TLS/SSL 규칙 및 정책 예

이 장에서는 모범 사례 및 권장 사항을 따르는 TLS/SSL 규칙이 포함된 SSL 정책의 구체적인 예를 제공하기 위해 이 가이드에서 설명하는 개념을 기반으로 합니다. 조직의 요구에 맞게 조정하여 상황에 이 예를 적용할 수 있어야 합니다.

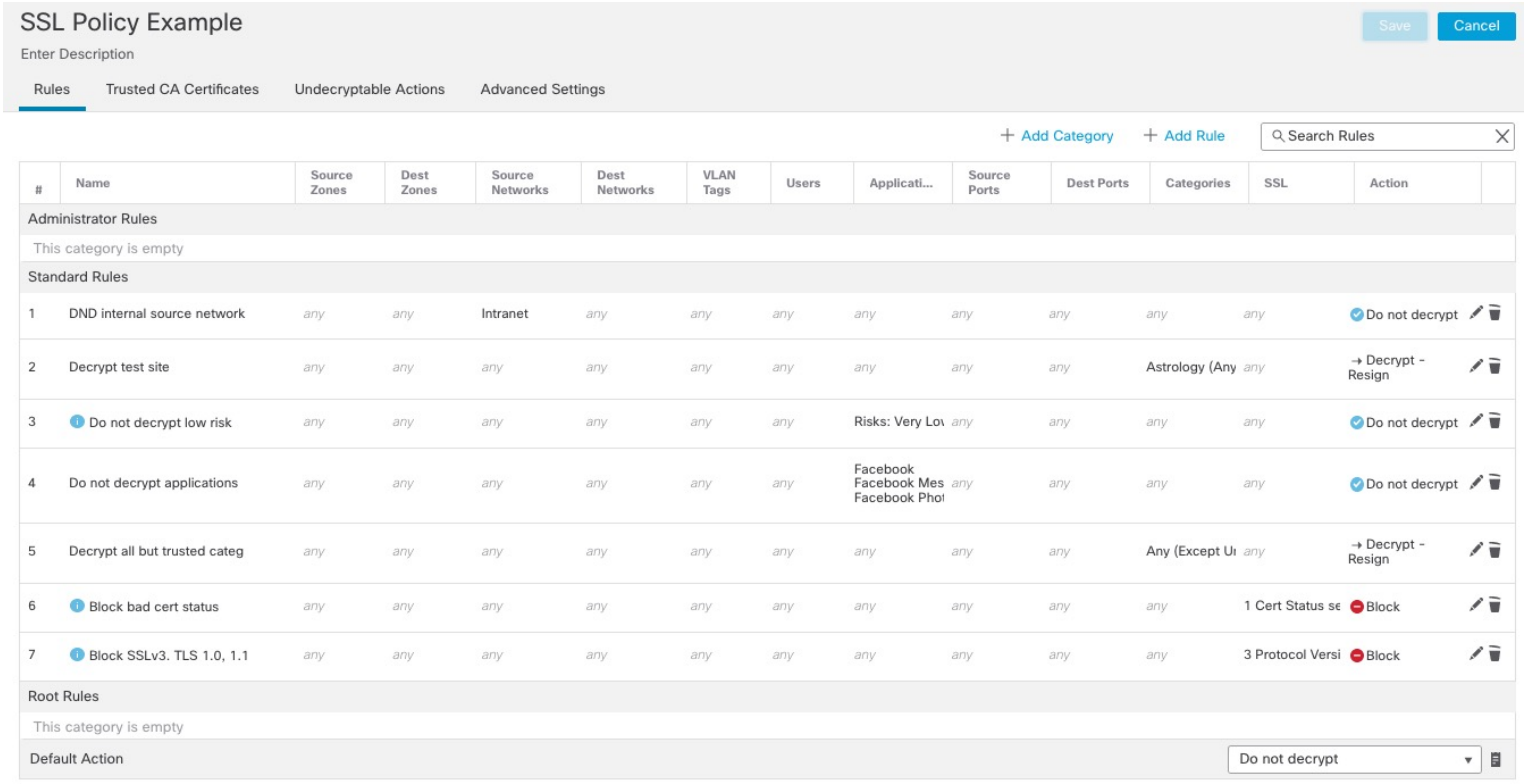
요약:

- 신뢰할 수 있는 트래픽(예: 대용량 압축 서버 백업 전송)의 경우 사전 필터링 및 플로우 오프로드를 사용하여 검사를 완전히 우회합니다.
- 특정 IP 주소에 적용되는 TLS/SSL 규칙과 같이 신속하게 평가할 수 있는 규칙을 먼저 배치합니다.
- 처리가 필요한 모든 TLS/SSL 규칙, **Decrypt - Resign(**암호 해독 - 다시 서명**)**규칙 및 안전하지 않은 프로토콜 버전 및 암호 그룹을 차단하는 규칙을 마지막에 배치합니다.

TLS/SSL 규칙 모범 사례

이 장에서는 모범 사례 및 권장 사항을 보여주는 TLS/SSL를 사용한 SSL 정책의 예를 제공합니다. 먼저 SSL 및 액세스 제어 정책에 대한 설정에 대해 설명한 다음 모든 규칙을 살펴보고 특정 방식으로 정렬하는 것이 권장되는 이유를 살펴보겠습니다.

다음은 이 장에서 다룰 SSL 정책입니다.



사전 필터 및 플로우 오프로드를 사용하여 검사 우회

사전 필터링은 시스템에서 더 많은 리소스를 사용하는 평가를 수행하기 전에 이루어지는 첫 번째 액세스 제어 단계입니다. 사전 필터링은 간단하고 빠르며 일찍 이루어집니다. 사전 필터링은 제한된 외부 헤더 기준을 사용하여 신속하게 트래픽을 처리합니다. 내부 헤더를 사용하며 검사 기능이 더 강력한 후속 평가와 사전 필터링을 비교해 보십시오.

다음 경우에 사전 필터링을 구성하십시오.

- 성능 향상 - 검사가 필요하지 않은 트래픽은 일찍 제외할수록 좋습니다. 캡슐화된 연결을 검사하지 않고 외부 캡슐화 헤더를 기반으로 특정 유형의 일반 텍스트, 패스스루 터널을 단축 경로 지정 또는 차단할 수 있습니다. 조기에 처리하는 것이 유리한 그 밖의 연결도 단축 경로를 지정하거나 차단할 수 있습니다.
- 캡슐화된 트래픽에 심층 검사 맞춤 설정 - 동일한 검사 기준을 사용하여 나중에 캡슐화된 연결을 처리할 수 있도록 특정 터널 유형의 영역을 다시 지정할 수 있습니다. 영역 재지정이 필요한 이유는 사전 필터링 후 액세스 제어가 내부 헤더를 사용하기 때문입니다.

Firepower 4100/9300를 사용 가능한 경우, 신뢰할 수 있는 트래픽이 더 나은 성능을 위해 검사 엔진을 우회할 수 있는 기술인 대규모 플로우 오프로드를 사용할 수 있습니다. 예를 들어 데이터 센터에서 서버 백업을 전송하는 데 사용할 수 있습니다.

관련 항목

대규모 플로우 오프로드

암호 해독 안 함 모범 사례

트래픽 로깅

아무것도 기록하지 않는 **Do Not Decrypt(**암호 해독 안 함**)** 규칙은 생성하지 않는 것이 좋습니다. 이러한 규칙은 매니지드 디바이스에서 여전히 처리에 시간이 걸리기 때문입니다. TLS/SSL 규칙 유형을 설정하는 경우 어떤 트래픽이 일치하는지 확인할 수 있도록 로깅을 활성화합니다.

해독 불가 트래픽에 대한 지침

웹사이트 자체를 해독할 수 없거나 웹사이트에서 SSL 피닝을 사용하여 사용자가 브라우저에서 오류 없이 해독된 사이트에 액세스하는 것을 효과적으로 방지하기 때문에 특정 트래픽을 해독할 수 없는 것으로 확인되었습니다.

인증서 피닝에 대한 자세한 내용은 TLS/SSL 피닝 정보의 내용을 참조하십시오.

이러한 사이트의 목록은 다음과 같이 유지 관리됩니다.

- **Cisco-Undecryptable-Sites**라는 DN(고유 이름) 그룹

트래픽을 암호 해독하고 이러한 사이트로 이동할 때 사용자의 브라우저에서 오류가 표시되지 않도록 하려면 TLS/SSL 규칙의 맨 아래에 **Do Not Decrypt(**암호 해독 안 함**)** 규칙을 설정하는 것이 좋습니다.

암호 해독 - 다시 서명 및 암호 해독 - 알려진 키 모범 사례

이 주제에서는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 및 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** TLS/SSL 규칙에 대한 모범 사례를 설명합니다.

