액세스 제어

다음 주제에서는 액세스 제어 규칙에 대해 설명합니다. 이러한 규칙은 디바이스를 통과할 수 있는 트래픽을 제어하며 침입 검사와 같은 고급 서비스를 트래픽에 적용합니다.

액세스 제어의 모범 사례

액세스 제어 정책은 내부 네트워크를 보호하고 부적절한 웹 사이트와 같은 바람직하지 않은 외부 네트워크 리소스에 사용자가 액세스하는 것을 방지하기 위한 기본 도구입니다. 따라서 이 정책에 각별한 주의를 기울이고 필요한 보호 및 연결성 수준을 얻도록 세밀하게 조정하는 것이 좋습니다.

다음 절차에서는 액세스 제어 정책을 사용하여 수행해야 하는 기본 작업에 대한 개요를 제공합니다. 이는 개요이며 각 작업을 수행하기 위한 전체 단계를 제공하지는 않습니다.

액세스 제어 정책에 접근하려면 **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

프로시저

단계 **1** 정책의 기본 작업을 구성합니다.

기본 작업은 정책의 특정 규칙과 일치하지 않는 연결을 처리합니다. 기본적으로 이 작업은 **Block(**차단**)**이므로 규칙에서 누락된 사항은 모두 차단됩니다. 따라서 원하는 트래픽을 허용하는 액세스 제어 규칙만 작성하면 됩니다. 이는 액세스 제어 정책을 구성하는 기존의 방법입니다.

기본적으로 트래픽을 허용하는 반대의 작업을 수행할 수 있으며, 원하지 않는 알려진 트래픽을 삭제하는 규칙을 작성할 수 있으므로 허용하려는 모든 항목에 대한 규칙이 필요하지는 않습니다. 이렇게

하면 신규 서비스를 쉽게 사용할 수 있지만, 원하지 않는 새 트래픽이 발견되기 전에 통과할 위험이 있습니다.

단계 **2** **Access Policy Settings(**액세스 정책 설정**)(**⚙**)** 버튼을 클릭하고, **TLS Server Identity Discovery(TLS** 서버 **ID** 검색**)** 옵션을 활성화합니다.

이 옵션을 활성화하지 않으면 TLS 1.3 트래픽이 원하는 규칙과 일치하지 않습니다.

단계 **3** 가능한 한 소수의 액세스 제어 규칙을 생성합니다.

기존 방화벽에서는 IP 주소와 포트의 다양한 조합에 대한 수만 개의 규칙을 생성하게 될 수 있습니다. 차세대 방화벽에서는 고급 검사를 사용하여 이러한 세부 규칙을 피할 수 있습니다. 규칙이 적을수록 시스템에서 트래픽을 더욱 빠르게 평가할 수 있으며 규칙 세트 내에서 문제를 보다 쉽게 발견하고 수정할 수 있습니다.

단계 **4** 액세스 제어 규칙에서 로깅 활성화합니다.

로깅을 활성화한 경우에만 일치하는 트래픽에 대한 통계가 수집됩니다. 로깅을 활성화하지 않으면 모니터링 대시보드가 정확하지 않습니다.

단계 **5** 매우 구체적인 규칙을 정책의 맨 위에 두고, 특정 규칙이 일치하는 연결과 일치하는 보다 일반적인 규칙보다 위에 있는지 확인합니다.

정책은 하향식으로 평가되며, 첫 번째 일치 항목이 적용됩니다. 따라서 특정 서브넷에 대한 모든 트래픽을 차단하는 규칙을 설정한 다음, 서브넷 내에서 단일 IP 주소에 대한 액세스를 허용하는 규칙을 따르면 첫 번째 규칙이 이를 차단하므로 해당 주소에 대한 트래픽은 허용되지 않습니다.

또한 기존 기준(예: 인그레스/이그레스 인터페이스, 소스/대상 IP 주소, 포트 또는 지리위치)만을 기반으로 트래픽을 대상으로 하는 규칙을 심층 검사가 필요한 규칙(예 : 사용자 기준, URL 필터링 또는 애플리케이션 필터링에 적용되는 규칙)보다 먼저 배치해야 합니다. 이러한 규칙은 검사가 필요하지 않으므로 규칙을 조기에 추가하면 일치하는 연결에 대한 액세스 제어 결정을 더욱 빨리 내릴 수 있습니다.

자세한 내용은 액세스 제어 규칙 순서에 대한 모범 사례, 14 페이지를 참조하십시오.

단계 **6** 차단 및 허용 규칙을 트래픽의 대상 하위 세트에 페어링합니다. 규칙입니다.

예를 들어, 대량의 HTTP / HTTPS 트래픽은 허용하되 음란물이나 도박과 같은 바람직하지 않은 사이트에 대한 액세스는 차단해야 할 경우가 많습니다. 그런 경우, 다음 규칙을 생성하고 정책 내에서 순차적으로 유지하여 이를 수행할 수 있습니다.(예 : 규칙 11 및 12)

- 내부 보안 영역(소스) 및 외부 보안 영역(대상), 그리고 모든 IP 주소, 포트 또는 지리위치에 적용되는, 바람직하지 않은 URL 범주를 대상으로 하는 URL 필터링 차단 규칙. 예를 들어 봇넷 차단, 아동 학대 콘텐츠, 암호 해독, DNS 터널링, 온라인 뱅킹 사기, 익스플로잇, 익스트림, 필터 회피, 도박, 해킹, 혐오 표현, 고위험 사이트 및 위치, 불법 활동, 불법 다운로드, 불법 약물, 악성 사이트, 악성 코드 사이트, 모바일 위협, P2P 악성 코드 노드, 피싱, 음란물, 스팸, 스파이웨어 및 애드웨어 등을 차단합니다.
- 내부 보안 영역(소스) 및 외부 보안 영역(대상) 그리고 모든 IP 주소, 포트 또는 지리위치에 적용되는, HTTP 및 HTTPS 애플리케이션에 대한 애플리케이션 필터링 허용 규칙. URL 필터링 규칙이 원치 않는 웹 리소스에 대한 액세스를 차단한 후 이 규칙은 다른 모든 HTTP/HTTPS 액세스를 허용합니다.

단계 **7** IP 주소 또는 포트에 관계없이 트래픽을 대상으로 하는 차세대 고급 방화벽 기능을 사용합니다.

공격자 또는 기타 악의적인 사용자는 기존의 액세스 제어 트래픽 일치 기준을 회피하기 위해 IP 주소 및 포트를 자주 변경할 수 있습니다. 대신 다음과 같은 차세대 기능을 사용하십시오.

- 사용자 기준 — 트래픽을 시작하는 사용자에 대한 정보를 얻으려면 ID 정책을 구성합니다. Active Directory 서버는 사용자를 그룹으로 구성하며, 사용자 그룹 멤버십을 기반으로 트래픽을 허용하거나 차단하는 액세스 제어 규칙을 생성할 수 있습니다. 예를 들어 엔지니어가 개발 서브넷에 액세스하도록 허용하면서 엔지니어 그룹에 속하지 않은 사람은 암묵적으로 차단할 수 있습니다. 개별 사용자 이름 대신 그룹을 사용하면 사람들이 네트워크에 추가될 때 규칙을 계속 업데이트할 필요가 없습니다.
- 애플리케이션 기준 — 애플리케이션 필터링 기준을 사용하여 애플리케이션 유형을 허용하거나 차단합니다. 따라서 사용자가 HTTP 연결에 대한 포트를 변경하면 시스템에서는 포트 80으로 이동하지 않더라도 HTTP임을 인식할 수 있습니다. 자세한 내용은 애플리케이션 필터링에 대한 모범 사례, 6 페이지를 참조하십시오.
- URL 범주 및 평판 기준 — 범주를 기반으로 URL 필터링을 사용하여 사이트 유형에 따라 사이트를 동적으로 허용하거나 차단합니다. 사이트 유형 또는 범주 내에서 사이트의 평판이 좋은 수행자인지 나쁜 수행자인지에 따라 규칙을 세밀하게 조정할 수 있습니다. 범주 및 평판을 사용하면 사이트가 URL을 변경할 때 규칙을 지속적으로 조정할 필요가 없습니다. URL을 기준으로 사이트를 수동으로 차단하려는 경우 이 작업을 수행해야 합니다. 자세한 내용은 효과적인 URL 필터링에 대한 모범 사례, 10 페이지를 참조하십시오.

  URL 범주/평판 필터링 규칙을 DNS 조회 요청의 FQDN에 적용할 수도 있습니다. 시스템은 차단된 범주/평판에 대한 DNS 회신을 방지하여 사용자의 연결 시도를 효과적으로 차단할 수 있습니다. 자세한 내용은 URL 범주 및 평판을 기준으로 DNS 요청 필터링, 13 페이지 섹션을 참조해 주십시오.

단계 **8** 모든 허용 규칙에 침입 검사를 적용합니다.

차세대 방화벽의 강력한 측면 중 하나는 동일한 디바이스를 사용하여 침입 검사 및 액세스 제어를 적용할 수 있다는 점입니다. 각 허용 규칙에 침입 정책을 적용합니다. 그러면 공격이 일반적으로 정상적인 경로를 통해 네트워크에 침입하는 경우 이를 탐지하여 공격 연결을 삭제할 수 있습니다.

기본 작업이 Allow(허용)인 경우 기본 작업과 일치하는 트래픽에 대해 침입 방지를 적용할 수도 있습니다.

단계 **9** 또한 원치 않는 IP 주소 및 URL을 차단하도록 보안 인텔리전스 정책을 구성합니다.

보안 인텔리전스 정책은 액세스 제어 정책보다 먼저 적용되므로 액세스 제어 규칙이 평가받기 전에 원치 않는 연결을 차단할 수 있습니다. 이를 통해 초기 차단을 제공하고 액세스 제어 규칙의 복잡성을 줄일 수 있습니다.

단계 **10** SSL 암호 해독 정책 구현을 고려하십시오.

시스템은 암호화된 트래픽에서 심층 검사를 수행할 수 없습니다. SSL 암호 해독 정책을 구성할 경우 액세스 제어 정책이 암호 해독된 트래픽 버전에 적용됩니다. 따라서 심층 검사에는 침입 정책을 사용하여 공격을 식별할 수 있으며, 애플리케이션 및 URL 필터링을 더욱 효과적으로 적용할 수 있으므로

규칙 일치가 보다 효율적입니다. 액세스 제어 정책에서 허용하는 모든 트래픽은 디바이스에서 전송되기 전에 다시 암호화되므로 최종 사용자의 암호화 보호는 손실되지 않습니다.

액세스 제어 개요

다음 항목에서는 액세스 제어 정책에 대해 설명합니다.

액세스 제어 규칙 및 기본 작업

액세스 제어 정책을 사용하여 네트워크 리소스에 대한 액세스를 허용하거나 차단합니다. 이 정책은 하향식으로 평가되는 순서가 지정된 규칙 집합으로 구성됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

다음을 기준으로 하여 액세스를 제어할 수 있습니다.

- 소스 및 대상 IP 주소, 프로토콜, 포트 및 인터페이스와 같은 기존 네트워크 특성(보안 영역 형식)
- 네트워크 개체 형식의 소스 또는 대상의 FQDN(Fully Qualified Domain Name). 트래픽 일치는 DNS 조회에서 이름에 대해 반환되는 IP 주소를 기준으로 합니다.
- Cisco Identity Services Engine(ISE)에서 소스 또는 대상에 할당한 SGT(Security Group Tag).
- 사용 중인 애플리케이션. 특정 애플리케이션을 기반으로 액세스를 제어할 수도 있고, 애플리케이션의 범주, 특정 특성으로 태그가 지정된 애플리케이션, 애플리케이션의 유형(클라이언트, 서버, 웹) 또는 애플리케이션의 위험이나 사업 타당성 등급을 포함하는 규칙을 생성할 수도 있습니다.
- 일반화된 URL 범주를 포함한 웹 요청의 대상 URL. 대상 사이트의 공개 평판에 따라 일치하는 범주를 세분화할 수 있습니다.
- DNS 조회 요청에서 FQDN의 URL 범주 및 평판. 원치 않는 범주 또는 좋지 않은 평판의 DNS 응답을 차단하여 후속 연결 시도를 효과적으로 방지할 수 있습니다.
- 요청을 하는 사용자 또는 사용자가 속한 사용자 그룹

허용한 암호화되지 않은 트래픽에 대해 IPS 검사를 적용하여 위협을 확인하고 공격으로 보이는 트래픽을 차단할 수 있습니다. 또한 파일 정책을 사용하여 금지된 파일이나 악성코드를 확인할 수도 있습니다.

