Cisco FireSIGHT 시스템에 SSL 검사 정책 구성

목차

소개

SSL 검사 기능을 사용하면 암호화된 트래픽을 검사하지 않고 차단하거나, 액세스 제어로 암호화된 트래픽 또는 해독된 트래픽을 검사할 수 있습니다.이 문서에서는 Cisco FireSIGHT System에서 SSL 검사 정책을 설정하는 컨피그레이션 단계에 대해 설명합니다.

사전 요구 사항

사용되는 구성 요소

- Cisco FireSIGHT Management Center
- Cisco Firepower 7000 또는 8000 어플라이언스
- 소프트웨어 버전 5.4.1 이상

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.

> **경고:** 관리되는 디바이스에 SSL 검사 정책을 적용하면 네트워크 성능에 영향을 미칠 수 있습니다.

구성

다음과 같은 방법으로 트래픽을 해독하도록 SSL 검사 정책을 구성할 수 있습니다.

1. 암호 해독 및 탈퇴:

- 옵션 1:FireSIGHT Center를 루트 CA(Certificate Authority)로 사용하거나
- 옵션 2:내부 CA가 인증서에 서명하도록 하거나
- 옵션 3:CA 인증서 및 키 가져오기

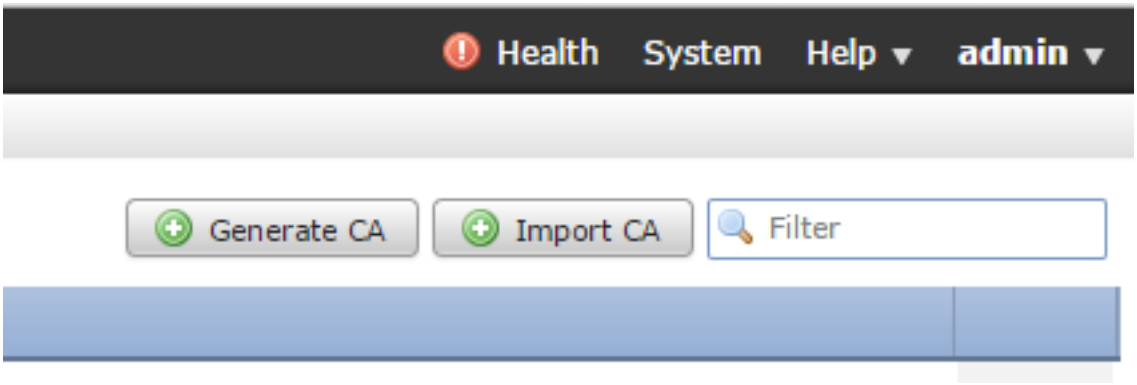
2. 알려진 인증서로 암호 해독:

- FireSIGHT Management Center에 로그인한 다음 Objects(개체)로 **이동합니다**.
- Objects(**개체**) 페이지에서 PKI**를** 확장하고 Internal CAs(**내부 CA)를 선택합니다**.

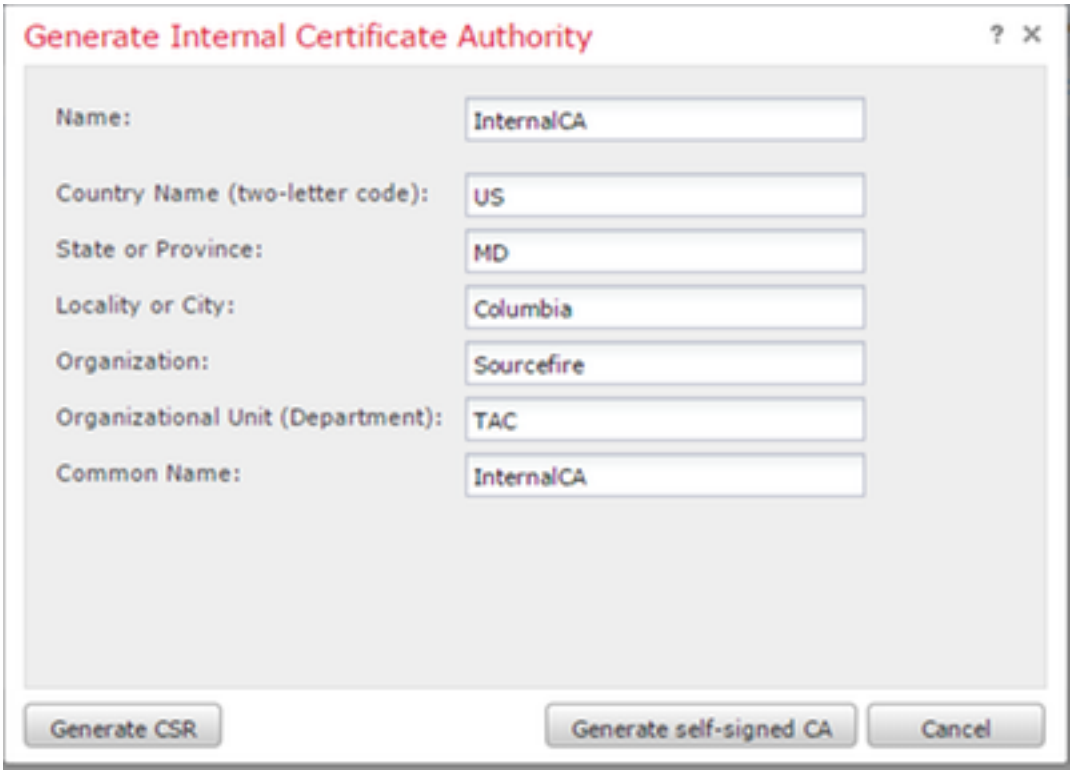
1. 암호 해독 및 탈퇴

옵션 1:FireSIGHT Center를 루트 CA(Certificate Authority)로 사용

i. **CA 생성을 클릭합니다**.



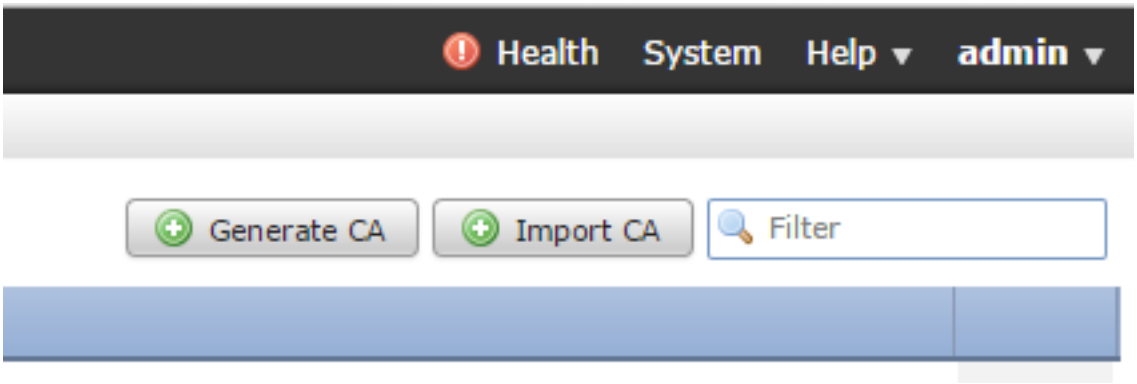
2.관련 정보 입력



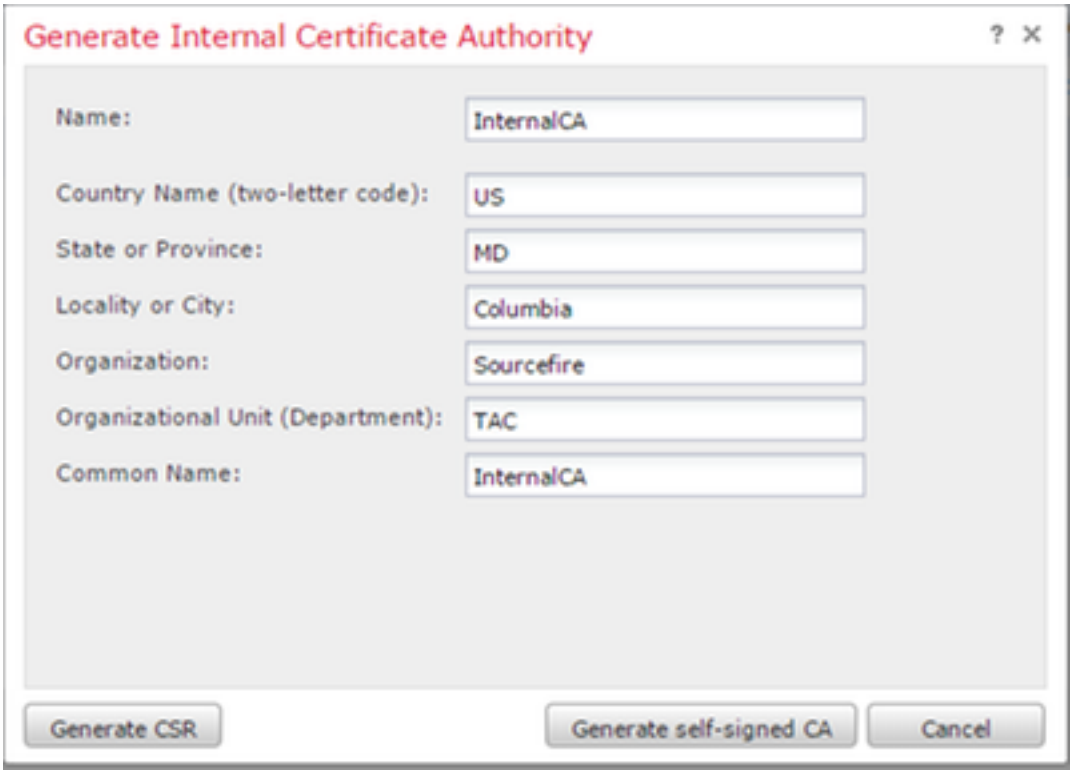
3.Generate **self-signed CA를 클릭합니다**.

