TLS/SSL 규칙 문제 해결

연결 이벤트를 사용해 네트워크의 애플리케이션이 TLS/SSL 피닝을 사용하고 있는지 여부를 진단할 수 있습니다. 애플리케이션이 TLS/SSL 피닝을 사용 중인 경우, TLS/SSL 규칙 지침 및 제한 사항를 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.

관련 항목

TLS/SSL 피닝 문제 해결, 1 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

- SSL 규칙으로 암호 해독 가능 연결 로깅의 설명에 따라 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

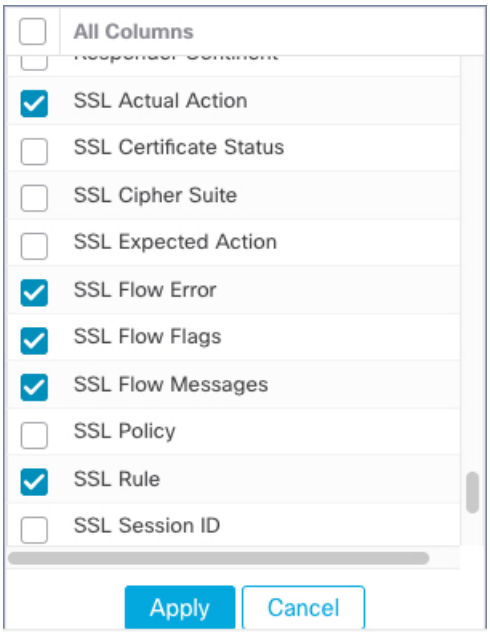
단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

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 연결 및 보안 인텔리전스 이벤트 필드에 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 사항를 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.
  - 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.
  - 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

연결 및 보안 인텔리전스 이벤트 테이블 사용
연결 및 보안 인텔리전스 이벤트 필드
연결 이벤트 필드에서 제공되는 정보
이벤트 검색
알 수 없는 또는 잘못된 인증서 또는 인증 기관 문제 해결, 4 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.
- SSL 규칙으로 암호 해독 가능 연결 로깅의 설명에 따라 TLS/SSL 규칙에 대한 로깅을 활성화합니다.

프로시저

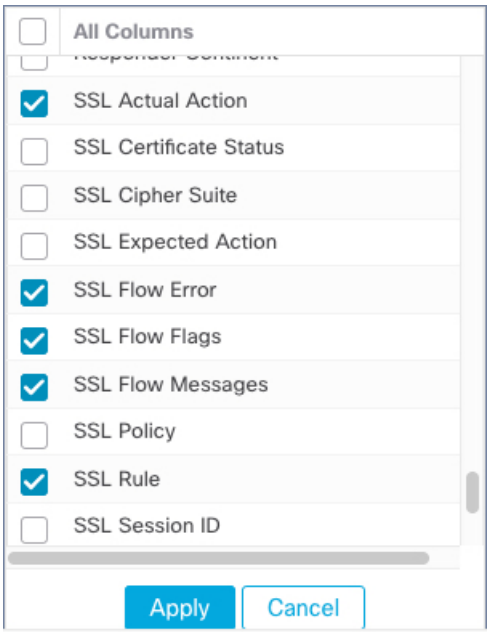
단계 **1** 아직 하지 않았다면 Firepower Management Center에 로그인합니다.

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 연결 및 보안 인텔리전스 이벤트 필드에 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 수신되었지만CA 인증서를 찾을 수 없거나 알려진 신뢰할 수있는 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.