빠른 시작 안내서

Cisco ASA FirePOWER 모듈

개정: 2014년 10월 1일

1 ASA FirePOWER 모듈

ASA FirePOWER 모듈은 NGIPS(Next-Generation Intrusion Prevention System, 차세대 침입 방지 시스템), AVC(Application Visibility and Control), URL 필터링, AMP(Advanced Malware Protection)와 같은 차세대 방화벽 서비스를 제공합니다. 단일 또는 다중 컨텍스트 모드에서 사용할 수 있으며, 라우팅 또는 투명 모드에서 사용할 수 있습니다.

이 모듈은 ASA SFR이라고도 합니다.

초기 구성 및 트러블슈팅을 위한 기본 CLI(Command line interface)가 있지만, 디바이스의 보안 정책은 FireSIGHT Management Center(이)라는 별도의 애플리케이션을 사용하여 구성합니다. 이는 별도의 FireSIGHT Management Center 어플라이언스에 호스팅하거나 가상 어플라이언스의 형태로 VMware 서버에 호스팅할 수 있습니다. FireSIGHT Management Center는 Defense Center라고도 합니다.

ASA에서 ASA FirePOWER 모듈을 사용하는 방법

ASA FirePOWER 모듈은 ASA와는 별개의 애플리케이션을 실행합니다. 이 모듈은 하드웨어 모듈(ASA 5585-X만 해당)이거나 소프트웨어 모듈(기타 모든 모델)입니다. 하드웨어 모듈일 경우 별도의 관리 및 콘솔 포트와 더불어 추가 데이터 인터페이스가 포함되는데 모듈 자체가 아닌 ASA에서 사용됩니다.

패시브("모니터 전용") 또는 인라인 구축 모드로 디바이스를 구성할 수 있습니다.

- 패시브 구축에서는 트래픽의 복사본이 디바이스에 보내지지만, ASA에 반환되지 않습니다. 패시브 모드에서는 네트워크에 영향을 주지 않고 디바이스가 트래픽을 어떻게 처리할지 확인할 수 있으며 트래픽의 내용을 평가할 수 있습니다.
- 인라인 구축의 경우, 실제 트래픽이 디바이스에 보내지며 트래픽 상태가 디바이스의 정책에 의해 영향을 받습니다. 불필요한 트래픽을 제거하고 정책에 따라 다른 조치를 취하고 나면, 트래픽이 추가적인 처리와 전송이 가능하도록 ASA로 돌아옵니다.

다음 섹션에서는 이러한 모드에 대해 자세히 설명합니다.

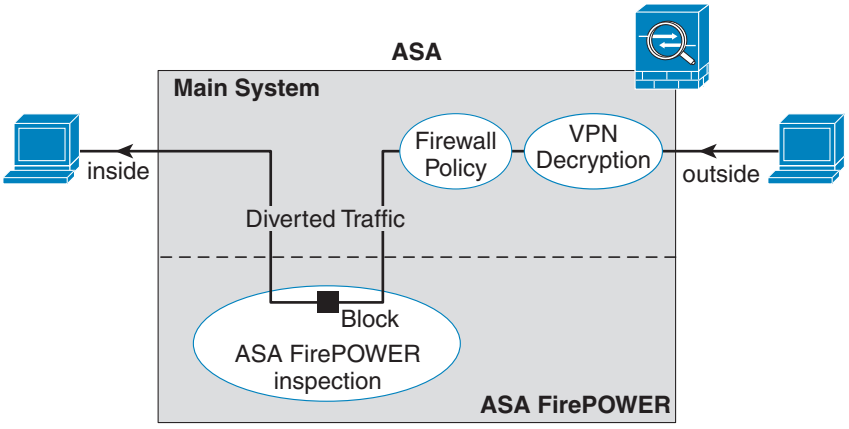
ASA FirePOWER 인라인 모드

인라인 모드에서 트래픽은 ASA FirePOWER 모듈에 전달되기 전에 방화벽 검사를 거칩니다. ASA FirePOWER 검사 대상 트래픽을 ASA에서 식별할 때 트래픽은 다음과 같이 ASA와 이 모듈을 지납니다.

1. 트래픽이 ASA에 들어갑니다.
2. 수신 VPN 트래픽이 해독됩니다.
3. 방화벽 정책이 적용됩니다.
4. 트래픽이 ASA FirePOWER 모듈에 보내집니다.
5. ASA FirePOWER 모듈이 트래픽에 보안 정책을 적용하고 알맞은 조치를 취합니다.
6. 유효 트래픽이 다시 ASA로 보내집니다. ASA FirePOWER 모듈이 보안 정책에 따라 일부 트래픽을 차단할 수 있으며, 그 트래픽은 전달되지 않습니다.
7. 발신 VPN 트래픽이 암호화됩니다.
8. 트래픽이 ASA를 떠납니다.

다음 그림은 인라인 모드에서 ASA FirePOWER 모듈을 사용할 때의 트래픽 흐름을 보여줍니다. 예시에서 볼 수 있듯이, 특정 애플리케이션에 허용되지 않는 트래픽을 모듈이 차단합니다. 나머지 모든 트래픽은 ASA를 통해 전달됩니다.

그림 1 ASA의 ASA FirePOWER 모듈 트래픽 흐름



참고 두 ASA 인터페이스의 호스트끼리 연결되었고 그 인터페이스 중 하나에서만 ASA FirePOWER 서비스 정책이 구성된 경우, 이 호스트 간의 모든 트래픽이 ASA FirePOWER 모듈에 보내집니다. ASA FirePOWER 인터페이스가 아닌 인터페이스에서 시작한 트래픽도 마찬가지입니다(양방향 기능).

