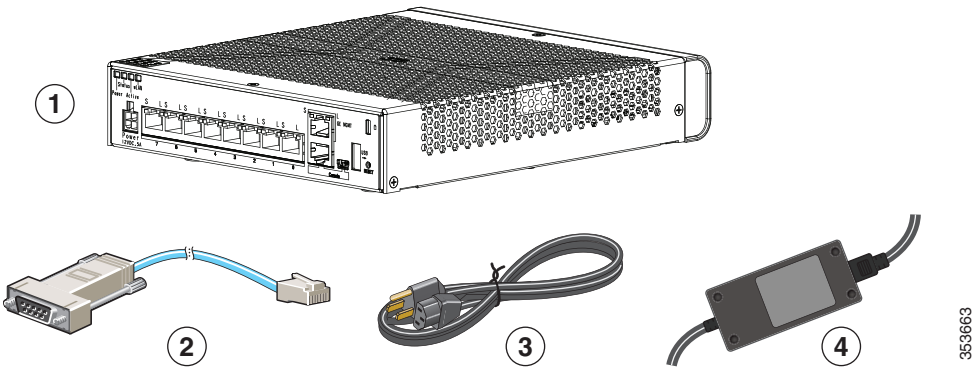
Cisco ASA 5506-X Series 빠른 시작 설명서

최종 업데이트: 2015년 7월 28일

1. 패키지 구성 내용

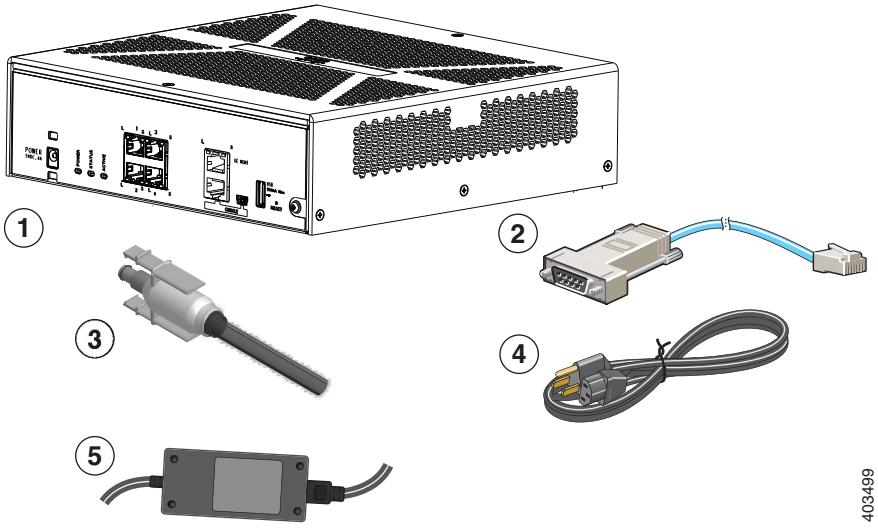
이 섹션에서는 섀시의 패키지 구성 내용을 보여줍니다. 구성 내용은 변경될 수 있으며, 각자의 정확한 구성에는 일부 항목이 추가되거나 제외될 수 있습니다.

ASA 5506-X 및 5506W-X



1	ASA 5506-X 또는 ASA 5506W-X 섀시	2	파란색 콘솔 케이블 및 시리얼 PC 터미널 어댑터 (DB-9 to RJ-45)
3	전원 케이블	4	전원 공급 장치

ASA 5506H-X



1	ASA 5506H-X 섀시	2	파란색 콘솔 케이블 및 시리얼 PC 터미널 어댑터 (DB-9 to RJ-45)
3	전력 코드 보존 잠금장치	4	전원 케이블
5	전원 공급 장치		

2. ASA 5506W-X 무선 액세스 포인트

ASA 5506W-X에는 ASA에 통합된 Cisco Aironet 702i 무선 액세스 포인트가 포함되어 있습니다. 이 액세스 포인트는 GigabitEthernet 1/9 인터페이스를 통해 내부적으로 ASA에 연결됩니다. 모든 **wifi** 클라이언트는 GigabitEthernet 1/9 네트워크에 속합니다. ASA 보안 정책은 **wifi** 네트워크가 다른 인터페이스에서 네트워크에 액세스하는 방법을 결정합니다. 액세스 포인트에는 외부 인터페이스 또는 스위치 포트가 포함되어 있지 않습니다.

