TLS/SSL 규칙을 사용한 암호 해독 조정

다음 주제에서는 TLS/SSL 조건 규칙을 구성하는 방법의 개요를 설명합니다.

TLS/SSL 규칙 조건 개요

기본적인 TLS/SSL 규칙은 디바이스에서 검사하는 모든 암호화된 트래픽에 해당 규칙 작업을 적용합니다. 암호화된 트래픽의 제어 및 해독을 개선하기 위해, 특정 유형의 트래픽을 처리하고 로깅하도록 규칙 조건을 구성할 수 있습니다. 각 TLS/SSL 규칙에는 0개, 1개 또는 그 이상의 규칙 조건이 포함될 수 있습니다. 트래픽이 해당 TLS/SSL 규칙의 모든 조건과 일치하는 경우에만 규칙이 트래픽과 일치합니다.

참고 트래픽이 규칙과 일치하면 디바이스는 구성된 규칙 작업을 트래픽에 적용합니다. 트래픽 로깅이 구성되어 있는 경우, 연결이 종료될 때 디바이스는 트래픽을 로깅합니다.

각 규칙 조건을 사용하면 매칭하려는 트래픽의 속성을 하나 이상 지정할 수 있으며, 이러한 속성에는 다음에 대한 세부 정보가 포함됩니다.

- 트래픽이 이동할 때 통과하는 보안 영역, IP 주소 및 포트, 원본 또는 대상 국가, 원본 또는 대상 VLAN을 포함한 트래픽의 흐름.
- 탐지된 IP 주소에 연결된 사용자.
- 트래픽에서 탐지된 애플리케이션을 포함한 트래픽 페이로드.
- 연결을 암호화하는 데 사용되는 TLS/SSL 프로토콜 버전, 암호 그룹, 서버 인증서를 포함한 연결 암호화.
- 서버 인증서의 고유 이름(DN)에 지정된 URL의 카테고리 및 평판.

관련 항목

네트워크 조건
VLAN 조건
사용자, 영역 및 ISE 속성 조건(사용자 제어)
애플리케이션 조건(애플리케이션 컨트롤)
포트 및 ICMP 코드 조건
HTTPS 트래픽 필터링
서버 인증서 기반 TLS/SSL 규칙 조건, 2 페이지
인증서 고유 이름 TLS/SSL 규칙 조건, 3 페이지
인증서 상태 TLS/SSL 규칙 조건, 7 페이지
암호 그룹 TLS/SSL 규칙 조건, 15 페이지
암호화 프로토콜 버전 TLS/SSL 규칙 조건, 18 페이지

암호 해독 조정 요구 사항 및 사전 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

서버 인증서 기반 TLS/SSL 규칙 조건

TLS/SSL 규칙은 서버 인증서 특성을 기반으로 암호화된 트래픽을 처리하고 해독할 수 있습니다. 다음 서버 인증서 속성을 기반으로 TLS/SSL 규칙을 구성할 수 있습니다.

- 고유 이름(DN) 조건을 사용하면 서버 인증서를 발급한 CA 또는 인증서 보유자를 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다. 발급자 DN에 따라, 사이트의 서버 인증서를 발급한 CA를 기준으로 트래픽을 처리할 수 있습니다.
- TLS/SSL 규칙의 인증서 조건을 사용하면 트래픽을 암호화하는 데 사용된 서버 인증서를 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다. 하나 이상의 인증서로 규칙을 구성할 수 있습니다. 인증서가 조건의 모든 인증서와 매칭될 경우, 트래픽은 규칙과 매칭됩니다.

- TLS/SSL 규칙의 인증서 상태 조건을 사용하면 트래픽을 암호화하는 데 사용된 서버 인증서의 상태를 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다. 상태에는 인증서가 유효한지, 취소되었는지, 만료되었는지, 아직 유효하지 않은지, 자체 서명되었는지, 신뢰할 수 있는 CA가 서명했는지 여부, CRL(인증서 해지 목록)이 유효한지 여부, 인증서의 SNI(서버 이름 표시)가 요청의 서버와 일치하는지 여부가 포함됩니다.
- TLS/SSL 규칙의 암호 그룹 조건을 사용하면 암호화된 세션을 협상하는 데 사용된 암호 그룹을 기준으로 암호화된 트래픽을 처리하고 검사할 수 있습니다.
- TLS/SSL 규칙의 세션 조건을 사용하면 트래픽을 암호화하는 데 사용된 SSL 또는 TLS 버전을 기준으로 암호화된 트래픽을 검사할 수 있습니다.