옵션 2:내부 CA가 인증서에 서명하도록 합니다.

나.Generate **CA를 클릭합니다**.

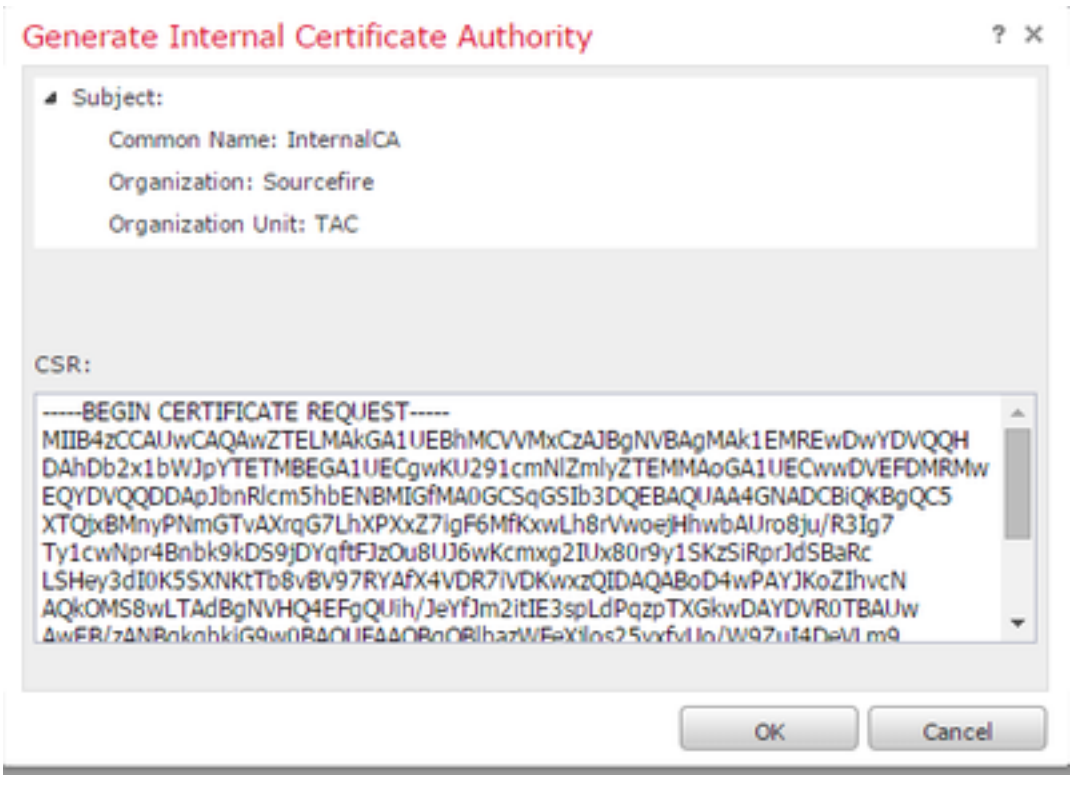


2.관련 정보를 입력합니다.



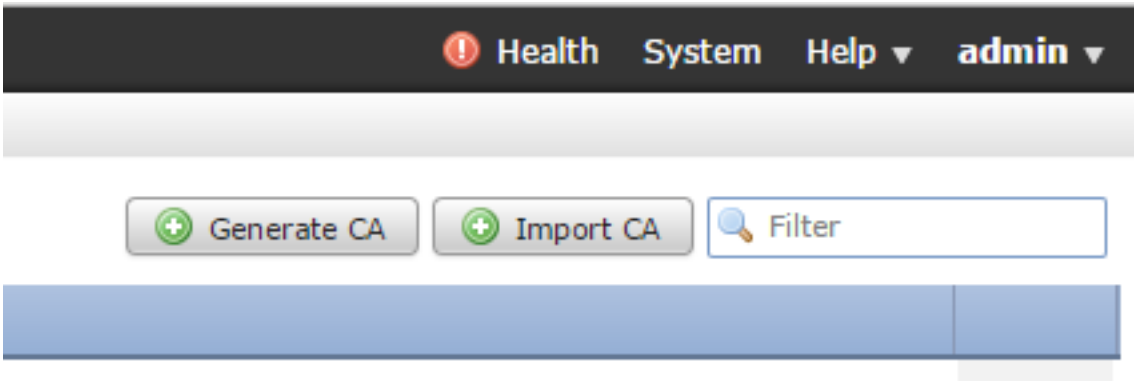
참고:서명 요청에 대한 템플릿이 있는지 확인하려면 CA 관리자에게 문의해야 할 수 있습니다.

3.BEGIN CERTIFICATE REQUEST(인증서 요청 시작) 및 —END CERTIFICATE REQUEST(인증서 요청 종료)를 포함한 전체 인증서를 복사한 다음 .req 확장자가 있는 텍스트 파일에 저장합니다.



참고: CA 관리자가 .req 이외의 다른 파일 확장명을 요청합니다.

옵션 3:CA 인증서 및 키 가져오기

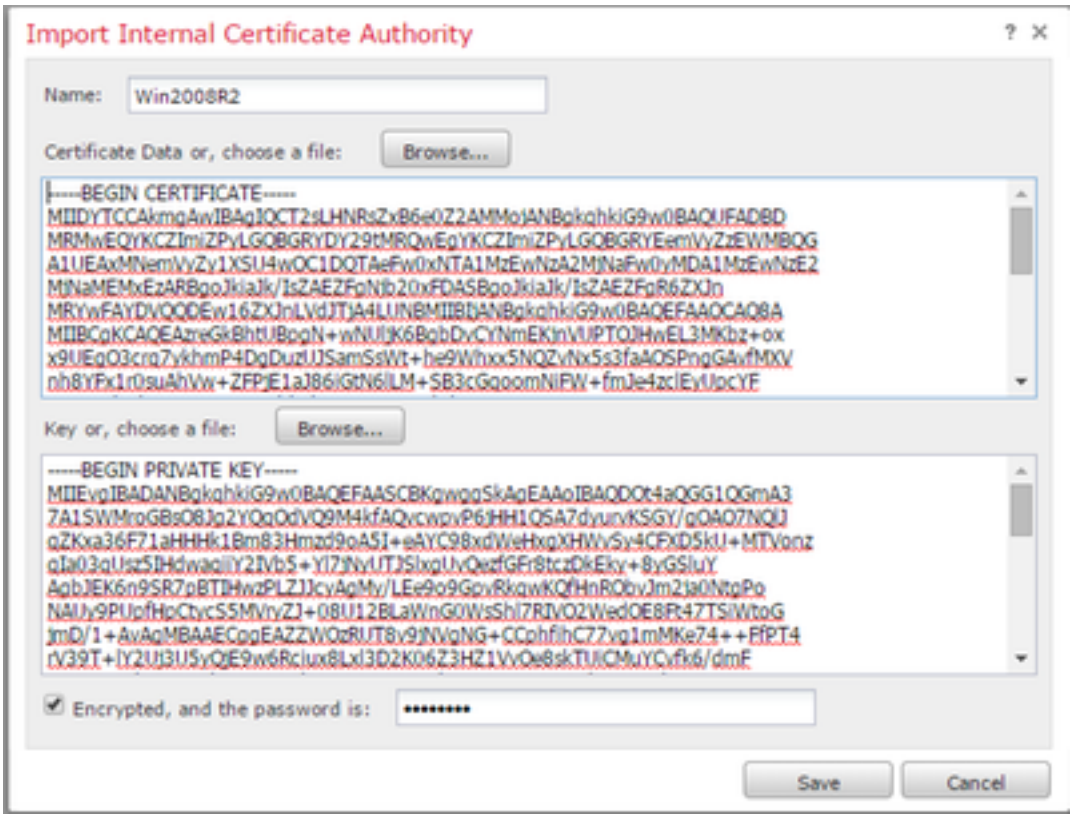


나.Import **CA를 클릭합니다**.