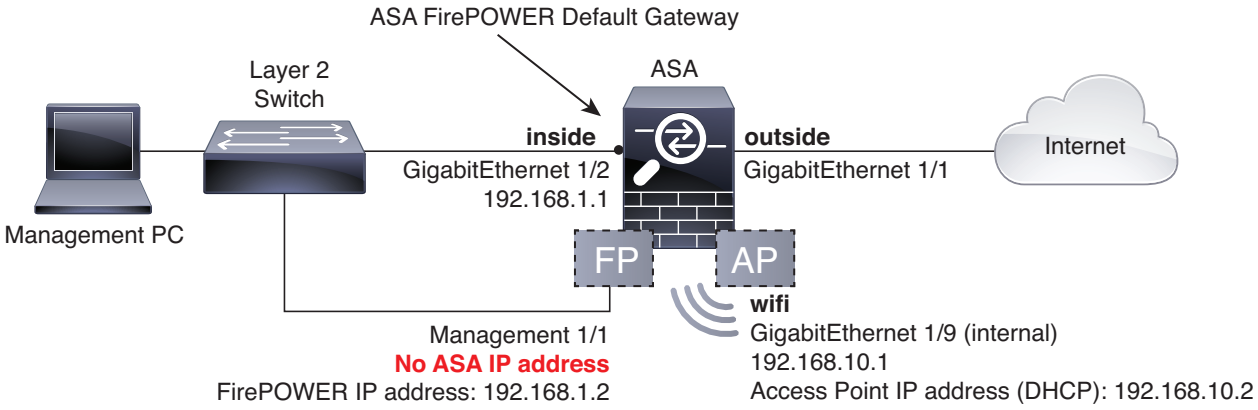
액세스 포인트에는 자동 이미지 또는 Cisco Unified Wireless 이미지가 포함되어 있습니다(주문에 따라). 자동 모드에서는 각 액세스 포인트를 개별적으로 관리할 수 있습니다. 통합 모드에서는 여러 액세스 포인트를 중앙에서 관리할 수 있도록 별도의 Wireless LAN Controller 디바이스를 사용할 수 있습니다.

Wireless LAN Controller에 대한 자세한 내용은 Cisco Wireless LAN Controller Software 설명서를 참조하십시오.

무선 액세스 포인트 하드웨어 및 소프트웨어에 대한 자세한 내용은 Cisco Aironet 700 Series 설명서를 참조하십시오.

3. 네트워크에 ASA 5506-X 구축

다음 그림에서는 ASA 5506-X with the ASA Firepower 모듈 및 내장된 무선 액세스 포인트(ASA 5506W-X)의 권장 네트워크 구축을 보여줍니다.



참고: 구축 시 별도의 내부 스위치를 사용해야 합니다.

기본 컨피그레이션에서는 다음과 같은 동작으로 위의 네트워크 구축을 활성화합니다.

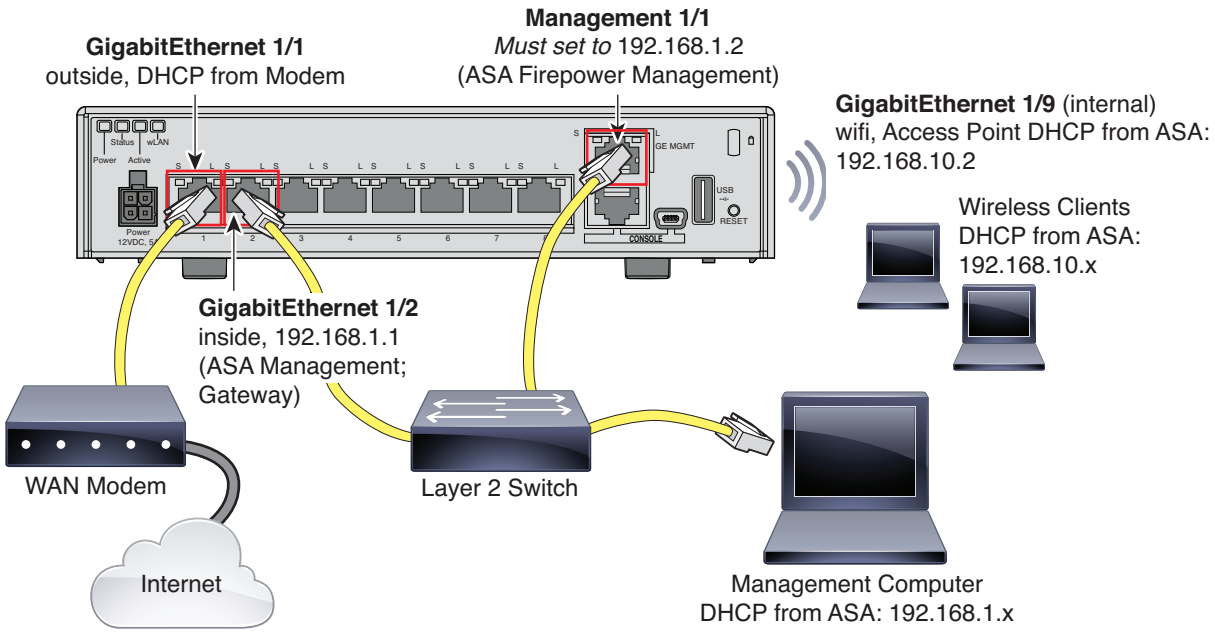
- **내부 --> 외부** 트래픽 흐름
- **DHCP**의 **외부 IP** 주소
- (ASA 5506W-X) **wifi <--> 내부**, **wifi --> 외부** 트래픽 흐름
- **내부** 및 **wifi**에서 클라이언트에 대한 **DHCP**. 액세스 포인트 자체와 모든 클라이언트는 ASA를 DHCP 서버로 사용합니다.
- **Management 1/1**은 **ASA Firepower 모듈**에 속합니다. 인터페이스는 가동 상태이지만, ASA에서는 *구성되어 있지 않습니다*. ASA Firepower 모듈은 이 인터페이스를 사용하여 **ASA 내부 네트워크에 액세스**하고, 내부 인터페이스를 **인터넷에 대한 게이트웨이**로 사용할 수 있습니다.

