SSL 정책

다음 주제는 SSL 정책 생성, 구성, 관리, 로깅의 개요를 제공합니다.

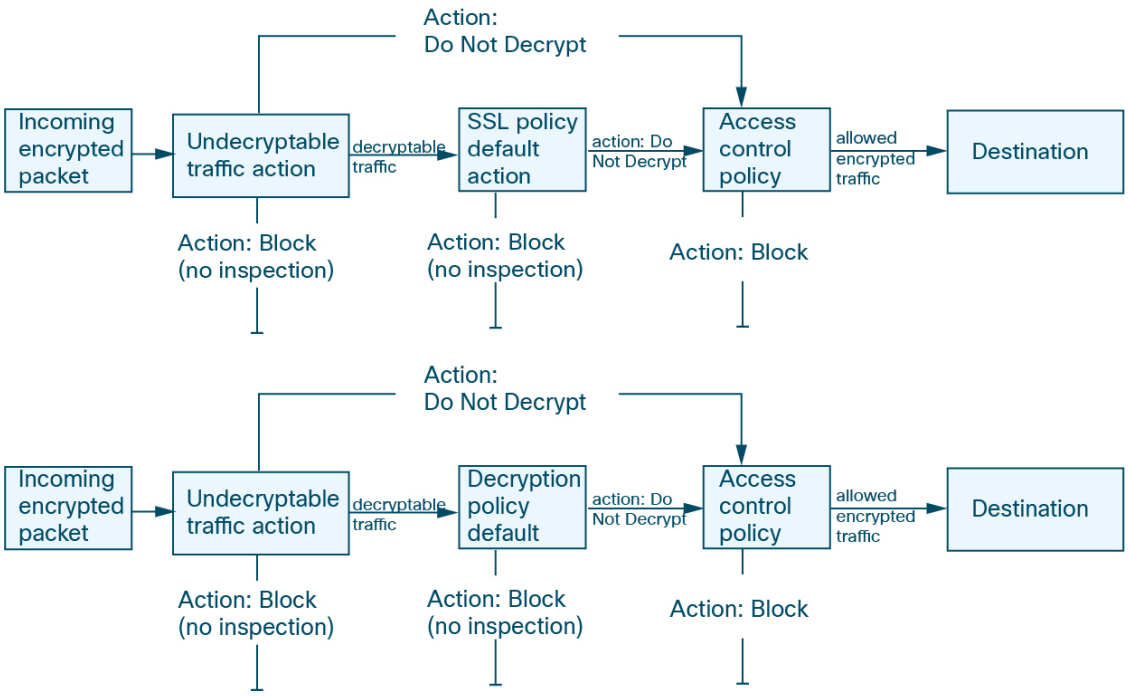
SSL 정책 개요

SSL 정책에 따라 시스템에서 네트워크의 암호화 트래픽을 처리하는 방식이 결정됩니다. 하나 이상의 SSL 정책을 구성하고 SSL 정책을 액세스 제어 정책에 연결한 다음 액세스 제어 정책을 매니지드 디바이스에 구축할 수 있습니다. 디바이스가 TCP 핸드셰이크를 탐지하면 먼저 액세스 제어 정책이 트래픽을 처리하고 검사합니다. 그 이후에 TCP 연결을 통한 TLS/SSL 암호화 세션을 식별할 경우, SSL 정책이 해당 과정을 이어받아 암호화 트래픽을 처리하고 해독합니다.

⚠

주의 *Snort 2*에만 해당됩니다. SSL 정책 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. 추가 또는 제거

다음 다이어그램에서 보여주는 것처럼 가장 간단한 SSL 정책은 정책이 구축된 디바이스에게 단일 기본 작업을 통해 암호화 트래픽을 처리하도록 지시합니다. 추가 검사 없이 해독 가능 트래픽을 차단하거나 액세스 제어로 아직 해독되지 않은 해독 가능한 트래픽을 검사하도록 기본 작업을 설정할 수 있습니다. 그러면 시스템에서 암호화 트래픽을 허용하거나 차단할 수 있습니다. 디바이스는 암호 해독 불가 트래픽을 탐지할 경우, 추가 검사 없이 트래픽을 차단하거나 암호 해독하지 않고 액세스 제어로 검사합니다.



더 복잡한 SSL 정책에서는 다양한 유형의 해독 불가 트래픽을 각기 다른 작업으로 처리하고, CA(인증 기관)에서 암호화 인증서를 발급하였는지 신뢰하는지에 따라 트래픽을 제어하고, 암호화 트래픽 로깅 및 처리를 정밀하게 제어하기 위해 TLS/SSL 규칙을 사용할 수 있습니다. 이러한 규칙은 다양한 기준에 따라 암호화 트래픽을 매칭하고 검사하기 때문에 간단할 수도 있고 복잡할 수도 있습니다.