규칙의 여러 암호 그룹, 인증서 발급자 또는 인증서 보유자를 탐지하려는 경우, 재사용 가능한 암호 그룹 및 고유 이름(DN) 개체를 생성하고 이를 규칙에 추가할 수 있습니다. 서버 인증서 및 특정 인증서 상태를 탐지하려면 해당 규칙에 대한 외부 인증서 및 외부 CA 개체를 생성해야 합니다.

인증서 고유 이름 **TLS/SSL** 규칙 조건

규칙 조건을 구성할 경우 리터럴 값을 수동으로 지정하고, 고유 이름(DN) 개체를 참조하거나 여러 개체가 포함된 고유 이름 그룹을 참조할 수 있습니다.

참고 **Decrypt - Known Key(**암호 해독 **-** 알려진 키**)** 작업도 선택할 경우 고유 이름(DN) 조건을 구성할 수 없습니다. 이 작업은 서버 인증서 선택을 통한 트래픽 해독이 필요하므로 인증서가 트래픽과 이미 일치합니다.

단일한 인증서 상태 규칙 조건의 여러 주체 및 발급자 DN을 대상으로 매칭할 수 있습니다. 규칙과 매칭하려면 하나의 공용 이름 또는 고유 이름(DN)만 매칭해야 합니다.

고유 이름(DN)을 수동으로 추가할 경우, 공용 이름 특성(**CN**)을 포함할 수 있습니다. `CN=` 없이 공용 이름(CN)을 추가하면 개체를 저장하기 전에 시스템이 `CN=`을 앞에 추가합니다.

다음 속성(**C, CN, O, OU**) 중 하나가 있는 고유 이름을 쉼표로 구분하여 추가할 수도 있습니다.

단일한 DN 조건에서 최대 50개의 리터럴 값 및 고유 이름(DN) 개체를 **Subject DNs(**주체 **DN)**에 추가하고, 50개의 리터럴 값 및 고유 이름(DN) 개체를 **Issuer DNs(**발급자 **DN)**에 추가할 수 있습니다.

시스템에서 제공된 DN 개체 그룹인 Cisco-Undecryptable-Sites에는 시스템이 해독할 수 없는 트래픽이 있는 웹사이트가 포함됩니다. 이 그룹을 DN 조건에 추가하면, 이러한 웹사이트에서 나가고 들어오는 트래픽을 차단하거나 해독하지 않도록 할 수 있으므로, 트래픽 해독을 시도하느라 시스템 리소스를 낭비하지 않아도 됩니다. 이 그룹의 개별 항목을 수정할 수 있습니다. 단, 이 그룹은 삭제할 수 없습니다. 시스템 업데이트로 인해 이 목록의 항목이 수정될 수 있지만 사용자 변경 사항은 그대로 유지됩니다.

암호화된 트래픽을 인증서 고유 이름(DN)으로 제어

프로시저

단계 **1** SSL 규칙 편집기에서 DN을 선택합니다.

단계 **2** **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 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 **3** 개체를 선택하려면 이를 클릭합니다. 모든 개체를 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Subject(**주체에 추가**)** 또는 **Add to Issuer(**발급자에 추가**)**를 클릭합니다.

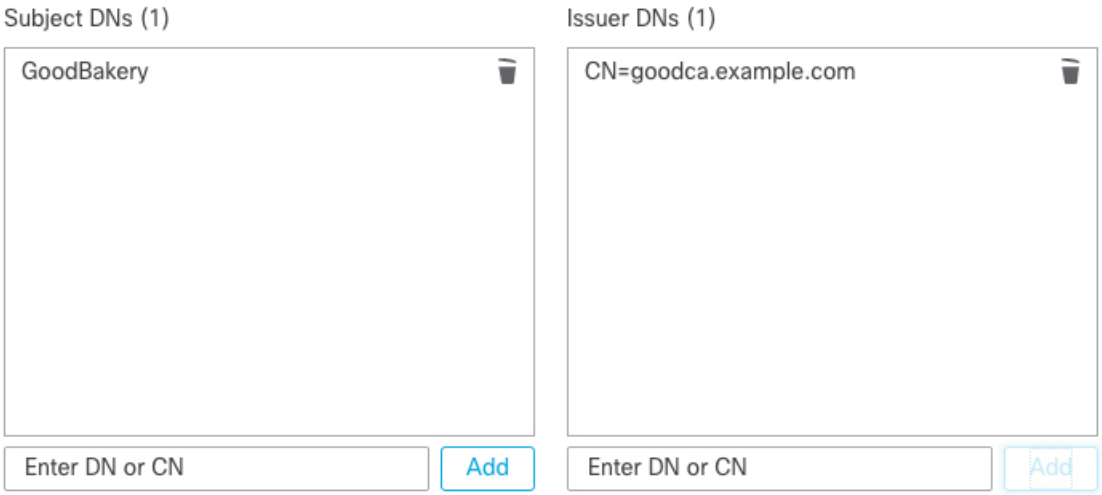
팁 선택한 영역을 끌어서 놓을 수도 있습니다.