참고: ASA 컨피그레이션에서는 이 인터페이스의 IP 주소를 구성하지 *마십시오*. Firepower 컨피그레이션에서만 IP 주소를 구성하십시오. 라우팅 관점에서는 **이 인터페이스를 ASA와 완전히 별개의 것으로 간주**해야 합니다.

- **내부** 인터페이스 및 **wifi** 인터페이스에서의 **ASDM 액세스**

참고: 내부 네트워크에 별도의 라우터를 구축하려는 경우 이렇게 하면 관리 및 내부 간에 라우팅할 수 있습니다. 이 경우 컨피그레이션을 적절하게 변경하여 Management 1/1에서 ASA 및 ASA FirePOWER 모듈을 모두 관리할 수 있습니다.

절차



1. 다음을 Layer 2 이더넷 스위치에 연결합니다.
   - GigabitEthernet 1/2 인터페이스(내부)
   - Management 1/1 인터페이스(ASA Firepower 모듈용)
   - 컴퓨터

   참고: 관리 인터페이스는 ASA Firepower 모듈에만 속한 별도의 디바이스처럼 작동하므로 동일한 네트워크에서 내부와 관리를 연결할 수 있습니다.
2. 예를 들면 GigabitEthernet 1/1(외부) 인터페이스를 WAN 디바이스(예: 케이블 모뎀)에 연결합니다.

   참고: 케이블 모뎀이 192.168.1.0/24 또는 192.168.10.0/24에 있는 외부 IP 주소를 제공하는 경우 다른 IP 주소를 사용하도록 ASA 컨피그레이션을 변경해야 합니다.

4. ASA 전원 켜기

1. 전원 케이블을 ASA에 연결하고 전기 콘센트에 꽂습니다.

   전원 케이블이 연결되면 전원이 자동으로 켜집니다. 전원 버튼이 없습니다.
2. ASA 뒷면의 전원 LED를 확인합니다. 장치의 전원이 켜져 있으면 녹색으로 표시됩니다.
3. ASA 뒷면의 상태 LED를 확인합니다. 시스템이 전원 켜기 진단을 통과하면 녹색으로 표시됩니다.

5. 무선 액세스 포인트(ASA 5506W-X) 활성화

ASA 5506W-X 무선 액세스 포인트는 기본적으로 비활성화됩니다. 무선 장치를 활성화하고 SSID 및 보안 설정을 구성할 수 있도록 액세스 포인트 GUI에 연결하십시오.

시작하기 전에

이 절차에서는 기본 컨피그레이션을 사용해야 합니다.

절차

1. 네트워크 내부의 ASA에 연결된 컴퓨터에서 웹 브라우저를 구동합니다.
2. **Address(주소)** 필드에 **http://192.168.10.2**를 입력합니다. 사용자 이름과 비밀번호를 입력하라는 프롬프트가 표시됩니다.

