TLS/SSL 규칙 시작하기

다음 주제에서는 TLS/SSL 규칙 생성, 관리, 문제 해결의 개요를 제공합니다.

참고

TLS 및 SSL이 서로 번갈아 가며 자주 사용되기 때문에 프로토콜 중 하나에 대해 논의 중임을 나타내기 위해 식 *TLS/SSL*을 사용합니다. SSL 프로토콜은 보다 안전한 TLS 프로토콜을 위해 IETF에서 더 이상 사용되지 않으므로 일반적으로 TLS만 참조하는 것으로 *TLS/SSL*을 해석할 수 있습니다.

예외는 SSL 정책입니다. FMC 구성 옵션은 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**이므로 *SSL policies(SSL* 정책*)*라는 용어를 사용합니다. 단, 이러한 정책은 TLS 및 SSL 트래픽에 대한 규칙을 정의하는 데 사용될 수 있습니다.

SSL 및 TLS 프로토콜에 대한 자세한 내용은 SSL과 TLS 비교 - 차이점은 무엇입니까?와 같은 리소스를 참조하십시오.

TLS/SSL 규칙 개요

TLS/SSL 규칙은 여러 매니지드 디바이스에서 암호화된 트래픽을 세부적으로 처리하는 방법을 제공합니다. 이를테면 추가 검사 없이 트래픽을 차단하거나 트래픽을 암호 해독하지 않고 액세스 제어로 검사하거나 액세스 제어 분석을 위해 트래픽을 암호 해독할 수 있습니다.

TLS/SSL 규칙 지침 및 제한 사항

TLS/SSL 규칙을 설정할 때는 다음 사항을 명심하십시오. TLS/SSL 규칙을 올바르게 설정하는 것은 복잡한 작업이지만 암호화된 트래픽을 처리하는 효과적인 구축에 필수적입니다. 제어할 수 없는 특정 애플리케이션 동작을 포함하여 여러 요인이 규칙을 구성하는 방법에 영향을 미칩니다.

또한 규칙은 다른 규칙을 선점하거나 추가 라이선스를 요구하거나 잘못된 구성을 포함할 수 있습니다. 규칙을 세심하게 구성하면 네트워크 트래픽 처리에 필요한 리소스도 줄일 수 있습니다. 지나치게 복잡한 규칙을 만들고 규칙의 순서를 잘못 지정하면 성능에 나쁜 영향을 줄 수 있습니다.

자세한 내용은 액세스 제어 규칙 순서에 대한 모범 사례를 참조하십시오.

관련 항목

TLS/SSL 암호 해독 사용 지침

매니지드 디바이스에서 암호화된 트래픽을 처리하는 경우에만 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙을 설정합니다. 암호 해독 규칙에는 성능에 영향을 미칠 수 있는 처리 오버헤드가 필요합니다.

패시브 또는 인라인 탭 모드 인터페이스가 있는 디바이스에서는 트래픽을 암호 해독할 수 없습니다.

TLS/SSL 규칙을 지원하지 않는 기능

RC4 암호 그룹은 지원되지 않습니다**.**

Rivest Cipher 4(*RC4* 또는 *ARC4*라고도 함) 암호 그룹은 취약성이 있는 것으로 알려져 있으며 안전하지 않은 것으로 간주됩니다. SSL 정책은 RC4 암호 그룹을 지원되지 않는 것으로 식별하기 때문에 조직의 요구 사항에 일치시키려면 정책의 **Undecryptable Actions(**암호 해독 불가 작업**)**

페이지에서 **Unsupported Cipher Suite(**지원되지 않는 암호 그룹**)** 작업을 설정해야 합니다. 자세한 내용은 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션를 참고하십시오.

패시브 및 인라인 탭 모드 인터페이스 지원되지 않음

TLS/SSL 패시브 또는 인라인 탭 모드 인터페이스에서 트래픽 암호를 해독할 수 없습니다.

TLS 1.3은 지원되지 않음

Firepower System은 현재 TLS 버전 1.3 암호화 또는 암호 해독을 지원하지 않습니다. 사용자가 TLS 1.3 암호화를 협상하는 웹사이트를 방문하면 웹 브라우저에서 다음과 유사한 오류가 표시될 수 있습니다.

- **ERR_SSL_PROTOCOL_ERROR**
- **SEC_ERROR_BAD_SIGNATURE**
- **ERR_SSL_VERSION_INTERFERENCE**

이 동작을 제어하는 방법에 대한 자세한 내용은 Cisco TAC에 문의하십시오.

TLS/SSL 암호 해독 금지 지침

다음에 의해 금지되는 경우 트래픽을 해독해서는 안 됩니다.

- 법. 예를 들어 일부 사법부는 금융 정보 해독을 금지합니다.
- 회사 정책. 예를 들어 회사에서 기밀 통신의 해독을 금지할 수 있습니다.
- 프라이버시 규정
- 인증서 고정(또는 *TLS/SSL*고정)을 사용하는 트래픽은 연결이 중단되지 않도록 암호화 상태를 유지해야 합니다.

특정 유형의 트래픽은 암호 해독을 우회하도록 선택하는 경우, 해당 트래픽에는 처리 작업이 수행되지 않습니다. 암호화된 트래픽은 먼저 SSL 정책에 따라 평가된 뒤 액세스 제어 정책으로 진행하여 최종 허용 또는 차단 결정을 수행합니다. 암호화된 트래픽은 다음을 포함하며 이에 국한되지 않는 모든 TLS/SSL 규칙 조건에서 허용 또는 차단될 수 있습니다.

- 인증서 상태(예: 만료됨 또는 유효하지 않은 인증서)
- 프로토콜 (예: 비보안 SSL 프로토콜)
- 네트워크(보안 영역, IP 주소, VLAN 태그 등)
- 정확한 URL 또는 URL 카테고리
- Port(포트)
- 사용자 그룹

TLS/SSL 암호 해독 - 파기 지침

하나의 CA(Certificate Authority) 인증서와 개인 키를 **Decrypt – Resign(**암호 해독 - 다시 서명**)** 작업에 연결할 수 있습니다. 트래픽이 이 규칙과 일치하는 경우, 시스템은 서버 인증서를 CA 인증서로 다시 서명한 다음 중간자(man-in-the-middle) 역할을 합니다. 클라이언트와 매니지드 디바이스 간, 매니지드 디바이스와 서버 간에 각각 하나씩 2개의 TLS/SSL 세션을 생성합니다. 각 세션은 서로 다른 암호화 세션 세부사항을 포함하며 시스템이 트래픽을 암호 해독하고 다시 암호화할 수 있도록 합니다.

모범 사례

다음과 같은 방법을 권장합니다.

- 발신 트래픽 암호 해독을 위한 **Decrypt - Resign(**암호 해독 - 파기**)** 규칙 작업입니다. 수신 트래픽에는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 작업을 권장합니다.

  Decrypt - Known Key(암호 해독 - 알려진 키**)**에 대한 자세한 내용은 TLS/SSL 암호 해독 - 알려진 키 지침, 5 페이지의 내용을 참조하십시오.

- 암호 해독 - 재서명 규칙 작업을 설정할 때는 키 교환 키만 바꾸기 확인란을 항상 확인해야 합니다.

  사용자가 직접 서명 인증서를 사용하는 웹사이트를 탐색하면, 웹 브라우저에서 보안 경고가 표시되며 안전하지 않은 사이트와 통신 중이라고 경고합니다.