2.인증서를 찾아보거나 붙여넣습니다.

3.개인 키로 이동하거나 개인 키로 붙여넣습니다.

4.암호화된 상자를 선택하고 비밀번호를 입력합니다.



참고: 비밀번호가 없는 경우 암호화된 상자를 선택하고 비워 둡니다.

2. 알려진 키로 해독

알려진 인증서 가져오기(암호 해독 및 사임의 대체)

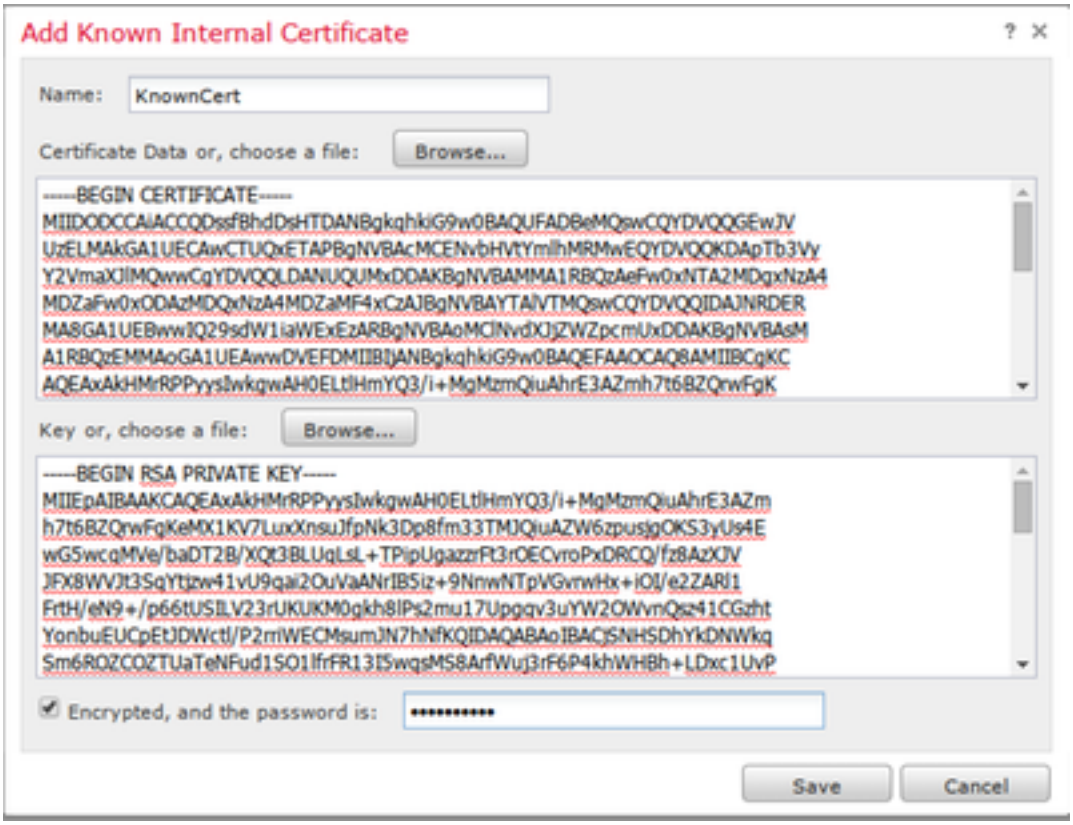
나.왼쪽의 Objects 페이지에서 PKI를 확장하고 Internal Certs를 선택합니다.

2.Add **Internal Cert를 클릭합니다**.

3.인증서를 찾아보거나 붙여넣습니다.

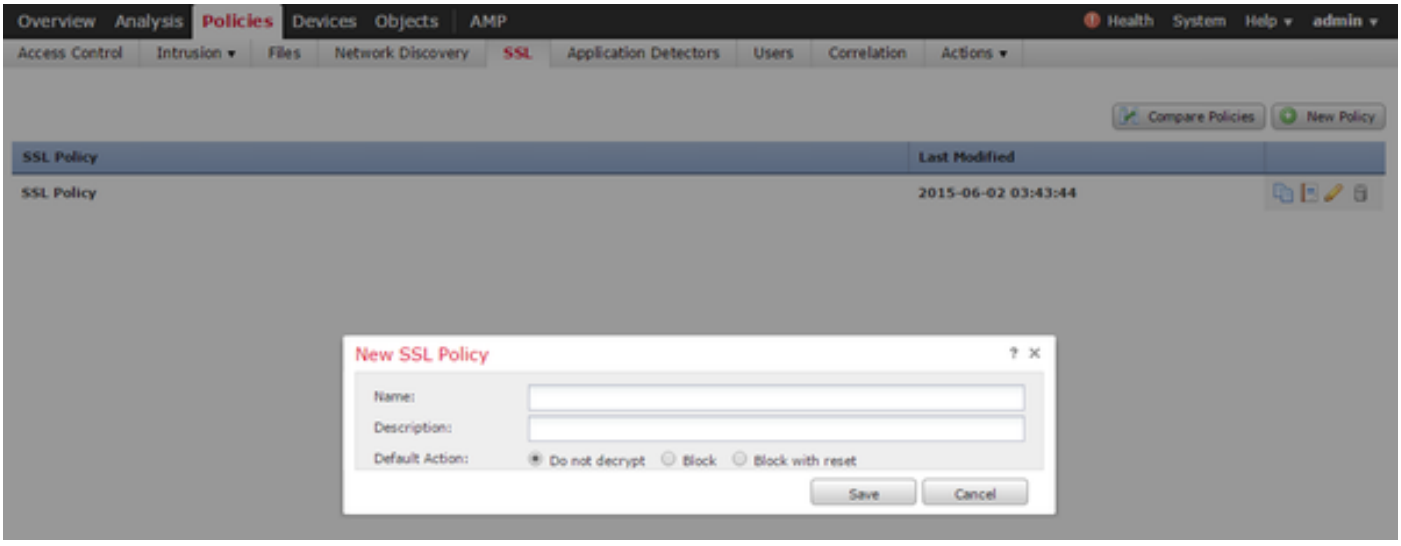
4.개인 키로 이동하거나 개인 키로 붙여넣습니다.

v. Encrypted(**암호화**) 상자를 선택하고 비밀번호를 입력합니다.



참고: 비밀번호가 없으면 **Encrypted** 상자를 비워 둡니다.

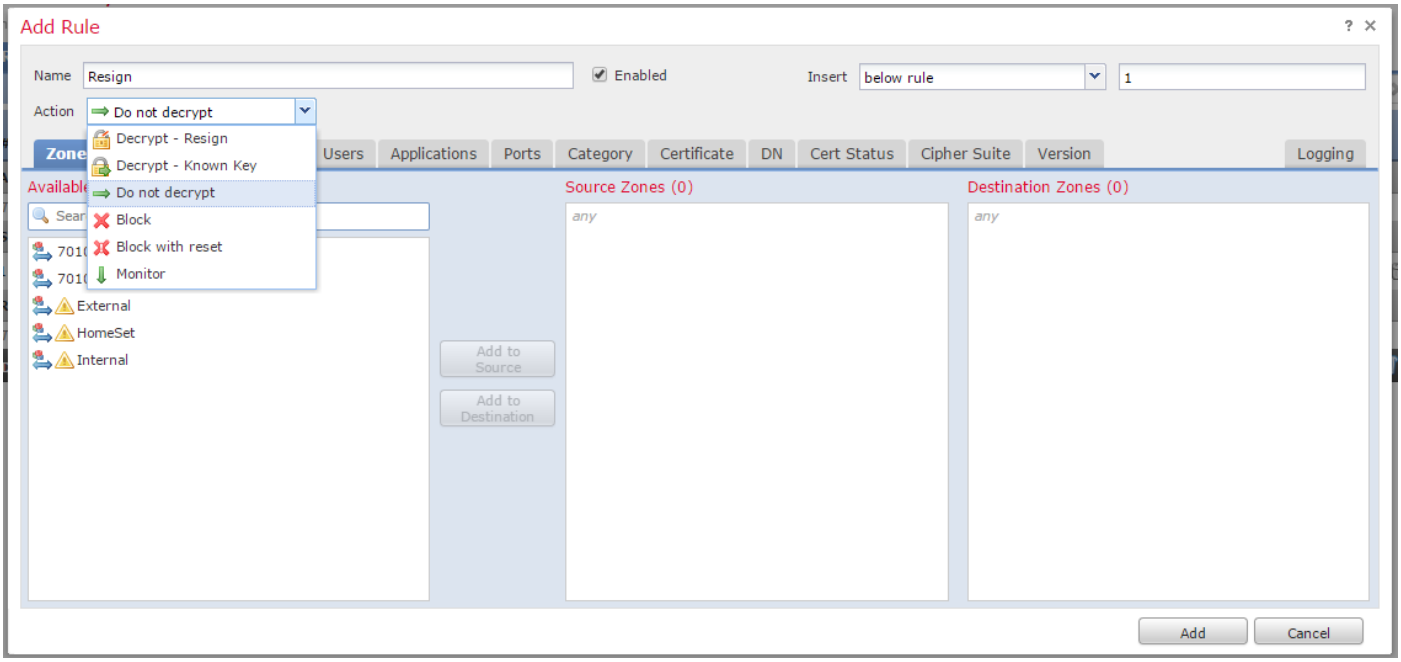
4. Policies(**정책) > SSL**로 이동한 다음 **New Policy(새 정책)를 클릭합니다**.