   참고: 액세스 포인트에 도달할 수 없고 ASA가 기본 컨피그레이션 상태이며 다른 네트워크 문제가 발견되지 않으면, 액세스 포인트 기본 컨피그레이션을 복원할 수 있습니다. ASA CLI에 액세스해야 합니다(ASA 콘솔 포트에 연결하거나, ASDM을 사용하여 텔넷 또는 SSH 액세스 구성). ASA CLI에서 **hw-module module wlan recover configuration**을 입력합니다.
3. 사용자 이름 **Cisco** 및 비밀번호 **Cisco**를 입력합니다. 액세스 포인트 GUI가 나타납니다.
4. 왼쪽에서 **Easy Setup(손쉬운 설정) > Network Configuration(네트워크 컨피그레이션)**을 클릭합니다.
5. **Radio Configuration(무선 컨피그레이션)** 영역에서 **Radio 2.4GHz** 및 **Radio 5GHz** 섹션 각각에 대해 다음 매개 변수를 설정하고 각 섹션에서 **Apply(적용)**를 클릭합니다.
   - **SSID**
   - **Broadcast SSID in Beacon**
   - **Universal Admin Mode: Disable**
   - **Security**(개별 선택)
6. 왼쪽에서 **Summary(요약)**를 클릭한 다음 **Network Interfaces(네트워크 인터페이스)**의 기본 페이지에서 2.4GHz 무선에 대한 핫링크를 클릭합니다.
7. **Settings(설정)** 탭을 클릭합니다.
8. **Enable Radio(무선 활성화)** 설정에서 **Enable(활성화)** 라디오 버튼을 클릭하고 페이지 하단에서 **Apply(적용)**를 클릭합니다.
9. 5GHz 무선에 대해서도 반복합니다.
10. 자세한 내용은 다음 설명서를 참조하십시오.
    - Wireless LAN Controller에 대한 자세한 내용은 Cisco Wireless LAN Controller Software 설명서를 참조하십시오.
    - 무선 액세스 포인트 하드웨어 및 소프트웨어에 대한 자세한 내용은 Cisco Aironet 700 Series 설명서를 참조하십시오.

6. ASDM 구동

ASDM을 실행하기 위한 요구 사항은 Cisco.com의 ASDM 릴리스 노트를 참조하십시오.

이 절차에서는 ASDM을 사용하여 ASA Firepower 모듈을 관리하려 한다고 가정합니다. FireSIGHT System을 사용하려면 모듈 CLI에 연결하여 설치 스크립트를 실행해야 합니다. ASA Firepower quick start guide를 참조하십시오.

