SSL 암호 해독

HTTPS와 같은 일부 프로토콜은 SSL(Secure Sockets Layer) 또는 그 후속 버전인 TLS(Transport Layer Security)를 사용하여 안전한 전송을 위해 트래픽을 암호화합니다. 시스템에서는 암호화된 연결을 검사할 수 없으므로 상위 레이어의 트래픽 특성을 고려하여 액세스 의사 결정을 내리는 액세스 규칙을 적용하려면 암호를 해독해야 합니다.

SSL 암호 해독 정보

일반적으로 연결은 액세스 제어 정책을 통해 허용되는지 아니면 차단되는지가 결정됩니다. 그러나 SSL 암호 해독 정책을 활성화하는 경우에는 암호화된 연결이 가장 먼저 SSL 암호 해독 정책을 통해 암호가 해독되어야 하는지 아니면 차단되어야 하는지가 결정됩니다. 암호 해독 여부와 관계없이 차단 해제된 연결은 모두 액세스 제어 정책을 통해 최종 허용/차단 여부가 결정됩니다.

참고 ID 정책에서 활성 인증 규칙을 구현하려면 SSL 암호 해독 정책을 활성화해야 합니다. SSL 암호 해독을 활성화하여 ID 정책을 활성화하되 다른 방법으로는 SSL 암호 해독을 구현하지 않으려는 경우에는 Do Not Decrypt(암호 해독 안 함)를 기본 작업으로 선택하고 추가 SSL 암호 해독 규칙을 생성하지 마십시오. ID 정책은 필요한 규칙이라면 무엇이든 자동으로 생성합니다.

다음 주제에서는 암호화된 트래픽 플로우 관리 및 암호 해독에 대해 자세히 설명합니다.

SSL 암호 해독을 구현하는 이유

HTTPS 연결과 같이 암호화된 트래픽은 검사할 수 없습니다.

은행 및 기타 금융 기관에 대한 연결 등 많은 연결이 합법적으로 암호화되어 있으며, 많은 웹 사이트에서 암호화를 사용하여 개인 정보 또는 민감한 데이터를 보호합니다. 예를 들어 device manager에 대한 연결은 암호화됩니다.

그러나 사용자는 암호화된 연결 내에서 부적절한 트래픽을 숨길 수도 있습니다.

SSL 암호 해독을 구현함으로써 연결을 암호 해독하고, 연결에 위협 또는 다른 부적절한 트래픽이 포함되어 있지 않은지 검사한 다음, 연결을 계속하도록 허용하기 전에 재암호화할 수 있습니다. 암호 해독된 트래픽은 액세스 제어 정책을 통과하고 암호 해독된 연결의 검사받은 특성(암호화된 특성 아님)을 기반으로 하는 규칙과 일치합니다. 따라서 액세스 제어 정책을 적용해야 하는 필요와 민감한 정보를 보호해야 하는 사용자의 필요 간의 균형을 유지할 수 있습니다.

또한, 네트워크에 원하지 않는 유형의 암호화된 트래픽을 차단하기 위해 SSL 암호 해독 규칙을 구성할 수 있습니다.

트래픽을 암호 해독한 다음 재암호화하면 디바이스의 처리 부하가 증가하므로 전체 시스템 성능이 감소된다는 점에 유의하십시오.

암호화된 트래픽에 적용할 수 있는 작업

SSL 암호 해독 규칙을 구성할 때 다음 주제에 설명된 작업을 적용할 수 있습니다. 이러한 작업은 명시적인 규칙과 일치하지 않는 모든 트래픽에 적용되는 기본 작업에도 사용할 수 있습니다.

참고 SSL 암호 해독 정책을 통과하는 모든 트래픽은 이후에 액세스 제어 정책을 통과해야 합니다. SSL 암호 해독 정책에서 삭제하는 트래픽을 제외하고는 액세스 제어 정책에 따라 최종 허용/삭제 여부가 결정됩니다.

재서명 암호 해독

트래픽 암호 해독 및 재서명을 선택하는 경우, 시스템이 MITM(Man-In-The-Middle) 역할을 합니다.

브라우저에서 https://www.cisco.com의 사용자 유형을 예로 들 수 있습니다. 트래픽이 위협 방어 디바이스에 도달하면 디바이스에서는 규칙에 지정된 CA 인증서를 사용하는 사용자와 협상하며 사용자와 위협 방어 디바이스 간에 SSL 터널을 구축합니다. 동시에 이 디바이스에서는 https://www.cisco.com에 접속하여 서버와 위협 방어 디바이스 간에 SSL 터널을 생성합니다.

따라서 사용자는 www.cisco.com에서 인증서 대신 SSL 암호 해독 규칙에 대해 구성된 CA 인증서를 보게 됩니다. 연결을 완료하려면 사용자가 인증서를 신뢰해야 합니다. 그러면 위협 방어 디바이스에서는 사용자와 대상 서버 간의 양방향 트래픽에서 암호 해독/재암호화를 수행합니다.

참고 클라이언트가 서버 인증서 재서명에 쓰이는 CA를 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.

재서명 암호 해독 작업으로 규칙을 구성할 경우 이 규칙은 구성된 규칙 조건과 더불어 참조된 내부 CA 인증서의 서명 알고리즘 유형을 기반으로 트래픽을 일치시킵니다. SSL 암호 해독 정책용 단일 재서명 인증서를 선택할 수 있으므로 이 경우 재서명 규칙에 대한 트래픽 일치를 제한할 수 있습니다.

예를 들어, 재서명 인증서가 EC(Elliptic Curve) 기반 CA 인증서인 경우에만 EC 알고리즘을 사용하여 암호화된 발신 트래픽이 재서명 암호 해독 규칙과 일치합니다. 이와 유사하게 글로벌 재서명 인증서가 RSA인 경우에만 RSA 알고리즘을 사용하여 암호화된 트래픽이 재서명 암호 해독 규칙과 일치합니다. 즉, 구성된 다른 모든 규칙 조건이 일치하더라도 EC 알고리즘을 사용하여 암호화된 발신 트래픽은 이 규칙과 일치하지 않습니다.

알려진 키 암호 해독

목적지 서버를 소유하고 있는 경우 알려진 키를 사용하여 암호 해독을 구현할 수 있습니다. 이 경우 사용자가 https://www.cisco.com에 대한 연결을 열면 인증서를 제시하는 위협 방어 디바이스인 경우에도 www.cisco.com에 대한 실제 인증서가 사용자에게 표시됩니다.

소속된 조직은 도메인 및 인증서의 소유자여야 합니다. cisco.com을 예로 드는 경우, 엔드 유저가 Cisco 인증서를 확인할 수 있으려면 실제로 cisco.com 도메인을 소유(즉, 엔드 유저가 Cisco Systems)하고 공용 CA에서 서명한 cisco.com 인증서의 소유권을 갖고 있어야만 합니다. 조직이 소유한 사이트에 대해 알려진 키를 사용해야만 암호를 해독할 수 있습니다.

알려진 키로 암호 해독을 수행하는 주요 목적은 HTTPS 서버로 향하는 트래픽을 암호 해독하여 외부 공격으로부터 서버를 보호하는 것입니다. 외부 HTTPS 사이트에 대한 클라이언트 측 트래픽을 검사하기 위해서는 서버를 소유하고 있지 않으므로 재서명 암호 해독을 사용해야 합니다.

참고 알려진 키 암호 해독을 사용하려면 서버 인증서 및 키를 내부 ID 인증서로 업로드한 다음 SSL 암호 해독 정책 설정에서 알려진 키 인증서 목록에 추가해야 합니다. 그러면 서버 주소를 대상 주소로 사용하여 알려진 키 암호 해독에 대한 규칙을 작성할 수 있습니다. SSL 암호 해독 정책에 인증서를 추가하는 데 대한 자세한 내용은 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 19 페이지를 참조하십시오.

암호 해독 안 함

특정 유형의 트래픽은 암호 해독을 우회하도록 선택하는 경우, 해당 트래픽에는 처리 작업이 수행되지 않습니다. 암호화된 트래픽은 일치하는 액세스 제어 규칙을 기반으로 허용 또는 차단되는 액세스 제어 정책으로 계속 진행됩니다.

차단

SSL 암호 해독 규칙과 일치하는 암호화된 트래픽을 간단하게 차단할 수 있습니다. SSL 암호 해독 정책에서 차단 기능을 사용하면 액세스 제어 정책에 연결할 수 없게 됩니다.

HTTPS 연결을 차단하는 경우 사용자에게 시스템 기본 차단 응답 페이지가 표시되지 않습니다. 대신 보안 연결 실패를 나타내는 브라우저의 기본 페이지가 표시됩니다. 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.

자동 생성된 SSL 암호 해독 규칙

SSL 암호 해독 정책의 활성화 여부와 관계없이, 시스템은 활성 인증을 구현하는 각 ID 정책 규칙에 대해 재서명 암호 해독 규칙을 자동으로 생성합니다. 이 작업은 HTTPS 연결에 대한 활성 인증을 활성화하는 데 필요합니다.