ASA FirePOWER 패시브(모니터 전용) 모드

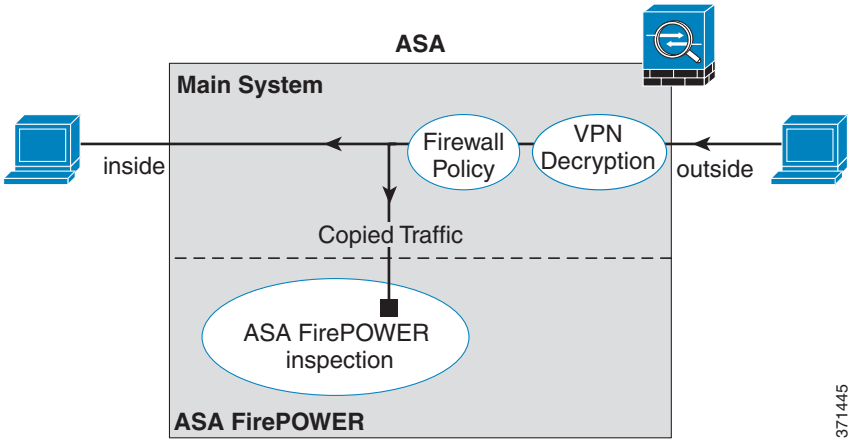
모니터 전용 모드의 트래픽 흐름은 인라인 모드와 동일합니다. 유일한 차이점은 ASA FirePOWER 모듈에서 다시 ASA에 트래픽을 전달하지 않는다는 것입니다. 그 대신 모듈은 트래픽에 보안 정책을 적용하고, 만약 인라인 모드였다면 어떻게 되었을지 보여줍니다. 이를테면 트래픽이 이벤트에서 "폐기되었을 것"이라고 표시합니다. 이 정보를 트래픽 분석에 활용하고 인라인 모드의 적합성 여부를 판단할 수 있습니다.

패시브 모드를 구성하려면 트래픽을 모듈에 리디렉션하는 모니터 전용 표시를 서비스 정책에 포함합니다.

참고 ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수는 없습니다. 오로지 하나의 보안 정책 유형만 허용됩니다. 다중 컨텍스트 모드의 경우, 일부 컨텍스트에 대해 모니터 전용 모드를 구성할 수 없고 또 다른 컨텍스트에서는 일반 인라인 모드를 구성할 수 없습니다.

다음 그림은 패시브 모드일 때의 트래픽 흐름을 보여줍니다.

그림 2 ASA FirePOWER 패시브 모니터 전용 모드



ASA FirePOWER 관리 액세스

ASA FirePOWER 모듈 관리를 위한 서로 다른 2가지 액세스 계층이 있습니다. 초기 구성(및 후속 문제 해결)과 정책 관리입니다.

초기 구성에서는 ASA FirePOWER 모듈에서 CLI를 사용해야 합니다. 다음 방법으로 CLI에 액세스할 수 있습니다.

- ASA 5585-X(하드웨어 모듈):
  - ASA FirePOWER 콘솔 포트 - 모듈의 콘솔 포트는 별도의 외부 콘솔 포트입니다.
  - ASA FirePOWER Management 1/0 인터페이스(SSH 사용)—기본 IP 주소(192.168.45.45/24)에 연결하거나 ASDM을 사용하여 관리 IP 주소를 변경한 다음 SSH를 사용하여 연결할 수 있습니다. 모듈의 관리 인터페이스는 별도의 외부 기가비트 이더넷 인터페이스입니다.

참고 **세션** 명령을 사용하여 ASA 백플레인을 통해 ASA FirePOWER 하드웨어 모듈 CLI에 액세스할 수 없습니다.

- 기타 모든 모델(소프트웨어 모듈):
  - 백플레인을 통한 ASA 세션— CLI를 통해 ASA에 액세스 가능한 경우 모듈에 대한 세션을 시작하고 모듈 CLI에 액세스할 수 있습니다.
  - ASA FirePOWER Management 0/0 인터페이스(SSH 사용)—기본 IP 주소(192.168.45.45/24)에 연결하거나 ASDM을 사용하여 관리 IP 주소를 변경한 다음 SSH를 사용하여 연결할 수 있습니다. ASA FirePOWER 관리 인터페이스는 ASA와 관리 인터페이스를 공유합니다. ASA 및 ASA FirePOWER 모듈을 위해 별도의 MAC 주소와 IP 주소가 지원됩니다. ASA FirePOWER IP 주소의 구성을 ASA FirePOWER 운영 체제에서 (CLI 또는 ASDM을 사용하여) 수행해야 합니다. 그러나 물리적 특성(예: 인터페이스 활성화)은 ASA에서 구성됩니다. ASA 인터페이스 구성(즉 인터페이스 이름)을 제거하여 이 인터페이스를 ASA FirePOWER 전용 인터페이스로 만들 수 있습니다. 이 인터페이스는 관리 전용입니다.

초기 구성을 수행한 다음 FireSIGHT Management Center을 사용하여 ASA FirePOWER 보안 정책을 구성합니다. 그런 다음 CLI, ASDM 또는 Cisco Security Manager를 사용하여 ASA FirePOWER 모듈에 트래픽을 보내기 위한 ASA 정책을 구성합니다.

ASA 기능과의 호환성

ASA에는 HTTP 검사를 비롯한 여러 고급 애플리케이션 검사 기능이 포함되어 있습니다. 그러나 ASA FirePOWER 모듈은 ASA보다 다양한 고급 HTTP 검사 기능을 제공하고 다른 애플리케이션을 위한 추가 기능(예: 애플리케이션 사용량 모니터링 및 제어)도 제공합니다.

ASA FirePOWER 모듈 기능을 십분 활용하려면 ASA FirePOWER 모듈에 보내는 트래픽에 대한 다음 지침을 참조하십시오.

- HTTP 트래픽에 대해서는 ASA 검사를 구성하지 마십시오.
- Cloud Web Security(ScanSafe) 검사를 구성하지 마십시오. 동일 트래픽에 대해 ASA FirePOWER 검사와 Cloud Web Security 검사를 모두 구성할 경우 ASA에서는 ASA FirePOWER 검사만 수행합니다.
- 기본 검사를 비롯하여 ASA의 다른 애플리케이션 검사는 ASA FirePOWER 모듈에서 지원됩니다.
- MUS(Mobile User Security) 서버를 사용하지 마십시오. ASA FirePOWER 모듈과 함께 사용할 수 없습니다.

2 ASA FirePOWER를 위한 지침

장애 조치 지침

직접적으로 장애 조치를 지원하지 않습니다. ASA 장애 조치 상황에서는 기존의 모든 ASA FirePOWER 흐름이 새로운 ASA로 전송됩니다. 새로운 ASA의 ASA FirePOWER 모듈이 그 시점부터 트래픽 검사를 시작합니다. 기존 검사 상태는 전송되지 않습니다.

고가용성 ASA 페어의 ASA FirePOWER 모듈에서 일관된 정책을 유지하여(FireSIGHT Management Center 사용) 일관성 있는 장애 조치 동작을 보장해야 합니다.

ASA 클러스터링 지침

직접적으로 클러스터링을 지원하지 않지만, 클러스터에서 이 모듈을 사용할 수 있습니다. 클러스터의 ASA FirePOWER 모듈에서 FireSIGHT Management Center를 사용하여 일관된 정책을 유지해야 합니다. 클러스터에 속한 디바이스에 대해 다른 ASA-인터페이스 기반 영역 정의를 사용하지 마십시오.

