암호 해독 정책

다음 주제는 암호 해독 정책 생성, 구성, 관리, 로깅의 개요를 제공합니다.

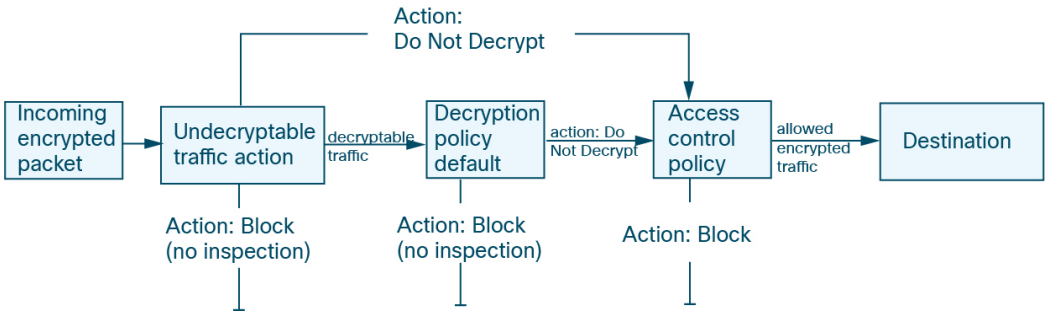
암호 해독 정책 정보

해독 정책에 따라 시스템에서 네트워크의 암호화 트래픽을 처리하는 방식이 결정됩니다. 하나 이상의 해독 정책을 구성하고 해독 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, 해독 정책이 해당 과정을 이어받아 암호화 트래픽을 처리하고 해독합니다.

수신 트래픽의 암호 해독(**Decrypt - Known Key(**암호 해독 **-** 알려진 키) 규칙 작업) 및 발신 트래픽(**Decrypt - Resign(**암호 해독 **-** 다시 서명) 규칙 작업)을 위한 규칙을 포함하여 여러 규칙을 동시에 생성할 수 있습니다. **Do Not Decrypt(**암호 해독 안 함**)** 또는 다른 규칙 작업(예: **Block(**차단**)** 또는 **Monitor(**모니터링**)**)이 포함된 규칙을 생성하려면 빈 암호 해독 정책을 생성하고 나중에 규칙을 추가합니다.

시작하려면 암호 해독 정책 생성, 2 페이지를 참조하십시오.

다음은 **Do Not Decrypt(**암호 해독 안 함**)** 규칙 작업이 포함된 암호 해독 정책의 예입니다.



다음 다이어그램에서 보여주는 것처럼 가장 간단한 해독 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.

해독 정책의 시스템 요구 사항 및 사전 요건

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

암호 해독 정책 생성

이 주제에서는 암호 해독 정책을 생성하고, 선택적으로 내부 또는 외부 서버를 보호하기 위한 하나 이상의 규칙을 생성하는 방법에 대해 설명합니다. 규칙 없이 암호 해독 정책을 생성하고 나중에 규칙을 추가할 수도 있습니다. **Do Not Decrypt(**암호 해독 안 함**)**, **Block(**차단**)**, **Block With Reset(**차단 후 재설정**)** 또는 **Monitor(**모니터링**)** 규칙 작업이 포함된 규칙을 생성하려면 빈 정책을 생성하는 것이 좋습니다.

시작하기 전에

암호 해독 요구 사항을 검토합니다.

- 암호 해독은 네트워크 트래픽을 심층 검사에 노출하는 방법입니다. 그러나 트래픽을 해독해서는 안 되는 경우도 있습니다.트래픽을 암호 해독해야 하는 경우와 하면 안 되는 경우

- 트래픽을 암호 해독하고 선택적으로 검사하여 내부 서버를 보호하려면 내부 서버에 대한 내부 인증서가 있어야 합니다.PKI
- 트래픽을 암호 해독하고 필요에 따라 검사하여 외부 서버를 보호하려면 트래픽을 재전송하는 데 사용할 내부 CA 개체를 업로드해야 합니다.PKI