단계 **5** 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.

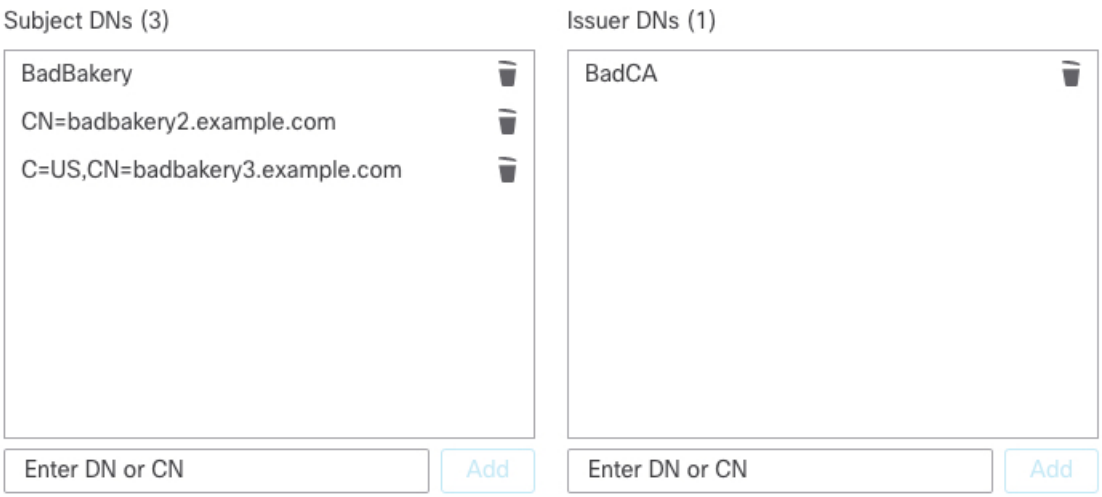
단계 **6** 규칙을 추가하거나 계속 수정합니다.

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.



다음 그림에는 badbakery.example.com에 발급된 인증서 및 연결된 도메인, 또는 badca.example.com에서 발급한 인증서를 검색하는 고유 이름(DN) 규칙 조건이 나와 있습니다. 이러한 인증서로 암호화된 트래픽은 다시 서명된 인증서를 사용하여 암호 해독됩니다.



다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

고유 이름 개체

인증서 TLS/SSL 규칙 조건

인증서 기반 TLS/SSL 규칙 조건을 만들 경우, 서버 인증서를 업로드할 수 있습니다. 인증서를 재사용 가능한 외부 인증서 개체로 저장하고, 이름을 서버 인증서와 연결할 수 있습니다. 또는 기존 외부 인증서 개체 및 개체 그룹으로 인증서 조건을 구성할 수 있습니다.

다음과 같은 인증서 고유 이름(DN) 특성을 기준으로, 외부 인증서 개체 및 개체 그룹에 따라 규칙 조건의 **Available Certificates(**사용 가능한 인증서**)** 필드를 검색할 수 있습니다.

- 주체 또는 발급자 공용 이름(CN)
- 주체 또는 발급자 조직(O)
- 주체 또는 발급자 부서(OU)

단일한 인증서 규칙 조건의 여러 인증서와 매칭되도록 선택할 수 있습니다. 업로드된 인증서와 매칭되는 트래픽을 암호화하는 데 인증서가 사용된 경우, 암호화된 트래픽은 규칙과 매칭됩니다.

단일한 인증서 조건에서 최대 50개의 외부 인증서 개체 및 외부 인증서 개체 그룹을 **Selected Certificates(**선택한 인증서**)**에 추가할 수 있습니다.

다음 사항을 참고하십시오.

- **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업도 선택할 경우 인증서 조건을 구성할 수 없습니다. 이 작업은 서버 인증서를 선택하여 트래픽을 해독해야 하므로, 이렇게 할 경우 인증서가 트래픽과 이미 매칭됩니다.
- 외부 인증서 개체가 포함된 인증서 조건을 구성할 경우, 암호 그룹 조건에 추가하는 모든 암호 그룹 또는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업에 연결되는 내부 CA 개체는 외부 인증서의 시그니처 알고리즘 유형과 매칭되어야 합니다. 예를 들어 규칙의 인증서 조건이 EC 기반 서버 인증서를 참조할 경우, 추가되는 모든 암호 그룹 또는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업과 연결되는 CA 인증서도 EC 기반이어야 합니다. 이때 시그니처 알고리즘 유형이 매칭되지 않을 경우, 정책 편집기에서는 규칙 옆에 경고가 표시됩니다.

