



## 트래픽 해독 이해

다음 주제에서는 TLS/SSL(Transport Layer Security/Secure Sockets Layer) 검사의 개요와 TLS/SSL 검사 구성 사전 조건을 설명하고 구축 시나리오를 자세히 설명합니다.



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

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

SSL 및 TLS 프로토콜에 대한 자세한 내용은 [SSL과 TLS 비교 - 차이점은 무엇입니까?](#)와 같은 리소스를 참조하십시오.

- [트래픽 암호 해독 설명, 1 페이지](#)
- [TLS 암호화 가속, 3 페이지](#)
- [TLS/SSL 모범 사례, 5 페이지](#)
- [TLS/SSL 정책 및 규칙을 구성하는 방법, 16 페이지](#)
- [TLS/SSL 검사 어플라이언스 구축 시나리오, 18 페이지](#)
- [TLS/SSL 기록, 26 페이지](#)

## 트래픽 암호 해독 설명

기본적으로 Firepower System은 SSL(Secure Socket Layer) 또는 그 후속 프로토콜인 TLS(Transport Layer Security) 프로토콜로 암호화된 트래픽을 검사할 수 없습니다. *TLS/SSL* 검사를 통해 검사 없이 암호화 트래픽을 차단하거나 액세스 제어를 사용하여 암호화되거나 해독된 트래픽을 검사할 수 있습니다. 시스템은 암호화된 세션을 처리할 때 트래픽에 대한 상세정보를 로깅합니다. 암호화된 트래픽의 검사 및 암호화된 세션 데이터의 분석을 결합하면 네트워크에서 암호화된 애플리케이션과 트래픽을 더 잘 인식하고 제어할 수 있습니다.

TLS/SSL 검사는 정책 기반 기능입니다. Firepower System에서 액세스 제어 정책은 SSL 정책을 비롯한 하위 정책 및 기타 구성을 호출하는 기본 구성입니다. SSL 정책을 액세스 제어와 연결하면 시스템은 해당 SSL 정책을 사용하여 암호화된 세션을 처리한 후 액세스 제어 규칙을 사용하여 해당 세션을 평가합니다. TLS/SSL 검사를 구성하지 않거나 디바이스에서 지원하지 않는 경우에는 액세스 제어 규칙이 암호화된 모든 트래픽을 처리합니다.

TLS/SSL 검사 구성에서 암호화된 트래픽 통과를 허용하는 경우에도 액세스 제어 규칙이 암호화된 트래픽을 처리합니다. 그러나 일부 액세스 제어 규칙 조건에는 암호화되지 않은 트래픽이 필요하므로 암호화된 트래픽과 일치하는 규칙이 더 적을 수 있습니다. 또한 기본적으로 시스템은 암호화된 페이지로드의 침입 및 파일 검사를 비활성화합니다. 이는 암호화 연결이 침입 및 파일 검사가 구성된 액세스 제어 규칙과 일치하는 경우, 오탐을 줄이고 성능을 높이는 데 도움이 됩니다.

시스템은 TCP 연결을 통해 TLS/SSL 핸드셰이크를 탐지하는 경우, 탐지된 트래픽의 암호 해독 가능 여부를 확인합니다. 확인할 수 없는 경우 구성된 작업을 적용합니다.

- 암호화된 트래픽 차단
- 암호화된 트래픽을 차단하고 TCP 연결 재설정
- 암호화된 트래픽을 해독하지 않음

시스템은 트래픽을 해독할 수 있는 경우, 추가 검사 없이 트래픽을 차단하거나 해독되지 않은 트래픽을 액세스 제어로 평가하거나 다음 방법 중 하나를 사용하여 트래픽을 해독합니다.

- 알려진 개인 키로 해독합니다. 외부 호스트가 네트워크의 서버와 TLS/SSL 핸드셰이크를 시작하면 시스템은 교환된 서버 인증서가 전에 시스템에 업로드된 서버 인증서와 일치하는지 확인합니다. 그런 다음 업로드된 개인 키를 사용하여 트래픽을 해독합니다.
- 서버 인증서를 다시 서명하여 암호를 해독합니다. 네트워크의 호스트가 외부 서버와의 TLS/SSL 핸드셰이크를 시작하면 시스템은 교환된 서버 인증서를 전에 업로드된 CA(Certificate Authority) 인증서로 다시 서명합니다. 그런 다음 업로드된 개인 키를 사용하여 트래픽을 해독합니다.



**참고** Firepower System은 상호 인증을 지원하지 않습니다. 즉, **클라이언트 인증서**를 FMC에 업로드하여 암호 해독-다시 서명 또는 암호 해독-알려진 키 TLS/SSL 규칙 작업에 사용할 수 없습니다. 자세한 내용은 **암호 해독 및 파기(발신 트래픽)**, 8 페이지 및 **알려진 키 암호 해독(수신 트래픽)**, 9 페이지의 내용을 참조하십시오.

암호 해독된 트래픽에는 원래 암호화되지 않은 트래픽과 동일한 트래픽 처리 및 분석, 즉 네트워크, 평판, 사용자 기반 액세스 제어, 침입 탐지 및 방지, Cisco Advanced Malware Protection(Cisco AMP), 검색이 적용됩니다. 시스템은 암호 해독된 트래픽 사후 분석을 차단하지 않는 경우, 대상 호스트로 전달하기 전에 트래픽을 다시 암호화합니다.



**참고** 매니지드 디바이스에서 암호화된 트래픽을 처리하는 경우, 암호 해독 규칙만 설정합니다. 암호 해독 규칙에는 성능에 영향을 미칠 수 있는 처리 오버헤드가 필요합니다.

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 암호화 가속

TLS 암호화 가속 다음 항목의 속도를 높입니다.

- TLS/SSL 암호화 및 복호화
- TLS/SSL 및 IPsec을 포함한 VPN

지원되는 하드웨어

다음 하드웨어 모델은 TLS 암호화 가속을 지원합니다.

- Firepower Threat Defense가 포함된 Firepower 2100
- Firepower Threat Defense가 포함된 Firepower 4100/9300

Firepower 4100/9300 FTD 컨테이너 인스턴스의 TLS 암호화 가속 지원에 대한 자세한 정보는 *FXOS* 환경 설정 가이드를 참조하십시오.

앞서 언급한 가상 어플라이언스 및 하드웨어 외에는 TLS 암호화 가속이 지원되지 않습니다.



**참고** TLS 암호화 가속 및 4100/9300에 대한 자세한 정보는 *FXOS* 환경 설정 사이트를 참조하십시오.

지원되는 기능 **TLS** 암호화 가속

TLS 암호화 가속이 지원하는 기능에는 다음이 포함됩니다.

- IPv4-IPv4 터널링 프로토콜만 지원됩니다. 다른 IP 터널링 프로토콜은 지원되지 않습니다.
- TLS/SSL GRE(Generic Routing Encapsulation) 터널에서 캡슐화된 트래픽 암호 해독

지원되지 않는 기능 **TLS** 암호화 가속

TLS 암호화 가속이 지원하지 않는 기능에는 다음이 포함됩니다.

- 검사 엔진이 연결을 유지하도록 구성되고 검사 엔진이 예기치 않게 실패하는 경우 엔진이 재시작될 때까지 TLS/SSL트래픽이 중단됩니다.

이 동작은 **configure snort preserve-connection {enable | disable}** 명령이 제어합니다.

## TLS 암호화 가속 지침 및 제한 사항

매니지드 디바이스에서 TLS 암호화 가속이 활성화된 경우, 다음에 유의하십시오.

### HTTP 전용 성능

트래픽을 암호 해독하지 않는 매니지드 디바이스에서 TLS 암호화 가속을 사용하면 성능에 영향을 줄 수 있습니다.

### FIPS(Federal Information Processing Standards)

TLS 암호화 가속 및 FIPS(Federal Information Processing Standard)가 모두 활성화되는 경우, 다음 옵션과의 연결은 실패합니다.

- 크기가 2,048 바이트보다 작은 RSA 키
- RC4(Rivest Cipher 4)
- 단일 데이터 암호화 표준(단일 DES)
- MD5(Merkle-Damgard 5)
- SSL v3

보안 인증 컴플라이언스 모드에서 작동하도록 Firepower Management Center 및 매니지드 디바이스를 구성하는 경우 FIPS가 활성화됩니다. 해당 모드에서 작동 중 연결을 허용하려면 웹 브라우저를 구성하여 더 안전한 옵션을 선택합니다.

자세한 내용:

- FIPS에서 지원되는 암호: [SSL 설정 정보](#)
- [보안 인증 컴플라이언스 모드](#).
- [공통 평가 기준](#)

### TLS 하트비트

일부 애플리케이션은 TLS 하트비트를 TLS(Transport Layer Security) 및 DTLS(Datagram Transport Layer Security) 프로토콜로 확장합니다. 이 프로토콜은 [RFC6520](#)에서 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.

자세한 내용은 [암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션](#)를 참고하십시오.

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

### TLS/SSL 초과 서브스크립션

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

TLS 암호화 가속이 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 **Handshake 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.

초과 서브스크립션이 많이 발생하는 경우, 다음 방법을 사용합니다.

- 매니지드 디바이스를 업그레이드하여 TLS/SSL 처리 용량을 늘립니다.
- SSL 정책을 변경하여 암호 해독 우선 순위가 높지 않은 트래픽의 **Do Not Decrypt**(암호 해독 안 함) 규칙을 추가합니다.