암호 해독 - 다시 서명 모범 사례

인증서 피닝을 사용하는 애플리케이션에 대해 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙을 설정하는 경우 다음 모범 사례를 준수해야 합니다.

- 이러한 규칙을 모든 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙 앞에 배치합니다.
- 인증서 피닝에 대한 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙 작업을 해당 애플리케이션에 대한 요청이 시작되는 네트워크로 제한합니다(네트워크 규칙 조건).

인증서 피닝에 대한 자세한 내용은 Firepower Management Center 디바이스 구성 가이드SSL 피닝 섹션을 참조하십시오.

암호 해독 - 알려진 키 모범 사례

Decrypt - Known Key(암호 해독 - 알려진 키**)** 규칙 작업은 내부 서버로 이동하는 트래픽에 사용하기 위한 것이므로 항상 이러한 규칙에 대상 네트워크를 추가해야 합니다(네트워크 규칙 조건). 이렇게 하면 트래픽이 서버가 있는 네트워크로 직접 이동하므로 네트워크의 트래픽이 줄어듭니다.

우선 적용할 TLS/SSL 규칙

패킷의 첫 번째 부분과 일치할 수 있는 규칙을 먼저 배치합니다. IP 주소를 참조하는 규칙(네트워크 규칙 조건)을 예로 들 수 있습니다.

마지막에 추가할 TLS/SSL 규칙

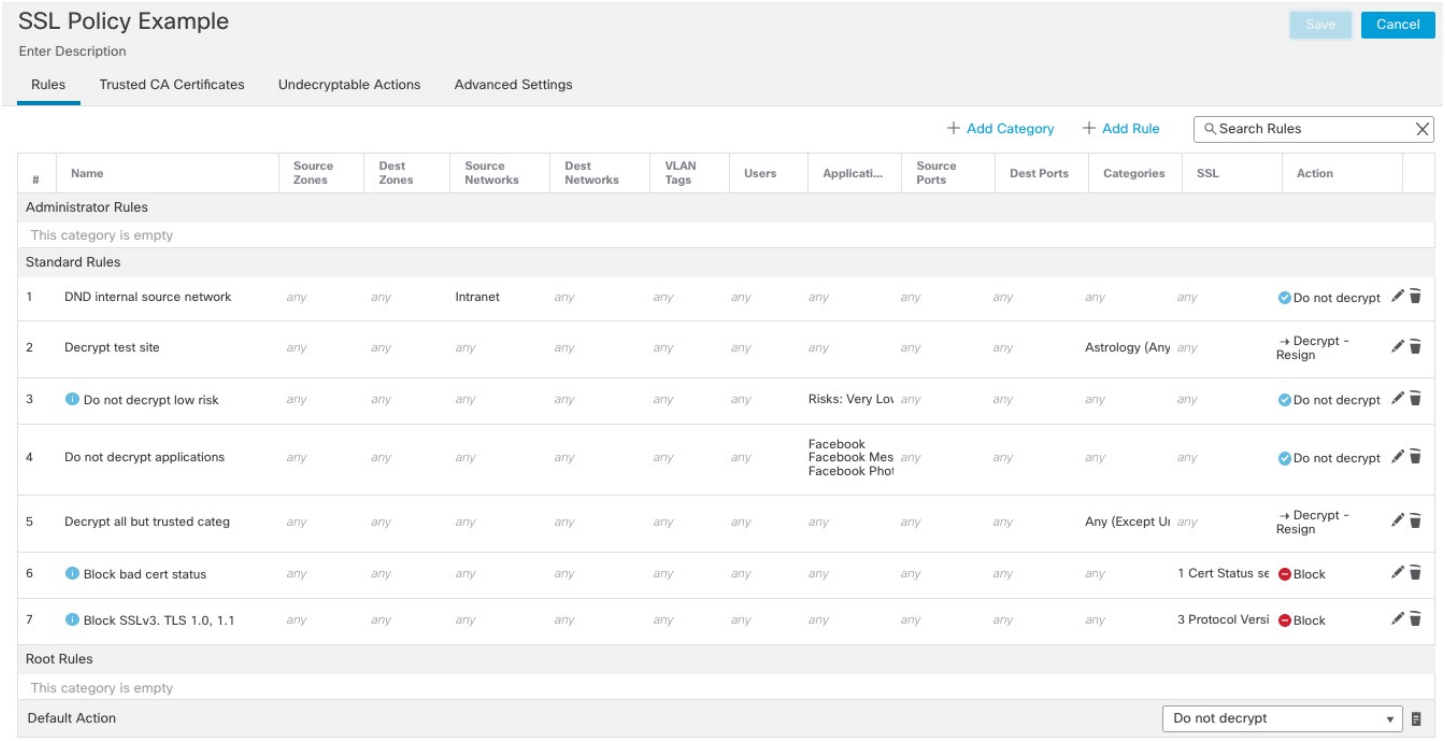
다음 규칙 조건이 있는 규칙은 시스템에서 가장 긴 시간 동안 트래픽을 검사해야 하므로 마지막 규칙이어야 합니다.

- 애플리케이션
- 카테고리
- 인증서
- 고유 이름(DN)
- 인증서 상태
- 암호 그룹
- 버전

SSL 정책 워크스루

이 장에서는 모범 사례를 사용하는 규칙을 사용하여 SSL 정책을 생성하는 방법을 단계별로 설명합니다. SSL 정책의 미리보기와 모범 사례의 개요, 그리고 정책의 규칙에 대한 설명이 차례로 표시됩니다.

다음은 이 장에서 다룰 SSL 정책입니다.



자세한 내용은 다음 섹션 중 하나를 참조하십시오.

관련 항목

권장 정책 및 규칙 설정, 5 페이지
사전 필터링할 트래픽, 9 페이지
첫 번째 TLS/SSL 규칙: 특정 트래픽 암호 해독 안 함, 9 페이지
다음 TLS/SSL 규칙: 특정 테스트 트래픽 암호 해독, 10 페이지
범주에 대한 암호 해독 - 다시 서명 규칙 생성, 13 페이지
낮은 위험 범주, 평판 또는 애플리케이션 암호 해독 안 함, 11 페이지
마지막 TLS/SSL 규칙: 인증서 및 프로토콜 버전 차단 또는 모니터링, 14 페이지

권장 정책 및 규칙 설정

다음 정책 설정을 사용하는 것이 좋습니다.

- SSL 정책:
  - 기본 작업 **Do not decrypt(**암호 해독 안 함**)**
  - 로깅을 활성화합니다.
  - **SSL v2 Session(SSL v2** 세션**)** 및 **Compressed Session(**압축 세션**)** 모두에 대해 **Undecryptable Actions(**암호 해독 불가 작업**)**를 **Block(**차단**)**으로 설정합니다.

- TLS/SSL 규칙: **Do Not Decrypt(**암호 해독 안 함**)** 규칙 작업이 있는 규칙을 제외한 모든 규칙에 대해 로깅을 활성화합니다. (이는 사용자가 결정합니다. 암호 해독되지 않은 트래픽에 대한 정보를 보려면 해당 규칙에 대한 로깅도 활성화합니다.)
- 액세스 제어 정책:
  - SSL 정책을 액세스 제어 정책에 연결합니다. (이 작업을 수행하지 않으면 SSL 정책 및 규칙이 적용되지 않습니다.)
  - 기본 정책 작업을 **Intrusion Prevention: Balanced Security and Connectivity(**침입 방지**:** 보안 및 연결의 균형**)**로 설정합니다.
  - 로깅을 활성화합니다.

관련 항목

SSL 정책 설정, 6 페이지
TLS/SSL 규칙 설정, 21 페이지
액세스 제어 정책 설정, 7 페이지

SSL 정책 설정

SSL 정책에 대해 권장되는 다음 모범 사례 설정을 구성하는 방법:

- 기본 작업 **Do not decrypt(**암호 해독 안 함**)**
- 로깅을 활성화합니다.
- **SSL v2 Session(SSL v2** 세션**)** 및 **Compressed Session(**압축 세션**)** 모두에 대해 **Undecryptable Actions(**암호 해독 불가 작업**)**를 **Block(**차단**)**으로 설정합니다.

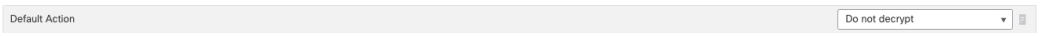
프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL** 버튼을 클릭합니다.

단계 **3** SSL 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** 페이지 하단의 **Default Action(**기본 작업**)** 목록에서 **Do Not Decrypt(**암호 해독 안 함**)**를 클릭합니다. 다음 그림은 예를 보여줍니다.



단계 **5** 행의 끝에서 **Logging(**로깅**)** ( )을 클릭합니다.

단계 **6** **Log at End of Connection(**연결 종료 시 로깅**)** 확인란을 선택합니다.