5. 이름을 입력하고 기본 조치를 **선택합니다**.SSL 정책 편집기 페이지가 나타납니다.SSL 정책 편집기 페이지는 Access Control Policy 편집기 페이지와 동일하게 작동합니다.

> **참고:** Default Action(**기본 작업**)에 대해 잘 모르겠으면 **Do not decrypt(해독 안 함)**가 권장되는 시작점입니다.

6. SSL 정책 편집기 페이지에서 **Add Rule**을 클릭합니다.Add Rule(규칙 추가) 창에서 규칙의 이름을 제공하고 기타 모든 관련 정보를 입력합니다.



다음 섹션에서는 **Add Rule** 창의 다양한 옵션에 대해 설명합니다.

작업

암호 해독 - 사임

- 센서는 MitM(Man in the Middle) 역할을 하며 사용자와의 연결을 수락한 다음 서버에 대한 새 연결을 설정합니다.예를 들면 다음과 같습니다.브라우저에서 https://www.facebook.com을 입력합니다.트래픽이 센서에 도달하면 센서가 선택한 CA 인증서를 사용하여 사용자와 협상하고 SSL 터널 A가 구축됩니다.동시에 센서가 https://www.facebook.com에 연결하여 SSL 터널 B를 생성합니다.
- 결과 종료:사용자는 Facebook이 아닌 규칙에서 인증서를 봅니다.
- 이 작업을 수행하려면 내부 CA가 필요합니다.키를 교체하려면 Replace Key를 선택합니다.사용자가 선택한 인증서를 받게 됩니다.

> **참고:** 수동 모드에서는 사용할 수 없습니다.

암호 해독 - 알려진 키

- 센서에는 트래픽 해독에 사용할 키가 있습니다.예를 들면 다음과 같습니다.브라우저에서 https://www.facebook.com을 입력합니다.트래픽이 센서에 도달하면 센서가 트래픽을 해독하고 트래픽을 검사합니다.
- 결과 종료:Facebook의 인증서 보기
- 이 작업에는 내부 인증서가 필요합니다.이는 Objects(개체) > **PKI> Internal Certs(내부 인증서)에 추가됩니다**.

> **참고:** 조직은 도메인 및 인증서의 소유자여야 합니다.facebook.com의 예를 들어, 최종 사용자가 facebook의 인증서를 볼 수 있는 유일한 방법은 도메인 facebook.com(예: 회사가 Facebook, Inc)을 소유하고 공용 CA에서 서명한 facebook.com 인증서의 소유권을 가지는 것

입니다.조직이 소유한 사이트의 알려진 키로만 해독할 수 있습니다.

알려진 키를 해독하는 주요 목적은 외부 공격으로부터 서버를 보호하기 위해 https 서버에 대한 트래픽 헤딩을 해독하는 것입니다.외부 https 사이트에 대한 클라이언트 측 트래픽 검사를 위해 서버를 소유하지 않고 외부 암호화 사이트에 연결하는 네트워크의 클라이언트 트래픽을 검사하려는 경우 decrypt resign을 사용합니다.

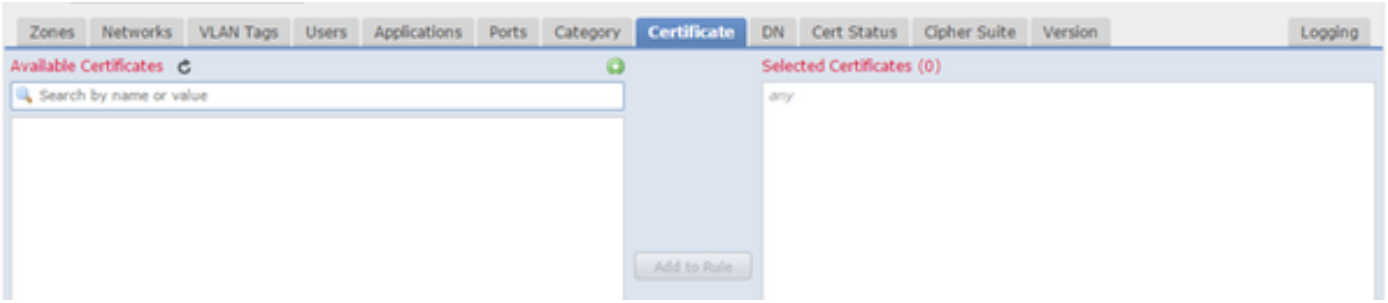
참고: DHE와 ECDHE가 해독하려면 In-line이어야 합니다.

암호 해독 안 함

트래픽은 SSL 정책을 우회하며 액세스 제어 정책으로 계속 이동합니다.

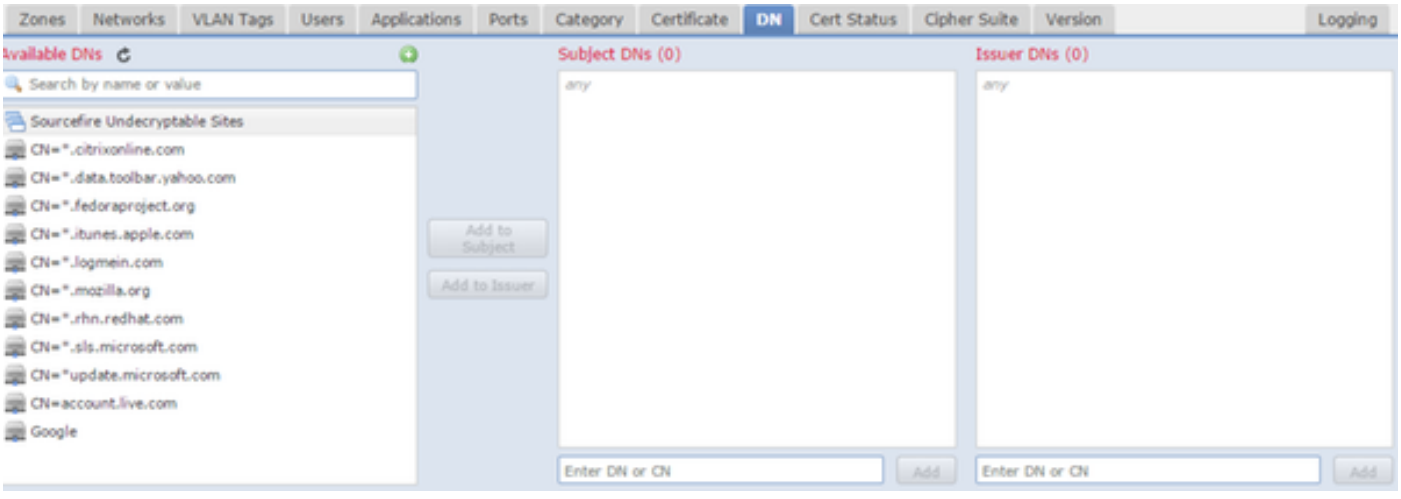
인증서

규칙은 이 특정 인증서를 사용하여 SSL 트래픽과 일치시킵니다.



DN

규칙은 인증서의 특정 도메인 이름을 사용하여 SSL 트래픽과 일치시킵니다.

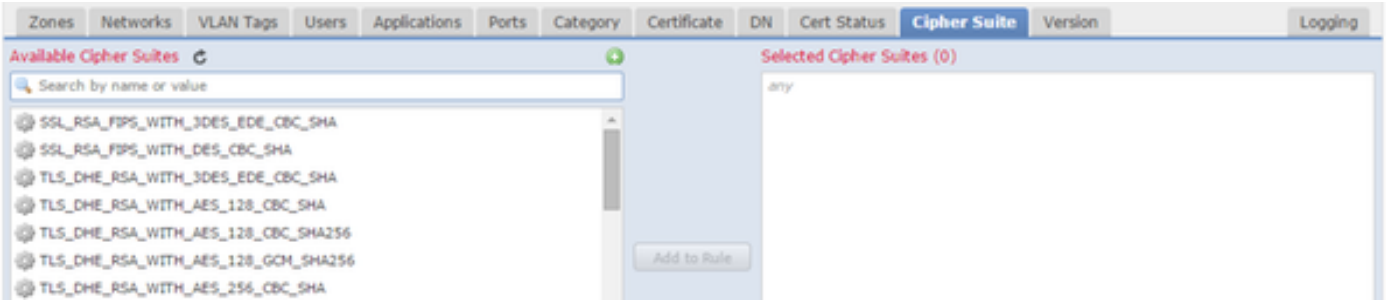


인증서 상태

규칙은 SSL 트래픽과 이러한 인증서 상태를 매칭합니다.