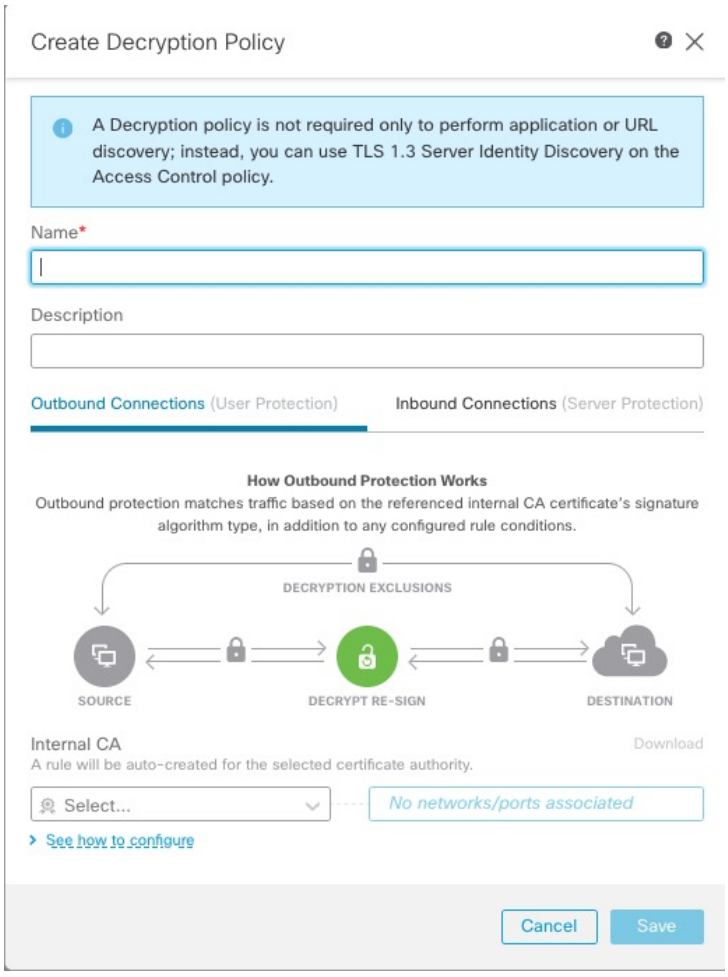
프로시저

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

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

단계 **3** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **4** **Name(**이름**)** 필드에 정책 이름을 입력하고 **Description(**설명**)** 필드에 선택적 설명을 입력합니다.



Outbound Connections(아웃바운드 연결**)** 탭 페이지에서는 **Decrypt - Resign(**암호 해독 - 서명**)** 규칙을 생성할 수 있습니다. 이러한 규칙에는 내부 인증서가 필요합니다. 이 인증서는 미리 생성하거나 (**Objects(**개체**)** > **Object Management(**개체 관리**)** > **PKI** > **Internal CAs(**내부 **CA)** 사용) 아웃바운드 연결 규칙의 일부로 생성할 수 있습니다.

Inbound Connections(인바운드 연결**)** 탭 페이지에서는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙을 생성할 수 있습니다. 이러한 규칙에는 내부 인증서가 필요합니다. 이 인증서는 미리 생성하거나(**Objects(**개체**)** > **Object Management(**개체 관리**)** > **PKI** > **Internal Certs(**내부 인증서**)** 사용) 인바운드 연결 규칙의 일부로 생성할 수 있습니다.

단계 **5** 액세스 제어에 다른 정책 연결에 설명된 대로 암호 해독 규칙을 액세스 제어 규칙과 연결합니다.

단계 **6**

단계 **7** 다음 섹션 중 하나를 계속 진행합니다.

향후 작업

- 아웃바운드 연결 보호를 사용하여 암호 해독 정책 생성, 4 페이지 (암호 해독 - 재서명)
- 인바운드 연결 보호를 사용하여 암호 해독 정책 생성, 7 페이지 (암호 해독 - 알려진 키)
- 다른 규칙 작업으로 암호 해독 정책 생성, 10 페이지

아웃바운드 연결 보호를 사용하여 암호 해독 정책 생성

이 작업에서는 아웃바운드 연결을 보호하는 규칙을 사용하여 암호 해독 정책을 생성하는 방법을 설명합니다. 즉, 대상 서버가 보호된 네트워크 외부에 있습니다. 이 유형의 규칙에는 **Decrypt - Resign(**암호 해독 - 재서명**)** 규칙 작업이 있습니다.