단계 **7** **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

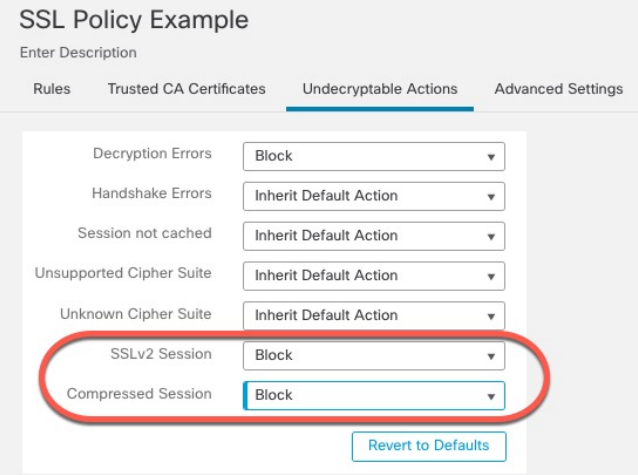
단계 **9** **Undecryptable Actions(**암호 해독할 수 없는 작업**)** 탭을 클릭합니다.

단계 **10** **SSLv2** 세션 및 압축된 세션에 대한 작업을 **Block(**차단**)**으로 설정하는 것이 좋습니다.

네트워크에서 SSL v2를 허용해서는 안 되며 압축된 TLS/SSL 트래픽은 지원되지 않으므로 해당 트래픽도 차단해야 합니다.

각 옵션 설정에 대한 자세한 내용은 Firepower Management Center 디바이스 구성 가이드참조하십시오.

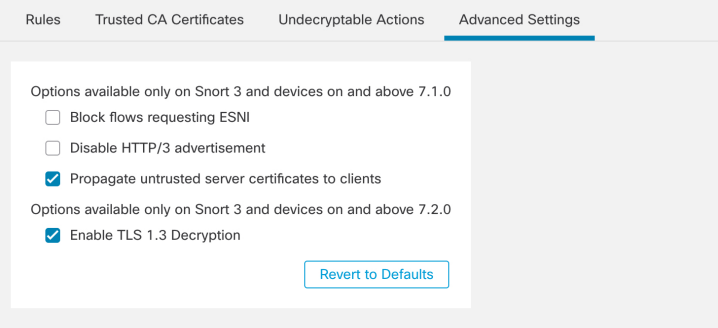
다음 그림은 예를 보여줍니다.



단계 **11** **Advanced Settings(**고급 설정**)** 탭 페이지를 클릭합니다.

단계 **12** **Enable TLS 1.3 Decryption(TLS 1.3** 암호 해독 활성화**)** 확인란을 선택합니다.

다음은 예입니다.



단계 **13** 페이지 상단에서 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

TLS/SSL 규칙을 구성하고 TLS/SSL 규칙 설정, 21 페이지에 설명된 대로 각 규칙을 설정합니다.

액세스 제어 정책 설정

액세스 제어 정책에 대해 권장되는 다음 모범 사례 설정을 구성하는 방법:

- SSL 정책을 액세스 제어 정책에 연결합니다. (이 작업을 수행하지 않으면 SSL 정책 및 규칙이 적용되지 않습니다.)
- 기본 정책 작업을 **Intrusion Prevention: Balanced Security and Connectivity(**침입 방지**:** 보안 및 연결의 균형**)**로 설정합니다.
- 로깅을 활성화합니다.

프로시저

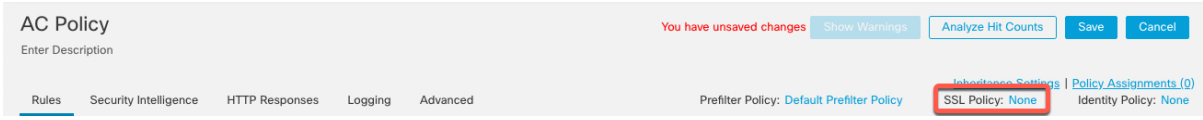
단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** 버튼을 클릭합니다.

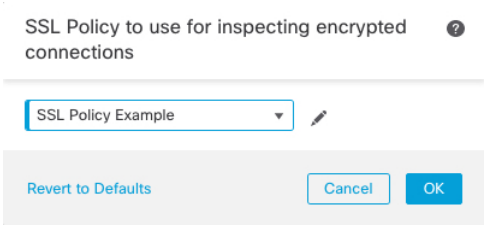
단계 **3** 액세스 제어 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** (SSL 정책이 아직 설정되지 않은 경우 나중에 이 작업을 수행할 수 있습니다.)

a) 다음 그림과 같이 페이지 상단의 **SSL Policy(SSL** 정책**)** 옆에 있는 **None(**없음**)**을 클릭합니다.



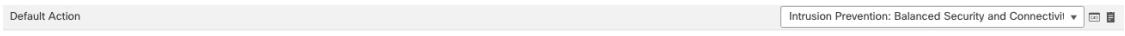
b) 목록에서 SSL 정책의 이름을 클릭합니다. 다음 그림은 예를 보여줍니다.



c) **OK(**확인**)**를 클릭합니다.

d) 페이지 상단에서 **Save(**저장**)**를 클릭합니다.

단계 **5** 페이지 하단의 **Default Action(**기본 작업**)** 목록에서 **Intrusion Prevention: Balanced Security and Connectivity(**침입 방지**:** 보안 및 연결의 균형**)**를 클릭합니다.
다음 그림은 예를 보여줍니다.



단계 **6** **Logging(**로깅**)** ( ) 버튼을 클릭합니다.

단계 **7** **Log at End of Connection(**연결 종료 시 로깅**)** 확인란을 선택하고 **OK(**확인**)**를 클릭합니다.

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

TLS/SSL 규칙 예시, 9 페이지의 내용을 참조하십시오.

TLS/SSL 규칙 예시

이 섹션에서는 모범 사례를 보여주는 TLS/SSL 규칙의 예를 제공합니다.

자세한 내용은 다음 섹션 중 하나를 참조하십시오.

관련 항목

사전 필터링할 트래픽, 9 페이지
첫 번째 TLS/SSL 규칙: 특정 트래픽 암호 해독 안 함, 9 페이지
다음 TLS/SSL 규칙: 특정 테스트 트래픽 암호 해독, 10 페이지
낮은 위험 범주, 평판 또는 애플리케이션 암호 해독 안 함, 11 페이지
범주에 대한 암호 해독 - 다시 서명 규칙 생성, 13 페이지
마지막 TLS/SSL 규칙: 인증서 및 프로토콜 버전 차단 또는 모니터링, 14 페이지

사전 필터링할 트래픽

사전 필터링은 시스템에서 더 많은 리소스를 사용하는 평가를 수행하기 전에 이루어지는 첫 번째 액세스 제어 단계입니다. 사전 필터링은 내부 헤더를 사용하며 검사 기능이 더 강력한 후속 평가에 비해 간단하고 빠르며 조기에 수행됩니다.

보안 요구 사항 및 트래픽 프로파일에 따라 사전 필터링을 고려하여 다음을 모든 정책 및 검사에서 제외해야 합니다.

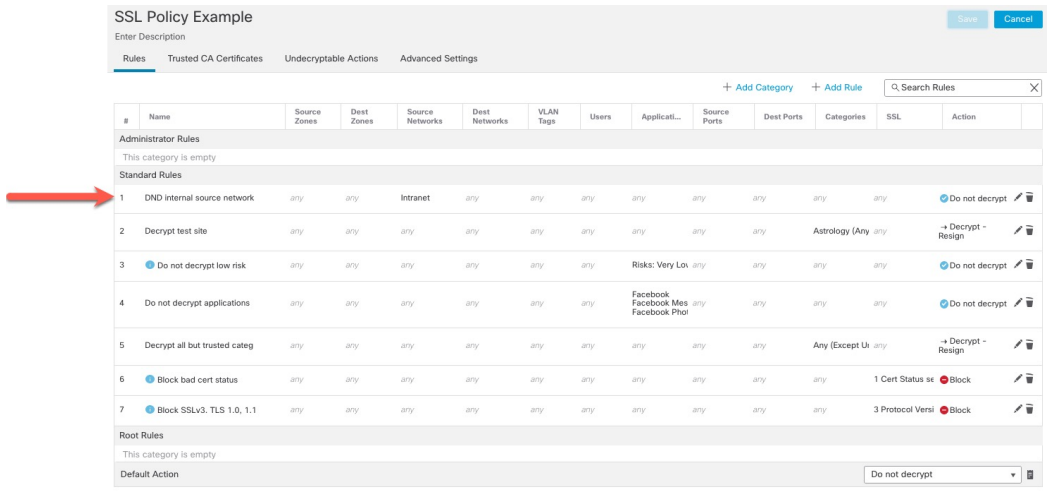
- Microsoft Outlook 365와 같은 일반적인 사내 애플리케이션
- Elephant 플로우(예: 서버 백업)

