액세스 제어 정책

다음 주제에서는 액세스 제어 정책을 사용하는 방법에 대해 설명합니다.

액세스 제어 정책 구성 요소

다음은 액세스 제어 정책의 주요 요소입니다.

이름 및 설명

각 액세스 제어 정책에는 고유한 이름이 있어야 합니다. 설명은 선택 사항입니다.

Inheritance Settings(상속 설정**)**

정책 상속을 사용하면 액세스 계층 제어 정책을 생성할 수 있습니다. 상위(또는 기본) 정책은 하위 항목에 대한 기본 설정을 정의하고 시행하며, 이는 특히 다중 도메인 구축에서 유용합니다.

정책 상속 설정을 통해 기본 정책을 선택할 수 있습니다. 현재 정책의 설정을 잠금 처리하여 하위 항목이 강제로 상속하도록 설정할 수도 있습니다. 하위 정책은 잠금 해제된 설정을 재정의할 수 있습니다.

Policy Assignment(정책 할당**)**

각 액세스 제어 정책은 이를 사용하는 디바이스를 식별합니다. 각 디바이스는 하나의 액세스 제어 정책에 의해 대상이 될 수 있습니다. 다중 도메인 구축에서는 도메인의 모든 디바이스가 동일한 기본 정책을 사용하도록 요구할 수 있습니다.

규칙

액세스 제어 규칙은 네트워크 트래픽 처리에 대한 세분화된 방법을 제공합니다. 액세스 제어 정책의 규칙은 상위 정책에서 상속된 규칙을 포함하여 1부터 번호가 매겨집니다. 시스템은 오름차순 규칙 번호에 따라 하향식 순서로 트래픽이 액세스 제어 규칙과 일치하는지를 확인합니다.

대부분의 경우, 시스템은 모든 규칙의 조건이 트래픽과 일치하는 첫 번째 액세스 제어 규칙에 따라 네트워크 트래픽을 처리합니다. 조건은 단순하거나 복잡할 수 있으며, 조건의 사용은 특정 라이선스에 따라 달라지는 경우가 많습니다.

기본 작업

기본 작업은 시스템이 다른 액세스 제어 구성에 의해 처리되지 않는 트래픽을 처리하고 기록하는 방법을 결정합니다. 기본 작업을 사용하여 추가 검사 없이 모든 트래픽을 차단하거나 신뢰할 수 있고, 침입 및 검색 데이터 트래픽을 검사할 수 있습니다.

액세스 제어 정책은 상위 정책에서 기본 작업을 상속할 수 있지만 이 상속을 적용할 수는 없습니다.

보안 인텔리전스

보안 인텔리전스는 악성 인터넷 콘텐츠에 대한 1차 방어선입니다. 이 기능을 사용하여 최신 IP 주소, URL, 도메인 이름 평판 인텔리전스에 따라 연결을 차단할 수 있습니다. 중요 리소스로 지속적으로 액세스할 수 있도록 차단 목록 항목을 사용자 지정 차단 안 함 목록 항목으로 재정의할 수 있습니다.

HTTP 응답

시스템이 사용자의 웹 사이트 요청을 차단하면 일반 시스템 제공 응답 페이지 또는 사용자 정의 페이지를 표시할 수 있습니다. 또한 사용자에게 경고하는 페이지를 표시할 수도 있지만 원래 요청한 사이트를 계속 진행할 수 있습니다.

로깅

액세스 제어 정책 로깅에 대한 설정을 통해 현재 액세스 제어 정책에 대한 기본 syslog 대상을 구성할 수 있습니다. 포함된 규칙 및 정책의 syslog 대상 설정이 사용자 정의 설정으로 명시적으로 무시되지 않는 한 설정은 액세스 제어 정책 및 포함된 모든 SSL, 사전 필터 및 침입 정책에 적용됩니다.

고급 액세스 제어 옵션

고급 액세스 제어 정책 설정은 일반적으로 약간의 변경이 필요하거나 변경이 필요하지 않습니다. 종종 기본 설정이 적합합니다. 수정할 수있는 고급 설정에는 트래픽 사전 처리, SSL 검사, ID 및 다양한 성능 옵션이 포함됩니다.

시스템 생성 액세스 제어 정책

사용자 디바이스의 초기 설정에 따라 시스템 제공 정책에 다음이 포함될 수 있습니다.

- 기본 액세스 제어 - 추가 검사 없이 모든 트래픽을 차단합니다.
- 기본 침입 예방 - 모든 트래픽을 허용하지만 균형 보안 및 연결성 침입 정책과 기본 침입 변수 집합을 검사합니다.
- 기본 네트워크 검색 - 검색 데이터를 검사하는 동안 모든 트래픽을 허용하지만 침입과 익스플로잇은 허용하지 않습니다.

액세스 제어 정책 요구 사항 및 사전 요건

모델 지원

Any(모든)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

액세스 제어 정책 관리

시스템에서 제공한 액세스 제어 정책을 편집하고 사용자 정의 액세스 제어 정책을 생성할 수 있습니다.

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.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을(를) 선택합니다.

단계 **2** 액세스 제어 정책 관리

- 복사- **Copy(**복사**)** ( )를 클릭합니다.
- 생성 - **New Policy(**새 정책**)**을 클릭합니다(기본 액세스 제어 정책 만들기, 4 페이지 참조).
- 삭제- **Delete(**삭제**)** ( )를 클릭합니다.
- 수정-**Edit(**수정**)** ( )를 클릭합니다. 액세스 제어 정책 수정, 5 페이지의 내용을 참조하십시오.
- 정책 잠금 또는 잠금 해제 - 액세스 제어 정책 잠금, 8 페이지의 내용을 참조하십시오.
- 상속 - 정책의 계층 보기를 확장하기 위해 하위 계층이 포함된 정책 옆의 더하기 아이콘을 클릭합니다.

- 가져오기/내보내기 - **Import/Explort(**가져오기/내보내기**)**를 클릭합니다. Cisco Secure Firewall Management Center 관리 가이드에서 가져오기/내보내기를 참조하십시오.
- 보고서- **Report(**보고서**)** ( )를 클릭합니다. 현재 정책 보고서 생성를 참조하십시오.

기본 액세스 제어 정책 만들기

새 액세스 제어 정책을 만들면 기본 작업 및 설정이 포함됩니다. 정책을 생성하면 즉시 편집 세션이 시작되므로 요구 사항에 맞게 정책을 조정할 수 있습니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을(를) 선택합니다.

단계 **2** **New Policy(**새로운 정책**)**를 클릭합니다.

단계 **3** 고유한 **Name(**이름**)**을 입력하고, 필요한 경우 **Description(**설명**)**을 입력합니다.

단계 **4** 필요한 경우 기본 정책 선택 드롭다운 목록에서 기본 정책을 선택합니다.

도메인에 액세스 제어 정책이 강제 적용되는 경우 이 단계는 선택 사항이 아닙니다. 기본 정책으로는 강제 적용된 정책 또는 그 하위 정책 중 하나를 선택해야 합니다.

기본 정책을 선택하면 기본 정책이 기본 작업을 정의하며 이 대화 상자에서 새 작업을 선택할 수 없습니다. 기본 작업으로 처리되는 연결에 대한 로깅은 기본 정책에 따라 달라집니다.

단계 **5** 기본 정책을 선택하지 않는 경우 초기 **Default Action(**기본 작업**)**을 지정합니다.

- **Block all traffic(**모든 트래픽을 차단**)**은 **Access Control: Block All Traffic(**액세스 제어**:** 모든 트래픽을 차단**)** 기본 작업을 통해 정책을 생성합니다.
- **Intrusion Prevention(**침입 방지**)**은 기본 침입 변수 집합과 연결된 **Intrusion Prevention: Balanced Security and Connectivity(**침입 방지**:** 균형 잡힌 보안 및 연결성**)** 기본 작업을 통해 정책을 생성합니다.
- **Network Discovery(**네트워크 검색**)**을 선택하면 **Network Discovery Only(**네트워크 검색 전용**)** 기본 작업이 포함된 정책을 생성합니다.