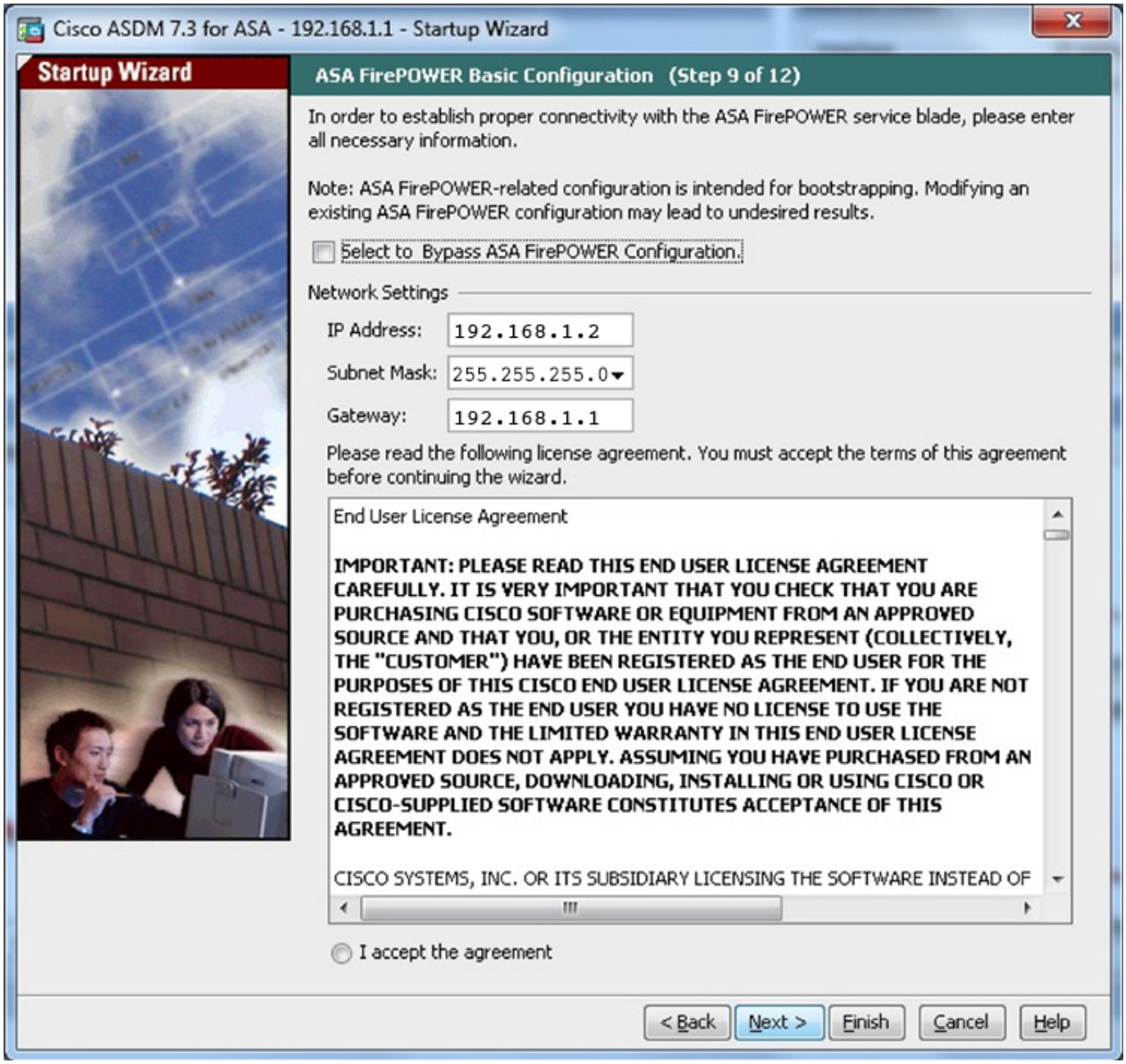
절차

1. ASA에 연결된 컴퓨터에서 웹 브라우저를 구동합니다.
2. Address(주소) 필드에 URL **https://192.168.1.1/admin**을 입력합니다. **Cisco ASDM** 웹 페이지가 나타납니다.

   관리 컴퓨터를 ASA에 무선 클라이언트로서 연결한 경우 **https://192.168.10.1/admin**에서 ASDM에 액세스할 수 있습니다.
3. 사용 가능한 옵션인 **Install ASDM Launcher(ASDM Launcher 설치)**, **Run ASDM(ASDM 실행)** 또는 **Run Startup Wizard(시작 마법사 실행)** 중 하나를 클릭합니다.
4. 선택한 옵션에 따라 ASDM을 구동하기 위한 화면의 지침을 수행합니다. **Cisco ASDM-IDM Launcher**가 나타납니다.

   Install ASDM Launcher(ASDM Launcher 설치)를 클릭하는 경우 Install an Identity Certificate for ASDM에 따라 ASA용 ID 인증서 및 ASA Firepower 모듈용 별도의 인증서를 설치해야 할 수 있습니다.
5. 사용자 이름과 비밀번호 필드를 비워두고 **OK(확인)**를 클릭합니다. 기본 ASDM 창이 나타납니다.
6. 설치된 ASA Firepower 모듈의 IP 주소를 입력하라는 메시지가 표시되면 취소하여 대화 상자를 닫습니다. 먼저 Startup Wizard(시작 마법사)를 사용하여 모듈 IP 주소를 올바른 IP 주소로 설정해야 합니다.

   ASDM은 ASA 백플레인을 통해 ASA Firepower 모듈 IP 주소 설정을 변경할 수 있습니다. 그러나 모듈을 관리하려면 ASDM은 네트워크를 통해 Management 1/1 인터페이스의 모듈(및 해당 새 IP 주소)에 도달할 수 있어야 합니다. 모듈 IP 주소가 내부 네트워크에 있으므로 권장 구축에서는 이 액세스를 허용합니다. IP 주소를 설정한 후 ASDM이 네트워크의 모듈에 도달할 수 없는 경우 오류가 표시됩니다.
7. **Wizards(마법사) > Startup Wizard(시작 마법사)**를 선택합니다.
8. 추가 ASA 설정을 원하는 대로 구성하거나, ASA Firepower Basic Configuration(ASA Firepower 기본 컨피그레이션) 화면에 도달할 때까지 화면을 건너뜁니다.