관련 항목

사전 필터링 및 액세스 제어 비교
사전 필터링 모범 사례

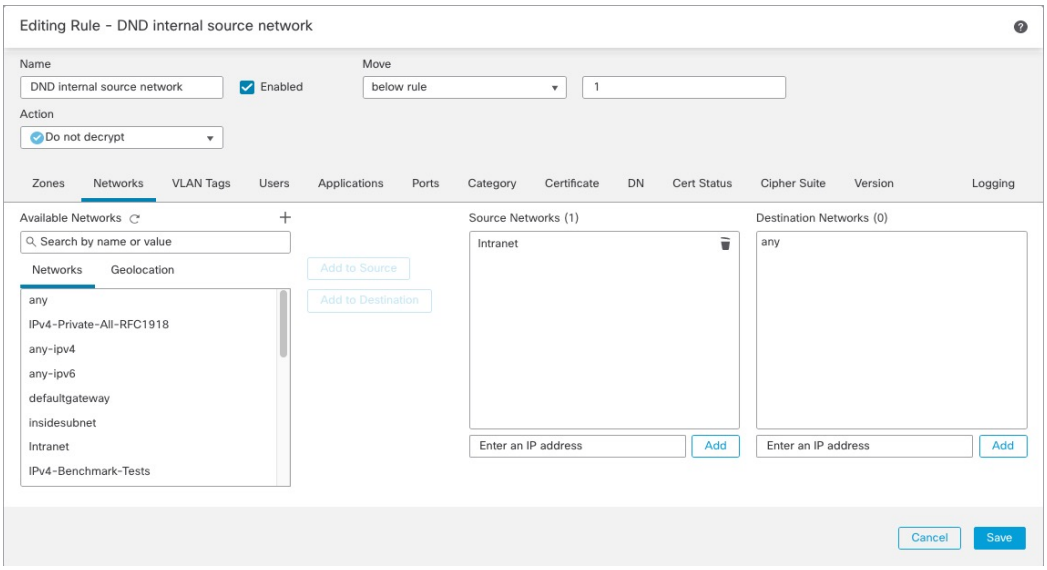
첫 번째 TLS/SSL 규칙: 특정 트래픽 암호 해독 안 함

이 예의 첫 번째 TLS/SSL 규칙은 내부 네트워크(**intranet**로 정의)로 이동하는 트래픽을 암호 해독하지 않습니다. **Do Not Decrypt(**암호 해독 안 함**)** 규칙 작업은 ClientHello 중에 일치하므로 매우 빠르게 처리됩니다.



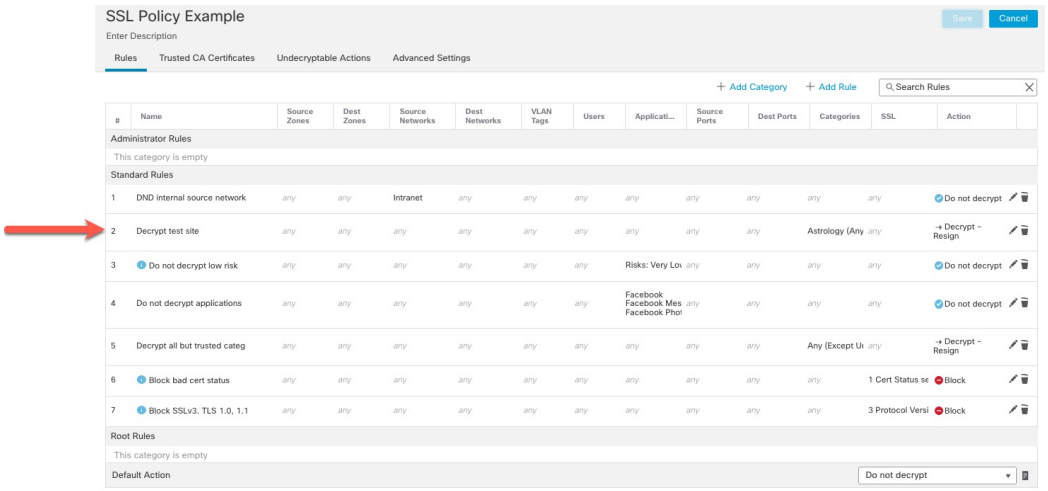
참고 내부 DNS 서버에서 내부 DNS 확인자(예: Cisco Umbrella 가상 어플라이언스)로 이동하는 트래픽이 있는 경우 여기에도 **Do Not Decrypt(**암호 해독 안 함**)** 규칙을 추가할 수 있습니다. 내부 DNS 서버가 자체 로깅을 수행하는 경우 사전 필터링 정책에 추가할 수도 있습니다.

그러나 인터넷 루트 서버(예: Active Directory에 내장된 Microsoft 내부 DNS 확인자)와 같이 인터넷으로 이동하는 DNS 트래픽에는 **Do Not Decrypt(**암호 해독 안 함**)** 규칙 또는 사전 필터링을 사용하지 않는 것이 좋습니다. 이러한 경우에는 트래픽을 완전히 검사하거나 차단을 고려해야 합니다.

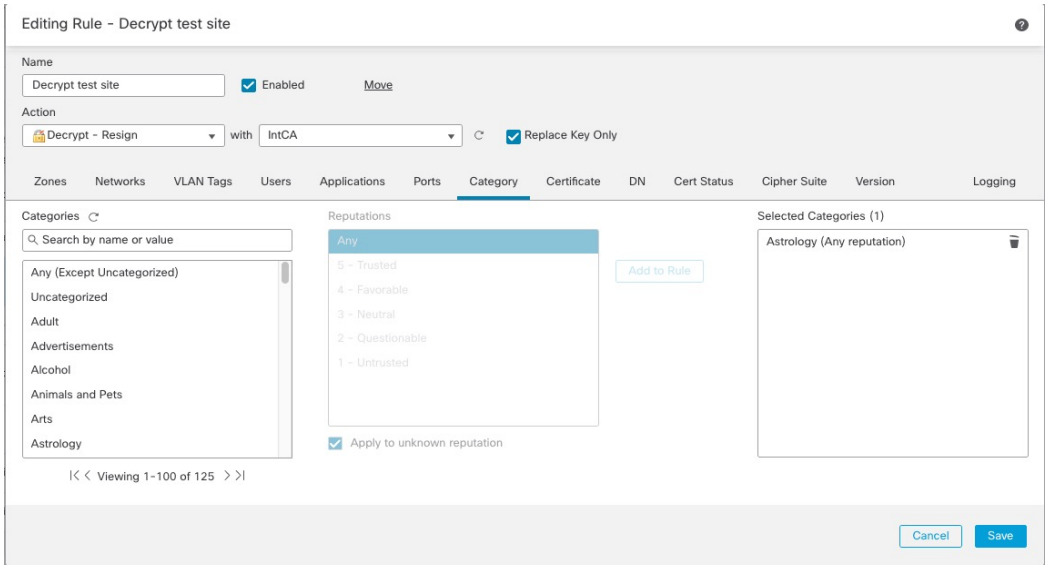


다음 TLS/SSL 규칙: 특정 테스트 트래픽 암호 해독

다음 규칙은 이 예에서 선택 사항입니다. 이를 사용하여 네트워크에서 허용할지 여부를 결정하기 전에 제한된 유형의 트래픽을 해독하고 모니터링합니다.



규칙 세부사항:

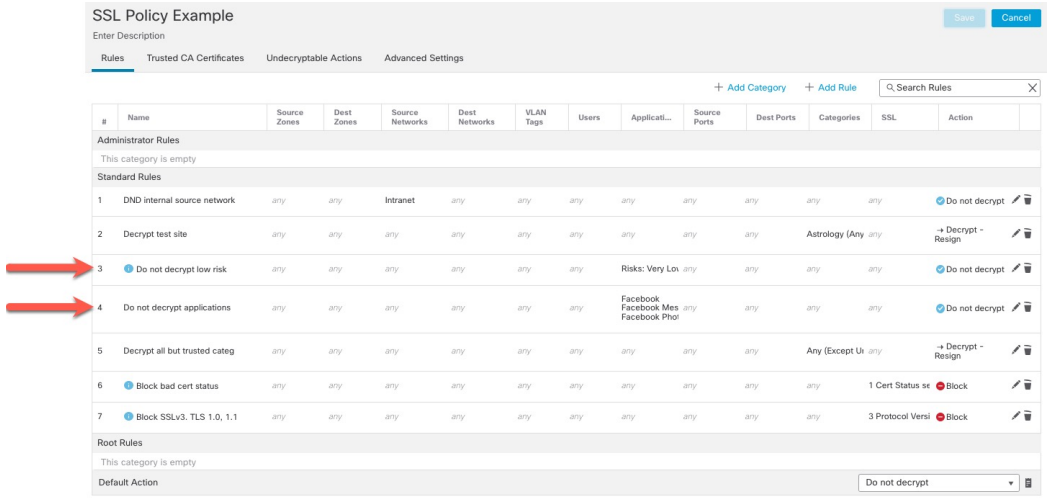


낮은 위험 범주, 평판 또는 애플리케이션 암호 해독 안 함

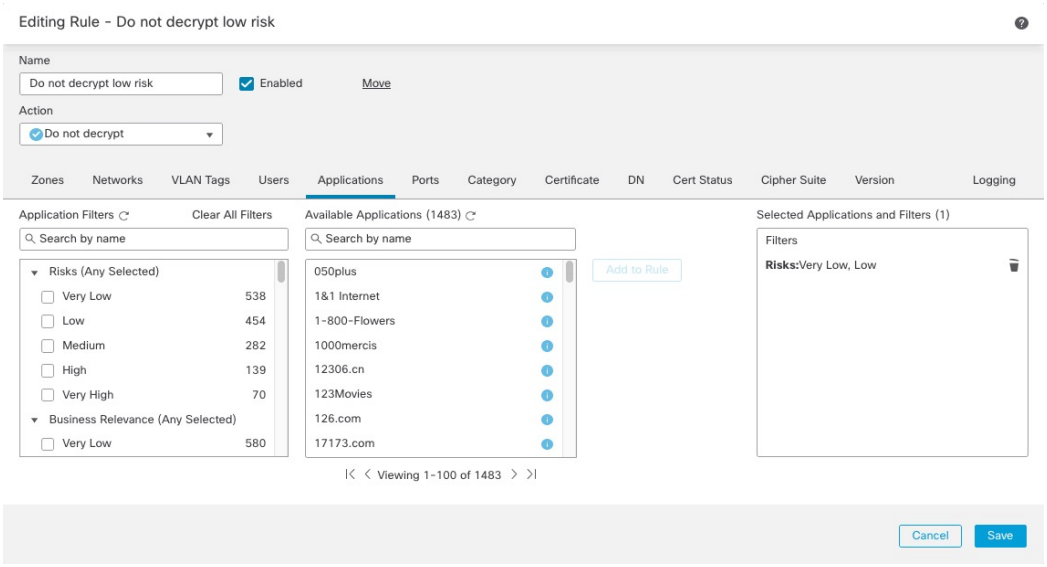
네트워크의 트래픽을 평가하여 어떤 것이 낮은 위험 범주, 평판 또는 애플리케이션과 일치하는지 확인하고 **Do Not Decrypt(**암호 해독 안 함**)** 작업으로 해당 규칙을 추가합니다. 시스템이 트래픽을 처리하는 데 더 많은 시간이 필요하므로 이러한 규칙은 더 구체적인 **Do Not Decrypt(**암호 해독 안 함**)** 규칙 뒤에 배치합니다.

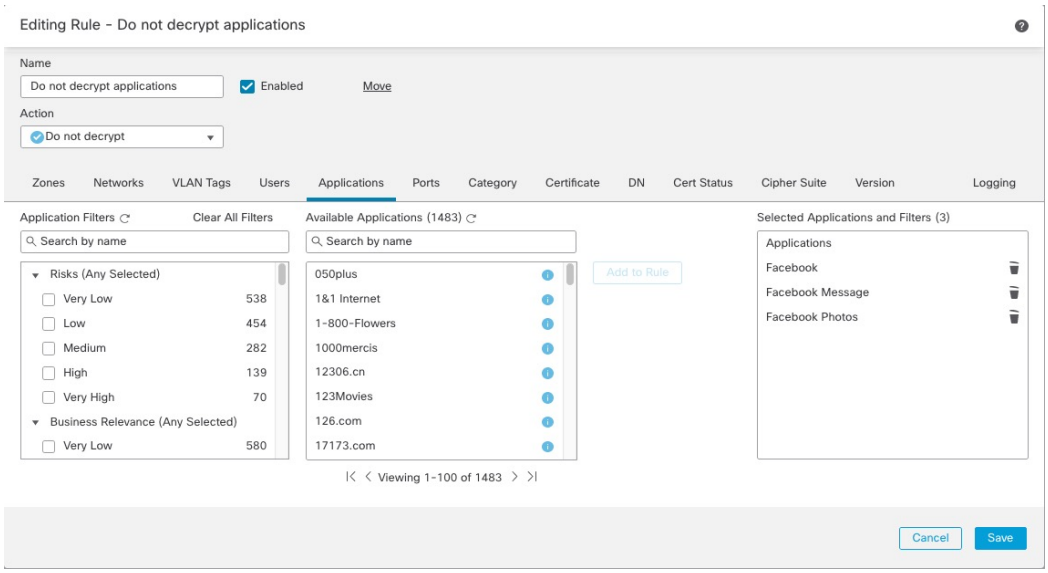
다음은 그 예입니다.

낮은 위험 범주, 평판 또는 애플리케이션 암호 해독 안 함



규칙 세부사항:





관련 항목

애플리케이션 제어 구성 모범 사례
애플리케이션 제어 권장 사항

범주에 대한 암호 해독 - 다시 서명 규칙 생성

이 주제에서는 분류되지 않은 모든 사이트에 대해 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업이 포함된 TLS/SSL 규칙을 생성하는 예를 보여줍니다. 이 규칙은 선택 사항인 **Replace Key Only(**키만 교체**)** 옵션을 사용하며, 이는 항상 **Decrypt-Resign(**암호 해독-재서명**)** 규칙 작업과 함께 권장됩니다.

키 교체만은 사용자가 자체 서명 인증서를 사용하는 사이트를 탐색할 때 웹 브라우저에 보안 경고가 표시되므로 사용자가 안전하지 않은 사이트와 통신하고 있음을 알 수 있습니다.

이 규칙을 맨 아래에 배치하면 두 가지 이점을 모두 누릴 수 있습니다. 정책의 이전에 규칙을 배치한 것처럼 성능에 영향을 미치지 않으면서 트래픽을 암호 해독하고 선택적으로 검사할 수 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** 아직 하지 않았다면 내부 CA(인증 기관)를 Firepower Management Center(**Objects(**개체**)** > **Object Management(**개체 관리**)**, **PKI** > 내부 **CA**)에 업로드합니다.

단계 **3** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL** 버튼을 클릭합니다.

단계 **4** SSL 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** **Add Rule(**규칙 추가**)**을 클릭합니다.

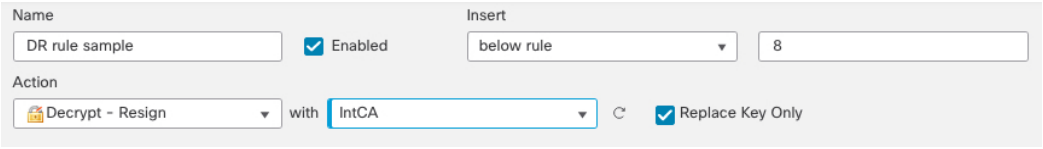
단계 **6** **Name(**이름**)** 필드에 규칙을 식별하는 이름을 입력합니다.

단계 **7** **Action(**작업**)** 목록에서 **Decrypt - Resign(**암호 해독 - 재서명**)**을 클릭합니다.

단계 **8** **with(**포함**)** 목록에서 내부 CA의 이름을 클릭합니다.

단계 **9** **Replace Key Only(**키만 교체**)** 상자를 선택합니다.

다음 그림은 예를 보여줍니다.



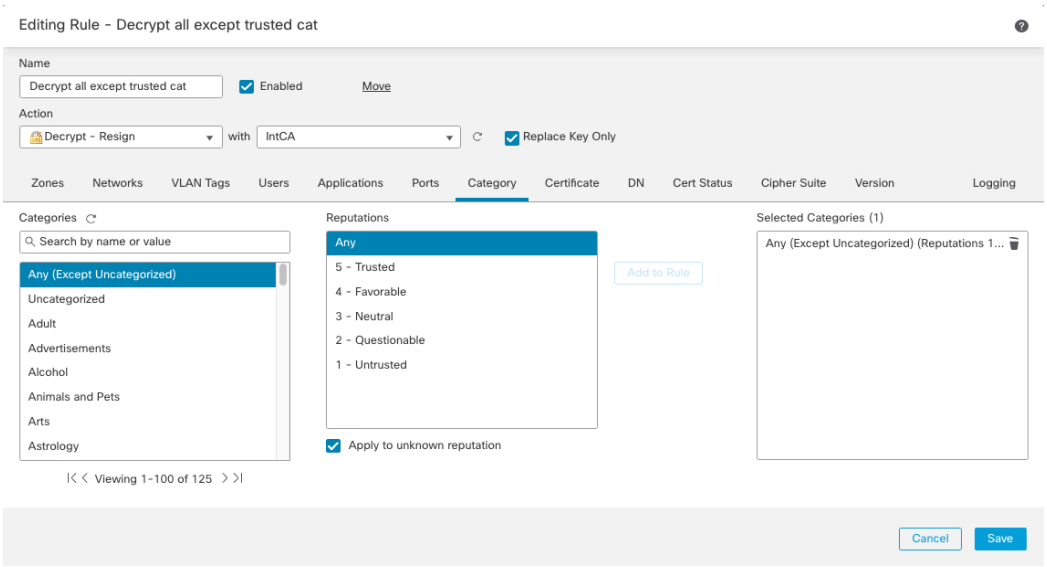
단계 **10** **Category(**범주**)** 탭 페이지를 클릭합니다.

