TLS/SSL 규칙

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 옵션이 **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL**이므로 *SSL* 정책이라는 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.

특히 TLS 암호화 가속에 관련된 지침은 TLS 암호화 가속를 참조하십시오.

관련 항목

TLS/SSL 암호 해독 사용 지침

일반 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.

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 정보, 41 페이지의 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.

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**,** 인라인 탭 모드 및 **SPAN** 인터페이스 지원되지 않음

TLS/SSL는 패시브, 인라인 탭 모드 또는 SPAN 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.

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, 6 페이지의 내용을 참조하십시오.

- 암호 해독 - 재서명 규칙 작업을 설정할 때는 **Replace Key Only(**키만 대체**)** 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 인증서

를 **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, 부록 F.1.1.1을 참조하십시오. (TLS 1.3에서 RFC 8446 부록 C.5로 교체됨)

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.

암호 해독 - 다시 서명 규칙 작업 및 인증서 서명 요청

Decrypt - Resign(암호 해독 - 다시 서명**)** 규칙 작업을 사용하려면 CSR(Certificate Signing Request)을 생성하고 신뢰할 수 있는 인증 기관의 서명을 받아야 합니다. (FMC를 사용하여 CSR: **Objects(**개체**)** > **Object Management(**개체 관리**)** > **PKI** > **Internal CAs(**내부 **CA)**를 생성할 수 있습니다.)

Decrypt - Resign(암호 해독 - 다시 서명**)** 규칙에서 사용하려면 CA(인증 기관)에 다음 확장 중 하나 이상이 있어야 합니다.

- **CA: TRUE**

  자세한 내용은 RFC3280, 섹션 4.2.1.10의 기본 제약 조건에 대한 설명을 참조하십시오.

- **KeyUsage=CertSign**

  자세한 내용은 RFC 5280, 섹션 4.2.1.3을 참조하십시오.

CSR 또는 CA에 위의 확장 중 하나 이상이 있는지 확인하려면 openssl 설명서와 같은 참조에 설명된 대로 **openssl** 명령을 사용할 수 있습니다.

이는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 검사가 작동하기 때문에 필요한데, 그 이유는 TLS/SSL 정책에서 사용된 인증서가 중간자 역할을 하고 모든 TLS/SSL 연결을 프록시하도록 인증서를 즉시 생성하고 서명하기 때문입니다.

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.

일치하지 않는 암호 그룹

인증서와 일치하지 않는 암호 그룹으로 TLS/SSL 규칙을 저장하려고 시도하면 다음과 같은 오류가 표시됩니다. 문제를 해결하려면 TLS/SSL 암호 그룹 확인, 46 페이지의 내용을 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.

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 **Information(**정보**)** ( )을 표시합니다. 모든 외부 인증서 개체 또는 모든 암호 그룹에 대해 서명 알고리즘 유형을 잘못 매칭할 경우, 정책은 규칙 옆에 경고 아이콘(**Warning(**경고**)** ( ))을 표시하며, SSL 정책과 연결된 액세스 제어 정책을 구축할 수 없습니다.

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, 부록 F.1.1.1을 참조하십시오. (TLS 1.3에서 RFC 8446 부록 C.5로 교체됨)

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.

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 사용자 지정 가능한 응답 페이지를 표시합니다.

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 구성

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.

애플리케이션이 TLS/SSL 피닝을 사용 중인지 확인하려면 를 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, 부록 F.1.1.1을 참조하십시오. (TLS 1.3에서 RFC 8446 부록 C.5로 교체됨)

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 및 영역 디렉터리 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`(인

터넷 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**)** 클라우드 서비스 설정에서 **Query Cisco CSI for Unknown URLs(Cisco CSI**에서 알 수 없는 **URL** 쿼리**)** 를 선택하여 제어할 수 있습니다.

이 옵션에 대한 자세한 내용은 Firepower Management Center 관리 가이드의 *Cisco Cloud*를 참조하십시오.

TLS/SSL 규칙 요구 사항 및 사정 요건

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

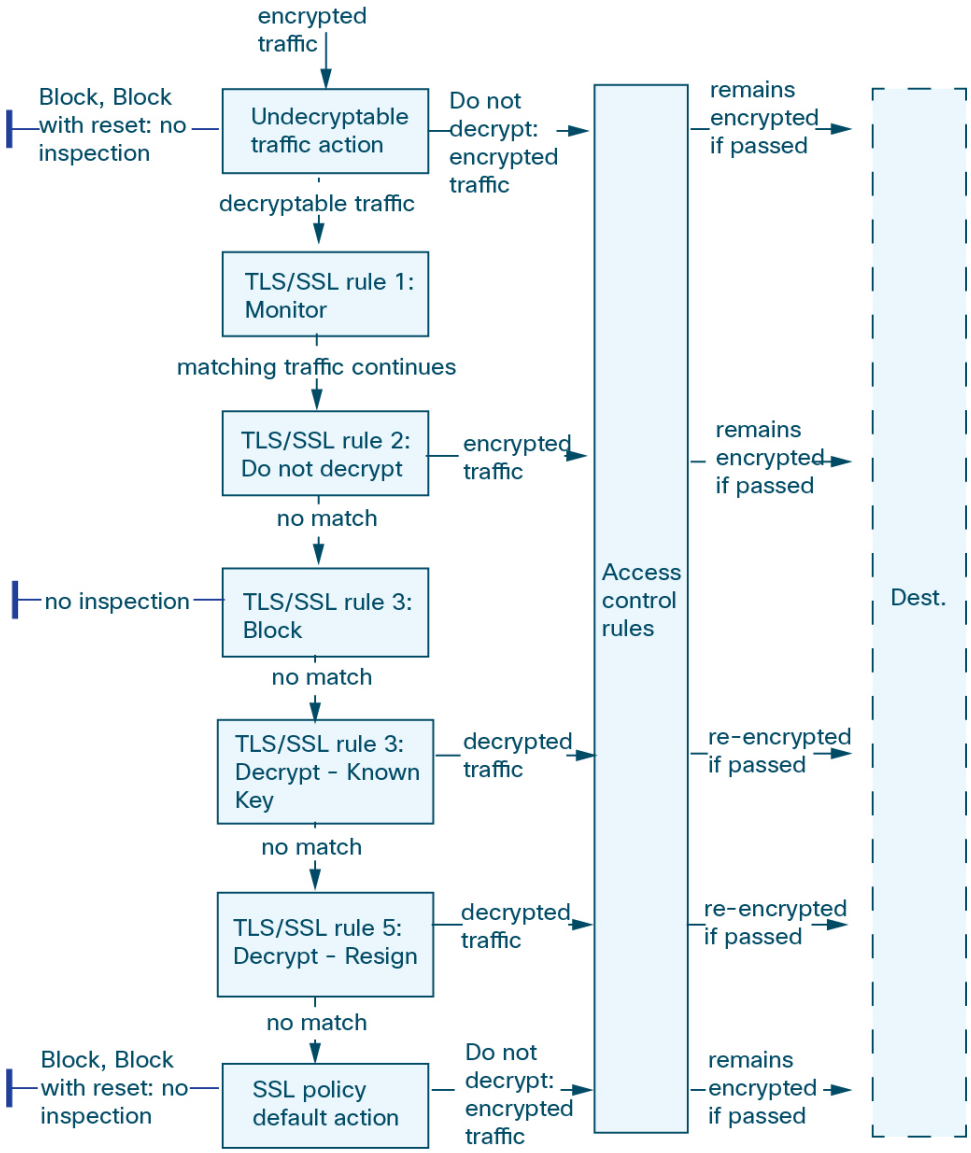
TLS/SSL 규칙 트래픽 처리

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 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 제어로 검사합니다. 그러나 일부 액세스 제

어 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. 시스

템은 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 인증서에 다시 서명한 다음 중간자(man-in-the-middle) 역할을 하여 트래픽 암호를 해독합니다.원하는 경

우 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(DN) 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
액세스 제어 규칙에 대한 모범 사례

TLS/SSL 규칙 조건

TLS/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 매칭하는 암호화 트래픽에 대해 다음 사항을 결정하는 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) 연결의 경우, 시스템이 세션 종료 시 이벤트를 생성합니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

주의 TLS/SSL 암호 해독이 비활성화되어 있을 때(액세스 컨트롤 정책에 SSL 정책이 포함되지 않을 때) 첫 번째 액티브 인증을 추가하거나 마지막 액티브 인증을 제거함 컨피그레이션 변경 사항을 구축할 때 Snort 프로세스가 재시작되므로 트래픽 검사가 일시적으로 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort 재시작 트래픽 동작을 참고하십시오.