암호 해독 정책을 생성할 때 여러 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 및 여러 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙을 포함하여 여러 규칙을 동시에 생성할 수 있습니다.

Threat Defense 기능 기록:

7.4 - 이 기능이 추가되었습니다.

시작하기 전에

아웃바운드 연결을 보호하는 암호 해독 정책을 생성하려면 먼저 아웃바운드 서버에 대한 내부 CA(certificate authority)를 업로드해야 합니다. 다음 방법 중 하나로 이 작업을 수행할 수 있습니다.

- **Objects(**개체**)** > **Object Management(**개체 관리**)** > **PKI** > **Internal CAs(**내부 **CA)**로 이동하여 PKI를 참조하여 내부 CA 개체를 생성합니다.
- 이 암호 해독 정책을 생성할 때

프로시저

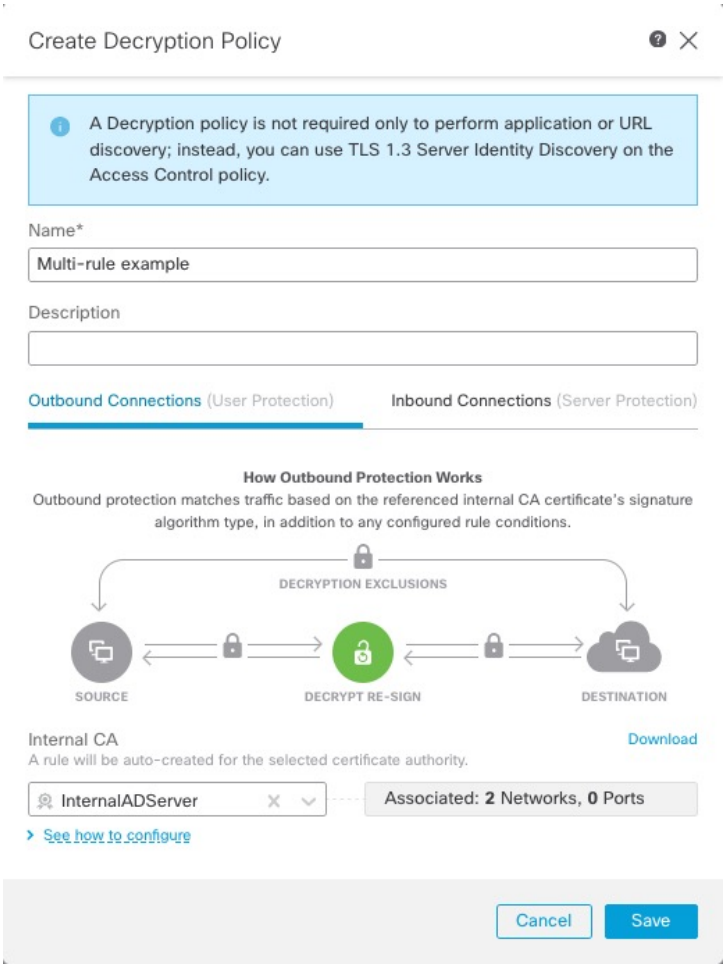
단계 **1** 아직 하지 않았다면 management center에 로그인합니다.

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

단계 **3** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **4** 정책에 고유한 **Name(**이름**)** 또는 **Description(**설명**)**을 지정합니다.

단계 **5** **Outbound Connections(**아웃바운드 연결**)** 탭을 클릭합니다.



단계 **6** 규칙에 대한 인증서를 업로드하거나 선택합니다.

시스템은 인증서당 하나의 규칙을 생성합니다.

단계 **7** (선택 사항). 네트워크 및 포트를 선택합니다.