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.

SSL 정책은 예외입니다. management center 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.

관련 항목

TLS/SSL 규칙 조건

SSL 정책 기본 작업

SSL 정책의 기본 작업은 정책의 비 모니터 규칙과 일치하지 않는 해독 가능한 암호화 트래픽을 시스템이 처리하는 방법을 결정합니다. TLS/SSL 규칙이 없는 SSL 정책을 구축하는 경우, 기본 작업은 네

트워크의 모든 해독 가능 트래픽이 처리되는 방법을 결정합니다. 기본 작업에 의해 차단된 암호화 트래픽에 대해서는 어떠한 검사도 수행하지 않습니다.

표 *1: SSL* 정책 기본 작업

기본 작업	암호화 트래픽에 미치는 영향
Block(차단)	추가 검사 없이 TLS/SSL 세션을 차단합니다.
Block with Reset(차단 후 재설정)	추가 검사 없이 TLS/SSL 세션을 차단하고 TCP 연결을 재설정합니다. 트래픽이 UDP와 같은 연결 없는 프로토콜을 사용하는 경우, 이 옵션을 선택합니다. 이 경우, 연결 없는 프로토콜은 재설정 될 때까지 다시 연결하려고 시도합니다. 이 작업은 브라우저에 연결 재설정 오류도 표시하므로 사용자는 연결이 차단된 것을 알 수 있습니다.
Do not decrypt(암호 해독 안 함)	액세스 제어를 통해 암호화된 트래픽을 검사합니다.

관련 항목

기본 SSL 정책 생성, 6 페이지

암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션

표 *2:* 해독 불가 트래픽 유형

유형	설명	기본 작업	사용 가능한 작업
압축된 세션	TLS/SSL 세션은 데이터 압축 방식을 적용합니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
SSLv2 세션	세션이 SSL 버전 2로 암호화됩니다. ClientHello 메시지가 SSL 2.0이고 전송된 트래픽의 나머지가 SSL 3.0일 경우 트래픽은 해독 가능합니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속

유형	설명	기본 작업	사용 가능한 작업
알 수 없는 암호 그룹	시스템에서 암호화 솔루션을 인식하지 않습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
지원되지 않는 암호 그룹	시스템에서 탐지된 암호화 솔루션 기반의 해독을 지원하지 않습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
캐싱되지 않는 세션	TLS/SSL 세션에서 세션 재사용이 활성화되었고 클라이언트 및 서버가 세션 식별자로 세션을 재설정했으며 시스템에서 해당 세션 식별자를 캐싱하지 않았습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
핸드셰이크 오류	TLS/SSL 핸드셰이크 협상 중에 오류가 발생했습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) Block(차단) Block with Reset(차단 후 재설정) 기본 작업 상속
해독 오류	트래픽 해독 중에 오류가 발생했습니다.	차단	Block(차단) Block with Reset(차단 후 재설정)

SSL 정책을 처음 생성할 때 기본 작업에 의해 처리되는 로깅 연결은 기본적으로 비활성화됩니다. 기본 작업에 대한 로깅 설정이 해독 불가 트래픽 처리에도 적용되므로 해독 불가 트래픽 작업에 의해 처리되는 로깅 연결은 기본적으로 비활성화됩니다.

브라우저가 인증서 고정을 사용하여 서버 인증서를 확인하는 경우 서버 인증서에 다시 서명을 하여 이 트래픽을 암호 해독할 수 없습니다. 자세한 내용은 TLS/SSL 규칙 지침 및 제한 사항을 참조하십시오.

관련 항목

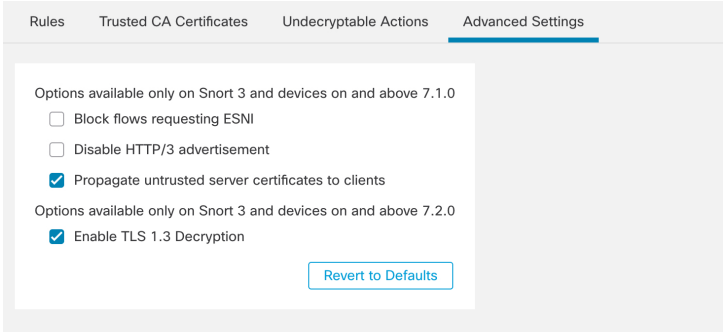
해독 불가 트래픽에 대한 기본 처리 설정, 7 페이지

SSL 정책 고급 옵션

SSL 정책의 **Advanced Settings(**고급 설정**)** 탭 페이지에는 정책이 적용되는 Snort 3에 대해 구성된 모든 매니지드 디바이스에 적용되는 전역 설정이 있습니다. 다음을 실행하는 모든 매니지드 디바이스에서는 이러한 설정이 모두 무시됩니다.