기본 작업을 선택하면 기본 작업으로 처리되는 연결 로깅이 처음에 비활성화됩니다. 나중에 정책을 수정할 때 활성화할 수 있습니다.

팁 기본적으로 모든 트래픽을 신뢰하거나 기본 정책을 선택하지만 기본 작업을 상속하지 않을 경우 기본 작업을 나중에 변경할 수 있습니다.

단계 **6** 필요에 따라 정책을 구축할 **Available Devices(**사용 가능한 디바이스**)**를 선택하고 **Add to Policy(**정책에 추가**)**(또는 드래그 앤 드롭)을 클릭하여 선택한 디바이스를 추가합니다. 표시되는 디바이스의 범위를 좁히려면 **Search(**검색**)** 필드에 검색 문자열을 입력합니다.

이 정책을 즉시 구축하려는 경우 이 단계를 수행해야 합니다.

단계 **7** **Save(**저장**)**를 클릭합니다.

편집을 위해 새 정책이 열립니다. 여기에 규칙을 추가하고 필요에 따라 다른 변경을 수행할 수 있습니다. 액세스 제어 정책 수정, 5 페이지의 내용을 참조하십시오.

관련 항목

액세스 제어 정책 기본 작업
액세스 제어 정책에 대한 대상 디바이스 설정, 13 페이지

액세스 제어 정책 수정

액세스 제어 정책을 수정할 때 정책을 잠가야 동시에 수정할 수 있는 다른 사람이 변경 사항을 재정의하지 않도록 해야 합니다.

현재 도메인에서 생성된 액세스 제어 정책만 편집할 수 있습니다. 또한 상위 액세스 제어 정책에 의해 잠긴 설정은 편집할 수 없습니다.

참고 정책을 잠그지 않은 경우 다음을 고려하십시오. 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** **Policies(**정책**)** > **Access Control(**액세스 제어**)**를 선택합니다.

단계 **2** 편집하려는 액세스 제어 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다.

단계 **3** 선택적으로, **Try New UI Layout(**새 **UI** 레이아웃 시도**)**을 클릭하여 버전 7.2에 도입된 사용자 인터페이스로 전환합니다.

이 절차에서는 이전 릴리스에서 제공되었던 레거시 **UI**(사용자 인터페이스)와 새 **UI**에서 작업을 수행하는 방법을 설명합니다. 두 인터페이스 모두 동일한 정책을 구성하며 차이점은 표시에만 있습니다.

Switch to Legacy UI(레거시 **UI**로 전환**)**를 클릭하여 레거시 UI로 돌아갈 수 있습니다.

단계 **4** (레거시 **UI**.) 기존 액세스 제어 정책을 편집합니다.

팁 여러 규칙을 Shift-클릭하거나 Control-클릭한 다음 마우스 오른쪽 버튼을 클릭하고 Edit(편집)을 선택하여 여러 규칙을 한 번에 편집할 수 있습니다. 대량 편집을 통해 규칙을 활성화 및 비활성화하고, 규칙 작업을 선택하고, 대부분의 검사 및 로깅 설정을 설정할 수 있습니다.

설정:

- 이름 및 설명 - 필드를 클릭하고 새 정보를 입력합니다.
- Default Action - **Default Action(**기본 작업**)** 드롭다운 목록에서 값을 선택합니다.
- Default Action Variable Set - **Intrusion Prevention(**침입 방지**)** 기본 작업과 관련된 변수 집합을 변경하려면 **Variables(**변수**)**()를 클릭합니다. 이때 나타나는 팝업 창에서 새로운 변수 집합을 선택하고 **OK(**확인**)**를 클릭합니다. 사용자는 또한 **Edit(**수정**)** ()을 클릭하여 선택한 변수 집합을 새 창에서 수정할 수 있습니다. 자세한 내용은 변수 관리를 참고하십시오.
- Default Action Logging - 기본 작업에 의해 처리된 연결에 대한 로깅 옵션을 변경하려면 **Logging(**로깅**)** ()을 클릭합니다. Cisco Secure Firewall Management Center 관리 가이드의 정책 기본 작업으로 연결 로깅을 참조하십시오.
- HTTP Responses - 시스템이 웹사이트 요청을 차단할 때 브라우저에 표시되는 내용을 지정하려면 **HTTP Responses(HTTP** 응답**)**를 클릭합니다. HTTP 응답 페이지 선택 섹션을 참조하십시오.
- Inheritance: Change Base Policy - 이 정책에 대한 기본 액세스 제어 정책을 변경하려면 **Inheritance Settings(**상속 설정**)**를 클릭합니다. 기본 액세스 제어 정책 선택, 10 페이지 섹션을 참조하십시오.
- Inheritance: Lock Settings in Descendants - 이 정책의 설정을 하위 정책에 적용하려면 **Inheritance Settings(**상속 설정**)**를 클릭합니다. 하위 액세스 제어 정책의 설정 잠금, 12 페이지 섹션을 참조하십시오.
- Policy Assignment: Targets - 이 정책의 대상이 되는 매니지드 디바이스를 식별하려면 **Policy Assignment(**정책 할당**)**를 클릭합니다. 액세스 제어 정책에 대한 대상 디바이스 설정, 13 페이지 섹션을 참조하십시오.
- Policy Assignment: Required in Domains - 이 정책을 하위 도메인에 적용하려면 **Policy Assignment(**정책 할당**)**를 클릭합니다. 도메인에 액세스 제어 정책 필요, 12 페이지 섹션을 참조하십시오.
- Rules - 액세스 제어 규칙을 관리하고 침입 및 파일 정책을 사용하여 악의적인 트래픽을 검사 및 차단하려면 **Rules(**규칙**)**를 클릭합니다. 액세스 제어 규칙 생성 및 수정 섹션을 참조하십시오.
- Rule Conflicts - 규칙 충돌 경고를 표시하려면 **Show rule conflicts(**규칙 충돌 표시**)**를 활성화합니다. 이전 규칙이 항상 트래픽과 먼저 일치하므로 특정 규칙이 트래픽과 일치하지 않으면 충돌이 발생합니다. 규칙 충돌을 판별하는 것은 리소스가 많이 사용될 수 있기 때문에 표시하는 데 시간이 걸릴 수 있습니다. 자세한 내용은 규칙 순서 지정 모범 사례를 참고하십시오.
- Security Intelligence - 최신 평판 인텔리전스에 따라 즉시 연결을 차단하려면 **Security Intelligence(**보안 인텔리전스**)**를 클릭합니다. 보안 인텔리전스 설정 섹션을 참조하십시오.
- Advanced Options - 사전 처리, SSL 검사, ID, 성능 및 기타 고급 옵션을 설정하려면 **Advanced(**고급**)**를 클릭합니다. 액세스 제어 정책 고급 설정, 15 페이지 섹션을 참조하십시오.

- Warnings - 액세스 제어 정책(및 해당 하위 항목 및 관련 정책)의 경고 또는 오류 목록을 보려면 **Show Warnings(**경고 표시**)**를 클릭합니다. 경고 및 오류는 트래픽 분석 및 흐름에 악영향을 미치거나 정책 배포를 방해할 수 있는 구성을 표시합니다. 경고가 없는 경우, 경고 표시가 나타나지 않습니다. 규칙 충돌 경고를 표시하려면 **Show rule conflicts(**규칙 충돌 표시**)**를 활성화합니다.

단계 **5** (새 **UI**) 기존 액세스 제어 정책을 편집합니다.

