ASDM(온박스 관리)을 사용하여 FirePOWER Module에서 SSL 암호 해독 구성

목차

소개

이 문서에서는 ASDM(온박스 관리)을 사용하여 FirePOWER 모듈에서 SSL(Secure Sockets Layer) 암호 해독 구성에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA(Adaptive Security Appliance) 방화벽, ASDM(Adaptive Security Device Manager) 지식
- FirePOWER 어플라이언스에 대한 지식
- HTTPS/SSL 프로토콜 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 6.0.0 이상을 실행하는 ASA FirePOWER 모듈(ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)
- 소프트웨어 버전 6.0.0 이상을 실행하는 ASA FirePOWER 모듈(ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

> **참고:**FirePOWER Module에 이 기능을 구성할 수 있는 **Protect** 라이센스가 있는지 확인합니다.라이센스를 확인하려면 Configuration(컨피그레이션) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > License(라이센스)로 이동합니다**.

배경 정보

Firepower Module은 인바운드 및 아웃바운드 SSL 연결을 해독하고 검사하며, 이 연결은 리디렉션됩니다.트래픽이 해독되면 facebook 채팅 등의 터널링된 애플리케이션이 탐지되고 제어됩니다.해독된 데이터는 위협, URL 필터링, 파일 차단 또는 악성 데이터를 검사합니다.

아웃바운드 SSL 암호 해독

Firepower 모듈은 아웃바운드 SSL 요청을 가로채고 사용자가 방문하려는 사이트에 대한 인증서를 다시 생성하여 아웃바운드 SSL 연결을 위한 전달 프록시 역할을 합니다. 발급 기관(CA)은 Firepower Self-Signed 인증서입니다.Firepower의 인증서가 존재하는 계층 구조의 일부가 아니거나 클라이언트의 브라우저 캐시에 추가되지 않은 경우 보안 사이트로 이동하는 동안 클라이언트가 경고를 받습니다.Decrypt-Resignmethod는 아웃바운드 SSL 암호 해독을 수행하는 데 사용됩니다.

인바운드 SSL 암호 해독

내부 웹 서버 또는 디바이스로 인바운드 트래픽의 경우 관리자는 보호된 서버의 인증서 및 키의 복사본을 가져옵니다.SSL 서버 인증서가 firepower 모듈에 로드되고 SSL 암호 해독 정책이 인바운드 트래픽에 대해 구성된 경우, 디바이스는 트래픽을 전달할 때 트래픽을 해독하고 검사합니다.그런 다음 이 보안 채널을 통해 전달되는 악성 콘텐츠, 위협, 악성코드를 탐지합니다.또한 Decrypt-Known Keymethod를 사용하여 인바운드 SSL 해독을 수행합니다.

SSL 암호 해독 구성

SSL 트래픽 해독 방법에는 두 가지가 있습니다.

- Decrypt - 아웃바운드 SSL 트래픽에 대한 Resign
- Decrypt - 인바운드 SSL 트래픽에 대해 알려짐

아웃바운드 SSL 암호 해독(Decrypt - Resign)

Firepower 모듈은 공용 SSL 서버에 대한 모든 SSL 협상에 대해 MITM(man-in-the-middle) 역할을 합니다.Firepower 모듈에 구성된 중간 CA 인증서를 사용하여 공용 서버의 인증서를 폐기합니다.

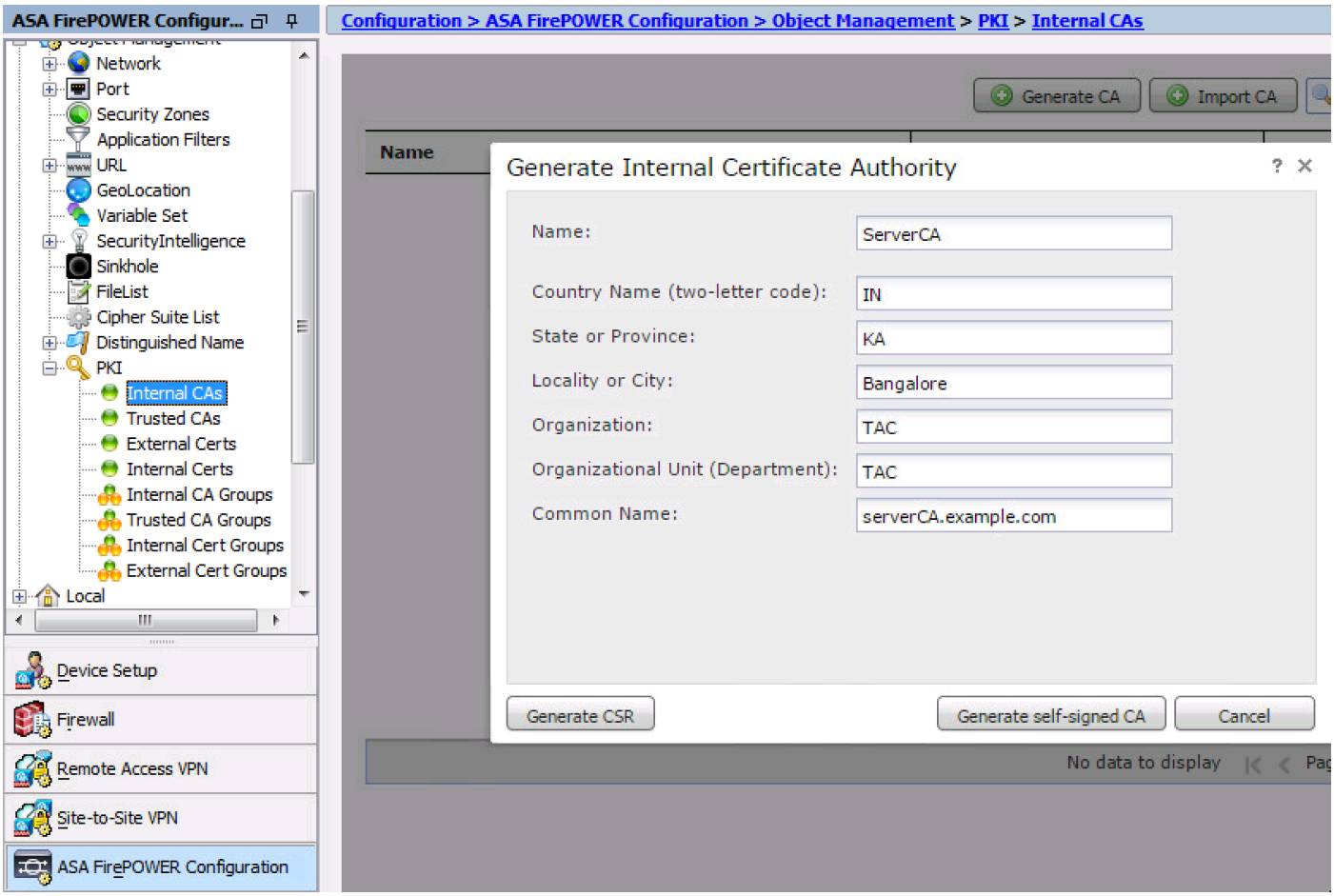
다음은 아웃바운드 SSL 암호 해독을 구성하는 세 가지 단계입니다.

