	FW + AVC	FW + AVC + IPS	현재 모델	FW + AVC	FW + AVC + IPS
Cisco ASA 5505	-	-	Cisco ASA 5506-X	250 Mbps	125 Mbps
Cisco ASA 5510	-	-	Cisco ASA 5508-X	450 Mbps	250 Mbps
Cisco ASA 5512	300 Mbps	150 Mbps	Cisco ASA 5516-X	850 Mbps	450 Mbps
Cisco ASA 5515-X	300 Mbps	250 Mbps	Cisco ASA 5516-X	850 Mbps	450 Mbps