모델 지침

- 5512-X부터 5585-X까지 최소 소프트웨어 요구 사항은 ASA Software 9.2(2.4) 및 ASA FirePOWER 5.3.1입니다.
- 다음 모델에서 지원됩니다. 이 모듈은 ASA 5585-X에서는 하드웨어 모듈이지만, 나머지 모든 모델에서는 소프트웨어 모듈입니다. 자세한 내용은 *Cisco ASA 호환성 매트릭스* (http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html)를 참조하십시오.
  - 5585-X(하드웨어 모듈)
  - 5555-X
  - 5545-X
  - 5515-X
  - 5512-X
- 5512-X부터 ASA 5555-X까지는 Cisco SSD(solid state drive)를 설치해야 합니다. 자세한 내용은 ASA 5500-X 하드웨어 설명서를 참조하십시오.

추가 지침 및 제한

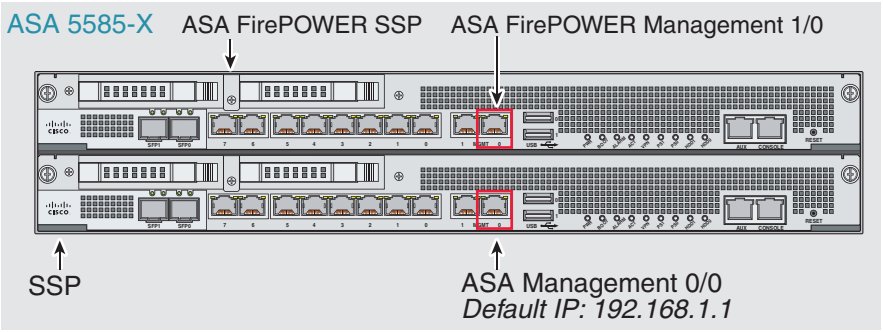
- ASA 기능과의 호환성, 4페이지 를 참조하십시오.
- 하드웨어 모듈에 설치된 소프트웨어 유형을 변경할 수 없습니다. ASA FirePOWER 모듈을 구매한 경우 나중에 여기에 다른 소프트웨어를 설치할 수 없습니다.
- ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수는 없습니다. 오로지 하나의 보안 정책 유형만 허용됩니다. 다중 컨텍스트 모드의 경우, 일부 컨텍스트에 대해 모니터 전용 모드를 구성할 수 없고 또 다른 컨텍스트에서는 일반 인라인 모드를 구성할 수 없습니다.

3 ASA FirePOWER 관리 인터페이스 연결

ASA FirePOWER 관리 인터페이스는 ASA FirePOWER 모듈에 대한 관리 액세스를 제공할 뿐 아니라 HTTP 프록시 서버 또는 DNS 서버에 대한 액세스 그리고 서명 업데이트 등을 위해 인터넷 액세스도 제공해야 합니다. 이 섹션에서는 권장 네트워크 구성에 대해 설명합니다. 실제 네트워크는 다를 수 있습니다.

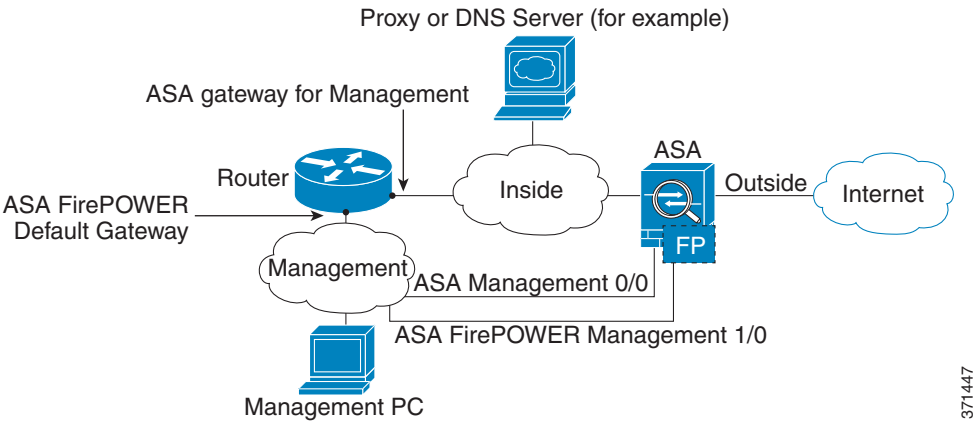
ASA 5585-X(하드웨어 모듈)

ASA FirePOWER 모듈은 ASA와는 별개의 관리 및 콘솔 인터페이스를 갖추고 있습니다. 초기 설정에서는 SSH를 통해 기본 IP 주소를 사용하여 ASA FirePOWER Management 1/0 인터페이스에 연결할 수 있습니다. 기본 IP 주소를 사용할 수 없는 경우, 콘솔 포트 또는 ASDM을 통해 관리 IP 주소를 변경한 다음 SSH를 사용할 수 있습니다. (ASA FirePOWER 관리 IP 주소 변경, 11페이지 를 참조하십시오.)



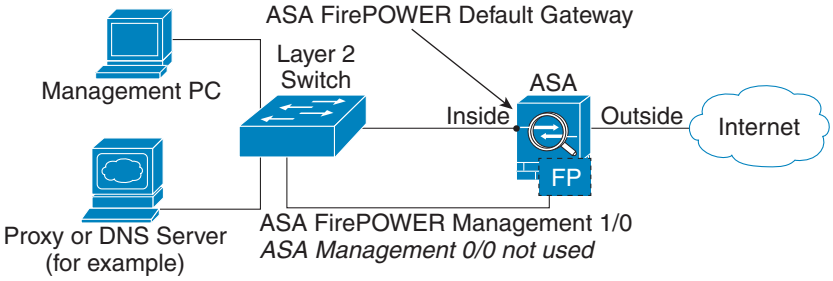
내부 라우터가 있는 경우

내부 라우터가 있다면 인터넷 액세스를 위한 관리 네트워크(ASA Management 0/0 및 ASA FirePOWER Management 1/0 인터페이스가 모두 포함될 수 있음)와 ASA 내부 네트워크 간 라우팅이 가능합니다. 내부 라우터를 통해 관리 네트워크에 접속할 수 있도록 반드시 ASA에 경로를 추가해야 합니다.