액세스 규칙과 일치하지 않는 모든 트래픽은 액세스 제어 기본 작업에 의해 처리됩니다. 기본적으로 트래픽을 허용하는 경우 트래픽에 침입 검사를 적용할 수 있습니다. 그러나 기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.

애플리케이션 필터링

액세스 제어 규칙을 사용하여 연결에 사용되는 애플리케이션을 기반으로 트래픽을 필터링할 수 있습니다. 시스템은 수많은 애플리케이션을 인식할 수 있으므로 모든 웹 애플리케이션을 차단하지 않고 웹 애플리케이션 하나만 차단하는 방법을 알아낼 필요가 없습니다.

널리 사용되는 몇 가지 애플리케이션의 경우 애플리케이션의 여러 측면을 필터링할 수 있습니다. 예를 들어 Facebook 전체를 차단하지 않고 Facebook Games만 차단하는 규칙을 생성할 수 있습니다.

일반 애플리케이션 특성을 기반으로 하는 규칙을 생성할 수도 있습니다. 그러면 위험 또는 사업 타당성, 유형, 범주 또는 태그를 선택하여 전체 애플리케이션 그룹을 차단하거나 허용할 수 있습니다. 그러나 애플리케이션 필터에서 범주를 선택할 때는 원치 않는 애플리케이션이 포함되지 않도록 일치하는 애플리케이션 목록을 확인해야 합니다**.** 가능한 그룹화에 대한 자세한 설명은 애플리케이션 기준, 24 페이지를 참조하십시오.

암호화된 트래픽과 암호 해독된 트래픽에 대한 애플리케이션 제어

애플리케이션이 암호화를 사용하는 경우에는 시스템이 애플리케이션을 식별하지 못할 수도 있습니다.

시스템은 SMTPS, POPS, FTPS, TelnetS, IMAPS를 비롯하여 StartTLS로 암호화된 애플리케이션 트래픽을 탐지할 수 있습니다. 또한, TLS ClientHello 메시지 내 서버 이름 지표 또는 서버 인증서의 주체 고유 이름 값에 따라 암호화된 특정 애플리케이션을 식별할 수 있습니다.

애플리케이션 필터 대화 상자를 사용하여 다음 태그를 선택한 후에 애플리케이션 목록을 검사하여 애플리케이션에서 암호 해독이 필요한지 확인합니다.

- **SSL** 프로토콜 - SSL 프로토콜로 태그가 지정된 트래픽은 암호를 해독할 필요가 없습니다. 시스템은 이 트래픽을 인식할 수 있으며 액세스 제어 작업을 적용할 수 있습니다. 나열된 애플리케이션에 대한 액세스 제어 규칙이 필요한 연결과 일치하는지를 확인해야 합니다.
- 암호 해독된 트래픽 - 트래픽을 먼저 암호 해독해야 시스템이 해당 트래픽을 인식할 수 있습니다. 이 트래픽에 대한 SSL 암호 해독 규칙을 구성합니다.

CIP(Common Industrial Protocol) 및 Modbus 애플리케이션(ISA 3000)에서 필터링

Cisco ISA 3000 디바이스에서 CIP(Common Industrial Protocol) 및 Modbus 전처리기를 활성화하고 액세스 제어 규칙에서 CIP 및 Modbus 애플리케이션을 필터링할 수 있습니다. 모든 CIP 애플리케이션 이름은 CIP Write와 같이 "CIP"로 시작합니다. Modbus용 애플리케이션은 하나뿐입니다.

전처리기를 활성화하려면 CLI 세션(SSH 또는 콘솔)에서 전문가 모드로 이동하고 다음 명령을 실행하여 이러한 SCADA(Supervisory Control and Data Acquisition) 애플리케이션 중 하나 또는 둘 다를 활성화해야 합니다.

sudo /usr/local/sf/bin/enable_scada.sh {cip | modbus | both}

예를 들어, 전처리기를 모두 활성화하려면 다음을 수행합니다.

```
> expert
admin@firepower:~$ sudo /usr/local/sf/bin/enable_scada.sh both
```

참고 이 명령은 모든 구축을 완료한 후에 실행해야 합니다. 이러한 전처리기는 구축 시 비활성화됩니다.

애플리케이션 필터링에 대한 모범 사례

애플리케이션 필터링 액세스 제어 규칙을 설계할 때 다음 권장 사항에 유의하십시오.

- 광고물 트래픽과 같이 웹 서버에서 참조된 트래픽을 처리하려면 참조하는 애플리케이션이 아닌 참조되는 애플리케이션의 일치 여부를 확인합니다.
- 애플리케이션 및 URL 기준을 동일한 규칙으로 결합하지 마십시오(특히 암호화된 트래픽의 경우).
- 태그가 지정된 **Decrypted Traffic(**암호 해독된 트래픽**)**에 대해 규칙을 작성하는 경우, 일치하는 트래픽을 암호 해독하는 SSL 암호 해독 규칙이 있는지 확인합니다. 이러한 애플리케이션은 암호 해독된 연결에서만 식별 가능합니다.
- TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 컨트롤 규칙과 일치하는지 확인하려면 액세스 컨트롤 설정에서 **TLS 1.3** 인증서 가시성을 활성화할 것을 권장합니다. 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다.
- 시스템은 Skype 애플리케이션 트래픽의 여러 유형을 탐지할 수 있습니다. Skype 트래픽을 제어하려면 개별 애플리케이션을 선택하는 대신 애플리케이션 필터 목록에서 Skype 태그를 선택합니다. 이렇게 하면 시스템이 동일한 방법으로 모든 Skype 트래픽을 탐지하고 제어할 수 있도록 할 수 있습니다.
- Zoho 메일에 대한 액세스를 제어하려면 Zoho 및 Zoho Mail 애플리케이션을 모두 선택합니다.

URL 필터링

액세스 제어 규칙을 사용하여 HTTP 또는 HTTPS 연결에 사용되는 URL을 기반으로 트래픽을 필터링할 수 있습니다. HTTPS는 암호화되어 있으므로 HTTPS보다 HTTP에 대한 URL 필터링이 더 간단합니다.

다음 기술을 사용하여 URL 필터링을 구현할 수 있습니다.

- 범주 및 평판 기반 URL 필터링 - URL 필터링 라이선스를 사용하면 URL의 일반 분류(범주) 및 위험 레벨(평판)을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다. 이는 원치 않는 사이트를 차단하는 단연 가장 쉽고 효과적인 방법입니다.
- 수동 URL 필터링 - 임의의 라이선스를 사용하여 개별 URL과 URL 그룹을 수동으로 지정해 웹 트래픽을 맞춤형 방식으로 더 상세하게 제어할 수 있습니다. 수동 필터링의 주요 목적은 카테고리 기반 차단 규칙에 대한 예외를 생성하는 것이지만 다른 목적으로도 수동 규칙을 사용할 수 있습니다.

다음 항목에서는 URL 필터링에 대해 자세히 설명합니다.

카테고리 및 평판을 기준으로 URL 필터링

URL 필터링 라이선스가 있으면 요청한 URL의 카테고리 및 평판을 기준으로 웹 사이트에 대한 액세스를 제어할 수 있습니다.

- 범주 - URL의 일반 분류입니다. 예를 들어 ebay.com은 경매 범주에 속하고 monster.com은 구직 범주에 속합니다. 하나의 URL이 여러 카테고리에 속할 수 있습니다.
- 평판 - URL이 사용자가 속한 조직의 보안 정책에 어긋나는 용도로 사용될 가능성입니다. 평판의 범위는 Untrusted(신뢰할 수 없음)(레벨 1)부터 Trusted(신뢰할 수 있음)(레벨 5)까지입니다.

URL 범주 및 평판을 사용하면 URL 필터링을 빠르게 구성할 수 있습니다. 예를 들어, 액세스 제어를 사용해 Illegal Drugs(불법 약물) 카테고리에서 신뢰할 수 없는 URL을 차단할 수 있습니다.

카테고리에 대한 설명은 https://www.talosintelligence.com/categories를 참조하십시오.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 보안 위협을 나타내거나 부적절한 콘텐츠를 제공하는 사이트가 나타나고 사라지는 속도는 새 정책을 업데이트하고 구축하는 속도보다 빠를 수 있습니다. Cisco는 새로운 사이트, 변경된 분류 및 변경된 평판이 있는 URL 데이터베이스를 업데이트하므로 규칙이 새로운 정보에 맞게 자동으로 조정됩니다. 따라서 새로운 사이트를 처리하기 위해 규칙을 편집할 필요가 없습니다.

일반 URL 데이터베이스 업데이트를 활성화하는 경우 시스템에서 URL 필터링에 최신 정보를 사용할 수 있습니다. 또한, Cisco CSI(Collective Security Intelligence)와의 통신을 활성화하여 알려지지 않은 카테고리 및 평판을 지닌 URL에 대한 최신 위협 인텔리전스를 얻을 수 있습니다. 자세한 내용은 URL Filtering(URL 필터링) 기본 설정 컨피그레이션의 내용을 참고하십시오.

참고 이벤트 및 애플리케이션 세부사항에서 URL 범주 및 평판 정보를 확인하려면 URL 조건을 사용하여 규칙을 하나 이상 생성해야 합니다.

URL의 카테고리 및 평판 조회

특정 URL의 카테고리 및 평판을 확인할 수 있습니다. 액세스 제어 규칙 또는 SSL 암호 해독 규칙의 URL 탭으로 이동하거나 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **URL Filtering Preferences(URL** 필터링 기본 설정**)**로 이동할 수 있습니다. 거기에서 **URL to Check(**확인할 **URL)** 필드에 URL을 입력하고 **Go(**이동**)**를 클릭하면 됩니다.

그러면 조회 결과를 표시하는 웹 사이트로 이동합니다. 이 정보를 이용하여 카테고리 및 평판 기준 URL 필터링 규칙의 동작을 확인할 수 있습니다.

분류에 동의하지 않는 경우, device manager에서 **Submit a URL Category Dispute(URL** 카테고리 이의 제기 제출**)**를 클릭하여 저희에게 의견을 알려주시면 됩니다.

수동 **URL** 필터링

개별 URL 또는 URL 그룹을 수동으로 필터링하여 카테고리 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의할 수 있습니다. 이러한 유형의 URL 필터링을 수행하는 데는 특별한 라이선스가 필요하지 않습니다.

예를 들어 액세스 제어를 사용하여 조직에 적합하지 않은 웹 사이트 카테고리를 차단할 수 있습니다. 그러나 해당 카테고리에 액세스 권한을 제공하려는 적합한 웹 사이트가 포함된 경우에는 해당 사이트에 수동 허용 규칙을 생성하여 해당 카테고리에 대한 차단 규칙 앞에 배치하면 됩니다.

수동 URL 필터링을 구성하려면 대상 URL을 사용하는 URL 개체를 생성합니다. 이 URL이 해석되는 방식은 다음 규칙을 기반으로 합니다.