팁 왼쪽 열에서 확인란을 선택한 다음 검색 상자 옆에 있는 **Select Action(**작업 선택**)** 드롭다운 목록에서 수행할 작업을 선택하여 한 번에 여러 규칙에 대해 작업을 수행할 수 있습니다. 대량 수정은 규칙을 활성화/비활성화, 복사, 복제, 이동, 삭제 및 수정하거나 적중 횟수 또는 관련 이벤트를 보는 데 사용할 수 있습니다.

다음 설정을 변경하거나 다음 작업을 수행할 수 있습니다.

- Name and Description(이름 및 설명) - 이름 옆에 있는 **Edit(**수정**)** ( )을 클릭하고 원하는 대로 변경한 다음 **Save(**저장**)**를 클릭합니다.
- Default Action - **Default Action(**기본 작업**)** 드롭다운 목록에서 값을 선택합니다.
- Default Action Settings(기본 작업 설정) - **Cog(**톱니바퀴**)** ( )를 클릭하고 원하는 대로 변경한 다음 **OK(**확인**)**를 클릭합니다. 로깅 설정, 외부 시스템 로그 서버 또는 SNMP 트랩 서버의 위치, 침입 방지 기본 작업과 관련된 변수 집합을 구성할 수 있습니다.
- Associated Policies(연결된 정책) - 패킷 플로우에서 정책을 편집하거나 변경하려면 정책 이름 아래에 있는 패킷 플로우 표시에서 정책 유형을 클릭합니다. **Prefilter Rules(**사전 필터 규칙**)**, **SSL**, **Security Intelligence(**보안 인텔리전스**)** 및 **Identity(ID)** 정책을 선택할 수 있습니다. 필요한 경우 **Access Control(**액세스 제어**)**을 클릭하여 액세스 제어 규칙으로 돌아갑니다.
- Policy Assignment(정책 할당) - 이 정책의 대상이 되는 매니지드 디바이스를 식별하거나 하위 도메인에서 이 정책을 적용하려면 **Targeted: x devices(**대상**: x** 디바이스**)** 링크를 클릭합니다.
- Rules - 액세스 제어 규칙을 관리하고 침입 및 파일 정책을 사용하여 악의적인 트래픽을 검사 및 차단하려면 **Add Rules(**규칙 추가**)**를 클릭하거나, 기존 규칙을 마우스 오른쪽 버튼으로 클릭하고 **Edit(**편집**)**을 선택하거나 다른 적절한 작업을 선택합니다. 각 규칙의 추가 ( ) 버튼에서도 작업을 수행할 수 있습니다. 액세스 제어 규칙 생성 및 수정의 내용을 참조하십시오.
- Layout(레이아웃) - 레이아웃을 변경하려면 규칙 목록 위에 있는 **Grid/Table View(**격자/테이블 보기**)** 아이콘을 사용합니다. 그리드 보기는 보기 쉬운 레이아웃에서 색상으로 구분된 개체를 제공합니다. 테이블 보기는 한 번에 더 많은 규칙을 볼 수 있도록 요약 목록을 제공합니다. 규칙에 영향을 주지 않고 보기를 자유롭게 전환할 수 있습니다.
- Columns(열)(테이블 보기만 해당) - 규칙 목록 위에 있는 **Show/Hide Columns(**열 표시/숨기기**)** 아이콘을 클릭하여 테이블에 표시할 정보를 선택합니다. 정보가 없는 모든 열, 즉 규칙에서 해당 조건을 사용하지 않는 모든 열을 신속하게 제거하려면 **Hide Empty Columns(**빈 열 숨기기**)**를 클릭합니다. 모든 사용자 지정을 취소하려면 **Revert to Default(**기본값으로 되돌리기**)**를 클릭합니다.
- Hit Counts(적중 횟수) - 각 규칙과 일치한 연결 수에 대한 통계를 보려면 **Analyze Hit Counts(**적중 횟수 분석**)**를 클릭합니다.

- Additional Settings(추가 설정) - 정책에 대한 추가 설정을 변경하려면 패킷 플로우 라인의 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 다음 옵션 중 하나를 선택합니다.
  - **Advanced Settings(**고급 설정**)**—사전 처리, SSL 검사, ID, 성능 및 기타 고급 옵션을 설정합니다. 액세스 제어 정책 고급 설정, 15 페이지의 내용을 참조하십시오.
  - **HTTP Responses(HTTP** 응답**)**—시스템이 웹사이트 요청을 차단할 때 브라우저에 표시되는 내용을 지정합니다. HTTP 응답 페이지 선택의 내용을 참조하십시오.
  - **Inheritance Settings(**상속 설정**)** - 이 정책에 대한 기본 액세스 제어 정책을 변경하고 하위 정책에서 이 정책의 설정을 적용합니다. 기본 액세스 제어 정책 선택, 10 페이지 및 하위 액세스 제어 정책의 설정 잠금, 12 페이지을(를) 참조하십시오.
  - **Logging(**기록**)** - 정책에 대한 기본 기록 옵션을 설정합니다.

단계 **6** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

관련 항목

규칙 및 기타 정책 경고
파일 및 침입 정책을 사용한 심층 검사

액세스 제어 정책 잠금

다른 관리자가 수정하지 못하도록 액세스 제어 정책을 잠글 수 있습니다. 정책을 잠그면 변경 사항을 저장하기 전에 다른 관리자가 정책을 수정하고 변경 사항을 저장할 경우 변경 사항이 무효화되지 않습니다. 잠금을 설정하지 않은 상태에서 여러 관리자가 동시에 정책을 수정하는 경우 변경 사항을 먼저 저장한 사람이 우선하며 다른 모든 사용자의 변경 사항은 지워집니다.

잠금은 액세스 제어 정책 자체에 대한 것입니다. 정책에서 사용되는 개체에는 잠금이 적용되지 않습니다. 예를 들어, 다른 사용자가 잠긴 액세스 제어 정책에 사용되는 네트워크 개체를 편집할 수 있습니다. 정책을 명시적으로 잠금 해제할 때까지 잠금이 유지되므로 로그아웃하고 나중에 수정 사항으로 돌아올 수 있습니다.

잠긴 경우 다른 관리자는 정책에 대해 읽기 전용 액세스 권한을 갖습니다. 그러나 다른 관리자는 매니지드 디바이스에 잠긴 정책을 할당할 수 있습니다.

시작하기 전에

액세스 제어 정책을 수정할 권한이 있는 사용자 역할은 해당 역할을 잠그고 다른 사용자가 잠근 정책을 잠금 해제할 권한이 있습니다.

그러나 다른 관리자가 잠근 정책의 잠금을 해제하는 기능은 다음 권한으로 제어됩니다. **Policies(**정책**)** > **Access Control(**액세스 제어**)** > **Access Control(**액세스 제어**)** > **Policy Modify Access Control(**액세스 제어 정책 수정**)** > **Override Access Control Policy Lock(**액세스 제어 정책 잠금 재정의**)**.

맞춤형 역할을 사용하는 경우 조직에서 이 권한을 할당하지 않아 잠금 해제 기능을 제한했을 수 있습니다. 이 권한이 없으면 정책을 잠근 관리자만 잠금을 해제할 수 있습니다.

프로시저

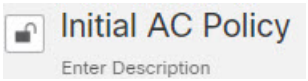
단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을(를) 선택합니다.

단계 **2** 잠그거나 잠금 해제하려는 액세스 제어 정책 옆에 있는 **Edit(**수정**)** ( )을 클릭합니다.

Lock Status(잠금 상태**)** 열에는 정책이 이미 잠겨 있는지 여부와 잠근 경우 잠근 사람이 표시됩니다. 빈 셀은 정책이 잠기지 않았음을 나타냅니다.

View(보기**)** ( )이 대신 표시되는 경우에는 설정이 상위 도메인에 속하거나 설정을 수정할 권한이 없는 것입니다. 또는 다른 사용자에 의해 잠겨 있습니다.

단계 **3** 정책을 잠그거나 잠금 해제하려면 정책 이름 옆의 잠금 아이콘을 클릭합니다.