1단계. CA 인증서를 구성합니다.

자체 서명 인증서 또는 중간 신뢰 CA 인증서를 인증서 사임에 대해 구성합니다.

자체 서명 CA 인증서 구성

자체 서명 CA 인증서를 구성하려면 Configuration(컨피그레이션) **> ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Object Management(개체 관리) > PKI > Internal CAs(내부 CA)로 이동하고 Generate CA(CA 생성)**를 클릭합니다.CA 인증서의 세부사항을 묻는 메시지가 표시됩니다.이미지에 표시된 대로 요구 사항에 따라 세부 정보를 입력합니다.



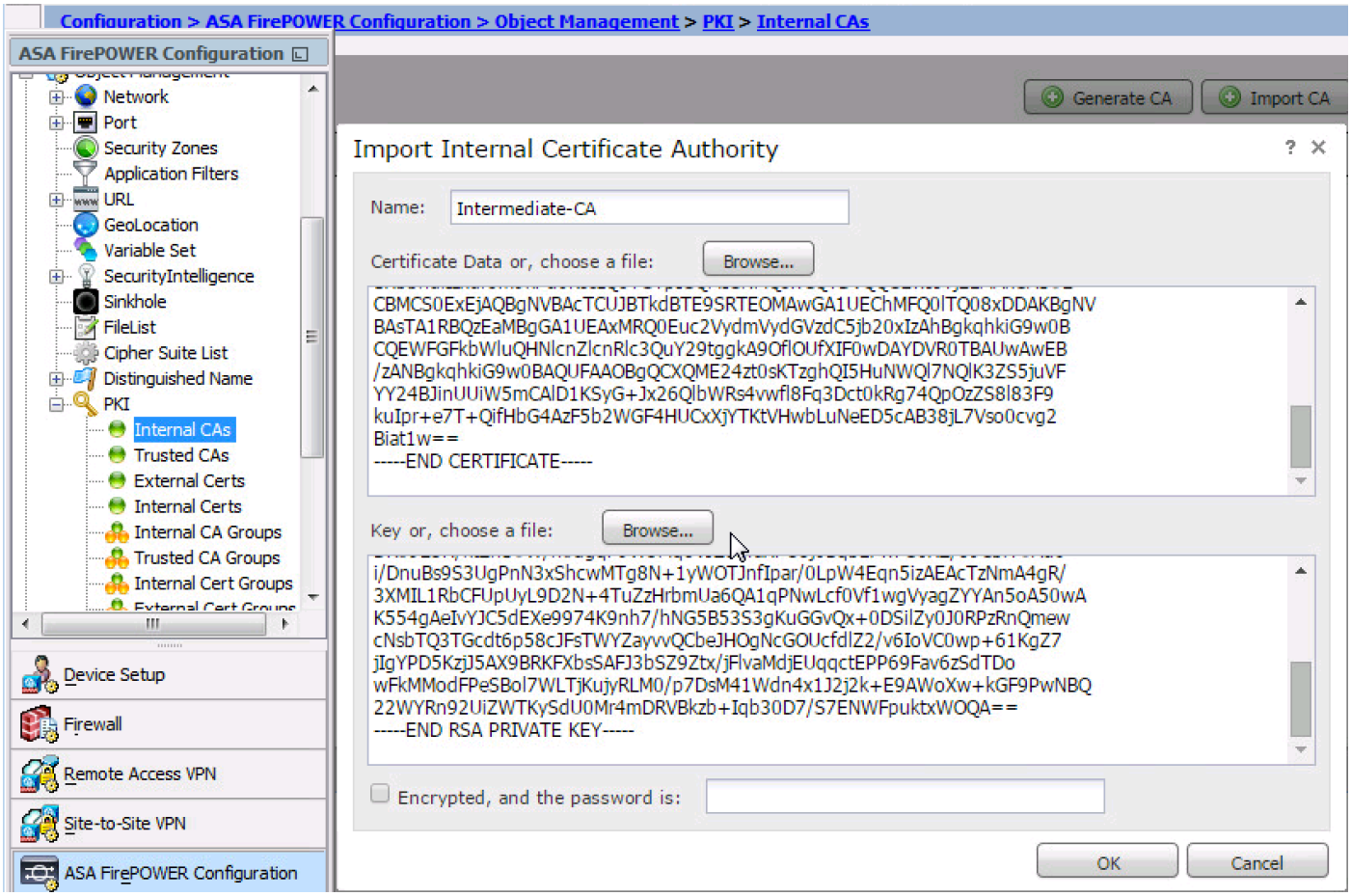
Generate self **signed CA(자체 서명 CA 생성)를** 클릭하여 내부 CA 인증서를 생성합니다.그런 다음 Generate **CSR(CSR 생성)**을 클릭하여 인증서 서명 요청을 생성합니다. 그러면 서명하기 위해 CA 서버와 공유됩니다.