  사용자가 신뢰할 수 있는 인증서를 사용하는 웹사이트를 탐색할 때는 보안 경고가 표시되지 않습니다.

세부 사항

Decrypt - Resign(암호 해독 - 다시 서명**)** 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 서명 알고리즘 유형을 기반으로 트래픽을 매칭합니다. CA 인증서를 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업과 연결하므로 서로 다른 서명 알고리즘으로 암호화된 여러 발신 트래픽 유형을 해독하는 TLS/SSL 규칙을 생성할 수 없습니다. 또한 규칙에 추가하는 외부 인증서 개체와 암호 그룹은 연결된 CA 인증서 암호화 알고리즘 유형과 매칭해야 합니다.

예를 들어 EC(Elliptic Curve) 알고리즘으로 암호화된 발신 트래픽은 작업에서 EC 기반 CA 인증서를 참조할 때만 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙과 일치합니다. 인증서 및 암호 그룹 규칙 조건을 생성하려면 EC 기반 외부 인증서와 암호 그룹을 규칙에 추가해야 합니다.

마찬가지로 RSA 기반 CA 인증서를 참조하는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙은 RSA 알고리즘으로 암호화된 발신 트래픽에만 일치합니다. EC 알고리즘으로 암호화된 발신 트래픽은 구성된 기타 모든 규칙 조건이 일치하더라도 이 규칙과 일치하지 않습니다.

지침 및 제한 사항

다음 사항도 유의하십시오.

익명 암호 그룹 지원되지 않음

본질적으로 익명 암호 그룹은 인증에 사용되지 않으며 키 교환을 사용하지 않습니다. 익명 암호 그룹은 제한적으로 사용됩니다. 자세한 내용은 RFC 5246, 섹션 A.5를 참조하십시오.

익명 암호 그룹이 인증에 사용되지 않으므로 규칙에서는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다.

일치하지 않는 암호 그룹

인증서와 일치하지 않는 암호 그룹으로 TLS/SSL 규칙을 저장하려고 시도하면 다음과 같은 오류가 표시됩니다. 문제를 해결하려면 TLS/SSL 암호 그룹 확인를 참조하십시오.

```
Traffic cannot match this rule; none of your selected cipher suites contain a
signature algorithm that the resigning CA's signature algorithm
```

신뢰할 수 없는 인증 기관

클라이언트가 서버 인증서 재서명에 쓰이는 CA(Certificate Authority)를 신뢰하지 않을 경우 신뢰할 수 없는 인증서임을 사용자에게 경고합니다. 이를 방지하려면 클라이언트가 신뢰하는 CA 저장소에 CA 인증서를 가져오십시오. 또는 조직에 개인 PKI가 있을 경우, 조직의 모든 클라이언트가 자동으로 신뢰하는 루트 CA에 의해 서명된 중간 CA 인증서를 발급한 다음 그 CA 인증서를 디바이스에 업로드할 수 있습니다.

HTTP 프록시 제한

클라이언트와 매니지드 디바이스 사이에 HTTP 프록시가 있고 클라이언트와 서버가 CONNECT HTTP 메서드를 사용하여 터널링된 TLS/SSL 연결을 설정할 경우, 시스템은 트래픽을 암호 해독할 수 없습니다. 시스템에서 이 트래픽을 처리하는 방법은 핸드셰이크 오류 해독 불가 작업에 의해 결정됩니다.

서명된 **CA** 업로드

내부 CA 개체를 생성하고 CSR(certificate signing request) 생성을 선택할 경우, 서명된 인증서를 개체에 업로드해야 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업에 이 CA를 사용할 수 있습니다.

TLS/SSL 암호 해독 - 알려진 키 지침

Decrypt - Known Key(암호 해독 - 알려진 키**)** 작업을 구성할 때 하나 이상의 서버 인증서 및 쌍 개인 키를 이 작업과 연결할 수 있습니다. 트래픽이 규칙과 일치하며 트래픽을 암호화하는 데 사용된 인증서가 작업과 연결된 인증서와 일치하는 경우, 시스템은 적절한 개인 키를 사용하여 세션 암호화 및 암호 해독 키를 얻습니다. 개인 키에 대한 액세스 권한이 있어야 하므로 이 작업은 조직에서 제어하는 서버에서 수신하는 트래픽의 해독에 가장 적합합니다.

다음 사항도 유의하십시오.

익명 암호 그룹 지원되지 않음

본질적으로 익명 암호 그룹은 인증에 사용되지 않으며 키 교환을 사용하지 않습니다. 익명 암호 그룹은 제한적으로 사용됩니다. 자세한 내용은 RFC 5246, 섹션 A.5를 참조하십시오.

익명 암호 그룹이 인증에 사용되지 않으므로 규칙에서는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다.

고유 이름 또는 인증서와 매칭할 수 없음

Decrypt - Known Key(암호 해독 - 알려진 키**)** 작업으로 TLS/SSL 규칙을 생성할 때 **Distinguished Name(**고유 이름**)** 또는 **Certificate(**인증서**)** 조건에서 매칭할 수 없습니다. 이 규칙이 트래픽과 매칭할 경우 인증서, 주체 DN, 발급자 DN이 규칙과 연결된 인증서와 이미 매칭한다고 전제합니다.

불일치 서명 알고리즘

Decrypt - Resign(암호 해독 - 다시 서명**)** 작업으로 규칙을 설정한 경우, 하나 이상의 외부 인증서 개체나 암호 그룹에서 서명 알고리즘 유형 불일치가 있다면 정책 편집기는 규칙 옆에 정보() 을 표시합니다. 모든 외부 인증서 개체 또는 모든 암호 그룹에 대해 서명 알고리즘 유형을 잘못 매칭할 경우, 정책은 규칙 옆에 경고 아이콘(경고( ))을 표시하며, SSL 정책과 연결된 액세스 제어 정책을 구축할 수 없습니다.

인증서 고정

고객의 브라우저가 인증서 고정을 사용하여 서버 인증서를 확인하는 경우, 서버 인증서에 다시 서명하여 이 트래픽을 암호 해독할 수 없습니다. 이 트래픽을 허용하려면 서버 인증서 공통 이름 또는 고유 이름(DN)과 일치하도록 **Do not decrypt(**암호 해독 안 함**)** 작업을 사용하여 TLS/SSL 규칙을 구성합니다.

TLS/SSL 차단 지침

해독된 트래픽이 **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)** 작업이 있는 액세스 제어 규칙과 일치하는 경우, 시스템은 검사 없이 일치하는 연결을 차단하고 사용자 지정 가능한 응답 페이지를 표시하지 않습니다.

규칙에서 로깅을 활성화했다면, **Analysis(**분석**)** > **Events(**이벤트**)** > **Connections(**연결**)**에) 연결 이벤트 2개가 표시됩니다. 하나는 인터랙티브 차단용이며, 다른 이벤트는 사용자의 사이트 진행 선택 여부를 표시합니다.

관련 항목

HTTP 응답 페이지 정보

TLS/SSL 인증서 고정 지침

일부 애플리케이션이 *TLS/SSL* 피닝또는 인증서 피닝이라는 기법을 사용하는데 이 기법에서는 원본 서버 인증서 지문이 애플리케이션 자체에 내장됩니다. 따라서 TLS/SSL 규칙을 **Decrypt - Resign(**암호 해독 - 재서명**)** 작업으로 구성하는 경우, 애플리케이션이 매니지드 디바이스로부터 재서명된 인증서를 수신할 때 확인이 실패하고 연결이 중단됩니다.