암호화된 트래픽을 인증서로 제어

프로시저

단계 **1** SSL 규칙 편집기에서 Certificate(인증서)를 선택합니다.

단계 **2** **Available Certificates(**사용 가능한 인증서**)**에서 추가할 서버 인증서를 다음과 같이 찾습니다.

- 조건에 추가할 수 있는 외부 인증서 개체를 즉시 추가하려면 **Available Certificates(**사용 가능한 인증서**)** 목록 위의 추가(+)를 클릭합니다.
- 추가할 인증서 개체 및 그룹을 검색하려면, **Available Certificates(**사용 가능한 인증서**)** 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 3 개체를 선택하려면 이를 클릭합니다. 모든 개체를 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 4 **Add to Rule(**규칙에 추가**)**을 클릭합니다.

팁 선택한 영역을 끌어서 놓을 수도 있습니다.

단계 5 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

외부 인증서 개체

인증서 상태 TLS/SSL 규칙 조건

구성하는 각 인증서 상태 TLS/SSL 규칙 조건의 경우, 지정된 상태가 있는 경우 또는 없는 경우에 대해 트래픽을 매칭할 수 있습니다. 하나의 규칙 조건에서 여러 개의 상태를 선택할 수 있습니다. 인증서가 선택한 상태와 매칭되는 경우, 규칙은 트래픽과 매칭됩니다.

단일한 인증서 상태 규칙 조건에 여러 인증서 상태가 있는 경우 또는 없는 경우와 매칭하도록 선택할 수 있습니다. 인증서는 규칙과 매칭하는 조건 중 하나에만 매칭되어야 합니다.

이 매개변수를 설정할 때는 암호 해독 규칙을 구성하는지 차단 규칙을 구성하는지를 고려해야 합니다. 일반적으로 차단 규칙의 경우에는 **Yes(**예**)**를, 암호 해독 규칙의 경우에는 **No(**아니요**)**를 클릭해야 합니다. 예:

- **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙을 구성하는 경우, 기본 동작은 만료된 인증서가 있는 트래픽을 해독하는 것입니다. 이 동작을 변경하려면 만료된 인증서가 있는 트래픽이 해독 및 재서명되지 않도록 **Expired(**만료됨**)**에 대해 **No(**아니요**)**를 클릭하십시오.
- **Block(**차단**)** 규칙을 구성하는 경우, 기본 동작은 만료된 인증서가 있는 트래픽을 허용하는 것입니다. 이 동작을 변경하려면 만료된 인증서가 있는 트래픽이 차단되도록 **Expired(**만료됨**)**에 대해 **Yes(**예**)**를 클릭하십시오.

다음 표에는 암호화 서버 인증서 상태를 기준으로 암호화된 트래픽을 시스템이 평가하는 방법이 설명되어 있습니다.

표 *1:* 인증서 상태 규칙 조건 기준

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
취소	정책이 서버 인증서를 발급한 CA를 신뢰하며, 정책에 업로드된 CA 인증서에 서버 인증서를 취소하는 CRL이 포함되어 있습니다.	정책이 서버 인증서를 발급한 CA를 신뢰하며, 정책에 업로드된 CA 인증서에 해당 인증서를 취소하는 CRL이 포함되어 있지 않습니다.
자체 서명	탐지된 서버 인증서에 동일한 주체 및 발급자 DN이 포함되어 있습니다.	탐지된 서버 인증서에 다른 주체 및 발급자 DN이 포함되어 있습니다.
유효	다음의 모든 사항이 유효합니다. • 정책이 인증서를 발급한 CA를 신뢰합니다. • 서명이 유효함 • 발급자가 유효함 • 정책의 신뢰할 수 있는 CA가 인증서를 취소하지 않음 • 현재 날짜가 인증서의 유효 시작일과 유효 만료일 사이에 해당함	다음 중 하나 이상이 유효하지 않습니다. • 정책이 인증서를 발급한 CA를 신뢰하지 않음 • 서명이 유효하지 않음 • 발급자가 유효하지 않음 • 정책의 신뢰할 수 있는 CA가 인증서를 취소함 • 현재 날짜가 인증서의 유효 시작일보다 이전입니다. • 현재 날짜가 인증서의 유효 만료일을 경과했습니다.
잘못된 서명	인증서의 시그니처를 인증서의 내용과 올바르게 확인할 수 없습니다.	인증서의 시그니처를 인증서의 내용과 올바르게 확인할 수 있습니다.
잘못된 발급자	발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장되지 않습니다.	발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장됩니다.
만료	현재 날짜가 인증서의 유효 만료일을 경과했습니다.	현재 날짜가 유효 만료일 이전이거나 해당일입니다.
아직 유효하지 않음	현재 날짜가 인증서의 유효 시작일보다 이전입니다.	현재 날짜가 유효 시작일 이후이거나 해당일입니다.