- 경로를 포함하지 않는 경우(즉, URL에 / 문자가 없음), 이 일치는 서버의 호스트 이름만을 기준으로 합니다. 호스트 이름은 :// 구분자 뒷부분 또는 호스트 이름의 의 뒷부분이 같아야 일치하는 것으로 간주됩니다. 예를 들어 ign.com은 ign.com 및 www.ign.com과 일치하지만 verisign.com과는 일치하지 않습니다.
- 하나 이상의 / 문자를 포함하는 경우, 전체 URL 문자열이 서버 이름, 경로 및 쿼리 파라미터를 비롯한 부분 문자열 일치에 사용됩니다. 그러나 서버가 재구성되고 페이지가 새 경로로 이동될 수 있으므로 개별 웹 페이지 또는 사이트 일부를 차단하거나 허용하기 위해 수동 URL 필터링은 사용하지 않는 것이 좋습니다. 부분 문자열 일치는 예기치 않은 일치로 이어질 수도 있으며, 이 경우에는 URL 개체에 포함하는 문자열도 쿼리 파라미터 내부에 있는 의도하지 않은 서버 또는 문자열의 경로와 일치됩니다.
- 시스템에서는 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 다시 말해, 특정 웹 사이트를 차단하는 경우 애플리케이션 조건을 사용하여 특정 프로토콜을 대상으로 하지 않는 한 해당 웹 사이트에 대한 HTTP 및 HTTPS 트래픽이 모두 차단됩니다. URL 개체를 생성할 때에는 개체 생성 시 프로토콜을 지정할 필요가 없습니다. 이를테면 http://example.com 대신 example.com을 사용하십시오.
- URL 개체를 사용하여 액세스 제어 규칙에서 HTTPS 트래픽을 매칭하려는 경우, 트래픽 암호화에 사용되는 공개 키 인증서에서 주체 CN을 사용하여 개체를 생성합니다. 또한 주체 CN에 포함된 하위 도메인은 무시되므로 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

  그러나 인증서의 주체 일반 이름은 웹 사이트의 도메인 이름과 아무런 관련도 없을 수 있습니다. 예를 들어, youtube.com 인증서의 주체 일반 이름은 *.google.com입니다(언제든 변경 가능). URL 필터링 규칙이 암호 해독된 트래픽에서 작동하도록 SSL 암호 해독 정책을 사용하여 HTTPS 트래픽을 암호 해독하면 더 일관성 있는 결과를 얻게 됩니다.

참고 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

HTTPS 트래픽 필터링

HTTPS 트래픽은 암호화되어 있기 때문에 HTTPS 트래픽에서 직접 URL 필터링을 수행하는 것은 HTTP 트래픽에서 그렇게 하는 것만큼 간단하지 않습니다. 따라서 SSL 암호 해독 정책을 사용하여 필터링하려는 모든 HTTPS 트래픽을 암호 해독하는 방법을 고려해야 합니다. 그래야 URL 필터링 액세스 제어 정책이 암호 해독된 트래픽에서 작동하며 일반 HTTP 트래픽을 대상으로 할 때 얻는 결과와 동일한 결과를 얻을 수 있습니다.

그러나 일부 HTTPS 트래픽을 암호 해독되지 않은 상태로 액세스 제어 정책에 전달하는 것을 허용하려면 규칙이 HTTP 트래픽과 일치하는 것과는 다른 방법으로 HTTPS 트래픽과 일치한다는 점을 이해해야 합니다. 시스템은 암호화된 트래픽을 필터링하기 위해 SSL 핸드셰이크 중에 전달된 정보(트래픽을 암호화하는 데 사용된 공개 키 인증서의 주체 공용 이름)를 기준으로 요청된 URL을 확인합니다. URL의 웹 사이트 호스트 이름과 주체 일반 이름 간에는 관련성이 적거나 없을 수 있습니다.

DNS 요청 필터링을 활성화하면 범주/평판 규칙에 대한 HTTPS 일치를 개선할 수 있습니다. 시스템은 사용자가 HTTPS 연결 시도를 시작하기 전에 DNS 확인 단계 도중 범주 및 평판을 확인하고 원치 않는 조합에 대한 DNS 응답을 차단할 수 있습니다. 허용되는 DNS 응답의 경우 시스템은 후속 HTTPS 연결에 사용할 수 있는 범주/평판 정보를 보유하게 됩니다. DNS 요청 필터링, 12 페이지의 내용을 참조하십시오.

HTTP 필터링과 달리, HTTPS 필터링은 주체 공용 이름 내의 서브도메인을 무시합니다. 수동으로 HTTPS URL을 필터링할 경우 하위 도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오. 또한, 사이트에서 사용하는 인증서의 콘텐츠를 검토하여 가지고 있는 도메인이 주체 일반 이름에서 사용된 적절한 도메인인지 그리고 이 이름이 다른 규칙과 충돌하지 않는지(예: 차단하려는 사이트의 이름이 허용하려는 이름과 중복될 수 있음) 확인합니다. 예를 들어, youtube.com 인증서의 주체 일반 이름은 *.google.com입니다(언제든 변경 가능).

참고 인증서 정보를 더 이상 사용할 수 없어 브라우저에서 TLS 세션을 다시 시작하는 경우에는 URL 개체가 HTTPS 트래픽과 일치되지 않습니다. 따라서 URL 개체를 주의하여 구성하더라도 HTTPS 연결에 대해 일관성 없는 결과를 얻을 수 있습니다.

암호화 프로토콜을 통해 트래픽 제어

시스템에서는 URL 필터링을 수행할 때 암호화 프로토콜(HTTP 대 HTTPS)을 무시합니다. 이는 수동 및 평판 기반 URL 조건 모두에 해당됩니다. 즉, URL 필터링에서는 다음 웹 사이트에 대한 트래픽을 똑같이 처리합니다.

- http://example.com
- https://example.com

HTTP 또는 HTTPS 트래픽 중 하나에만 일치하는 규칙을 구성하려면 대상 조건에서 TCP 포트를 지정하거나 규칙에 애플리케이션 조건을 추가합니다. 예를 들어 각각 TCP 포트/애플리케이션 및 URL 조건을 갖춘 2개의 액세스 제어 규칙을 작성하여 어떤 사이트에 대한 HTTPS 액세스를 허용하되 HTTP 액세스는 허용하지 않을 수 있습니다.

첫 번째 규칙은 웹 사이트에 대한 HTTPS 트래픽을 허용합니다.

작업: Allow(허용)
TCP 포트 또는 애플리케이션: HTTPS(TCP 포트 443)
URL: example.com

두 번째 규칙은 동일한 웹 사이트에 대한 HTTP 액세스를 차단합니다.

작업: Block(차단)
TCP 포트 또는 애플리케이션: HTTP(TCP 포트 80)
URL: example.com

URL 및 애플리케이션 필터링 비교

URL 및 애플리케이션 필터링에는 유사한 점이 있습니다. 하지만 다음과 같이 매우 뚜렷한 목적을 위해 필터링 기능을 사용해야 합니다.

- URL 필터링은 전체 웹 서버에 대한 액세스를 차단하거나 허용하는 데 사용되는 가장 좋은 방법입니다. 예를 들어, 네트워크에서 모든 유형의 도박을 허용하지 않으려는 경우 URL 필터링 규칙을 생성하여 도박 카테고리를 차단할 수 있습니다. 이 규칙을 사용하면 사용자는 카테고리 내 모든 웹 서버의 모든 페이지에 액세스할 수 없습니다.
- 애플리케이션 필터링은 호스팅 사이트와 관계없이 특정 애플리케이션을 차단하거나 기타 허용 가능한 웹 사이트의 특정 기능을 차단하는 데 유용합니다. 예를 들어, 모든 Facebook을 차단하지 않고 Facebook의 게임 애플리케이션만 차단할 수 있습니다.

애플리케이션과 URL 기준을 결합하면 예기치 않은 결과가 발생할 수 있기 때문에(특히 암호화된 트래픽의 경우) 이는 URL 및 애플리케이션 기준에 대한 별도의 규칙을 생성하기에 좋은 정책입니다. 애플리케이션과 URL 기준을 단일 규칙에서 결합해야 하는 경우, 애플리케이션 및 URL 결합 규칙이 더 일반적인 애플리케이션 전용 또는 URL 전용 규칙에 대한 예외 역할을 하지 않는 한, 이러한 규칙은 간단한 애플리케이션 전용 또는 URL 전용 규칙 이후에 배치해야 합니다. URL 필터링 차단 규칙은 애플리케이션 필터링보다 더 광범위하기 때문에 애플리케이션 전용 규칙보다 상위에 배치해야 합니다.

애플리케이션과 URL 기준을 결합하는 경우, 원치 않는 사이트 및 애플리케이션에 대한 액세스를 허용하지 않으려면 네트워크를 더 신중하게 모니터링해야 할 수 있습니다.

효과적인 URL 필터링에 대한 모범 사례

URL 필터링 액세스 제어 규칙을 설계할 때 다음 권장 사항에 유의하십시오.

- 가능한 경우 항상 카테고리 및 평판 차단 기능을 사용합니다. 이렇게 하면 새 사이트가 카테고리에 추가될 때 자동으로 차단되며, 사이트의 평판이 높아지거나 낮아지는 경우 평판을 기반으로 하는 차단 기능이 조정됩니다.
- URL 카테고리 일치를 사용할 때는 사이트의 로그인 페이지가 사이트 자체의 카테고리와 다른 카테고리에 포함되는 경우가 있음을 고려해야 합니다. 예를 들어 Gmail은 Web-based Email(웹 기반 이메일) 카테고리에 포함되지만 로그인 페이지는 Search Engines and Portals(검색 엔진 및 포털) 카테고리에 포함됩니다. 카테고리에 대해 여러 작업이 포함된 각기 다른 규칙이 있는 경우 의도하지 않은 결과가 발생할 수 있습니다.

- URL 개체를 사용하여 전체 웹 사이트를 대상으로 하고 카테고리 차단 규칙에 대한 예외를 설정합니다. 즉, 예외를 설정하지 않는다면 카테고리 규칙에서 차단될 특정 사이트를 허용합니다.
- URL 개체를 사용하여 웹 서버를 수동으로 차단하려는 경우 보안 인텔리전스 정책에서 차단하는 것이 훨씬 더 효과적입니다. 보안 인텔리전스 정책은 액세스 제어 규칙이 평가되기 전에 연결을 삭제하므로 더욱 빠르고 효율적인 차단을 가능하게 합니다.
- HTTPS 연결을 가장 효과적으로 필터링하려면 SSL 암호 해독 규칙을 구현하여 액세스 제어 규칙을 작성 중인 대상 트래픽의 암호를 해독합니다. 암호 해독된 HTTPS 연결은 액세스 제어 정책에서 HTTP 연결로 필터링되므로 HTTPS 필터링에 대한 모든 제한을 피할 수 있습니다.
- TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 컨트롤 규칙과 일치하는지 확인하려면 액세스 컨트롤 설정에서 **TLS 1.3** 인증서 가시성을 활성화할 것을 권장합니다. 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다.
- URL 필터링은 전체 웹 서버를 차단하는 반면, 애플리케이션 필터링은 웹 서버와 관계없이 특정 애플리케이션 사용을 대상으로 하므로 애플리케이션 필터링 규칙보다 URL 차단 규칙을 먼저 배치합니다.
- 카테고리를 알 수 없는 고위험 사이트를 차단하려면 Uncategorized(카테고리가 지정되지 않음) 카테고리를 선택하고 평판 슬라이더를 Questionable(의심스러움) 또는 Untrusted(신뢰할 수 없음)으로 조정합니다.
- DNS 요청 필터링도 활성화하여 전반적인 URL 필터링 효율성을 높일 수 있습니다. DNS 요청 필터링을 사용하는 경우 시스템에서 DNS 조회 시간에 FQDN의 URL 범주 및 평판을 결정하므로, 후속 HTTP/HTTPS 요청이 동일한 대상으로 향하는 경우 이 정보를 사용할 수 있습니다. 추가로 범주/평판을 차단하는 경우 웹 세션 설정 단계가 아닌 DNS 요청 단계에서 연결 시도가 중단됩니다. DNS 요청 필터링, 12 페이지의 내용을 참조하십시오.