자세한 내용:

- 해독 규칙 조건
- 네트워크 규칙 조건
- 포트 규칙 조건

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 규칙 조건을 추가합니다. 해독 규칙 조건
- 기본 정책 작업을 추가합니다. 해독 정책 기본 작업, 11 페이지
- Cisco Secure Firewall Management Center 관리 가이드 의 정책 기본 작업으로 연결 로깅에 설명된 대로 기본 작업에 대한 로깅 옵션을 구성합니다.
- 고급 정책 속성을 설정합니다.해독 정책 고급 옵션, 14 페이지
- 액세스 제어에 다른 정책 연결의 설명대로 해독 정책을 액세스 제어 정책에 연결합니다.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

아웃바운드 보호를 위해 내부 **CA** 업로드

이 작업에서는 아웃바운드 연결을 보호하는 암호 해독 규칙을 생성할 때 내부 인증 기관을 업로드하는 방법을 설명합니다. CA 인증서 및 개인 키 가져오기에 설명된 대로 **Objects(**개체**)** > **Object Management(**개체 관리**)**를 사용하여 내부 CA를 업로드할 수도 있습니다.

시작하기 전에

내부 인증 기관 개체에 설명된 형식 중 하나의 내부 인증 기관이 있는지 확인합니다.

프로시저

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

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

단계 **3** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **4** **Name(**이름**)** 필드에 정책 이름을 입력하고 **Description(**설명**)** 필드에 선택적 설명을 입력합니다.

단계 **5** **Outbound Connections(**아웃바운드 연결**)** 탭을 클릭합니다.

단계 **6** **Internal CA(**내부 **CA)** 목록에서 **Create New(**새로 만들기**)** > **Upload CA(CA** 업로드**)**를 클릭합니다.

단계 **7** 내부 CA에 이름을 지정합니다.

단계 **8** 제공된 필드에서 인증서 및 개인 키를 붙여넣거나 찾아봅니다.

단계 **9** CA에 비밀번호가 있는 경우 **Encrypted(**암호화됨**)** 확인란을 선택하고 옆에 있는 필드에 비밀번호를 입력합니다.

아웃바운드 보호를 위해 내부 **CA** 생성

이 작업에서는 아웃바운드 연결을 보호하는 암호 해독 규칙을 생성할 때 내부 인증 기관을 선택적으로 생성할 수 있는 방법을 설명합니다. **Objects(**개체**)** > **Object Management(**개체 관리**)**에서 설명한 대로 CSR에 응답하여 발행된 서명된 인증서 업로드를 사용하여 이러한 작업을 수행할 수도 있습니다.

시작하기 전에

내부 인증 기관 개체에 설명된 대로 내부 인증 기관 개체를 생성하기 위한 요구 사항을 이해해야 합니다.

프로시저

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

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

단계 **3** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **4** **Name(**이름**)** 필드에 정책 이름을 입력하고 **Description(**설명**)** 필드에 선택적 설명을 입력합니다.

단계 **5** **Outbound Connections(**아웃바운드 연결**)** 탭을 클릭합니다.

단계 **6** **Internal CA(**내부 **CA)** 목록에서 **Create New(**새로 만들기**)** > **Generate CA(CA** 생성**)**를 클릭합니다.

단계 **7** 내부 CA에 **Name(**이름**)**을 지정하고 2자로 된 **Country Name(**국가 이름**)**을 제공합니다.

단계 **8** **Self-Signed(**자체 서명**)** 또는 **CSR**을 클릭합니다.

이러한 옵션에 대한 자세한 내용은 내부 인증 기관 개체의 내용을 참조하십시오.

단계 **9** 제공된 필드에 요청된 정보를 입력합니다.

단계 **10** **Save(**저장**)**를 클릭합니다.

단계 **11** **CSR**을 선택한 경우 서명 요청이 완료되면 다음과 같이 **Install Certificate(**인증서 설치**)**를 클릭합니다.

a) 이 절차의 이전 단계를 반복합니다.

b) **Internal CA(**내부 **CA)** 목록에서 다음과 같이 CA를 편집합니다.

c) **Install Certificate(**인증서 설치**)**를 클릭합니다.

d) 화면의 프롬프트에 따라 작업을 완료합니다.

인바운드 연결 보호를 사용하여 암호 해독 정책 생성

이 작업에서는 인바운드 연결을 보호하는 규칙을 사용하여 암호 해독 정책을 생성하는 방법을 설명합니다. 즉, 대상 서버가 보호된 네트워크 내부에 있습니다. 이 유형의 규칙에는 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 작업이 있습니다.

암호 해독 정책을 생성할 때 여러 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 및 여러 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙을 포함하여 여러 규칙을 동시에 생성할 수 있습니다.