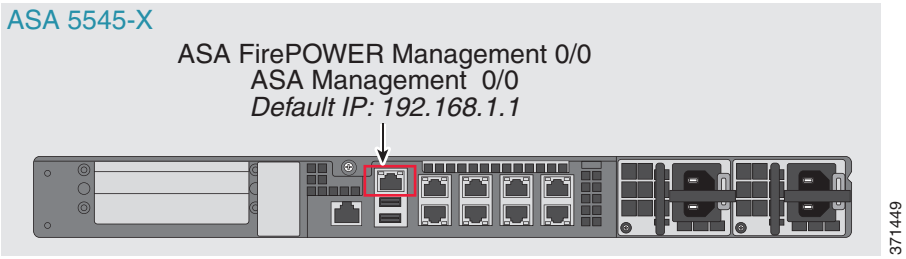
내부 라우터가 없는 경우

내부 네트워크가 하나뿐이라면 별도의 관리 네트워크를 둘 수 없습니다. 네트워크 간 라우팅에 내부 라우터가 필요하기 때문입니다. 그러한 경우 Management 0/0 인터페이스 대신 내부 인터페이스에서 ASA를 관리할 수 있습니다. ASA FirePOWER 모듈은 ASA와는 별개의 디바이스이므로 ASA FirePOWER Management 1/0 주소가 내부 인터페이스와 동일한 네트워크에 있도록 구성할 수 있습니다.



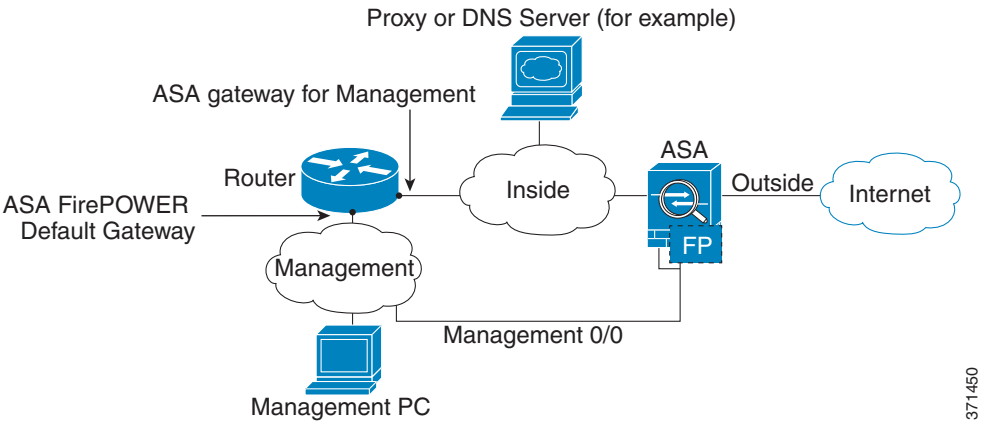
ASA 5512-X ~ ASA 5555-X(소프트웨어 모듈)

이 모델은 ASA FirePOWER 모듈을 소프트웨어 모듈로 실행하며, ASA FirePOWER 관리 인터페이스는 Management 0/0 인터페이스를 ASA. 초기 설정에서 SSH를 통해 ASA FirePOWER 기본 IP 주소에 연결할 수 있습니다. 기본 IP 주소를 사용할 수 없는 경우, 백플레인을 통해 ASA FirePOWER와의 세션을 시작하거나 ASDM을 사용하여 관리 IP 주소를 변경한 다음 SSH를 사용할 수 있습니다.



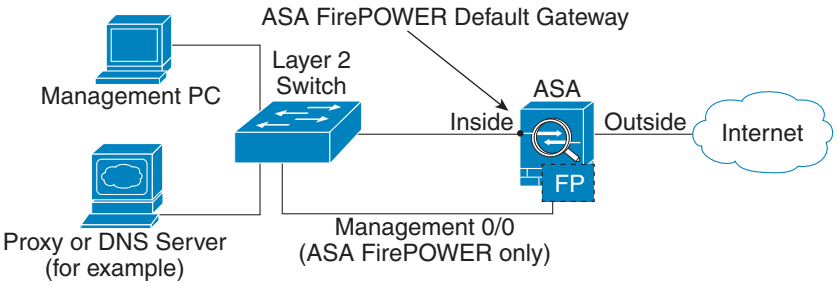
내부 라우터가 있는 경우

내부 라우터가 있으면, 인터넷 연결을 위한 Management 0/0 네트워크(ASA 및 ASA FirePOWER 관리 IP 주소 모두 포함)와 내부 네트워크 간 라우팅이 가능합니다. 내부 라우터를 통해 관리 네트워크에 접속할 수 있도록 반드시 ASA에 경로를 추가해야 합니다.



내부 라우터가 없는 경우

내부 네트워크가 하나뿐이라면 별도의 관리 네트워크를 둘 수 없습니다. 그러한 경우 Management 0/0 인터페이스 대신 내부 인터페이스에서 ASA를 관리할 수 있습니다. ASA에서 구성된 이름을 Management 0/0 인터페이스에서 제거하더라도 그 인터페이스의 ASA FirePOWER IP 주소는 여전히 구성 가능합니다. ASA FirePOWER 모듈은 ASA와는 별개의 디바이스이므로 ASA FirePOWER 관리 주소가 내부 인터페이스와 동일한 네트워크에 있도록 구성*할 수* 있습니다.



참고 Management 0/0에 대해 ASA에서 구성된 이름을 제거해야 합니다. ASA에서 구성되었다면 ASA FirePOWER 주소가 ASA와 동일한 네트워크에 있어야 합니다. 즉 다른 ASA 인터페이스에서 이미 구성된 모든 네트워크가 제외됩니다. 이름이 구성되지 않은 경우 ASA FirePOWER 주소는 ASA 내부 네트워크를 비롯한 어떤 네트워크의 주소도 가능합니다.

4 ASA에서 ASDM 시작

기본 ASA 구성을 통해 기본 관리 IP 주소(192.168.1.1)에 연결할 수 있습니다. 네트워크에 따라 ASDM 액세스를 위해 ASA 관리 IP 주소를 변경하거나 추가 ASA 인터페이스를 구성해야 하는 경우도 있습니다(ASA FirePOWER 관리 인터페이스 연결, 5페이지 참조).

ASA 5512-X부터 ASA 5555-X까지는 별도의 관리 네트워크가 없을 경우(내부 라우터가 없는 경우, 7페이지 참조), 관리를 위한 내부 인터페이스를 구성*할 뿐 아니라* Management 0/0 인터페이스에서 그 이름을 제거해야 합니다. 인터페이스 및 관리 설정을 변경하려면 ASA 구성 설명서를 참조하십시오.

1단계 관리 PC에서 웹 브라우저를 시작합니다.