단계 **11** **Categories(**범주**)** 목록의 상단에서 **Any (Except Uncategorized)(**모두**(**미분류 제외**))**를 클릭합니다.

단계 **12** **Reputations(**평판**)** 목록에서 **Any(**모두**)**를 클릭합니다.

단계 **13** **Add to Rule(**규칙에 추가**)**을 클릭합니다.

다음 그림은 예를 보여줍니다.

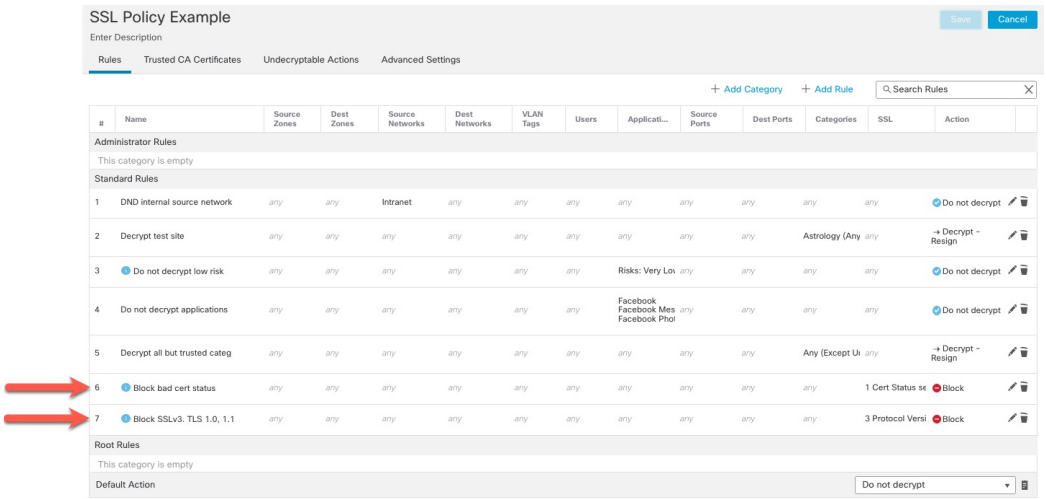


관련 항목

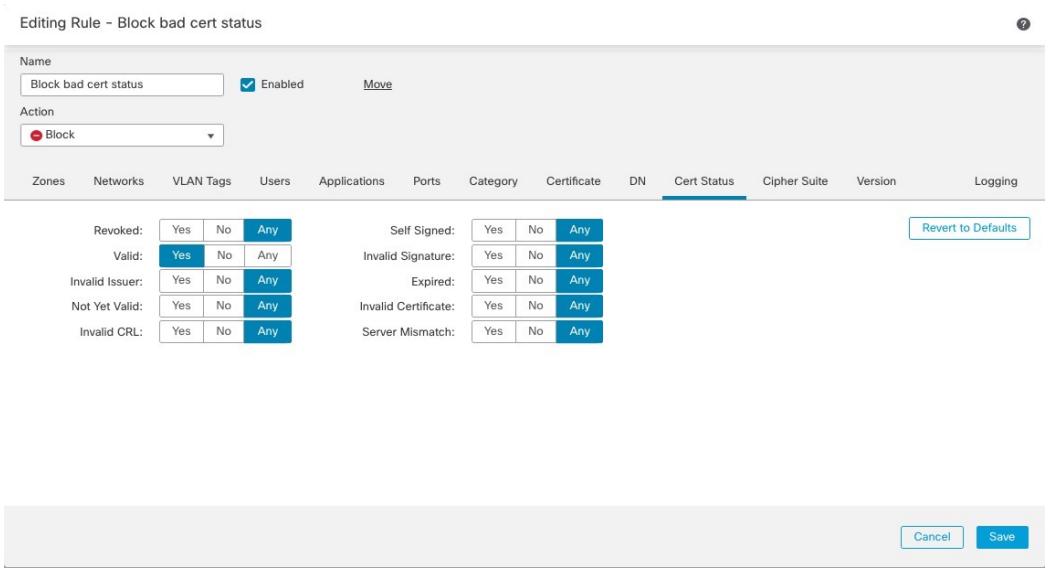
내부 인증 기관 개체

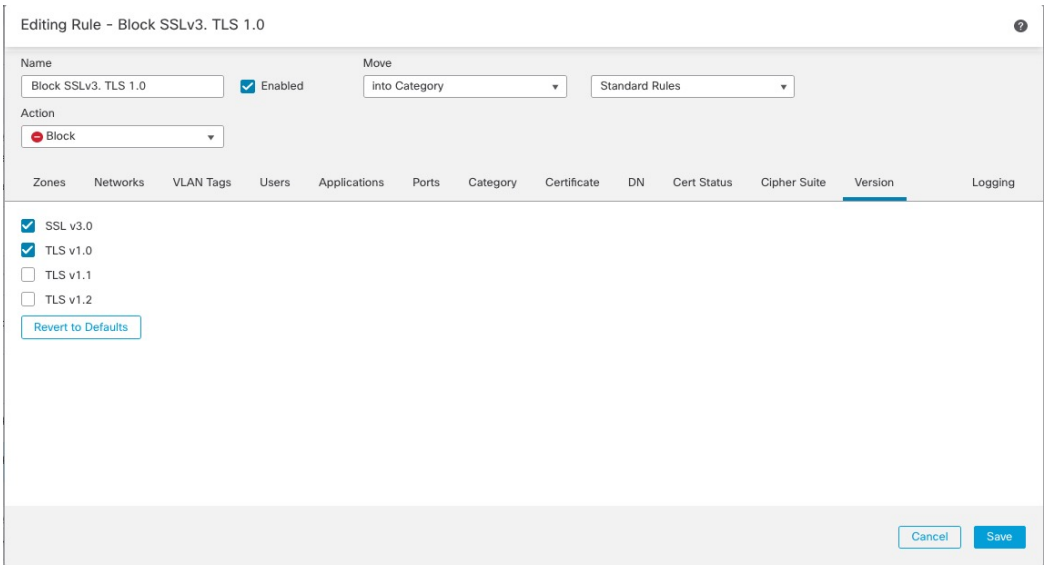
마지막 TLS/SSL 규칙: 인증서 및 프로토콜 버전 차단 또는 모니터링

마지막 TLS/SSL 규칙은 가장 구체적이고 가장 많은 처리를 필요로 하기 때문에 잘못된 인증서 및 안전하지 않은 프로토콜 버전을 모니터링하거나 차단하는 규칙입니다.


SSL Policy Example
Enter Description
Save
Cancel
Rules
Trusted CA Certificates
Undecryptable Actions
Advanced Settings
Add Category
Add Rule
Search Rules
Name Source Zones Dest Zones Source Networks Dest Networks VLAN Tags Users Applicati... Source Ports Dest Ports Categories SSL Action
Administrator Rules
This category is empty
Standard Rules
1 DND internal source network Intranet Do not decrypt
2 Decrypt test site Astrology (Any → Decrypt - Resign
3 Do not decrypt low risk Risks: Very Lo Do not decrypt
4 Do not decrypt applications Facebook Facebook Mes Facebook Phot Do not decrypt
5 Decrypt all but trusted categ Any (Except U → Decrypt - Resign
6 Block bad cert status 1 Cert Status se Block
7 Block SSLv3. TLS 1.0, 1.1 3 Protocol Versi Block
Root Rules
This category is empty
Default Action
Do not decrypt

규칙 세부사항:


Editing Rule - Block bad cert status
Name
Block bad cert status
Enabled
Move
Action
Block
Zones Networks VLAN Tags Users Applications Ports Category Certificate DN Cert Status Cipher Suite Version Logging
Revoked: Yes No Any
Valid: Yes No Any
Invalid Issuer: Yes No Any
Not Yet Valid: Yes No Any
Invalid CRL: Yes No Any
Self Signed: Yes No Any
Invalid Signature: Yes No Any
Expired: Yes No Any
Invalid Certificate: Yes No Any
Server Mismatch: Yes No Any
Revert to Defaults
Cancel
Save



관련 항목

예: 인증서 상태 모니터링 또는 차단 TLS/SSL 규칙, 16 페이지
예: 프로토콜 버전 모니터링 또는 차단 TLS/SSL 규칙, 18 페이지
선택적 예: 인증서 고유 이름을 모니터링 또는 차단 TLS/SSL 규칙, 19 페이지

예: 인증서 상태 모니터링 또는 차단 TLS/SSL 규칙

마지막 TLS/SSL 규칙은 가장 구체적이고 가장 많은 처리를 필요로 하기 때문에 잘못된 인증서 및 안전하지 않은 프로토콜 버전을 모니터링하거나 차단하는 규칙입니다. 이 섹션의 예에서는 인증서 상태별로 트래픽을 모니터링하거나 차단하는 방법을 보여줍니다.