Threat Defense 기능 기록:

7.4 - 이 기능이 추가되었습니다.

시작하기 전에

인바운드 연결을 보호하는 암호 해독 정책을 생성하려면 먼저 내부 서버에 대한 내부 인증서를 업로드해야 합니다. 다음 방법 중 하나로 이 작업을 수행할 수 있습니다.

- **Objects(**개체**)** > **Object Management(**개체 관리**)** > **PKI** > **Internal Certs(**내부 인증서**)**로 이동하고 PKI를 참조하여 내부 인증서 개체를 생성합니다.
- 이 암호 해독 정책을 생성할 때

프로시저

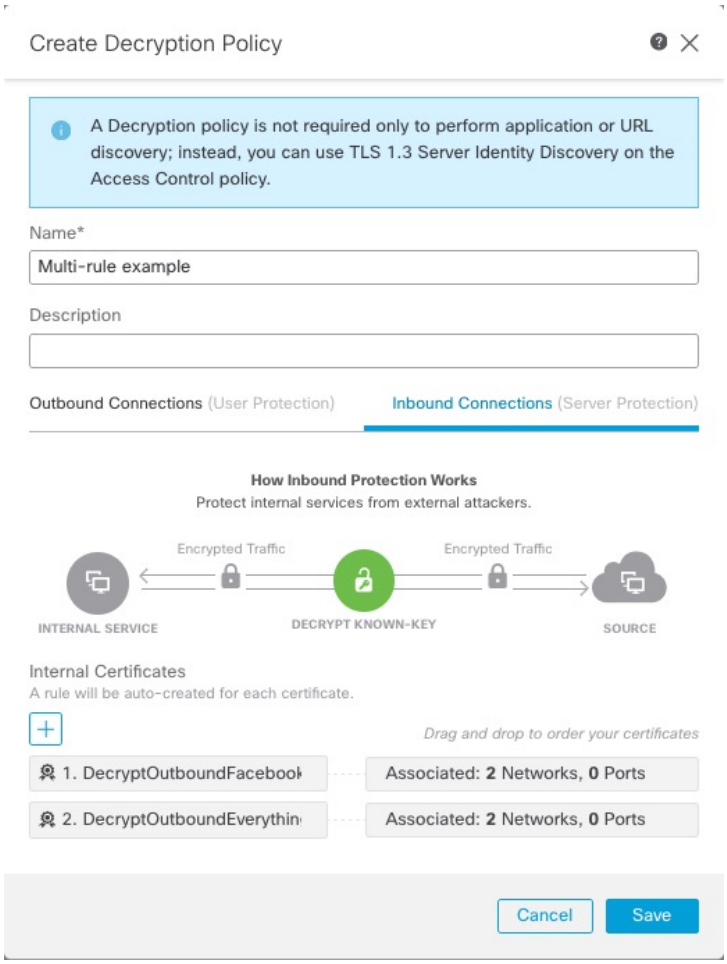
단계 **1** management center에 로그인합니다.

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

단계 **3** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **4** 정책에 고유한 **Name(**이름**)** 또는 **Description(**설명**)**을 지정합니다.

단계 **5** **Inbound Connections(**인바운드 연결**)** 탭을 클릭합니다.



단계 **6** 규칙에 대한 인증서를 업로드하거나 선택합니다.

시스템은 인증서당 하나의 규칙을 생성합니다.

단계 **7** (선택 사항). 네트워크 및 포트를 선택합니다.

자세한 내용:

- 해독 규칙 조건
- 네트워크 규칙 조건
- 포트 규칙 조건

단계 **8** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 규칙 조건을 추가합니다. 해독 규칙 조건

- 기본 정책 작업을 추가합니다. 해독 정책 기본 작업, 11 페이지
- Cisco Secure Firewall Management Center 관리 가이드의 정책 기본 작업으로 연결 로깅에 설명된 대로 기본 작업에 대한 로깅 옵션을 구성합니다 .
- 고급 정책 속성을 설정합니다.해독 정책 고급 옵션, 14 페이지
- 액세스 제어에 다른 정책 연결의 설명대로 해독 정책을 액세스 제어 정책에 연결합니다.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

다른 규칙 작업으로 암호 해독 정책 생성

Do Not Decrypt(암호 해독 안 함**)**, **Block(**차단**)**, **Block With Reset(**재설정 후 차단**)** 또는 **Monitor(**모니터링**)** 규칙 작업이 포함된 암호 해독 규칙을 생성하려면 암호 해독 정책을 생성하고 규칙을 추가하도록 정책을 수정합니다.