활성 인증 규칙에는 **Active Authentication(**활성 인증**)** 규칙 작업 또는 **Use active authentication if passive or VPN identity cannot be established(**패시브 또는 **VPN ID**를 설정할 수 없는 경우 활성 인증 사용**)**가 선택된 **Passive Authentication(**패시브 인증**)** 규칙 작업이 있습니다.

관련 항목

보안 영역 규칙 조건
네트워크 규칙 조건
VLAN 태그 규칙 조건
사용자 규칙 조건
애플리케이션 규칙 조건
포트 규칙 조건
범주 규칙 조건, 19 페이지
서버 인증서 기반 TLS/SSL 규칙 조건, 19 페이지

보안 영역 규칙 조건

보안 영역은 네트워크를 세그멘테이션화하여 여러 디바이스에 걸쳐 인터페이스를 그룹화하는 방법을 통해 트래픽 흐름을 관리하고 분류할 수 있도록 지원합니다.

영역 규칙의 조건은 소스 및 대상 보안 영역을 통해 트래픽을 제어합니다. 소스 및 대상 영역 모두 영역 조건에 추가할 경우 소스 영역 중 하나의 인터페이스에서 트래픽 매치를 시작하고 대상 영역 중 하나의 인터페이스에서 종료해야 합니다.

영역의 모든 인터페이스가 동일한 유형이어야 하는 것과 마찬가지로(모든 인라인, 수동, 스위칭 또는 라우팅), 영역 조건에 사용된 모든 영역도 동일한 유형이어야 합니다. 패시브 방식으로 구축된 디바이스는 트래픽을 전송하지 않으므로 패시브 인터페이스를 대상 영역으로 하면서 영역을 사용할 수 없습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

팁 영역으로 규칙을 제한하는 것은 시스템 성능을 개선할 수 있는 가장 좋은 방법 중 하나입니다. 규칙이 디바이스의 인터페이스를 통과하는 트래픽에 적용되지 않을 경우, 해당 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.

보안 영역 조건 및 멀티테넌시

다중 도메인 구축에서, 상위 도메인에 생성된 영역은 다른 도메인의 디바이스에 있는 인터페이스를 포함할 수 있습니다. 하위 도메인의 영역 조건을 구성할 경우, 컨피그레이션은 사용자가 볼 수 있는 인터페이스에만 적용됩니다.

네트워크 규칙 조건

네트워크 규칙 조건은 내부 헤더를 사용하여 트래픽의 소스 및 대상 IP 주소를 기준으로 삼아 트래픽을 제어합니다. 외부 헤더를 사용하는 터널 규칙에는 네트워크 조건 대신 터널 엔드포인트 조건이 있습니다.

사전 정의된 개체를 사용하여 네트워크 조건을 작성하거나, 수동으로 개별 IP 주소 또는 주소 블록을 지정할 수 있습니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 IP 주소를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

VLAN 태그 규칙 조건

참고 액세스 규칙의 VLAN 태그는 인라인 집합에만 적용됩니다. VLAN 태그가 있는 액세스 규칙은 방화벽 인터페이스의 트래픽과 일치하지 않습니다.

VLAN 규칙 조건은 Q-in-Q(스택 VLAN) 트래픽을 포함한 VLAN 태그가 있는 트래픽을 제어합니다. 시스템은 가장 안쪽의 VLAN 태그를 사용하여 VLAN 트래픽을 필터링하며, 규칙에서 가장 바깥쪽의 VLAN 태그를 사용하는 사전 필터 정책은 예외입니다.

다음 Q-in-Q 지원에 유의하십시오.

- Firepower 4100/9300의 FTD - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).
- 다른 모든 모델의 FTD:
  - 인라인 집합 및 패시브 인터페이스 - Q-in-Q를 지원합니다(최대 2개의 VLAN 태그 지원).
  - 방화벽 인터페이스 - Q-in-Q를 지원하지 않습니다(하나의 VLAN 태그만 지원).

사전 정의된 개체를 사용하여 VLAN 조건을 작성하거나, 1에서 4094 사이의 VLAN 태그를 수동으로 입력할 수 있습니다. VLAN 태그의 범위를 지정하려면 하이픈을 사용합니다.

최대 50개의 VLAN 조건을 지정할 수 있습니다.

클러스터에서 VLAN 일치에 문제가 발생하면 액세스 제어 정책 고급 옵션인 Transport/Network Preprocessor Settings(전송/네트워크 전처리기 구성)를 편집하고 **Ignore VLAN header when tracking connections(**연결 추적 시 **VLAN** 헤더 무시**)** 옵션을 선택합니다.

참고 시스템은 각 리프 도메인에 대해 별도의 네트워크 맵을 작성합니다. 다중 도메인 구축에서 리터럴 VLAN 태그를 사용하여 이 컨피그레이션을 제한하면 예기치 않은 결과가 발생할 수 있습니다. 하위 도메인 관리자는 재정의가 활성화된 개체를 사용하여 로컬 환경에 맞게 글로벌 컨피그레이션을 조정할 수 있습니다.

사용자 규칙 조건

사용자 규칙 조건은 연결을 시작한 사용자 또는 사용자가 속한 그룹을 기준으로 트래픽을 매칭합니다. 예를 들어, Finance 그룹의 모든 사용자가 네트워크 리소스에 액세스하는 것을 금지하도록 Block(차단) 규칙을 구성할 수 있습니다.

액세스 제어 규칙의 경우에만 먼저 액세스 제어에 다른 정책 연결에 설명된 대로 ID 정책을 액세스 제어 정책과 연결해야 합니다.

구성된 영역에 대한 사용자 및 그룹을 구성하는 것 외에도 다음 특수 ID 사용자에 대한 정책을 설정할 수 있습니다.

- Failed Authentication(실패한 인증): 캡티브 포털(captive portal) 인증에 실패한 사용자입니다.
- Guest(게스트): 캡티브 포털에서 게스트 사용자로 구성된 사용자입니다.
- No Authentication Required(인증 필요 없음): ID가 **No Authentication Required(**인증 필요 없음**)** 규칙 작업과 일치하는 사용자입니다.
- Unknown(알 수 없음): 식별할 수 없는 사용자입니다. 예를 들어 구성된 영역에 의해 다운로드되지 않은 사용자입니다.

애플리케이션 규칙 조건

시스템에서 IP 트래픽을 분석할 때, 사용자의 네트워크에서 자주 사용되는 애플리케이션을 식별하여 분류할 수 있습니다. 이 검색 기반 애플리케이션 인식은 애플리케이션 컨트롤을 위한 기본 요소로, 애플리케이션 트래픽을 제어하는 기능입니다.

시스템에서 제공되는 애플리케이션 필터는 유형, 위험, 사업 타당성, 카테고리, 태그라는 기본 특성에 따라 애플리케이션을 구성하여 애플리케이션 컨트롤을 수행할 수 있도록 지원합니다. 시스템에서 제공되는 필터를 조합하거나 애플리케이션을 맞춤형으로 조합하여 재사용 가능한 사용자 정의 필터를 생성할 수 있습니다.

정책의 애플리케이션 규칙 조건마다 적어도 하나의 탐지기가 활성화되어야 합니다. 애플리케이션에 탐지기가 활성화되지 않은 경우, 시스템은 시스템에서 제공된 모든 탐지기를 해당 애플리케이션에 자동으로 활성화합니다. 시스템에서 제공된 탐지기가 없는 경우, 시스템은 가장 최근에 수정된 사용자 정의 탐지기를 애플리케이션에 활성화합니다. 애플리케이션 탐지기에 대한 자세한 내용은 애플리케이션 탐지기 기초을 참조하십시오.

두 애플리케이션 필터를 모두 사용하거나 개별적으로 지정된 애플리케이션을 사용하여 완전한 커버리지를 보장할 수 있습니다. 그러나 액세스 제어 규칙 순서를 지정하기 전에 다음을 참고하십시오.

(Snort 2만 해당.) 애플리케이션 컨트롤의 일부로, 액세스 제어 규칙을 사용하여 콘텐츠 제한(예: 안전 검색 및 YouTube EDU)을 시행할 수도 있습니다.