## TLS 암호화 가속 상태 보기

이 주제에서는 TLS 암호화 가속 활성화 여부를 확인하는 방법을 설명합니다.

Firepower Management Center에서 다음 작업을 수행합니다.

프로시저

단계 1 Firepower Management Center에 로그인합니다.

단계 2 **Devices**(디바이스) > **Device Management**(디바이스 관리)를 클릭합니다.

단계 3 수정(✎)을 클릭하여 매니지드 디바이스를 편집합니다.

단계 4 **Device**(디바이스) 페이지를 클릭합니다. TLS 암호화 가속 상태가 **General**(일반) 섹션에 표시됩니다.

## TLS/SSL 모범 사례

이 섹션에서는 암호 해독 정책 및 규칙을 생성할 때 고려해야 하는 정보를 설명합니다.



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

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

SSL 및 TLS 프로토콜에 대한 자세한 내용은 [SSL과 TLS 비교 - 차이점은 무엇입니까?](#)와 같은 리소스를 참조하십시오.

#### 관련 항목

[암호 해독 사례, 6 페이지](#)

[트래픽을 암호 해독해야 하는 경우와 하면 안 되는 경우, 7 페이지](#)

[기타 TLS/SSL 규칙 작업, 9 페이지](#)

[TLS/SSL 규칙 구성 요소, 12 페이지](#)

[TLS/SSL 규칙 순서 평가, 13 페이지](#)

## 암호 해독 사례

해독된 트래픽만 Firepower 시스템의 위협 방어 및 정책 시행 기능을 사용할 수 있습니다. Firepower 시스템을 통과할 때 암호화되는 트래픽은 허용하거나 차단할 수 있지만, 심층 검사 또는 (침입 방지를 포함한) 전체 정책 시행의 대상이 되지 않습니다.

모든 암호화된 연결은 다음과 같습니다.

- TLS/SSL 암호 해독 정책을 통해 전송하여 암호 해독 또는 차단 여부를 결정합니다.

비보안 SSL 프로토콜을 사용하는 트래픽이나 만료 또는 유효하지 않은 인증서가 있는 트래픽 같은, 네트워크에서 허용하고 싶지 않은 유형의 암호화된 트래픽을 차단하도록 TLS/SSL 암호화 규칙을 구성할 수 있습니다.

- 암호 해독 여부와 관계없이 차단 해제된 연결은 모두 액세스 제어 정책을 통해 최종 허용 또는 차단 여부가 결정됩니다.

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

#### 요약:

- 암호화된 트래픽은 정책을 이용해 허용 또는 차단할 수 있습니다. 암호화된 트래픽은 검사할 수 없습니다.
- 암호 해독한 트래픽은 위협 방어 및 정책 시행의 영향을 받습니다. 암호 해독된 트래픽은 정책을 이용해 허용하거나 차단할 수 있습니다.

관련 항목

[파일 및 침입 정책을 사용한 심층 검사](#)

## 트래픽을 암호 해독해야 하는 경우와 하면 안 되는 경우

이 섹션에서는 트래픽을 암호 해독해야 하는 경우와, 암호화된 방화벽을 통과하도록 허용해야 하는 경우에 대한 지침을 제공합니다.

트래픽을 암호 해독하면 안 되는 경우

다음에 의해 금지되는 경우 트래픽을 해독해서는 안 됩니다.

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

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

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

*SSL* 정책은 이 트래픽에 대한 암호 해독 금지 작업을 제공하지 않습니다. 자세한 내용은 [TLS/SSL 규칙 Do Not Decrypt\(암호 해독 안 함\) 작업](#)의 내용을 참조하십시오.



참고

이 항목의 끝에 있는 관련 정보 링크를 이용하면 규칙 평가의 다양한 측면에 대한 설명을 확인할 수 있습니다. URL 및 애플리케이션 필터링 같은 조건에는 암호화된 트래픽 관련 제한이 적용됩니다. 이러한 제한을 이해하고 있어야 합니다.

트래픽을 암호 해독해야 하는 경우

암호화된 트래픽은 암호를 해독해야 *Firepower* 시스템의 위협 보호 및 정책 시행 기능을 사용할 수 있습니다. 매니지드 디바이스가 (메모리와 처리 능력에 따라) 트래픽 암호 해독을 허용한다면, 법률이

나 관련 규정의 보호를 받지 않는 트래픽은 암호 해독해야 합니다. 암호 해독할 트래픽을 결정해야 한다면, 네트워크에서 트래픽을 허용하는 데 따르는 위험을 바탕으로 결정을 내리십시오. Firepower 시스템은 URL 평판, 암호 그룹, 프로토콜 및 기타 다양한 요소를 포함하는 규칙 조건을 사용하여 트래픽을 분류하는 유연한 프레임워크를 제공합니다.

Firepower 시스템은 다음 섹션에서 설명하는 두 가지 암호 해독 방법을 제공합니다.

#### 관련 항목

- [암호 해독 및 파기\(발신 트래픽\), 8 페이지](#)
- [알려진 키 암호 해독\(수신 트래픽\), 9 페이지](#)
- [TLS/SSL 규칙 지침 및 제한 사항](#)
- [SSL 규칙 순서](#)
- [URL 조건\(URL 필터링\)](#)
- [애플리케이션 규칙 순서](#)

## 암호 해독 및 파기(발신 트래픽)

**Decrypt - Resign**(암호 해독 - 파기) TLS/SSL 규칙 작업은 Firepower 시스템이 중간자 역할을 해 차단, 암호 해독, (트래픽이 허용하는 경우) 검사, 재암호화를 수행하게 합니다. **Decrypt - Resign**(암호 해독 - 파기) 규칙 작업은 발신 트래픽과 함께 사용됩니다. 즉 대상 서버가 보호되는 네트워크 외부에 있습니다.

FTD 디바이스는 규칙에 지정된 내부 CA(Certificate Authority) 개체를 이용해 클라이언트와 협상하며, 클라이언트와 FTD 디바이스 간의 SSL 터널을 구축합니다. 동시에 이 디바이스는 대상 웹 사이트에 접속하여 서버와 FTD 디바이스 간에 SSL 터널을 생성합니다.

따라서 클라이언트는 대상 서버에서 인증서 대신 SSL 암호 해독 규칙에 대해 구성된 CA 인증서를 보게 됩니다. 연결을 완료하려면 클라이언트가 인증서를 신뢰해야 합니다. 그러면 FTD 디바이스에서는 클라이언트와 대상 서버 간의 양방향 트래픽에서 암호 해독/재암호화를 수행합니다.

#### 사전 요구 사항

**Decrypt - Resign**(암호 해독 - 파기) 규칙 작업을 사용하려면 CA 파일 및 페어링된 개인 키 파일을 이용해 내부 CA 개체를 만들어야 합니다. CA 및 개인 키가 없다면 Firepower System에서 생성하면 됩니다.



**참고** Firepower System은 상호 인증을 지원하지 않습니다. 즉, [클라이언트 인증서](#)를 FMC에 업로드하여 암호 해독-다시 서명 또는 암호 해독-알려진 키 TLS/SSL 규칙 작업에 사용할 수 없습니다. 자세한 내용은 [암호 해독 및 파기\(발신 트래픽\), 8 페이지](#) 및 [알려진 키 암호 해독\(수신 트래픽\), 9 페이지](#)의 내용을 참조하십시오.

#### 관련 항목

- [TLS/SSL 규칙 암호 해독 작업](#)
- [외부 인증서 개체](#)



## 알려진 키 암호 해독(수신 트래픽)

**Decrypt - Known Key**(암호 해독 - 알려진 키) TLS/SSL 규칙 작업은 서버의 개인 키를 사용하여 트래픽을 해독합니다. **Decrypt - Known Key**(암호 해독 - 알려진 키) 규칙 작업은 수신 트래픽과 함께 사용됩니다. 즉 대상 서버가 보호되는 네트워크 내부에 있습니다.

알려진 키로 암호 해독을 수행하는 주요 목적은 외부 공격으로부터 서버를 보호하는 것입니다.

사전 요구 사항

**Decrypt - Known Key**(암호 해독 - 알려진 키) 규칙 작업을 사용하려면 서버의 인증서 파일 및 페어링된 개인 키 파일을 이용해 내부 인증서 개체를 만들어야 합니다.



**참고** Firepower System은 상호 인증을 지원하지 않습니다. 즉, **클라이언트 인증서**를 FMC에 업로드하여 암호 해독-다시 서명 또는 암호 해독-알려진 키 TLS/SSL 규칙 작업에 사용할 수 없습니다. 자세한 내용은 **암호 해독 및 과기(발신 트래픽)**, 8 페이지 및 **알려진 키 암호 해독(수신 트래픽)**, 9 페이지의 내용을 참조하십시오.

관련 항목

[TLS/SSL 규칙 암호 해독 작업](#)

[내부 인증서 개체](#)

## 기타 TLS/SSL 규칙 작업

다음 섹션에서는 다른 TLS/SSL 규칙 작업에 대해 설명합니다.