SSL 암호 해독 정책을 활성화하면 Identity Policy Active Authentication Rules(ID 정책 활성 인증 규칙) 머리글 아래에서 이 규칙을 확인할 수 있습니다. 이러한 규칙은 SSL 암호 해독 정책 상단에 읽기 전용으로 그룹화되어 있습니다. ID 정책을 변경해야만 규칙을 변경할 수 있습니다.

암호 해독이 불가능한 트래픽 처리

연결의 암호 해독이 불가능하게 만드는 몇 가지 특성이 있습니다. 연결에 다음 특성이 있는 경우, 연결이 다른 방법으로 일치할 수 있는 어떤 규칙과도 관계없이 기본 작업이 연결에 적용됩니다. 암호 해독 안 함 대신 차단을 기본 작업으로 선택하는 경우, 합법적인 트래픽의 과도한 삭제를 포함한 문제가 발생할 수 있습니다. 고급 및 해독 불가 트래픽 설정 구성, 20 페이지에 설명된 대로 기본 동작을 변경할 수 있습니다.

- 압축된 세션 — 데이터 압축이 연결에 적용되었습니다.
- SSLv2 세션 — 지원되는 최소 SSL 버전은 SSLv3입니다.
- 알려지지 않은 암호 그룹 — 시스템에서 연결에 대한 암호 그룹을 인식하지 않습니다.

- 지원되지 않는 암호 그룹 — 시스템에서 탐지된 암호 그룹을 기반으로 암호 해독을 지원하지 않습니다.
- 세션이 캐시되지 않음 — SSL 세션에서 세션 재사용이 활성화되었고 클라이언트 및 서버가 세션 식별자로 세션을 재설정했으며 시스템에서 해당 세션 식별자를 캐시하지 않았습니다.
- 핸드셰이크 오류 — SSL 핸드셰이크 협상 중에 오류가 발생했습니다.
- 암호 해독 오류 — 암호 해독 작업 중에 오류가 발생했습니다.
- 패시브 인터페이스 트래픽 — 패시브 인터페이스(패시브 보안 영역)의 모든 트래픽은 암호 해독할 수 없습니다.

SSL 암호 해독을 위한 라이선스 요건

SSL 암호 해독 정책을 사용하는 데에는 특수 라이선스가 필요하지 않습니다.

그러나 URL 카테고리 및 평판을 일치 기준으로 사용하는 규칙을 생성하려면 **URL** 라이선스가 필요합니다. 라이선스 구성에 대한 자세한 내용은 선택 가능한 라이선스 활성화 또는 비활성화를 참조하십시오.

SSL 암호 해독에 대한 지침

SSL 암호 해독 정책을 구성하고 모니터링할 때는 다음 사항에 유의하십시오.

- 액세스 제어 규칙이 다음에 해당할 때 신뢰 또는 차단으로 설정된 규칙과 일치하는 연결의 경우 SSL 암호 해독 정책이 우회됩니다.
  - 보안 영역, 네트워크, 지리위치 및 포트를 트래픽 일치 기준으로만 사용하는 경우.
  - 검사가 필요한 다른 규칙(예: 애플리케이션이나 URL을 기준으로 하는 연결과 일치하는 규칙) 앞에 오거나 침입 또는 파일 검사를 적용하는 규칙을 허용하는 경우.
- URL 카테고리 일치를 사용할 때는 사이트의 로그인 페이지가 사이트 자체의 카테고리와 다른 카테고리에 포함되는 경우가 있음을 고려해야 합니다. 예를 들어 Gmail은 "웹 기반 이메일" 카테고리에 포함되지만 로그인 페이지는 "인터넷 포털" 카테고리에 포함됩니다. 이러한 사이트에 대한 연결을 암호 해독하려면 두 카테고리를 모두 규칙에 포함해야 합니다.
- VDB(Vulnerability Database) 업데이트에서 사용되지 않는 애플리케이션을 제거하는 경우, 삭제된 애플리케이션을 사용하는 SSL 암호 해독 규칙 또는 애플리케이션 필터를 변경해야 합니다. 이러한 규칙을 수정할 때까지는 변경 사항을 구축할 수 없습니다. 또한 문제를 해결하기 전에는 시스템 소프트웨어 업데이트를 설치할 수 없습니다. Application Filters(애플리케이션 필터) 개체 페이지 또는 규칙의 Application(애플리케이션) 탭에서는 이러한 애플리케이션 이름 뒤에 "(사용되지 않음)"이라고 표시됩니다.

- 활성 인증 규칙이 있는 경우에는 SSL 암호 해독 정책을 비활성화할 수 없습니다. SSL 암호 해독 정책을 비활성화하려면 ID 정책을 비활성화하거나 활성 인증을 사용하는 ID 규칙을 삭제해야 합니다.

SSL 암호 해독 정책을 구현 및 유지 관리하는 방법

SSL 암호 해독 정책을 사용하여 암호화된 트래픽을 일반 텍스트 트래픽으로 전환할 수 있으므로 URL 필터링, 침입 및 악성코드 제어 그리고 기타 서비스(DPI(Deep Packet Inspection)를 필요로 함)를 적용할 수 있습니다. 정책에서 트래픽을 허용하는 경우, 트래픽은 디바이스를 떠나기 전에 다시 암호화됩니다.

SSL 암호 해독 정책은 암호화된 트래픽에만 적용됩니다. 암호화되지 않은 연결은 SSL 암호 해독 규칙을 기준으로 평가되지 않습니다.

일부 다른 보안 정책과 달리 SSL 암호 해독 정책은 인증서가 만료되거나 목적지 서버에서 변경될 수 있기 때문에 적극적으로 모니터링하고 유지 관리해야 합니다. 또한, MITM(Man-In-The-Middle) 공격과 재서명 암호 해독 작업은 구분할 수 없기 때문에 클라이언트 소프트웨어의 변경 사항에 따라 특정 연결을 암호 해독하는 능력이 변경될 수 있습니다.

다음 절차에서는 SSL 암호 해독 정책을 구현하고 유지 관리하는 엔드 투 엔드 프로세스에 대해 설명합니다.

프로시저

단계 **1** 재서명 암호 해독 규칙을 구현할 경우 필요한 내부 CA 인증서를 생성합니다.

내부 CA(인증 기관) 인증서를 사용해야 합니다. 다음과 같은 옵션이 있습니다. 사용자가 인증서를 신뢰해야 하므로 클라이언트 브라우저가 이미 신뢰하도록 구성되어 있는 인증서를 업로드하거나 업로드하는 인증서가 브라우저의 신뢰 저장소에 추가되어 있는지 확인합니다.

- 디바이스 자체에서 서명한 자체 서명 내부 CA 인증서를 생성합니다. 자체 서명 내부 및 내부 CA 인증서 생성의 내용을 참조하십시오.
- 외부 신뢰 CA 또는 조직 내부의 CA에서 서명한 키와 내부 CA 인증서를 업로드합니다. 내부 및 내부 CA 인증서 업로드의 내용을 참조하십시오.

단계 **2** 알려진 키 암호 해독 규칙을 구현할 경우, 각 내부 서버에서 인증서와 키를 수집합니다.

서버에서 인증서와 키를 얻어야 하므로 알려진 키 암호 해독은 제어하고 있는 서버에만 사용할 수 있습니다. 이러한 인증서와 키를 내부 인증서(내부 CA 인증서 아님)로 업로드합니다. 내부 및 내부 CA 인증서 업로드의 내용을 참조하십시오.

단계 **3** SSL 암호 해독 정책 활성화, 9 페이지.

정책을 활성화하는 경우 몇 가지 기본 설정도 구성합니다.

단계 **4** 기본 SSL 암호 해독 작업 구성, 10 페이지.

의심스러운 경우에는 **Do Not Decrypt(**암호 해독 안 함**)**를 기본 동작으로 선택합니다. 액세스 제어 정책은 여전히 필요한 경우 기본 SSL 암호 해독 규칙과 일치하는 트래픽을 삭제할 수 있습니다.

단계 **5** SSL 암호 해독 규칙 구성, 11 페이지.

암호 해독할 트래픽과 적용할 암호 해독 유형을 확인합니다.

단계 **6** 알려진 키 암호 해독을 구성하는 경우 SSL 암호 해독 정책 설정을 편집하여 해당 인증서를 포함합니다. 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 19 페이지의 내용을 참조하십시오.

단계 **7** 필요시 재서명 암호 해독 규칙에 사용된 CA 인증서를 다운로드하고 클라이언트 워크스테이션에서 브라우저에 업로드합니다.

인증서를 다운로드하고 클라이언트에게 배포하는 데 대한 자세한 내용은 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 21 페이지를 참조하십시오.

단계 **8** 주기적으로 재서명 및 알려진 키 인증서를 업데이트합니다.