⚠

주의 액세스 제어 규칙을 올바르게 설정하지 못하는 경우, 차단해야 하는 트래픽이 허용되는 등 예기치 못한 결과가 발생할 수 있습니다. 일반적으로 애플리케이션 제어 규칙은 액세스 제어 목록에서 낮은 순위에 있어야 합니다. 한 예로 IP 주소에 기반한 애플리케이션 제어 규칙의 경우 매칭되려면 시간이 더 오래 걸리기 때문입니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 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 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

애플리케이션 필터의 이점

애플리케이션 필터는 애플리케이션 컨트롤을 신속하게 구성하는 데 도움이 됩니다. 예를 들어 시스템에서 제공되는 필터를 손쉽게 사용하여 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 식별하고 차단하는 액세스 제어 규칙을 생성할 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 시스템에서는 해당 세션을 차단합니다.

애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 이를 통해 시스템이 애플리케이션 트래픽을 정상적으로 제어할 수 있습니다. Cisco에서는 시스템 및 VDB(Vulnerability Database) 업데이트를 통해 애플리케이션 탐지기를 자주 업데이트하고 추가하므로, 시스템에서는 최신 탐지기를 사용하여 애플리케이션 트래픽을 모니터링할 수 있습니다. 자체 탐지기를 생성하고 이러한 탐지기로 탐지한 애플리케이션에 특성을 할당할 수도 있으며, 이는 기존 필터에 자동으로 추가됩니다.

애플리케이션 특성

시스템은 다음 표에서 설명하는 조건을 사용해 탐지하는 각 애플리케이션을 구별합니다. 애플리케이션 필터로 이러한 특성을 사용합니다.

표 *1:* 애플리케이션 특성

특성	설명	예
유형	애플리케이션 프로토콜은 호스트 간 통신을 나타냅니다. 클라이언트는 호스트에서 실행 중인 소프트웨어를 나타냅니다. 웹 애플리케이션은 HTTP 트래픽에 대한 콘텐츠 또한 요청 URL을 나타냅니다.	HTTP 및 SSH는 애플리케이션 프로토콜입니다. 웹 브라우저 및 이메일 클라이언트는 클라이언트입니다. MPEG 비디오 및 Facebook은 웹 애플리케이션입니다.
위험	애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성입니다.	피어 투 피어 애플리케이션은 고위험 경향이 있습니다.
사업 타당성	애플리케이션이 오락이 아닌 조직의 비즈니스 운영 컨텍스트 내에서 사용될 가능성입니다.	게임 애플리케이션은 비즈니스 연관성이 매우 낮은 경향이 있습니다.
Category(카테고리)	가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.	Facebook은 소셜 네트워킹 카테고리에 포함됩니다.
Tag(태그)	애플리케이션에 대한 추가 정보. 애플리케이션에는 0부터 원하는 수만큼의 태그를 포함할 수 있습니다.	비디오 스트리밍 웹 애플리케이션은 종종 높은 대역폭 및 광고 표시 태그가 지정됩니다.

관련 항목

애플리케이션 제어 구성 모범 사례

포트 규칙 조건

포트 조건을 사용하면 소스 및 대상 포트를 기준으로 트래픽을 제어할 수 있습니다.

특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.

포트 기반 규칙 모범 사례

포트를 지정하는 것은 애플리케이션을 대상으로 하는 기존의 방법입니다. 그러나 고유한 포트를 사용하여 액세스 제어 블록을 우회하도록 애플리케이션을 설정할 수 있습니다. 따라서 트래픽을 대상으로 지정하려면 가능한 경우 항상 포트 기준 대신 애플리케이션 필터링 기준을 사용하십시오.

FTD와 같이 제어와 데이터 흐름을 위해 별도의 채널을 동적으로 여는 애플리케이션에도 애플리케이션 필터링이 권장됩니다. 포트 기반 액세스 제어 규칙을 사용하면 이러한 종류의 애플리케이션이 올바르게 작동하지 못하게 되어 적절한 연결이 차단될 수 있습니다.

소스 및 대상 포트 제약 조건 사용

소스 및 대상 포트 제약 조건을 모두 추가할 경우 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어, 소스 포트로 DNS over TCP를 추가한 경우, 대상 포트에 Yahoo 메신저 음성 채팅(TCP)을 추가할 수 있지만 Yahoo 메신저 음성 채팅(UDP)은 해당되지 않습니다.

소스 포트만 또는 대상 포트만 추가할 경우 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. 예를 들어, DNS over TCP 및 DNS over UDP 모두를 단일 액세스 제어 규칙의 소스 포트 조건으로 추가할 수 있습니다.

범주 규칙 조건

가장 중요한 기능을 설명하는 일반 애플리케이션 분류. 각 애플리케이션은 적어도 하나의 카테고리에 속합니다.

자세한 내용은 애플리케이션 규칙 조건를 참고하십시오.

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.

관련 항목

인증서 TLS/SSL 규칙 조건, 20 페이지
인증서 상태 TLS/SSL 규칙 조건, 26 페이지

외부 인증 증명 신뢰, 25 페이지
인증서 상태를 기준으로 트래픽 매칭
암호 그룹 TLS/SSL 규칙 조건, 31 페이지
암호화 프로토콜 버전 TLS/SSL 규칙 조건, 34 페이지

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 CN(Common Name) 또는 URL이 인증서의 SAN(Subject Alternative Name)에 포함되어 있습니다.

  사용자가 브라우저에 입력하는 URL이 CN(Common Name)과 일치합니다.

- 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.
- 시스템이 새 서버로의 암호화된 세션을 처음 탐지할 때는 ClientHello 처리에 인증서 데이터를 사용할 수 없으므로 첫 번째 세션이 암호 해독되지 않습니다. 초기 세션 후에는 매니지드 디바이스가 서버 인증서 메시지에서 데이터를 캐시합니다. 같은 클라이언트로부터의 후속 연결에 대해 시스템은 ClientHello 메시지가 인증서 조건이 포함된 규칙과 최종적으로 일치하는지를 확인하여 메시지를 처리함으로써 암호 해독 가능성을 최대화할 수 있습니다.

고유 이름(DN) 규칙 조건

이 주제에서는 TLS/SSL 규칙에서 고유 이름 조건을 사용하는 방법에 대해 설명합니다. 확실하지 않은 경우 웹 브라우저를 사용하여 인증서의 SAN(주체 대체 이름) 및 Common Name(일반 이름)을 찾은 다음 이러한 값을 고유 이름 조건으로 TLS/SSL 규칙에 추가할 수 있습니다.

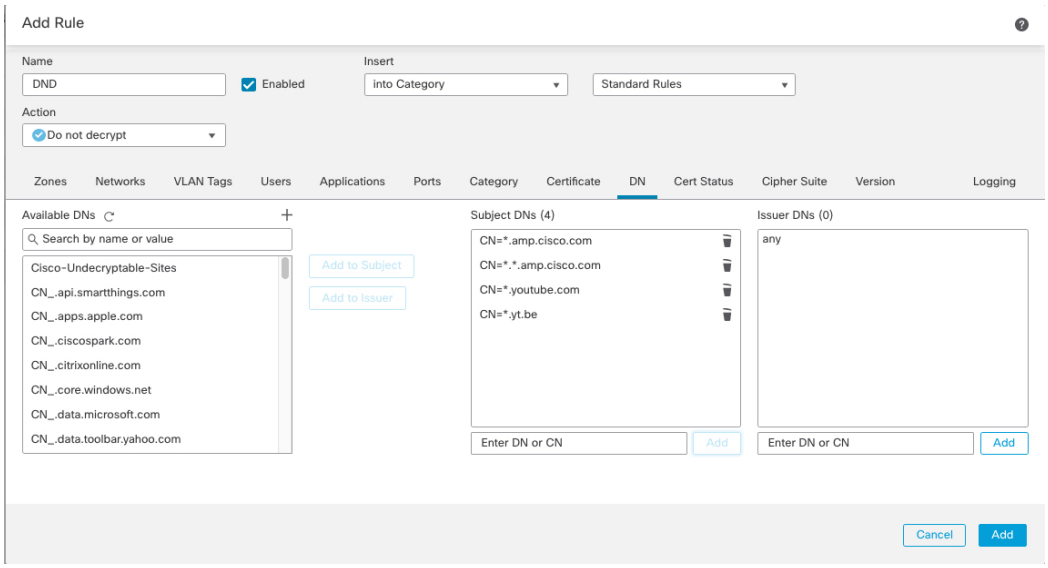
SAN에 대한 자세한 내용은 RFC 528, 섹션 4.2.1.6을 참조하십시오.