정책이 상위 정책에서 설정을 상속하는 경우 잠금 아이콘을 클릭할 때 다음 옵션 중 하나를 선택해야 합니다.

- **Lock/Unlock This Policy(**이 정책 잠금/잠금 해제**)** - 잠금 또는 잠금 해제는 이 정책에만 적용됩니다.
- **Lock/Unlock This Policy and Parents in the Hierarchy(**이 정책 및 상위 계층 구조의 상위 잠금/잠금 해제**)** - 이 정책 및 모든 상위 정책이 잠기거나 잠금 해제됩니다. 다른 관리자가 상위 정책을 이미 잠근 경우 메시지가 표시되며 해당 상위 정책은 잠글 수 없습니다. 정책 잠금을 해제할 때 Override Access Control Policy Lock(액세스 제어 정책 잠금 재정의) 권한이 있으면 다른 사용자가 잠근 경우에도 모든 상위 정책이 잠금 해제됩니다.

액세스 제어 정책 상속 관리

상속은 다른 정책을 액세스 제어 정책에 대한 기본 정책으로 사용하는 것과 관련이 있습니다. 이렇게 하면 하나의 정책을 사용하여 여러 정책에 적용할 수 있는 몇 가지 베이스라인 특성을 정의할 수 있습니다. 상속이 어떻게 작동하는지 이해하려면 액세스 제어 정책 상속의 내용을 참조하십시오.

프로시저

단계 **1** 상속 설정을 변경하려는 액세스 제어 정책을 편집합니다. 액세스 제어 정책 수정, 5 페이지 섹션을 참조하십시오.

단계 **2** (레거시 **UI**.) 정책 상속 관리:

- Change Base Policy - 이 정책에 대한 기본 액세스 제어 정책을 변경하려면 기본 액세스 제어 정책 선택, 10 페이지에 설명된 대로 **Inheritance Settings(**상속 설정**)**를 클릭합니다.
- Lock Settings in Descendants - 이 정책의 설정을 하위 정책에 적용하려면 하위 액세스 제어 정책의 설정 잠금, 12 페이지에 설명된 대로 **Inheritance Settings(**상속 설정**)**를 클릭합니다.
- Required in Domains - 이 정책을 하위 도메인에 적용하려면 도메인에 액세스 제어 정책 필요, 12 페이지에 설명된 대로 **Policy Assignment(**정책 할당**)**를 클릭합니다.
- Inherit Settings from Base Policy - 기본 액세스 제어 정책에서 설정을 상속하려면 **Security Intelligence(**보안 인텔리전스**)**, **HTTP Responses(HTTP** 응답**)** 또는 **Advanced(**고급**)**을 클릭하고 기본 정책에서 액세스 제어 정책 설정 상속, 11 페이지의 지침에 따라 진행합니다.

단계 **3** (신규 **UI**) 정책 상속 관리:

- Change Base Policy — 이 정책에 대한 기본 액세스 제어 정책을 변경하려면 패킷 플로우 라인 끝에 있는 **More(**추가**)** 드롭다운 화살표에서 **Inheritance Settings(**상속 설정**)**를 선택하고 기본 액세스 제어 정책 선택, 10 페이지에 설명된 대로 진행합니다.
- Lock Settings in Descendants - 이 정책의 설정을 하위 정책에 적용하려면 패킷 플로우 라인 끝에 있는 **More(**추가**)** 드롭다운 화살표에서 **Inheritance Settings(**상속 설정**)**를 선택하고 하위 액세스 제어 정책의 설정 잠금, 12 페이지에 설명된 대로 진행합니다.
- Required in Domains - 이 정책을 하위 도메인에 적용하려면 **Targeted: x devices(**대상**: x** 디바이스**)**를 클릭하고 도메인에 액세스 제어 정책 필요, 12 페이지에 설명된 대로 진행합니다.
- Inherit Settings from Base Policy - 기본 액세스 제어 정책에서 설정을 상속하려면 패킷 플로우 라인 끝에 있는드롭다운 화살표에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭하거나 **HTTP Responses(HTTP** 응답**)** 또는 **Advanced Settings(**고급 설정**)**를 클릭하고 기본 정책에서 액세스 제어 정책 설정 상속, 11 페이지의 지침에 따라 진행합니다.

기본 액세스 제어 정책 선택

하나의 액세스 제어 정책을 다른 정책에 대한 기본(상위)으로 사용할 수 있습니다. 잠금 해제된 설정을 변경할 수 있지만 기본적으로 하위 정책은 기본 정책에서 설정을 상속받습니다.

현재 액세스 제어 정책에 대한 기본 정책을 변경하면 시스템은 새 기본 정책에서 잠긴 설정으로 현재 정책을 갱신합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Inheritance Settings(**상속 설정**)**(**Legacy UI(**레거시 **UI)**)를 클릭합니다. **New UI(**새 **UI)**의 패킷 플로우 라인 끝에 있는 **More(**더 보기**)**드롭다운 화살표에서 **Inheritance Settings(**상속 설정**)**를 선택합니다.

단계 **2** **Select Base Policy(**기본 정책 선택**)** 드롭다운 목록에서 정책을 선택합니다.

다중 도메인 구축의 경우 현재 도메인에서 액세스 제어 정책이 필요할 수 있습니다. 기본 정책으로 시행된 정책 또는 그 하위 항목 중 하나만 선택할 수 있습니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

기본 정책에서 액세스 제어 정책 설정 상속

새 하위 정책은 기본 정책에서 많은 설정을 상속받습니다. 이 설정이 기본 정책에서 잠금 해제되어 있으면 재정의할 수 있습니다.

나중에 기본 정책의 설정을 다시 상속하면 시스템은 기본 정책의 설정을 표시하고 컨트롤을 흐릿하게 표시합니다. 하지만 시스템은 사용자가 변경한 내용을 저장하고 상속을 다시 사용하지 않도록 설정하면 복원합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Security Intelligence(**보안 인텔리전스**)**, **HTTP Responses(HTTP** 응답**)** 또는 **Advanced(**고급**)**(**Legacy UI(**레거시 **UI)**)를 클릭합니다. **New UI(**새 **UI)**에서 **Security Intelligence(**보안 인텔리전스**)**를 클릭하거나 패킷 플로우 라인 끝 있는 **More(**추가**)** 드롭다운 화살표에서 **HTTP Responses(HTTP** 응답**)** 또는 **Advanced Settings(**고급 설정**)**을 선택합니다.

단계 **2** 상속할 각 설정에 대해 **Inherit from base policy(**상속 정책에서 상속**)** 확인란을 선택합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **3** **Save(**저장**)**를 클릭합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

하위 액세스 제어 정책의 설정 잠금

모든 하위 정책에 설정을 적용하려면 액세스 제어 정책에서 설정을 잠급니다. 하위 정책은 잠금 해제된 설정을 재정의할 수 있습니다.

설정을 잠그면 시스템은 하위 정책에서 이미 적용된 재정의를 저장하므로 설정을 다시 해제하면 재정의를 복원할 수 있습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Inheritance Settings(**상속 설정**)(Legacy UI(**레거시 **UI))**를 클릭합니다. **New UI(**새 **UI)**의 패킷 플로우 라인 끝에 있는 **More(**더 보기**)**드롭다운 화살표에서 **Inheritance Settings(**상속 설정**)**를 선택합니다.

단계 **2** Child Policy Inheritance Settings(하위 정책 상속 설정) 영역에서 잠그려는 설정을 선택합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다.

단계 **3** **OK(**확인**)**를 클릭하여 상속 설정을 저장합니다.