TLS/SSL 피닝은 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이 문제를 방지하거나 해결하는 방법은 없습니다. 다음 옵션을 이용할 수 있습니다.

- **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙 앞에 오는 이러한 애플리케이션 규칙에 대해서는 **Do not Decrypt(**암호 해독 안 함**)**를 생성하십시오.
- 웹 브라우저를 사용하여 애플리케이션에 액세스하도록 사용자에게 지시합니다.

규칙 순서 지정에 대한 자세한 내용은 SSL 규칙 순서를 참조하십시오.

TLS/SSL 하트비트 지침

일부 애플리케이션은 *TLS* 하트비트를 TLS(Transport Layer Security) 및 DTLS(Datagram Transport Layer Security) 프로토콜로 확장합니다. 이 프로토콜은 RFC6520에서 정의합니다. TLS 하트비트는 연결 상태를 확인하는 방법을 제공합니다. 즉 클라이언트 또는 서버가 특정 바이트의 데이터를 전송하고 상대방의 에코 응답을 요청합니다. 성공한 경우, 암호화된 데이터가 전송됩니다.

Max Heartbeat Length(최대 하트비트 길이**)**를 NAP(Network Analysis Policy)에서 구성하고 TLS 하트비트를 처리하는 방법을 결정할 수 있습니다. 자세한 내용은 SSL 전처리기을 참조하십시오.

TLS/SSL 익명 암호 그룹 제한

본질적으로 익명 암호 그룹은 인증에 사용되지 않으며 키 교환을 사용하지 않습니다. 익명 암호 그룹은 제한적으로 사용됩니다. 자세한 내용은 RFC 5246, 섹션 A.5를 참조하십시오.

익명 암호 그룹이 인증에 사용되지 않으므로 규칙에서는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다.

익명 암호 그룹은 TLS/SSL 규칙의 암호 그룹 조건에 추가할 수 있지만 시스템은 ClientHello 처리 중에 자동으로 익명 암호 그룹을 제거합니다. 시스템이 규칙을 사용하도록 하려면 ClientHello가 처리되지 않도록 하는 순서로 TLS/SSL 규칙을 구성해야 합니다. 자세한 내용은 SSL 규칙 순서를 참고하십시오.

TLS/SSL 노멀라이저 지침

인라인 표준화 전처리기에서 **Normalize Excess Payload(**초과 페이로드 표준화**)** 옵션을 활성화할 경우, 전처리기가 해독된 트래픽을 표준화할 때 패킷을 삭제하고 잘린 패킷으로 대체할 수 있습니다. 이로써 TLS/SSL 세션이 종료되지는 않습니다. 트래픽이 허용될 경우, 잘린 패킷이 TLS/SSL 세션의 일부로 암호화됩니다.

기타 TLS/SSL 규칙 지침

사용자 및 그룹

규칙에 사용자 또는 그룹을 추가한 다음 해당 그룹이나 사용자를 제외하도록 영역 설정을 변경하는 경우, 해당 규칙은 효과가 없습니다. (영역을 비활성화하는 경우에도 마찬가지입니다.) 영역에 대한 자세한 내용은 영역 생성를 참조하십시오.

TLS/SSL 규칙의 카테고리

SSL 정책에 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업이 있지만 웹사이트가 암호 해독되지 않는 경우, 해당 정책에 연결된 규칙에서 **Category(**범주**)** 페이지를 확인합니다.

경우에 따라 웹사이트는 인증 또는 기타 목적을 위해 다른 사이트로 리디렉션되며, 리디렉션된 사이트의 URL 카테고리 분류는 암호 해독하려는 사이트의 URL 카테고리 분류와 다를 수 있습니다. 예를 들어 `gmail.com`(웹 기반 이메일 카테고리)은 인증을 위해 `accounts.gmail.com`(인터넷 포털 카테고리)으로 리디렉션됩니다. SSL 규칙에 모든 관련 카테고리가 포함되어야 합니다.

참고 URL 범주를 기반으로 트래픽을 완전히 처리하려면 URL 필터링도 구성해야 합니다. URL 필터링 장을 참조하십시오.

로컬 데이터베이스에 없는 **URL**에 대한 쿼리

Decrypt - Resign(암호 해독 **-** 다시 서명**)** 규칙을 생성하고 로컬 데이터베이스에 카테고리와 평판이 없는 웹사이트로 사용자가 이동하는 경우, 데이터가 해독되지 않을 수 있습니다. 일부 웹사이트는 로컬 데이터베이스에서 카테고리가 분류되어 있지 않으며, 이 경우 이러한 웹사이트의 데이터는 기본적으로 암호 해독되지 않습니다.

이 동작은 **System(**시스템**) > Integration(**통합**) > Cloud Services** 설정에서 **Query Cisco cloud for unknown URLs(Cisco Cloud**에서 알 수 없는 **URL** 쿼리**)**를 선택하여 제어할 수 있습니다.

이 옵션에 대한 자세한 내용은 Cisco Cloud를 참고하십시오.

TLS/SSL 규칙 요구 사항 및 사정 요건

모델 지원

NGIPSv를 제외한 모두

지원되는 도메인

모든

사용자 역할

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

TLS/SSL 규칙 생성 및 수정

프로시저

단계 **1** Firepower Management Center에 로그인합니다.

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

단계 **3** SSL 정책 옆에 있는 수정( )을 클릭합니다.

보기 ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **4** 다음 옵션을 이용할 수 있습니다.

- 새 규칙을 추가하려면 **Add Rule(**규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 수정( )을 클릭합니다.

단계 **5** 규칙의 **Name(**이름**)**을 입력합니다.

단계 **6** 규칙이 **Enabled(**활성화**)** 상태인지 여부를 지정합니다.

단계 **7** 규칙 위치를 지정합니다(TLS/SSL 규칙 순서 평가 참고).

단계 **8** 규칙 **Action(**작업**)**을 클릭합니다(TLS/SSL 규칙 동작 구성, 18 페이지 참고).

단계 **9** 규칙 조건 및 옵션을 구성합니다.

a) **Zones(**영역**)**를 클릭하고 보안 영역에 따라 규칙 조건을 구성합니다(인터페이스 조건 참고).

b) **Networks(**네트워크**)**를 클릭하고 네트워크 또는 지리적 위치에 따라 규칙 조건을 구성합니다(네트워크 조건 참고).

c) **VLAN** 태그를 클릭하고 VLAN에 따라 규칙 조건을 구성합니다(VLAN 조건 참고).

d) **Users(**사용자**)**를 클릭하고 사용자 및 그룹에 따라 규칙 조건을 구성합니다(사용자, 영역 및 ISE 속성 조건(사용자 제어) 참고).

e) **Applications(**애플리케이션**)**를 클릭하고 애플리케이션에 따라 규칙 조건을 구성합니다(애플리케이션 조건(애플리케이션 컨트롤) 참고).

f) **Ports(**포트**)**를 클릭하고 통신 포트에 따라 규칙 조건을 구성합니다(포트 및 ICMP 코드 조건 참고).

g) **Category(**범주**)**를 클릭하고 URL 평판에 따라 규칙 조건을 구성합니다. URL 필터링에 관한 장(HTTPS 트래픽 필터링 포함)을 참고하십시오.

h) **Certificate(**인증서**)**를 클릭하고 TLS/SSL 서버 인증서에 따라 규칙 조건을 구성합니다(서버 인증서 기반 TLS/SSL 규칙 조건 참고).

i) **DN**을 클릭하고 고유 이름을 기준으로 규칙 조건을 구성합니다(인증서 고유 이름 TLS/SSL 규칙 조건 참고).

j) **Cert Status(**인증 상태**)**를 클릭하고 TLS/SSL 인증서 상태에 따라 규칙 조건을 구성합니다(인증서 상태 TLS/SSL 규칙 조건 참고).

k) **Cipher Suite(**암호 그룹**)**을 클릭하고 암호 그룹에 따라 규칙 조건을 구성합니다(암호 그룹 TLS/SSL 규칙 조건 참고).

l) **Version(**버전**)**을 클릭하고 TLS 또는 SSL 프로토콜 버전에 따라 규칙 조건을 구성합니다(암호화 프로토콜 버전 TLS/SSL 규칙 조건 참고).

m) **Logging(**로깅**)**을 클릭하고 규칙의 로깅 옵션을 구성합니다(연결 로깅 모범 사례 참고).