중간 CA 인증서 구성

다른 서드파티 CA에서 서명한 중간 CA 인증서를 구성하려면 Configuration(구성) > **ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Object Management(개체 관리) > PKI > Internal CAs(내부 CA)로 이동하고 Import CA(CA 가져오기)**를 클릭합니다.

인증서의 이름을 지정합니다.로컬 컴퓨터에서 인증서를 찾아 업로드하거나 Certificate Data(인증서 데이터) 옵션에서 인증서 내용을 복사하여 붙여넣습니다.인증서의 개인 키를 지정하려면 키 파일을 찾아보거나 **Key** 옵션에 키를 복사하여 붙여 넣습니다.

키가 암호화된 경우 Encrypted 확인란을 **활성화하고** 비밀번호를 지정합니다.OK(**확인**)를 클릭하여 이미지에 표시된 대로 인증서 내용을 저장합니다.



2단계. SSL 정책을 구성합니다.

SSL 정책은 암호 해독 작업을 정의하고 해독 Decrypt-Resign 방법이 적용되는 트래픽을 식별합니다.비즈니스 요구 사항 및 조직 보안 정책에 따라 여러 SSL 규칙을 구성합니다.

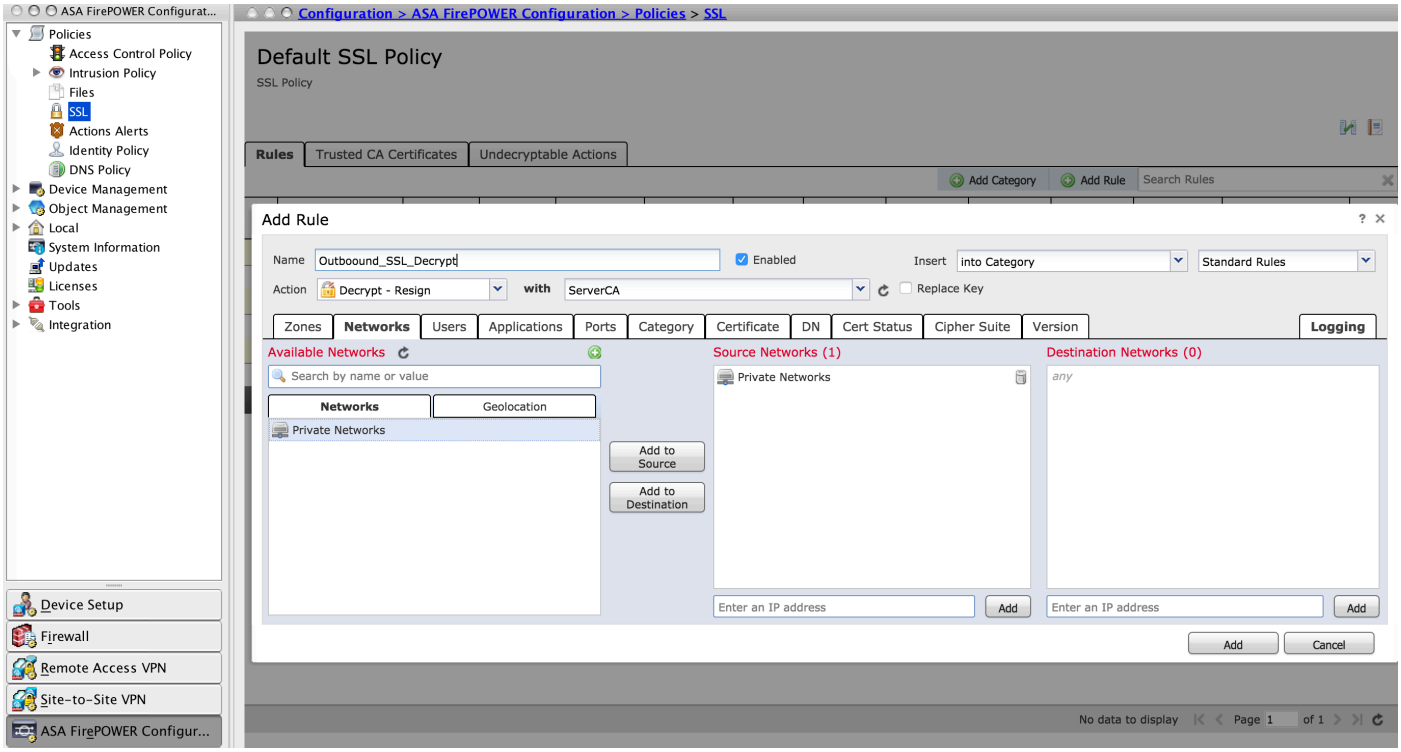
SSL 정책을 구성하려면 Configure(구성) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Policies(정책) > SSL**로 이동하고 **Add Rule(규칙 추가)을** 클릭합니다.