아래 섹션에서는 다음에 대해 설명합니다.

- DN 규칙 일치 예
- Firepower System에서 SNI 및 SAN을 사용하는 방법
- 인증서의 일반 이름 및 주체 대체 이름을 찾는 방법
- DN 규칙 조건을 추가하는 방법

DN 규칙 일치 예

다음은 Do Not Decrypt(암호 해독 안 함) 규칙에 있는 DN 규칙 조건의 예입니다. `amp.cisco.com` 또는 YouTube로 전송되는 트래픽을 암호 해독하지 않으려는 경우를 가정해 보겠습니다. 다음과 같이 DN 조건을 설정할 수 있습니다.



위의 DN 규칙 조건은 다음 URL과 일치하므로 이전 규칙에서 차단한 트래픽의 암호 해독이 해제됩니다.

- www.amp.cisco.com
- auth.amp.cisco.com
- auth.us.amp.cisco.com
- www.youtube.com

- kids.youtube.com
- www.yt.be

위의 DN 규칙 조건은 다음 URL과 일치하지 않으므로 트래픽은 Do Not Decrypt(암호 해독 안 함) 규칙과 일치하지 않지만 동일한 SSL 정책의 다른 TLS/SSL 규칙과 일치할 수 있습니다.

- amp.cisco.com
- youtube.com
- yt.be

위의 호스트 이름과 일치시키려면 규칙에 CN을 추가합니다(예를 들어, `CN=yt.be`를 추가하면 해당 URL과 일치).

Firepower System에서 SNI 및 SAN을 사용하는 방법

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

SNI와 인증서의 CN 또는 SAN 간에 일치하는 항목이 있는 경우 규칙에 나열된 DN과 비교할 때 SNI를 사용합니다. SNI가 없거나 인증서와 일치하지 않는 경우, 규칙에 나열된 DN과 비교할 때 인증서의 CN을 사용합니다.

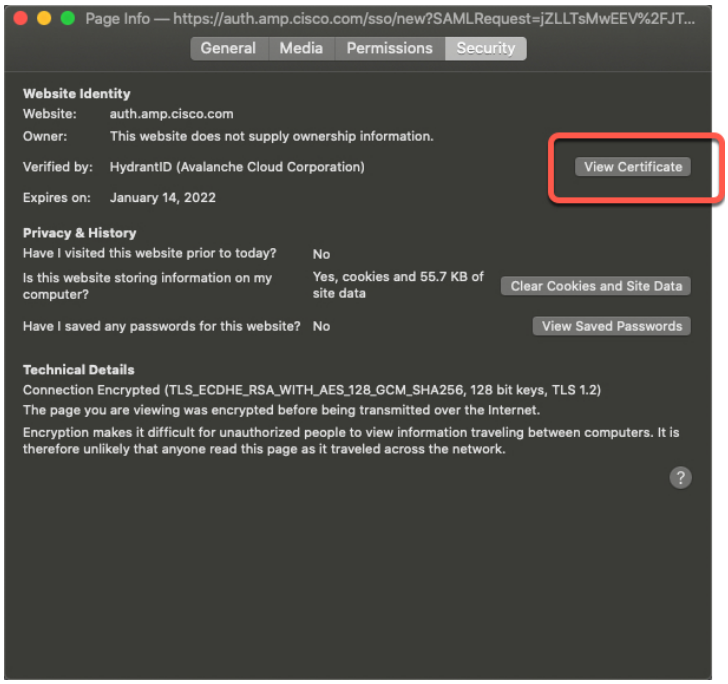
인증서의 일반 이름 및 주체 대체 이름을 찾는 방법

인증서의 일반 이름을 찾으려면 다음 단계를 사용합니다. 이러한 단계를 사용하여 자체 서명 인증서의 일반 이름 및 SAN을 찾을 수도 있습니다.

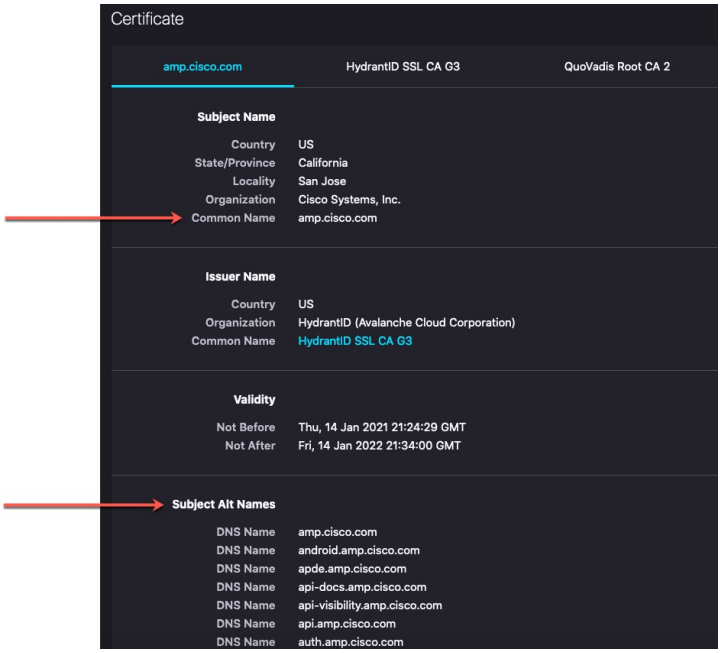
이 단계는 Firefox에 적용되지만 다른 브라우저도 유사합니다. 다음 절차에서는 `amp.cisco.com`을 예로 들어 설명합니다.

1. Firefox에서 `amp.cisco.com`으로 이동합니다.
2. 브라우저의 위치 표시줄에서 URL 왼쪽에 있는  을 클릭합니다.
3. **Connection secure(**연결 보안 **)** > **More Information(**추가 정보**)**을 클릭합니다.

   (비보안 또는 자체 서명 인증서의 경우 **Connection not secure(**연결 비보안**)** > **More Information(**추가 정보**)**을 클릭합니다.
4. Page Info(페이지 정보) 대화 상자에서 **View Certificate(**인증서 보기**)**를 클릭합니다.



5. 다음 페이지에 인증서 세부 정보가 표시됩니다.



다음에 유의하십시오.

- `CN=auth.amp.cisco.com`은 DN 규칙 조건으로 사용되는 경우 해당 호스트 이름(즉, SNI)과만 일치합니다. SNI `amp.cisco.com`이 일치하지 않습니다.
- 최대한 많은 도메인 이름 필드를 일치시키려면 와일드카드를 사용하십시오.

예를 들어 `auth.amp.cisco.com`과 일치시키려면 `CN=*.amp.cisco.com`을 사용합니다. `auth.us.amp.cisco.com`을 매칭하려면 `CN=*.*.amp.cisco.com`을 사용합니다.

`CN=*.example.com`과 같은 DN은 `www.example.com`과 일치하지만 `example.com`과 일치하지 않습니다. 두 SNI를 일치시키려면 규칙 조건에서 2개의 DN을 사용합니다.

- 그러나 와일드 카드를 사용하지 마십시오. 예를 들어 `CN=*.google.com`과 같은 DN 개체는 매우 많은 수의 SAN과 일치합니다. `CN=*.google.com` 대신 `CN=*.youtube.com`과 같은 DN 개체를 DN 개체로 사용하여 `www.youtube.com`과 같은 이름과 일치시킵니다.

  `CN=*.youtube.com`, `CN=youtu.be`, `CN=*.yt.be` 등과 같이 SAN과 일치하는 SNI의 변형을 사용할 수도 있습니다.