관련 항목

[TLS/SSL 규칙 차단 작업](#)

[TLS/SSL 규칙 모니터링 작업](#)

## TLS 1.3 서버 ID 검색

**RFC 8446**에서 정의한 TLS(Transport Layer Security) 프로토콜 1.3의 최신 버전은 보안 통신을 제공하기 위해 많은 웹 서버에서 선호하는 프로토콜입니다. TLS 1.3 프로토콜은 추가 보안을 위해 서버의 인증서를 암호화하며, 액세스 제어 규칙의 애플리케이션 및 URL 필터링 기준과 일치하는 데 인증서가 필요하므로 Firepower System은 전체 패킷의 암호를 해독하지 않고 서버 인증서를 추출하는 방법을 제공합니다.

다음과 같은 경우, **TLS 서버 ID** 검색이라고 하는 기능을 활성화할 수 있습니다.

- SSL 정책을 액세스 제어 정책과 연결
- 액세스 제어 정책에 대한 고급 설정 설정

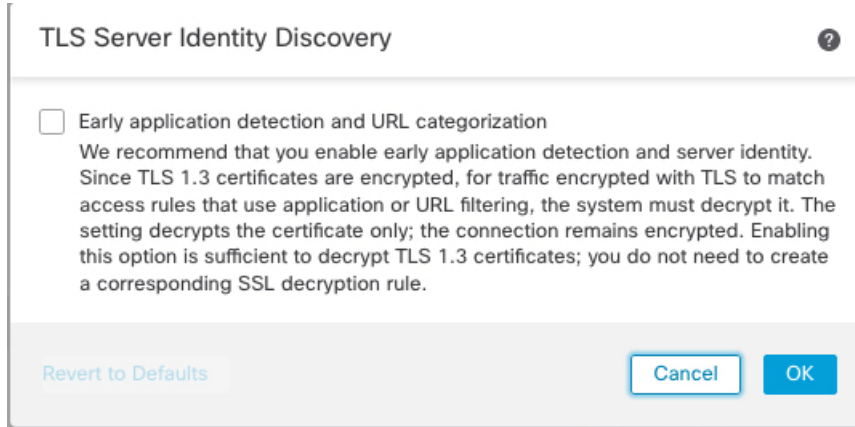
애플리케이션 또는 URL 기준에서 일치시키려는 트래픽에 대해 특히 트래픽을 심층 검사하려는 경우, 이를 활성화하는 것이 좋습니다. 서버 인증서를 추출하는 과정에서 트래픽이 암호 해독되지 않으므로 SSL 정책이 필요하지 않습니다.



참고

- TLS 서버 ID 검색은 하드웨어 플랫폼에 따라 성능을 저하시킬 수 있습니다.
- TLS 서버 ID 검색은 인라인 탭 모드 또는 패시브 모드 구축에서 지원되지 않습니다.

다음 그림에는 액세스 제어 정책의 고급 설정에서 TLS 서버 ID 검색을 활성화하는 예가 나와 있습니다.



관련 항목

- [기본 SSL 정책 생성](#)
- [액세스 제어에 다른 정책 연결](#)

## TLS/SSL 규칙 예시

다음 섹션에서는 권장되는 TLS/SSL 규칙을 설정하는 예시를 제공합니다.

관련 항목

- [비보안 프로토콜 차단](#), 10 페이지

### 비보안 프로토콜 차단

이 예에서는 TLS 1.0, TLS 1.1 및 SSLv3 같은, 더 이상 안전하지 않은 것으로 간주되는 TLS 및 SSL 프로토콜을 네트워크에서 차단하는 방법을 보여줍니다.

모든 비보안 프로토콜은 악용 가능하기 때문에 네트워크에서 제외해야 합니다. 이 예에서는 다음을 수행합니다.

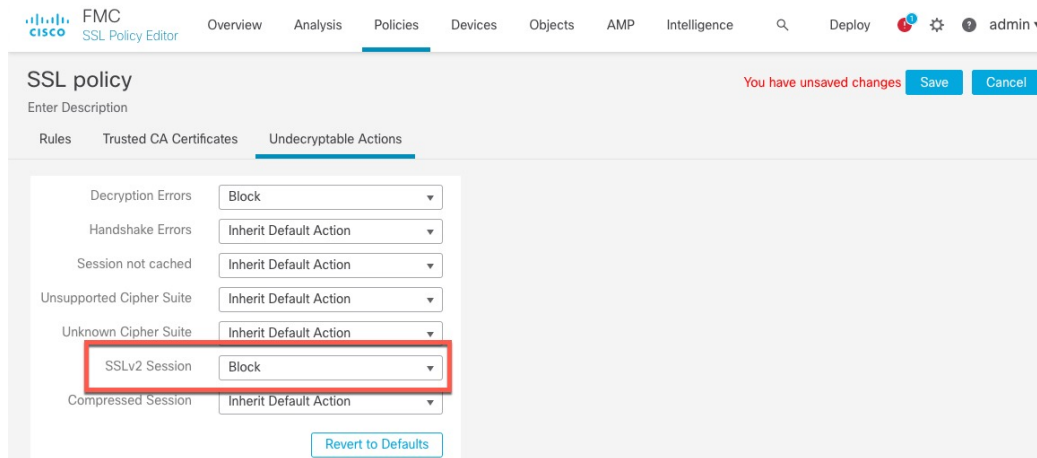
- SSL 규칙의 **Version(버전)** 페이지를 사용하여 일부 프로토콜을 차단할 수 있습니다.
- Firepower 시스템은 SSLv2르 해독 불가로 간주하기 때문에, SSL 정책에 대한 **Undecryptable Actions(해독 불가 작업)**을 사용하여 차단할 수 있습니다.

## 프로시저

- 단계 1 아직 하지 않았다면 Firepower Management System에 로그인합니다.
- 단계 2 **Policies(정책) > Access Control(액세스 제어) > SSL**을 클릭합니다.
- 단계 3 SSL 정책을 추가하거나 수정합니다.
- 단계 4 **Add Rule(규칙 추가)**을 클릭합니다.
- 단계 5 **Name(이름)** 필드에 규칙의 이름을 입력합니다.
- 단계 6 **Action(작업)** 목록에서 **Block(차단)** 또는 **Block with reset(차단 후 재설정)**을 클릭합니다.
- 단계 7 **Version(버전)** 페이지를 클릭합니다.
- 단계 8 **SSL v3.0, TLS 1.0, TLS 1.1** 같은 더 이상 안전하지 않은 프로토콜의 확인란을 선택합니다. 안전한 것으로 간주되는 프로토콜의 확인란은 선택 취소합니다.

다음 그림은 예를 보여줍니다.

- 단계 9 필요에 따라 다른 규칙 조건을 선택합니다.
- 단계 10 규칙을 저장합니다.
- 단계 11 SSL 정책 페이지에서 **Undecryptable Actions(암호 해독할 수 없는 작업)**를 클릭합니다.
- 단계 12 **SSLv2 Session(SSLv2 세션)** 목록에서 **Block(차단)** 또는 **Block with reset(차단 후 재설정)**을 클릭합니다. 다음 그림은 예를 보여줍니다.



단계 13 **Save**(저장)를 클릭합니다.

단계 14 이 규칙은 구체적인 규칙이므로, 정책에서 애플리케이션 매칭 규칙 같은 일반 규칙보다 순위가 높아야 합니다.

다음에 수행할 작업

- 구성 변경사항을 구축합니다. [컨피그레이션 변경 사항 구축](#)의 내용을 참조하십시오.

관련 항목

[TLS/SSL 규칙 조건](#)

## TLS/SSL 규칙 구성 요소

각 TLS/SSL 규칙에는 다음과 같은 구성 요소가 있습니다.

상태

기본적으로 규칙이 활성화됩니다. 규칙을 비활성화하는 경우 시스템에서 규칙을 사용하여 네트워크 트래픽을 평가하지 않고, 해당 규칙에 대한 경고 및 오류 생성을 중지합니다.

위치

SSL 정책의 규칙은 1부터 시작하여 번호가 지정됩니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 규칙과 일치하는지를 확인합니다. 모니터링 규칙을 제외하면, 트래픽에 일치하는 첫 번째 규칙이 트래픽을 처리하는 규칙입니다.

조건

조건은 규칙이 처리하는 특정 트래픽을 지정합니다. 조건은 보안 영역, 네트워크 또는 지리위치, VLAN, 포트, 애플리케이션, 요청된 URL, 사용자, 인증서, 인증서 주체 또는 발급자, 인증서 상태, 암

호 그룹 또는 암호화 프로토콜 버전별로 트래픽 일치 여부를 확인할 수 있습니다. 조건의 사용은 대상 디바이스 라이선스에 따라 달라질 수 있습니다.

#### 작업

규칙의 작업은 시스템이 일치하는 트래픽을 처리하는 방법을 결정합니다. 일치하는 암호화 트래픽을 모니터링, 허용, 차단 또는 암호 해독할 수 있습니다. 해독되고 허용된 암호화 트래픽은 추가 검사 대상입니다. 시스템은 차단된 암호화 트래픽에 대해 검사를 수행하지 않습니다.

#### 로깅

규칙의 로깅 설정은, 처리하는 트래픽에 대해 시스템에서 유지하는 레코드를 관리합니다. 규칙과 매칭하는 트래픽을 기록할 수 있습니다. SSL 정책의 설정에 따라 시스템이 암호화 세션을 차단하거나 암호 해독 없이 전달되도록 허용할 때 연결을 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. Firepower Management Center 데이터베이스는 물론 시스템 로그(syslog)나 SNMP 트랩 서버에도 연결을 로깅할 수 있습니다.