단계 **10** **Save(**저장**)**를 클릭합니다.

다음과 같은 오류가 표시되면 TLS/SSL 암호 그룹 확인: **Traffic cannot match this rule; none of your selected cipher suites contain a signature algorithm that the resigning CA's signature algorithm**를 참조하십시오.

다음에 수행할 작업

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

규칙 카테고리에 TLS/SSL 규칙 추가

프로시저

단계 1 SSL 규칙 편집기의 **Insert(**삽입**)** 드롭다운 목록에서 **Into Category(**카테고리에**)**를 선택한 후 사용할 카테고리를 선택합니다.

단계 2 **Save(**저장**)**를 클릭합니다.

팁 규칙을 저장하면 최종적으로 해당 카테고리에 위치합니다.

다음에 수행할 작업

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

번호로 TLS/SSL 규칙 포지셔닝

프로시저

단계 1 SSL 규칙 편집기의 **Insert(**삽입**)** 드롭다운 목록에서 **above rule(**규칙 위**)** 또는 **below rule(**규칙 아래**)**을 선택한 후 적절한 규칙 번호를 입력합니다.

단계 2 **Save(**저장**)**를 클릭합니다.

팁 규칙을 저장하면 지정한 위치에 배치됩니다.

다음에 수행할 작업

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

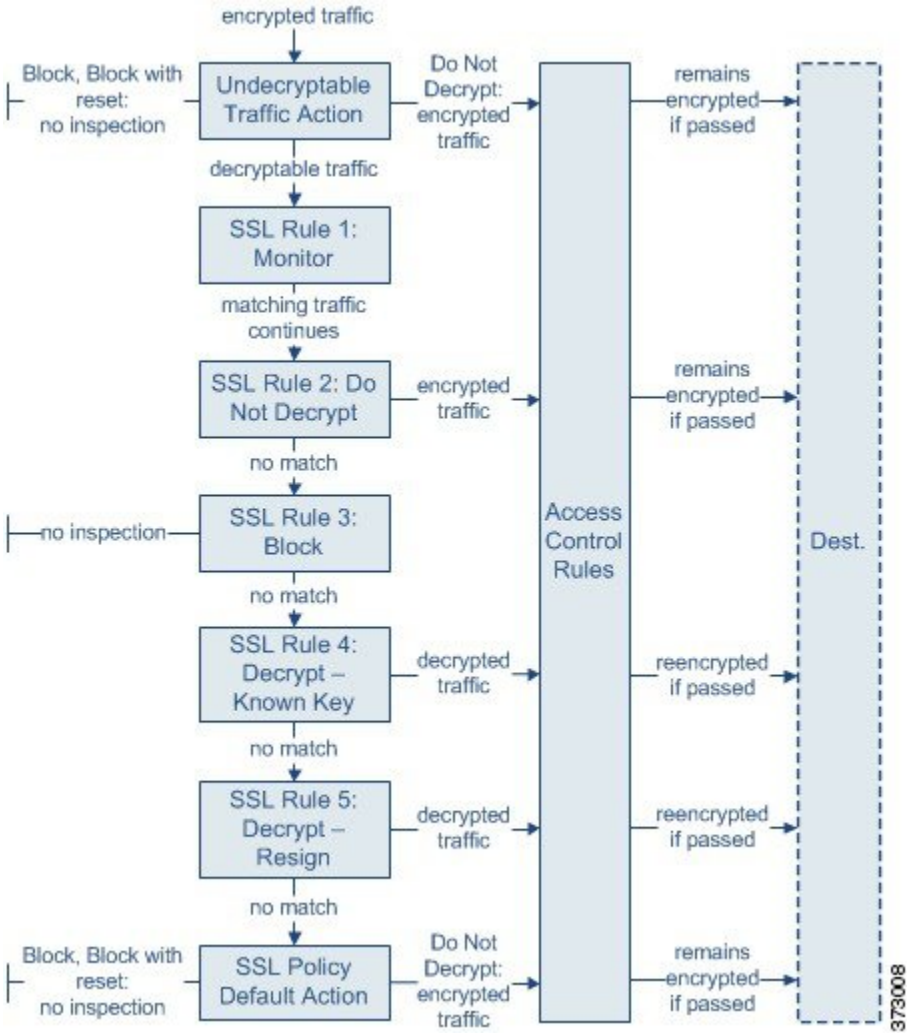
TLS/SSL 규칙 트래픽 처리

시스템은 사용자가 지정하는 순서대로 트래픽이 TLS/SSL 규칙과 일치하는지 확인합니다. 대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 TLS/SSL 규칙에 따라 암호화된 트래픽을 처리합니다. 조건은 간단할 수도 있고 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지리위

치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서 고유 이름(DN), 인증서 상태, 암호 그룹 또는 암호화 프로토콜 버전별로 트래픽을 제어할 수 있습니다.

각 규칙에는 작업이 있는데, 작업은 일치하는 암호화되거나 암호 해독된 트래픽을 액세스 제어로 모니터링, 차단 또는 검사할지 여부를 결정합니다. 시스템은 차단하는 암호화 트래픽을 추가 검사하지 않습니다. 암호화된 트래픽과 해독 불가 트래픽은 액세스 제어로 검사합니다. 그러나 일부 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적을 수 있습니다. 또한 기본적으로 시스템은 암호화된 페이로드의 침입 및 파일 검사를 비활성화합니다.

다음 시나리오는 인라인 구축에서 SSL 규칙이 트래픽을 처리하는 방식을 요약한 것입니다.



이 시나리오에서, 트래픽은 다음과 같이 평가됩니다.

- **Undecryptable Traffic Action**은 암호화 트래픽을 먼저 평가합니다. 시스템에서 해독할 수 없는 트래픽은 추가 검사 없이 차단하거나 액세스 제어 검사를 위해 전달합니다. 매칭하지 않는 암호화 트래픽은 다음 규칙으로 진행합니다.