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
잘못된 인증서		인증서가 유효합니다. 다음의 모든 사항이 유효합니다. • 유효한 인증서 확장. • 인증서를 지정된 용도로 사용할 수 있습니다. • 유효한 기본 제약 조건 경로 길이. • Not Before 및 Not After의 유효한 값. • 유효한 이름 제약 조건. • 루트 인증서를 지정된 용도로 신뢰할 수 있습니다. • 루트 인증서가 지정된 용도를 수락합니다.

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
	인증서가 유효하지 않습니다. 다음 중 하나 이상이 유효하지 않습니다. • 유효하지 않거나 일치하지 않는 인증서 확장. 즉, 인증서 확장에 유효하지 않은 값(예를 들어 잘못된 인코딩) 또는 다른 확장과 일치하지 않는 일부 값이 있습니다. • 인증서를 지정된 용도로 사용할 수 없습니다. • 기본 제약 조건 경로 길이 매개변수가 초과됐습니다. 자세한 내용은 RFC 5280, 섹션 4.2.1.9를 참조하십시오. • Not Before 또는 Not After의 인증서 값이 잘못되었습니다. 이러한 날짜는 UTCTime 또는 GeneralizedTime으로 인코딩될 수 있습니다. 자세한 내용은 RFC 5280 섹션 4.1.2.5를 참조하십시오. • 이름 제약 조건의 형식이 인식되지 않습니다. 예를 들어 RFC 5280, 섹션 4.2.1.10에서 언급되지 않은 양식의 이메일 주소 형식입니다. 이것은 잘못된 확장 또는 현재 지원되지 않는 일부 새로운 기능 때문일 수 있습니다. 지원되지 않는 이름 제약 조건 유형이 발생했습니다. OpenSSL은 현재 디렉터리 이름, DNS 이름, 이메일 및 URI 유형을 지원합니다. • 루트 인증서 인증 기관을 지정된 용도로 신뢰할 수 없습니다.	

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
	• 루트 인증서 인증 기관이 지정된 용도를 거부합니다.	
유효하지 않은 CRL	Certificate Revocation List(CRL) 디지털 서명이 유효하지 않습니다. 다음 중 하나 이상이 유효하지 않습니다. • CRL의 Next Update(다음 업데이트) 또는 Last Update(마지막 업데이트) 필드의 값이 유효하지 않습니다. • CRL이 아직 유효하지 않습니다. • CRL이 만료되었습니다. • CRL 경로를 확인하는 중에 오류가 발생했습니다. 이 오류는 확장된 CRL 확인이 활성화된 경우에만 발생합니다. • CRL을 찾을 수 없습니다. • 찾을 수 있는 유일한 CRL이 인증서의 범위와 일치하지 않습니다.	CRL이 유효합니다. 다음의 모든 사항이 유효합니다. • Next Update(다음 업데이트) 및 Last Update(마지막 업데이트) 필드가 유효합니다. • CRL의 날짜가 유효합니다. • 경로가 유효합니다. • CRL을 찾았습니다. • CRL이 인증서의 범위와 일치합니다.

인증서는 둘 이상의 상태와 일치할 수 있지만 규칙으로 인해 트래픽에서는 작업을 한 번만 수행할 수 있습니다.

CA가 인증서를 발급하거나 취소했는지 확인하려면 루트 및 중간 CA 인증서와 관련 CRL을 개체로 업로드해야 합니다. 그런 다음 이러한 신뢰할 수 있는 CA 개체를 SSL 정책의 신뢰할 수 있는 CA 인증서 목록에 추가합니다.

외부 인증 증명 신뢰

루트 및 중간 CA 인증서를 SSL 정책에 추가하여 CA를 신뢰할 수 있으며, 그런 다음 이러한 신뢰할 수 있는 CA를 활용하면 트래픽을 암호화하는 데 사용된 서버 인증서를 식별할 수 있습니다.

신뢰할 수 있는 CA 인증서에 업로드된 CRL(Certificate Revocation List: 인증서 폐기 목록)이 포함되어 있는 경우, 신뢰할 수 있는 CA가 암호 인증서를 취소한 것인지 확인할 수도 있습니다.

프로시저

단계 **1** SSL 규칙 편집기에서 **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)**를 선택합니다.

단계 **2** **Available Trusted CAs(**사용 가능한 신뢰할 수 있는 인증서**)**에서 추가할 신뢰할 수 있는 CA를 다음과 같이 찾습니다.