단계 **4** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

도메인에 액세스 제어 정책 필요

도메인의 모든 디바이스가 동일한 기본 액세스 제어 정책 또는 그 하위 정책 중 하나를 사용하도록 요구할 수 있습니다. 이 절차는 다중 도메인 구축에만 해당됩니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Policy Assignments(**정책 할당**) (Legacy UI(**레거시 **UI))**를 클릭합니다. **New UI(**새 **UI)**에서 **Targeted: x devices(**대상**: x** 디바이스**)** 링크를 클릭합니다.

단계 **2** **Required on Domains(**도메인에 대한 필수 요소**)**를 클릭합니다.

단계 **3** 도메인 목록을 구축합니다.

- Add(추가) - 현재 액세스 제어 정책을 적용할 도메인을 선택한 다음 **Add(**추가**)**를 클릭하거나 선택한 도메인 목록으로 끌어다 놓습니다.
- Delete(삭제) - 리프 도메인 옆에 있는 **Delete(**삭제**)** ( )을 클릭하거나 상위 도메인을 오른쪽 클릭하고 **Delete Selected(**선택 항목 삭제**)**를 선택합니다.
- Search(검색) - 검색 필드에 검색 문자열을 입력합니다. **Clear(**지우기**)** ( )을 클릭하여 검색 내용을 삭제합니다.

단계 **4** **OK(**확인**)**를 클릭하여 도메인 적용 설정을 저장합니다.

단계 **5** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

액세스 제어 정책에 대한 대상 디바이스 설정

액세스 제어 정책은 이를 사용하는 디바이스를 지정합니다. 각 디바이스는 하나의 액세스 제어 정책에 의해 대상이 될 수 있습니다. 다중 도메인 구축에서는 도메인의 모든 디바이스가 동일한 기본 정책을 사용하도록 요구할 수 있습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Policy Assignments(**정책 할당**)** (**Legacy UI(**레거시 **UI)**)를 클릭합니다. **New UI(**새 **UI)**에서 **Targeted: x devices(**대상**: x** 디바이스**)** 링크를 클릭합니다.

단계 **2** **Targeted Devices(**대상 디바이스**)**에 대상 목록을 만듭니다.

- Add(추가) - 하나 이상의 **Available Devices(**사용 가능한 디바이스**)**를 선택한 다음 **Add to Policy(**정책에 추가**)**를 클릭하거나 **Selected Devices(**선택한 디바이스**)** 목록으로 드래그앤 드롭합니다.
- Delete(삭제) - 단일 디바이스 옆에 있는 **Delete(**삭제**)** ( )을 클릭하거나 여러 디바이스를 선택하고 오른쪽 클릭한 다음 **Delete Selected(**선택 항목 삭제**)**를 선택합니다.
- Search(검색) - 검색 필드에 검색 문자열을 입력합니다. **Clear(**지우기**)** ( )을 클릭하여 검색 내용을 삭제합니다.

Impacted Devices(영향을 받는 디바이스**)**에서 시스템은 할당된 액세스 제어 정책이 현재 정책의 하위 디바이스를 나열합니다. 현재 정책의 변경 사항은 이러한 디바이스에 영향을 줍니다.

단계 **3** (다중 도메인 구축에만 해당) 필요에 따라 **Required on Domains(**도메인에 대한 필수 요소**)**를 클릭하여 선택한 하위 도메인의 모든 디바이스가 동일한 기본 정책을 사용하도록 요구할 수 있습니다.

단계 **4** **OK(**확인**)**를 클릭하여 대상 디바이스 설정을 저장합니다.

단계 **5** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

액세스 제어 정책용 로깅 설정

액세스 제어 정책에 대한 기본 시스템 로그 대상 및 시스템 로그 알림을 구성할 수 있습니다. 포함된 규칙 및 정책의 syslog 대상 설정이 사용자 정의 설정으로 명시적으로 무시되지 않는 한 설정은 액세스 제어 정책 및 포함된 모든 SSL/TLS 암호 해독, 사전 필터 및 침입 정책에 적용됩니다.

기본 작업으로 처리되는 연결에 대한 로깅은 초기에는 비활성화됩니다.

IPS and File and Malware Settings(IPS와 파일 및 악성코드 설정)는 일반적으로 시스템 로그 메시지를 보내는 페이지 위쪽의 옵션을 선택한 후에만 적용됩니다.

기본 **Syslog** 설정

- **Send using specific syslog alert(**특정 **syslog** 알림을 사용하여 전송**)** - 이 옵션을 선택하면 Cisco Secure Firewall Management Center 관리 가이드에 있는 시스템 로그 알림 응답 생성의 지침에 따라 구성된 대로 선택한 시스템 로그 알림을 기반으로 이벤트가 전송됩니다. 목록에서 syslog 알림을 선택하거나 이름, 로깅 호스트, 포트, 기능 및 심각도를 지정하여 syslog 알림을 추가할 수 있습니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드의 침입 시스템 로그 알림에 대한 시설 및 심각도를 참조하십시오. 이 옵션은 모든 디바이스에 적용할 수 있습니다.
- 디바이스에 구축된 위협 방어 플랫폼 설정 정책에 구성된 시스템 로그 설정 사용 - 이 옵션을 선택하고 심각도를 선택하면 선택한 심각도와 함께 연결 또는 침입 이벤트가 플랫폼 설정에서 구성된 시스템 로그 수집기로 전송됩니다. 이 옵션을 사용하면 플랫폼 설정에서 구성하고 액세스 제어 정책의 설정을 다시 사용하여 syslog 구성을 통합할 수 있습니다. 이 섹션에서 선택한 심각도는 모든 연결 및 침입 이벤트에 적용됩니다. 기본 심각도는 ALERT입니다.

  이 옵션은 Secure Firewall Threat Defense 디바이스 6.3 이상에만 적용됩니다.

IPS 설정

- **Send Syslog messages for IPS events(IPS** 이벤트에 대한 **Syslog** 메시지 전송**)** — IPS 이벤트를 시스템 로그 메시지로 전송합니다. 재정의하지 않는 한 위에 설정된 기본값이 사용됩니다.
- **Show/Hide Overrides(**재정의 표시/숨기기**)** - 기본 시스템 로그 대상 및 심각도를 사용하려는 경우 이러한 옵션을 비워 둡니다. 그렇지 않으면 IPS 이벤트에 대해 다른 시스템 로그 서버 대상을 설정하고 이벤트의 심각도를 변경할 수 있습니다.

파일 및 악성코드 설정

- **Send Syslog messages for File and Malware events(**파일 및 악성코드 이벤트에 대한 시스템 로그 메시지 전송**)**—파일 및 악성 프로그램 이벤트를 시스템 로그 메시지로 보냅니다. 재정의하지 않는 한 위에 설정된 기본값이 사용됩니다.
- **Show/Hide Overrides(**재정의 표시/숨기기**)** - 기본 시스템 로그 대상 및 심각도를 사용하려는 경우 이러한 옵션을 비워 둡니다. 그렇지 않으면 파일 및 악성코드 이벤트에 대해 다른 시스템 로그 서버 대상을 설정하고 이벤트의 심각도를 변경할 수 있습니다.

액세스 제어 정책 고급 설정

고급 액세스 제어 정책 설정은 일반적으로 약간의 변경이 필요하거나 변경이 필요하지 않습니다. 기본 설정은 대부분의 배포에 적합합니다. 액세스 제어 정책의 여러 고급 사전 처리 및 성능 옵션은 Cisco Secure Firewall Management Center 관리 가이드 의 침입 규칙 업데이트에 설명된 규칙 업데이트에 의해 수정될 수 있습니다.

보기 아이콘(**View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

주의 트래픽 검사를 일시적으로 중단하는 Snort 프로세스를 재시작하는 고급 설정 수정 목록은 구축 또는 활성화 시 Snort 프로세스를 재시작하는 컨피그레이션을 확인하세요. 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.