로깅에 대한 자세한 내용은 [연결 로깅 모범 사례](#)를 참조하십시오.



**팁** TLS/SSL 규칙을 올바르게 생성하고 순서를 지정하는 것은 복잡한 작업입니다. 정책을 신중하게 계획하지 않으면 규칙이 다른 규칙을 선점하거나, 추가 라이선스를 요구하거나, 잘못된 구성을 포함할 수 있습니다. 시스템이 트래픽을 예상대로 처리할 수 있도록 SSL 정책 인터페이스는 규칙에 대한 강력한 경고 및 오류 피드백 시스템을 갖추고 있습니다.

#### 관련 항목

- [보안 영역 조건](#)
- [네트워크 조건](#)
- [VLAN 조건](#)
- [포트 및 ICMP 코드 조건](#)
- [애플리케이션 조건\(애플리케이션 컨트롤\)](#)
- [URL 조건\(URL 필터링\)](#)
- [사용자, 영역 및 ISE 속성 조건\(사용자 제어\)](#)
- [액세스 제어 규칙 순서에 대한 모범 사례](#)

## 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 규칙

에 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 문서](#)를 참조하십시오.



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

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

관련 항목

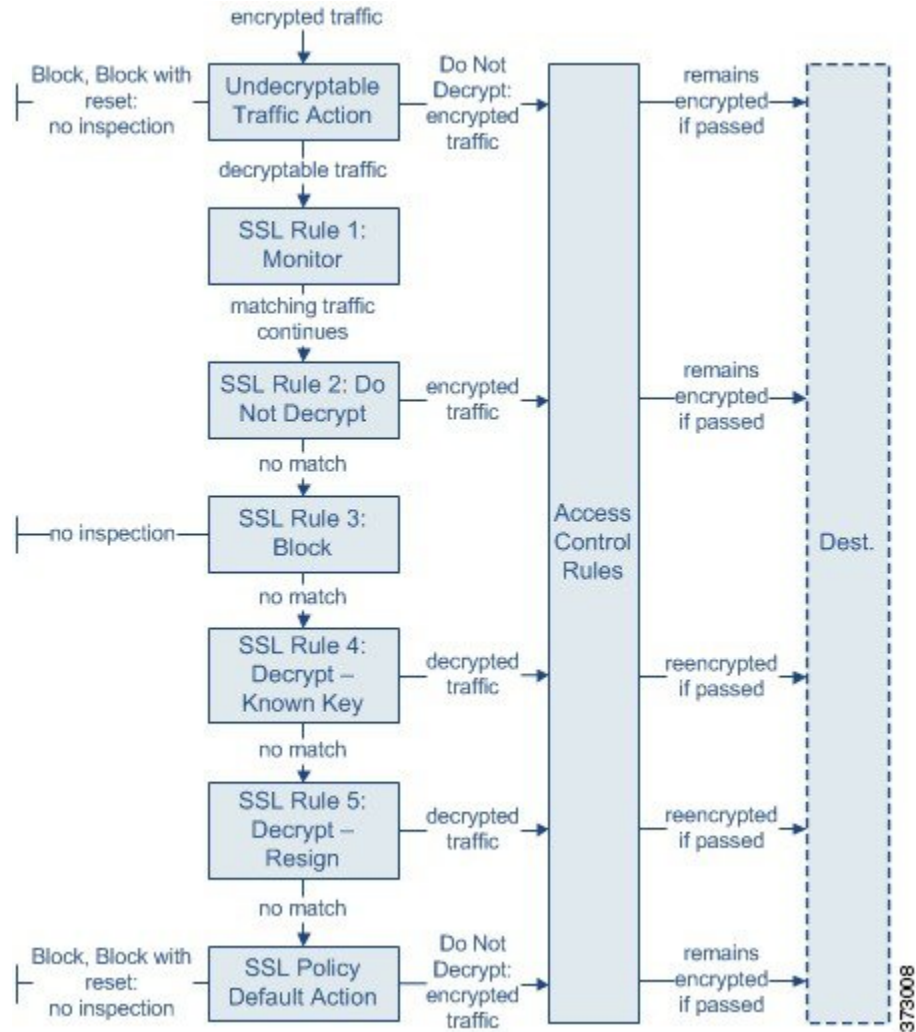
[암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션](#)

[SSL 규칙 순서](#)

[액세스 제어 규칙 순서에 대한 모범 사례](#)

## 다중 규칙 예시

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



이 시나리오에서, 트래픽은 다음과 같이 평가됩니다.

- **Undecryptable Traffic Action**은 암호화 트래픽을 먼저 평가합니다. 시스템에서 해독할 수 없는 트래픽은 추가 검사 없이 차단하거나 액세스 제어 검사를 위해 전달합니다. 매칭하지 않는 암호화 트래픽은 다음 규칙으로 진행합니다.
- **TLS/SSL 규칙 1: Monitor**(모니터링)가 다음으로 암호화 트래픽을 평가합니다. Monitor(모니터링) 규칙은 암호화 트래픽을 추적하고 로깅하지만 트래픽 플로우에 영향을 주지 않습니다. 시스템은 허용할지 아니면 거부할지 여부를 결정하기 위해 계속해서 트래픽을 추가 규칙에 일치시킵니다.
- **TLS/SSL 규칙 2: Do Not Decrypt**(암호 해독 안 함)가 세 번째로 암호화 트래픽을 평가합니다. 일치하는 트래픽은 암호 해독되지 않습니다. 시스템은 이 트래픽을 액세스 제어로 검사하지만 파일 또는 침입 검사는 하지 않습니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.
- **TLS/SSL 규칙 3: Block**(차단)에서 네 번째로 암호화 트래픽을 평가합니다. 일치하는 트래픽은 추가 검사 없이 차단됩니다. 일치하지 않는 트래픽은 다음 규칙으로 계속 진행됩니다.

- **TLS/SSL 규칙 4: Decrypt - Known Key**(암호 해독 - 알려진 키)에서 다섯 번째로 암호화 트래픽을 평가합니다. 네트워크에 수신된 매칭 트래픽은 업로드된 개인 키를 사용하여 해독됩니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사 결과에 따라 시스템이 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **TLS/SSL 규칙 5: Decrypt - Resign**(암호 해독 - 다시 서명)이 최종 규칙입니다. 트래픽이 이 규칙과 일치하면 시스템은 업로드된 CA 인증서로 서버 인증서를 다시 서명한 다음 중간자(man-in-the-middle) 역할을 하여 트래픽 암호를 해독합니다. 그런 다음 해독된 트래픽은 액세스 제어 규칙에 따라 평가됩니다. 액세스 제어 규칙은 해독된 트래픽과 암호화되지 않은 트래픽을 동일하게 처리합니다. 이 추가 검사 결과에 따라 시스템이 트래픽을 차단할 수 있습니다. 나머지 모든 트래픽은 다시 암호화된 후에 목적지로 갈 수 있습니다. 이 SSL 규칙과 매칭하지 않는 트래픽은 다음 규칙으로 진행합니다.
- **SSL Policy Default Action**(SSL 정책 기본 작업)은 어떤 TLS/SSL 규칙과도 일치하지 않는 모든 트래픽을 처리합니다. 이 기본 작업은 암호화 트래픽을 추가 검사 없이 차단하거나 해독하지 않고 액세스 제어 검사를 위해 전달합니다.

## TLS/SSL 정책 및 규칙을 구성하는 방법

이 항목에서는 네트워크에서 TLS/SSL 트래픽을 차단, 모니터링 또는 허용하는 정책의 SSL 정책 및 TLS/SSL 규칙을 구성하려면 완료해야 하는 작업에 대한 개요를 제공합니다.

이 작업을 수행하려면 관리자, 액세스 관리자 또는 Network Admin(네트워크 관리자)여야 합니다. NGIPSv을(를) 제외한 모든 디바이스 유형에서 SSL 정책을 구성할 수 있습니다.