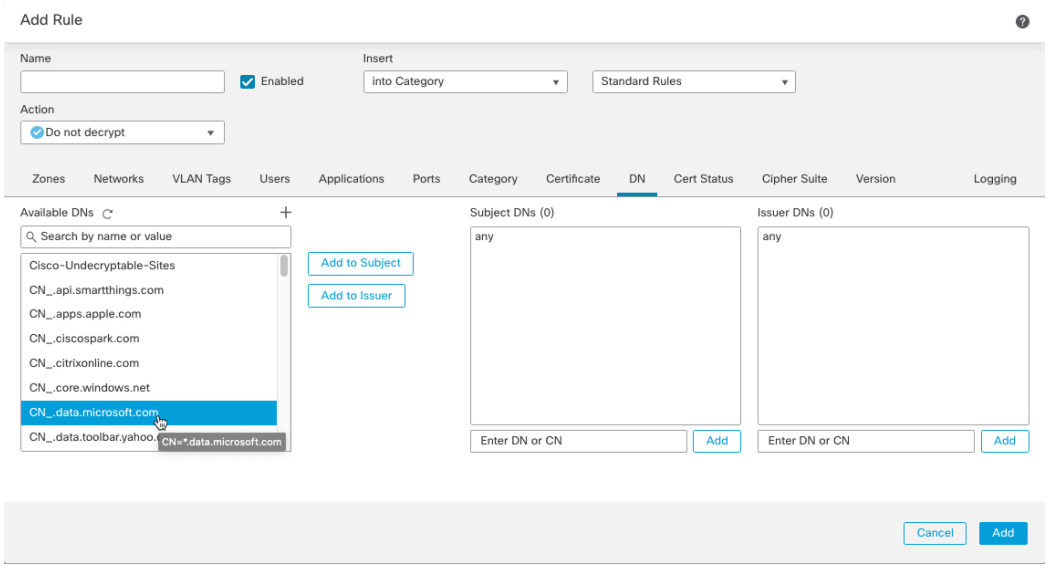
- 자체 서명 인증서도 동일한 방식으로 작동해야 합니다. 발급자 DN이 주체 DN과 동일하면 자체 서명 인증서임을 확인할 수 있습니다.

DN 규칙 조건을 추가하는 방법

일치시킬 CN을 확인한 후 다음 방법 중 하나로 TLS/SSL 규칙을 편집합니다.

- 기존 DN을 사용합니다.

  DN의 이름을 클릭한 다음 **Add to Subject(**주체에 추가**)** 또는 **Add to Issuer(**발급자에 추가**)**를 클릭합니다. (**Add to Subject(**주체에 추가**)**가 훨씬 더 일반적입니다.) DN 개체의 값을 보려면 마우스 포인터를 개체 위로 이동합니다.)

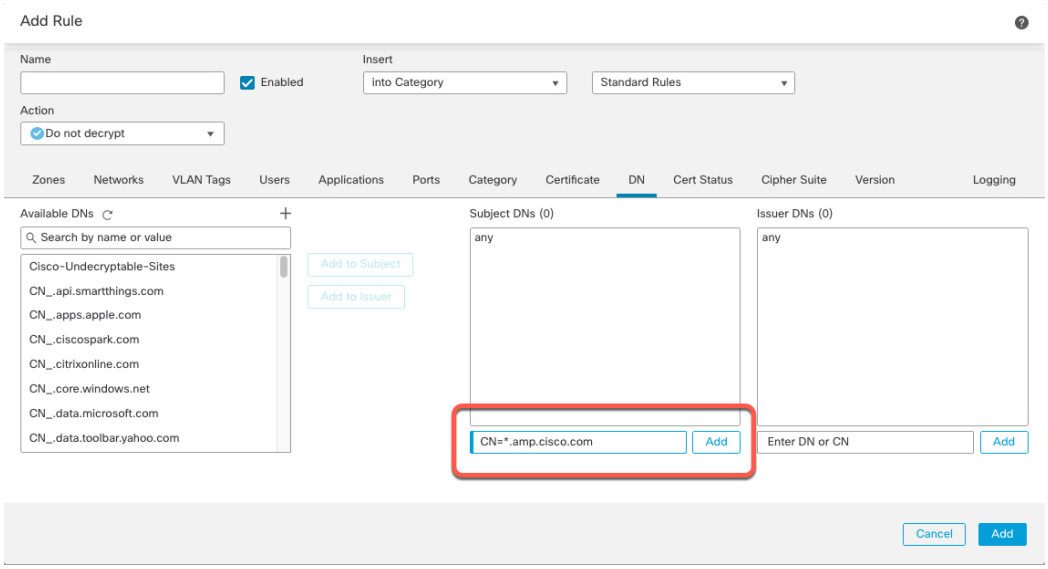


- 새 DN 개체를 생성합니다.

  Available DNs(사용 가능한 DN) 오른쪽에 있는 **Add(**추가**)** (+)을 클릭합니다. DN 개체는 이름과 값으로 구성되어야 합니다.

- DN을 직접 추가합니다.

Subject DNs(주체 DN) 필드 또는 **Issuer DNs(발급자 DN)** 필드의 맨 아래에 있는 필드에 DN을 입력합니다. (제목 **DN**이 더 일반적입니다.) DN을 입력한 후 **Add(추가)**를 클릭합니다.



관련 항목

고유 이름(DN) 개체

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.

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.

프로시저

단계 **1** 아직 하지 않았다면 FMC에 로그인합니다.

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

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

단계 **4** **Add Rule(**규칙 추가**)**를 클릭해 새 TLS/SSL 규칙을 추가하거나 **Edit(**수정**)** ( )를 클릭하여 기존 규칙을 편집합니다.

단계 **5** **Certificate(**인증서**)** 탭을 클릭합니다.

단계 **6** **Available Certificates(**사용 가능한 인증서**)**에서 추가할 신뢰할 수 있는 CA를 다음과 같이 찾습니다.

- 신뢰할 수 있는 CA 개체를 즉시 추가한 다음 조건에 추가하려면 **Available Certificates(**사용 가능한 인증서**)** 목록 위의 **Add(**추가**)** ( )을 클릭합니다.
- 추가할 신뢰할 수 있는 CA 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 **7** 개체를 선택하려면 이를 클릭합니다. 모든 개체를 선택하려면 마우스 오른쪽 버튼을 클릭한 다음 **Select All(**모두 선택**)**을 선택합니다.

단계 **8** **Add to Rule(**규칙에 추가**)**을 클릭합니다.

팁 선택한 영역을 끌어서 놓을 수도 있습니다.

단계 **9** 규칙을 추가하거나 계속 수정합니다.

다음에 수행할 작업

- 인증서 상태 TLS/SSL 규칙 조건을 SSL 규칙에 추가합니다. 자세한 내용은 인증서 상태를 기준으로 트래픽 매칭를 참조하십시오.
- Deploy configuration changes(구성 변경 사항 구축), Firepower Management Center 관리 가이드 참조.

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 ***2:*** 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.

상태 확인	상태가 **Yes**로 설정	상태가 **No**로 설정
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.
서버 불일치	서버 이름이 서버의 서버 이름 표시(SNI) 이름과 일치하지 않습니다. 이는 서버 이름을 스푸핑하려는 시도를 나타낼 수 있습니다.	서버 이름이 클라이언트가 액세스를 요청하는 서버의 SNI 이름과 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.

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.
- SSL 규칙에서 **Cipher Suite(**암호 그룹**)** 조건에 익명 암호 그룹을 추가할 수 있습니다. 단, 다음 사항에 유의해야 합니다.
  - 시스템은 ClientHello 처리 중에 익명 암호 그룹을 자동으로 제거합니다. 시스템이 규칙을 사용하도록 하려면 ClientHello가 처리되지 않도록 하는 순서로 TLS/SSL 규칙을 구성해야 합니다. 자세한 내용은 SSL 규칙 순서를 참고하십시오.
  - 규칙에서는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 작업을 사용할 수 없습니다. 시스템은 익명 암호 그룹으로 암호화된 트래픽을 암호 해독할 수 없기 때문입니다.
- 암호 그룹을 규칙 조건으로 지정할 때는 규칙이 ClientHello 메시지에 지정된 전체 암호 그룹 목록이 아닌 ServerHello 메시지에서 협상된 암호 그룹과 일치하는지를 고려합니다. ClientHello 처리 중에 매니지드 디바이스는 ClientHello 메시지에서 지원되지 않는 암호 그룹을 제거합니다. 그러나 이 제거로 인해 지정된 모든 암호 그룹이 제거되는 경우에는 원본 목록이 유지됩니다. 시스템이 지원되지 않는 암호 그룹을 유지하는 경우 후속 평가에서는 세션이 암호 해독되지 않습니다.

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.

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. 트래픽이 **Monitor(**모니터링**)** 규칙 조건과 일치하는 경우 ClientHello 메시지는 수정되지 않습니다.

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 Firepower Management Center 관리 가이드의 연결 이벤트 필드 채우기 요구 사항을 참조하십시오.