- 7.1 이전 버전
- Snort 2

다음은 예입니다.



ESNI를 요청하는 차단 플로우

암호화된 서버 이름 표시(ESNI(초안 제안에 대한 링크))는 클라이언트가 요청하는 내용을 TLS 1.3 서버에 알리는 방법입니다. SNI는 암호화되므로 시스템에서 서버를 확인할 수 없으므로 선택적으로 이러한 연결을 차단할 수 있습니다.

HTTP/3 광고 비활성화

이 옵션은 다음과 같은 이유로 TCP 연결의 ClientHello에서 HTTP/3(RFC 9114)을 제거합니다.

- RFC 9114에 설명된 대로 HTTP/3는 TCP 전송 프로토콜이 아닌 QUIC 전송 프로토콜의 일부입니다.
- QUIC는 Firepower 시스템에서 아직 지원되지 않습니다.
- 클라이언트의 HTTP/3 광고 차단을 통해 공격 및 회피 시도로부터 보호

신뢰할 수 없는 서버 인증서를 클라이언트에 전파

이는 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙 작업과 일치하는 트래픽에만 적용됩니다.

서버 인증서를 신뢰할 수 없는 경우 매니지드 디바이스의 CA(인증 기관)를 서버 인증서로 대체하려면 이 옵션을 활성화합니다. 신뢰할 수 없는 서버 인증서는 Secure Firewall Management Center에서 신

뢰할 수 있는 CA로 나열되지 않은 인증서입니다. **Objects(**개체**)** > **Object Management(**개체 관리**)** > **PKI** > **Trusted CAs(**신뢰하는 **CA)**).

TLS 1.3 암호 해독 활성화

(Snort 3만 해당.) 슬라이더를 이동하여 이 Management Center로 관리되는 Threat Defense 디바이스가 TLS 1.3 트래픽을 해독할 수 있도록 합니다.

슬라이더를 비활성화 위치로 이동하면 시스템은 TLS 1.2 트래픽만 암호 해독합니다.

관련 정보

TLS/SSL 규칙 모범 사례

SSL 정책의 시스템 요구 사항 및 사전 요건

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

기본 SSL 정책 생성

SSL 정책을 구성하려면 정책에 고유한 이름과 기본 작업을 지정해야 합니다.

프로시저

단계 **1** 아직 하지 않았다면 management center에 로그인합니다.
단계 **2** **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **SSL** 버튼을 클릭합니다.
단계 **3** **New Policy(**새로운 정책**)**를 클릭합니다.
단계 **4** 정책에 고유한 **Name(**이름**)** 또는 **Description(**설명**)**을 지정합니다.
단계 **5** **Default Action(**기본 작업**)**을 지정합니다(SSL 정책 기본 작업, 2 페이지 참조).
단계 **6** 기본 작업에 대한 로깅 옵션을 구성합니다.
단계 **7** **Save(**저장**)**를 클릭합니다.

향후 작업

- 해독 불가 트래픽에 대한 기본 처리를 설정합니다(해독 불가 트래픽에 대한 기본 처리 설정, 7 페이지 참조).
- 암호 해독 불가능한 트래픽의 기본 처리에 대한 로깅 옵션을 구성합니다..
- 고급 정책 속성을 설정합니다.SSL 정책 고급 옵션, 5 페이지
- 액세스 제어에 다른 정책 연결의 설명대로 SSL 정책을 액세스 제어 정책에 연결합니다.
- Deploy configuration changes(구성 변경 사항 구축)참조.

해독 불가 트래픽에 대한 기본 처리 설정

시스템에서 해독하거나 검사하지 못하는 암호화 트래픽의 특정 유형을 처리하도록 SSL 정책 레벨에서 해독 불가 트래픽 작업을 설정할 수 있습니다. TLS/SSL 규칙이 없는 SSL 정책을 구축하는 경우, 해독 불가 트래픽 작업은 네트워크의 모든 해독 불가 암호화 트래픽이 처리되는 방법을 결정합니다.

해독 불가 트래픽의 유형에 따라 다음 작업을 선택할 수 있습니다.