일반 설정

옵션	설명
연결 이벤트에 저장하고자 하는 최대 **URL** 문자	사용자가 요청한 각 URL에 저장하는 문자 수를 사용자 정의합니다. 사용자가 최초 차단을 건너뛴 후 웹사이트를 다시 차단하기 전에 걸린 시간을 맞춤화하려면, 차단된 웹사이트의 사용자 우회 시간 제한 설정를 참고하십시오.
인터랙티브 차단을 허용하여 다음 시간**(**초**)** 동안 차단 바이패스	차단된 웹사이트의 사용자 우회 시간 제한 설정의 내용을 참조하십시오.
URL 캐시 누락 조회 다시 시도	시스템에서 로컬로 저장된 범주 및 평판이 없는 URL을 처음 발견하면 나중에 해당 URL을 더 빠르게 처리할 수 있도록 클라우드에서 해당 URL을 조회하고 결과를 로컬 데이터 저장소에 추가합니다. 이 설정은 시스템이 클라우드에서 URL의 범주 및 평판을 조회해야 할 때 수행할 작업을 결정합니다. 기본적으로 이 설정은 활성화되어 있습니다. 시스템은 클라우드에서 URL의 평판 및 범주를 확인하는 동안 트래픽을 일시적으로 지연시키고 클라우드 판정을 사용하여 트래픽을 처리합니다. 이 설정을 비활성화하는 경우: 시스템이 로컬 캐시에 없는 URL을 발견하면 트래픽은 분류되지 않고 평판 없는 트래픽에 대해 설정된 규칙에 따라 즉시 전달되고 처리됩니다. 수동 구축에서 시스템은 패킷을 보유할 수 없기 때문에 조회를 재시도하지 않습니다.

옵션	설명
Threat Intelligence Director 활성화	구성된 디바이스에 TID 데이터 게시를 중지하려면 이 옵션을 비활성화합니다.
DNS 트래픽에 대한 평판 시행 활성화	이 옵션은 URL 필터링 성능 및 효율성 향상을 위해 기본적으로 활성화됩니다. 자세한 내용 및 추가 지침은 DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별 및 하위 주제를 참조하십시오.
정책 적용 중에 트래픽 검사	특정 설정이 Snort 프로세스 재시작을 필요로 하지 않는 경우 구축 설정을 변경할 때 트래픽을 검사하려면 정책 적용 중 트래픽 검사가 기본 값(활성화)로 설정되어 있는지 확인해야 합니다. 이 옵션이 활성화된 경우 리소스 수요로 인해 약간의 패킷이 검사 없이 삭제될 수 있습니다. 또한 일부 컨피그레이션을 구축하면 Snort 프로세스가 재시작되므로 트래픽 검사가 중단됩니다. 이 중단 기간 동안 트래픽이 삭제되는지 아니면 추가 검사 없이 통과되는지는 대상 디바이스가 트래픽을 처리하는 방법에 따라 달라집니다. 자세한 내용은 Snort® 재시작 시나리오를 참조하십시오.

관련 정책

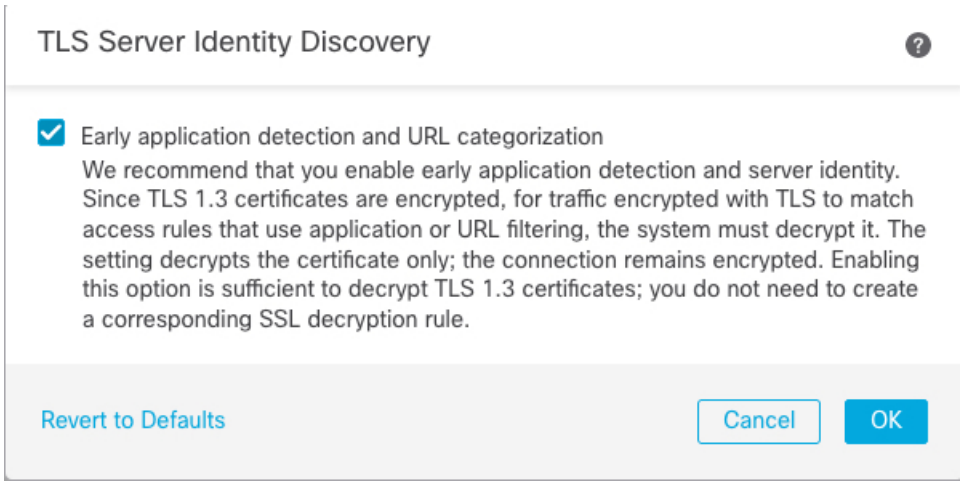
고급 설정을 사용해 액세스 제어와 하위 정책(암호 해독, ID, 사전 필터)을 연결하려면 액세스 제어에 다른 정책 연결, 21 페이지의 내용을 참조하십시오.

TLS 서버 ID 검색

RFC 8446에서 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.

액세스 제어 정책에 대한 고급 설정을 구성하는 경우 *TLS 서버 ID 검색*이라고 하는 기능을 활성화할 수 있습니다.

TLS 서버 ID 검색을 활성화하려면 **Advanced(고급)** 탭을 클릭하고 설정에 대해 **Edit(수정)** ( )을 클릭한 다음 **Early application detection and URL categorization(조기 애플리케이션 탐지 및 URL 분류)**을 선택합니다.



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

참고

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

네트워크 분석 및 침입 정책

고급 네트워크 분석 및 침입 정책을 설정하면 다음을 수행할 수 있습니다.

- 시스템이 트래픽을 검사하는 방법을 정확히 결정하기 전에 통과해야 하는 패킷을 검사하는 데 사용되는 침입 정책 및 관련 변수 세트를 지정합니다.
- 다양한 사전 처리 옵션을 제어하는 액세스 제어 정책의 기본 네트워크 분석 정책을 변경합니다
- 사전 처리 옵션을 특정 보안 영역, 네트워크, VLAN에 맞춰 조정하기 위해 맞춤형 네트워크 분석 규칙과 네트워크 분석 정책을 사용합니다.

자세한 내용은 네트워크 분석 및 침입 정책에 대한 고급 액세스 컨트롤 설정를 참고하십시오.

위협 방어 서비스 정책

특정 트래픽 클래스에 서비스를 적용하기 위해 위협 방어 서비스 정책을 사용할 수 있습니다. 예를 들어 모든 TCP 애플리케이션에 적용되는 것과 반대로, 특정 TCP 애플리케이션과 관련된 시간 제한

컨피그레이션을 만드는 서비스 정책을 사용할 수 있습니다. 이 정책은 threat defense 디바이스에만 적용되며 다른 디바이스 유형에 대해서는 무시됩니다. 서비스 정책 규칙은 액세스 제어 규칙 이후에 적용됩니다. 자세한 내용은 서비스 정책를 참고하십시오.

파일 및 악성코드 설정

파일 및 악성코드 탐지 성능 및 저장 조정은 파일 컨트롤 및 악성코드 대응 에 대한 성능 옵션과 관련된 정보를 제공합니다.

포트스캔 위협 탐지

포트스캔 탐지기는 모든 유형의 트래픽에서 포트스캔 활동을 탐지하고 방지하여 최종 공격으로부터 네트워크를 보호하도록 설계된 위협 탐지 메커니즘입니다. 포트스캔 트래픽은 허용된 트래픽과 거부된 트래픽 모두에서 효율적으로 탐지할 수 있습니다.을 참조하십시오.

엘리펀트 플로우 설정

엘리펀트 플로우는 Snort 코어에 대한 위협을 유발할 수 있는 크고 긴 지속 시간의 플로우입니다. 시스템 스트레스, CPU 호깅, 패킷 삭제 등을 줄이기 위해 엘리펀트 플로우에 적용할 수 있는 두 가지 작업이 있습니다. 이러한 작업은 다음과 같습니다.

- Bypass any or all applications(일부 또는 모든 애플리케이션 우회) - 이 작업은 Snort 검사에서 플로우를 우회합니다.
- Throttle(스로틀) - 이 작업은 엘리펀트 플로우에 동적 속도 제한 정책(10% 감소)을 적용합니다.