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 하드웨어 가속 모니터링

다음 항목에서는 TLS/SSL의 상태를 모니터링하는 방법에 대해 설명합니다.

정보 카운터

알림 카운터

오류 카운터

치명적 카운터

TLS/SSL 규칙 문제 해결

다음 주제에서는 TLS/SSL 규칙 문제를 해결하는 방법을 설명합니다.

TLS/SSL 초과 서브스크립션 정보

TLS/SSL 오버서브스크립션은 매니지드 디바이스가 TLS/SSL 트래픽으로 오버로드된 상태입니다. 모든 매니지드 디바이스에서 TLS/SSL오버서브스크립션이 발생할 수 있지만 TLS 암호화 가속를 지원하는 매니지드 디바이스만 이를 처리하는 구성 방법을 제공합니다.

TLS 암호화 가속가 활성화된 매니지드 디바이스가 오버서브스크립션되는 경우, 매니지드 디바이스가 수신하는 모든 패킷은 SSL 정책 **Undecryptable Actions(**암호 해독 불가 작업**)**의 **Handshake Errors(**핸드셰이크 오류**)** 설정에 따라 수행됩니다.

- 기본 작업 상속
- Do not decrypt(암호 해독 안 함)
- Block(차단)
- Block with Reset(차단 후 재설정)

SSL 정책 **Undecryptable Actions(**암호 해독 불가 작업**)**의 **Handsake Errors(**핸드셰이크 오류**)**에 대한 설정이 **Do Not decrypt(**암호 해독 안 함**)**이며 관련 액세스 제어 정책이 트래픽을 검사하도록 구성하는 경우, 검사가 이루어지며 암호 해독은 진행되지 않습니다.

TLS/SSL 초과 서브스크립션 문제 해결

매니지드 디바이스에서 TLS 암호화 가속가 활성화된 경우, 연결 이벤트를 보고 디바이스에 초과 스크립션이 발생하는지 여부를 확인할 수 있습니다. 최소한 연결 이벤트의 테이블 보기에 **SSL Flow Flags(SSL** 플로우 플래그**)**를 추가해야 합니다.

시작하기 전에

- **Undecryptable Actions(**암호 해독할 수 없는 작업**)** 페이지에서 **Handshake Error(**핸드셰이크 오류**)** 설정을 사용하여 SSL 정책을 구성합니다.

자세한 내용은 해독 불가 트래픽에 대한 기본 처리 설정를 참고하십시오.

- FMC 및 FTD 관리 네트워크 운영 가이드의 TLS/SSL 규칙에서 암호 해독 가능한 연결 로깅에 대한 섹션에 설명된 대로 SSL 규칙에 대한 로깅을 활성화합니다.

프로시저

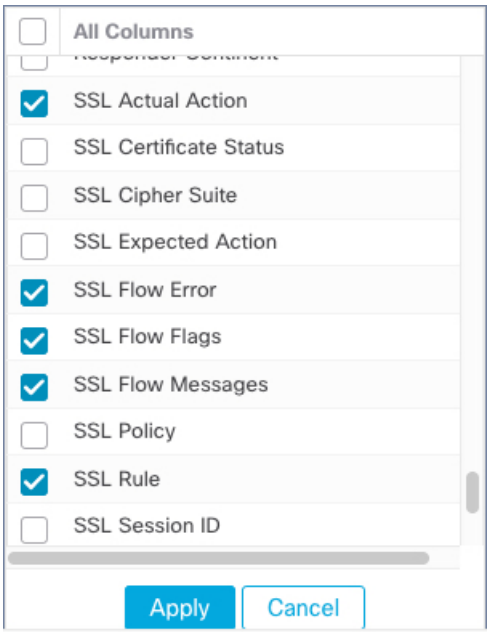
단계 **1** 아직 로그인하지 않았다면 FMC에 로그인합니다.

단계 **2** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 클릭합니다.

단계 **3** **Table View of Connection Events(**연결 이벤트 테이블 보기**)**를 클릭합니다.

단계 **4** 최소한 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)**에 대한 열을 추가하려면 연결 이벤트 테이블에 있는 임의의 열에서 **x**를 클릭합니다.

다음 예는 **SSL Actual Action(SSL** 실제 작업**)**, **SSL Flow Error(SSL** 플로우 오류**)**, **SSL Flow Flags(SSL** 플로우 플래그**)**, **SSL Flow Messages(SSL** 플로우 메시지**)**, **SSL Policy(SSL** 정책**)**, **SSL Rule(SSL** 규칙**)** 열을 연결 이벤트 테이블에 추가하는 방법을 보여줍니다. (대화 상자의 Disabled Columns(비활성화된 열) 섹션을 확인합니다.)



열은 Firepower Management Center 관리 가이드 의 연결 및 보안 인텔리전스 이벤트 필드에 설명된 순서대로 추가됩니다.

단계 **5** **Apply(**적용**)**를 클릭합니다.

TLS/SSL 초과 서브스크립션은 **SSL Flow Flags(SSL** 플로우 플래그**)** 열의 `ERROR_EVENT_TRIGGERED` 및 `OVER_SUBSCRIBED` 값으로 표시됩니다.

단계 **6** TLS/SSL 초과 서브스크립션이 발생하는 경우, 매니지드 디바이스에 로그인하고 다음 명령 중 하나를 입력합니다.

Command(명령**)**	결과
show counters	**TCP_PRX BYPASS_NOT_ENOUGH_MEM**의 값이 큰 경우, SSL 트래픽 용량이 더 큰 디바이스로 업그레이드하거나 우선 순위가 낮은 암호화된 트래픽에 **Do Not Decrypt(**암호 해독 안 함**)** 규칙을 사용하는 것이 좋습니다.
show snort tls-offload	**BYPASS_NOT_ENOUGH_MEM**의 값이 큰 경우, SSL 트래픽 용량이 더 큰 디바이스로 업그레이드하거나 우선 순위가 낮은 암호화된 트래픽에 **Do Not Decrypt(**암호 해독 안 함**)** 규칙을 사용하는 것이 좋습니다.

TLS 하트비트 정보

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.

TLS 암호화 가속이 활성화된 매니지드 디바이스가 TLS 하트비트 확장을 사용하는 패킷이 발생하는 경우, 해당 매니지드 디바이스는 SSL 정책 **Undecryptable Actions(**암호 해독 불가 작업**)**의 **Decryption Errors(**암호 해독 오류**)**에 대한 설정에서 지정된 작업을 수행합니다.

- Block(차단)
- Block with Reset(차단 후 재설정)

관련 항목

TLS 하트비트 문제 해결, 39 페이지

TLS 하트비트 문제 해결

매니지드 디바이스에서 TLS 암호화 가속가 활성화된 경우, 연결 이벤트를 보고 디바이스에 TLS 하트비트 확장이 있는 트래픽이 발생하는지 확인할 수 있습니다. 최소한 연결 이벤트의 테이블 보기에 **SSL Flow Messages(SSL** 플로우 메시지**)**를 추가해야 합니다.

시작하기 전에

SSL 하트비트는 연결 이벤트 테이블 보기에서 **SSL Flow Messages(SSL** 플로우 메시지**)** 열의 HEARTBEAT 값으로 표시됩니다. 네트워크의 애플리케이션이 SSL 하트비트를 사용하는지 확인하려면 먼저 다음 작업을 수행 합니다.

- **Undecryptable Actions(**암호 해독할 수 없는 작업**)** 페이지에서 **Decryption Error(**암호 해독 오류**)** 설정을 사용하여 SSL 정책을 설정합니다.

  자세한 내용은 해독 불가 트래픽에 대한 기본 처리 설정를 참고하십시오.

- FMC 및 FTD 관리 네트워크 운영의 설명에 따라 SSL 규칙에 대한 로깅을 활성화합니다.