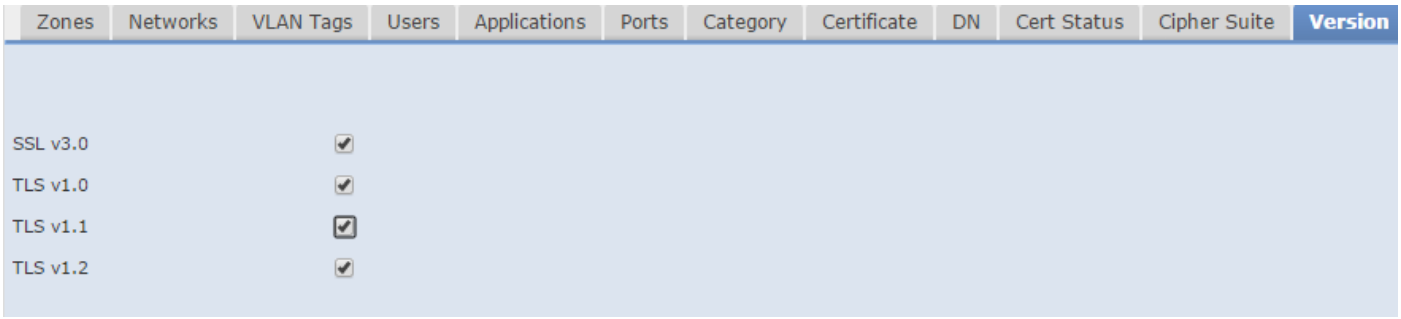
암호 그룹

규칙은 이러한 암호 그룹을 사용하여 SSL 트래픽과 일치시킵니다.



버전

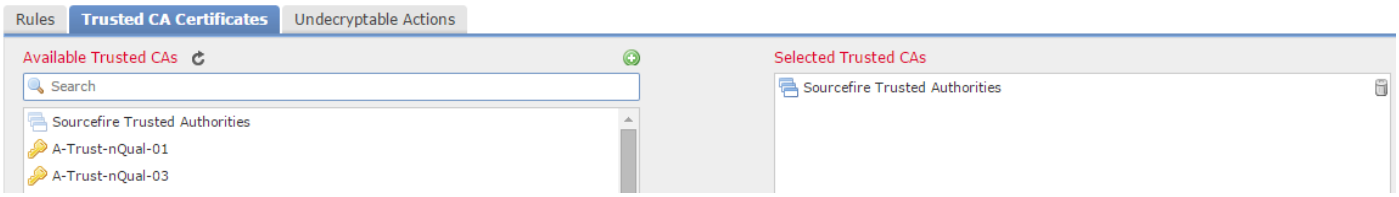
규칙은 선택한 SSL 버전의 SSL 트래픽에만 적용됩니다.



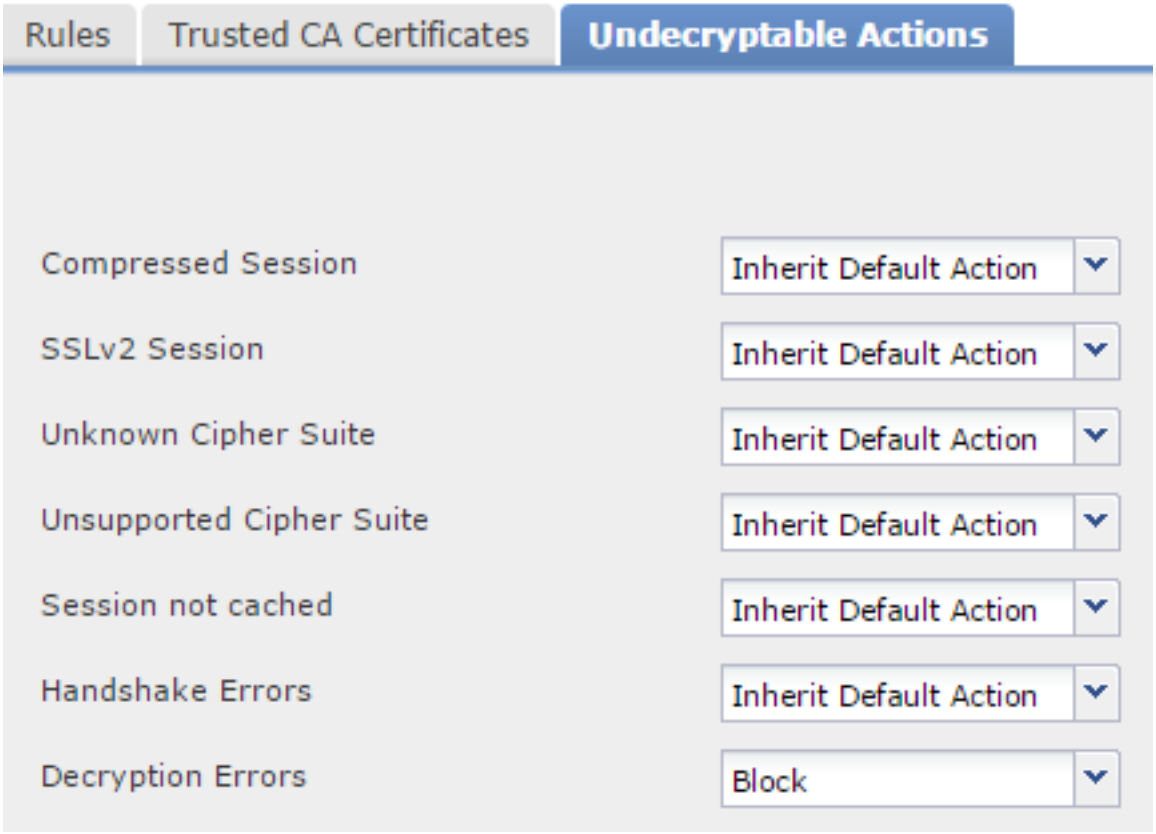
로깅

SSL 트래픽에 대한 연결 이벤트를 보려면 로깅을 활성화합니다.

7. Trusted **CA Certificate를 클릭합니다**.신뢰할 수 있는 CA가 정책에 추가되는 위치입니다.



8. 해독 불가 **조치를 클릭합니다**.센서가 트래픽을 해독할 수 없는 작업은 다음과 같습니다.정의는 FireSIGHT Management Center의 온라인 도움말(**Help > Online**)에서 확인할 수 있습니다.