- **TLS/SSL** 규칙 **1: Monitor(**모니터링**)**가 다음으로 암호화 트래픽을 평가합니다. Monitor(모니터링) 규칙은 암호화 트래픽을 추적하고 로깅하지만 트래픽 플로우에 영향을 주지 않습니다. 시스템은 허용할지 아니면 거부할지 여부를 결정하기 위해 계속해서 트래픽을 추가 규칙에 일치시킵니다.
- **TLS/SSL** 규칙 **2: Do Not Decrypt(**암호 해독 안 함**)**가 세 번째로 암호화 트래픽을 평가합니다. 일치하는 트래픽은 암호 해독되지 않습니다. 시스템은 이 트래픽을 액세스 제어로 검사하지만 파일 또는 침입 검사는 하지 않습니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- **TLS/SSL** 규칙 **3: Block(**차단**)**에서 네 번째로 암호화 트래픽을 평가합니다. 일치하는 트래픽은 추가 검사 없이 차단됩니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- **TLS/SSL** 규칙 **4: Decrypt - Known Key(**암호 해독 - 알려진 키**)**에서 다섯 번째로 암호화 트래픽을 평가합니다. 네트워크에 수신된 매칭 트래픽은 업로드된 개인 키를 사용하여 해독됩니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사 결과에 따라 시스템이 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **TLS/SSL** 규칙 **5: Decrypt - Resign(**암호 해독 - 다시 서명**)**이 최종 규칙입니다. 트래픽이 이 규칙과 일치하면 시스템은 업로드된 CA 인증서로 서버 인증서를 다시 서명한 다음 중간자(man-in-the-middle) 역할을 하여 트래픽 암호를 해독합니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사 결과에 따라 시스템이 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **SSL Policy Default Action(SSL** 정책 기본 작업**)**은 어떤 TLS/SSL 규칙과도 일치하지 않는 모든 트래픽을 처리합니다. 이 기본 작업은 암호화 트래픽을 추가 검사 없이 차단하거나 해독하지 않고 액세스 제어 검사를 위해 전달합니다.

암호화된 트래픽 검사 설정

암호화 세션 특성을 기반으로 암호화 트래픽을 제어하고 암호화 트래픽을 해독하려면 재사용 가능한 PKI(Public Key Infrastructure) 개체를 생성해야 합니다. SSL 정책에 신뢰받는 CA(certificate authority) 인증서를 업로드하고 SSL 규칙 조건을 생성하는 시점에 이 정보를 추가하여 해당 개체를 생성할 수 있습니다. 그러나 이 개체를 미리 구성하면 잘못된 개체가 생성될 가능성이 줄어듭니다.

인증서 및 쌍 키를 사용하여 암호화 트래픽 해독

세션 암호화에 사용되는 서버 인증서와 개인 키를 업로드하여 내부 인증서 개체를 구성하면 들어오는 암호화된 트래픽을 암호 해독할 수 있습니다. **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업이 있는 SSL 규칙에서 해당 개체를 참조하고 트래픽이 해당 규칙과 일치하는 경우, 시스템은 업로드된 개인 키를 사용하여 세션의 암호를 해독합니다.

또한 CA 인증서와 개인 키를 업로드하여 내부 CA 개체를 구성하면 시스템이 나가는 트래픽도 암호 해독할 수 있습니다. **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업이 있는 SSL 규칙에서 해당 개체를 참조하고 트래픽이 해당 규칙과 일치하는 경우, 시스템은 클라이언트 브라우저로 전달된 서버 인증

서에 다시 서명한 다음 중간자(man-in-the-middle) 역할을 하여 트래픽 암호를 해독합니다.원하는 경우 전체 인증서가 아닌 SSC(자가 서명 인증서) 키만 교체할 수 있습니다. 이 경우 사용자의 브라우저에는 SSC(자가 서명 인증서) 키 알림이 표시됩니다.

암호화 세션 특성 기반의 트래픽 제어

시스템은 세션 협상에 사용된 암호 그룹 또는 서버 인증서를 기반으로 암호화 트래픽을 제어할 수 있습니다. 여러 재사용 가능 개체 중 하나를 구성하고 TLS/SSL 규칙 조건에서 해당 개체를 참조하여 트래픽의 일치 여부를 확인할 수 있습니다. 다음 표에서는 구성할 수 있는 재사용 가능 개체의 여러 유형에 대해 설명합니다.

다음을 구성할 경우	다음 조건을 기반으로 암호화 트래픽 제어 가능
하나 이상의 암호 그룹을 포함한 암호 그룹 목록	암호화 세션 협상에 사용되는 암호 그룹이 암호 그룹 목록에 있는 암호 그룹의 일치 여부를 확인합니다.
조직에서 신뢰하는 CA 인증서를 업로드하는 방법으로 신뢰할 수 있는 CA 개체 구성	다음 조건에서 신뢰할 수 있는 CA가 세션 암호화에 사용된 서버 인증서를 신뢰합니다. • CA가 직접 인증서를 발급한 경우 • CA가 중개 CA에 인증서를 발급했고, 이 중개 CA가 서버 인증서를 발급한 경우
서버 인증서를 업로드하는 방법으로 외부 인증서 개체 구성	세션 암호화에 사용된 서버 인증서가 업로드된 서버 인증서와 일치합니다
인증서 주체 또는 발급자 고유 이름(DN)을 포함하는 DN 개체	세션 암호화에 사용된 인증서의 주체 또는 발급자 공용 이름(CN), 국가, 조직 또는 조직 단위가 구성된 고유 이름(DN)과 일치합니다

관련 항목

암호 그룹 목록
고유 이름 개체
PKI 개체

TLS/SSL 규칙 순서 평가

SSL 정책에서 TLS/SSL 규칙을 생성할 때는, 규칙 편집기에서 **Insert(**삽입**)** 목록을 이용해 순위를 지정해야 합니다. SSL 정책의 TLS/SSL 규칙에는 1부터 시작하는 숫자가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 TLS/SSL 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 규칙의 모든 조건이 트래픽과 일치하는 첫 번째 TLS/SSL 규칙에 따라 네트워크 트래픽을 처리합니다. Monitor(모니터링) 규칙(트래픽을 로깅하지만 트래픽 흐름에 영향을 주지 않음)의 경우를 제외하고 트래픽이 규칙과 일치하면 시스템은 추가적이고 우선 순위가 낮은 규칙에 대해 계속해서 트래픽을 평가하지 않습니다. 조건은 간단할 수도 있고 복잡할 수도 있습니다. 보안 영역, 네트워크 또는 지리위치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서

고유 이름(DN), 인증서 상태, 암호 그룹 또는 암호화 프로토콜 버전별로 트래픽을 제어할 수 있습니다.

각 규칙에는 작업이 있는데, 작업은 일치하는 암호화되거나 암호 해독된 트래픽을 액세스 제어로 모니터링, 차단 또는 검사할지 여부를 결정합니다. 시스템은 차단하는 암호화 트래픽을 추가 검사하지 않습니다. 암호화된 트래픽과 해독 불가 트래픽은 액세스 제어 대상입니다. 그러나 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로, 암호화된 트래픽과 일치하는 규칙이 더 적습니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

팁 TLS/SSL 규칙 순서가 올바르면 네트워크 트래픽 처리에 필요한 리소스가 줄어들면서 규칙 선점이 방지됩니다. 사용자가 생성한 규칙이 모든 조직과 배포에 고유하더라도 사용자의 필요를 처리하는 동안 성능을 최적화할 수 있는 규칙을 언제 지시할지에 대해 몇 가지 따라야 할 지침이 있습니다.

번호로 규칙의 순서를 지정하는 것 외에도 카테고리로 규칙을 그룹화할 수 있습니다. 기본적으로 시스템에서는 Administrator(관리자), Standard(표준) 그리고 Root(루트)의 3가지 카테고리를 제공합니다. 맞춤형 카테고리를 추가할 수는 있지만 시스템에서 제공하는 카테고리를 삭제하거나 순서를 변경할 수는 없습니다.