- 재서명 인증서 - 만료되기 전에 이 인증서를 업데이트합니다. device manager를 통해 인증서를 생성하는 경우, 유효 기간은 5년입니다. 인증서의 유효 기간을 확인하려면 **Objects(**개체**)** > **Certificates(**인증서**)**를 선택하고 목록에서 인증서를 찾은 다음 Actions(작업) 열에서 이에 대한 정보 아이콘( )을 클릭합니다. 정보 대화 상자에는 유효 기간 및 몇 가지 기타 특성이 표시됩니다. 이 페이지에서 대체 인증서를 업로드할 수도 있습니다.
- 알려진 키 인증서 - 모든 알려진 키 암호 해독 규칙의 경우, 목적지 서버의 현재 인증서와 키를 업로드했는지 확인해야 합니다. 또한, 지원되는 서버에서 인증서와 키가 변경될 때마다 새 인증서와 키를 내부 인증서로 업로드하고 새 인증서를 사용하도록 SSL 암호 해독 설정을 업데이트해야 합니다.

단계 **9** 외부 서버에 대해 누락된, 신뢰할 수 있는 CA 인증서를 업로드합니다.

시스템에는 신뢰할 수 있는 CA 루트 및 중간 인증서(서드파티에서 발급)가 다양하게 포함되어 있습니다. 이러한 항목은 암호 해독 재서명 규칙에 대해 위협 방어과(와) 대상 서버 간의 연결을 협상할 때 필요합니다.

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. **Objects(**개체**)** > **Certificates(**인증서**)** 페이지에서 인증서를 업로드합니다. 신뢰할 수 있는 CA 인증서 업로드의 내용을 참조하십시오.

SSL 암호 해독 정책 구성

SSL 암호 해독 정책을 사용하여 암호화된 트래픽을 일반 텍스트 트래픽으로 전환할 수 있으므로 URL 필터링, 침입 및 악성코드 제어 그리고 기타 서비스(DPI(Deep Packet Inspection)를 필요로 함)를 적용할 수 있습니다. 정책에서 트래픽을 허용하는 경우, 트래픽은 디바이스를 떠나기 전에 다시 암호화됩니다.

SSL 암호 해독 정책은 암호화된 트래픽에만 적용됩니다. 암호화되지 않은 연결은 SSL 암호 해독 규칙을 기준으로 평가되지 않습니다.

참고 VPN 터널은 SSL 암호 해독 정책이 평가되기 전에 암호 해독되므로 정책은 터널에 적용되지 않습니다. 그러나 터널 내의 암호화된 연결은 모두 SSL 암호 해독 정책을 기준으로 평가받습니다.

다음 절차에서는 SSL 암호 해독 정책을 구성하는 방법에 대해 설명합니다. SSL 암호 해독 생성 및 관리의 엔드 투 엔드 프로세스에 대한 설명은 SSL 암호 해독 정책을 구현 및 유지 관리하는 방법, 6 페이지를 참조하십시오.

시작하기 전에

SSL 암호 해독 규칙 테이블에는 다음과 같이 두 가지 섹션이 있습니다.

- **Identity Policy Active Authentication Rules(ID** 정책 활성 인증 규칙**)** - ID 정책을 활성화하고 활성 인증을 사용하는 규칙을 생성하는 경우, 시스템에서는 정책이 작동하도록 설정하는 데 필요한 SSL 암호 해독 규칙을 자동으로 생성합니다. 이러한 규칙은 항상 직접 생성하는 SSL 암호 해독 규칙보다 먼저 평가됩니다. 또한, 이러한 규칙은 ID 정책을 변경하는 방식으로 간접적으로만 변경할 수 있습니다.
- **SSL Native Rules(SSL** 기본 규칙**)** - 이미 구성한 규칙입니다. 규칙은 이 섹션에만 추가할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

정책을 아직 활성화하지 않은 경우 **Enable SSL Decryption(SSL** 암호 해독 활성화**)**을 클릭하여 SSL 암호 해독 정책 활성화, 9 페이지에 설명된 대로 정책 설정을 구성합니다.

단계 **2** 정책의 기본 작업을 구성합니다.

가장 안전한 방법은 **Do Not Decrypt(**암호 해독 안 함**)**를 선택하는 것입니다. 자세한 내용은 기본 SSL 암호 해독 작업 구성, 10 페이지의 내용을 참고하십시오.

단계 **3** SSL 암호 해독 정책을 관리합니다.

SSL 암호 해독 설정을 구성하고 나면 이 페이지에 모든 규칙이 순서대로 나열됩니다. 목록의 맨 위에서부터 규칙과 트래픽의 일치 여부를 확인하며, 첫 번째로 일치하는 규칙에 따라 적용할 작업이 결정됩니다. 이 페이지에서는 다음을 수행할 수 있습니다.

- 정책을 비활성화하려면 **SSL Decryption Policy(SSL** 암호 해독 정책**)** 토글을 클릭합니다. **Enable SSL Decryption(SSL** 암호 해독 활성화**)**을 클릭하여 다시 활성화할 수 있습니다.
- 정책에서 사용된 인증서의 목록을 포함한 정책 설정을 수정하려면 **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼(⚙)을 클릭하십시오.(SSL 암호 해독 설정 구성, 19 페이지참조) 또한, 클라

이언트에게 배포할 수 있도록 재서명 암호 해독 규칙에 사용되는 인증서를 다운로드할 수 있습니다. 다음 주제를 참조하십시오.

- 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 19 페이지
- 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 21 페이지

- 규칙을 구성하려면 다음을 수행합니다.
  - 새 규칙을 생성하려면 + 버튼을 클릭합니다. SSL 암호 해독 규칙 구성, 11 페이지의 내용을 참조하십시오.
  - 기존 규칙을 수정하려면 Actions(작업) 열에서 해당 규칙의 수정 아이콘()을 클릭합니다. 테이블에서 속성을 클릭하여 규칙 속성을 선택적으로 수정할 수도 있습니다.
  - 더 이상 필요하지 않은 규칙을 삭제하려면 Actions(작업) 열에서 해당 규칙의 삭제 아이콘()을 클릭합니다.
- 규칙을 이동하려면 규칙을 수정하고 **Order(**순서**)** 드롭다운 목록에서 새 위치를 선택합니다.
- 예를 들어 제거 또는 변경된 URL 카테고리 때문에 어떤 규칙에 문제가 생긴 경우에는 검색 상자 옆에 있는 **See Problem Rules(**문제 규칙 참조**)** 링크를 클릭하여 해당 규칙만 표시하도록 테이블을 필터링합니다. 이러한 규칙에서 필요한 서비스를 제공하도록 수정 및 교정(또는 삭제)하십시오.

SSL 암호 해독 정책 활성화

SSL 암호 해독 규칙을 구성하기 전에 정책을 활성화하고 몇 가지 기본 설정을 구성해야 합니다. 다음 절차에서는 정책을 직접 활성화하는 방법에 대해 설명합니다. ID 정책을 활성화하는 경우에도 정책을 활성화할 수 있습니다. ID 정책의 경우 SSL 암호 해독 정책을 활성화해야 합니다.

시작하기 전에

SSL 암호 해독 정책이 없는 릴리스에서 업그레이드했지만 활성 인증 규칙이 있는 ID 정책을 구성한 경우에는 SSL 암호 해독 정책이 이미 활성화되어 있습니다. 사용할 재서명 암호 해독 인증서를 선택하고 선택적으로 사전 정의된 규칙을 활성화합니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 **2** 정책 설정을 구성하려면 **Enable SSL Decryption(SSL** 암호 해독 활성화**)**을 클릭합니다.

- 처음으로 정책을 활성화한 경우, SSL Decryption Configuration(SSL 암호 해독 컨피그레이션) 대화 상자가 열립니다. 다음 단계를 계속 진행합니다.

- 이미 한 번 정책을 구성했다가 비활성화한 경우, 간단히 이전 설정 및 규칙을 사용하여 정책을 다시 활성화할 수 있습니다. **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼()을 클릭하여 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 19 페이지에 설명된 대로 설정을 컨피그레이션할 수 있습니다.

단계 **3** **Decrypt Re-Sign Certificate(**재서명 암호 해독 인증서**)**에서 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다.

사전 정의된 NGFW-Default-InternalCA 인증서를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create Internal CA(**내부 **CA** 생성**)**를 클릭하여 생성합니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼()을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 21 페이지도 참조하십시오.

단계 **4** (선택 사항). **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)** 아래에서 **+**를 클릭하고 정책에서 신뢰할 인증서 또는 인증서 그룹을 선택합니다.

기본 그룹인 CTA(Cisco-Trusted-Authorities)에는 시스템 정의된 신뢰할 수 있는 CA 인증서가 모두 포함됩니다. 추가 인증서를 업로드한 경우 여기서 인증서를 추가하거나 사용자의 그룹에서 이를 수집하여 여기에서 그룹을 선택할 수 있습니다. CTA(Cisco-Trusted-Authorities) 그룹을 교체하거나 사용자의 그룹을 추가하기만 하면 됩니다. 인증서의 서명 기관이 이 목록에 없는 사이트에 대한 인증서를 수락하라는 메시지가 사용자에게 표시됩니다. 인증서를 신뢰할 수 없다는 이유 만으로 사이트에 대한 액세스가 차단되지는 않습니다.