- 신뢰할 수 있는 CA 개체를 즉시 추가한 다음 조건에 추가하려면 **Available Trusted CAs(**사용 가능한 신뢰할 수 있는 **CA)** 목록 위의 추가(+)을 클릭합니다.
- 추가할 신뢰할 수 있는 CA 개체 및 그룹을 검색하려면, **Available Trusted CAs(**사용 가능한 신뢰할 수 있는 **CA)** 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 **3** 개체를 선택하려면 이를 클릭합니다. 모든 개체를 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭합니다.

팁 선택한 영역을 끌어서 놓을 수도 있습니다.

단계 **5** 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 인증서 상태 TLS/SSL 규칙 조건을 SSL 규칙에 추가합니다. 자세한 내용은 인증서 상태를 기준으로 트래픽 매칭, 13 페이지를 참조하십시오.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

신뢰할 수 있는 인증 기관 개체

신뢰할 수 있는 외부 인증서 기관 설정

식별된 서버 인증서에는 신뢰할 수 있는 CA가 서명한 인증서가 포함됩니다. 신뢰할 수 있는 CA 인증서를 SSL 정책에 추가한 후 인증서 상태 조건이 포함된 TLS/SSL 규칙을 구성하여 이 트래픽에 대해 매칭할 수 있습니다.

팁 루트 CA의 트러스트 체인 내의 모든 인증서를 신뢰할 수 있는 CA 인증서 목록에 업로드하며, 여기에는 루트 CA 인증서 및 모든 중간 CA 인증서가 포함됩니다. 이렇게 하지 않으면 중간 CA가 발급한 신뢰할 수 있는 인증서를 탐지하는 것이 더 어려워집니다. 또한 루트 발급자 CA를 기반으로 트래픽을 신뢰하도록 인증서 상태 조건을 구성하는 경우, 신뢰할 수 있는 CA의 신뢰 체인 내의 모든 트래픽은 불필요한 해독 없이 허용될 수 있습니다.

SSL 정책을 생성하면 은 Trusted CA Certificates(신뢰할 수 있는 CA 인증서) 탭에 기본 신뢰할 수 있는 CA 개체 그룹인 Cisco Trusted Authorities를 입력합니다.

그룹의 개별 항목을 수정하고, 이 그룹을 SSL 정책에 포함할지 선택할 수 있습니다. 단, 이 그룹은 삭제할 수 없습니다. 시스템 업데이트로 인해 이 목록의 항목이 수정될 수 있으나, 사용자 변경 사항은 그대로 유지됩니다.

인증서 상태를 기준으로 트래픽 매칭

시작하기 전에

- 신뢰할 수 있는 CA 개체 또는 그룹을 SSL 정책에 추가합니다. 자세한 내용은 외부 인증 증명 신뢰, 11 페이지를 참조하십시오.

프로시저

단계 **1** Firepower Management Center에서 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**을 선택합니다.

단계 **2** 새 정책을 추가하거나 기존 정책을 편집합니다.

단계 **3** 새 TLS/SSL 규칙을 추가하거나 기존 규칙을 편집합니다.

단계 **4** Add Rule(규칙 추가) 또는 Editing Rule(규칙 편집) 대화 상자에서 **Cert Status(**인증서 상태**)**를 선택합니다.

단계 **5** 각 인증서 상태에는 다음과 같은 옵션이 있습니다.

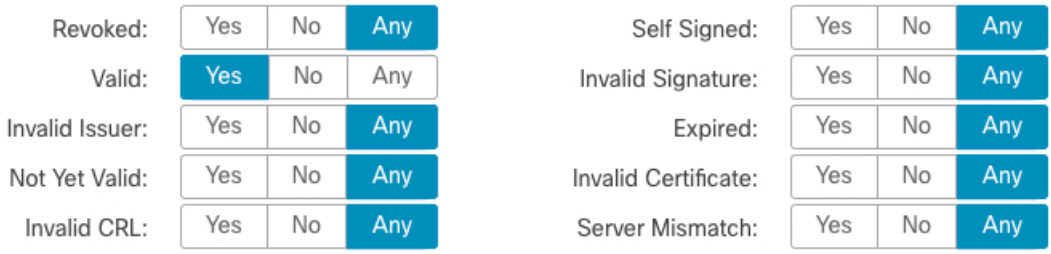
- 해당 인증서 상태가 있는 경우에 매칭하려면 **Yes**를 선택합니다.
- 해당 인증서 상태가 없는 경우에 매칭하려면 **No**를 선택합니다.
- 규칙을 매칭할 때 조건을 건너뛰려면 **Any(**모두**)**를 선택합니다. 다시 말해 **Any(**모두**)**를 선택하면 인증서 상태가 있건 없건 규칙이 매칭됩니다.

단계 **6** 규칙을 추가하거나 계속 수정합니다.