### 프로시저

|      | 명령 또는 동작                   | 목적   |
|------|----------------------------|--|
| 단계 1 | SSL 정책을 생성합니다.             | SSL 정책은 하나 이상의 규칙에 대한 컨테이너입니다. 액세스 제어를 위해 SSL 정책 및 해당 규칙을 사용하려면, 나중에 SSL 정책을 액세스 제어 정책과 연결해야 합니다. 자세한 내용은 <a href="#">기본 SSL 정책 생성</a> 의 내용을 참조하십시오. |
| 단계 2 | SSL 정책에 대한 기본 작업을 설정합니다.   | 기본 작업은 트래픽이 SSL 정책에 정의된 어떤 규칙과도 일치하지 않을 때 수행됩니다. <a href="#">SSL 정책 기본 작업</a> 의 내용을 참조하십시오.  |
| 단계 3 | 해독 불가 트래픽을 처리하는 방법을 지정합니다. | 비보안 프로토콜, 사용 및 알 수 없는 암호 그룹을 비롯한 여러 이유 때문에, 혹은 핸드셰이크 또는 암호 해독 관련 오류 때문에 트래픽의 암호를 해독하지 못할 수도 있습니다. <a href="#">암호 해</a>                               |



|      | 명령 또는 동작  | 목적   |
|------|---|--|
|      |   | 독을 할 수 없는 트래픽에 대한 기본 처리 옵션의 내용을 참조하십시오.  |
| 단계 4 | <b>Decrypt - Known Key</b> (암호 해독 - 알려진 키)(네트워크의 서버에 들어오는 트래픽을 암호 해독하는 용도) TLS/SSL 규칙의 경우에는 내부 인증서 개체를 생성합니다.     | 내부 인증서 개체는 사용자 서버의 인증서와 개인 키를 사용합니다. 내부 인증서 개체의 내용을 참조하십시오.  |
| 단계 5 | <b>Decrypt - Resign</b> (암호 해독 - 파기)(네트워크 외부에 있는 서버로 가는 트래픽을 암호 해독하는 용도) TLS/SSL 규칙의 경우에는 내부 인증 기관(CA) 개체를 생성합니다. | 내부 CA 개체는 CA 및 개인 키를 사용합니다. 내부 인증 기관 개체의 내용을 참조하십시오.   |
| 단계 6 | TLS/SSL 규칙을 생성합니다.  | <ul style="list-style-type: none"> <li>차단, 차단 후 재설정, 인터랙티브 차단: TLS/SSL 규칙 동작 구성의 내용을 참조하십시오.</li> <li>암호 해독 안 함: TLS/SSL 규칙 동작 구성의 내용을 참조하십시오.</li> <li><b>Decrypt - Resign</b>(암호 해독 - 파기): 암호 해독 설정 - 재서명 작업의 내용을 참조하십시오.</li> <li><b>Decrypt - Known Key</b>(암호 해독 - 알려진 키): 암호 해독 설정 - 알려진 키 작업의 내용을 참조하십시오.</li> <li><b>Monitor</b>(모니터링): TLS/SSL 규칙 동작 구성의 내용을 참조하십시오.</li> </ul> |
| 단계 7 | SSL 정책을 액세스 제어 정책에 연결합니다.   | SSL 정책을 액세스 제어 정책과 연결하지 않으면 아무런 효과도 발생하지 않습니다. 이 작업을 수행한 후에는 액세스 제어 규칙과 일치하는 트래픽을 허용 하거나 차단하고, 다른 작업을 수행할 수 있습니다. 액세스 제어에 다른 정책 연결의 내용을 참조하십시오.  |
| 단계 8 | 암호 해독된 트래픽을 허용 또는 차단하도록 액세스 제어 규칙을 구성합니다.   | 액세스 제어 정책 구성 요소의 내용을 참조하십시오.   |
| 단계 9 | 액세스 제어 정책을 매니지드 디바이스에 구축합니다.  | 효과를 발휘하려면 정책은 매니지드 디바이스에 구축해야 합니다. 키퍼그레이션 변경 사항 구축의 내용을 참조하십시오.  |

## TLS/SSL 검사 어플라이언스 구축 시나리오

이 섹션에서는 Life Insurance Example, Inc. 생명보험사(LifeIns)가 프로세스 감사를 위해 암호화된 트래픽에서 SSL 검사를 사용하는 몇 가지 시나리오를 보여줍니다. LifeIns는 비즈니스 프로세스를 기반으로 다음을 구축할 계획입니다.

- Underwriting 부서를 위한 인라인 구축의 FTD 디바이스 하나
- 두 디바이스를 관리하기 위한 Firepower Management Center 하나

### Customer Service 비즈니스 프로세스

LifeIns는 고객을 위해 고객 대면 웹사이트를 생성했습니다. LifeIns는 웹사이트와 이메일을 통해 잠재 고객으로부터 보험 증권에 대한 암호화된 질문과 요청을 수신합니다. LifeIns의 Customer Service 부서는 24시간 내에 이를 처리하고 필요한 정보를 제공합니다. Customer Service는 수신 연락처 메트릭 수집을 확장하고자 합니다. LifeIns에는 Customer Service에 대해 설정된 내부 감사 검토가 있습니다.

LifeIns는 또한 온라인으로 암호화된 신청서를 수신합니다. Customer Service 부서는 사례 파일을 Underwriting 부서로 전송하기 전 24시간 내에 신청서를 처리합니다. Customer Service는 온라인 양식으로 전송된, 명백하게 잘못된 신청서를 필터링하며, 이 과정에 상당한 시간이 소요됩니다.

### Underwriting 비즈니스 프로세스

LifeIns의 보험업자는 암호화된 의료 정보 요청을 Medical Repository Example, LLC 의료 데이터 저장소(MedRepo)에 온라인으로 제출합니다. MedRepo는 요청을 검토하고, 72시간 내에 암호화된 레코드를 LifeIns로 전송합니다. 그 후 보험업자는 신청서에 서명하고 보험 증권 및 요금 결정 사항을 제출합니다. Underwriting은 메트릭 수집을 확장하고자 합니다.

최근에 알 수 없는 소스에서 LifeIns에 스푸핑된 응답을 전송했습니다. LifeIns의 보험업자는 올바른 인터넷 사용에 대한 교육을 받았지만, LifeIns의 IT 부서는 의료 응답 양식을 전송하는 모든 암호화된 트래픽을 분석하고 모든 스푸핑 시도를 차단하고자 합니다.

LifeIns는 6개월 교육 기간을 거쳐 하급 보험업자를 배치합니다. 최근에 이러한 보험업자가 암호화된 의료 규제 요청을 MedRepo의 고객 서비스 부서에 잘못 제출했습니다. MedRepo는 응답 과정에서 여러 불만 사항을 LifeIns에 제출했습니다. LifeIns는 신입 보험업자 교육 기간을 연장하고 MedRepo에 제출하는 보험업자 요청에 대해 감사를 수행할 계획입니다.

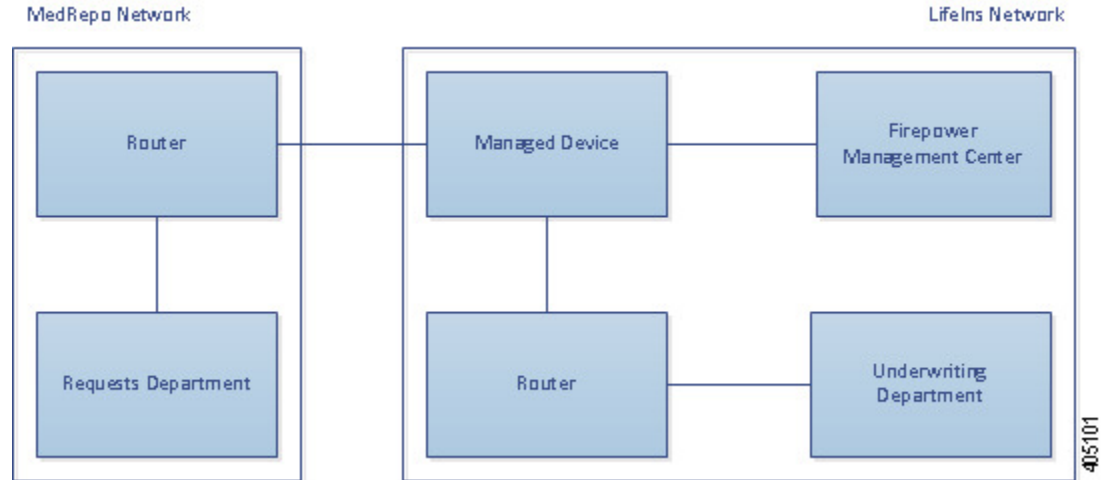
## 인라인 구축의 트래픽 암호 해독

LifeIns의 비즈니스 요구 사항에서는 Underwriting에서 다음을 수행하도록 규정합니다.

- 신입 및 하급 보험업자를 감사하여, MedRepo에 대한 정보 요청이 모든 해당 규정을 준수하는지 확인합니다.
- 보험 가입 메트릭 수집 프로세스 개선
- MedRepo에서 온 것처럼 보이는 모든 요청을 검토하고 모든 스푸핑 시도 삭제

- Underwriting 부서에서 MedRepo의 Customer Service 부서로 이동하는 모든 부적절한 규제 요청 삭제
- 상급 보험업자는 감사하지 않음

LifeIns는 Underwriting 부서를 위한 인라인 구축에 디바이스를 구축할 계획입니다.



MedRepo의 네트워크에서 오는 트래픽은 MedRepo의 라우터로 이동합니다. 트래픽이 LifeIns의 네트워크로 라우팅됩니다. 매니지드 디바이스는 트래픽을 수신하고, 허용되는 트래픽을 LifeIns의 라우터에 전달하고, 이벤트를 관리 Firepower Management Center로 전송합니다. LifeIns의 라우터는 트래픽을 목적지 호스트로 라우팅합니다.

관리 Firepower Management Center에서 Access Control 및 SSL Editor 맞춤형 역할을 보유한 사용자는 다음을 수행하도록 SSL 액세스 제어를 구성합니다.

- Underwriting 부서로 전송되는 모든 암호화된 트래픽 로깅
- LifeIns의 Underwriting 부서에서 MedRepo의 Customer Service 부서로 잘못 전송된 모든 암호화된 트래픽 차단
- MedRepo에서 LifeIns의 Underwriting 부서, 그리고 LifeIns의 하급 보험업자가 MedRepo의 Requests 부서로 전송한 모든 암호화된 트래픽 해독
- 상급 보험업자가 전송한 암호화된 트래픽은 해독하지 않음

또한 사용자는 해독된 트래픽을 맞춤형 침입 정책으로 검사하도록 액세스 제어를 구성하고 다음을 수행할 수 있습니다.