웹 사이트를 차단할 때 사용자에게 표시되는 내용

URL 필터링 규칙을 사용하여 웹 사이트를 차단할 때 사용자에게 표시되는 내용은 사이트가 암호화되어 있는지에 따라 달라집니다.

- HTTP 연결 - 사용자에게는 시간이 초과되거나 재설정된 연결의 경우에 표시되는 일반적인 브라우저 페이지가 아닌 시스템 기본 차단 응답 페이지가 표시됩니다. 이 페이지에서는 연결이 의도적으로 차단되었다는 내용이 명확하게 표시됩니다.
- HTTPS(암호화된) 연결 - 사용자에게 시스템 기본 차단 응답 페이지가 표시되지 않습니다. 대신 보안 연결 실패를 나타내는 브라우저의 기본 페이지가 표시됩니다. 오류 메시지는 사이트가 정책으로 인해 차단되었음을 나타내지 않습니다. 대신 일반적인 암호화 알고리즘이 없다는 오류가 표시될 수 있습니다. 이 메시지만으로는 연결이 의도적으로 차단되었는지를 명확하게 파악할 수 없습니다.

또한, 명시적 URL 필터링 규칙이 아닌 다른 액세스 제어 규칙이나 기본 작업에 의해 웹 사이트가 차단될 수도 있습니다. 예를 들어 전체 네트워크 또는 지리위치를 차단하는 경우 해당 네트워크나 지리

위치의 웹 사이트도 모두 차단됩니다. 이러한 규칙으로 인해 차단된 사용자에게는 아래 제한에서 설명하는 응답 페이지가 표시될 수도 있고 표시되지 않을 수도 있습니다.

URL 필터링을 구현할 때는 사이트가 의도적으로 차단될 때 표시될 수 있는 내용 및 차단 대상 사이트 유형을 엔드 유저에게 설명하는 것이 좋습니다. 그렇지 않으면 엔드 유저가 차단된 연결의 트러블슈팅을 수행하는 데 오랜 시간을 쓸 수 있습니다.

HTTP 대응 페이지의 제한

시스템에서 웹 트래픽을 차단할 때 HTTP 대응 페이지가 항상 표시되는 것은 아닙니다.

- 승격된 액세스 제어 규칙(단순한 네트워크 조건만 사용하여 초기에 배치된 차단 규칙)으로 인해 웹 트래픽이 차단될 때는 시스템에서 응답 페이지를 표시하지 않습니다.
- 시스템에서 요청된 URL을 식별하기 전에 웹 트래픽이 차단되면 시스템은 응답 페이지를 표시하지 않습니다.
- 액세스 제어 규칙에 의해 차단되는 암호화된 연결에 대해서는 시스템이 응답 페이지를 표시하지 않습니다.

DNS 요청 필터링

HTTP/HTTPS가 아닌 연결 시도에도 DNS 조회 요청에 URL 범주 및 평판 데이터베이스를 적용할 수 있습니다.

예를 들어 사용자가 www.example.com에 대한 FTP 연결을 시도하는 경우, 해당 FQDN(Fully Qualified Domain Name)에 대한 DNS 조회 요청이 표시될 때 www.example.com의 범주 및 평판을 조회하도록 시스템을 설정할 수 있습니다. 반환된 범주/평판에 대한 DNS/URL 필터링 규칙이 차단 규칙인 경우 시스템은 DNS 회신을 차단합니다. 따라서 사용자는 FQDN에 대한 IP 주소를 가져오지 않으며, 연결 시도는 실패합니다.

DNS 조회 요청 필터링을 활성화하면 URL 필터링 규칙을 HTTP/HTTPS 이외의 프로토콜로 확장하고, FTP, TFTP, SCP, ICMP 및 기타 프로토콜에서 웹 액세스를 위해 차단하는 사이트에 대한 연결을 설정하는 것을 방지할 수 있습니다. 이는 사용자가 FQDN 이름을 사용하는 한 작동하므로 DNS 조회가 필요합니다. 사용자가 IP 주소를 사용하는 경우 DNS 요청이 없으므로 DNS 요청 차단이 불가능합니다.

HTTP/HTTPS 트래픽의 경우 DNS 요청 시간에 범주/평판 조회를 수행하면 웹 세션을 설정하기 전에 연결을 방지할 수 있으므로 시스템 성능이 향상될 수 있습니다. 이는 암호화된 HTTPS에 특히 유용할 수 있습니다. DNS 요청 단계에서 거부함으로써 시스템에서 HTTPS 연결을 확인할 수 없으므로 암호 해독 규칙을 평가할 필요가 없고, 암호화된 세션을 올바른 액세스 제어 규칙과 일치시키는 더욱 어려운 작업을 수행할 필요도 없습니다.

DNS 요청 필터링 지침

DNS 요청 필터링을 설정할 때는 다음 사항에 유의하십시오.

- DNS 요청 필터링은 DNS 세션에서만 작동합니다. DNS 회신을 허용하는 경우(즉, URL 필터링 규칙 작업이 Allow(허용)임), 사용자가 반환한 IP 주소로 설정하는 후속 연결은 액세스 제어 규칙

과 별도로 일치됩니다. 연결이 다른 규칙과 일치될 수 있으므로 다른 이유로 차단 또는 허용될 수 있습니다. 예를 들어, FTP에서 DNS 조회를 통해 IP 주소를 가져오도록 허용하는 경우 FTP 연결을 금지하는 또 다른 액세스 제어 규칙이 있을 수 있으며, 그 결과 연결이 차단됩니다.

- URL/DNS 요청 필터링 규칙 이전의 액세스 제어 규칙과 일치하는 DNS 조회 요청은 일치하는 규칙에 따라 허용되거나 차단됩니다. 이러한 연결에 대해서는 범주/평판 조회가 이루어지지 않습니다.
- 이 기능을 사용하려면 범주/평판을 기반으로 URL 필터링을 구현해야 합니다. 이 유형의 URL 필터링에 대한 URL 필터링 라이선스가 있어야 합니다. 범주/평판을 기반으로 하는 URL 필터링 규칙이 없는 경우, DNS 요청 필터링이 적합하지 않으므로 이를 활성화해서는 안 됩니다.
- DNS 필터링에 의해 생성되는 연결 이벤트에는 DNS Query(DNS 쿼리), URL Category(URL 범주) 및 URL Reputation(URL 평판)과 같은 특수 관심 필드가 포함됩니다. DNS Query(DNS 쿼리) 필드에는 조회 요청에 대한 FQDN(Fully Qualified Domain Name)이 표시됩니다. DNS 필터링 이벤트의 경우 URL 필드가 비어 있습니다.
- DNS 요청 필터링은 URL 범주 및 평판 데이터베이스만 사용합니다. 일치하는 액세스 제어 규칙에서 정의된 URL 개체 또는 기타 수동 URL 필터링은 무시됩니다. 수동 DNS 이름 차단을 구현하려면 보안 인텔리전스 DNS 정책을 사용합니다.

URL 범주 및 평판을 기준으로 DNS 요청 필터링

다음 절차에서는 DNS 조회 요청 필터링을 구현하는 방법을 설명합니다.

시작하기 전에

아직 활성화되지 않은 경우 URL 라이선스를 활성화해야 합니다.

프로시저

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

단계 **2** 필요한 경우 **Access Policy Settings(**액세스 정책 설정**)**( ) 버튼을 클릭하고, **Reputation Enforcement on DNS Traffic(DNS** 트래픽에 대한 평판 시행**)** 옵션을 선택한 다음 **OK(**확인**)**를 클릭합니다.

이 옵션은 액세스 제어 정책에 대한 DNS 요청 필터링을 활성화합니다. 이 옵션은 기본적으로 활성화되어 있습니다.

단계 **3** DNS 요청에도 적용되는 URL 범주 및 평판을 기반으로 필터링을 구현하려면 기존 URL 필터링 규칙을 평가하거나 새 규칙을 생성합니다.

URL 필터링은 일반적으로 HTTP/HTTPS 트래픽에만 적용되므로 애플리케이션 또는 포트를 기준으로 이러한 규칙을 제한할 이유가 없습니다. 하지만 이러한 제한이 있는 경우 규칙을 DNS 요청에도 적용할 수 있는지 확인합니다.

- **Source/Destination(**소스/대상**)** 탭에서 **Destination Ports(**대상 포트**)** 필드가 **Any(**모두**)**인 경우 변경할 필요가 없습니다. 포트를 지정한 경우 **DNS over UDP** 및 **DNS over TCP**를 목록에 추가합니다.

- **Applications(**애플리케이션**)** 탭에서 애플리케이션 목록이 **Any(**모두**)**인 경우 변경할 필요가 없습니다. 애플리케이션 또는 애플리케이션 필터를 지정한 경우 **DNS** 애플리케이션을 목록 또는 필터에 추가합니다. 다른 DNS 관련 옵션은 이 목적과 관련이 없습니다.

액세스 제어 규칙 생성에 대한 자세한 내용은 액세스 제어 규칙 구성, 20 페이지를 참조하십시오.

단계 **4** 이전 규칙을 평가하여 DNS 요청이 해당 규칙과 일치하지 않는지 확인합니다.

DNS 요청이 범주 및 평판 사양이 있는 URL 필터링 규칙과 일치하는 경우에만 범주 및 평판이 결정됩니다. URL 필터링 규칙이 DNS 요청 필터링을 우회하는 것보다 이전에 액세스 제어 정책의 규칙과 일치하는 DNS 요청. 이러한 DNS 요청은 차단 또는 허용되는 일치 규칙에 따라 처리됩니다.

침입, 파일 및 악성코드 검사

침입 정책 및 파일 정책은 트래픽이 원하는 대상에 도달하도록 허용하기 전에 최종 방어선으로 함께 사용됩니다.

- 침입 정책은 시스템의 침입 방지 기능을 제어합니다.
- 파일 정책은 시스템의 파일 제어 및 악성코드 방어 기능을 제어합니다.

기타 모든 트래픽 처리는 네트워크 트래픽에서 침입, 금지된 파일 및 악성코드를 검사하기 전에 수행됩니다. 침입 또는 파일 정책을 액세스 제어 규칙과 연결하여 시스템이 액세스 제어 규칙의 조건과 일치하는 트래픽을 통과시키기 전에 침입 정책이나 파일 정책 또는 두 정책을 모두 사용하여 트래픽을 먼저 검사하도록 명령할 수 있습니다.

트래픽을 허용하는 규칙에 대해서만 침입 및 파일 정책을 구성할 수 있습니다. 트래픽을 **trust(**신뢰**)** 또는 **block(**차단**)**하도록 설정된 규칙에 대해서는 검사가 수행되지 않습니다. 또한, 액세스 제어 정책의 기본 작업이 허용이면 침입 정책은 구성할 수 있지만 파일 정책은 구성할 수 없습니다.

액세스 제어 규칙으로 처리되는 단일한 연결의 경우, 침입 검사 전에 파일 검사가 이루어집니다. 즉, 시스템에서는 파일 정책 또는 침입에 의해 차단된 파일은 검사하지 않습니다. 파일 검사 내에서 유형을 기준으로 한 간단한 차단은 악성코드 검사 및 차단보다 우선합니다. 세션에서 파일이 탐지되고 차단될 때까지, 세션의 패킷은 침입 검사 대상이 될 수 있습니다.

참고 기본적으로, 시스템에서는 암호화된 페이로드의 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. 검사는 암호화되지 않은 트래픽에 대해서만 작동합니다.

액세스 제어 규칙 순서에 대한 모범 사례

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다. 다음 권장 사항을 참고하십시오.