IAB(Intelligent Application Bypass) 설정

IAB(Intelligent Application Bypass)는 트래픽이 검사 성능 및 플로우 임계값 조합을 초과하는 경우 건너뛸 애플리케이션이나 우회할 테스트를 지정하는 전문가 레벨 컨피그레이션입니다. 자세한 내용은 IAB(Intelligent Application Bypass)를 참고하십시오.

전송/네트워크 레이어 전처리 설정

고급 전송 및 네트워크 전처리 설정은 액세스 제어 정책을 배포하는 모든 네트워크, 영역 및 VLAN에 글로벌로 적용됩니다. 네트워크 분석 정책이 아닌 액세스 제어 정책에서 이 고급 설정을 구성합니다. 자세한 내용은 고급 전송/네트워크 전처리기 설정를 참고하십시오.

탐지 향상 설정

고급 탐지 향상 설정은 다음을 가능하게 하는 적응형 프로파일을 구성할 수 있습니다.

- 액세스 제어 규칙에서 파일 정책 및 애플리케이션을 사용합니다.
- 침입 규칙에서 서비스 메타 데이터를 사용합니다.
- 수동 구축에서는 네트워크 호스트 운영 시스템에 기반해 패킷 프래그먼트 및 TCP 스트림의 리어셈블리를 개선합니다.

자세한 내용은 적응형 프로파일를 참고하십시오.

성능 설정 및 대기 시간 기반 성능 설정

침입 방지 성능 조정 정보는 시도된 침입의 트래픽을 분석할 때 시스템 성능 향상에 관한 정보를 제공합니다.

레이턴시 기반 성능 설정 관련 정보는 패킷 및 침입 규칙 레이턴시 임계값 구성을 참조하십시오.

암호화된 가시성 엔진

이 기능에 대한 자세한 내용은 암호화된 가시성 엔진을 참조하십시오.

암호화된 가시성 엔진

암호화된 가시성 엔진(EVE)은 암호를 해독하지 않고도 암호화된 세션에 대한 더 많은 가시성을 제공하는 데 사용됩니다. 암호화된 세션에 대한 이러한 인사이트는 Cisco의 VDB(취약성 데이터베이스)에 패키지된 Cisco의 오픈 소스 라이브러리에서 가져옵니다. 라이브러리는 암호화된 수신 세션을 핑거프린트하고 분석하여 알려진 핑거프린트 집합과 일치시킵니다. 이 알려진 핑거프린트 데이터베이스는 Cisco VDB에서도 사용할 수 있습니다.

액세스 제어 정책의 **Advanced(**고급**)** 탭에 있는 **Encrypted Visibility Engine (EVE)(**암호화된 가시성 엔진 **(EVE))** 토글 버튼을 사용하여 EVE를 활성화하거나 비활성화합니다. management center 7.1에서 암호화된 가시성 엔진은 암호화된 트래픽에 대한 더 많은 가시성을 제공하는 데만 사용됩니다. 해당 트래픽에 대한 작업을 시행하지 않습니다.

management center 7.2에서 EVE(암호화된 가시성 엔진)에는 다음과 같은 향상된 기능이 있습니다.

- management center 7.2에서 EVE를 사용하려면 디바이스에 유효한 위협 라이선스가 있어야 합니다. 위협 라이선스가 없으면 정책에 경고가 표시되고 구축이 허용되지 않습니다.
- EVE에서 파생된 정보를 사용하여 트래픽에 대한 액세스 제어 정책 작업을 수행할 수 있습니다.
- Cisco Secure Firewall 7.2에 포함된 VDB에는 높은 신뢰도 값으로 EVE에서 탐지한 일부 프로세스에 애플리케이션을 할당할 수 있는 기능이 있습니다. 또는 맞춤형 애플리케이션 탐지기를 생성하여 다음을 수행할 수 있습니다.
  - EVE 탐지 프로세스를 새로운 사용자 정의 애플리케이션에 매핑합니다.
  - EVE 탐지 프로세스에 애플리케이션을 할당하는 데 사용되는 프로세스 신뢰도의 기본 제공 값을 재정의합니다.

    맞춤형 애플리케이션 탐지기 설정 및 EVE 프로세스 할당 지정를 참조하십시오.
- EVE는 암호화된 트래픽에서 클라이언트 Hello 패킷을 생성한 클라이언트의 운영 체제 유형 및 버전을 탐지할 수 있습니다.
- EVE는 QUIC(빠른 UDP 인터넷 연결) 트래픽의 핑거프린트 및 분석도 지원합니다. Client Hello 패킷의 서버 이름이 **Connection Events(**연결 이벤트**)** 페이지의 URL 필드에 표시됩니다.

참고 암호화된 가시성 엔진 기능은 Snort 3을 실행하는 management center 매니지드 디바이스에서만 지원됩니다. 이 기능은 Snort 2 디바이스, device manager 매니지드 디바이스 또는 CDO에서 지원되지 않습니다.

암호화된 가시성 엔진 토글 버튼이 활성화되고 액세스 제어 정책이 구축되면 시스템을 통해 라이브 트래픽 전송을 시작할 수 있습니다. **Connection Events(**연결 이벤트**)** 페이지에서 로깅된 연결 이벤트를 볼 수 있습니다. 연결 이벤트에 액세스하려면 management center에서 **Analysis(**분석**)** > **Connections(**연결**)** > **Events(**이벤트**)**로 이동하여 **Table View of Connection Events(**연결 이벤트의 테이블 보기**)** 탭을 클릭합니다. **Analysis(**분석 **)** 메뉴 아래에 있는 **Unified Events(**통합 이벤트**)** 뷰어에서 연결 이벤트 필드를 볼 수도 있습니다. 암호화 가시성 엔진은 연결을 시작한 클라이언트 프로세스, 클라이언트의 OS 및 프로세스에 악성코드가 포함되어 있는지 여부를 식별할 수 있습니다.

Connection Events(연결 이벤트**)** 페이지에서 암호화된 가시성 엔진에 대해 다음 열이 추가됩니다. 언급된 열을 명시적으로 활성화해야 합니다.

- 암호화된 가시성 프로세스 이름
- 암호화된 가시성 프로세스 신뢰도 점수
- 암호화된 가시성 위협 신뢰도
- 암호화된 가시성 위협 신뢰도 점수
- 탐지 유형

이러한 필드에 대한 자세한 내용은 Cisco Firepower Management Center 관리 가이드의 연결 및 보안 인텔리전스 이벤트 필드 섹션을 참조하십시오.

참고 **Connection Events(**연결 이벤트**)** 페이지에서 프로세스에 애플리케이션이 할당된 경우 **Detection Type(**탐지 유형**)** 열에 EVE에서 클라이언트 애플리케이션을 식별했음을 나타내는 암호화된 가시성 엔진이 표시됩니다. 프로세스 이름에 애플리케이션을 할당하지 않은 경우 **Detection Type(**탐지 유형**)** 열에 클라이언트 애플리케이션을 식별한 엔진이 AppID임을 나타내는 **AppID**가 표시됩니다.

두 개의 대시보드에서 분석 정보를 볼 수 있습니다. **Overview(**개요**)** > **Dashboards(**대시보드**)** 아래에서 **Dashboard(**대시보드**)**를 클릭합니다. **Summary Dashboard(**요약 대시보드**)** 창에서 스위치 대시보드 링크를 클릭하고 드롭다운 상자에서 **Application Statistics(**애플리케이션 통계**)**를 선택합니다. 다음 두 개의 대시보드를 보려면 **Encrypted Visibility Engine(**암호화 가시성 엔진**)** 탭을 선택합니다.