- 연결 차단.
- 연결을 차단한 다음 재설정. 이 옵션은 UDP와 같이 연결이 차단될 때까지 계속 연결을 시도하는 연결 없는 프로토콜의 경우에 바람직합니다.
- 액세스 제어를 통해 암호화된 트래픽 검사.
- SSL 정책에서 기본 작업 상속.

프로시저

단계 **1** 아직 하지 않았다면 management center에 로그인합니다.

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

단계 **3** SSL 정책 이름 옆의 **Edit(**수정**)** ( )을 클릭합니다.

단계 **4** SSL 정책 편집기에서 **Undecryptable Actions(**암호 해독할 수 없는 작업**)**을 클릭합니다.

단계 **5** 각 필드에서 SSL 정책의 기본 작업 또는 해독 불가 트래픽 유형에서 수행할 다른 작업을 선택합니다. 자세한 내용은 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 3 페이지 및 SSL 정책 기본 작업, 2 페이지를 참고하십시오.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 암호 해독 불가능한 트래픽 작업으로 처리되는 연결에 대한 기본 로깅을 구성합니다
- Deploy configuration changes(구성 변경 사항 구축)참조.

SSL 정책 관리

SSL 정책 편집기에서 다음을 수행할 수 있습니다.

- TLS/SSL 규칙 추가, 편집, 삭제, 활성화, 비활성화, 구성.
- 신뢰할 수 있는 CA 인증서 추가.
- 시스템에서 해독할 수 없는 암호화 트래픽의 처리 결정.
- 기본 작업 및 해독 불가 트래픽 작업에 의해 처리되는 트래픽 로깅.
- 고급 옵션을 설정합니다.

다중 도메인 구축에서 시스템은 현재 도메인에서 생성된 정책을 표시하며 이러한 정책은 수정할 수 있습니다. 상위 도메인에서 생성된 정책도 표시되지만, 이러한 정책은 수정할 수 없습니다. 하위 도메인에서 생성된 정책을 보고 수정하려면 해당 도메인으로 전환하십시오.

한 번에 사용자 한 명이 단일 브라우저 창을 사용하여 정책을 수정해야 합니다. 여러 사용자가 동일한 정책을 저장할 경우 마지막으로 저장한 변경사항이 유지됩니다. 편의상 시스템에는 현재 각 정책을 수정하고 있는 사용자(있는 경우)에 대한 정보가 표시됩니다. 세션의 개인 정보를 보호하기 위해 정책 편집기에서 30분 동안 아무런 작업을 하지 않으면 경고가 표시됩니다. 60분이 지나면 시스템에서 변경사항을 삭제합니다.

프로시저

단계 **1** 아직 하지 않았다면 management center에 로그인합니다.

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

단계 **3** SSL 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교를 참조하십시오.
- 복사- **Copy(**복사**)** ()를 클릭합니다.
- 생성 - **New Policy(**새 정책**)**을 클릭합니다(기본 SSL 정책 생성, 6 페이지 참조).
- 삭제- **Delete(**삭제**)** ()를 클릭합니다. 컨트롤이 흐리게 표시되는 경우에는 컨피그레이션이 상위 도메인에 속하거나 컨피그레이션을 수정할 권한이 없는 것입니다.
- 보고서- **Report(**보고서**)** ()를 클릭합니다. 현재 정책 보고서 생성를 참조하십시오.
- 편집-**Edit(**수정**)** ()를 클릭합니다. **View(**보기**)** ()이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.
- 신뢰할 수 있는 CA 인증서를 SSL 정책에 추가하려면 외부 인증 증명 신뢰의 내용을 참조하십시오.

- SSL 정책이 해독 불가 트래픽을 처리하는 방법을 구성하려면 해독 불가 트래픽에 대한 기본 처리 설정, 7 페이지의 내용을 참조하십시오.
- SSL 정책 고급 설정 - SSL 정책 고급 옵션, 5 페이지의 내용을 참조하십시오.
- Import/Export(가져오기/내보내기) - Secure Firewall Management Center 및 Threat Defense Management Network 관리의 구성 가져오기 및 내보내기에 대한 섹션을 참조하십시오.
- 암호 해독할 수 없는 트래픽 처리 및 SSL 규칙과 일치하지 않는 트래픽에 대한 연결을 기록하려면 Cisco Secure Firewall Management Center 관리 가이드 에서 정책 기본 작업을 사용한 연결 기록을 참조하십시오.
- 구축 - **Deploy(**구축**)** > **Deployment(**구축**)**를 선택합니다. 구성 변경 사항 구축의 내용을 참조하십시오.