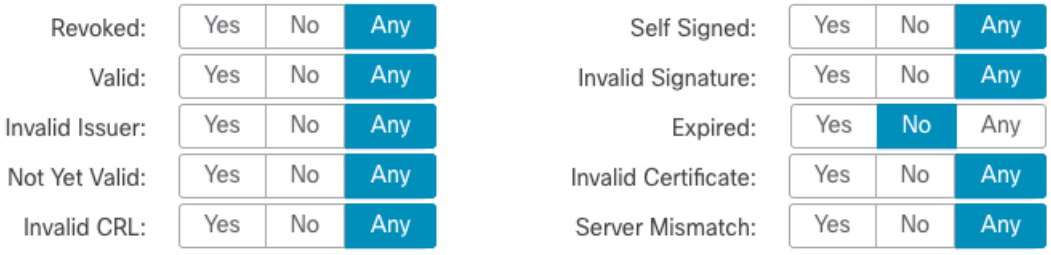
예

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.

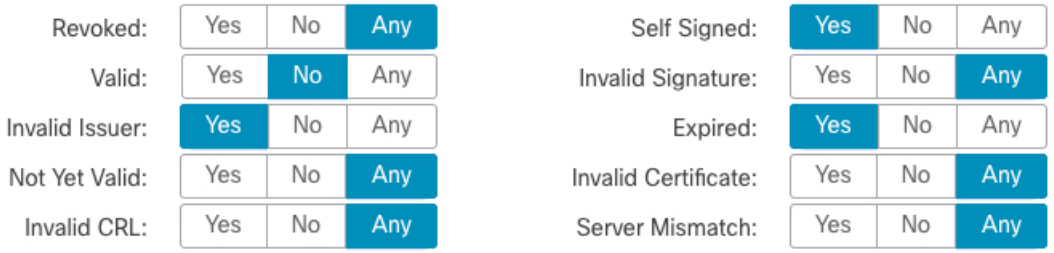
다음 그림에는 유효한 인증서를 확인하는 인증서 상태 규칙 조건이 나와 있습니다. 이러한 인증서는 Verified Authority에서 발급하였으며, CRL에 포함되지 않고, 유효 시작일과 유효 만료일 사이의 기간이 아직 남아 있는 상태입니다. 이러한 인증서로 암호화된 트래픽은 컨피그레이션으로 인해, 액세스 제어를 통해 해독 및 검사되지 않습니다.

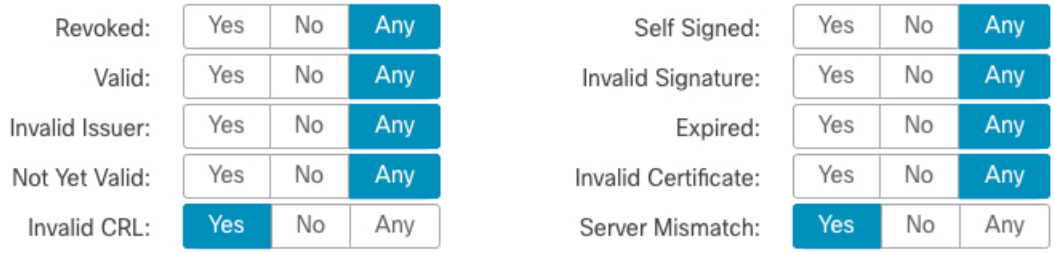


다음 그림에는 상태가 없는지 확인하는 인증서 상태 규칙 조건이 나와 있습니다. 이 경우 컨피그레이션으로 인해, 만료되지 않은 인증서로 암호화된 트래픽과 매칭을 수행하며 해당 트래픽을 모니터링합니다.



다음 그래픽에는 몇 가지 상태가 있는 경우 또는 없는 경우와 매칭하는 인증서 상태 규칙 조건이 나와 있습니다. 이 구성에서는 잘못된 사용자가 발급한 인증서, 자체 서명 인증서, 유효하지 않거나 만료된 인증서로 암호화된 수신 트래픽과 규칙이 일치하는 경우 알려진 키를 사용하여 트래픽이 암호 해독됩니다.





다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

암호 그룹 TLS/SSL 규칙 조건

시스템에서는 암호 그룹 규칙 조건에 추가할 수 있는 미리 정의된 암호 그룹을 제공합니다. 여러 암호 그룹이 포함된 암호 그룹 목록 개체를 추가할 수도 있습니다.

참고 새 암호 그룹을 추가할 수 없습니다. 또한 미리 정의된 암호 그룹을 수정하거나 삭제할 수 없습니다.

단일한 암호 그룹 조건의 **Selected Cipher Suites(**선택한 암호화 그룹**)**에 최대 50개의 암호 그룹 및 암호 그룹 목록을 추가할 수 있습니다. 다음과 같은 암호 그룹을 암호 그룹 조건에 추가할 수 있습니다.