2단계 Address(주소) 필드에 **https://***ASA_IP_address***/admin**이라는 URL을 입력합니다. 기본 ASA 관리 IP 주소는 192.168.1.1입니다.

3단계 **Run ASDM(ASDM 실행)**을 클릭하여 Java Web Start 애플리케이션을 실행합니다. 또는 이 페이지에서 ASDM 시작 프로그램을 다운로드할 수 있습니다.

4단계 나타나는 대화 상자의 안내에 따라 인증서를 수락합니다. Cisco ASDM-IDM Launcher 대화 상자가 나타납니다.

5단계 사용자 이름과 비밀번호 필드를 비워 둔 채로 **OK(확인)**를 클릭합니다. 기본 ASDM 창이 나타납니다.

5 ASA FirePOWER 소프트웨어 모듈 설치 또는 다시 이미징

ASA와 ASA FirePOWER 모듈을 구매한 경우 모듈 소프트웨어 및 필요한 SSD가 즉시 구성 가능한 상태로 미리 설치되어 있습니다. ASA FirePOWER 소프트웨어 모듈을 기존 ASA에 추가하려는 경우 또는 SSD를 교체해야 하는 경우, 다음 절차에 따라 ASA FirePOWER 부트 소프트웨어를 설치하고 SSD를 분할하고 시스템 소프트웨어를 설치해야 합니다.

모듈을 다시 이미징하는 절차도 동일하지만, 먼저 ASA FirePOWER 모듈을 제거해야 합니다. SSD를 교체할 경우 시스템을 다시 이미징합니다.

실제로 SSD를 설치하는 방법에 대한 자세한 내용은 ASA 하드웨어 설명서를 참조하십시오.

사전 요구 사항

- 플래시(disk0)에서 3GB + 부트 소프트웨어 크기만큼의 공간이 있어야 합니다.
- 다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.
- 실행 중인 다른 소프트웨어 모듈은 모두 종료해야 합니다. 이 디바이스는 한 번에 하나의 소프트웨어 모듈을 실행할 수 있습니다. ASA CLI에서 이 작업을 해야 합니다. 예를 들어, 다음 명령은 IPS 소프트웨어 모듈을 종료하고 제거한 다음 ASA를 다시 로드합니다. CX 모듈을 제거하는 명령도 동일하지만, **cxsc** 키워드를 **ips** 대신 사용합니다.

  ```
  호스트 이름 # sw-module module ips shutdown
  호스트 이름 # sw-module module ips uninstall
  호스트 이름 # reload
  ```

- IPS 또는 CX 모듈에 트래픽을 리디렉션하는 서비스 정책이 활성 상태라면 그 정책을 제거해야 합니다. 예를 들어, 글로벌 정책이라면 **no service-policy** *ips_policy* **global**을 사용할 수 있습니다. 서비스 정책에 포함된 다른 규칙을 유지해야 하는 경우, 해당 정책 맵에서 또는 (리디렉션이 클래스에 대한 유일한 작업이라면) 전체 트래픽 클래스에서 리디렉션 명령을 제거하면 됩니다. CLI 또는 ASDM을 사용하여 정책을 제거할 수 있습니다.
- 모듈을 다시 이미징할 때 동일한 종료 및 제거 명령을 사용하여 기존 이미지를 제거합니다. 이를테면 **sw-module module sfr uninstall**을 실행합니다.
- Cisco.com에서 ASA FirePOWER 부트 이미지와 시스템 소프트웨어 패키지를 다운로드합니다.

절차

1단계 디바이스에 부트 이미지를 다운로드합니다. 시스템 소프트웨어를 전송하지 마십시오. 나중에 SSD에 다운로드됩니다. 다음 옵션이 있습니다.

- ASDM—먼저 부트 이미지를 워크스테이션에 다운로드하거나 FTP, TFTP, HTTP, HTTPS, SMB 또는 SCP 서버에 저장합니다. 그런 다음 ASDM에서 **Tools(툴) > File Management(파일 관리)**를 선택하고 알맞은 **파일 전송** 명령(**로컬 PC와 플래시 간** 또는 **원격 서버와 플래시 간**)을 선택합니다. ASA의 disk0에 부트 소프트웨어를 전송합니다.
- ASA CLI—먼저 TFTP, FTP, HTTP 또는 HTTPS 서버에 부트 이미지를 저장한 다음 **copy** 명령을 사용하여 플래시에 다운로드합니다. 다음 예에서는 TFTP를 사용합니다. <TFTP Server>에 해당 서버의 IP 주소 또는 호스트 이름을 입력합니다.

  ```
  ciscoasa# copy tftp://<TFTP SERVER>/asasfr-5500x-boot-5.3.1-58.img
  disk0:/asasfr-5500x-boot-5.3.1-58.img
  ```

2단계 Cisco.com에서 제공하는 ASA FirePOWER 시스템 소프트웨어를 ASA FirePOWER 관리 인터페이스에서 액세스 가능한 HTTP, HTTPS 또는 FTP 서버에 다운로드합니다.

3단계 다음 명령을 입력하여 ASA FirePOWER 모듈 부트 이미지 위치를 ASA disk0에서 설정합니다.

```
호스트 이름 # sw-module module sfr recover configure image disk0:file_path
```

"ERROR: Another service (cxsc) is running, only one service is allowed to run at any time(오류: 다른 서비스(cxsc)가 실행 중입니다. 한 번에 하나의 서비스만 실행할 수 있습니다)"과 같은 메시지가 표시된다면 다른 소프트웨어 모듈이 이미 구성된 것입니다. 그 모듈을 종료하고 제거해야 위 섹션에서 설명한 대로 새 모듈을 설치할 수 있습니다.

예:

```
호스트 이름 # sw-module module sfr recover configure image
disk0:asasfr-5500x-boot-5.3.1-58.img
```

4단계 다음 명령을 입력하여 ASA FirePOWER 부트 이미지를 로드합니다.

```
호스트 이름 # sw-module module sfr recover boot
```

5단계 ASA FirePOWER 모듈이 부팅되는 동안 약 5분 ~ 15분 기다렸다가 이제 실행 중인 ASA FirePOWER 부트 이미지와의 콘솔 세션을 엽니다. 세션을 열고 Enter 키를 눌러야 로그인 프롬프트가 표시되는 경우도 있습니다. 기본 사용자 이름은 **admin**, 기본 비밀번호는 **Admin123**입니다.

```
호스트 이름 # session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

모듈 부트가 완료되지 않을 경우 **session** 명령이 실패하고 ttyS1을 통해 연결할 수 없다는 메시지가 표시됩니다. 기다렸다가 다시 해보십시오.

6단계 **setup** 명령을 사용하여 시스템 소프트웨어 패키지를 설치할 수 있도록 시스템을 구성합니다.