암호 해독 정책을 생성할 때 여러 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 및 여러 **Decrypt - Resign(**암호 해독 - 다시 서명**)** 규칙을 포함하여 여러 규칙을 동시에 생성할 수 있습니다.

프로시저

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

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

단계 **3** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **4** 정책에 고유한 **Name(**이름**)** 또는 **Description(**설명**)**을 지정합니다.

단계 **5** 암호 해독 정책 이름 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

단계 **6** **Add Rule(**규칙 추가**)**을 클릭합니다.

단계 **7** 규칙 이름을 제공합니다.

단계 **8** **Action(**작업**)** 목록에서 규칙 작업을 클릭하고 자세한 내용은 다음 섹션 중 하나를 참조하십시오.

- 해독 규칙 암호 해독 안 함 작업
- 해독 규칙 차단 작업
- 해독 규칙 모니터링 작업

단계 **9** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- 규칙 조건을 추가합니다. 해독 규칙 조건
- 기본 정책 작업을 추가합니다. 해독 정책 기본 작업, 11 페이지

- Cisco Secure Firewall Management Center 관리 가이드 의 정책 기본 작업으로 연결 로깅에 설명된 대로 기본 작업에 대한 로깅 옵션을 구성합니다.
- 고급 정책 속성을 설정합니다.해독 정책 고급 옵션, 14 페이지
- 액세스 제어에 다른 정책 연결의 설명대로 해독 정책을 액세스 제어 정책에 연결합니다.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

해독 정책 기본 작업

해독 정책의 기본 작업은 정책의 비 모니터 규칙과 일치하지 않는 해독 가능한 암호화 트래픽을 시스템이 처리하는 방법을 결정합니다. 해독 규칙이 없는 해독 정책을 구축하는 경우, 기본 작업은 네트워크의 모든 해독 가능 트래픽이 처리되는 방법을 결정합니다. 기본 작업에 의해 차단된 암호화 트래픽에 대해서는 어떠한 검사도 수행하지 않습니다.

해독 정책 기본 작업을 설정하려면:

1. 아직 하지 않았다면 management center에 로그인합니다.
2. **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Decryption(**해독**)** 버튼을 클릭합니다.
3. 해독 정책 이름 옆의 **Edit(**수정**)** ( )을 클릭합니다.
4. Default Action(기본 작업) 행의 목록에서 다음 작업 중 하나를 클릭합니다.

표 *1:* 해독 정책 기본 작업

기본 작업	암호화 트래픽에 미치는 영향
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.

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) 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) 차단 Block with Reset(차단 후 재설정) 기본 작업 상속
알 수 없는 암호 그룹	시스템에서 암호화 솔루션을 인식하지 않습니다.	기본 작업 상속	Do not decrypt(암호 해독 안 함) 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) 차단 Block with Reset(차단 후 재설정) 기본 작업 상속

유형	설명	기본 작업	사용 가능한 작업
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) 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) 차단 Block with Reset(차단 후 재설정) 기본 작업 상속
해독 오류	트래픽 해독 중에 오류가 발생했습니다.	차단	차단 Block with Reset(차단 후 재설정)

해독 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 해독 규칙 지침 및 제한 사항을 참조하십시오.

관련 항목

해독 불가 트래픽에 대한 기본 처리 설정, 13 페이지

해독 불가 트래픽에 대한 기본 처리 설정

시스템에서 해독하거나 검사하지 못하는 암호화 트래픽의 특정 유형을 처리하도록 해독 정책 레벨에서 해독 불가 트래픽 작업을 설정할 수 있습니다. 해독 규칙이 없는 해독 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.

- 해독 정책에서 기본 작업 상속.