이름: 규칙의 이름을 지정합니다.

작업: 작업을 Decrypt **- Resign**으로 지정하고 이전 단계에서 구성된 드롭다운 목록에서 CA 인증서를 선택합니다.

여러 옵션(영역, 네트워크, 사용자 등)이 지정되어 해독해야 할 트래픽을 정의하므로 트래픽을 매칭할 조건을 규칙에 정의합니다.

SSL 암호 해독 이벤트를 생성하려면 이미지에 표시된 대로 logging logging 옵션을 활성화합니다.



Add(**추가**)를 클릭하여 SSL 규칙을 추가합니다.

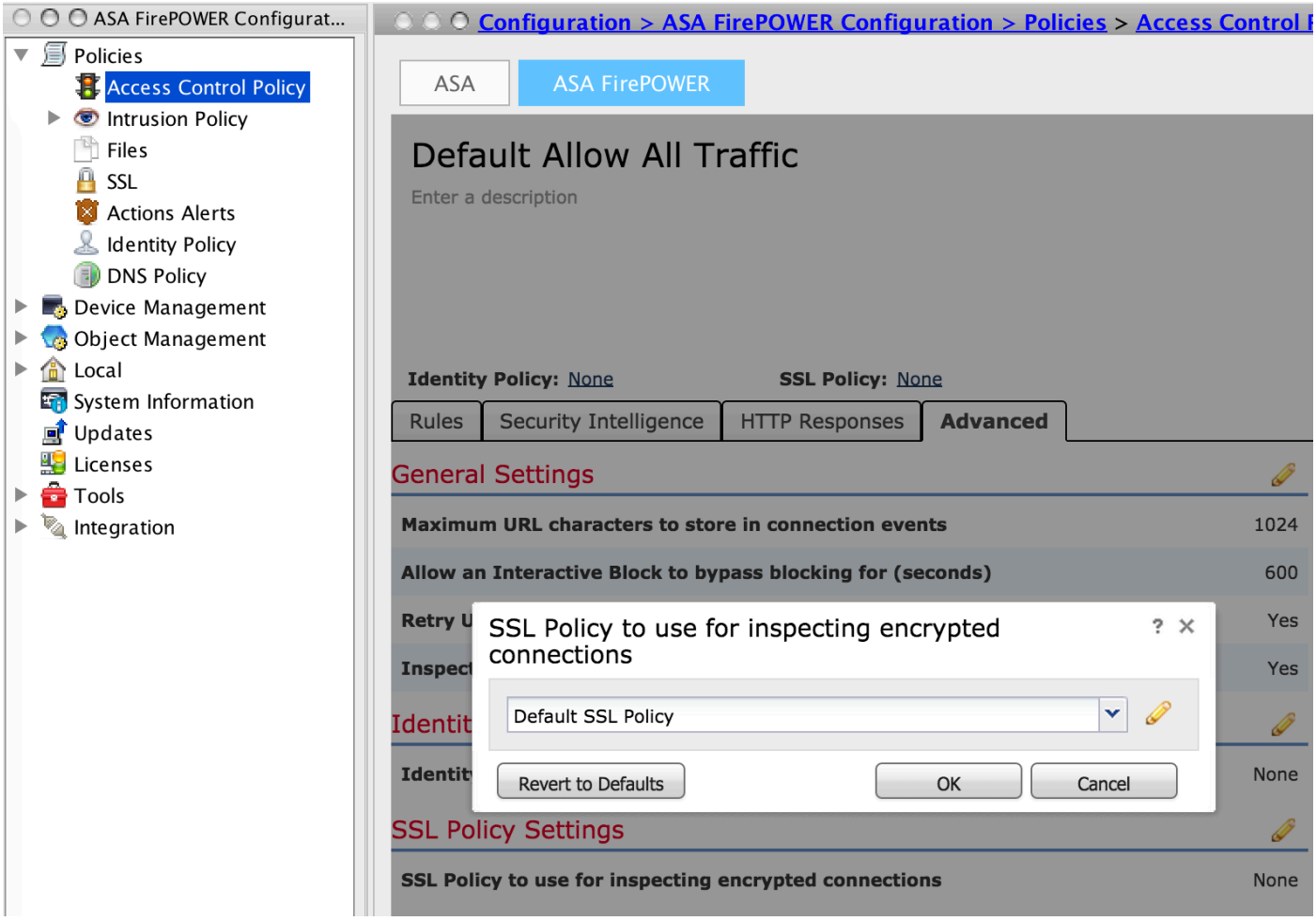
Store **ASA Firepower Changes(ASA Firepower 변경 사항 저장**)를 클릭하여 SSL 정책의 컨피그레이션을 저장합니다.

3단계. 액세스 제어 정책 구성

적절한 규칙으로 SSL 정책을 구성한 후에는 액세스 제어에서 SSL 정책을 지정하여 변경 사항을 구현해야 합니다.

액세스 제어 정책을 구성하려면 Configuration(컨피그레이션) > ASA Firepower Configuration(ASA Firepower 컨피그레이션) **> Policies(정책) > Access Control(액세스 제어)로 이동합니다.**

SSL 정책 중 **None**(없음)을 클릭하거나 Advanced(고급) **> SSL Policy Setting(SSL 정책 설정)**으로 **이동합니다.**드롭다운 목록에서 SSL 정책을 지정하고 이미지에 표시된 대로 **OK**를 클릭하여 저장합니다.



클릭 **ASA Firepower 변경 사항 저장** SSL 정책의 컨피그레이션을 저장합니다.