```
asasfr-boot> setup


                Welcome to SFR Setup
                 [hit Ctrl-C to abort]
               Default values are inside []
```

다음 값을 입력하라는 메시지가 표시됩니다. 관리 주소와 게이트웨이 및 DNS 정보는 구성해야 할 핵심 설정입니다.

- 호스트 이름—공백 없이 최대 65자의 영숫자. 하이픈은 사용 가능합니다.
- 네트워크 주소—정적 IPv4 또는 IPv6 주소를 설정하거나 DHCP(IPv4) 또는 IPv6 무상태(stateless) 자동 구성을 사용할 수 있습니다.
- DNS 정보—하나 이상의 DNS 서버를 식별해야 하며, 도메인 이름을 설정하고 도메인을 검색할 수도 있습니다.
- NTP 정보—시스템 시간 설정을 위해 NTP를 활성화하고 NTP 서버를 구성할 수 있습니다.

7단계 **system install** 명령을 사용하여 시스템 소프트웨어 이미지를 설치합니다.

system install [**noconfirm**] *url*

확인 메시지에 응답하지 않으려면 **noconfirm** 옵션을 포함합니다. HTTP, HTTPS 또는 FTP URL을 사용합니다. 사용자 이름과 비밀번호가 필요할 경우 이를 입력하라는 메시지가 나타납니다.

설치가 완료되면 시스템이 다시 부팅됩니다. 애플리케이션 구성 요소가 설치되고 ASA FirePOWER 서비스가 시작할 때까지 10분가량 기다립니다. **show module sfr** 출력에서 모든 프로세스가 Up으로 표시되어야 합니다.

예를 들면 다음과 같습니다.

```
asasfr-boot> system install http://asasfr-sys-5.3.1-44.pkg
Verifying
Downloading
Extracting
Package Detail
        Description:                   Cisco ASA-FirePOWER 5.3.1-44 System Install
        Requires reboot:               Yes

Do you want to continue with upgrade? [y]: y
Warning: Please do not interrupt the process or turn off the system.
Doing so might leave system in unusable state.

Upgrading
Starting upgrade process ...
Populating new system image

Reboot is required to complete the upgrade. Press 'Enter' to reboot the system.
(press Enter)
Broadcast message from root (ttyS1) (Mon Feb 17 19:28:38 2014):

The system is going down for reboot NOW!
Console session with module sfr terminated.
```

8단계 ASA FirePOWER 모듈에 대한 세션을 엽니다. 전 기능 모듈로 로그인했으므로 다른 로그인 프롬프트가 표시될 것입니다.

```
asa3# session sfr
Opening command session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Sourcefire ASA5555 v5.3.1 (build 44)
Sourcefire3D login:
```

9단계 사용자 이름 **admin** 및 비밀번호 **Sourcefire**로 로그인합니다.

10단계 프롬프트에 따라 시스템 구성을 완료합니다.

먼저 EULA(최종 사용자 라이센스 계약)를 읽고 동의해야 합니다. 그런 다음 프롬프트에 따라 admin 비밀번호를 변경하고 관리 주소 및 NDS 설정을 구성합니다. IPv4 및 IPv6 관리 주소 모두 구성할 수 있습니다. 예를 들면 다음과 같습니다.

```
System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat 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]: 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]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)

This sensor must be managed by a Defense Center.  A unique alphanumeric
registration key is always required.  In most cases, to register a sensor
to a Defense 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 Defense 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 Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

11단계 **configure manager add** 명령을 사용하여 이 디바이스를 구성할 FireSIGHT Management Center 어플라이언스를 식별합니다.

등록 키가 제공되는데, 이는 FireSIGHT Management Center에서 인벤토리에 디바이스를 추가할 때 사용합니다. 다음 예는 간단한 사례를 보여줍니다. NAT 경계가 있을 경우 명령이 달라집니다. FireSIGHT Management Center에 ASA FirePOWER추가, 12페이지 를 참조하십시오.

```
> configure manager add 10.89.133.202 123456
Manager successfully configured.
```

12단계 브라우저에서 HTTPS 연결을 통해 FireSIGHT Management Center에 로그인합니다. 위에서 입력한 호스트 이름 또는 주소를 사용합니다. 예를 들면, https://DC.example.com으로 연결합니다.

디바이스 관리(**Devices(디바이스) > Device Management(디바이스 관리)**) 페이지를 사용하여 디바이스를 추가합니다. 자세한 내용은 온라인 도움말 또는 *FireSIGHT System 사용자 설명서*의 디바이스 관리(Managing Devices) 장을 참조하십시오.

팁 FireSIGHT Management Center를 통해 NTP 및 시간 설정도 구성할 수 있습니다. **System(시스템) > Local(로컬) > System Policy(시스템 정책)** 페이지에서 로컬 정책을 수정할 때 Time Synchronization(시간 동기화) 설정을 사용합니다.

6 ASA FirePOWER 관리 IP 주소 변경

기본 관리 IP 주소를 사용할 수 없는 경우 ASA에서 관리 IP 주소를 설정하면 됩니다. 관리 IP 주소를 설정한 다음 SSH를 통해 ASA FirePOWER 모듈에 액세스하여 추가 설정을 수행할 수 있습니다.

이미 (ASA FirePOWER CLI에서 기본 ASA FirePOWER 설정 구성, 11페이지 의 설명대로) 초기 시스템 설정에서 ASA FirePOWER CLI를 통해 관리 주소를 구성했다면, ASA CLI 또는 ASDM을 통해 구성할 필요 없습니다.

참고 소프트웨어 모듈의 경우 ASA FirePOWER CLI에 액세스하여 ASA CLI에서 세션을 시작하는 방법으로 설정을 수행할 수 있습니다. 그리고 과정에서 ASA FirePOWER 관리 IP 주소를 설정할 수 있습니다. 하드웨어 모듈은 콘솔 포트를 통해 초기 설정을 완료할 수 있습니다.

다중 컨텍스트 모드의 경우 시스템 실행 공간에서 이 절차를 수행합니다.

1단계 ASDM에서 **Wizards(마법사) > Startup Wizard(시작 마법사)**를 선택합니다.

2단계 초기 화면에서 **Next(다음)**를 클릭하여 ASA FirePOWER Basic Configuration(기본 구성) 화면까지 진행합니다.

3단계 새 관리 IP 주소, 서브넷 마스크, 기본 게이트웨이를 입력합니다.