- 구체적인 규칙은 일반적인 규칙보다 먼저 배치해야 합니다(특히, 구체적인 규칙이 일반적인 규칙에 대한 예외인 경우).
- IP 주소, 보안 영역, 포트 번호 등 레이어-3/4 기준만을 기반으로 하여 트래픽을 삭제하는 규칙은 가능한 한 먼저 배치해야 합니다. 레이어-3/4 기준은 검사하지 않고 신속하게 평가될 수 있기 때문에 이러한 규칙은 검사(예: 애플리케이션 또는 URL 기준을 사용하는 검사)가 필요한 규칙보다 먼저 배치하는 것이 좋습니다. 물론 이러한 규칙에 대한 예외는 해당 규칙보다 상위에 배치해야 합니다.
- 구체적인 삭제 규칙은 가능한 경우 항상 정책 상위에 둡니다. 이렇게 하면 부적절한 트래픽에 대해 가능한 한 빠른 결정을 내릴 수 있습니다.
- 애플리케이션 및 URL 기준을 모두 포함하는 규칙은 애플리케이션 및 URL 기준이 결합된 규칙이 더 일반적인 애플리케이션 전용 또는 URL 전용 규칙에 대한 예외 역할을 하지 않는 한, 간단한 애플리케이션 전용 또는 URL 전용 규칙 이후에 배치해야 합니다. 애플리케이션과 URL 기준을 결합하면 예기치 않은 결과가 발생할 수 있기 때문에(특히 암호화된 트래픽의 경우) 가능한 경우 항상 URL 및 애플리케이션 필터링에 대해 별도의 규칙을 생성하는 것이 좋습니다.

NAT 및 액세스 규칙

NAT를 구성한 경우라도, 액세스 규칙은 액세스 규칙 일치를 확인할 때 항상 실제 IP 주소를 사용합니다. 예를 들어 내부 서버 10.1.1.5가 외부에서 공개적으로 라우팅 가능한 IP 주소 209.165.201.5를 갖도록 NAT를 구성할 경우, 외부 트래픽이 내부 서버에 액세스하는 것을 허용하는 액세스 규칙은 서버의 매핑된 주소(209.165.201.5)가 아니라 실제 IP 주소(10.1.1.5)를 참조해야 합니다.

기타 보안 정책이 액세스 제어에 영향을 미치는 방식

기타 보안 정책은 액세스 제어 규칙이 작동하고 연결과 일치하는 방식에 영향을 미칠 수 있습니다. 액세스 규칙을 구성할 때 다음 사항에 유의하십시오.

- **SSL Decryption(SSL** 암호 해독**)** 정책 — SSL 암호 해독 규칙은 액세스 제어보다 먼저 평가됩니다. 따라서 암호화된 연결이 일부 유형의 암호 해독을 적용하는 SSL 암호 해독 규칙과 일치하는 경우, 이 연결은 액세스 제어 정책에서 평가되는 일반 텍스트(암호 해독됨) 연결입니다. 액세스 규칙은 연결의 암호화된 버전을 확인하지 않습니다. 또한, 트래픽을 삭제하는 SSL 암호 해독 규칙과 일치하는 모든 연결은 액세스 제어 정책에서 확인되지 않습니다. 마지막으로, 암호 해독 안 함 규칙과 일치하는 모든 암호화된 연결은 암호화된 상태에서 평가됩니다.
- **Identity(ID)** 정책 — 연결은 소스 IP 주소에 대한 사용자 매핑이 있는 경우에만 사용자(및 사용자 그룹)와 일치됩니다. 사용자 또는 그룹 멤버십의 핵심인 액세스 규칙은 ID 정책에 의해 사용자 ID가 수집된 연결하고만 일치할 수 있습니다.
- **Security Intelligence(**보안 인텔리전스**)** 정책 — 삭제된 연결은 액세스 제어 정책에서 확인되지 않습니다. 차단 안 함 목록과 일치하는 연결은 이후에 액세스 제어 규칙과 일치되며, 궁극적으로 연결을 처리하는 방법(허용 또는 삭제)을 결정하는 액세스 제어 규칙입니다.
- **VPN**(사이트 대 사이트 또는 원격 액세스) — VPN 트래픽은 항상 액세스 제어 정책을 대상으로 평가되며 연결은 일치 규칙에 기초하여 허용 또는 삭제됩니다. 그러나 VPN 터널 자체는 액세스

제어 정책이 평가되기 전에 암호 해독됩니다. 액세스 제어 정책은 터널 자체가 아니라 VPN 터널 내부에 임베드된 연결을 평가합니다.

액세스 제어를 위한 라이선스 요건

액세스 제어 정책을 사용하는 데에는 특수 라이선스가 필요하지 않습니다.

그러나 액세스 제어 정책에 포함된 특수 기능에 대해서는 다음과 같은 라이선스가 필요합니다. 라이선스 구성에 대한 자세한 내용은 선택 가능한 라이선스 활성화 또는 비활성화를 참조하십시오.

- **URL** 라이선스 - URL 카테고리 및 평판을 일치 기준으로 사용하는 규칙을 생성하는 데 필요합니다.
- 위협 라이선스 - 액세스 규칙 또는 기본 작업에서 침입 정책을 구성하는 데 필요합니다. 파일 정책을 사용하려면 이 라이선스도 필요합니다(악성코드 라이선스도 필요함).
- 악성코드 라이선스 - 액세스 규칙에서 파일 정책을 구성하는 데 필요합니다. 위협은 파일 정책에도 필요합니다.

액세스 제어 정책에 대한 지침 및 제한 사항

다음은 액세스 제어에 대한 몇 가지 추가적인 제한 사항입니다. 규칙에서 예상된 결과를 얻고 있는지 평가할 때 이 제한 사항을 고려하십시오.

- URL 데이터베이스 업데이트에 추가되거나(신규, 수신), 사용되지 않거나(발신) 삭제된 카테고리가 포함된 경우, 영향을 받는 액세스 제어 규칙을 변경할 수 있는 유예 기간이 있습니다. 영향을 받는 규칙에는 규칙에 영향을 미치는 문제에 대한 설명과 카테고리 변경에 대한 자세한 내용을 참조할 수 있는 Cisco Talos Intelligence Group(Talos) 웹 사이트의 링크가 있는 정보 메시지가 표시되어 있습니다. 규칙을 업데이트하여 최신 URL 데이터베이스에서 사용할 수 있는 적절한 범주를 사용하도록 해야 합니다.

  유예 기간을 수용하려면 새로 추가된 수신 카테고리를 적절한 규칙에 추가하되 사용하지 않는 발신 카테고리를 제거하지 마십시오. 이때 규칙에는 신규 및 기존 카테고리가 포함되어야 합니다. 새 카테고리는 기존 카테고리에 삭제 표시가 된 경우에 적용됩니다. 기존 범주가 최종 삭제된 경우, 규칙을 수정하여 삭제된 카테고리를 제거하고 컨피그레이션을 재구축해야 합니다. 삭제된 카테고리를 사용하는 규칙을 모두 수정할 때까지는 컨피그레이션을 구축하지 못하도록 차단됩니다. 주의해야 하는 규칙을 기준으로 필터링하려면 테이블 위쪽에 있는 문제 규칙 참조 링크를 클릭하십시오.

- Device Manager는 디렉터리 서버에서 최대 50,000명의 사용자에 대한 정보를 다운로드할 수 있습니다. 디렉터리 서버에 50,000개가 넘는 사용자 계정이 포함되어 있으면 액세스 규칙에서 사용자를 선택할 때 또는 사용자 기반 대시보드 정보를 확인할 때 가능한 이름이 모두 표시되지 않으며, 다운로드한 이름에 대해서만 규칙을 작성할 수 있습니다.

  이 50,000명 제한은 그룹과 연결된 이름에도 적용됩니다. 그룹의 구성원이 50,000명보다 많으면 다운로드한 50,000개의 이름에 대해서만 그룹 구성원 자격과의 일치 여부를 확인할 수 있습니다.

- VDB(Vulnerability Database) 업데이트에서 사용되지 않는 애플리케이션을 제거하는 경우, 삭제된 애플리케이션을 사용하는 액세스 제어 규칙 또는 애플리케이션 필터를 변경해야 합니다. 이러한 규칙을 수정할 때까지는 변경 사항을 구축할 수 없습니다. 또한 문제를 해결하기 전에는 시스템 소프트웨어 업데이트를 설치할 수 없습니다. Application Filters(애플리케이션 필터) 개체 페이지 또는 규칙의 Application(애플리케이션) 탭에서는 이러한 애플리케이션 이름 뒤에 "(사용되지 않음)"이라고 표시됩니다.
- FQDN(Fully Qualified Domain Name) 네트워크 개체를 소스 또는 대상 기준으로 사용하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **DNS Server(DNS** 서버**)**에서 데이터 인터페이스용 DNS도 구성해야 합니다. 시스템은 관리 DNS 서버 설정을 사용하여 액세스 제어 규칙에 사용되는 FQDN 개체 조회를 수행하지 않습니다. FQDN 확인 트러블슈팅에 대한 정보는 일반 DNS 문제 문제 해결의 내용을 참조하십시오.

  FQDN으로 액세스를 제어하는 방식은 최선형 메커니즘이라는 점에 유의하십시오. 다음과 같은 점을 고려하십시오.

  - DNS 회신은 스푸핑될 수 있기 때문에 완전히 신뢰할 수 있는 내부 DNS 서버만 사용하십시오.
  - 특히 아주 인기 있는 서버에 대한 일부 FQDN에는 자주 변경되는 IP 주소가 여러 개 있을 수 있습니다. 시스템에서는 캐시된 DNS 조회 결과를 사용하므로 사용자는 캐시에는 아직 없는 새 주소를 가져올 수 있습니다. 따라서 FQDN에서 인기 사이트를 차단하여 일관성 없는 결과가 나올 수 있습니다.
  - 인기 있는 FQDN의 경우, 다양한 DNS 서버에서 일련의 다양한 IP 주소를 반환할 수 있습니다. 따라서 컨피그레이션한 것이 아닌 다른 DNS 서버를 사용자가 사용하는 경우, FQDN 기반 액세스 제어 규칙은 클라이언트에서 사용하는 사이트의 모든 IP 주소에 적용되지 않을 수 있으며 규칙에 대해 원하는 결과를 얻지 못할 수 있습니다.
  - 일부 FQDN DNS 항목의 경우에는 TTL(Time to Live) 값이 매우 짧습니다. 이로 인해 조회 테이블이 다시 컴필레이션되는 일이 자주 발생하여 전체 시스템 성능에 영향을 미칠 수 있습니다.

- 활발하게 사용 중인 규칙을 수정하는 경우 더 이상 Snort가 검사하지 않는 설정된 연결에는 변경 사항이 적용되지 않습니다. 새 규칙은 이후 연결의 일치 여부를 확인하는 데 사용됩니다. 또한 Snort가 활발하게 특정 연결을 검사하는 중인 경우, 변경된 일치 기준 또는 작업 기준을 기존 연결에 적용할 수 있습니다. 변경 사항이 모든 현재 연결에 적용되게 해야 하는 경우, 디바이스 CLI에 로그인한 다음 **clear conn** 명령을 사용하여 설정된 연결을 종료하면 됩니다. 이 경우 연결의 소스에서 연결 재설정을 시도하므로 새 규칙과 적절하게 일치한다고 가정합니다.
- 시스템은 연결에서 애플리케이션 또는 URL을 식별하기 위해 3~5개의 패킷을 사용합니다. 따라서 올바른 액세스 제어 규칙이 지정된 연결에 대해 즉시 일치되지 않을 수 있습니다. 그러나 애플리케이션/URL이 확인되고 나면 일치 규칙을 기반으로 연결이 처리됩니다. 암호화된 연결의 경우, 이는 SSL 핸드셰이크에서 서버 인증서 교환 이후에 발생합니다.
- 시스템은 애플리케이션이 식별된 연결에서 페이로드가 없는 패킷에 기본 정책 작업을 적용합니다.