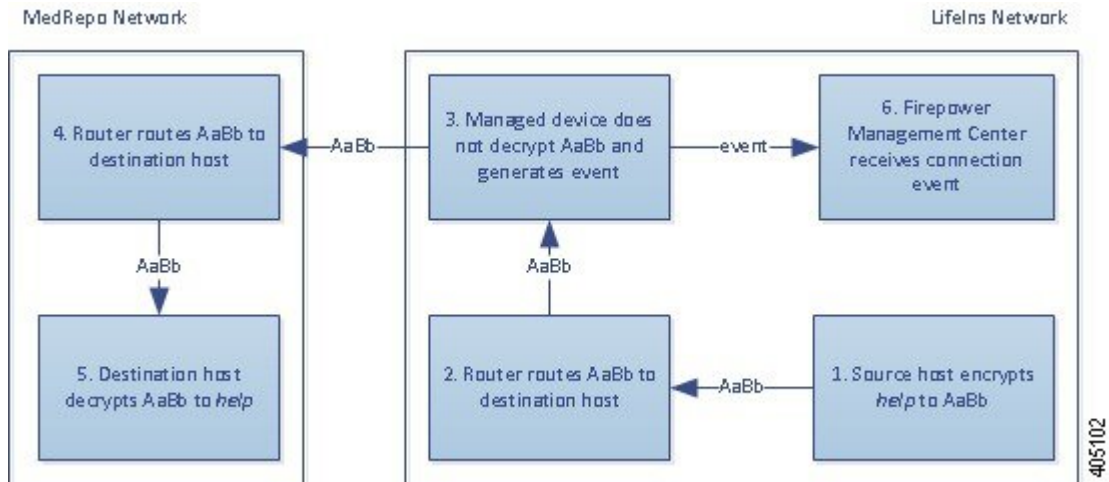
- 스푸핑 시도가 포함된 경우 해독된 트래픽을 차단하고 스푸핑 시도 로깅
- 규정을 준수하지 않는 정보가 포함된 해독된 트래픽을 차단하고 부적절한 정보 로깅
- 다른 모든 암호화된 트래픽 및 해독된 트래픽 허용

시스템은 해독된 트래픽을 목적지 호스트로 전송하기 전에 다시 암호화합니다.

다음 시나리오에서 사용자는 원격 서버에 온라인으로 정보를 제출합니다. 사용자의 브라우저는 서버와 TCP 연결을 설정하고 SSL 핸드셰이크를 시작합니다. 매니지드 디바이스는 이 트래픽을 수신합니다. 핸드셰이크와 연결 상세정보를 기반으로 시스템은 연결을 로깅하고 트래픽에 대해 조치를 취합니다. 시스템은 트래픽을 차단하는 경우 TCP 연결도 단습니다. 그렇지 않은 경우, 클라이언트와 서버는 SSL 핸드셰이크를 완료하여 암호화된 세션을 설정합니다.

## 인라인 구축의 암호화된 트래픽 모니터링

Underwriting 부서에서 주고받는 모든 SSL 암호화 트래픽에 대해 시스템은 연결을 로깅합니다.

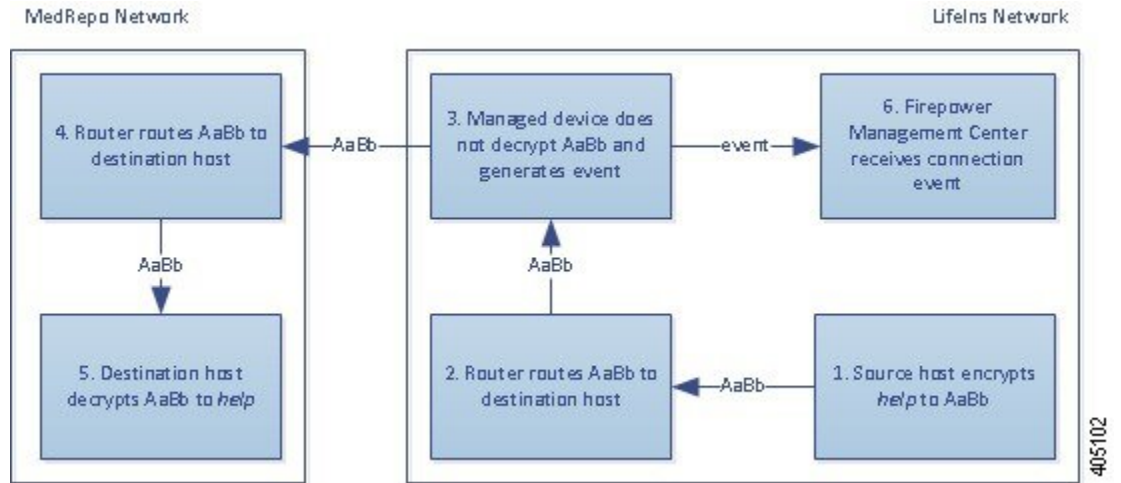


다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(help). 클라이언트가 이를 암호화하고(AaBb) 암호화된 트래픽을 MedRepo의 Requests 부서 서버로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 트래픽을 해독하지 않습니다.  
액세스 제어 정책은 계속해서 암호화된 트래픽을 처리하고 허용한 다음, 세션이 종료된 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Underwriting 부서 서버는 암호화된 정보 요청을 수신하고(AaBb) 이를 일반 텍스트로 해독합니다(help).
6. Firepower Management Center은 연결 이벤트를 수신합니다.

## 인라인 구축의 암호화된 트래픽 암호 해독

상급 보험업자로부터 시작된 모든 TLS/SSL 암호화 트래픽의 경우, 매니지드 디바이스는 암호 해독 없이 트래픽을 허용하고 연결을 로깅합니다.

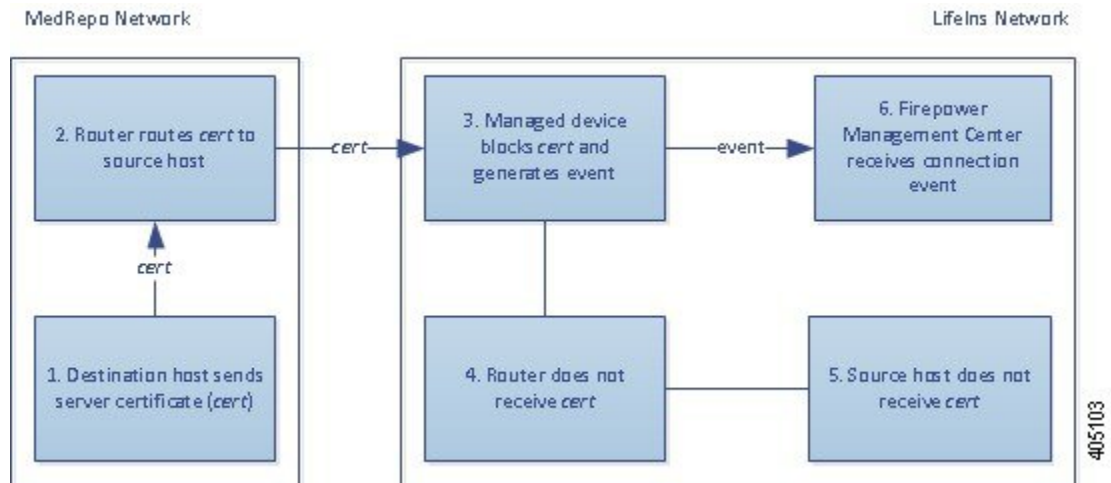


다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(*help*). 클라이언트가 이를 암호화하고(*AaBb*) 암호화된 트래픽을 MedRepo의 Requests 부서 서버로 전송합니다.
2. LifeIns의 라우터가 암호화된 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 이 트래픽을 해독하지 않습니다.  
액세스 제어 정책은 계속해서 암호화된 트래픽을 처리하고 허용한 다음, 세션이 종료된 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Requests 부서 서버는 암호화된 정보 요청을 수신하고(*AaBb*) 이를 일반 텍스트로 해독합니다(*help*).
6. Firepower Management Center은 연결 이벤트를 수신합니다.

## 인라인 구축의 암호화된 트래픽 차단

LifeIns의 Underwriting 부서에서 MedRepo의 Customer Service 부서로 부적절하게 전송된 모든 SMTPS 이메일 트래픽에 대해 시스템은 추가 검사 없이 SSL 핸드셰이크 중에 트래픽을 차단하고 연결을 로깅합니다.