프로시저

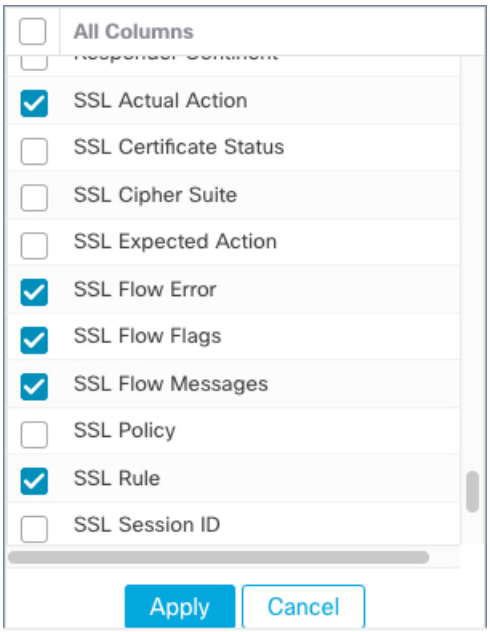
단계 **1** 아직 로그인하지 않았다면 FMC에 로그인합니다.

단계 **2** **Analysis(**분석**)** > **Connection(**연결**)** > **Events(**이벤트**)**를 클릭합니다.

단계 **3** **Table View of Connection Events(**연결 이벤트 테이블 보기**)**를 클릭합니다.

단계 **4** 최소한 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)**에 대한 열을 추가하려면 연결 이벤트 테이블에 있는 임의의 열에서 **x**를 클릭합니다.

다음 예는 **SSL Actual Action(SSL** 실제 작업**)**, **SSL Flow Error(SSL** 플로우 오류**)**, **SSL Flow Flags(SSL** 플로우 플래그**)**, **SSL Flow Messages(SSL** 플로우 메시지**)**, **SSL Policy(SSL** 정책**)**, **SSL Rule(SSL** 규칙**)** 열을 연결 이벤트 테이블에 추가하는 방법을 보여줍니다.



열은 Firepower Management Center 관리 가이드 의 연결 및 보안 인텔리전스 이벤트 필드에 설명된 순서대로 추가됩니다.

단계 **5** **Apply(**적용**)**를 클릭합니다.
TLS 하트비트는 **SSL Flow Messages(SSL** 플로우 메시지**)** 열의 `HEARTBEAT` 값으로 표시됩니다.

단계 **6** 네트워크의 애플리케이션이 SSL 하트비트를 사용하는 경우, TLS/SSL 규칙 지침 및 제한 사항, 2 페이지를 참조하십시오.

TLS/SSL 피닝 정보

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 피닝이 발생하고 있는지 확인하려면, Facebook 같은 모바일 애플리케이션에 로그인을 시도합니다. 네트워크 연결 오류가 표시되는 경우, 웹 브라우저를 사용하여 로그인 합니다. (예를 들어, Facebook 모바일 애플리케이션에는 로그인이 불가능하더라도 Safari나 Chrome을 사용하여 Facebook에 로그인할 수 있습니다.) Firepower Management Center 연결 이벤트를 TLS/SSL 피닝의 추가 증거로 사용할 수 있습니다.

참고 TLS/SSL 피닝은 모바일 애플리케이션에 국한되지 않습니다.

네트워크의 애플리케이션 SSL 피닝을 사용하는 경우, TLS/SSL 인증서 고정 지침, 7 페이지의 내용을 참조하십시오.

관련 항목

TLS/SSL 피닝 문제 해결, 41 페이지

TLS/SSL 피닝 문제 해결

연결 이벤트를 보고 디바이스에 SSL 피닝이 발생하는지 확인할 수 있습니다. 최소한 연결 이벤트의 테이블 보기에 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)** 열을 추가해야 합니다.

시작하기 전에

- FMC 및 FTD 관리 네트워크 운영 가이드의 TLS/SSL 규칙에서 암호 해독 가능한 연결 로깅에 대한 섹션에 설명된 대로 TLS/SSL 규칙에 대한 로깅을 활성화합니다.
- Facebook 같은 모바일 애플리케이션에 로그인합니다. 네트워크 연결 오류가 표시되면 Chrome 또는 Safari를 사용하여 Facebook에 로그인합니다. 웹 브라우저를 사용한 로그인은 가능하지만 기본 애플리케이션을 사용한 로그인은 불가능할 경우, 피닝이 발생할 가능성이 높습니다.

프로시저

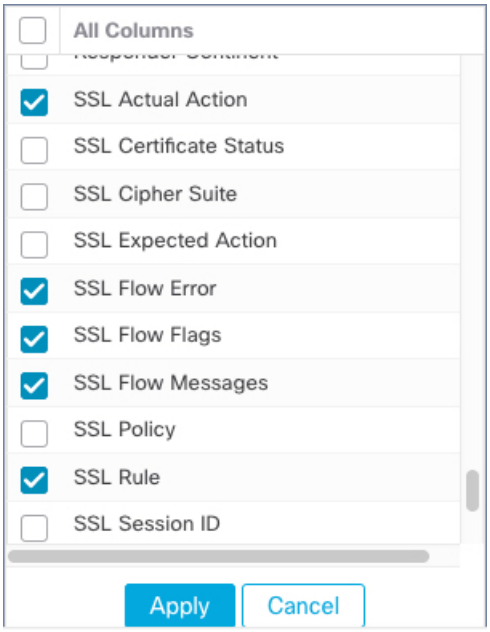
단계 **1** 아직 로그인하지 않았다면 FMC에 로그인합니다.

단계 **2** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 클릭합니다.

단계 **3** **Table View of Connection Events(**연결 이벤트 테이블 보기**)**를 클릭합니다.

단계 **4** 최소한 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)**에 대한 열을 추가하려면 연결 이벤트 테이블에 있는 임의의 열에서 **x**를 클릭합니다.

다음 예는 **SSL Actual Action(SSL** 실제 작업**)**, **SSL Flow Error(SSL** 플로우 오류**)**, **SSL Flow Flags(SSL** 플로우 플래그**)**, **SSL Flow Messages(SSL** 플로우 메시지**)**, **SSL Policy(SSL** 정책**)**, **SSL Rule(SSL** 규칙**)** 열을 연결 이벤트 테이블에 추가하는 방법을 보여줍니다.



열은 FMC 및 FTD 관리 네트워크 운영 가이드의 연결 및 보안 인텔리전스 이벤트 필드 섹션에 설명된 순서대로 추가됩니다.

단계 **5** **Apply(**적용**)**를 클릭합니다.

단계 **6** 다음 단락에서는 SSL 피닝 동작을 식별하는 방법을 설명합니다.

단계 **7** 네트워크의 애플리케이션이 SSL 피닝을 사용하는지 확인하려면 TLS/SSL 규칙 지침 및 제한 사항, 2 페이지를 참조하십시오.

다음에 수행할 작업

TLS/SSL 연결 이벤트를 사용하여 다음 중 하나를 찾으면 TLS/SSL 피닝이 발생하는지 확인할 수 있습니다.

- 클라이언트가 서버에서 SERVER_HELLO, SERVER_CERTIFICATE, SERVER_HELLO_DONE 메시지를 수신하는 즉시 SSL ALERT 메시지와 TCP 재설정을 차례로 전송하는 애플리케이션이 다음과 같은 증상을 보입니다. (`Unknown CA (48)` 알림은 패킷 캡처를 사용하여 볼 수 있습니다.)
  - SSL Flow Flags(SSL 플로우 플래그) 열에 `ALERT_SEEN`이 표시되지만 `APP_DATA_C2S` 또는 `APP_DATA_S2C`는 표시되지 않습니다.
  - 매니지드 디바이스에 SSL 하드웨어 가속이 활성화된 경우, SSL Flow Messages(SSL 플로우 메시지) 열에는 일반적으로 `CLIENT_ALERT`, `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`이 표시됩니다.
  - 매니지드 디바이스가 SSL 하드웨어 가속을 지원하지 않거나 이 기능이 비활성화되어 있는 경우, SSL Flow Messages(SSL 플로우 메시지) 열에는 일반적으로 `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`이 표시됩니다.
  - SSL Flow Error(SSL 플로우 오류) 열에 `Success`(성공)가 표시됩니다.
- 알림을 전송하지 않고 대신 SSL 핸드셰이크가 완료된 후 TCP 재설정을 전송하는 애플리케이션이 다음과 같은 증상을 보입니다.
  - SSL Flow Flags(SSL 플로우 플래그) 열에 `ALERT_SEEN`, `APP_DATA_C2S`, or `APP_DATA_S2C`가 표시되지 않습니다.
  - 매니지드 디바이스에 SSL 하드웨어 가속이 활성화된 경우, SSL Flow Messages(SSL 플로우 메시지) 열에는 일반적으로 `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`, `CLIENT_KEY_EXCHANGE`, `CLIENT_CHANGE_CIPHER_SPEC`, `CLIENT_FINISHED`, `SERVER_CHANGE_CIPHER_SPEC`, `SERVER_FINISHED`가 표시됩니다.
  - 매니지드 디바이스가 SSL 하드웨어 가속을 지원하지 않거나 이 기능이 비활성화되어 있는 경우, SSL Flow Messages(SSL 플로우 메시지) 열에는 일반적으로 `CLIENT_HELLO`, `SERVER_HELLO`, `SERVER_CERTIFICATE`, `SERVER_KEY_EXCHANGE`, `SERVER_HELLO_DONE`, `CLIENT_KEY_EXCHANGE`, `CLIENT_CHANGE_CIPHER_SPEC`, `CLIENT_FINISHED`,`SERVER_CHANGE_CIPHER_SPEC`, `SERVER_FINISHED`가 표시됩니다.
  - SSL Flow Error(SSL 플로우 오류) 열에 `Success`(성공)가 표시됩니다.