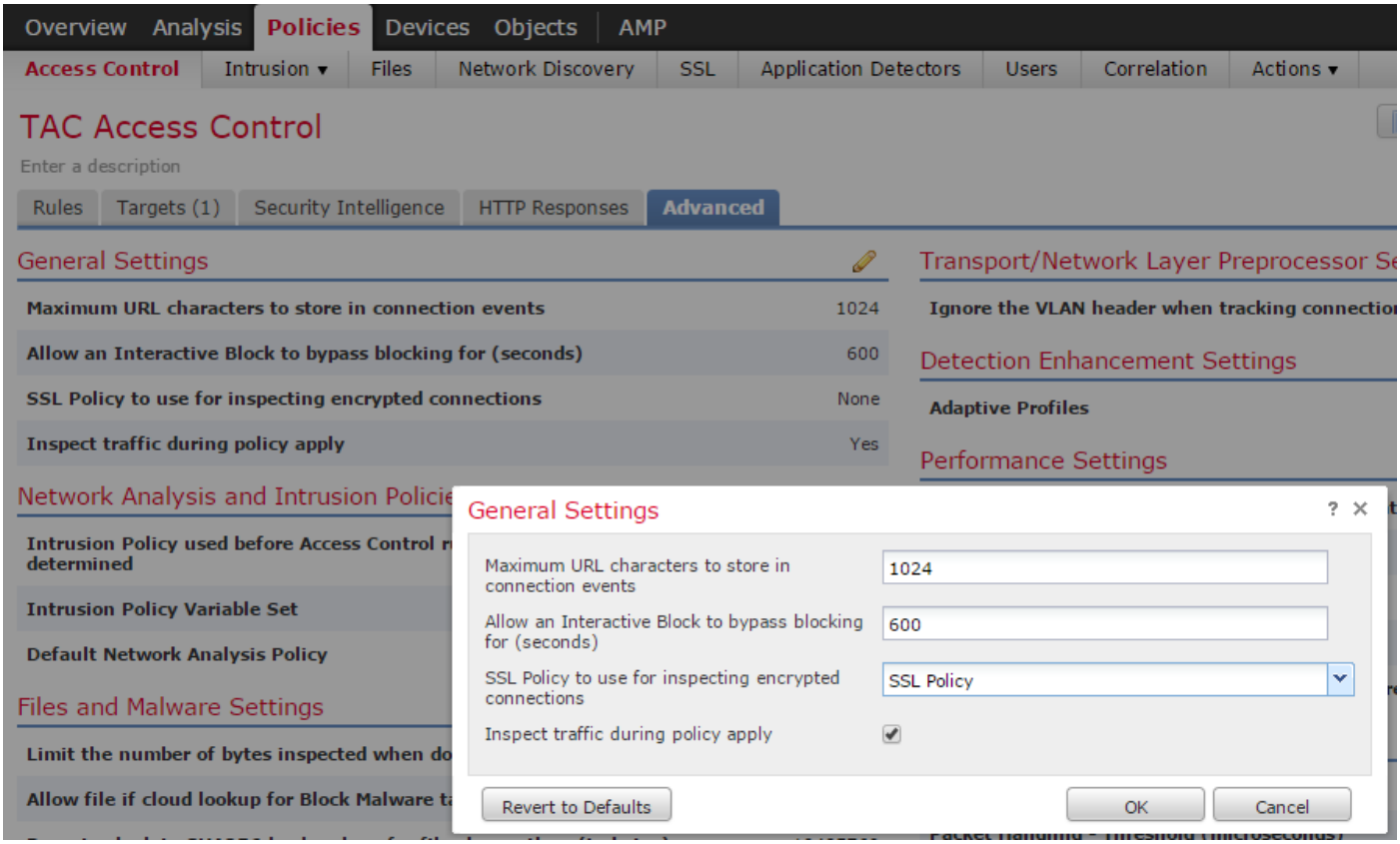
- **압축된 세션**:SSL 세션은 데이터 압축 방법을 적용합니다.
- **SSLv2 세션**:세션이 SSL 버전 2로 암호화됩니다. 클라이언트 hello 메시지가 SSL 2.0이고 전송된 트래픽의 나머지는 SSL 3.0인 경우 트래픽이 해독할 수 있습니다.
- **알 수 없는 암호 그룹**:시스템에서 암호 그룹을 인식하지 못합니다.
- **지원되지 않는 암호 그룹**:시스템은 탐지된 암호 그룹을 기반으로 암호 해독을 지원하지 않습니다.
- **세션이 캐시되지 않음**:SSL 세션에서 세션 재사용이 활성화되고, 클라이언트와 서버가 세션 식별자로 세션을 재설정했으며, 시스템이 해당 세션 식별자를 캐시하지 않았습니다.
- **핸드셰이크 오류**:SSL 핸드셰이크 협상 중 오류가 발생했습니다.
- **암호 해독 오류**:트래픽 암호 해독 중에 오류가 발생했습니다.

참고: 기본적으로 이러한 작업은 기본 작업을 상속합니다.기본 작업이 Block(차단)인 경우 예기치 않은 문제가 발생할 수 있습니다.

9. 정책을 저장합니다.

10. **정책 > 액세스 제어로 이동합니다**.정책을 수정하거나 새 액세스 제어 정책을 만듭니다.

11. **고급을** 클릭하고 **일반 설정**을 **편집합니다**.



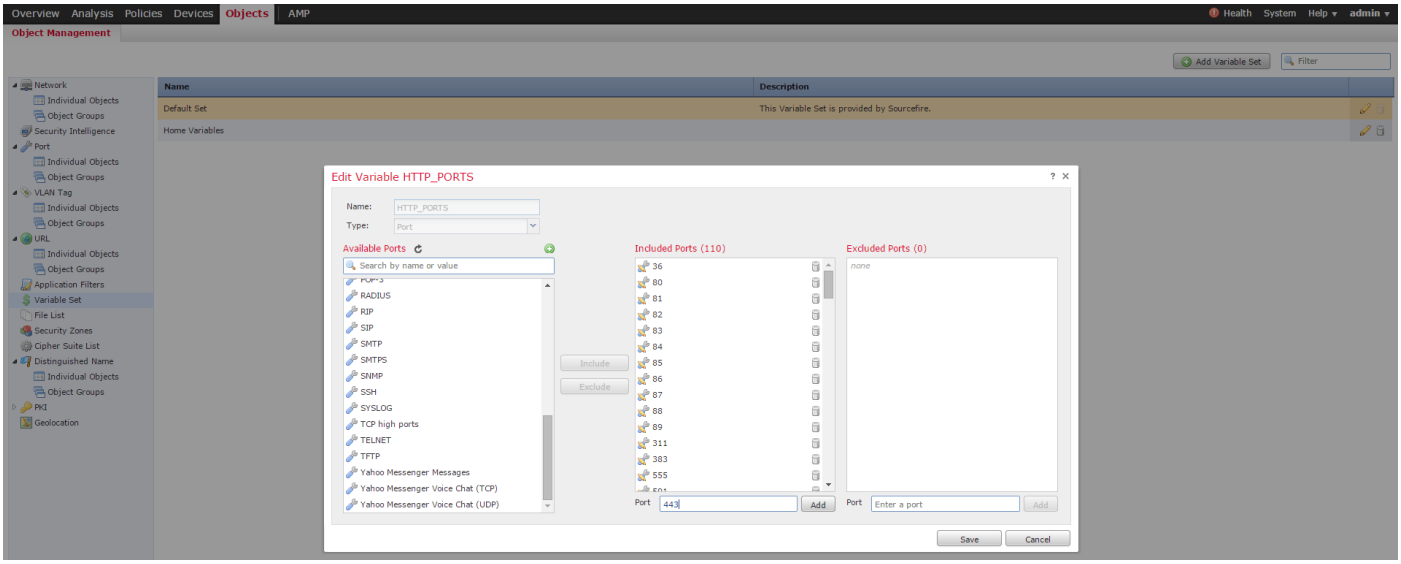
12. 드롭다운 메뉴에서 **SSL 정책**을 선택합니다.

13. **확인**을 클릭하여 저장합니다.

추가 구성

올바른 식별을 위해 침입 정책에 대해 다음 사항을 변경해야 합니다.

나.$HTTP_PORTS 변수에는 포트 443 및 정책에 의해 해독될 https 트래픽이 있는 기타 모든 포트가 포함되어야 합니다(**Objects > Object Management > Variable Set > Edit the variable set).**



2.암호화된 트래픽을 검사하는 네트워크 분석 정책에는 HTTP 프리프로세서 설정의 포트 필드에 포트 443(및 정책에 의해 해독될 https 트래픽이 있는 다른 포트)이 포함되어 있어야 합니다. 그렇지

않으면 http 콘텐츠 한정자를 사용하는 http 규칙(예: http_uri, http_header 등)이 트리거되지 않습니다. 이는 정의된 http 포트에서 정의되고 지정된 포트를 통해 이동하지 않는 트래픽에 대한 http 버퍼가 채워지지 않기 때문입니다.

3.(선택 사항이지만 더 나은 검사를 위해 권장) Perform Stream Reassembly on Both Ports 필드의 **TCP Stream Configuration 설정에 https 포트를** 추가합니다.

4.예약된 유지 관리 기간 동안 수정된 액세스 제어 정책을 다시 적용합니다.

> **경고:** 이 수정된 정책으로 인해 심각한 성능 문제가 발생할 수 있습니다.네트워크 중단 또는 성능에 대한 위험을 줄이려면 운영 시간 외에 테스트를 수행해야 합니다.