- **Top Encrypted Visibility Engine Discovered Processes(**상위 **TLS** 핑거프린트 발견 프로세스**)** - 네트워크에서 사용 중인 상위 TLS 프로세스 이름 및 연결 수를 표시합니다. 테이블에서 프로세스 이름을 클릭하면 프로세스 이름별로 필터링된 **Connection Events(**연결 이벤트**)** 페이지의 필터링된 보기를 볼 수 있습니다.
- **Connections by Encrypted Visibility Engine(**암호화된 가시성 엔진에 의한 연결**)** — 신뢰 수준(Very High(매우 높음), Very Low(매우 낮음) 등)별로 연결을 표시합니다. 테이블에서 위협 신뢰

도 레벨을 클릭하여 신뢰도 레벨별로 필터링된 **Connection Events(**연결 이벤트**)** 페이지의 필터링된 보기를 볼 수 있습니다.

management center 7.2에서 EVE는 SSL 세션의 운영 체제 유형 및 버전을 탐지할 수 있습니다. 애플리케이션, 패키지 관리 소프트웨어 등을 실행하는 등 운영 체제를 정상적으로 사용하면 OS 탐지가 트리거될 수 있습니다. 클라이언트 OS 탐지를 보려면 EVE 토글을 활성화하는 것 외에도 **Policies(**정책**)** > **Network Discovery(**네트워크 검색**)**에서 **Hosts(**호스트**)**를 활성화해야 합니다. 호스트 IP 주소에서 가능한 운영 체제 목록을 보려면 **Analysis(**분석**)** > **Hosts(**호스트**)** > **Network Map(**네트워크 맵**)**을 클릭한 다음 필요한 호스트를 선택합니다.

액세스 제어에 다른 정책 연결

액세스 제어 정책의 고급 설정을 사용하여 다음 각각의 하위 정책 중 하나를 액세스 제어 정책과 연결합니다.

- 사전 필터 정책 — 제한된 네트워크(레이어 4) 외부-헤더 기준을 사용하여 초기에 트래픽 처리를 수행합니다.
- SSL 정책 — SSL(Secure Socket Layer) 또는 TLS(Transport Layer Security)로 암호화된 애플리케이션 레이어 프로토콜 트래픽을 모니터링, 암호 해독, 차단하거나 허용합니다.

주의 *Snort 2*에만 해당됩니다. SSL 정책을 추가 또는 제거하면 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.

- ID 정책 — 영역 및 트래픽과 관련된 인증 방법에 따라 사용자 식별을 수행합니다.

시작하기 전에

SSL 정책을 액세스 제어 정책과 연결하기 전에 액세스 제어 정책 고급 설정, 15 페이지에서 TLS 서버 ID 검색에 대한 정보를 검토합니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **Advanced(**고급**)** 탭(레거시 **UI**)를 클릭합니다. 새 **UI**의 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **2** 해당하는 Policy Settings(정책 설정) 영역에서 **Edit(**수정**)** ( )을 클릭합니다.

보기 아이콘(**View(**보기**)** ( ))이 대신 표시되는 경우에는 설정이 상위 정책에서 상속되거나 설정을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **3** 드롭다운 목록에서 정책을 선택합니다.

사용자가 생성한 정책을 선택할 경우, 표시된 편집 내용을 클릭하여 정책을 수정할 수 있습니다.

단계 **4** **OK(**확인**)**를 클릭합니다.

단계 **5** **Save(**저장**)**를 클릭하여 액세스 제어 정책을 저장합니다.

다음에 수행할 작업

- Deploy configuration changes(구성 변경 사항 구축)참조.

관련 항목

Snort® 재시작 시나리오

정책 적중 횟수 보기

적중 횟수는 정책 규칙 또는 기본 작업이 연결과 일치한 횟수를 나타냅니다. 정책 적중 횟수는 정책과 일치하는 연결의 첫 번째 패킷에 대해서만 증가합니다. 이 정보를 사용하여 규칙의 효과를 식별할 수 있습니다. 적중 횟수 정보는 액세스 제어 및 threat defense 디바이스에 적용되는 사전 필터 규칙에만 사용할 수 있습니다.

참고

- 리부팅 및 업그레이드 시에도 개수가 유지됩니다.
- 개수는 HA 쌍 또는 클러스터의 각 유닛에서 개별적으로 유지 관리됩니다.
- 디바이스에서 구축이나 작업이 진행 중일 때 적중 횟수 정보를 얻을 수 없습니다.
- **show rule hits** 명령을 사용하여 디바이스 CLI에서 규칙 적중 횟수 정보를 볼 수도 있습니다.
- 액세스 제어 정책 페이지에서 Hit Count(적중 횟수) 페이지에 액세스한 경우 사전 필터 규칙을 보거나 편집할 수 없으며 그 반대의 경우도 마찬가지입니다.

시작하기 전에

맞춤형 사용자 역할을 사용하는 경우 역할에 다음 권한이 포함되어 있는지 확인합니다.

- View Device(디바이스 보기) - 적중 횟수를 확인합니다.
- 적중 횟수를 새로 고치려면 디바이스를 수정합니다.

프로시저

단계 **1** 액세스 제어 정책 또는 사전 필터 정책 편집기에서 페이지 오른쪽 상단의 **Analyze Hit Counts(**적중 횟수 분석**)**를 클릭합니다.

단계 **2** Hit Count(적중 횟수) 페이지에서 **Select a device(**디바이스 선택**)** 드롭다운 목록에서 디바이스를 선택합니다.

이 디바이스에 대한 적중 횟수를 생성하는 것이 처음이 아닌 경우 드롭다운 상자 옆에 마지막으로 조회된 적중 횟수 정보가 표시됩니다. 또한 **Last Deployed(**마지막 구축**)** 시간을 확인하여 최근 정책 변경 내용을 확인합니다.

단계 **3** **Fetch Current Hit Count(**현재 적중 횟수 가져오기**)**를 클릭하여 적중 횟수 데이터를 가져오거나, 이미 적중 횟수 데이터를 가져온 경우 새 숫자를 확인하려면 **Refresh(**새로 고침**)**를 클릭합니다.

단계 **4** 데이터를 보고 분석합니다.

다음을 수행할 수 있습니다.

- 이러한 정책에 대한 적중 횟수를 전환하려면 **Prefilter(**사전 필터**)** 또는 **AC Policy(AC** 정책**)**를 클릭합니다.
- **Filter Rules/Policy(**필터 규칙/정책**)** 상자에 검색 문자열을 입력하여 특정 규칙을 검색합니다.
- **Filter by(**필터링 기준**)** 필드에서 이러한 옵션을 선택하여 목록을 적중 규칙 또는 규칙 적중 안 함으로 광범위하게 제한합니다. 적중 규칙을 볼 때 **In Last(**마지막 날짜**)** 필드에서 시간 범위를 선택하여 목록을 추가로 제한할 수 있습니다(예: 지난 1일).
- **Cog(**톱니바퀴**)** ()을 클릭하고 표시할 열을 선택하여 표시된 열을 변경합니다.
- 규칙 이름을 클릭하여 편집하거나 마지막 열의 **View(**보기**)** ()을 클릭하여 규칙 세부 정보를 봅니다. 규칙 이름을 클릭하면 편집할 수 있는 정책 페이지에서 규칙 이름이 강조 표시됩니다.
- 규칙을 오른쪽 클릭하고 **Clear Hit Count(**적중 횟수 지우기**)**를 선택하여 규칙의 적중 횟수 정보를 지웁니다(0으로 재설정). Ctrl 키를 누른 상태에서 클릭하여 여러 규칙을 선택할 수 있습니다. 이 작업을 취소할 수 없습니다.
- 페이지의 왼쪽 하단에 있는 **Generate CSV(CSV** 생성**)**를 클릭하여 페이지의 세부 정보에 대한 쉼표로 구분된 값 보고서를 생성합니다.

단계 **5** **Close(**닫기**)**를 클릭하여 Policy(정책) 페이지로 돌아갑니다.