목록을 비워 두거나 빈 인증서 그룹만 선택하면 SSL 암호 해독 정책에서 모든 인증서를 신뢰합니다.

단계 **5** 초기 SSL 암호 해독 규칙을 선택합니다.

시스템에는 다음과 같이 유용하게 활용할 수 있는, 사전 정의된 규칙이 있습니다.

- **Sensitive_Data** - 이 규칙은 금융 서비스 또는 보건 및 의료 URL 카테고리(은행, 의료 서비스 등 포함)에 있는 웹 사이트와 일치하는 트래픽을 암호 해독하지 않습니다. 이 규칙을 구현하려면 URL 라이선스를 활성화해야 합니다.

단계 **6** **Enable(**활성화**)**을 클릭합니다.

기본 SSL 암호 해독 작업 구성

특정 SSL 암호 해독 규칙과 일치하지 않는 암호화된 연결은 SSL 암호 해독 정책의 기본 작업에 의해 처리됩니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 **2** **Default Action(**기본 작업**)** 필드에서 아무 곳이나 클릭합니다.

단계 **3** 일치하는 트래픽에 적용할 작업을 선택합니다.

- **Do Not Decrypt(**암호 해독 안 함**) -** 암호화된 연결을 허용합니다. 그러면 액세스 제어 정책이 암호화된 연결을 평가하고 액세스 제어 규칙을 기반으로 삭제 또는 허용합니다.
- **Block(**차단**) -** 연결을 즉시 삭제합니다. 연결은 액세스 제어 정책으로 전달되지 않습니다.

단계 **4** (선택 사항). 기본 작업에 대한 로깅을 구성합니다.

기본 작업과 일치하는 트래픽에 대한 로깅을 활성화해야 대시보드 데이터 또는 이벤트 뷰어에 해당 트래픽이 포함됩니다. 다음 옵션 중에서 선택합니다.

- **At End of Connection(**연결 종료 시**)** — 연결 종료 시 이벤트를 생성합니다.
  - **Send Connection Events To(**다음으로 연결 이벤트 보내기**)** — 외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우, syslog 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server(**새 **Syslog** 서버 생성**)**를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 비활성화하려면 서버 목록에서 **Any(**모두**)**를 선택합니다.

    디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.
- **No Logging(**로깅 없음**)** — 이벤트를 생성하지 않습니다.

단계 **5** **Save(**저장**)**를 클릭합니다.

SSL 암호 해독 규칙 구성

SSL 암호 해독 규칙을 사용하여 암호화된 연결 처리 방법을 결정합니다. SSL 암호 해독 정책의 규칙은 위에서부터 아래로 평가됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

SSL 기본 규칙 섹션에서만 규칙을 생성하고 편집할 수 있습니다.

참고 VPN 연결(사이트 대 사이트 및 원격 액세스 모두)에 대한 트래픽은 SSL 암호 해독 정책이 연결을 평가하기 전에 암호 해독됩니다. 따라서 SSL 암호 해독 규칙은 VPN 연결에 적용되지 않으며 이러한 규칙을 생성할 때 VPN 연결을 고려할 필요가 없습니다. 그러나 VPN 터널 내에서 사용된 암호화된 연결은 모두 평가됩니다. 예를 들어, RA VPN 연결을 통과하는 내부 서버에 대한 HTTPS 연결은 SSL 암호 해독 규칙을 기준으로 평가됩니다. 단, RA VPN 터널 자체는 이미 암호 해독되어 있으므로 이를 통과하는 경우에는 평가되지 않습니다.

시작하기 전에

알려진 키 암호 해독 규칙을 생성하는 경우, 목적지 서버(내부 인증서 역할)의 인증서 및 키를 업로드하고, SSL 암호 해독 정책 설정을 편집하여 이 인증서를 사용합니다. 알려진 키 규칙은 일반적으로

규칙의 대상 네트워크 기준에서 목적지 서버를 지정합니다. 자세한 내용은 알려진 키 및 재서명 암호 해독을 위한 인증서 구성, 19 페이지의 내용을 참고하십시오.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

SSL 암호 해독 규칙(활성 인증 ID 규칙에 대해 자동으로 생성된 규칙 제외)을 구성하지 않은 경우, **Add Pre-Defined Rules(**사전 정의된 규칙 추가**)**를 클릭하여 사전 정의된 규칙을 추가할 수 있습니다. 원하는 규칙을 선택하라는 프롬프트가 표시됩니다.

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘()을 클릭합니다.

단계 **3** **Order(**순서**)**에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.

SSL Native Rules(SSL 기본 규칙**)** 섹션에만 규칙을 삽입할 수 있습니다. Identity Policy Active Authentication Rules(ID 정책 활성 인증 규칙)가 ID 정책에서 자동으로 생성되며, 이 규칙은 읽기 전용입니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

단계 **4** **Tile(**제목**)**에서 규칙의 이름을 입력합니다.

이름에는 공백을 포함할 수 없지만, 영숫자 및 특수 문자(+, ., _, -)는 사용할 수 있습니다.

단계 **5** 일치하는 트래픽에 적용할 작업을 선택합니다.

각 옵션에 대한 자세한 내용은 다음을 참조하십시오.

- 재서명 암호 해독, 2 페이지
- 알려진 키 암호 해독, 3 페이지
- 암호 해독 안 함, 4 페이지
- 차단, 4 페이지

단계 **6** 다음 탭을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source/Destination(**소스/대상**)** - 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 TCP 포트입니다. 기본값은 영역, 주소, 지리

적 위치 및 TCP 포트입니다. SSL 암호 해독 규칙에 대한 소스/대상 기준, 14 페이지의 내용을 참조하십시오.

- **Application(애플리케이션)** - 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 애플리케이션입니다. 기본값은 암호화된 애플리케이션입니다. SSL 암호 해독 규칙에 대한 애플리케이션 기준, 15 페이지를 참조하십시오.
- **URL** - 웹 요청의 URL 카테고리입니다. 기본값은 일치를 위해 고려되지 않은 URL 카테고리와 평판입니다. SSL 암호 해독 규칙에 대한 URL 기준, 16 페이지의 내용을 참조하십시오.
- **Users(사용자)** - ID 소스, 사용자 또는 사용자 그룹입니다. ID 정책에 따라 트래픽 일치에 사용자 및 그룹 정보를 사용할 수 있는지가 결정됩니다. 이 기준을 사용하려면 ID 정책을 구성해야 합니다. SSL 암호 해독 규칙에 대한 사용자 기준, 17 페이지의 내용을 참조하십시오.
- **Advanced(고급)** - SSL/TLS 버전 및 인증서 상태와 같이 연결에서 사용하는 인증서에서 파생된 특성입니다. SSL 암호 해독 규칙에 대한 고급 기준, 18 페이지의 내용을 참조하십시오.

조건을 수정하려면 해당 조건 내의 + 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화상자에서 **OK(확인)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

SSL 암호 해독 규칙에 조건을 추가하는 경우 다음 팁을 고려하십시오.

- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용하려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어, URL 카테고리를 기반으로 트래픽을 암호 해독하는 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어, 최대 50개의 애플리케이션 또는 애플리케이션 필터에 대해 애플리케이션 제어를 적용하는 단일 규칙을 사용할 수 있습니다. 따라서 단일 조건의 항목 간 관계는 OR이고 조건 유형 간의 관계(예: 소스/대상과 애플리케이션 간의 관계)는 AND가 됩니다.
- 일치하는 URL 카테고리에는 URL 필터링 라이선스가 필요합니다.

단계 **7** (선택 사항). 규칙에 대해 로깅을 구성합니다.

대시보드 데이터 또는 이벤트 뷰어에 포함될 규칙과 일치하는 트래픽에 대한 로깅을 활성화해야 합니다. 다음 옵션 중에서 선택합니다.

- **At End of Connection(연결 종료 시)** — 연결 종료 시 이벤트를 생성합니다.
  - **Send Connection Events To(다음으로 연결 이벤트 보내기)** — 외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우, syslog 서버를 정의하는 서버 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server(새 Syslog 서버 생성)**를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 비활성화하려면 서버 목록에서 Any(모두)를 선택합니다.

    디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.
- **No Logging(로깅 없음)** — 이벤트를 생성하지 않습니다.

단계 **8** **OK(**확인**)**를 클릭합니다.

SSL 암호 해독 규칙에 대한 소스/대상 기준

SSL 암호 해독 규칙의 소스/대상 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치) 또는 트래픽에서 사용되는 TCP 포트를 정의합니다. 기본값은 영역, 주소, 지리적 위치 또는 TCP 포트입니다. TCP는 SSL 암호 해독 규칙과 일치되는 유일한 프로토콜입니다.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

다음 기준을 사용하여 규칙과 일치하는 소스 및 대상을 식별할 수 있습니다.