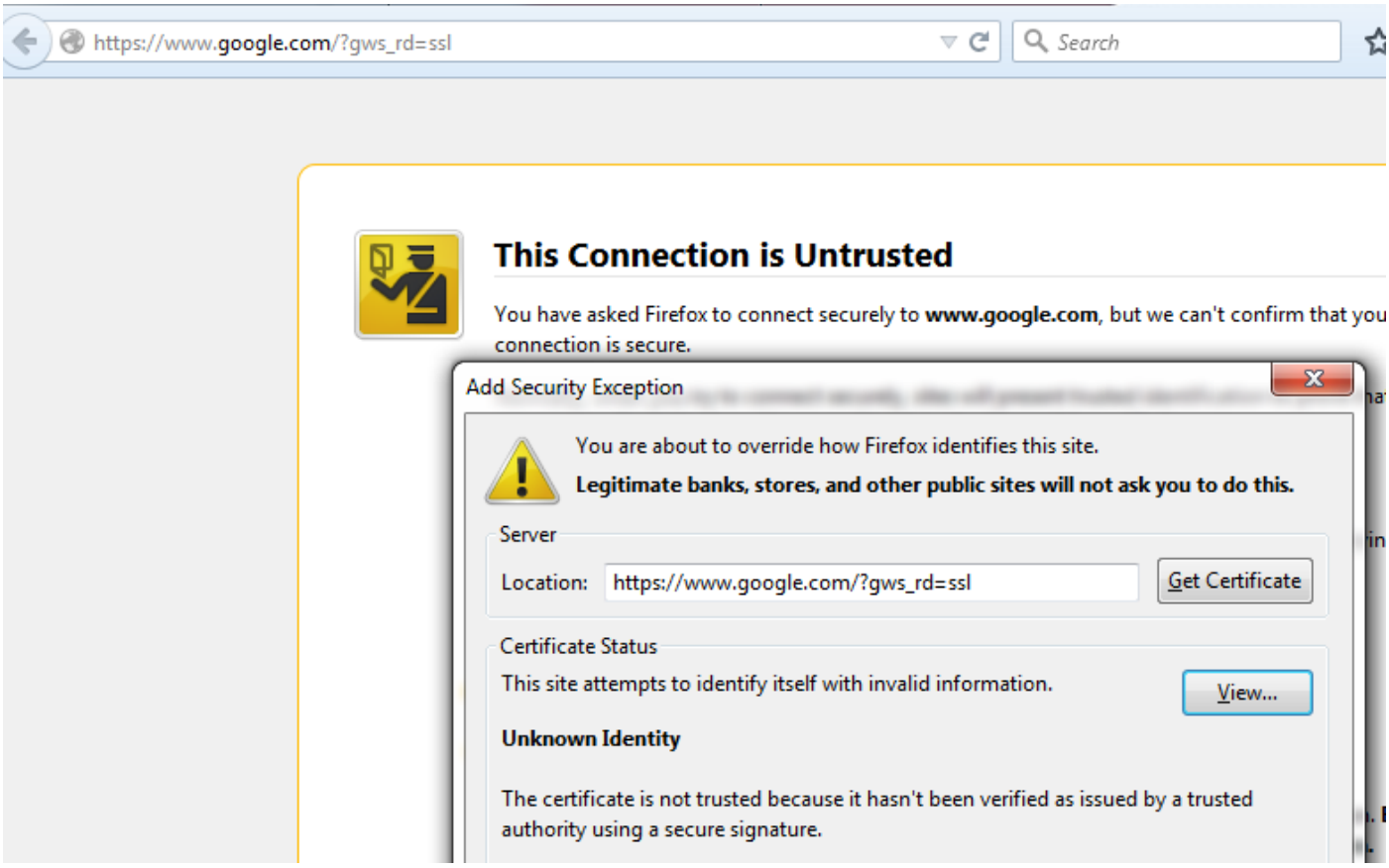
확인

암호 해독 - 사입

1. 웹 브라우저를 엽니다.

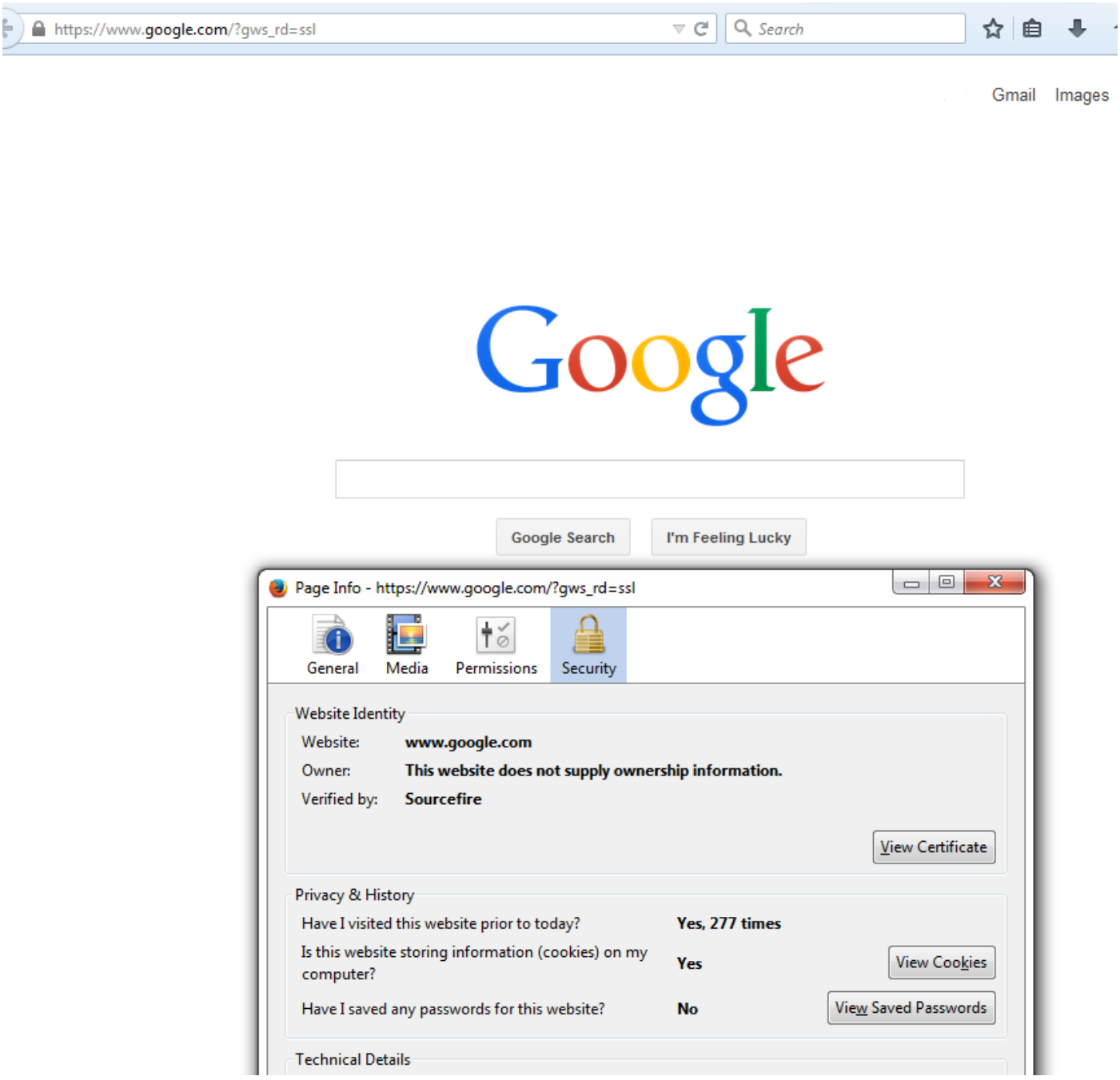
> **참고:** Firefox 브라우저는 아래 예에 사용됩니다. 이 예제는 Chrome에서 작동하지 않을 수 있습니다.자세한 내용은 문제 해결 섹션을 참조하십시오.

2. SSL 웹 사이트로 이동합니다.아래 예에서 https://www.google.com은 금융 기관의 웹 사이트도 사용할 것입니다.다음 페이지 중 하나가 표시됩니다.



> **참고:**인증서 자체가 신뢰되지 않고 서명 CA 인증서를 브라우저에서 신뢰하지 않는 경우 위의 페이지가 표시됩니다.브라우저에서 신뢰할 수 있는 CA 인증서를 결정하는 방법을 알아보려

면 아래 Trusted Certificate Authorities 섹션을 참조하십시오.



참고: 이 페이지가 표시되면 트래픽에 성공적으로 다시 서명했습니다.다음 섹션에서 **검증됨 :Sourcefire**.

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	www.google.com
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	13:E3:D5:7D:4E:5F:8F:E7

Issued By

Common Name (CN)	Sourcefire TAC
Organization (O)	Sourcefire
Organizational Unit (OU)	Tac

Period of Validity

Begins On	5/6/2015
Expires On	8/3/2015

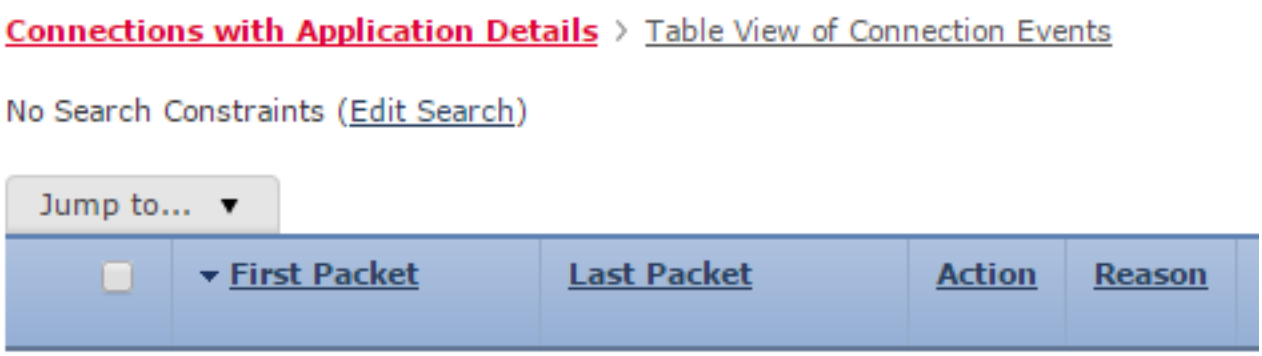
Fingerprints

SHA-256 Fingerprint	20:00:CB:25:13:8B:1F:89:4D:4A:CF:C5:E2:21:38:92: 06:66:00:2E:B7:83:27:72:98:EA:B1:6A:10:B3:67:A1
SHA1 Fingerprint	1B:C2:30:D9:66:84:DB:97:CF:A9:5E:5F:29:DA:4C:3F:13:E9:DE:5D

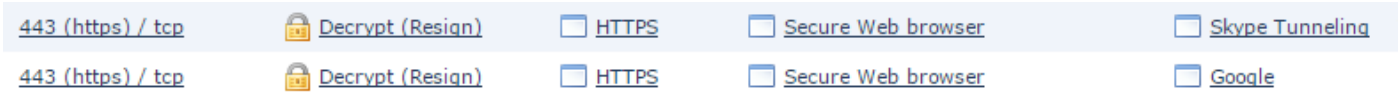
참고: 이것은 동일한 인증서를 자세히 살펴본 것입니다.