- 특히 보안 영역, 네트워크 개체 및 포트 개체에 대한 일치 기준은 가능한 경우 항상 비워 둡니다. 예를 들어, 모든 인터페이스가 포함된 영역을 생성하는 대신 보안 영역 기준을 비워 두기만 하면 시스템에서 모든 인터페이스에 대한 트래픽을 더 효율적으로 일치시킬 수 있습니다. 여러 기준을 지정하는 경우 시스템에서는 지정된 기준의 모든 콘텐츠 조합에 대해 일치시켜야 합니다.
- 소스 또는 대상 기준에 대해 IP 주소를 지정하는 경우 동일한 규칙에서 IPv4 및 IPv6 주소를 혼합하지 마십시오. IPv4 및 IPv6 주소에 대해 별도의 규칙을 생성하십시오.
- 관련 Rfc를 위반하는 GRE 터널은 삭제 됩니다. 예를 들어, GRE 터널이 RFC와 달리 예약된 비트에 0이 아닌 값을 포함하는 경우 이는 삭제 됩니다. 비규격 GRE 터널을 허용해야 하는 경우 원격 관리자를 사용하고 세션을 신뢰하는 사전 필터 규칙을 구성해야 합니다. device manager를 사용하여 사전 필터 규칙을 구성할 수 없습니다.

액세스 제어 정책 구성

액세스 제어 정책을 사용하여 네트워크 리소스에 대한 액세스를 제어합니다. 이 정책은 하향식으로 평가되는 순서가 지정된 규칙 집합으로 구성됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다. 트래픽과 일치하는 규칙이 없으면 페이지 맨 아래에 표시된 기본 작업이 적용됩니다.

액세스 제어 정책을 구성하려면 **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.

액세스 제어 테이블에는 모든 규칙이 순서대로 나열됩니다. 각 규칙에 대해 다음을 수행합니다.

- 맨 왼쪽 열의 규칙 번호 옆에 있는 > 버튼을 클릭하여 규칙 다이어그램을 엽니다. 다이어그램을 통해 규칙이 어떻게 트래픽을 제어하는지 시각화할 수 있습니다. 버튼을 다시 클릭하여 다이어그램을 닫습니다.
- 대부분의 셀에서는 인라인 수정이 허용됩니다. 예를 들어, 작업을 클릭하여 다른 작업을 선택하거나 소스 네트워크 개체를 클릭하여 소스 기준을 추가 또는 변경할 수 있습니다.
- 규칙을 이동하려면 규칙 위에 마우스를 올려놓고 이동 아이콘( )이 나타나면 이를 클릭하여 규칙을 새 위치로 끌어 놓습니다. 규칙을 수정하고 순서 목록에서 새 위치를 선택하여 규칙을 이동할 수도 있습니다. 규칙은 처리할 순서대로 배치해야 합니다. 특정 규칙, 특히 더 일반적인 규칙에 대한 예외를 정의하는 규칙은 목록 위쪽에 있어야 합니다.
- 맨 오른쪽 열에는 규칙의 작업 버튼이 포함되어 있습니다. 셀 위에 마우스를 올려 놓으면 버튼이 표시됩니다. 규칙은 수정( )하거나 삭제( )할 수 있습니다.
- 액세스 컨트롤 설정 ( ) 버튼을 클릭하여 정책 내 특정 규칙이 아닌 액세스 컨트롤 정책에 적용되는 설정을 구성합니다.
- 테이블에서 적중 횟수 열을 추가 또는 제거하려면 테이블 위쪽에 있는 **Toggle Hit Counts(**적중 횟수 토글**)** 아이콘( )을 클릭합니다. 적중 횟수 열은 규칙에 대한 총 적중 횟수와 최종 적중 날짜 및 시간과 함께 이름 열의 오른쪽에 표시됩니다. 적중 횟수 정보는 토글 버튼을 클릭하면 가져올 수 있습니다. 최신 정보를 얻으려면 **refresh(**새로고침**)** 아이콘( )을 클릭하십시오.

- 예를 들어 제거 또는 변경된 URL 카테고리 때문에 어떤 규칙에 문제가 생긴 경우에는 검색 상자 옆에 있는 **See Problem Rules(**문제 규칙 참조**)** 링크를 클릭하여 해당 규칙만 표시하도록 테이블을 필터링합니다. 이러한 규칙에서 필요한 서비스를 제공하도록 수정 및 교정(또는 삭제)하십시오.

다음 항목에서는 정책을 구성하는 방법을 설명합니다.

기본 작업 구성

특정 액세스 규칙과 일치하지 않는 연결은 액세스 제어 정책의 기본 작업에 의해 처리됩니다.

프로시저

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

단계 **2** **Default Action(**기본 작업**)** 필드에서 아무 곳이나 클릭합니다.

단계 **3** 일치하는 트래픽에 적용할 작업을 선택합니다.

- **Trust(**신뢰**)** - 어떤 종류든 추가 검사 없이 트래픽을 허용합니다.
- **Allow(**허용**)** - 침입 정책이 적용되는 트래픽을 허용합니다.
- **Block(**차단**)** - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.

단계 **4** 작업이 **Allow(**허용**)**인 경우 침입 정책을 선택합니다.

정책 옵션에 대한 설명은 침입 정책 설정, 28 페이지를 참조하십시오.

단계 **5** (선택 사항). 기본 작업에 대한 로깅을 구성합니다.

기본 작업과 일치하는 트래픽에 대한 로깅을 활성화해야 대시보드 데이터 또는 이벤트 뷰어에 해당 트래픽이 포함됩니다. 로깅 설정, 29 페이지의 내용을 참조하십시오.

단계 **6** **OK(**확인**)**를 클릭합니다.

액세스 컨트롤 정책 설정 구성

정책 내 특정 규칙이 아닌 액세스 컨트롤 정책에 적용되는 설정을 구성할 수 있습니다.

프로시저

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

단계 **2** **Access Policy Settings(**액세스 정책 설정**)** ( ) 버튼을 클릭합니다.

단계 **3** 설정을 구성합니다.

- **TLS Server Identity Discovery(TLS** 서버 **ID** 검색**)** - TLS 1.3 인증서가 암호화됩니다. 애플리케이션 또는 URL 필터링을 사용하는 액세스 규칙과 일치하도록 TLS 1.3으로 암호화된 트래픽의 경우 시스템은 TLS 1.3 인증서를 암호 해독해야 합니다. 암호화된 연결이 올바른 액세스 제어 규칙과 일치하는지 확인하려면 이 옵션을 활성화하는 것이 좋습니다. 설정은 인증서만 암호 해독합니다. 연결은 암호화된 상태로 유지됩니다. 이 옵션을 활성화하면 TLS 1.3 인증서를 해독할 수 있습니다. 해당 SSL 암호 해독 규칙을 생성할 필요가 없습니다.
- **Reputation Enforcement on DNS Traffic(DNS** 트래픽에 대한 평판 시행**)** - URL 필터링 범주 및 평판 규칙을 DNS 조회 요청에 적용하려면 이 옵션을 활성화합니다. 조회 요청의 FQDN(Fully Qualified Domain Name)에 차단 중인 범주 및 평판이 있는 경우 시스템은 DNS 응답을 차단합니다. 사용자는 DNS 확인을 받지 않으므로 연결을 완료할 수 없습니다. 웹 이외의 트래픽에 URL 범주 및 평판 필터링을 적용하려면 이 옵션을 사용합니다. 자세한 내용은 DNS 요청 필터링, 12 페이지를 참고하십시오.

단계 **4** **OK(**확인**)**를 클릭합니다.

액세스 제어 규칙 구성

액세스 제어 규칙을 사용하여 네트워크 리소스에 대한 액세스를 제어합니다. 액세스 제어 정책의 규칙은 위에서부터 아래로 평가됩니다. 트래픽에 적용되는 규칙은 모든 트래픽 기준이 일치하는 첫 번째 규칙입니다.

프로시저

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

단계 **2** 다음 중 하나를 수행합니다.

- 새 규칙을 생성하려면 **+** 버튼을 클릭합니다.
- 기존 규칙을 수정하려면 해당 규칙의 수정 아이콘()을 클릭합니다.

더 이상 필요하지 않은 규칙을 삭제하려면 해당 규칙의 삭제 아이콘()을 클릭합니다.

단계 **3** **Order(**순서**)**에서 순서가 지정된 규칙 목록에 규칙을 삽입할 위치를 선택합니다.

규칙은 처음 일치하는 항목을 기준으로 적용되므로, 매우 구체적인 트래픽 일치 기준이 포함된 규칙이 보다 일반적인 기준이 포함된 정책(규칙이 일치하지 않는 경우 일치하는 트래픽에 적용됨) 위에 표시되도록 삽입해야 합니다.

기본적으로는 규칙이 목록의 끝에 추가됩니다. 나중에 규칙의 위치를 변경하려는 경우 이 옵션을 수정합니다.

단계 **4** **Tile(**제목**)**에서 규칙의 이름을 입력합니다.

이름에는 공백을 포함할 수 없지만, 영숫자 및 특수 문자(+, ., _, -)는 사용할 수 있습니다.

단계 **5** 일치하는 트래픽에 적용할 작업을 선택합니다.

- **Trust(신뢰)** - 어떤 종류든 추가 검사 없이 트래픽을 허용합니다.
- **Allow(허용)** - 정책에서 침입 및 기타 검사 설정이 적용되는 트래픽을 허용합니다.
- **Block(차단)** - 트래픽을 무조건 삭제합니다. 트래픽은 검사되지 않습니다.

단계 **6** 다음 탭을 적절하게 조합하여 트래픽 일치 기준을 정의합니다.

- **Source/Destination(소스/대상)** — 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치), 주소에 할당된 SGT(Security Group Tag) 또는 트래픽에서 사용되는 프로토콜과 포트입니다. 기본값은 모든 영역, 주소, 지리적 위치, SGT, 프로토콜 및 포트입니다. 소스/대상 기준, 22 페이지의 내용을 참조하십시오.
- **Application(애플리케이션)** - 유형, 범주, 태그, 위험, 사업 타당성에 따라 애플리케이션을 정의하는 필터 또는 애플리케이션입니다. 기본값은 모든 애플리케이션입니다. 애플리케이션 기준, 24 페이지의 내용을 참조하십시오.
- **URL** - 웹 또는 DNS 조회 요청의 URL 또는 URL 범주입니다. 기본값은 모든 URL입니다. URL 기준, 26 페이지의 내용을 참조하십시오.
- **Users(사용자)** - ID 소스, 사용자 또는 사용자 그룹입니다. ID 정책에 따라 트래픽 일치에 사용자 및 그룹 정보를 사용할 수 있는지가 결정됩니다. 이 기준을 사용하려면 ID 정책을 구성해야 합니다. 사용자 기준, 27 페이지의 내용을 참조하십시오.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 팝업 대화상자에서 **OK(확인)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

조건을 액세스 제어 규칙에 추가할 경우 다음 팁을 고려하십시오.

- 규칙마다 여러 조건을 구성할 수 있습니다. 규칙을 트래픽에 적용하려면 트래픽이 규칙의 모든 조건과 일치해야 합니다. 예를 들어, 특정 호스트 또는 네트워크에 대해 URL 필터링을 수행하는 단일 규칙을 사용할 수 있습니다.
- 규칙의 각 조건에 대해 최대 50개의 기준을 추가할 수 있습니다. 조건의 기준 중 어느 것이든 모두 일치하는 트래픽은 조건을 만족합니다. 예를 들어, 최대 50개의 애플리케이션 또는 애플리케이션 필터에 대해 애플리케이션 제어를 적용하는 단일 규칙을 사용할 수 있습니다. 따라서 단일 조건의 항목 간 관계는 OR이고 조건 유형 간의 관계(예: 소스/대상과 애플리케이션 간의 관계)는 AND가 됩니다.
- 일부 기능을 사용하려면 적절한 라이선스를 활성화해야 합니다.