기본 컨피그레이션으로 작업하려면 다음 값을 설정합니다.

- **IP Address(IP 주소)**–192.168.1.2
- **Subnet Mask(서브넷 마스크)** - 255.255.255.0
- **Gateway(게이트웨이)** - 192.168.1.1

9. **I accept the agreement(동의함)**를 클릭하고, **Next(다음)**를 클릭하거나 **Finish(완료)**를 클릭하여 마법사를 종료합니다.
10. ASDM을 종료한 후 다시 구동합니다. 홈 페이지에 ASA Firepower 탭이 표시됩니다.

7. 다른 ASDM 마법사 및 고급 컨피그레이션 실행

ASDM에는 보안 정책 구성을 위한 여러 마법사가 포함되어 있습니다. 사용 가능한 모든 마법사는 **Wizards(마법사)** 메뉴에서 확인할 수 있습니다.

ASA를 계속 구성하려면 Navigating the Cisco ASA Series Documentation에서 사용 중인 소프트웨어 버전에 대해 사용 가능한 설명서를 참조하십시오.

8. ASA Firepower 모듈 구성

ASDM을 사용하여 모듈 보안 정책을 구성하고 트래픽을 모듈로 전송합니다.

참고: FireSIGHT Management Center를 사용하여 ASA Firepower 모듈을 관리할 수도 있습니다. 자세한 내용은 ASA Firepower Module Quick Start Guide를 참조하십시오.

절차

1. ASDM의 ASA Firepower 페이지를 사용하여 모듈 보안 정책을 구성합니다. 정책 구성 방법에 대해 자세히 알아보려면 어떤 페이지에서든 **Help(도움말)**를 클릭하거나 **Help(도움말) > ASA Firepower Help Topics(도움말 항목)**를 선택할 수 있습니다.
2. 트래픽을 모듈로 전송하려면 **Configuration(컨피그레이션) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)**를 선택합니다.
3. **Add(추가) > Add Service Policy Rule(서비스 정책 규칙 추가)**을 선택합니다.
4. 특정 인터페이스에 정책을 적용할지 아니면 전역 범위에 적용할지 선택하고 **Next(다음)**를 클릭합니다.
5. 트래픽 일치를 구성합니다. 예를 들어, 인바운드 액세스 규칙을 통과한 모든 트래픽이 모듈에 리디렉션되도록 **Any Traffic(모든 트래픽)** 일치를 선택합니다. 또는 포트, ACL(출처 및 대상 기준), 기존 트래픽 클래스에 따라 더 엄격한 기준을 적용할 수도 있습니다. 나머지 옵션은 이 정책에서 그리 유용하지 않습니다. 트래픽 클래스 정의를 완료하고 **Next(다음)**를 클릭합니다.
6. Rule Actions(규칙 작업) 페이지에서 **ASA Firepower Inspection(ASA Firepower 검사)** 탭을 클릭합니다.
7. **Enable ASA Firepower for this traffic flow(이 트래픽 흐름에서 ASA Firepower 활성화)** 확인란을 선택합니다.
8. If ASA Firepower Card Fails(ASA Firepower 카드 실패 시) 영역에서 다음 중 하나를 클릭합니다.
   - **Permit traffic(트래픽 허용)** - 모듈을 사용할 수 없는 경우 검사 없이 모든 트래픽을 허용하도록 ASA를 설정합니다.
   - **Close traffic(트래픽 차단)** - 모듈을 사용할 수 없는 경우 모든 트래픽을 차단하도록 ASA를 설정합니다.
9. (선택 사항) 트래픽의 읽기 전용 사본을 모듈에 보내려면(패시브 모드) **Monitor-only(모니터링 전용)**를 선택합니다.
10. **Finish(완료)**를 클릭하고 **Apply(적용)**를 클릭합니다.

    필요에 따라 이 절차를 반복하여 추가 트래픽 흐름을 구성합니다.

9. 다음으로 살펴볼 내용

- ASA Firepower 모듈 및 ASA 작동에 대한 자세한 내용은 ASA/ASDM 방화벽 컨피그레이션 가이드의 "ASA Firepower 모듈" 장 또는 ASDM 온라인 도움말을 참조하십시오. 모든 ASA/ASDM 설명서에 대한 링크는 Navigating the Cisco ASA Series Documentation에 있습니다.
- ASA Firepower 컨피그레이션에 대한 자세한 내용은 온라인 도움말, ASA Firepower Module User Guide 또는 FireSIGHT System User Guide를 참조하십시오.