3. Management Center에서 **Analysis > Connections > Events로 이동합니다**.

4. 워크플로에 따라 SSL 암호 해독 옵션이 표시될 수도 있고 표시되지 않을 수도 있습니다.Table **View of Connection Events를 클릭합니다**.



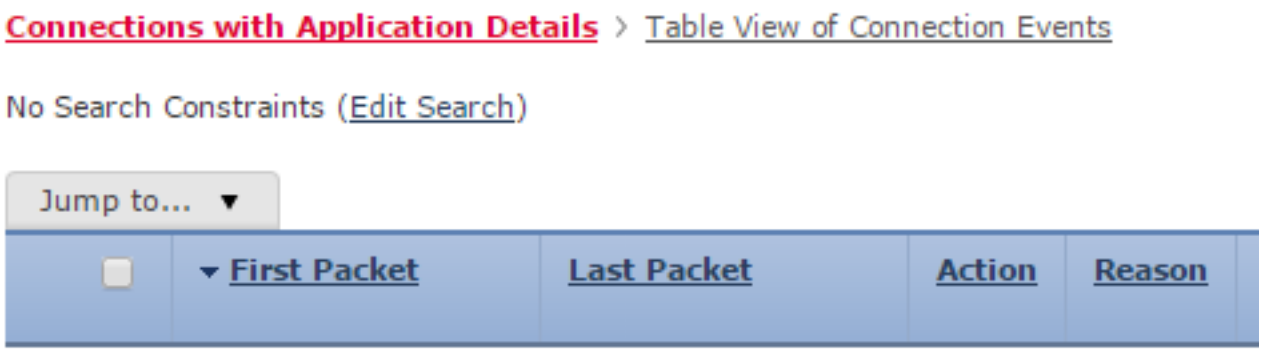
5. 오른쪽으로 스크롤하여 SSL 상태를 확인합니다.다음과 유사한 옵션이 표시됩니다.



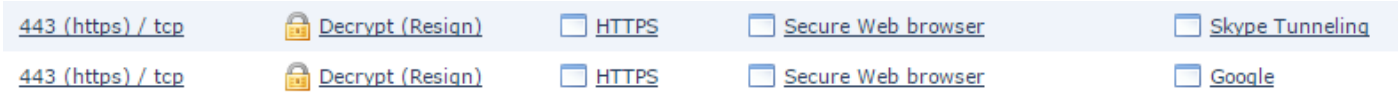
암호 해독 - 알려진 인증서

1. FireSIGHT Management Center에서 **Analysis > Connections > Events로 이동합니다**.

2. 워크플로에 따라 SSL 암호 해독 옵션이 표시되거나 표시되지 않을 수 있습니다.Table **View of Connection Events를 클릭합니다**.



3. 오른쪽으로 스크롤하여 SSL 상태를 확인합니다.다음과 유사한 옵션이 표시됩니다.



문제 해결

문제 1:일부 웹 사이트는 Chrome 브라우저에서 로드되지 않을 수 있습니다.

예

www.google.com은 Chrome을 사용하여 Decrypt - Resign으로 로드되지 않을 수 있습니다.

이유

Google Chrome 브라우저는 Google 속성에 대한 부정 인증서를 탐지하여 중간자 공격을 방지할 수 있습니다.Chrome 브라우저(클라이언트)가 google.com 도메인(서버)에 연결을 시도하며 유효한 Google 인증서가 아닌 인증서가 반환되면 브라우저는 연결을 거부합니다.

솔루션

이 경우 DN=*.google.com, *.gmail.com, *.youtube.com에 대한 **Do Not Decrypt(암호 해독 안 함)** 규칙을 추가합니다.그런 다음 브라우저 캐시와 기록을 지웁니다.

문제 2:일부 브라우저에서 신뢰할 수 없는 경고/오류를 가져오는 중

예

Internet Explorer 및 Chrome을 사용하여 사이트에 연결할 때 보안 경고가 표시되지 않지만 Firefox 브라우저를 사용할 경우 브라우저를 닫았다가 다시 열 때마다 연결을 신뢰해야 합니다.

이유

신뢰할 수 있는 CA 목록은 브라우저에 따라 다릅니다.인증서를 신뢰하는 경우 이는 브라우저 간에 전달되지 않으며 신뢰할 수 있는 항목은 일반적으로 브라우저가 열려 있는 동안에만 유지되므로, 인증서가 닫히면 신뢰할 수 있는 모든 인증서가 정리되고 다음에 브라우저를 열고 사이트를 방문할 때 신뢰할 수 있는 인증서 목록에 다시 추가해야 합니다.

솔루션

이 시나리오에서는 IE와 Chrome 모두 운영 체제에서 신뢰할 수 있는 CA 목록을 사용하지만 Firefox에서는 자체 목록을 유지합니다.따라서 CA 인증서를 OS 저장소로 가져왔지만 Firefox 브라우저로 가져오지 않았습니다.Firefox에서 보안 경고를 받지 않으려면 CA 인증서를 신뢰할 수 있는 CA로 브라우저에 가져와야 합니다.

신뢰할 수 있는 인증 기관

SSL 연결이 설정되면 브라우저에서 먼저 이 인증서가 신뢰되는지 확인합니다(즉, 이전에 이 사이트에 접속한 적이 있으며 브라우저에서 이 인증서를 신뢰하도록 수동으로 알리십시오). 인증서를 신뢰할 수 없는 경우 브라우저에서 이 사이트에 대한 인증서를 확인한 CA(Certificate Authority) 인증서를 확인합니다.브라우저에서 CA 인증서를 신뢰하는 경우 신뢰할 수 있는 인증서로 간주하여 연결을 허용합니다.CA 인증서를 신뢰할 수 없으면 브라우저에 보안 경고가 표시되고 인증서를 신뢰할 수 있는 인증서로 수동으로 추가해야 합니다.

브라우저의 신뢰할 수 있는 CA 목록은 브라우저의 구현에 전적으로 의존하며, 각 브라우저는 다른 브라우저와 달리 신뢰할 수 있는 목록을 채울 수 있습니다.일반적으로 현재 브라우저는 신뢰할 수 있는 CA 목록을 채우는 두 가지 방법을 사용합니다.

1. 운영 체제가 신뢰하는 신뢰할 수 있는 CA 목록을 사용합니다
2. 신뢰할 수 있는 CA 목록이 소프트웨어와 함께 제공되며 브라우저에 내장되어 있습니다.

가장 일반적인 브라우저의 경우 신뢰할 수 있는 CA는 다음과 같이 채워집니다.

- **Google Chrome**:운영 체제의 신뢰할 수 있는 CA 목록
- **Firefox**:자체 신뢰할 수 있는 CA 목록 유지
- **Internet Explorer**:운영 체제의 신뢰할 수 있는 CA 목록
- **Safari**:운영 체제의 신뢰할 수 있는 CA 목록

클라이언트에서 표시되는 동작은 이에 따라 달라지므로 차이점을 아는 것이 중요합니다.예를 들어, Chrome 및 IE용 신뢰할 수 있는 CA를 추가하려면 CA 인증서를 OS의 신뢰할 수 있는 CA 저장소로 가져와야 합니다.CA 인증서를 OS의 신뢰할 수 있는 CA 저장소로 가져오면 이 CA에서 서명한 인증서를 사용하여 사이트에 연결할 때 더 이상 경고가 표시되지 않습니다.Firefox 브라우저에서 CA 인증서를 브라우저 자체의 신뢰할 수 있는 CA 저장소로 수동으로 가져와야 합니다.이렇게 하면 해당 CA에서 확인한 사이트에 연결할 때 더 이상 보안 경고가 표시되지 않습니다.

참조

- SSL 규칙 시작