단계 **7** (선택 사항). 허용 작업을 사용하는 정책의 경우 암호화되지 않은 트래픽에 대한 추가 검사를 구성할 수 있습니다. 다음 링크 중 하나를 클릭합니다.

- **Intrusion Policy(침입 정책)** — **Intrusion Policy(침입 정책)** > **On(켜기)**을 선택하고 트래픽에서 침입과 익스플로잇을 검사할 침입 검사 정책을 선택합니다. 침입 정책 설정, 28 페이지의 내용을 참조하십시오.
- **File Policy(파일 정책)** - 트래픽에서 차단해야 하는 파일과 악성코드가 포함된 파일을 검사하기 위한 파일 정책을 선택합니다. 파일 정책 설정, 28 페이지의 내용을 참조하십시오.

단계 **8** (선택 사항). 규칙에 대해 로깅을 구성합니다.

기본적으로 규칙과 일치하는 트래픽에 대해서는 연결 이벤트가 생성되지 않습니다. 단, 파일 정책을 선택하면 파일 이벤트가 기본적으로 생성됩니다. 이 행동은 변경할 수 있습니다. 정책과 일치하는 트래픽에 대한 로깅을 활성화해야 대시보드 데이터 또는 이벤트 뷰어에 해당 트래픽이 포함됩니다. 로깅 설정, 29 페이지의 내용을 참조하십시오.

침입 이벤트는 항상 일치하는 액세스 규칙의 로깅 컨피그레이션과 관계없이 삭제하거나 알리도록 설정된 침입 규칙에 대해 생성됩니다.

단계 **9** **OK(**확인**)**를 클릭합니다.

소스/대상 기준

액세스 규칙의 Source/Destination(소스/대상) 기준은 트래픽이 통과하는 보안 영역(인터페이스), IP 주소/IP 주소의 국가나 대륙(지리적 위치), 주소에 할당된 SGT(Security Group Tag) 또는 트래픽에서 사용되는 프로토콜과 포트를 정의합니다. 기본값은 모든 영역, 주소, 지리적 위치, SGT, 프로토콜 및 포트입니다.

조건을 수정하려면 해당 조건 내의 **+** 버튼을 클릭하고 필요한 개체나 요소를 선택한 후에 **OK(**확인**)**를 클릭합니다. 기준에 개체가 필요한데 필요한 개체가 없는 경우에는 새 개체 생성을 클릭하면 됩니다. 개체 또는 요소의 **x**를 클릭하면 정책에서 해당 개체나 요소를 제거할 수 있습니다.

다음 기준을 사용하여 규칙과 일치하는 소스 및 대상을 식별할 수 있습니다.

소스 영역**,** 대상 영역

트래픽이 통과하는 인터페이스를 정의하는 보안 영역 개체입니다. 기준은 하나 또는 둘 다 정의할 수도 있고 둘 다 정의하지 않을 수도 있습니다. 지정되지 않은 기준은 임의 인터페이스의 트래픽에 적용됩니다.

- 영역 내 인터페이스의 디바이스에서 나가는 트래픽에 일치시키기 위해서는 대상 영역에 해당 영역을 추가합니다.
- 영역 내 인터페이스를 통해 디바이스로 들어오는 트래픽에 일치시키기 위해서는 소스 영역에 해당 영역을 추가합니다.
- 규칙에 소스와 대상 영역 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 소스 영역 중 하나에서 발생해야 하며 대상 영역 중 하나를 통해 전송되어야 합니다.

트래픽이 디바이스로 들어오거나 디바이스에서 나가는 위치를 기준으로 규칙을 적용해야 하는 경우 이 기준을 사용해야 합니다. 예를 들어 내부 호스트로 이동하는 모든 트래픽에서 침입을 검사하려는 경우에는 내부 영역을 **Destination Zones(**대상 영역**)**로 선택하고 소스 영역은 비워 둡니다. 규칙에서 침입 필터링을 구현하려면 규칙 작업이 **Allow(**허용**)**여야 하며 규칙에서 침입 정책을 선택해야 합니다.

참고 단일 규칙에서 패시브 보안 영역과 라우팅 보안 영역을 함께 사용할 수는 없습니다. 또한 패시브 보안 영역은 소스 영역으로만 지정할 수 있으며 대상 영역으로 지정할 수는 없습니다.

소스 네트워크, 대상 네트워크

트래픽의 네트워크 주소나 위치를 정의하는 네트워크 개체 또는 지리적 위치입니다.

- 특정 IP 주소 또는 지리적 위치에서 나오는 트래픽을 일치시키려면 소스 네트워크를 구성합니다.
- 특정 IP 주소 또는 지리적 위치로 향하는 트래픽을 일치시키려면 대상 네트워크를 구성합니다.
- 규칙에 소스와 대상 네트워크 조건을 모두 추가한 경우, 일치하는 트래픽은 반드시 지정된 IP 주소 중 하나에서 발생해야 하며 그 목적지가 대상 IP 주소 중 하나여야 합니다.

이 기준을 추가할 때는 다음 탭에서 선택합니다.

- 네트워크 - 제어하려는 트래픽의 소스 또는 대상 IP 주소를 정의하는 네트워크 개체 또는 그룹을 선택합니다. FQDN(Fully Qualified Domain Name)을 사용하여 주소를 정의하는 개체를 사용할 수 있습니다. 주소는 DNS 조회를 통해 확인됩니다.
- 지리위치 - 소스 또는 대상 국가나 대륙을 기준으로 트래픽을 제어하려면 지리적 위치를 선택합니다. 대륙을 선택하면 대륙 내의 모든 국가가 선택됩니다. 규칙에서 지리적 위치를 직접 선택하는 방법 외에, 위치를 정의하기 위해 생성한 지리위치 개체를 선택할 수도 있습니다. 지리적 위치를 사용하면 특정 국가에서 사용될 수 있는 모든 IP 주소를 몰라도 해당 국가에 대한 액세스를 쉽게 제한할 수 있습니다.

참고 최신 지리적 위치 데이터를 사용하여 트래픽을 필터링하려면 GeoDB(geolocation database)를 정기적으로 업데이트하는 것이 좋습니다.

소스 포트, 대상 포트/프로토콜

트래픽에 사용되는 프로토콜을 정의하는 포트 개체입니다. TCP/UDP의 경우 여기에는 포트가 포함될 수 있습니다. ICMP의 경우에는 코드와 유형이 포함될 수 있습니다.

- 특정 프로토콜이나 포트에서 나오는 트래픽을 일치시키려면 소스 포트를 구성합니다. 소스 포트는 TCP/UDP 전용일 수 있습니다.
- 특정 프로토콜이나 포트로 향하는 트래픽을 일치시키려면 대상 포트/프로토콜을 구성합니다. 조건에 대상 포트만 추가할 경우, 다른 전송 프로토콜을 사용하는 포트를 추가할 수 있습니다. ICMP 및 기타 비TCP/UDP 사양은 대상 포트에서만 허용되며 소스 포트에서는 허용되지 않습니다.
- 특정 TCP/UDP 포트에서 발생하는 트래픽과 특정 TCP/UDP 포트로 향하는 트래픽을 모두 일치시키려면 두 포트를 모두 구성합니다. 조건에 소스 및 대상 포트를 모두 추가한 경우, 단일 전송 프로토콜(TCP 또는 UDP)을 공유하는 포트만 추가할 수 있습니다. 예를 들어 포트 TCP/80에서 포트 TCP/8080으로 이동하는 트래픽을 대상으로 지정할 수 있습니다.

소스 **SGT** 그룹**,** 대상 **SGT** 그룹

ISE(Identity Services Engine)에서 다운로드되는 트래픽에 할당된 SGT를 식별하는 SGT(Security Group Tag) 그룹 개체입니다. ISE ID 소스를 정의하는 경우에만 이러한 개체를 사용할 수 있습니다. 그렇지 않으면 이 섹션은 나타나지 않습니다. 엑세스 제어를 위한 SGT 사용 방법에 대한 자세한 내용은 TrustSec SGT(Security Group Tag)를 사용하여 네트워크 액세스를 제어하는 방법, 34 페이지를 참조하십시오.

- 소스에 그룹에 정의된 SGT 중 하나가 있는 트래픽을 일치시키려면 소스 **SGT** 그룹을 구성합니다.
- 그룹에 정의된 SGT 중 하나를 포함하는 대상에 트래픽을 일치시키려면 대상 **SGT** 그룹을 구성합니다.
- 규칙에 소스와 대상 SGT 조건을 모두 추가한 경우 일치하는 트래픽은 반드시 지정된 태그 중 하나를 가진 소스에서 발생해야 하며 대상 태그 중 하나로 대상이 지정되어 있어야 합니다.

애플리케이션 기준

액세스 규칙의 애플리케이션 기준은 IP 연결 또는 필터에 사용되는 애플리케이션을 정의하며 유형, 범주, 태그, 위험 또는 사업 타당성에 따라 애플리케이션을 정의합니다. 기본값은 모든 애플리케이션입니다.

규칙에서 개별 애플리케이션을 지정할 수 있으나 애플리케이션 필터를 사용하면 정책 생성 및 관리가 간소화됩니다. 예를 들어, 위험도가 높고 비즈니스 관련성이 낮은 모든 애플리케이션을 식별하여 차단하는 액세스 제어 규칙을 만들 수 있습니다. 사용자가 이러한 애플리케이션 중 하나를 사용하려고 할 경우, 세션은 차단됩니다.

이와 더불어 Cisco에서는 시스템 및 VDB(Vulnerability Database)를 통해 추가 애플리케이션 탐지기를 자주 업데이트하고 추가합니다. 따라서 규칙을 수동으로 업데이트하지 않아도 위험도가 높은 애플리케이션을 차단하는 규칙이 새 애플리케이션에 자동으로 적용될 수 있습니다.

규칙에서 애플리케이션 및 필터를 직접 지정하거나 이러한 특성을 정의하는 애플리케이션 필터 개체를 생성할 수 있습니다. 이 두 가지 경우의 사양은 동일하지만, 개체를 사용하면 복잡한 규칙을 생성할 때에도 시스템 제한(기준당 항목 50개)을 유지하기가 더욱 쉽습니다.

애플리케이션 및 필터 목록을 수정하려면 조건 내에서 **+** 버튼을 클릭하고 개별 탭에 나열된 원하는 애플리케이션 또는 애플리케이션 필터 개체를 선택한 후에 팝업 대화 상자에서 **OK(**확인**)**를 클릭합니다. 탭 중 하나에서 **Advanced Filter(**고급 필터**)**를 클릭하면 필터 기준을 선택하거나 특정 애플리케이션을 검색할 수 있습니다. 애플리케이션, 필터 또는 개체에 대해 **x**를 클릭하면 정책에서 해당 항목을 제거할 수 있습니다. **Save As Filter(**필터로 저장**)** 링크를 클릭하면 아직 개체가 아닌 결합된 기준을 새 애플리케이션 필터 개체로 저장할 수 있습니다.

참고 선택한 애플리케이션을 VDB 업데이트를 통해 제거한 경우 애플리케이션 이름 뒤에 "(Depredcated(사용되지 않음))"이라고 표시됩니다. 이러한 애플리케이션은 필터에서 제거해야 합니다. 그렇지 않으면 후속 구축 및 시스템 소프트웨어 업그레이드가 차단됩니다.

다음과 같은 고급 필터 기준을 사용하여 규칙과 일치하는 애플리케이션이나 필터를 식별할 수 있습니다. 이러한 애플리케이션 또는 필터는 애플리케이션 필터 개체에서 사용되는 것과 같은 요소입니다.