관련 항목

- 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션
- SSL 규칙 순서
- 액세스 제어 규칙 순서에 대한 모범 사례

TLS/SSL 규칙 조건

SSL 규칙의 조건은 규칙에서 처리하는 암호화 트래픽의 유형을 식별합니다. 조건은 단순하거나 복잡할 수 있으며, 하나의 규칙에 둘 이상의 조건 유형을 지정할 수 있습니다. 트래픽이 규칙의 모든 조건을 충족해야 규칙이 트래픽에 적용됩니다.

규칙에 대해 특정 조건을 구성하지 않으면 시스템은 해당 기준에 따라 트래픽을 매칭하지 않습니다. 예를 들어 인증서 조건이 있지만 버전 조건이 없는 규칙은 세션 SSL 또는 TLS 버전과 무관하게 세션 협상에 쓰인 서버 인증서를 기반으로 트래픽을 평가합니다.

모든 TLS/SSL 규칙에는 일치하는 암호화 트래픽에 대해 다음을 결정하는 연결된 작업이 있습니다.

- 처리: 가장 중요한 것은 규칙의 조건과 일치하는 암호화된 트래픽을 시스템이 모니터링, 신뢰, 차단 또는 암호 해독할지 여부를 규칙 작업이 제어한다는 것입니다.
- 로깅: 이 규칙 작업은 일치하는 암호화 트래픽에 대한 상세정보를 언제 어떻게 로깅할 수 있는지 결정합니다.

TLS/SSL 검사 구성에서 해독된 트래픽을 처리, 검사, 로깅합니다.

- SSL 정책의 암호 해독 불가 작업은 시스템에서 암호 해독할 수 없는 트래픽을 처리합니다.
- 정책의 기본 작업은 Monitor(모니터링)가 아닌 TLS/SSL 규칙의 조건을 충족하지 않는 트래픽을 처리합니다.

시스템에서 암호화된 세션을 차단하거나 신뢰할 때 연결 이벤트를 로깅할 수 있습니다. 또한 시스템이 나중에 트래픽을 처리하거나 검사하는 방법과 관계없이 액세스 제어 규칙을 통한 추가 평가를 위해 시스템이 해독하는 연결을 반드시 로깅하도록 설정할 수도 있습니다. 암호화 세션의 연결 로그는 세션 암호화에 사용된 인증서와 같은 해독 세부 사항이 포함되어 있습니다. 연결 종료 이벤트만 로깅할 수 있지만 다음 예외가 적용됩니다.

- 차단된 연결(Block(차단), Block with reset(차단 후 재설정))의 경우, 시스템이 즉시 세션을 종료하고 이벤트를 생성합니다.
- Do not decrypt(암호 해독 안 함)로 지정된 신뢰할 수 있는 연결의 경우, 시스템이 세션 종료 시 이벤트를 생성합니다.

TLS/SSL 규칙 조건 유형

SSL 규칙을 추가하거나 수정할 때 규칙 편집기의 왼쪽 아래에 있는 탭을 사용하여 규칙 조건을 추가하고 수정합니다.

표 *1: TLS/SSL* 규칙 조건 유형

조건	암호화 트래픽 매칭	세부 사항
영역	특정 보안 영역의 인터페이스를 통해 디바이스에 들어오거나 디바이스에서 나감	보안 영역은 배포 및 보안 정책에 따라 하나 이상의 인터페이스를 논리적으로 그룹화한 것입니다. 한 영역의 인터페이스는 여러 디바이스에 위치할 수 있습니다.
네트워크	해당 소스 또는 대상 IP 주소, 국가 또는 대륙	명시적으로 IP 주소를 지정할 수 있습니다. 지리위치 기능을 사용하여 해당 소스 또는 대상 국가나 대륙에 근거하여 트래픽을 제어할 수도 있습니다.
VLAN 태그	VLAN별로 태그됨	시스템에서는 가장 안쪽의 VLAN 태그를 사용하여 VLAN을 기준으로 패킷을 확인합니다.
포트	해당 소스 또는 대상 포트	TCP 포트를 기반으로 암호화 트래픽을 제어할 수 있습니다.

조건	암호화 트래픽 매칭	세부 사항
사용자	세션에 개입된 사용자별	모니터링되는 암호화 세션에 쓰인 호스트에 로그인한 LDAP 사용자를 기반으로 암호화 트래픽을 제어할 수 있습니다. Microsoft Active Directory 서버에서 검색된 개별 사용자 또는 그룹을 기준으로 트래픽을 제어할 수 있습니다.
애플리케이션	세션에서 탐지되는 애플리케이션별	암호화 세션에서 개별 애플리케이션에 대한 액세스를 제어하거나 유형, 위험, 비즈니스 연관성, 범주와 같은 기본 특성에 따라 액세스를 필터링할 수 있습니다.
범주	인증서 주체 DN을 기반으로 하여 세션에서 요청된 URL을 기준으로 매칭	URL의 일반 분류 및 위험 레벨을 기반으로 네트워크 사용자가 액세스 가능한 웹사이트를 제한할 수 있습니다.
고유 이름(DN)	사용자가 브라우저에 입력하는 URL이 CN(Common Name)과 일치하거나, URL이 인증서의 SAN(Subject Alternative Name)에 포함되어 있습니다.	서버 인증서를 발급한 CA 또는 서버 인증서 소유자를 기반으로 암호화 트래픽을 제어할 수 있습니다.
인증서	암호화 세션의 협상에 쓰이는 서버 인증서를 기준으로 매칭	암호화 세션의 협상을 위해 사용자의 브라우저에 전달된 서버 인증서를 기반으로 암호화 트래픽을 제어할 수 있습니다.
인증서 상태	암호화 세션의 협상에 쓰이는 서버 인증서의 속성을 기준으로 매칭	서버 인증서의 상태를 기반으로 암호화 트래픽을 제어할 수 있습니다.
암호 그룹	암호화 세션의 협상에 쓰이는 암호 그룹을 기준으로 매칭	서버에서 암호화 세션의 협상을 위해 선택한 암호 그룹을 기반으로 암호화 트래픽을 제어할 수 있습니다.
버전	세션 암호화에 쓰이는 SSL 또는 TLS 버전을 기준으로 매칭	세션 암호화에 쓰이는 SSL 또는 TLS 버전을 기반으로 암호화 트래픽을 제어할 수 있습니다.

관련 항목

- 네트워크 기반 TLS/SSL 규칙 조건
- 사용자 기반 TLS/SSL 규칙 조건
- 암호화된 트래픽의 평판 기반 URL 차단
- 서버 인증서 기반 TLS/SSL 규칙 조건

TLS/SSL 규칙 작업

다음 섹션에서는 TLS/SSL 규칙과 함께 사용할 수 있는 작업을 설명합니다.

TLS/SSL 규칙 모니터링 작업

Monitor(모니터링**)** 작업은 트래픽을 허용하거나 거부하도록 설계되지 않았습니다. 이 작업의 기본 목적은 일치하는 트래픽의 처리 방식에 상관없이 연결 로깅을 강제하는 것입니다. 그런 다음 추가 규칙이 있다면 매칭하여 트래픽을 신뢰, 차단, 해독할지 여부를 결정합니다. 일치하는 첫 번째 비 Monitor(모니터링) 규칙은 트래픽 흐름과 추가 검사를 결정합니다. 추가로 일치하는 규칙이 없는 경우, 시스템은 기본 작업을 사용합니다.