소스 영역**,** 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 외부 호스트에서 내부 호스트로 이동하는 모든 트래픽을 암호 해독하려는 경우에는 외부 영역을 **Source Zones(**소스 영역**)**로, 내부 영역을 **Destination Zones(**대상 영역**)**로 선택합니다.

소스 네트워크**,** 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다.

참고 알려진 키 암호 해독 규칙의 경우 업로드한 인증서와 키를 사용하는 목적지 서버의 IP 주소를 사용하는 개체를 선택합니다.

- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

소스 포트**,** 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP 프로토콜 및 포트는 SSL 암호 해독 규칙에 대해서만 지정할 수 있습니다.

- TCP 포트에서 발생하는 트래픽을 일치시키려면 **Source Ports(**소스 포트**)**를 구성합니다.
- TCP 포트로 향하는 트래픽을 일치시키려면 **Destination Ports/Protocols(**대상 포트/프로토콜**)**를 구성합니다.
- 특정 TCP 포트에서 발생하는 트래픽과 특정 TCP 포트로 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

SSL 암호 해독 규칙에 대한 애플리케이션 기준

SSL 암호 해독 규칙의 애플리케이션 기준은 유형, 카테고리, 태그, 위험 또는 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 IP 연결에 사용되는 애플리케이션을 정의합니다. 기본값은 SSL 프로토콜 태그가 있는 모든 애플리케이션입니다. SSL 암호 해독 규칙은 어떤 암호화되지 않은 애플리케이션과도 일치시킬 수 없습니다.

규칙에서 개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 사업 타당성이 낮은 모든 애플리케이션을 암호 해독하거나 차단하는 SSL 암호 해독 규칙을 생성할 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 암호 해독되거나 차단됩니다.

이와 더불어 Cisco에서는 시스템 및 VDB(Vulnerability Database)를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션에 대한 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

규칙에서 애플리케이션 및 필터를 직접 지정하거나 이러한 특성을 정의하는 애플리케이션 필터 개체를 생성할 수 있습니다. 이 두 가지 경우의 사양은 동일하지만, 개체를 사용하면 복잡한 규칙을 생성할 때에도 시스템 제한(기준당 항목 50개)을 유지하기가 더욱 쉽습니다.

애플리케이션 및 필터 목록을 수정하려면 조건 내에서 **+** 버튼을 클릭하고 개별 탭에 나열된 원하는 애플리케이션 또는 애플리케이션 필터 개체를 선택한 후에 팝업 대화 상자에서 **OK(**확인**)**를 클릭합

니다. 탭 중 하나에서 **Advanced Filter(**고급 필터**)**를 클릭하면 필터 기준을 선택하거나 특정 애플리케이션을 검색할 수 있습니다. 애플리케이션, 필터 또는 개체에 대해 **x**를 클릭하면 정책에서 해당 항목을 제거할 수 있습니다. **Save As Filter(**필터로 저장**)** 링크를 클릭하면 아직 개체가 아닌 결합된 기준을 새 애플리케이션 필터 개체로 저장할 수 있습니다.

애플리케이션 기준과 고급 필터를 구성하고 애플리케이션을 선택하는 방법에 대한 자세한 내용은 애플리케이션 필터 개체 구성를 참조하십시오.

SSL 암호 해독 규칙에서 애플리케이션 기준을 사용할 때 다음 팁을 고려하십시오.

- 시스템은 StartTLS를 사용하여 암호화되는 해독된 애플리케이션을 식별할 수 있습니다. 여기에는 SMTPS, POPS, FTPS, TelnetS, IMAPS 같은 애플리케이션이 포함됩니다. 또한, 시스템은 TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서 주체 고유 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다.
- 시스템은 서버 인증서 교환 이후에만 애플리케이션을 식별할 수 있습니다. SSL 핸드셰이크 중에 교환된 트래픽이 애플리케이션 조건을 포함하는 SSL 규칙의 다른 모든 조건과 일치하지만 식별이 완료되지 않은 경우, SSL 정책을 사용하여 패킷을 통과하도록 할 수 있습니다. 이러한 동작을 통해 핸드셰이크가 완료되므로 애플리케이션을 식별할 수 있습니다. 시스템에서 식별을 완료하면, 애플리케이션 조건과 매칭되는 나머지 세션 트래픽에 SSL 규칙 작업을 적용합니다.
- 선택한 애플리케이션을 VDB 업데이트를 통해 제거한 경우 애플리케이션 이름 뒤에 "(Depredcated(사용되지 않음))"이라고 표시됩니다. 이러한 애플리케이션은 필터에서 제거해야 합니다. 그렇지 않으면 후속 구축 및 시스템 소프트웨어 업그레이드가 차단됩니다.

SSL 암호 해독 규칙에 대한 URL 기준

SSL 암호 해독 규칙의 URL 기준은 웹 요청의 URL이 속하는 카테고리를 정의합니다. 또한, 암호 해독, 차단 또는 암호 해독 없이 허용할 사이트의 상대적인 평판을 지정할 수 있습니다. 기본값은 URL 카테고리를 기반으로 하는 연결과 일치하지 않습니다.

예를 들어, 암호화된 모든 게임 사이트를 차단하거나 신뢰할 수 없는 소셜 네트워킹 사이트를 암호 해독할 수 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL을 찾아보려고 시도하는 경우, 세션이 차단 또는 암호 해독됩니다. URL 카테고리 일치에 대한 자세한 정보는 카테고리 및 평판을 기준으로 URL 필터링의 내용을 참조하십시오.

범주 탭

+를 클릭하고 원하는 범주를 선택한 후에 **OK(**확인**)**를 클릭합니다. 카테고리의 **x**를 클릭하면 정책에서 해당 카테고리를 제거할 수 있습니다.

기본적으로는 평판과 관계없이 선택한 각 범주의 모든 URL에 규칙을 적용합니다. 평판을 기준으로 하여 규칙을 제한하려면 각 범주의 아래쪽 화살표를 클릭하고 임의 체크 박스 선택을 취소한 후에 평판 슬라이더를 사용하여 평판 레벨을 선택합니다. 평판 슬라이더의 왼쪽에는 암호 해독 없이 허용할 사이트가, 오른쪽에는 암호 해독하거나 차단할 사이트가 표시됩니다. 평판 사용 방식은 규칙 작업에 따라 달라집니다.

- 규칙이 연결을 암호 해독하거나 차단하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 높은 평판도 모두 선택됩니다. 예를 들어, **Questionable sites(**의심스러운 사이트**)**(레벨

2)를 암호 해독하거나 차단하는 규칙을 구성하는 경우, **Untrusted(**신뢰할 수 없음**)**(레벨 1) 사이트도 자동으로 암호 해독되거나 차단됩니다.

- 규칙이 연결을 암호 해독 없이 허용(암호 해독 안 함)하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 낮은 평판도 모두 선택됩니다. 예를 들어, **Favorable sites(**선호 사이트**)**(레벨 4)를 암호 해독하지 않는 규칙을 구성하는 경우, **Trusted(**신뢰할 수 있음**)**(레벨 5) 사이트도 자동으로 암호 해독되지 않습니다.

평판을 알 수 없는 URL을 평판 일치에 포함하려면 **Include Sites with Unknown Reputation(**평판을 알 수 없는 사이트 포함**)** 옵션을 선택합니다. 새 사이트는 일반적으로 등급이 지정되지 않으며, 사이트의 평판을 알 수 없거나 확인할 수 없는 다른 이유가 있을 수 있습니다.

URL의 카테고리 확인

특정 URL의 카테고리 및 평판을 확인할 수 있습니다. **URL to Check(**확인할 **URL)** 상자에서 URL을 입력하고 **Go(**이동**)**를 클릭하십시오. 결과를 볼 수 있는 외부 웹 사이트로 연결됩니다. 분류에 동의하지 않는 경우 **Submit a URL Category Dispute(URL** 카테고리 이의 제출**)** 링크를 클릭하고 저희에게 알려주십시오.

SSL 암호 해독 규칙에 대한 사용자 기준

SSL 암호 해독 규칙의 사용자 기준은 IP 연결의 사용자 또는 사용자 그룹을 정의합니다. 규칙에 사용자 또는 사용자 그룹 기준을 포함하려면 ID 정책 및 관련 디렉터리 서버를 구성해야 합니다.

ID 정책에 따라 특정 연결에 대해 사용자 ID가 수집되는지가 결정됩니다. ID가 설정된 경우에는 호스트의 IP 주소가 식별된 사용자와 연결됩니다. 그러므로 해당 소스 IP 주소가 사용자에 매핑된 트래픽은 해당 사용자가 보내는 것으로 간주됩니다. IP 패킷 자체는 사용자 ID 정보를 포함하지 않으므로 이 IP 주소에서 사용자로의 매핑은 가능한 최적의 근사치입니다.