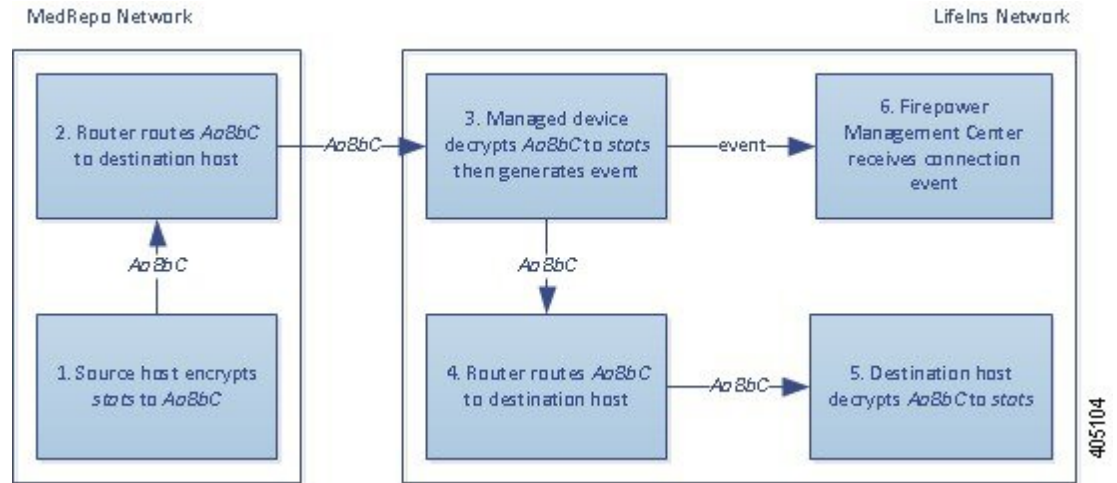


다음 단계가 발생합니다.

1. 클라이언트 브라우저에서 TLS/SSL 핸드셰이크 설정 요청을 받으면 Customer Service 부서 서버는 TLS/SSL 핸드셰이크의 다음 단계로서 LifeIns 보험업자에게 서버 인증서(cert)를 전송합니다.
2. MedRepo의 라우터는 인증서를 수신한 다음 LifeIns 보험업자에게 라우팅합니다.
3. 매니지드 디바이스는 추가 검사 없이 트래픽을 차단하고 TCP 연결을 종료하며, 연결 이벤트를 생성합니다.
4. 내부 라우터는 차단된 트래픽을 수신하지 않습니다.
5. 보험업자는 차단된 트래픽을 수신하지 않습니다.
6. Firepower Management Center은 연결 이벤트를 수신합니다.

## 인라인 구축에서 개인 키로 암호화된 트래픽 검사

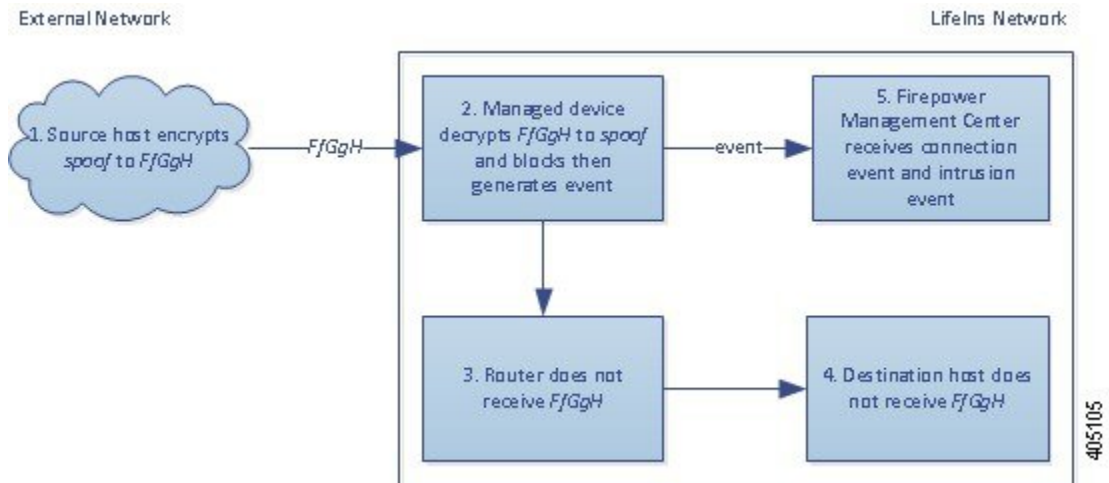
MedRepo에서 LifeIns의 Underwriting 부서로 전송되는 모든 TLS/SSL 암호화 트래픽에 대해 시스템은 업로드된 서버 개인 키를 사용하여 세션 키를 가져온 다음 트래픽을 암호 해독하고 연결을 로깅합니다. 합법적인 트래픽은 Underwriting 부서로 전송되기 전에 허용되고 다시 암호화됩니다.



다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(stats). 클라이언트가 이를 암호화하고(AaBbC) 암호화된 트래픽을 Underwriting 부서 서버로 전송합니다.
2. 외부 라우터가 트래픽을 수신한 다음 Underwriting 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 업로드된 알려진 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(stats).  
액세스 제어 정책은 맞춤형 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 스푸핑 시도를 찾지 않습니다. 디바이스는 암호화된 트래픽을 전달한 다음(AaBbC) 세션 종료 후 연결 이벤트를 생성합니다.
4. 내부 라우터가 트래픽을 수신한 다음 Underwriting 부서 서버로 라우팅합니다.
5. Underwriting 부서 서버는 암호화된 정보를 수신하고(AaBbC) 이를 일반 텍스트로 해독합니다(stats).
6. Firepower Management Center은 암호화된 트래픽과 해독된 트래픽에 대한 정보가 포함된 연결 이벤트를 수신합니다.

이와 반대로, 스푸핑 시도를 나타내는 해독된 트래픽은 삭제됩니다. 시스템은 연결 및 스푸핑 시도를 로깅합니다.



다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출하고(spooof), MedRepo, LLC에서 시작된 것으로 보이는 트래픽을 변경합니다. 클라이언트가 이를 암호화하고(FfGgH) 암호화된 트래픽을 Underwriting 부서 서버로 전송합니다.
2. 매니지드 디바이스는 업로드된 알려진 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(spooof).  
액세스 제어 정책은 맞춤형 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 스푸핑 시도를 찾습니다. 디바이스는 트래픽을 차단한 다음 침입 이벤트를 생성하며, 세션 종료 후 연결 이벤트를 생성합니다.
3. 내부 라우터는 차단된 트래픽을 수신하지 않습니다.
4. Underwriting 부서 서버는 차단된 트래픽을 수신하지 않습니다.
5. Firepower Management Center은 암호화된 트래픽 및 해독된 트래픽에 대한 정보가 포함된 연결 이벤트, 그리고 스푸핑 시도에 대한 침입 이벤트를 수신합니다.

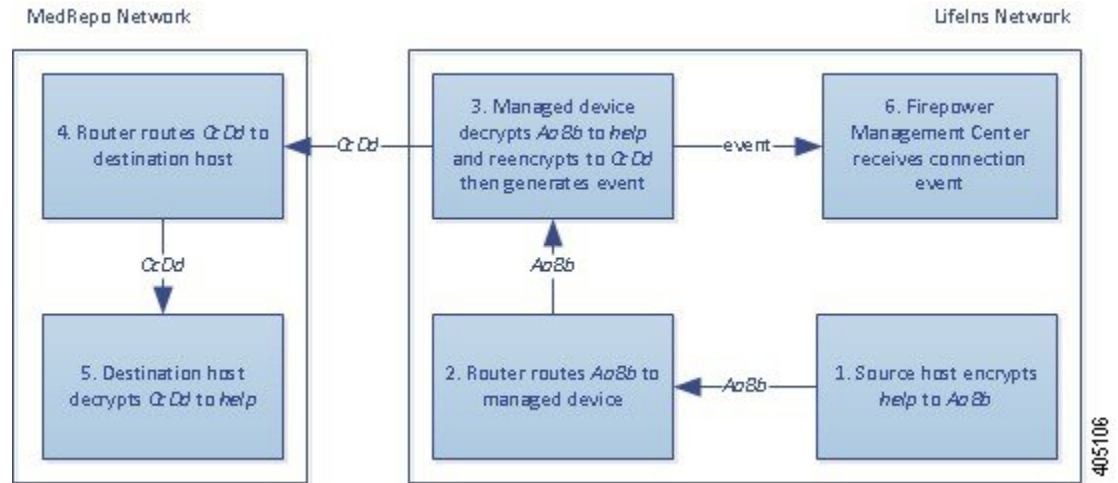
## 인라인 구축에서 다시 서명된 인증서로 암호화된 트래픽 검사

신입 및 하급 보험업자가 MedRepo의 Requests 부서로 전송하는 모든 TLS/SSL 암호화 트래픽에 대해 시스템은 다시 서명된 서버 인증서를 사용하여 세션 키를 얻은 다음 트래픽을 암호 해독하고 연결을 로깅합니다. 합법적인 트래픽은 MedRepo로 전송되기 전에 허용되고 다시 암호화됩니다.



**참고** 서버 인증서에 다시 서명하여 인라인 구축에서 트래픽을 해독할 때 디바이스는 중간자(man-in-the-middle) 역할을 합니다. 클라이언트와 매니지드 디바이스 간, 매니지드 디바이스와 서버 간에 각각 하나씩 2개의 TLS/SSL 세션을 생성합니다. 그 결과 각 세션에는 서로 다른 암호 세션 세부 사항이 포함됩니다.