참고 **Block(**차단**)**또는 **Block with reset(**차단 후 재설정**)**규칙 작업이 있는 규칙에서만 암호 그룹 및 버전규칙 조건을 사용합니다. 다른 규칙 작업과 함께 규칙에서 이러한 조건을 사용하면 시스템의 ClientHello 처리를 방해하여 예기치 않은 성능이 발생할 수 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL** 버튼을 클릭합니다.

단계 **3** SSL 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** TLS/SSL 규칙 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **6** Add Rule(규칙 추가) 대화 상자에서 **Name(**이름**)** 필드에 다이얼 규칙 이름을 입력합니다.

단계 **7** **Cert Status(**인증서 상태**)**를 클릭합니다.

단계 **8** 각 인증서 상태에는 다음과 같은 옵션이 있습니다.

- 해당 인증서 상태가 있는 경우에 매칭하려면 **Yes**를 클릭합니다.
- 해당 인증서 상태가 없는 경우에 매칭하려면 **No**를 클릭합니다.
- 규칙을 매칭할 때 조건을 건너뛰려면 **Any(모두)**를 클릭합니다. 다시 말해 **Any(모두)**를 선택하면 인증서 상태가 있건 없건 규칙이 매칭됩니다.

단계 **9** **Action(작업)** 목록에서 **Monitor(모니터링)**를 클릭하여 규칙과 일치하는 트래픽만 모니터링하고 로깅하거나 **Block(차단)** 또는 **Block with Reset(차단 후 재설정)**을 클릭하여 트래픽을 차단하고 선택적으로 연결을 재설정합니다.

단계 **10** 규칙에 대한 변경 사항을 저장하려면 페이지 하단에서 **Save(저장)**를 클릭합니다.

단계 **11** 정책에 대한 변경 사항을 저장하려면 페이지 상단에서 **Save(저장)**를 클릭합니다.

예

조직에서는 Verified Authority 인증 기관을 신뢰합니다. 조직에서는 Spammer Authority 인증 기관을 신뢰하지 않습니다. 시스템 관리자가 Verified Authority 인증서 및 Verified Authority에서 발급한 중간 CA 인증서를 시스템에 업로드합니다. Verified Authority가 이전에 발급한 인증서를 취소했으므로 시스템 관리자는 Verified Authority가 제공한 CRL을 업로드합니다.

다음 그림에는 유효한 인증서를 확인하는 인증서 상태 규칙 조건이 나와 있습니다. 이러한 인증서는 Verified Authority에서 발급하였으며, CRL에 포함되지 않고, 유효 시작일과 유효 만료일 사이의 기간이 아직 남아 있는 상태입니다. 이러한 인증서로 암호화된 트래픽은 컨피그레이션으로 인해, 액세스 제어를 통해 해독 및 검사되지 않습니다.

Revoked:	Yes	No	**Any**	Self Signed:	Yes	No	**Any**
Valid:	**Yes**	No	Any	Invalid Signature:	Yes	No	**Any**
Invalid Issuer:	Yes	No	**Any**	Expired:	Yes	No	**Any**
Not Yet Valid:	Yes	No	**Any**	Invalid Certificate:	Yes	No	**Any**
Invalid CRL:	Yes	No	**Any**	Server Mismatch:	Yes	No	**Any**

다음 그림에는 상태가 없는지 확인하는 인증서 상태 규칙 조건이 나와 있습니다. 이 경우 컨피그레이션으로 인해, 만료되지 않은 인증서로 암호화된 트래픽과 매칭을 수행하며 해당 트래픽을 모니터링합니다.

Revoked:	Yes	No	**Any**	Self Signed:	Yes	No	**Any**
Valid:	Yes	No	**Any**	Invalid Signature:	Yes	No	**Any**
Invalid Issuer:	Yes	No	**Any**	Expired:	Yes	**No**	Any
Not Yet Valid:	Yes	No	**Any**	Invalid Certificate:	Yes	No	**Any**
Invalid CRL:	Yes	No	**Any**	Server Mismatch:	Yes	No	**Any**

다음 예에서는 수신 트래픽이 유효하지 않은 발급자가 있고, 자체 서명되고, 만료되고, 유효하지 않은 인증서를 사용하는 경우 이 규칙 조건과 일치합니다.

Revoked:	Yes	No	**Any**	Self Signed:	**Yes**	No	Any
Valid:	Yes	**No**	Any	Invalid Signature:	Yes	No	**Any**
Invalid Issuer:	**Yes**	No	Any	Expired:	**Yes**	No	Any
Not Yet Valid:	Yes	No	**Any**	Invalid Certificate:	Yes	No	**Any**
Invalid CRL:	Yes	No	**Any**	Server Mismatch:	Yes	No	**Any**

다음 그래픽은 요청의 SNI가 서버 이름과 일치하거나 CRL이 유효하지 않은 경우에 일치하는 인증서 상태 규칙 조건을 보여줍니다.

Revoked:	Yes	No	**Any**	Self Signed:	Yes	No	**Any**
Valid:	Yes	No	**Any**	Invalid Signature:	Yes	No	**Any**
Invalid Issuer:	Yes	No	**Any**	Expired:	Yes	No	**Any**
Not Yet Valid:	Yes	No	**Any**	Invalid Certificate:	Yes	No	**Any**
Invalid CRL:	**Yes**	No	Any	Server Mismatch:	**Yes**	No	Any

예: 프로토콜 버전 모니터링 또는 차단 TLS/SSL 규칙

이 예에서는 TLS 1.0, TLS 1.1 및 SSLv3 같은, 더 이상 안전하지 않은 것으로 간주되는 TLS 및 SSL 프로토콜을 네트워크에서 차단하는 방법을 보여줍니다. 여기에는 프로토콜 버전 규칙의 작동 방식에 대한 자세한 정보가 포함되어 있습니다.

모든 비보안 프로토콜은 악용 가능하기 때문에 네트워크에서 제외해야 합니다. 이 예에서는 다음을 수행합니다.

- SSL 규칙의 **Version(**버전**)** 페이지를 사용하여 일부 프로토콜을 차단할 수 있습니다.
- Firepower 시스템은 SSLv2르 해독 불가로 간주하기 때문에, SSL 정책에 대한 **Undecryptable Actions(**해독 불가 작업**)**을 사용하여 차단할 수 있습니다.
- 마찬가지로, 압축 TLS/SSL은 지원되지 않으므로 차단해야 합니다.

참고 **Block(**차단**)**또는 **Block with reset(**차단 후 재설정**)**규칙 작업이 있는 규칙에서만 암호 그룹 및 버전규칙 조건을 사용합니다. 다른 규칙 작업과 함께 규칙에서 이러한 조건을 사용하면 시스템의 ClientHello 처리를 방해하여 예기치 않은 성능이 발생할 수 있습니다.

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 2 **Policies(정책)** > **Access Control(액세스 제어)** > **SSL** 버튼을 클릭합니다.

단계 3 SSL 정책 옆에 있는 **Edit(수정)** ( )을 클릭합니다.

단계 4 TLS/SSL 규칙 옆에 있는 **Edit(수정)** ( )을 클릭합니다.

단계 5 **Add Rule(규칙 추가)**을 클릭합니다.