센서에 액세스 제어 정책을 구축해야 합니다.정책을 적용하기 전에 모듈에서 **액세스 제어 정책**이 **오래되었음을** 나타냅니다. 센서에 변경 사항을 배포하려면 **[배포]를** 클릭하고 [FirePOWER 변경 사항 **배포] 옵션을 선택합니다.**변경 사항을 확인하고 Deploy(구축)를 **클릭합니다.**

> **참고:**버전 5.4.x에서 센서에 액세스 정책을 적용해야 하는 경우 **Apply ASA FirePOWER Changes(ASA FirePOWER 변경 사항 적용)를** 클릭합니다.

> **참고:**Monitoring(모니터링) **> ASA Firepower Monitoring(ASA Firepower 모니터링) > Task Status(작업 상태)로 이동합니다.**그런 다음 구성 변경을 신청하여 작업이 완료되었는지 확인합니다.

인바운드 SSL 암호 해독(Decrypt - Known)

인바운드 SSL 암호 해독(Decrypt-Known) 방법은 서버 인증서 및 개인 키를 구성한 인바운드 SSL 트래픽을 해독하는 데 사용됩니다.서버 인증서 및 개인 키를 Firepower 모듈로 가져와야 합니다 .SSL 트래픽이 Firepower 모듈에 도달하면 트래픽을 해독하고 해독된 트래픽에 대한 검사를 수행합니다.검사 후 Firepower 모듈은 트래픽을 다시 암호화하여 서버로 전송합니다.

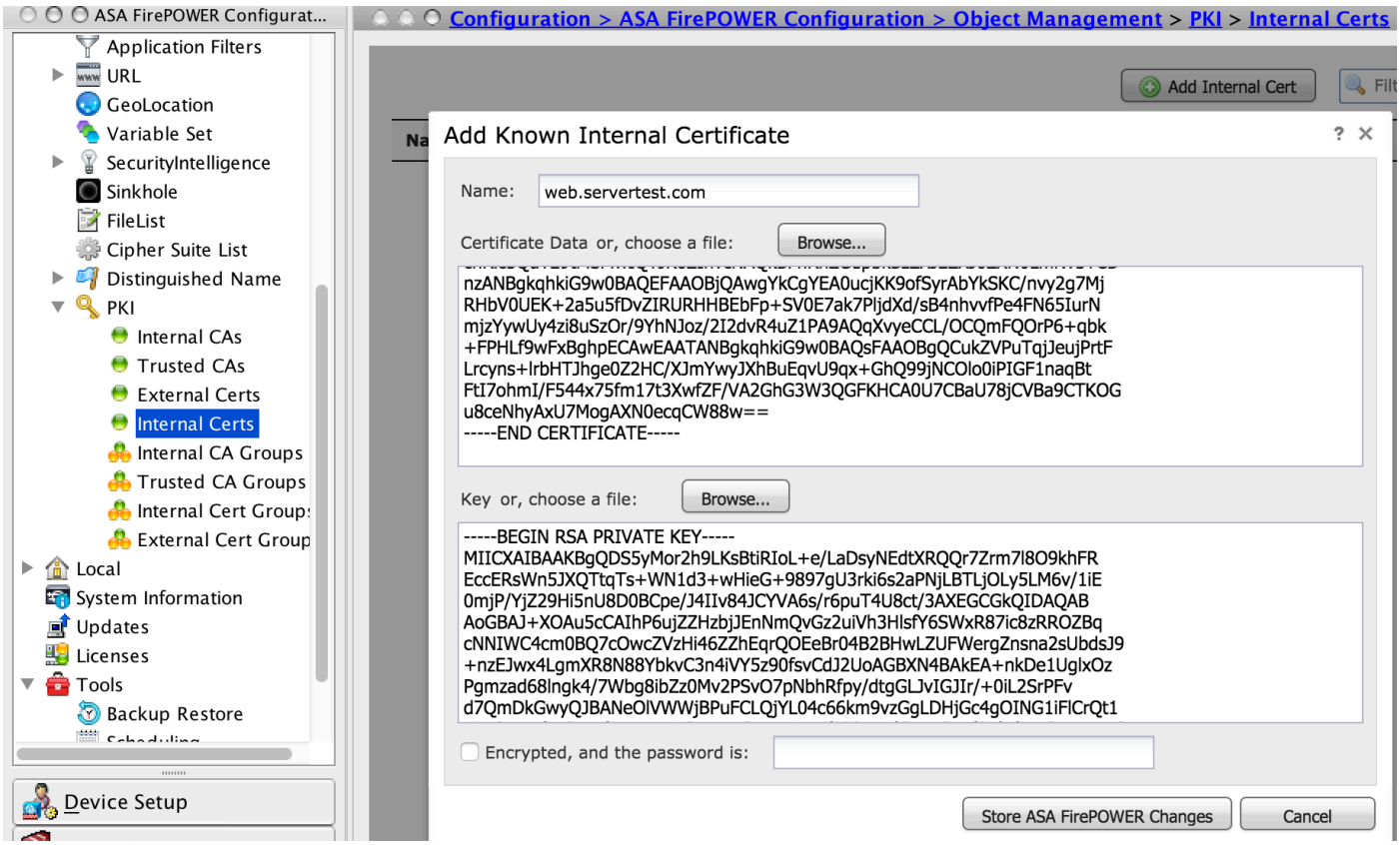
다음은 아웃바운드 SSL 암호 해독을 구성하는 4단계입니다.

1단계. 서버 인증서 및 키를 가져옵니다.

Server Certificate and Key(서버 인증서 및 키)를 가져오려면 Configuration(구성) **> ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Object Management(개체 관리) > PKI > Internal Certs(내부 인증서)**로 이동하고 **Add Internal Cert(내부 인증서 추가)**를 클릭합니다.