- SSL_RSA_FIPS_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_FIPS_WITH_DES_CBC_SHA

- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- TLS_DH_Anon_WITH_AES_128_GCM_SHA256
- TLS_DH_Anon_WITH_AES_256_GCM_SHA384
- TLS_DH_Anon_WITH_CAMELLIA_128_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_128_CBC_SHA256
- TLS_DH_Anon_WITH_CAMELLIA_256_CBC_SHA
- TLS_DH_anon_WITH_CAMELLIA_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_NULL_SHA
- TLS_ECDHE_ECDSA_WITH_RC4_128_SHA
- TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_NULL_SHA
- TLS_ECDHE_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_128_CBC_SHA256
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA
- TLS_RSA_WITH_CAMELLIA_256_CBC_SHA256
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_RC4_128_SHA

다음에 유의하십시오.

- 구축에 대해 지원되지 않는 암호 그룹을 추가하는 경우, 구성을 구축할 수 없습니다. 예를 들어 패시브 구축은 DHE(Diffie-Hellman Ephemeral) 또는 ECDHE(Ephemeral Elliptic Curve Diffie-Hellman) 암호 그룹을 사용한 트래픽 암호 해독을 지원하지 않습니다. 이러한 암호 그룹이 포함된 규칙을 생성할 경우 액세스 제어 정책을 구축할 수 없습니다.
- 암호 그룹이 포함된 암호 그룹 조건을 구성할 경우, 인증서 조건에 추가하는 외부 인증서 개체 또는 **Decrypt - Resign(**암호 해독 **-** 다시 서명**)** 작업에 연결되는 내부 CA 개체는 암호 그룹의 시그니처 알고리즘 유형과 매칭되어야 합니다. 예를 들어 규칙의 암호 그룹 조건이 EC 기반 암호

그룹을 참조할 경우, 추가되는 모든 서버 인증서 또는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업과 연결되는 CA 인증서도 EC 기반이어야 합니다. 이때 시그니처 알고리즘 유형이 매칭되지 않을 경우, 정책 편집기에서는 규칙 옆에 경고 아이콘이 표시됩니다.

- 시스템은 익명 암호 그룹으로 암호화된 트래픽을 해독할 수 없습니다. 익명 암호 그룹을 **Cipher Suite(**암호 그룹**)** 조건에 추가할 경우, SSL 규칙에서 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다.

암호화된 트래픽을 암호 그룹으로 제어

프로시저

단계 **1** SSL 규칙 편집기에서 Cipher Suite(암호 그룹)를 선택합니다.

단계 **2** **Available Cipher Suites(**사용 가능한 암호 그룹**)**에서 추가할 암호 그룹을 다음과 같이 찾습니다.

- 조건에 추가할 수 있는 암호 그룹 목록을 즉시 추가하려면 **Available Cipher Suites(**사용 가능한 암호 그룹**)** 목록 위의 추가(+)를 클릭합니다.
- 추가할 암호 그룹 및 목록을 검색하려면, **Available Cipher Suites** 목록 위의 **Search by name or value** 프롬프트를 클릭한 다음 암호 그룹의 이름을 입력하거나 암호 그룹의 값을 입력합니다. 입력을 수행하면 목록이 업데이트되어 일치하는 암호 그룹을 표시합니다.

단계 **3** 암호 그룹을 선택하려면 클릭합니다. 모든 암호 그룹을 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭합니다.

팁 선택한 암호 그룹을 끌어서 놓을 수도 있습니다.

단계 **5** 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

관련 항목

암호 그룹 목록

암호화 프로토콜 버전 TLS/SSL 규칙 조건

SSL 버전 3.0, 또는 TLS 버전 1.0, 1.1, 1.2로 암호화된 트래픽과 매칭되도록 선택할 수 있습니다. 기본적으로, 규칙을 생성할 때 모든 프로토콜 버전이 선택됩니다. 여러 버전을 선택할 경우, 선택한 버전과 매칭되는 암호화된 트래픽은 규칙과 매칭됩니다. 규칙 조건을 저장할 경우 하나 이상의 프로토콜 버전을 선택해야 합니다.

SSL v2.0은 버전 규칙 조건에서 선택할 수 없습니다. 시스템에서는 SSL 버전 2.0으로 암호화된 트래픽의 암호 해독을 지원하지 않습니다. 해독 불가능한 작업을 구성하여 추가 검사 없이 이 트래픽을 허용하거나 차단하도록 할 수 있습니다.

트래픽을 암호화 프로토콜 버전으로 제어

프로시저

단계 **1** SSL 규칙 편집기에서 Version(버전)을 선택합니다.

단계 **2** 매칭할 프로토콜 버전을 선택합니다.

단계 **3** 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.