EULA에도 동의해야 합니다.

4단계 **Finish(완료)**를 클릭하여 나머지 화면을 건너뛰거나 **Next(다음)**를 클릭하여 나머지 화면을 거쳐 마법사를 완료합니다.

7 ASA FirePOWER CLI에서 기본 ASA FirePOWER 설정 구성

보안 정책을 구성하기에 앞서 ASA FirePOWER 모듈에서 기본 네트워크 설정과 기타 매개 변수를 구성해야 합니다. 이 절차에서는 (부트 이미지뿐 아니라) 전체 시스템 소프트웨어가 설치되었음을 전제로 합니다. 즉 직접 설치한 다음 모듈이 사전 설치된 디바이스를 구매했거나, 하드웨어 모듈에 이미 설치된 상태일 수 있습니다.

또한 초기 구성을 수행하는 것으로 가정합니다. 초기 구성 과정에서 이러한 설정에 대한 프롬프트가 표시됩니다. 나중에 이 설정을 변경해야 하는 경우 다양한 **configure network** 명령을 사용하여 개별 설정을 변경합니다. **configure network** 명령에 대한 자세한 내용은 **?** 도움말 명령을 사용하고 *FireSIGHT System 사용자 설명서* 또는 FireSIGHT Management Center의 온라인 도움말을 참조하십시오.

1단계 다음 중 하나를 수행합니다.

- (모든 모듈) SSH를 사용하여 ASA FirePOWER 관리 IP 주소에 연결합니다.
- (소프트웨어 모듈만) ASA CLI에서 모듈과의 세션을 엽니다(일반 운영 구성 설명서의 "Getting Started(시작)" 장에서 ASA CLI 액세스에 관한 설명 참조). 다중 컨텍스트 모드에서는 시스템 실행 공간에서 세션을 엽니다.

  호스트 이름 # **session sfr**

2단계 사용자 이름 **admin** 및 비밀번호 **Sourcefire**로 로그인합니다.

3단계 프롬프트에 따라 시스템 구성을 완료합니다.

먼저 EULA(최종 사용자 라이센스 계약)를 읽고 동의해야 합니다. 그런 다음 프롬프트에 따라 admin 비밀번호를 변경하고 관리 주소 및 NDS 설정을 구성합니다. IPv4 및 IPv6 관리 주소 모두 구성할 수 있습니다. FireSIGHT Management Center에서 센서를 관리해야 한다는 메시지가 표시되면 구성이 완료된 것입니다.

예를 들면 다음과 같습니다.

```
System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: <new password>
Confirm new password: <repeat 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]: 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]: 10.86.118.3
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.252.0
Enter the IPv4 default gateway for the management interface []: 10.86.116.1
Enter a fully qualified hostname for this system [Sourcefire3D]: asasfr.example.com
Enter a comma-separated list of DNS servers or 'none' []: 10.100.10.15,
10.120.10.14
Enter a comma-separated list of search domains or 'none' [example.net]: example.com
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
(Wait for the system to reconfigure itself.)

This sensor must be managed by a Defense Center.  A unique alphanumeric
registration key is always required.  In most cases, to register a sensor
to a Defense 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 Defense 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 Defense Center, you must use the same
registration key and, if necessary, the same NAT ID when you add this
sensor to the Defense Center.
```

4단계 이제 이 디바이스를 관리할 FireSIGHT Management Center를 식별해야 합니다(FireSIGHT Management Center에 ASA FirePOWER추가, 12페이지 의 설명 참조).

8 FireSIGHT Management Center에 ASA FirePOWER추가

FireSIGHT Management Center(Defense Center라고도 함)는 별도의 서버로서 동일한 모델 또는 서로 다른 모델의 여러 FirePOWER 디바이스를 관리합니다. FireSIGHT Management Center는 대규모 구축 환경을 관리하는 데 적합합니다. 여러 디바이스 간에 구성의 일관성을 유지하고 효율적인 트래픽 분석을 지원합니다.

ASA 5512-X부터 5585-X까지는 FireSIGHT Management Center에 모듈을 등록해야 합니다. 다른 방법으로는 모듈을 구성할 수 없습니다.

FireSIGHT Management Center에 디바이스를 등록하려면 **configure manager add** 명령을 사용합니다. FireSIGHT Management Center에 디바이스를 등록하려면 반드시 고유한 영숫자 등록 키가 필요합니다. 이는 사용자가 지정하는 간단한 키이며, 라이센스 키와 다릅니다.

대개의 경우, 다음과 같이 FireSIGHT Management Center의 호스트 이름 또는 IP 주소를 등록 키와 함께 사용합니다.

```
configure manager add DC.example.com my_reg_key
```

그러나 디바이스와 FireSIGHT Management Center 사이에 NAT 디바이스가 있을 경우, 다음과 같이 고유한 NAT ID를 등록 키와 함께 입력하고 호스트 이름 대신 DONTRESOLVE를 지정합니다.

```
configure manager add DONTRESOLVE my_reg_key my_nat_id
```

1단계 다음 중 하나를 수행합니다.

- (모든 모듈) SSH를 사용하여 ASA FirePOWER 관리 IP 주소에 연결합니다.

- (소프트웨어 모듈만) ASA CLI에서 모듈과의 세션을 엽니다(일반 운영 구성 설명서의 "Getting Started(시작)" 장에서 ASA CLI 액세스에 관한 설명 참조). 다중 컨텍스트 모드에서는 시스템 실행 공간에서 세션을 엽니다.

  호스트 이름 # **session sfr**

2단계 사용자 이름 **admin** 또는 CLI 구성(관리자) 액세스 레벨의 다른 사용자 이름으로 로그인합니다.

3단계 프롬프트에서 FireSIGHT Management Center에 디바이스를 등록합니다. **configure manager add** 명령을 사용하는데, 그 구문은 다음과 같습니다.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

여기서

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}에서는 FireSIGHT Management Center의 정규화된 호스트 이름 또는 IP 주소를 지정합니다. FireSIGHT Management Center의 직접적인 주소 지정이 불가능할 경우 DONTRESOLVE를 사용합니다.
- *reg_key*는 FireSIGHT Management Center에 디바이스를 등록하는 데 필요한 고유한 영숫자 등록 키입니다.
- *nat_id*는 FireSIGHT Management Center와 디바이스 간 등록 프로세스에서 사용되는 선택적 영숫자 문자열입니다. 호스트 이름이 DONTRESOLVE로 설정된 경우에 필요합니다.