규칙에는 최대 50개의 사용자나 그룹을 추가할 수 있으므로 일반적으로는 개별 사용자를 선택하는 것보다 그룹을 선택하는 것이 더 효율적입니다. 예를 들어 외부 네트워크에서 오는 엔지니어링 그룹에 대한 트래픽을 해독하는 규칙을 생성하고 이 그룹에서 나오는 발신 트래픽의 암호를 해독하지 않는 별도의 규칙을 만들 수 있습니다. 그러면 신규 엔지니어에 대해 규칙을 적용하려는 경우 디렉터리 서버의 엔지니어링 그룹에 해당 엔지니어를 추가하기만 하면 됩니다.

해당 소스 내 모든 사용자에게 적용할 ID 소스도 선택할 수 있습니다. 따라서 여러 Active Directory 도메인을 지원하는 경우, 도메인에 근거하여 차등 암호 해독을 제공할 수 있습니다.

사용자 목록을 수정하려면 조건 내의 **+** 버튼을 클릭하고 다음 기술 중 하나를 사용하여 원하는 사용자 또는 사용자 그룹을 선택합니다. 사용자 또는 그룹의 **x**를 클릭하면 정책에서 해당 사용자나 그룹을 제거할 수 있습니다.

- **Identity Sources(ID** 소스**)** - 선택한 소스에서 얻은 모든 사용자에게 규칙을 적용하려면 AD 영역 또는 로컬 사용자 데이터베이스 같은 ID 소스를 선택합니다. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 바로 생성합니다.
- **Groups(**그룹**)** - 원하는 사용자 그룹을 선택합니다. 그룹은 디렉터리 서버에서 그룹을 구성하는 경우에만 사용할 수 있습니다. 그룹을 선택하면 하위 그룹을 포함하여 그룹의 모든 멤버에게 규칙이 적용됩니다. 하위 그룹을 다르게 처리하려는 경우에는 하위 그룹용으로 별도의 액세스 규칙을 생성한 다음 액세스 제어 정책에서 상위 그룹용 규칙 위에 배치해야 합니다.

- **Users(**사용자**)** - 개별 사용자를 선택합니다. 사용자 이름에는 Realm\username과 같은 ID 소스가 접두사로 붙습니다.

  Special-Identities-Realm에서 일부 사용자는 기본으로 제공됩니다.

  - **Failed Authentication(**실패한 인증**)** - 사용자에게 인증하라는 메시지가 표시되었는데 사용자가 허용되는 최대 횟수 이내에 유효한 사용자 이름/비밀번호 쌍을 입력하지 못했습니다. 인증에 실패해도 사용자의 네트워크 액세스가 차단되지는 않지만, 이러한 사용자의 네트워크 액세스를 제한하는 액세스 규칙을 작성할 수 있습니다.
  - **Guest(**게스트**)** - 게스트 사용자는 ID 규칙이 이러한 사용자를 게스트로 지칭하도록 구성된다는 점을 제외하면 실패한 인증 사용자와 비슷합니다. 즉, 게스트 사용자 역시 인증하라는 메시지가 표시되었지만, 최대 시도 횟수 이내에 인증하지 못한 사용자입니다.
  - **No Authentication Required(**인증 필요 없음**)** - 사용자의 연결이 인증을 지정하지 않은 ID 규칙과 일치하여 인증하라는 메시지가 표시되지 않았습니다.
  - **Unknown(**알 수 없음**)** - IP 주소에 대한 사용자 매핑이 없으며 아직 실패한 인증 기록이 없습니다. 이는 일반적으로 해당 주소에서 HTTP 트래픽이 아직 전송되지 않았음을 의미합니다.

SSL 암호 해독 규칙에 대한 고급 기준

고급 트래픽 일치 기준은 연결에 사용되는 인증서에서 파생된 특성과 관련이 있습니다. 다음 옵션 중 하나 또는 모두를 구성할 수 있습니다.

인증서 속성

선택한 속성 중 하나와 일치하는 트래픽은 규칙의 인증서 속성 옵션과 일치합니다. 다음을 구성할 수 있습니다.

인증서 상태

인증서 상태가 **Valid(**유효함**)** 또는 **Invalid(**유효하지 않음**)**인지 여부입니다. 인증서 상태가 중요하지 않은 경우, **Any(**모두**)**(기본값)를 선택합니다.

인증서는 다음 조건을 모두 충족하는 경우 유효한 것으로 간주되며, 그렇지 않은 경우에는 유효하지 않습니다.

- 정책이 인증서를 발급한 CA를 신뢰합니다.
- 인증서의 내용에 대해 인증서의 서명을 제대로 검증할 수 있습니다.
- 발급자 CA 인증서가 정책의 신뢰할 수 있는 CA 인증서 목록에 저장됩니다.
- 정책의 신뢰할 수 있는 CA가 인증서를 취소하지 않음
- 현재 날짜가 인증서의 유효 시작일과 유효 만료일 사이에 해당합니다.

자체 서명

서버 인증서에 동일한 주체 및 발급자 고유 이름이 포함되어 있는지 여부입니다. 다음 중 하나를 선택합니다.

- **Self-Signing(**자체 서명**)** — 서버 인증서가 자체 서명되었습니다.
- **CA-Signing(CA** 서명**)** — 서버 인증서가 CA(인증 기관)에 의해 서명되었습니다. 즉, 발급자와 주체가 동일하지 않습니다.
- **Any(**모두**)** — 인증서가 일치 기준으로 자체 서명되었는지를 신경 쓰지 않습니다.

지원되는 버전

일치하는 SSL/TLS 버전입니다. 규칙은 선택한 버전 중 하나를 사용하는 트래픽에 적용됩니다. 기본값은 모든 버전입니다. **SSL 3.0**, **TLS 1.0**, **TLS 1.1**, **TLS 1.2**, **TLS 1.3** 중에서 선택합니다.

예를 들어 TLSv1.2/3 연결만 허용하려는 경우 하위 버전에 대한 차단 규칙을 생성할 수 있습니다.

TLS 1.3 연결을 일치시키려면 Snort 3을 사용해야 합니다.

나열되지 않은 버전(예: SSL v2.0)을 사용하는 트래픽은 SSL 암호 해독 정책에 대한 기본 작업에 의해 처리됩니다.

SSL 암호 해독 설정 구성

트래픽을 해독하는 규칙이 있는 경우 인증서 설정을 구성해야 합니다. 또한 설정을 수정하여 암호화된 트래픽에 암호 해독이 적용되는 방식을 변경할 수 있습니다. 다음 주제에서는 옵션에 대해 설명합니다.

알려진 키 및 재서명 암호 해독을 위한 인증서 구성

재서명하거나 알려진 키를 사용하여 암호 해독을 구현하는 경우, SSL 암호 해독 규칙에서 사용할 수 있는 인증서를 식별해야 합니다. 모든 인증서가 유효하고 만료되지 않았는지 확인합니다.

특히 알려진 키 암호 해독의 경우, 암호 해독 중인 연결을 지닌 각 목적지 서버의 현재 인증서 및 키가 시스템에 있는지 확인해야 합니다. 알려진 키 암호 해독 규칙과 함께 암호 해독을 위해 목적지 서버의 실제 인증서와 키를 사용합니다. 따라서 위협 방어 디바이스에는 항상 현재 인증서 및 키가 있어야 합니다. 그러지 않으면 암호 해독에 실패합니다.

알려진 키 규칙으로 목적지 서버에서 인증서 또는 키를 변경할 때마다 새로운 내부 인증서와 키를 업로드합니다. 단, 내부 CA 인증서가 아니라 내부 인증서로 업로드합니다. 다음 절차를 통해 인증서를 업로드하거나 **Objects(**개체**)** > **Certificates(**인증서**)** 페이지로 이동하여 인증서를 업로드할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 **2** **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼(⚙)을 클릭합니다.

필요한 경우 **Basic(**기본**)** 탭을 선택합니다.

단계 **3** **Decrypt Re-Sign Certificate(**재서명 암호 해독 인증서**)**에서 재서명된 인증서를 이용하여 암호 해독을 구현하는 규칙에 사용할 내부 CA 인증서를 선택합니다.

사전 정의된 NGFW-Default-InternalCA 인증서를 사용하거나, 생성 또는 업로드한 인증서를 사용할 수 있습니다. 인증서가 아직 없으면 **Create Internal CA(**내부 **CA** 생성**)**를 클릭하여 생성합니다.

클라이언트 브라우저에서 인증서를 아직 설치하지 않은 경우, 다운로드 버튼( )을 클릭하여 복사본을 획득합니다. 인증서 설치 방법에 대한 자세한 내용은 각 브라우저에 대한 설명서를 참조하십시오. 재서명 암호 해독 규칙을 위한 CA 인증서 다운로드, 21 페이지도 참조하십시오.

단계 **4** 알려진 키를 사용하여 암호를 해독하는 각 규칙의 경우 목적지 서버의 내부 인증서 및 키를 업로드합니다.

a) **Decrypt Known-Key Certificates(**알려진 키 암호 해독 인증서**)** 아래에서 +를 클릭합니다.
b) 내부 ID 인증서를 선택하거나 **Create New Internal Certificate(**새 내부 인증서 생성**)**를 클릭하여 바로 업로드합니다.
c) **OK(**확인**)**를 클릭합니다.