Monitor(모니터링) 규칙의 주요 목표는 네트워크 트래픽을 추적하는 것이므로 시스템은 규칙의 로깅 구성이나 나중에 연결을 처리하는 기본 작업에 관계없이 모니터링되는 트래픽의 연결 종료 이벤트를 Firepower Management Center 데이터베이스에 자동으로 로깅합니다.

TLS/SSL 규칙 Do Not Decrypt(암호 해독 안 함) 작업

Do Not Decrypt(암호 해독 안 함**)** 작업은 액세스 제어 정책의 규칙 및 기본 작업을 통한 평가를 위해 암호화 트래픽을 전달합니다. 일부 액세스 제어 규칙 조건은 암호화되지 않은 트래픽을 요구하므로 이 트래픽이 더 적은 수의 규칙과 매칭할 수도 있습니다. 시스템은 암호화된 트래픽에 대해 침입 또는 파일 검사와 같은 심층 검사를 수행할 수 없습니다.

Do Not Decrypt(암호 해독 안 함**)** 규칙 작업의 일반적인 이유는 다음과 같습니다.

- TLS/SSL 트래픽 암호 해독이 법률로 금지되는 경우.
- 신뢰할 수 있는 사이트.
- 트래픽을 검사하면 지장을 줄 수 있는 사이트(예: Windows 업데이트).
- 연결 이벤트를 사용하여 TLS/SSL 연결 이벤트의 값을 보기 위해. (연결 이벤트 필드를 보기 위해 트래픽을 해독할 필요가 없습니다.) 자세한 내용은 연결 이벤트 필드 채우기 요구 사항를 참고하십시오.

자세한 내용은 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션을 참조해 주십시오.

TLS/SSL 규칙 차단 작업

Firepower System은 시스템을 통과해선 안 되는 트래픽에 대한 다음 TLS/SSL 규칙 작업을 제공합니다.

- **Block(**차단**)**을 이용해 연결을 종료하면 클라이언트 브라우저에 오류가 발생합니다.

  오류 메시지는 사이트가 정책으로 인해 차단되었음을 나타내지 않습니다. 대신 일반적인 암호화 알고리즘이 없다는 오류가 표시될 수 있습니다. 이 메시지만으로는 연결이 의도적으로 차단되었는지를 명확하게 파악할 수 없습니다.

- **Block with reset(**차단 후 재설정**)**을 이용해 연결을 종료하고 재설정하면, 클라이언트 브라우저에 오류가 발생합니다.

  이 오류는 연결이 재설정되었음을 표시하지만 이유는 표시하지 않습니다.

팁 패시브 또는 인라인(탭 모드) 구축에서는 디바이스에서 직접 트래픽을 검사하지 않으므로 **Block(**차단**)** 또는 **Block with reset(**차단 후 재설정**)** 작업을 사용할 수 없습니다. **Block(**차단**)** 또는 **Block with reset(**차단 후 재설정**)** 작업의 규칙을 생성할 경우 여기에 보안 영역 조건의 패시브 또는 인라인(탭 모드) 인터페이스가 포함된다면 정책 편집기는 해당 규칙의 옆에 경고(⚠)를 표시합니다.

TLS/SSL 규칙 암호 해독 작업

Decrypt - Known Key(암호 해독 - 알려진 키**)** 및 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 작업은 암호화된 트래픽을 암호 해독합니다. 시스템에서는 액세스 제어를 통해 암호 해독된 트래픽을 검사합니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 검색 데이터를 위해 트래픽을 조사하고 침입, 금지된 파일, 악성코드를 탐지하여 차단할 수 있습니다. 허용된 트래픽은 다시 암호화되어 목적지에 전달됩니다.

신뢰할 수 있는 CA(Certification Authority)의 인증서를 사용하여 트래픽의 암호를 해독하는 것이 좋습니다. 이렇게 하면 연결 이벤트의 SSL Certificate Status(SSL 인증서 상태) 열에 **Invalid Issuer**가 표시되지 않습니다.

신뢰할 수 있는 개체를 추가하는 방법에 대한 자세한 내용은 신뢰할 수 있는 인증 기관 개체를 참조하십시오.

TLS/SSL 규칙 동작 구성

시작하기 전에

참조:

- TLS/SSL 규칙 차단 작업, 17 페이지
- TLS/SSL 규칙 Do Not Decrypt(암호 해독 안 함) 작업, 17 페이지
- TLS/SSL 규칙 모니터링 작업, 17 페이지

프로시저

단계 **1** SSL 정책 편집기에는 다음과 같은 옵션이 있습니다.

- 새 규칙을 추가하려면 **Add Rule(**규칙 추가**)**을 클릭합니다.
- 기존 규칙을 수정하려면 수정( )을 클릭합니다.

단계 2 **Action(**작업**)** 드롭다운 목록에서 규칙 작업을 선택합니다.

- 암호화된 트래픽을 차단하려면 **Block(**차단**)**을 선택합니다.
- 암호화된 트래픽을 차단하고 연결을 재설정하려면 **Block with reset(**차단 후 재설정**)**을 선택합니다.
- 수신 트래픽을 해독하려면 암호 해독 설정 - 알려진 키 작업, 20 페이지의 자세한 내용을 참조하십시오.
- 발신 트래픽을 해독하려면 암호 해독 설정 - 재서명 작업, 19 페이지를 참조하십시오.
- 암호화된 트래픽을 로깅하려면 **Monitor(**모니터링**)**를 선택합니다.
- 암호화된 트래픽을 해독하지 않으려면 **Do not decrypt(**암호 해독 안 함**)**를 선택합니다.

단계 3 **Add(**추가**)**를 클릭합니다.

다음에 수행할 작업

- 규칙 소개에 설명된 대로 규칙 조건을 구성합니다.
- 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

암호 해독 설정 - 재서명 작업

시작하기 전에

TLS/SSL 암호 해독 - 파기 지침, 4 페이지의 내용을 참조하십시오.

프로시저

단계 1 SSL 규칙 편집기의 **Action(**작업**)** 목록에서 **Decrypt - Resign(**암호 해독 - 다시 서명**)**을 선택합니다.

단계 2 목록에서 내부 CA 인증서 개체를 선택합니다.

단계 3 **Replace Key(**키 바꾸기**) Replace Key Only(**키만 바꾸기**)** 를 선택합니다.

암호 해독 - 재서명 규칙 작업을 설정할 때는 키 교환 키만 바꾸기 확인란을 항상 확인해야 합니다.

사용자가 직접 서명 인증서를 사용하는 웹사이트를 탐색하면, 웹 브라우저에서 보안 경고가 표시되며 안전하지 않은 사이트와 통신 중이라고 경고합니다.

사용자가 신뢰할 수 있는 인증서를 사용하는 웹사이트를 탐색할 때는 보안 경고가 표시되지 않습니다.

단계 4 **Add(**추가**)**를 클릭합니다.

단계 5 선택 사항. SSL 정책에서 신뢰할 수 있는 CA 인증서를 사용하여 연결 이벤트의 SSL Certificate Status(SSL 인증서 상태) 열에서 **Invalid Issuer**를 방지하려면 정책에 인증서를 추가합니다.

a) SSL 정책 편집기 페이지에서 **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)**를 클릭합니다.

b) 알려진 키에 해당하는 CA 인증서를 SSL 정책에 추가합니다.