프로시저

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

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

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

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

단계 **5** 각 필드에서 해독 정책의 기본 작업 또는 해독 불가 트래픽 유형에서 수행할 다른 작업을 선택합니다. 자세한 내용은 암호 해독을 할 수 없는 트래픽에 대한 기본 처리 옵션, 12 페이지 및 해독 정책 기본 작업, 11 페이지를 참고하십시오.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

- 암호 해독 불가능한 트래픽 작업으로 처리되는 연결에 대한 기본 로깅을 구성합니다. Cisco Secure Firewall Management Center 관리 가이드의 정책 기본 작업으로 연결 로깅을 참조하십시오.
- 구성 변경 사항을 구축합니다. 구성 변경 사항 구축의 내용을 참고하십시오.

해독 정책 고급 옵션

해독 정책의 **Advanced Settings(**고급 설정**)** 탭 페이지에는 정책이 적용되는 Snort 3에 대해 구성된 모든 매니지드 디바이스에 적용되는 전역 설정이 있습니다.

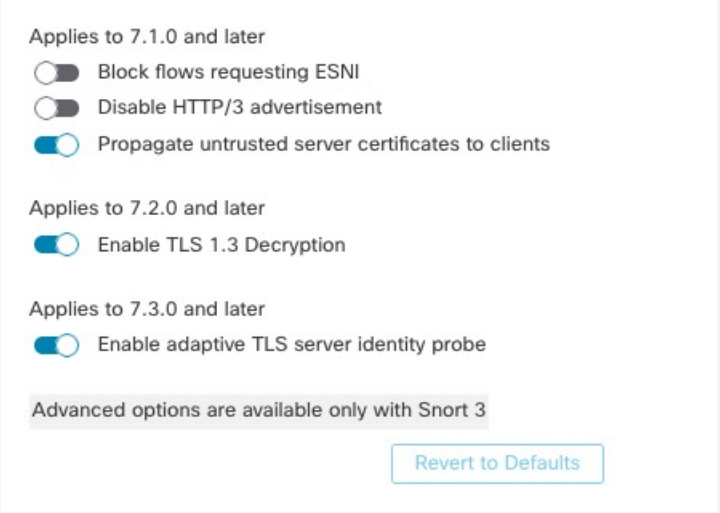
Threat Defense 기능 기록:

- 7.3 - 추가된 적응형 TLS 서버 ID 프로브를 활성화했습니다.
- 7.2 - 추가된 TLS 1.3 해독을 활성화했습니다.
- 7.1 - 초기 옵션.

해독 정책 다음을 실행하는 매니지드 디바이스에서는 고급 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 신뢰할 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.

적응형 **TLS** 서버 **ID** 프로브 활성화

TLS 1.3 암호 해독이 활성화되면 자동으로 활성화됩니다. 프로브는 서버와의 부분적인 TLS 연결이며, 그 목적은 서버 인증서를 가져와 캐시하는 것입니다. (인증서가 이미 캐시된 경우 프로브가 설정되지 않습니다.)

암호 해독 정책이 연결된 액세스 제어 정책에서 TLS 1.3 Server Identity Discovery(TLS 1.3 서버 ID 검색)가 비활성화된 경우, 신뢰할 수 없는 SNI(Server Name Indication)를 사용하려고 시도합니다.

적응형 TLS 서버 ID 프로브는 이전 릴리스와 달리 모든 연결에서 발생하는 것이 아니라 다음 조건에서 발생합니다.

- Certificate Issuer(인증서 발급자) - 암호 해독 규칙의 DN 규칙 조건에 있는 **Issuer DNs(**발급자 **DN)** 값이 일치하는 경우 일치합니다.

  자세한 내용은 고유 이름(DN) 규칙 조건을 참고하십시오.

- Certificate Status(인증서 상태) - 암호 해독 규칙에서 일치하는 **Cert Status(**인증서 상태**)** 조건이 있는 경우 일치합니다.

  자세한 내용은 인증서 상태 해독 규칙 조건을 참고하십시오.

- Internal/External Certificate(내부/외부 인증서) - 내부 인증서를 **Decrypt - Known Key(**암호 해독 - 알려진 키**)** 규칙 작업에 사용된 인증서와 일치시킬 수 있습니다. 외부 인증서는 **Certificates(**인증서**)** 규칙 조건에서 일치시킬 수 있습니다.