단계 **5** (선택 사항). **Trusted CA Certificates(**신뢰할 수 있는 **CA** 인증서**)** 아래에서 +를 클릭하고 정책에서 신뢰할 인증서 또는 인증서 그룹을 선택합니다.

기본 그룹인 CTA(Cisco-Trusted-Authorities)에는 시스템 정의된 신뢰할 수 있는 CA 인증서가 모두 포함됩니다. 이 설정을 변경할 수 있는 주요 사례는 다음과 같습니다.

- 기본 그룹에 없는 신뢰할 수 있는 CA 인증서를 사용하고자 합니다. 그러면 SSL 암호 해독 정책 설정에서 기본 그룹과 새 그룹을 모두 선택합니다. 신뢰할 수 있는 추가 CA 인증서를 업로드한 경우 이 작업을 수행할 수 있습니다.
- 기본 그룹에 있는 것보다 더욱 제한된 신뢰할 수 있는 CA 인증서 목록을 사용하고자 합니다. 그러면 델타 뿐 아니라 신뢰할 수 있는 인증서의 전체 목록이 포함된 그룹을 생성하고 이를 SSL 암호 해독 정책 설정에서 단독 그룹으로 선택합니다.

인증서의 서명 기관이 이 목록에 없는 사이트에 대한 인증서를 수락하라는 메시지가 사용자에게 표시됩니다. 인증서를 신뢰할 수 없다는 이유 만으로 사이트에 대한 액세스가 차단되지는 않습니다.

목록을 비워 두거나 빈 인증서 그룹만 선택하면 SSL 암호 해독 정책에서 모든 인증서를 신뢰합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

고급 및 해독 불가 트래픽 설정 구성

기본 동작을 사용하지 않는 경우 고급 암호 해독 설정 및 해독 불가 트래픽에 대한 설정을 구성할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 **2** **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼( )을 클릭합니다.

단계 **3** **Advanced(**고급**)** 탭에서 **TLS 1.3 Decryption(TLS 1.3** 암호 해독**)** 활성화 여부를 선택합니다.

TLS 1.3 암호 해독을 활성화하는 경우, TLS 1.3에 적용해야 하는 각 규칙의 고급 탭에서 TLS 1.3 옵션도 선택해야 합니다. TLS 1.3을 암호 해독하려면 Snort 3을 실행 중이어야 합니다.

단계 **4** **Undecryptable Actions(**암호 해독 불가 작업**)** 탭에서 시스템이 암호 해독을 구현하는 규칙과 일치하는 연결을 처리하는 방법을 수정합니다. 단, 연결을 암호 해독할 수 없는 경우에 해당합니다.

기본값은 이러한 연결에 기본 작업과 동일한 작업을 적용하는 것입니다. 암호 해독 오류는 예외이며, 차단 또는 차단 후 재설정만 선택할 수 있습니다.

새 카테고리에 대한 설명은 암호 해독이 불가능한 트래픽 처리, 4 페이지을(를) 참조하십시오.

단계 **5** **OK(**확인**)**를 클릭합니다.

재서명 암호 해독 규칙을 위한 CA 인증서 다운로드

트래픽을 암호 해독하려는 경우, 사용자는 TLS/SSL을 사용하는 애플리케이션에서 신뢰할 수 있는 루트 인증 기관으로 정의된 암호화 프로세스에 사용되는 내부 CA 인증서를 보유하고 있어야 합니다. 일반적으로 인증서를 생성하거나 인증서를 하나 가져오게 되는 경우, 해당 인증서는 아직 이러한 애플리케이션에서 신뢰할 수 있는 인증서로 정의되어 있지 않습니다. 기본적으로 대부분의 웹 브라우저에서는 사용자가 HTTPS 요청을 전송할 때 클라이언트 애플리케이션에서 웹 사이트의 보안 인증서에 문제가 있음을 알려주는 경고 메시지를 표시합니다. 일반적으로 오류 메시지는 신뢰할 수 있는 인증 기관에서 웹 사이트의 보안 인증서를 발행한 것이 아니거나 알 수 없는 기관에서 웹 사이트를 인증했음을 나타냅니다. 하지만 경고는 MITM(Man-In-The-Middle) 공격이 진행 중일 수 있다는 점을 나타낼 수도 있습니다. 일부 다른 클라이언트 애플리케이션은 사용자에게 이 경고 메시지를 표시하지 않으며 사용자가 인식할 수 없는 인증서를 수락하도록 허용하지도 않습니다.

사용자에게 필수 인증서를 제공하는 데에는 다음과 같은 옵션이 있습니다.

루트 인증서를 수락하도록 사용자에게 알림

조직의 사용자에게 회사의 새로운 정책에 대해 알리고 조직에서 제공하는 루트 인증서를 신뢰할 수 있는 소스로 수락하도록 통지할 수 있습니다. 사용자는 다음에 사이트에 액세스할 때 다시 프롬프트가 나타나지 않도록 인증서를 수락하고 신뢰할 수 있는 루트 인증 기관 보관 영역에 저장해야 합니다.

참고 사용자는 대체 인증서를 생성한 CA 인증서를 수락하고 신뢰해야 합니다. 대신 사용자가 대체 서버 인증서를 신뢰하는 경우, 사용자는 방문하는 서로 다른 각 HTTPS 사이트에 대해 계속 경고를 보게 됩니다.

클라이언트 디바이스에 루트 인증서 추가

신뢰할 수 있는 루트 인증 기관으로 네트워크에 있는 모든 클라이언트 디바이스에 루트 인증서를 추가할 수 있습니다. 이렇게 하면 클라이언트 애플리케이션이 루트 인증서를 포함하는 트랜잭션을 자동으로 수락합니다.

인증서를 이메일 발송하거나 공유 사이트에 배치하는 방식을 통해 사용자가 인증서를 사용할 수 있게 하거나 인증서를 기업 워크스테이션 이미지에 통합하고 애플리케이션 업데이트 시설을 사용하여 사용자에게 자동으로 배포되게 할 수 있습니다.

다음 절차에서는 내부 CA 인증서를 다운로드하고 Windows 클라이언트에 설치하는 방법에 대해 설명합니다.

프로시저

단계 **1** device manager에서 인증서를 다운로드합니다.

a) **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

b) **SSL Decryption Settings(SSL** 암호 해독 설정**)** 버튼(⚙)을 클릭합니다.

c) 다운로드 버튼(⬇)을 클릭합니다.

d) 다운로드 위치를 선택하고 선택적으로 파일 이름(확장자 제외)을 변경한 다음 **Save(**저장**)**를 클릭합니다.

이제 SSL Decryption Settings(SSL 암호 해독 설정) 대화 상자에서 취소 작업을 할 수 있습니다.

단계 **2** 클라이언트 시스템의 웹 브라우저에서 신뢰할 수 있는 루트 인증 기관 보관 영역에 인증서를 설치하거나 클라이언트가 직접 인증서를 설치할 수 있도록 합니다.

프로세스는 운영 체제 및 브라우저의 유형에 따라 달라집니다. 예를 들어, Windows에서 실행 중인 Internet Explorer 및 Chrome에는 다음과 같은 프로세스를 사용할 수 있습니다. Firefox의 경우, **Tools(**도구**)** > **Options(**옵션**)** > **Advanced(**고급**)** 페이지를 통해 설치합니다.

a) 시작 메뉴에서 제어판 > 인터넷 옵션을 선택합니다.

b) 내용 탭을 선택합니다.

c) 인증서 버튼을 클릭하여 인증서 대화 상자를 엽니다.

d) 신뢰할 수 있는 루트 인증 기관 탭을 선택합니다.

e) 가져오기를 클릭하고 마법사를 따라 다운로드한 파일(<uuid>_internalCA.crt)을 찾아 선택한 다음 신뢰할 수 있는 루트 인증 기관 보관 영역에 추가합니다.

f) 마침을 클릭합니다.

성공적으로 가져왔음을 알리는 메시지가 표시됩니다. 잘 알려진 서드파티 인증 기관에서 인증서를 얻는 대신 자체 서명 인증서를 생성한 경우 Windows에서 인증서를 검증할 수 없다는 중간 대화 상자 경고가 표시될 수 있습니다.

이제 인증서 및 인터넷 옵션 대화 상자를 닫으면 됩니다.

예: 네트워크에서 이전 SSL/TLS 버전 차단

일부 조직에서는 정부 규제 또는 회사 정책에 따라 이전 버전의 SSL 또는 TLS를 사용하지 못하도록 해야 합니다. SSL 암호 해독 정책을 사용하여 금지한 SSL/TLS 버전을 사용하는 트래픽을 차단할 수

있습니다. 금지된 트래픽을 즉시 파악할 수 있도록 SSL 암호 해독 정책의 맨 위에 이 규칙을 배치해 보십시오.

다음 예에서는 모든 SSL 3.0 및 TLS 1.0 연결을 차단합니다.

시작하기 전에

이 절차에서는 SSL 암호 해독 정책 활성화, 9 페이지에 설명된 대로 SSL 암호 해독 정책을 이미 활성화한 것으로 가정합니다.