이미지에 표시된 대로 인증서의 이름을 지정합니다.찾아보기를 **선택하여** 로컬 컴퓨터에서 인증서를 선택하거나 인증서 **데이터**에 인증서 내용을 복사하여 **붙여넣습니다**.인증서의 개인 키를 지정하려면 키 파일을 찾아보거나 옵션 **Key**에서 키를 복사하여 붙여 넣습니다.

키가 암호화되어 있으면 Encrypted(암호화됨) 확인란을 **활성화하고** 이미지에 표시된 대로 비밀번호를 지정합니다.



Store **ASA FirePOWER Changes를 클릭하여** 인증서 내용을 저장합니다.

2단계. CA 인증서를 가져옵니다(선택 사항).

내부 중간 또는 루트 CA 인증서에서 서명한 서버 인증서의 경우 CA 인증서의 내부 체인을 firepower 모듈로 가져와야 합니다.가져오기를 수행한 후 firepower 모듈은 서버 인증서를 검증할 수 있습니다.

CA 인증서를 가져오려면 Configuration(구성) **> ASA Firepower Configuration(ASA Firepower 컨피그레이션) > Object Management(개체 관리) > Trusted CAs(신뢰할 수 있는 CA)로** 이동하고 **Add Trusted CA(신뢰할 수 있는 CA 추가)**를 클릭하여 CA 인증서를 추가합니다.

3단계. SSL 정책을 구성합니다.

SSL 정책은 인바운드 트래픽을 해독하기 위해 Decrypt-known 메서드를 구성하려는 작업과 서버 세부사항을 정의합니다.여러 내부 서버가 있는 경우 서로 다른 서버 및 처리하는 트래픽을 기반으

로 여러 SSL 규칙을 구성합니다.

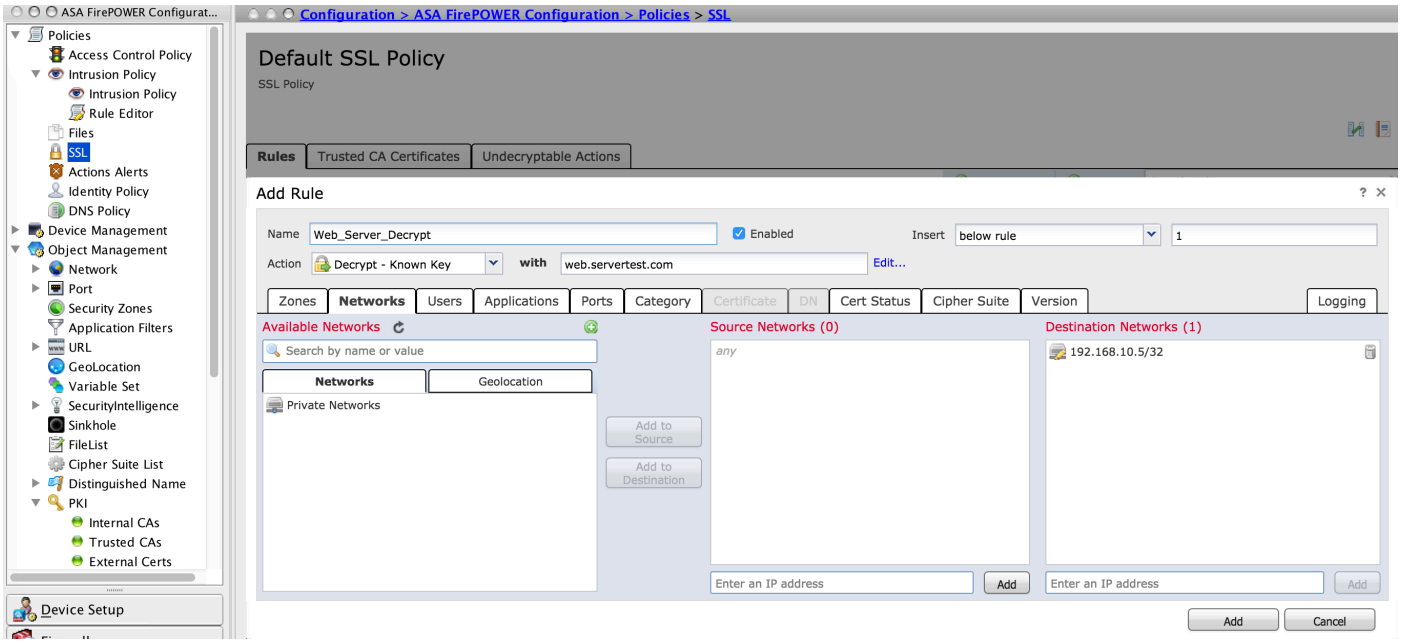
SSL 정책을 구성하려면 Configure(구성) **> ASA FirePOWER Configuration(ASA FirePOWER 컨피그레이션) > Policies(정책) > SSL**로 이동하고 **Add Rule(규칙 추가)**을 클릭합니다.

이름: 규칙의 이름을 지정합니다.

작업: 작업을 Decrypt **- known**으로 지정하고 이전 단계에서 구성된 드롭다운 목록에서 CA 인증서를 선택합니다.

SSL 암호 해독을 활성화할 서버의 흥미로운 트래픽을 정의하기 위해 여러 옵션(네트워크, 애플리케이션, 포트 등)이 지정되므로 이 규칙과 일치시킬 조건을 정의합니다. 신뢰할 수 있는 CA 인증서 탭의 **선택된 신뢰할 수 있는 CA에서** 내부 CA를 지정합니다.

SSL 암호 해독 이벤트를 생성하려면 logging logging 옵션을 **활성화합니다**.