관련 항목

알 수 없는 또는 잘못된 인증서 또는 인증 기관 문제 해결, 44 페이지

알 수 없는 또는 잘못된 인증서 또는 인증 기관 문제 해결

연결 이벤트를 보고 디바이스에 알 수 없는 인증 기관, 잘못된 인증서 또는 알 수 없는 인증서가 있는지 확인할 수 있습니다. TLS/SSL 인증서가 고정된 경우에도 이 절차를 사용할 수 있습니다. 최소한 연결 이벤트의 테이블 보기에 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)** 열을 추가해야 합니다.

시작하기 전에

- TLS/SSL 암호 해독 규칙을 설정합니다.
- FMC 및 FTD 관리 네트워크 운영 가이드의 TLS/SSL 규칙에서 암호 해독 가능한 연결 로깅에 대한 섹션에 설명된 대로 TLS/SSL 규칙에 대한 로깅을 활성화합니다.

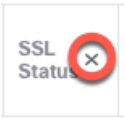
프로시저

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

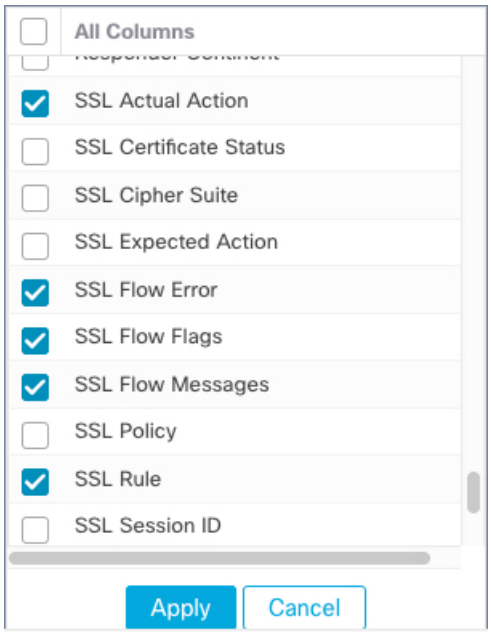
단계 **2** **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**를 클릭합니다.

단계 **3** **Table View of Connection Events(**연결 이벤트 테이블 보기**)**를 클릭합니다.

단계 **4** 최소한 **SSL Flow Flags(SSL** 플로우 플래그**)** 및 **SSL Flow Messages(SSL** 플로우 메시지**)**에 대한 열을 추가하려면 연결 이벤트 테이블에 있는 임의의 열에서 **x**를 클릭합니다.



다음 예는 **SSL Actual Action(SSL** 실제 작업**)**, **SSL Flow Error(SSL** 플로우 오류**)**, **SSL Flow Flags(SSL** 플로우 플래그**)**, **SSL Flow Messages(SSL** 플로우 메시지**)**, **SSL Policy(SSL** 정책**)**, **SSL Rule(SSL** 규칙**)** 열을 연결 이벤트 테이블에 추가하는 방법을 보여줍니다.



열은 FMC 및 FTD 관리 네트워크 운영 가이드의 연결 및 보안 인텔리전스 이벤트 필드 섹션에 설명된 순서대로 추가됩니다.

단계 **5** **Apply(**적용**)**를 클릭합니다.

단계 **6** 다음 표에서는 인증서 또는 인증 기관이 잘못되었거나 누락되었는지 확인할 수 있는 방법에 대해 설명합니다.

SSL 플로우 플래그	의미
CLIENT_ALERT_SEEN_UNKNOWN_CA	유효한 인증서 체인 또는 부분 체인이 SSL 클라이언트 애플리케이션에서 수신되었지만 CA 인증서를 찾을 수 없거나 알려진 신뢰할 수 있는 CA와 일치할 수 없으므로 인증서가 수락되지 않았음을 나타냅니다. 이 메시지는 항상 복구 불가능한 오류를 나타냅니다.
CLIENT_ALERT_SEEN_BAD_CERTIFICATE	인증서가 손상되었거나 올바르게 확인되지 않은 서명이 포함되어 있거나 다른 문제가 있습니다.
CLIENT_ALERT_SEEN_CERTIFICATE_UNKNOWN	일부 다른(지정되지 않은) 문제가 발생하여 인증서를 처리할 수 없게 되었습니다.

TLS/SSL 암호 그룹 확인

시작하기 전에

이 주제에서는 암호 그룹 조건이 있는 TLS/SSL 규칙을 저장할 때 다음과 같은 오류가 표시되는 경우에 수행해야 하는 작업을 설명합니다.

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

이 오류는 TLS/SSL 규칙 조건에 대해 선택한 하나 이상의 암호 그룹이 TLS/SSL 규칙에 사용되는 인증서와 호환되지 않음을 나타냅니다. 이 문제를 해결하려면 사용 중인 인증서에 액세스할 수 있어야 합니다.

참고 이 주제에 나온 작업에서는 사용자가 TLS/SSL 암호화의 작동 원리에 대해 알고 있다고 가정합니다.

프로시저

단계 **1** 지정된 암호 그룹으로 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 또는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)**가 포함된 SSL 규칙을 저장하려고 하면 다음과 같은 오류가 표시됩니다.

예제**:**

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

단계 **2** 트래픽 암호 해독에 사용 중인 인증서를 찾고, 필요하다면 openssl 명령을 실행할 수 있는 시스템에 인증서를 복사합니다.

단계 **3** 인증서에서 사용되는 서명 알고리즘을 표시하려면 다음 명령을 실행합니다.

openssl x509 -in *CertificateName* **-text -noout**

출력의 처음 몇 행은 다음과 비슷하게 표시됩니다.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4105 (0x1009)
    Signature Algorithm: ecdsa-with-SHA256
```

단계 **4** **Signature algorithm**은 다음을 알려줍니다.

- 사용되는 암호화 기능(앞의 예에서 **ECDSA**은 Elliptic Curve Digital Signature Algorithm을 뜻합니다).
- 암호화된 메시지의 다이제스트를 생성하는 데 사용되는 해시 함수(앞의 예에서는 **SHA256**).

단계 **5** OpenSSL at University of Utah 같은 리소스에서 이러한 값과 일치하는 암호 그룹을 검색합니다. 암호 그룹은 RFC 형식이어야 합니다.

Mozilla wiki의 Server Side TLS 또는 RFC 5246의 부록 C 같은 다양한 다른 사이트도 검색할 수 있습니다. Microsoft 문서의 Cipher Suites in TLS/SSL (Schannel SSP)에는 암호 그룹에 대한 상세한 설명이 나와 있습니다.

단계 **6** 필요한 경우, OpenSSL 이름을 Firepower Management System서 사용하는 RFC 이름으로 변환합니다. `https://testssl.sh` 사이트의 RFC mapping list를 참조하십시오.

단계 **7** 앞의 예에서 **ecdsa-with-SHA256**는 Mozilla wiki의 Modern Compatibility List에서 찾을 수 있습니다.

a) 이름에 **ECDSA** 및 **SHA-256**가 있는 암호 그룹만 선택하십시오. 다음 암호 그룹이 뒤에 나옵니다.

```
ECDHE-ECDSA-AES128-GCM-SHA256
ECDHE-ECDSA-AES128-SHA256
```

b) RFC mapping list에서 해당 RFC 암호 그룹을 찾습니다. 다음 암호 그룹이 뒤에 나옵니다.

```
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
```

단계 **8** TLS/SSL 규칙에 이전 암호 그룹을 추가합니다.