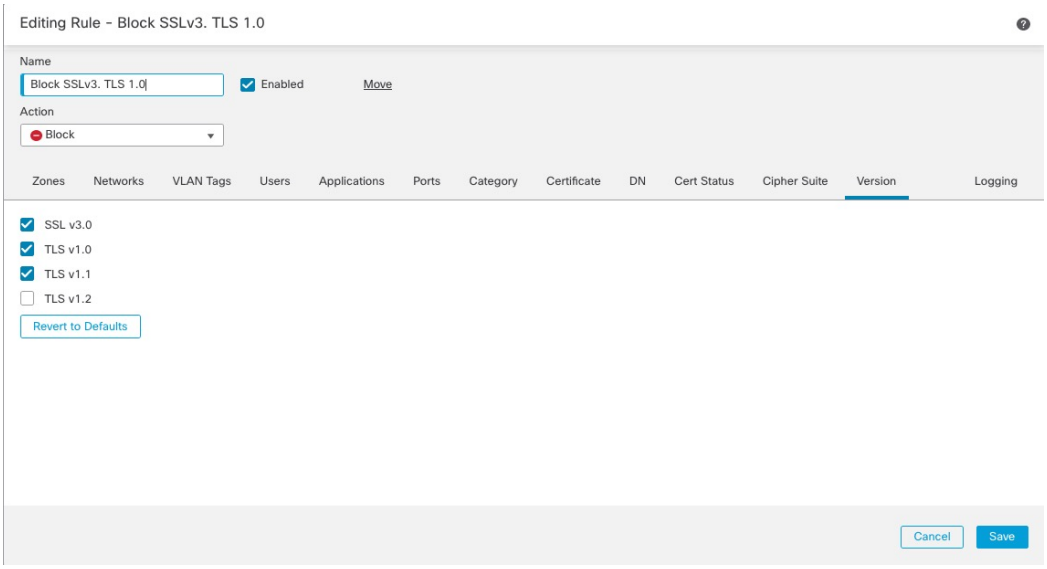
단계 6 Add Rule(규칙 추가) 대화 상자에서 **Name(이름)** 필드에 다이얼 규칙 이름을 입력합니다.

단계 7 **Action(작업)** 목록에서 **Block(차단)** 또는 **Block with reset(차단 후 재설정)**을 클릭합니다.

단계 8 **Version(버전)** 페이지를 클릭합니다.

단계 9 **SSL v3.0**, **TLS 1.0**, **TLS 1.1** 같은 더 이상 안전하지 않은 프로토콜의 확인란을 선택합니다. 안전한 것으로 간주되는 프로토콜의 확인란은 선택 취소합니다.

다음 그림은 예를 보여줍니다.



단계 10 필요에 따라 다른 규칙 조건을 선택합니다.

단계 11 **Save(저장)**를 클릭합니다.

선택적 예: 인증서 고유 이름을 모니터링 또는 차단 TLS/SSL 규칙

이 규칙은 서버 인증서의 고유 이름(Distinguished Name)을 기준으로 트래픽을 모니터링하거나 차단하는 방법에 대한 아이디어를 제공합니다. 좀 더 자세한 정보를 제공하기 위해 포함되었습니다.

고유 이름은 국가 코드, 일반 이름, 조직 및 조직 단위로 구성될 수 있지만 일반적으로 공용 이름으로만 구성됩니다. 예를 들어 `https://www.cisco.com`에 대한 인증서의 공통 이름은 `cisco.com`입니다. (그러나 항상 간단한 것은 아닙니다. 고유 이름(DN) 규칙 조건의 고유 이름 규칙 조건 섹션에서 일반 이름을 찾는 방법을 확인할 수 있습니다.)

클라이언트 요청에서 URL의 호스트 이름 부분은 SNI(Server Name Indication)입니다. 클라이언트는 TLS 핸드셰이크에서 SNI 확장을 사용하여 연결할 호스트 이름(예: `auth.amp.cisco.com`)을 지정합니

다. 그런 다음 서버는 단일 IP 주소에서 모든 인증서를 호스팅하는 동안 연결을 설정하는 데 필요한 해당 개인 키 및 인증서 체인을 선택합니다.

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL** 버튼을 클릭합니다.

단계 **3** SSL 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** TLS/SSL 규칙 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **6** Add Rule(규칙 추가) 대화 상자에서 **Name(**이름**)** 필드에 다이얼 규칙 이름을 입력합니다.

단계 **7** **Action(**작업**)** 목록에서 **Block(**차단**)** 또는 **Block with reset(**차단 후 재설정**)**을 클릭합니다.

단계 **8** **DN**을 클릭합니다.

단계 **9** **Available DNs(**사용 가능한 **DN)**에서 추가할 고유 이름을 다음과 같이 찾습니다.

- 고유 이름(DN) 개체를 즉시 추가한 다음 조건에 추가하려면 **Available DNs(**사용 가능한 **DN)** 목록 위의 **Add(**추가**)** ( )을 클릭합니다.
- 추가할 고유 이름(DN) 개체 및 그룹을 검색하려면, **Available DNs(**사용 가능한 **DN)** 목록 위의 **Search by name or value(**이름 또는 값으로 검색**)** 프롬프트를 클릭한 다음 개체의 이름을 입력하거나, 개체의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 개체를 표시합니다.

단계 **10** 개체를 선택하려면 이를 클릭합니다. 모든 개체를 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **11** **Add to Subject(**주체에 추가**)** 또는 **Add to Issuer(**발급자에 추가**)**를 클릭합니다.

팁 선택한 영역을 끌어서 놓을 수도 있습니다.

단계 **12** 수동으로 지정할 리터럴 공용 이름(CN) 또는 고유 이름(DN)을 추가합니다. **Subject DNs(**주체 **DN)** 또는 **Issuer DNs(**발급자 **DN)** 목록 아래의 **Enter DN or CN(DN** 또는 **CN** 입력**)** 프롬프트를 클릭한 다음, 공용 이름(CN) 또는 고유 이름(DN)을 입력하고 **Add(**추가**)**를 클릭합니다.

두 목록 중 하나에 CN 또는 DN을 추가할 수 있지만, **Subject DNs(**주체 **DN)** 목록에 추가하는 것이 더 일반적입니다.

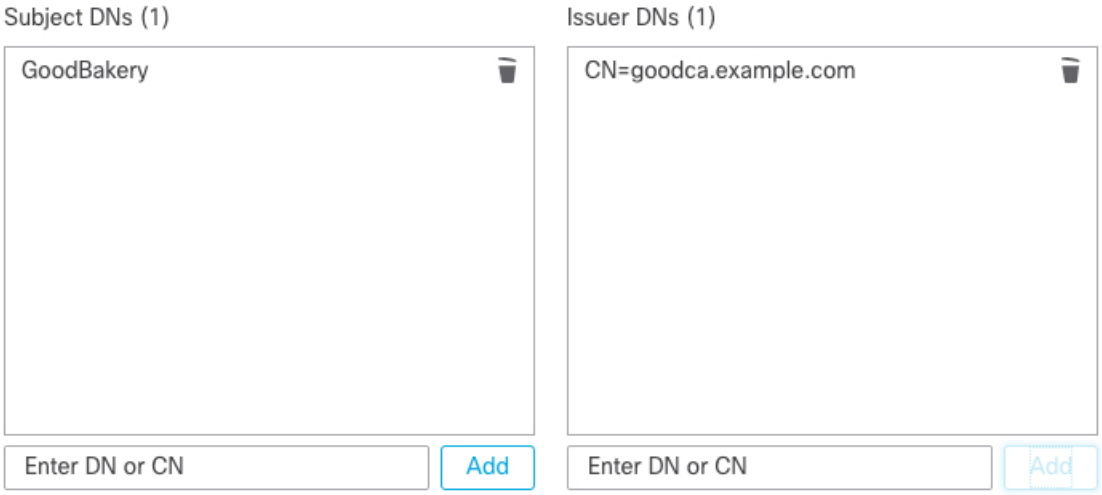
단계 **13** 규칙을 추가하거나 계속 수정합니다.

단계 **14** 완료되면 규칙에 대한 변경 사항을 저장하려면 페이지 하단에서 **Save(**저장**)**를 클릭합니다.

단계 **15** 정책에 대한 변경 사항을 저장하려면 페이지 상단에서 **Save(**저장**)**를 클릭합니다.

예

다음 그림에는 goodbakery.example.com에 발급되었거나 goodca.example.com에서 발급한 인증서를 검색하는 고유 이름(DN) 규칙이 나와 있습니다. 이러한 인증서로 암호화된 트래픽은 허용되며 액세스 제어 규칙의 대상이 됩니다.



TLS/SSL 규칙 설정

TLS/SSL 규칙에 대한 권장 모범 사례 설정을 구성하는 방법입니다.

TLS/SSL 규칙: **Do Not Decrypt(**암호 해독 안 함**)** 규칙 작업이 있는 규칙을 제외한 모든 규칙에 대해 로깅을 활성화합니다. (이는 사용자가 결정합니다. 암호 해독되지 않은 트래픽에 대한 정보를 보려면 해당 규칙에 대한 로깅도 활성화합니다.)

프로시저

단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL** 버튼을 클릭합니다.

단계 **3** SSL 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** TLS/SSL 규칙 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **5** **Logging(**로깅**)** 탭을 클릭합니다.

단계 **6** **Log at End of Connection(**연결 종료 시 로깅**)**을 클릭합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

단계 **8** 페이지 맨 위에서 **Save**를 클릭합니다.