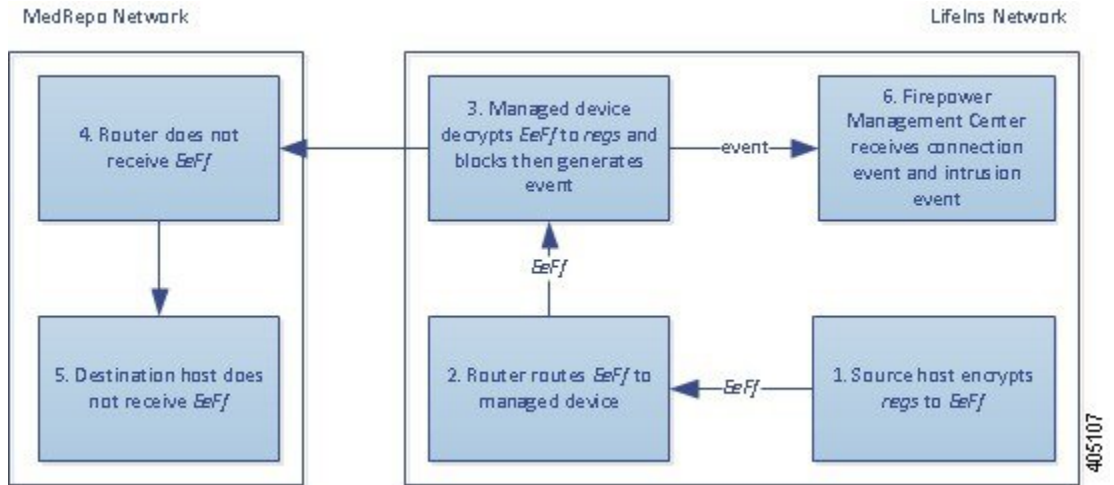
다음 단계가 발생합니다.

1. 사용자가 일반 텍스트 요청을 제출합니다(help). 클라이언트가 이를 암호화하고(AaBb) 암호화된 트래픽을 Requests 부서 서버로 전송합니다.
2. 내부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 다시 서명된 서버 인증서 및 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(help).  
 액세스 제어 정책은 맞춤형 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 부적절한 요청을 찾지 않습니다. 디바이스는 트래픽을 다시 암호화하여(ccDd) 통과하도록 허용합니다. 세션 종료 후 연결 이벤트를 생성합니다.
4. 외부 라우터가 트래픽을 수신한 다음 Requests 부서 서버로 라우팅합니다.
5. Requests 부서 서버는 암호화된 정보를 수신하고(ccDd) 이를 일반 텍스트로 해독합니다(help).
6. Firepower Management Center은 암호화된 트래픽과 해독된 트래픽에 대한 정보가 포함된 연결 이벤트를 수신합니다.



**참고** 다시 서명된 서버 인증서로 트래픽을 암호화하면 클라이언트 브라우저에 신뢰되지 않은 인증서에 대한 경고가 표시됩니다. 이 경고가 표시되지 않도록 하려면 CA 인증서를 조직의 도메인 루트 신뢰할 수 있는 인증서 저장소 또는 클라이언트 신뢰할 수 있는 인증서 저장소에 추가하십시오.

이와 반대로, 규정 요구 사항을 충족하지 못하는 정보를 포함하는 해독된 트래픽은 삭제됩니다. 시스템은 연결 및 비준수 정보를 로깅합니다.



다음 단계가 발생합니다.

1. 사용자가 규정 요구 사항을 준수하지 않는 일반 텍스트 요청을 제출합니다(*regs*). 클라이언트가 이를 암호화하고(*EeFf*) 암호화된 트래픽을 *Requests* 부서 서버로 전송합니다.
2. 내부 라우터가 트래픽을 수신한 다음 *Requests* 부서 서버로 라우팅합니다.
3. 매니지드 디바이스는 다시 서명된 서버 인증서 및 개인 키로 얻은 세션 키를 사용하여 이 트래픽을 일반 텍스트로 해독합니다(*regs*).

액세스 제어 정책은 맞춤형 침입 정책을 이용해 계속해서 해독된 트래픽을 처리하며 부적절한 요청을 찾습니다. 디바이스는 트래픽을 차단한 다음 침입 이벤트를 생성하며, 세션 종료 후 연결 이벤트를 생성합니다.

4. 외부 라우터는 차단된 트래픽을 수신하지 않습니다.
5. *Requests* 부서 서버는 차단된 트래픽을 수신하지 않습니다.
6. Firepower Management Center은 암호화된 트래픽 및 해독된 트래픽에 대한 정보가 포함된 연결 이벤트, 그리고 부적절한 요청에 대한 침입 이벤트를 수신합니다.

## TLS/SSL 기록

| 기능                               | 버전  | 세부 사항  |
|----------------------------------|-----|--|
| 평판이 알려지지 않은 URL의 처리를 지정할 수 있는 기능 | 6.7 | 자세한 내용은 <a href="#">URL 필터링 기록</a> 섹션을 참조해 주십시오.         |
| 해독 - 알려진 키 규칙을 위한 ClientHello 수정 | 6.7 | 자세한 내용은 <a href="#">ClientHello 메시지 처리</a> 섹션을 참조해 주십시오. |

| 기능  | 버전      | 세부 사항   |
|---|---------|---|
| 트래픽이 액세스 제어 규칙의 URL 및 애플리케이션 기준과 일치하도록 TLS 1.3 트래픽에서 인증서를 추출하는 기능.    | 6.7     | 새 화면/수정된 화면: <b>Policies(정책)</b> > <b>Access Control(액세스 제어)</b> > (액세스 제어 정책 편집) > <b>Advanced(고급)</b> 링크.<br><br>자세한 내용은 다음 섹션을 참조하십시오. <a href="#">TLS 1.3 서버 ID 검색, 9 페이지</a>   |
| 범주 및 평판 기반 URL 필터링 변경   | 6.5     | 자세한 내용은 <a href="#">URL 필터링 기록</a> 섹션을 참조해 주십시오.  |
| TLS 암호화 가속 비활성화할 수 없습니다.  | 6.4     | TLS 암호화 가속 지원되는 모든 디바이스에서 활성화됩니다.<br><br>기본 인터페이스를 가진 매니지드 디바이스에서 TLS 암호화 가속을 비활성화할 수 없습니다.<br><br>FTD 컨테이너 인스턴스에서 TLS 암호화 가속에 대한 지원은 이 테이블의 다음 행에 설명된 대로 제한됩니다.<br><br>제거된 명령:<br><br><b>system support ssl-hw-accel enable</b><br><b>system support ssl-hw-accel disable</b><br><b>system support ssl-hw-status</b> |
| Firepower 4100/9300 모듈/보안 엔진에서 하나의 FTD 컨테이너 인스턴스에서의 TLS 암호화 가속에 대한 지원 | 6.4     | 이제 모듈/보안 엔진에서 하나의 FTD 컨테이너 인스턴스에 대해 TLS 암호화 가속을 활성화할 수 있습니다. TLS 암호화 가속은 다른 컨테이너 인스턴스의 경우, 비활성화되지만 기본 인스턴스의 경우에는 활성화됩니다.<br><br>신규/수정된 명령:<br><br><b>config hwCrypto enable</b><br><br><b>show crypto accelerator status</b> 가 <b>system support ssl-hw-status</b> 를 대체)  |
| TLS/SSL 하드웨어 가속 이제 다음으로 지칭 <b>TLS</b> 암호화 가속                          | 6.4     | TLS/SSL 암호화 및 암호 해독 가속을 지원하는 디바이스가 늘어난 것을 반영하여 이름이 변경되었습니다. 가속화는 디바이스에 따라 소프트웨어 또는 하드웨어에서 수행될 수 있습니다.<br><br>영향을 받는 화면: TLS 암호화 가속의 상태를 보려면 <b>Devices(디바이스)</b> > <b>Device Management(디바이스 관리)</b> > <b>Device(디바이스), General(일반)</b> 페이지.  |
| 지원되는 Extended Master Secret 확장 ( <a href="#">RFC 7627</a> 참조)         | 6.3.0.1 | SSL 정책, 특히 <b>Decrypt - Resign(암호 해독 - 다시 서명)</b> 또는 <b>Decrypt - Known Key(암호 해독 - 알려진 키)</b> 규칙 작업이 있는 정책의 경우, TLS Extended Master Secret 확장이 지원됩니다.  |
| 지원되지 않는 Extended Master Secret 확장                                     | 6.3     | 확장은 <b>Decrypt - Resign(암호 해독 - 다시 서명)</b> 규칙에 대한 Client_hello 수정 도중 제거됩니다.   |

| 기능   | 버전      | 세부 사항   |
|--|---------|---|
| TLS/SSL 하드웨어 가속 기본적으로 활성화                    | 6.3     | TLS/SSL 하드웨어 가속 지원되는 모든 디바이스에서 기본적으로 활성화되지만 원하는 경우 비활성화할 수 있습니다.  |
| 지원되는 Extended Master Secret 확장 (RFC 7627 참조) | 6.2.3.9 | SSL 정책, 특히 <b>Decrypt - Resign</b> (암호 해독 - 다시 서명) 또는 <b>Decrypt - Known Key</b> (암호 해독 - 알려진 키) 규칙 작업이 있는 정책의 경우, TLS 확장 마스터 암호 확장이 지원됩니다. |
| 지원되는 카테고리 및 평판 조건                            | 6.2.2   | 카테고리/평판 조건이 있는 액세스 제어 규칙 또는 SSL 규칙.   |