프로시저

단계 **1** **Policies(**정책**)** > **SSL Decryption(SSL** 암호 해독**)**을 선택합니다.

단계 **2** **+** 버튼을 클릭하여 새 규칙을 생성합니다.

단계 **3** Order(순서)에서 **1**을 선택하여 규칙을 정책의 맨 위에 배치하거나 네트워크에 가장 적합한 숫자를 선택합니다.

기본적으로 규칙은 정책의 끝에 추가됩니다.

단계 **4** **Title(**제목**)**에서 규칙의 이름(예: Block_SSL3.0_and_TLS1.0)을 입력합니다.

단계 **5** **Action(**작업**)**에서 **Block(**차단**)**을 선택합니다. 그러면 규칙과 일치하는 모든 트래픽이 즉시 삭제됩니다.

단계 **6** **Source/Destination(**소스/대상**)**, **Applications(**애플리케이션**)**, **URL**, **Users(**사용자**)** 탭의 모든 옵션에 대한 기본값은 그대로 둡니다.

단계 **7** **Advanced(**고급**)** 탭을 클릭한 다음, **Supported Versions(**지원되는 버전**)**에서 SSL3.0 및 TLS1.0을 선택하고 TLS1.1 및 TLS1.2, TLS 1.3은 선택 취소합니다.

단계 **8** (선택 사항) 차단된 연결을 반영하는 대시보드 및 이벤트가 필요한 경우 **Logging(**로깅**)** 탭을 클릭하고 **At End of Connection(**연결 종료 시**)**을 선택합니다. 외부 syslog 서버를 사용 중인 경우, 해당 서버를 선택할 수도 있습니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

이제 정책을 구축할 수 있습니다. 정책이 구축되면 시스템을 통과하는 SSL 3.0 또는 TLS 1.0 연결이 끊어집니다.

참고 SSL 2.0 연결은 정책에 대한 기본 작업에 의해 처리됩니다. 이 연결도 끊어지게 하려면 기본 작업을 Block(차단)으로 변경합니다.

다음에 수행할 작업

이 규칙을 구현하는 경우 권장 사항은 다음과 같습니다.

- 모든 유형의 암호 해독 규칙에 대해 모든 SSL/TLS 옵션이 선택되어 있는 Advanced(고급) 탭의 기본 설정을 그대로 둡니다. 이를 모든 버전에 적용하면 핸드셰이크 프로세스가 간소화됩니다. 그러나 초기 차단 규칙에서는 계속 SSL 3.0 및 TLS 1.0 연결을 방지합니다.

- 일반적으로 정책에 대한 기본 작업으로 Do Not Decrypt(암호 해독 안 함)를 사용하는 것이 좋습니다. 그러나 SSL 2.0 연결은 항상 기본 작업에 의해 처리되므로 Block(차단)을 대신 사용할 수 있습니다. 그러나 모든 해독 가능 트래픽에 대한 기본 작업으로 Do Not Decrypt(암호 해독 안 함)를 적용하려면, 트래픽 일치 기준에 대한 모든 기본값을 허용하는 정책의 끝에서 Do Not Decrypt(암호 해독 안 함) 규칙을 생성합니다. 이 규칙은 지원되는 TLS 연결 중 테이블의 이전 규칙과 일치하지 않는 연결과 일치하며 해당 TLS 버전에 대해 기본값 역할을 합니다.

SSL 암호 해독 모니터링 및 트러블슈팅

다음 주제에서는 SSL 암호 해독 정책을 모니터링하고 트러블슈팅하는 방법을 설명합니다.

SSL 암호 해독 모니터링

대시보드에서 암호 해독에 대한 정보와 로깅을 활성화한 규칙(또는 기본 작업)과 일치하는 트래픽에 대한 이벤트를 확인할 수 있습니다.

SSL 암호 해독 대시보드

전체 암호 해독 통계를 평가하려면 **Monitoring(**모니터링**)** > **SSL Decryption(SSL** 암호 해독**)** 대시보드를 확인합니다. 이 대시보드에는 다음과 같은 정보가 표시됩니다.

- 암호화된 텍스트 트래픽과 일반 텍스트 트래픽의 백분율 비교
- SSL 규칙별로 암호 해독된 암호화된 트래픽의 양

Events(이벤트)

대시보드뿐만 아니라 이벤트 뷰어(**Monitoring(**모니터링**)** > **Events(**이벤트**)**)에도 암호화된 트래픽에 대한 SSL 정보가 포함됩니다. 다음은 이벤트 평가 시 활용할 수 있는 몇 가지 팁입니다.

- 일치하는 트래픽을 차단한 SSL 규칙(또는 기본 작업)과 일치하기 때문에 삭제된 연결의 경우, **Action(**작업**)**은 "차단"이어야 하며 **Reason(**이유**)**은 "SSL 차단"을 나타내야 합니다.
- **SSL Actual Action(SSL** 실제 작업**)** 필드는 시스템이 연결에 적용한 실제 작업을 나타냅니다. 이는 일치하는 규칙에 정의된 작업을 나타내는 **SSL Expected Action(SSL** 예상 작업**)** 과 다를 수 있습니다. 예를 들어 연결이 암호 해독을 적용하는 규칙과 일치할 수 있으나, 어떠한 이유로든 암호 해독되지 않을 수 있습니다.

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리**(SSL** 또는 인증 기관 피닝**)**

스마트폰 및 기타 디바이스용 일부 앱은 SSL(또는 인증 기관) 피닝이라는 기술을 사용합니다. SSL 피닝 기술은 원래 서버 인증서의 해시를 앱 자체에 포함합니다. 따라서 앱이 위협 방어 디바이스에서 재서명된 인증서를 받으면 해시 검증에 실패하고 연결이 중단됩니다.

이때 기본적인 증상은 사용자가 사이트 앱을 사용해서는 웹 사이트에 연결할 수 없지만 웹 브라우저를 사용하면 연결할 수 있다는 것입니다(앱으로 연결에 실패한 디바이스에서 브라우저를 사용할 때도 연결 가능). 사용자가 Facebook iOS 또는 Android 앱은 사용할 수 없지만 Safari나 Chrome에서 https://www.facebook.com을 입력하면 연결할 수 있는 경우를 예로 들 수 있습니다.

SSL 피닝은 특별히 메시지 가로채기(man-in-the-middle) 공격을 차단하는 데 사용되므로 이러한 현상을 해결하는 방법은 없습니다. 다음 옵션 중에서 선택해야 합니다.

- 앱 사용자를 지원합니다. 이 경우 사이트로의 트래픽을 암호 해독할 수 없습니다. SSL Decryption(SSL 암호 해독) 규칙의 Application(애플리케이션) 탭에서 사이트 애플리케이션용 Do Not Decrypt(암호 해독 안 함) 규칙을 생성하고, 이 규칙을 연결에 적용할 Decrypt Re-sign(재서명 암호 해독) 규칙 앞에 배치합니다.
- 사용자들이 브라우저만 사용하도록 강제합니다. 사이트로의 트래픽을 암호 해독해야 하는 경우에는 사용자에게 네트워크를 통해 연결할 때 사이트 앱을 사용할 수 없으며 브라우저만 사용해야 함을 알려야 합니다.

기타 세부정보

특정 사이트가 브라우저에서는 작동하는데 동일 디바이스의 앱에서는 작동하지 않는 경우 SSL 피닝 인스턴스를 살펴봐야 합니다. 하지만 심층적으로 확인하려면 연결 이벤트를 사용해 브라우저 테스트와 더불어 SSL 피닝을 확인할 수 있습니다.

앱은 두 가지 방식으로 해시 검증 장애를 처리할 수 있습니다.

- Facebook 등의 그룹 1 앱은 서버에서 SH, CERT, SHD 메시지를 받는 즉시 SSL ALERT 메시지를 보냅니다. Alert는 보통 SSL 피닝을 나타내는 "Unknown CA (48)(알 수 없는 CA(48))" 알림입니다. 알림 메시지 후에는 TCP Reset(TCP 재설정)이 전송됩니다. 이벤트 세부사항에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN이 포함되어 있습니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 CLIENT_HELLO, SERVER_HELLO, SERVER_CERTIFICATE, SERVER_KEY_EXCHANGE, SERVER_HELLO_DONE입니다.
- Dropbox 등의 그룹 2 앱은 알림을 보내지 않습니다. 대신 핸드셰이크가 완료될 때까지 기다렸다가 TCP Reset(TCP 재설정)을 전송합니다. 이벤트에는 다음 증상이 표시됩니다.
  - SSL Flow Flag(SSL 플로우 플래그)에는 ALERT_SEEN, APP_DATA_C2S 또는 APP_DATA_S2C가 포함되어 있지 않습니다.
  - SSL Flow Message(SSL 플로우 메시지)는 보통 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_FINISHED입니다.

재서명 암호 해독이 브라우저에서는 작동하지만 앱에서는 작동하지 않는 웹 사이트 처리(SSL 또는 인증 기관 피닝)