다음에 수행할 작업

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

암호 해독 설정 - 알려진 키 작업

시작하기 전에

TLS/SSL 암호 해독 - 알려진 키 지침, 5 페이지의 내용을 참조하십시오.

프로시저

단계 **1** SSL 규칙 편집기의 **Action(**작업**)** 목록에서 **Decrypt - Known Key(**암호 해독 - 알려진 키**)**를 선택합니다.

단계 **2** **Click to select decryption certs** 필드를 클릭합니다.

단계 **3** **Available Certificates(**사용 가능한 인증서**)** 목록에서 하나 이상의 내부 인증서 개체를 클릭한 다음 **Add to Rule(**규칙에 추가**)**을 클릭합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Add(**추가**)**를 클릭합니다.

단계 **6** 선택 사항. SSL 정책에서 신뢰할 수 있는 CA 인증서를 사용하여 연결 이벤트의 SSL Certificate Status(SSL 인증서 상태) 열에서 **Invalid Issuer**를 방지하려면 정책에 인증서를 추가합니다.

a) SSL 정책 편집기 페이지에서 **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)**를 클릭합니다.

b) 알려진 키에 해당하는 CA 인증서를 SSL 정책에 추가합니다.

다음에 수행할 작업

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

TLS/SSL 관리 규칙

SSL 정책 편집기의 **Rules(**규칙**)**를 사용하여 정책에서 TLS/SSL 규칙을 추가, 편집, 이동, 활성화, 비활성화, 삭제하고 기타 방식으로 관리할 수 있습니다.

TLS/SSL 규칙 검색

공백과 인쇄 가능 특수 문자가 포함된 영숫자 문자열을 사용하여 TLS/SSL 규칙의 목록에서 일치하는 값을 찾을 수 있습니다. 검색은 규칙에 추가한 규칙 조건 및 규칙 이름을 검사합니다. 규칙 조건을

위해 검색은 각 조건 유형(영역, 네트워크, 애플리케이션, 등)에 추가할 수 있는 모든 이름 또는 값에 일치합니다. 여기에는 개별 개체 이름 또는 값, 그룹 개체 이름, 그룹 내 개별 개체 이름 또는 값, 그리고 문자 값이 포함됩니다.

완전한 또는 부분 검색 문자열을 사용할 수 있습니다. 일치 값을 위한 열은 각 일치하는 규칙에 강조 표시됩니다. 예를 들어, 스트링 `100Bao`의 전체 또는 일부를 최소한도로 검색하는 경우, 애플리케이션 열은 100Bao 애플리케이션을 추가한 각 규칙에 강조 표시됩니다. `100Bao`라는 이름의 규칙도 있다면 Name 및 Applications 열 모두 하이라이트됩니다.

이전에 일치하는 규칙 또는 다음에 일치하는 규칙 각각으로 이동할 수 있습니다. 상태 메시지는 현재 일치하는 규칙과 일치하는 총 수를 나타냅니다.

일치는 여러 페이지로 구성된 규칙 목록의 어느 페이지에서나 발생할 수 있습니다. 첫 번째 일치가 첫 번째 페이지에 없는 경우, 첫 번째 일치가 발생한 페이지가 표시됩니다. 마지막 일치 중일 때 다음 일치를 선택하면 첫 번째 일치로 이동하며, 첫 번째 일치 중일 때 이전 일치를 선택하면 마지막 일치로 이동합니다.

TLS/SSL 규칙 검색

프로시저

단계 **1** SSL 정책 편집기에서 **Search Rules(**검색 규칙**)** 프롬프트를 클릭하고 검색 문자열을 입력한 다음 Enter를 누릅니다.

팁 일치하는 값을 가진 규칙의 열이 강조 표시되며, 이는 명시된 (첫 번째) 일치를 위한 강조 표시와는 차별화됩니다.

단계 **2** 관심이 가는 규칙을 찾으십시오.

- 일치하는 규칙을 탐색하려면 **Next-Match(**다음 일치**)** 또는 **Previous-Match(**이전 일치**)**를 클릭합니다.
- 페이지를 새로 고침하고 검색 문자열 및 강조 표시를 지우려면, 지우기(✕)을 클릭합니다.

TLS/SSL 규칙 활성화 및 비활성화

TLS/SSL 규칙을 생성하면 기본적으로 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다. SSL 정책에서 규칙의 목록을 볼 때 비활성화된 규칙은 회색으로 표시됩니다. 단, 이 규칙은 수정 가능합니다. 규칙 편집기를 사용하여 TLS/SSL 규칙을 활성화하거나 비활성화할 수도 있습니다.

프로시저

단계 1 SSL 정책 편집기에서 규칙을 마우스 오른쪽 버튼으로 클릭하고 규칙 상태를 선택합니다.

단계 2 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

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

TLS/SSL 규칙 이동

프로시저

단계 1 SSL 정책 편집기에서 각 규칙의 빈 영역을 클릭하여 규칙을 선택합니다.

단계 2 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Cut(**잘라내기**)**을 선택합니다.

단계 3 잘라낸 규칙을 붙여넣을 위치 옆에 있는 규칙의 빈 영역을 마우스 오른쪽 버튼으로 클릭하고 **Paste above(**위 붙여넣기**)** 또는 **Paste below(**아래 붙여넣기**)**를 선택합니다.

팁 TLS/SSL 규칙을 복사하여 다른 SSL 정책에 붙여넣을 수는 없습니다.

단계 4 **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

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

새새 TLS/SSL 규칙 카테고리 추가

추가 정책을 생성하지 않고 Standard Rules(표준 규칙) 카테고리와 Root Ruels(루트 규칙) 카테고리 사이에 맞춤형 카테고리를 생성하여 규칙을 추가 구성할 수 있습니다. 추가한 카테고리의 이름을 변경하고 삭제할 수 있습니다. 이 카테고리를 이동할 수는 없지만 이 카테고리 안으로, 이 카테고리 안에서, 이 카테고리 밖으로 규칙을 이동할 수는 있습니다.

프로시저

단계 1 정책 편집기에서 **Add Category(**카테고리 추가**)**를 클릭합니다.

팁 정책에 이미 규칙이 포함된 경우, 새로운 규칙을 추가하기 전에 기존 규칙에 대한 행의 빈 영역을 클릭하여 새로운 카테고리의 위치를 지정합니다. 기존 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Insert new category(**새 카테고리 삽입**)**를 선택할 수도 있습니다.

단계 **2** **Name(**이름**)**을 입력합니다.

단계 **3** 다음 옵션을 이용할 수 있습니다.

- 첫 번째 **Insert(**삽입**)** 드롭다운 목록에서 **above Category(**카테고리 위**)**를 선택한 후 두 번째 드롭다운 목록에서 규칙을 배치할 위치 아래의 카테고리를 선택합니다.
- 드롭다운 목록에서 **below rule(**규칙 아래**)**을 선택한 다음, 기존 규칙 번호를 입력합니다. 이 옵션은 최소 하나의 규칙이 정책에 존재할 경우에만 유효합니다.
- 드롭다운 목록에서 **above rule(**규칙 위**)**을 선택한 다음 기존 규칙 번호를 입력합니다. 이 옵션은 최소 하나의 규칙이 정책에 존재할 경우에만 유효합니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

팁 삭제한 카테고리의 규칙은 상위 카테고리에 추가됩니다.

단계 **5** **Save(**저장**)**를 클릭합니다.