Add(**추가**)를 클릭하여 SSL 규칙을 추가합니다.

그런 다음 Store **ASA Firepower Changes(ASA Firepower 변경 사항 저장)를** 클릭하여 SSL 정책의 컨피그레이션을 저장합니다.

4단계. 액세스 제어 정책을 구성합니다.

적절한 규칙으로 SSL 정책을 구성한 후에는 액세스 제어에서 SSL 정책을 지정하여 변경 사항을 구현해야 합니다.

액세스 제어 정책을 구성하려면 Configuration(컨피그레이션) > ASA Firepower Configuration(ASA Firepower 컨피그레이션) **> Policies(정책) > Access Control(액세스 제어)로 이동합니다.**

SSL 정책 옆에 있는 **None** 옵션을 클릭하거나 **Advanced(고급) > SSL Policy Setting(SSL 정책 설정)**으로 이동하고 드롭다운 목록에서 SSL 정책을 지정하고 **OK(확인)를 클릭하여** 저장합니다.

클릭 **ASA Firepower 변경 사항 저장** SSL 정책의 컨피그레이션을 저장합니다.

액세스 제어 정책을 구축해야 합니다.정책을 적용하기 전에 모듈에서 액세스 제어 정책이 오래된

것을 확인할 수 있습니다. 센서에 변경 사항을 배포하려면 [배포]를 클릭하고 [FirePOWER 변경 사항 **배포] 옵션을 선택하십시오.**변경 사항을 확인하고 팝업 창에서 Deploy를 클릭합니다.

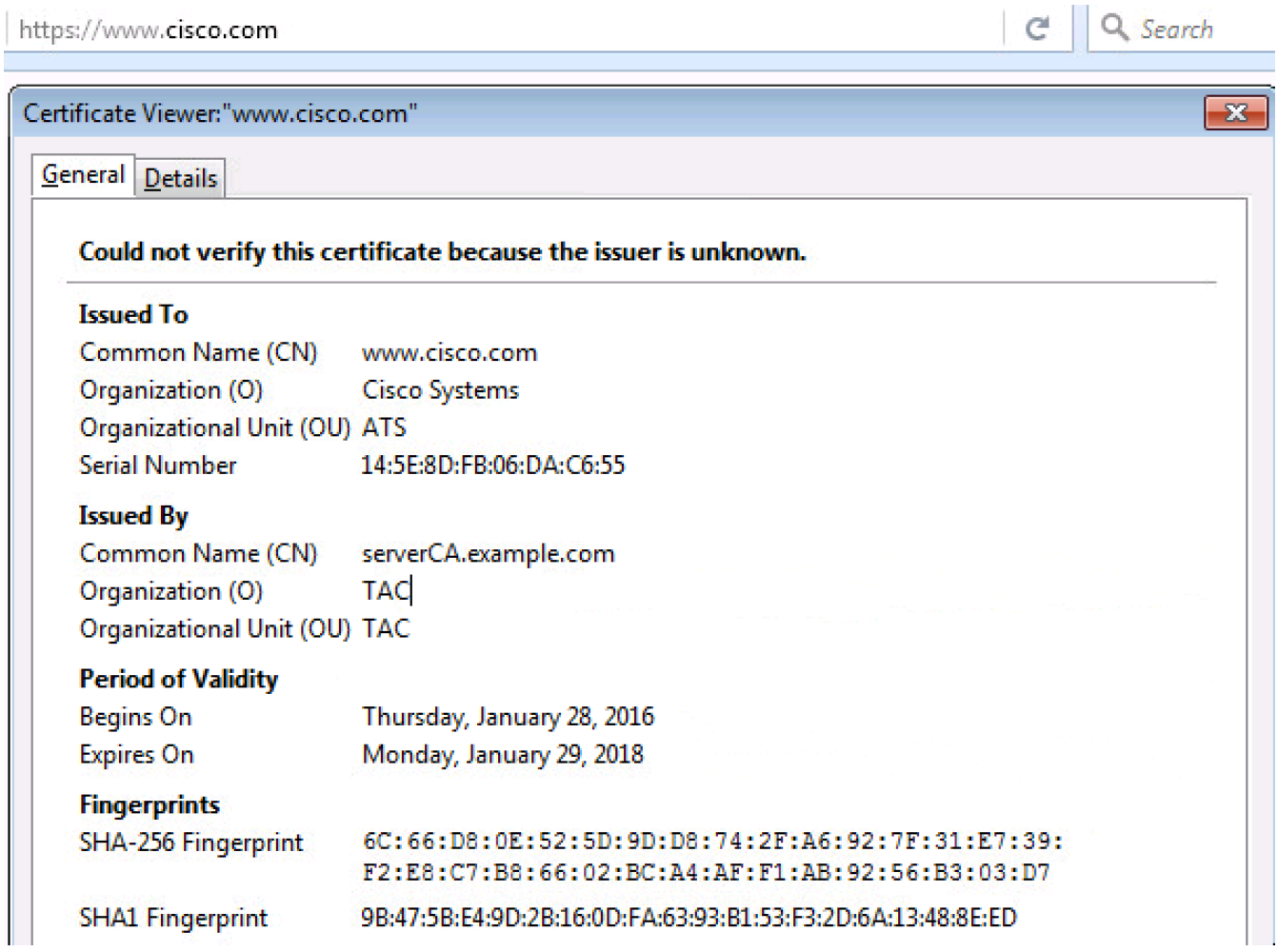
> **참고:**버전 5.4.x에서 센서에 액세스 정책을 적용해야 하는 경우 **Apply ASA FirePOWER Changes(ASA FirePOWER 변경 사항 적용)를 클릭합니다**.