  자세한 내용은 알려진 키 암호 해독(수신 트래픽) 및 인증서 해독 규칙 조건를 참조하십시오.

- 애플리케이션 ID - 액세스 제어 정책 또는 암호 해독 정책에서 애플리케이션 규칙 조건과 일치시킬 수 있습니다.

  자세한 내용은 애플리케이션 규칙 조건을 참고하십시오.

- URL Category(URL 범주) - 액세스 제어 정책의 **URL** 규칙 조건과 일치시킬 수 있습니다.

  자세한 내용은 URL 규칙 조건을 참고하십시오.

참고 적응형 **TLS** 서버 검색 모드 활성화는 AWS에 구축된 Secure Firewall Threat Defense Virtual에서 지원되지 않습니다. Secure Firewall Management Center에서 관리하는 그러한 매니지드 디바이스가 있는 경우, 디바이스가 서버 인증서 추출을 시도할 때마다 연결 이벤트 **PROBE_FLOW_DROP_BYPASS_PROXY**가 증가합니다.

관련 정보

TLS 1.3 암호 해독 모범 사례, 17 페이지

TLS 1.3 암호 해독 모범 사례

권장 사항: 고급 옵션을 활성화해야 하는 경우

해독 정책 및 액세스 제어 정책에는 트래픽의 암호 해독 여부와 상관없이 트래픽 처리 방법에 영향을 주는 고급 옵션이 있습니다.

고급 옵션은 다음과 같습니다.

- 해독 정책:
  - TLS 1.3 암호 해독
  - TLS 적응형 서버 ID 프로브
- 액세스 제어 정책: TLS 1.3 서버 ID 검색

  액세스 제어 정책 설정이 암호 해독 정책 설정보다 우선적으로 적용됩니다.

다음 표를 사용하여 활성화할 옵션을 결정합니다.

TLS 적응형 서버 **ID** 프로브 설정(암호 해독 정책)	**TLS 1.3** 서버 **ID** 검색 설정(액세스 제어 정책)	결과	권장 시점
활성화됨	비활성화됨	암호 해독 정책에 해독 정책 고급 옵션, 14 페이지에 지정된 규칙 조건이 모두 포함되고 서버 인증서가 캐시되지 않은 경우 적응형 프로브가 전송됩니다.	• 액세스 제어 규칙에서 애플리케이션 또는 URL 조건을 사용하지 않음 • 트래픽 암호 해독 중
활성화됨	활성화	서버 인증서가 캐시되지 않은 경우 프로브가 항상 전송됩니다.	액세스 제어 규칙에 URL 또는 애플리케이션 조건이 있는 경우에만 사용
비활성화	활성화	서버 인증서가 캐시되지 않은 경우 프로브가 항상 전송됩니다.	권장하지 않음.
비활성화됨	비활성화	프로브가 전송되지 않습니다.	매우 제한적입니다. 트래픽을 암호 해독하지 않고 액세스 제어 규칙에서 애플리케이션 또는 URL 조건을 사용하지 않는 경우에만 사용

참고 캐시된 TLS 서버의 인증서는 특정 threat defense의 모든 Snort 인스턴스에 사용할 수 있습니다. 캐시는 CLI 명령을 사용하여 지울 수 있으며 디바이스가 재부팅될 때 자동으로 지워집니다.

참조

자세한 내용은 secure.cisco.com에서 TLS 서버 ID 검색에 대한 설명을 참조하십시오.

해독 정책 관리

해독 정책 편집기에서 다음을 수행할 수 있습니다.

- 해독 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**)** > **Decryption(**해독**)** 버튼을 클릭합니다.

단계 **3** 해독 정책 관리:

- 비교 - **Compare Policies(**정책 비교**)**를 클릭합니다. 정책 비교를 참고하십시오.
- 복사- **Copy(**복사**)** ( )를 클릭합니다.
- 생성 - **New Policy(**새 정책**)**을 클릭합니다(기본 해독 정책 생성 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 해독 정책에 추가하려면 외부 인증 증명 신뢰의 내용을 참조하십시오.
- 해독 정책이 해독 불가 트래픽을 처리하는 방법을 구성하려면 해독 불가 트래픽에 대한 기본 처리 설정, 13 페이지의 내용을 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.