4단계 브라우저에서 HTTPS 연결을 통해, 위에서 입력한 호스트 이름 또는 주소를 사용하여 FireSIGHT Management Center에 로그인합니다. 예를 들면, https://DC.example.com으로 연결합니다.

디바이스 관리(**Devices(디바이스) > Device Management(디바이스 관리)**) 페이지를 사용하여 디바이스를 추가합니다. 자세한 내용은 온라인 도움말 또는 *FireSIGHT System 사용자 설명서*의 디바이스 관리(Managing Devices) 장을 참조하십시오.

9 ASA FirePOWER 모듈의 보안 정책 구성

보안 정책은 NGIPS 필터링, 애플리케이션 필터링과 같이 모듈에서 제공하는 서비스를 제어합니다.

FireSIGHT Management Center에서 모듈의 보안 정책을 구성할 수 있습니다.

보안 정책 구성을 위한 CLI는 없습니다.

FireSIGHT Management Center에서 보안 정책 구성

다음 방법 중 하나로 FireSIGHT Management Center를 엽니다.

- 웹 브라우저에서 **https://***DC_address*를 엽니다. 여기서 *DC_address*는 FireSIGHT Management Center에 ASA FirePOWER 추가, 12페이지 에서 정의한 관리자의 DNS 이름 또는 IP 주소입니다. 예를 들면, https://dc.example.com으로 연결합니다.
- ASDM에서는 **Home(홈)(홈) > ASA FirePOWER Status(ASA FirePOWER 상태)**를 선택하고 대시보드 맨 아래의 링크를 클릭합니다.

보안 정책을 구성하는 방법에 대한 자세한 내용은 *FireSIGHT System 사용자 설명서* 또는 FireSIGHT Management Center의 온라인 도움말을 참조하십시오.

10 ASA FirePOWER 모듈에 트래픽 리디렉션

특정 트래픽을 지정하는 서비스 정책을 생성하여 ASA FirePOWER 모듈에 트래픽을 리디렉션합니다.

패시브("모니터 전용") 또는 인라인 구축 모드로 디바이스를 구성할 수 있습니다.

- 패시브 구축에서는 트래픽의 복사본이 디바이스에 보내지지만, ASA에 반환되지 않습니다. 패시브 모드에서는 네트워크에 영향을 주지 않고 디바이스가 트래픽을 어떻게 처리할지 확인할 수 있으며 트래픽의 내용을 평가할 수 있습니다.
- 인라인 구축의 경우, 실제 트래픽이 디바이스에 보내지며 트래픽 상태가 디바이스의 정책에 의해 영향을 받습니다. 불필요한 트래픽을 제거하고 정책에 따라 다른 조치를 취하면 트래픽이 ASA로 반환되어 추가적인 처리와 전송이 이루어집니다.

ASA에서 모니터 전용 모드와 일반 인라인 모드를 동시에 구성할 수는 없습니다. 오로지 하나의 보안 정책 유형만 허용됩니다. 다중 컨텍스트 모드의 경우, 일부 컨텍스트에 대해 모니터 전용 모드를 구성할 수 없고 또 다른 컨텍스트에서는 일반 인라인 모드를 구성할 수 없습니다.

시작하기 전에

- (ASA FirePOWER로 대체된) IPS 또는 CX 모듈에 트래픽을 리디렉션하는 서비스 정책이 활성 상태일 경우 먼저 이 정책을 제거한 다음 ASA FirePOWER 서비스 정책을 구성해야 합니다.
- 반드시 ASA와 ASA FirePOWER에서 일관된 정책을 구성하십시오. 두 정책 모두 트래픽의 패시브 또는 인라인 모드를 반영해야 합니다.
- 다중 컨텍스트 모드에서는 각 보안 컨텍스트 내에서 이 절차를 수행합니다.

절차

1단계 ASDM에서는 **Configuration(구성) > Firewall(방화벽) > Service Policy Rules(서비스 정책 규칙)**를 선택합니다.

2단계 **Add(추가) > Add Service Policy Rule(서비스 정책 규칙 추가)**을 선택합니다.

3단계 특정 인터페이스에 정책을 적용할지 아니면 글로벌 범위에 적용할지 선택하고 **Next(다음)**를 클릭합니다.

4단계 트래픽 일치를 구성합니다. 이를테면, 인바운드 액세스 규칙을 통과한 모든 트래픽이 모듈에 리디렉션되도록 **Any Traffic(모든 트래픽)** 일치를 선택합니다. 또는 포트, ACL(출처 및 목적지 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.

5단계 Rule Actions(규칙 작업) 페이지에서 **ASA FirePOWER Inspection(ASA FirePOWER 검사)** 탭을 클릭합니다.

6단계 **Enable ASA FirePOWER for this traffic flow(이 트래픽 흐름에서 ASA FirePOWER 사용)** 확인란을 선택합니다.

7단계 If ASA FirePOWER Card Fails(ASA FirePOWER 카드 실패 시) 영역에서 다음 중 하나를 선택합니다.

- **Permit traffic(트래픽 허용)**—모듈을 사용할 수 없을 경우 모든 트래픽을 검사하지 않고 허용하도록 ASA를 설정합니다.
- **Close traffic(트래픽 차단)**—모듈을 사용할 수 없을 경우 모든 트래픽을 차단하도록 ASA을 설정합니다.

8단계 (선택 사항) 트래픽의 읽기 전용 사본을 모듈에 보내려면(패시브 모드) **Monitor-only(모니터 전용)**를 선택합니다. 이 옵션을 선택하면 트래픽이 인라인 모드에서 전송됩니다. 자세한 내용은 ASA FirePOWER 패시브(모니터 전용) 모드, 3페이지 를 참조하십시오.

9단계 **Finish(완료)**와 **Apply(적용)**를 차례로 클릭합니다.

추가 트래픽 흐름을 구성하려면 이 절차를 반복합니다.

11 다음 단계

- ASA FirePOWER 모듈에 대한 자세한 내용은 ASA/ASDM 방화벽 구성 설명서의 "ASA FirePOWER 모듈" 장 또는 ASDM 온라인 도움말을 참조하십시오. 모든 ASA/ASDM 문서의 링크는 다음 사이트에 있습니다.

  http://www.cisco.com/c/en/us/td/docs/security/asa/roadmap/asaroadmap.html
- FireSIGHT Management Center(Defense Center)에 대한 자세한 내용은 애플리케이션의 온라인 도움말 또는 *FireSIGHT System 사용자 설명서*를 참조하십시오.

  http://www.cisco.com/c/en/us/support/security/defense-center/products-installation-and-configuration-guides-list.html

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2014 Cisco Systems, Inc. All rights reserved.

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

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