> **참고:**Monitoring(모니터링) **> ASA Firepower Monitoring(ASA Firepower 모니터링) > Task Status(작업 상태)로 이동합니다.**그런 다음 구성 변경을 신청하여 작업이 완료되었는지 확인합니다.

다음을 확인합니다.

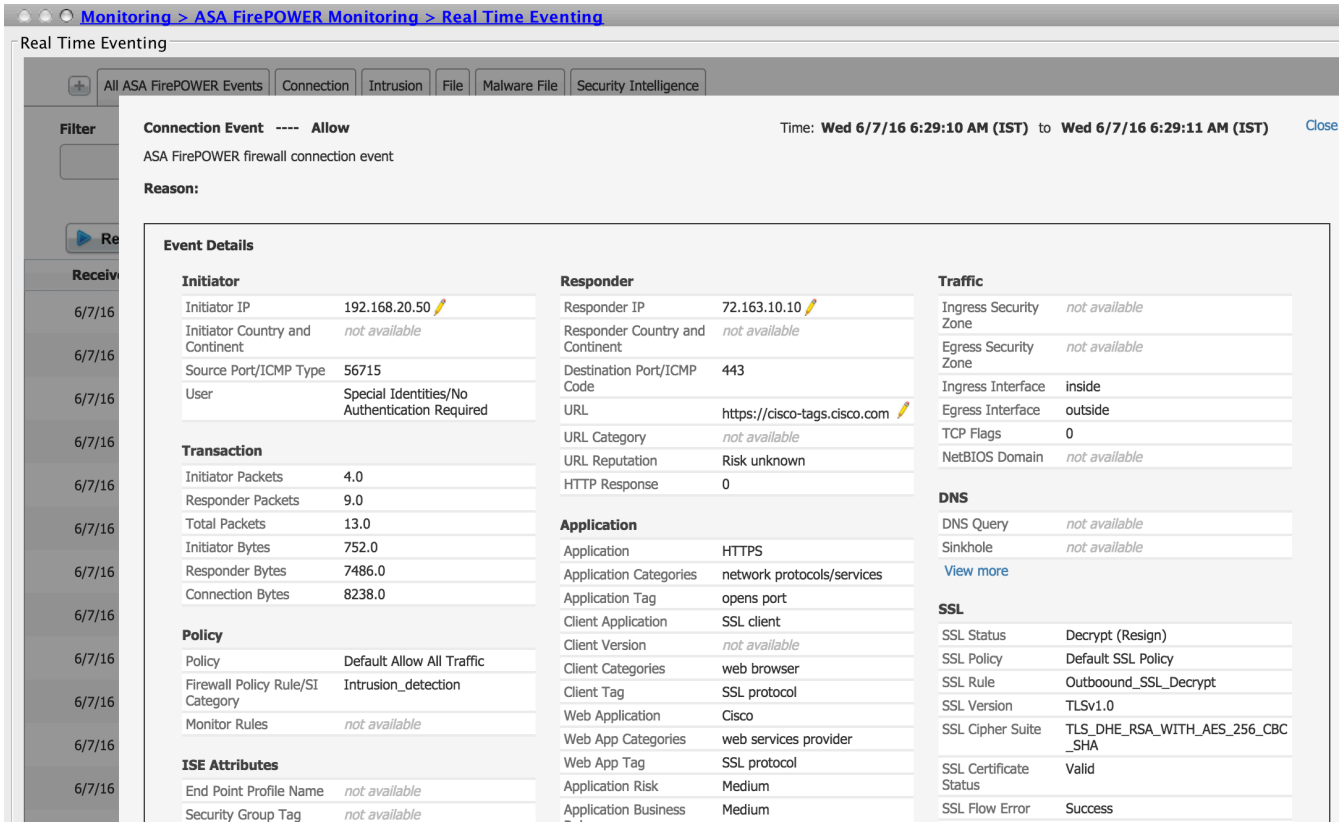
이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

- 아웃바운드 SSL 연결의 경우 내부 네트워크에서 공용 SSL 웹 사이트를 탐색하면 인증서 오류 메시지가 표시됩니다.인증서 내용을 확인하고 CA 정보를 확인합니다.Firepower 모듈에서 구성한 내부 CA 인증서가 나타납니다.SSL 인증서를 찾아보려면 오류 메시지를 수락합니다.오류 메시지를 방지하려면 CA 인증서를 브라우저의 신뢰할 수 있는 CA 목록에 추가합니다.



- 어떤 SSL 정책 및 SSL 규칙이 트래픽에 의해 히치되었는지 확인하려면 연결 이벤트를 확인합니다.Monitoring(**모니터링) > ASA FirePOWER Monitoring(ASA FirePOWER 모니터링) >**

Real-Time Eventing(실시간 이벤트)으로 이동합니다. 이벤트를 선택하고 View Details(세부 정보 보기)를 **클릭합니다**.SSL 암호 해독 통계를 확인합니다.



- 액세스 제어 정책 구축이 성공적으로 완료되었는지 확인합니다.
- SSL 정책이 액세스 제어 정책에 포함되었는지 확인합니다.
- SSL 정책에 인바운드 및 아웃바운드 방향에 대한 적절한 규칙이 포함되어 있는지 확인합니다.
- SSL 규칙에 흥미로운 트래픽을 정의하기 위한 적절한 조건이 포함되어 있는지 확인합니다.
- 연결 이벤트를 모니터링하여 SSL 정책 및 SSL 규칙을 확인합니다.
- SSL 암호 해독 상태를 확인합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- 기술 지원 및 문서 – Cisco Systems