참고 단일 필터 기준으로 여러 선택 항목이 OR 관계를 갖습니다. 예를 들어, 위험은 높음 OR 매우 높음입니다. 반면 필터 간의 관계는 AND입니다. 즉, 위험은 높음 OR 매우 높음 AND 사업 타당성은 낮음 OR 매우 낮음과 같습니다. 필터를 선택하면 디스플레이의 애플리케이션 목록이 업데이트되어 기준을 충족하는 애플리케이션만 표시됩니다. 이러한 필터를 사용하여 개별적으로 추가하려는 애플리케이션을 찾거나, 규칙에 추가할 적절한 필터를 선택하고 있는지를 확인할 수 있습니다.

위험

애플리케이션이 조직의 보안 정책과 상반되는 용도로 사용될 가능성(매우 낮음~매우 높음)

사업 타당성

조직의 비즈니스 운영(레크리에이션과 반대) 컨텍스트 내에서 애플리케이션이 사용될 가능성(매우 낮음~매우 높음)

유형

애플리케이션 유형:

- 애플리케이션 프로토콜 - 호스트 간의 통신을 나타내는 HTTP, SSH 등의 애플리케이션 프로토콜
- 클라이언트 프로토콜 - 호스트에서 실행 중인 소프트웨어를 나타내는 웹 브라우저, 이메일 클라이언트 등의 클라이언트
- 웹 애플리케이션 - HTTP 트래픽의 요청 URL 또는 콘텐츠를 나타내는 MPEG 비디오, Facebook 등의 웹 애플리케이션

범주

가장 중요한 기능을 설명하는 일반 애플리케이션 분류

태그

애플리케이션에 대한 추가 정보로, 범주와 비슷합니다.

암호화된 트래픽의 경우, 시스템은 **SSL** 프로토콜 태그가 지정된 애플리케이션만 사용하여 트래픽을 식별하고 필터링할 수 있습니다. 이 태그가 없는 애플리케이션은 암호화되지 않은 트래픽 또는 해독된 트래픽에서만 탐지할 수 있습니다. 또한 암호화된 트래픽 또는 암호화되지 않은 트래픽이 아닌 암호 해독된 트래픽에서만 탐지할 수 있는 애플리케이션에는 암호 해독된 트래픽 태그가 할당됩니다.

애플리케이션 목록**(**디스플레이 하단**)**

이 목록은 목록 위의 옵션에서 필터를 선택하면 업데이트되므로 현재 필터와 일치하는 애플리케이션을 확인할 수 있습니다. 이 목록을 사용하여 규칙에 필터 기준을 추가하려는 경우 필터가

적절한 애플리케이션을 대상으로 하는지를 확인할 수 있습니다. 특정 애플리케이션을 추가하려는 경우 이 목록에서 선택합니다.

URL 기준

액세스 규칙의 URL 기준은 웹 요청에 사용되는 URL 또는 요청된 URL이 속하는 범주를 정의합니다. 범주가 일치하는 경우 허용하거나 차단할 사이트의 상대적 평판을 지정할 수도 있습니다. 기본적으로는 모든 URL이 허용됩니다.

DNS 조회 요청 필터링을 활성화하면 범주 및 평판 설정이 조회 요청의 FQDN(Fully Qualified Domain Name)에도 적용됩니다. 범주 및 평판 설정만 DNS 요청 필터링에 적용됩니다. 수동 URL 필터링은 무시됩니다.

URL 카테고리 및 평판을 통해 액세스 제어 규칙의 URL 조건을 신속하게 만들 수 있습니다. 예를 들어, 모든 게임 사이트 또는 신뢰할 수 없는 소셜 네트워킹 사이트를 차단할 수 있습니다. 사용자가 해당 카테고리 및 평판 조합을 가진 URL 검색을 시도하는 모든 경우, 세션이 차단됩니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리도 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 예상대로 제어할 수 있습니다. 마지막으로, Cisco의 위협 인텔리전스는 새로운 URL, 새로운 범주 및 기존 URL의 새로운 범주와 위험이 적용되어 지속적으로 업데이트되므로 시스템은 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 악성코드, 스팸, 봇넷, 피싱과 같은 보안 위협을 나타내는 악성 사이트는 새로운 정책을 업데이트하고 구축하는 것보다 빠르게 나타났다 사라질 수 있습니다.

URL 목록을 수정하려면 조건 내의 + 버튼을 클릭하고 다음 기술 중 하나를 사용하여 원하는 범주 또는 URL을 선택합니다. 범주 또는 개체의 **x**를 클릭하면 정책에서 해당 범주나 개체를 제거할 수 있습니다.

URL 탭

+를 클릭하고 URL 개체 또는 그룹을 선택한 후에 **OK(**확인**)**를 클릭합니다. 필요한 개체가 없는 경우에는 **Create New URL(**새 **URL** 생성**)**을 클릭하면 됩니다.

참고 특정 사이트를 대상으로 하도록 URL 개체를 구성하기 전에 수동 URL 필터링에 대한 정보를 자세히 확인하십시오.

범주 탭

+를 클릭하고 원하는 범주를 선택한 후에 **OK(**확인**)**를 클릭합니다.

카테고리에 대한 설명은 https://www.talosintelligence.com/categories를 참조하십시오.

기본적으로는 평판과 관계없이 선택한 각 범주의 모든 URL에 규칙을 적용합니다. 평판을 기준으로 하여 규칙을 제한하려면 각 범주의 아래쪽 화살표를 클릭하고 임의 체크 박스 선택을 취소한 후에 평판 슬라이더를 사용하여 평판 레벨을 선택합니다. 평판 슬라이더의 왼쪽은 허용할 사이트를, 오른쪽은 차단할 사이트를 나타냅니다. 평판 사용 방식은 규칙 작업에 따라 달라집니다.

- 규칙이 웹 액세스를 차단하거나 모니터링하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 높은 모든 평판도 선택됩니다. 예를 들어, **Questionable sites(**의심스러운 사이트**)**(레

벨 2)를 차단하거나 모니터링하는 규칙을 구성하는 경우, **Untrusted(**신뢰할 수 없음**)**(레벨 1) 사이트도 자동으로 차단되거나 모니터링됩니다.

- 규칙이 웹 액세스를 허용하는 경우 평판 레벨을 선택하면 해당 레벨보다 심각도가 낮은 모든 평판도 선택됩니다. 예를 들어, **Favorable sites(**선호 사이트**)**(레벨 4)를 허용하는 규칙을 구성하는 경우, **Trusted(**신뢰할 수 있음**)(**레벨 **5)** 사이트도 자동으로 허용됩니다.

평판을 알 수 없는 URL을 평판 일치에 포함하려면 **Include Sites with Unknown Reputation(**평판을 알 수 없는 사이트 포함**)** 옵션을 선택합니다. 새 사이트는 일반적으로 등급이 지정되지 않으며, 사이트의 평판을 알 수 없거나 확인할 수 없는 다른 이유가 있을 수 있습니다.

URL의 카테고리 확인

특정 URL의 카테고리 및 평판을 확인할 수 있습니다. **URL to Check(**확인할 **URL)** 상자에서 URL을 입력하고 **Go(**이동**)**를 클릭하십시오. 결과를 볼 수 있는 외부 웹 사이트로 연결됩니다. 분류에 동의하지 않는 경우 **Submit a URL Category Dispute(URL** 카테고리 이의 제출**)** 링크를 클릭하고 저희에게 알려주십시오.

사용자 기준

액세스 규칙의 사용자 기준은 IP 연결의 사용자 또는 사용자 그룹을 정의합니다. 액세스 규칙에 사용자 또는 사용자 그룹 기준을 포함하려면 ID 정책 및 연관된 디렉터리 서버를 구성해야 합니다.

ID 정책에 따라 특정 연결에 대해 사용자 ID가 수집되는지가 결정됩니다. ID가 설정된 경우에는 호스트의 IP 주소가 식별된 사용자와 연결됩니다. 그러므로 해당 소스 IP 주소가 사용자에 매핑된 트래픽은 해당 사용자가 보내는 것으로 간주됩니다. IP 패킷 자체는 사용자 ID 정보를 포함하지 않으므로 이 IP 주소에서 사용자로의 매핑은 가능한 최적의 근사치입니다.

규칙에는 최대 50개의 사용자나 그룹을 추가할 수 있으므로 일반적으로는 개별 사용자를 선택하는 것보다 그룹을 선택하는 것이 더 효율적입니다. 예를 들어 엔지니어링 그룹의 개발 네트워크 액세스를 허용하는 규칙을 생성한 다음 네트워크에 대한 기타 모든 액세스를 거부하는 후속 규칙을 생성할 수 있습니다. 그러면 신규 엔지니어에 대해 규칙을 적용하려는 경우 디렉터리 서버의 엔지니어링 그룹에 해당 엔지니어를 추가하기만 하면 됩니다.

해당 소스 내 모든 사용자에게 적용할 ID 소스도 선택할 수 있습니다. 따라서 여러 Active Directory 도메인을 지원하는 경우, 도메인에 근거하여 리소스에 대한 차등 액세스를 제공할 수 있습니다.

사용자 목록을 수정하려면 조건 내의 **+** 버튼을 클릭하고 다음 기법 중 하나를 사용하여 원하는 ID를 선택하십시오. ID의 **x**를 클릭하면 정책에서 제거할 수 있습니다.

- **Identity Sources(ID** 소스**)** - 선택한 소스에서 얻은 모든 사용자에게 규칙을 적용하려면 AD 영역 또는 로컬 사용자 데이터베이스 같은 ID 소스를 선택합니다. 필요한 영역이 아직 없는 경우, **Create New Identity Realm(**새 **ID** 영역 생성**)**을 클릭하여 바로 생성합니다.
- **Groups(**그룹**)** - 원하는 사용자 그룹을 선택합니다. 그룹은 디렉터리 서버에서 그룹을 구성하는 경우에만 사용할 수 있습니다. 그룹을 선택하면 하위 그룹을 포함하여 그룹의 모든 멤버에게 규칙이 적용됩니다. 하위 그룹을 다르게 처리하려는 경우에는 하위 그룹용으로 별도의 액세스 규칙을 생성한 다음 액세스 제어 정책에서 상위 그룹용 규칙 위에 배치해야 합니다.
- **Users(**사용자**)** - 개별 사용자를 선택합니다. 사용자 이름에는 Realm\username과 같은 ID 소스가 접두사로 붙습니다.

Special-Identities-Realm에서 일부 사용자는 기본으로 제공됩니다.

- **Failed Authentication(**실패한 인증**)** - 사용자에게 인증하라는 메시지가 표시되었는데 사용자가 허용되는 최대 횟수 이내에 유효한 사용자 이름/비밀번호 쌍을 입력하지 못했습니다. 인증에 실패해도 사용자의 네트워크 액세스가 차단되지는 않지만, 이러한 사용자의 네트워크 액세스를 제한하는 액세스 규칙을 작성할 수 있습니다.
- **Guest(**게스트**)** - 게스트 사용자는 ID 규칙이 이러한 사용자를 게스트로 지칭하도록 구성된다는 점을 제외하면 실패한 인증 사용자와 비슷합니다. 즉, 게스트 사용자 역시 인증하라는 메시지가 표시되었지만, 최대 시도 횟수 이내에 인증하지 못한 사용자입니다.
- **No Authentication Required(**인증 필요 없음**)** - 사용자의 연결이 인증을 지정하지 않은 ID 규칙과 일치하여 인증하라는 메시지가 표시되지 않았습니다.
- **Unknown(**알 수 없음**)** - IP 주소에 대한 사용자 매핑이 없으며 아직 실패한 인증 기록이 없습니다. 이는 일반적으로 해당 주소에서 HTTP 트래픽이 아직 전송되지 않았음을 의미합니다.

침입 정책 설정

Cisco는 방화벽 시스템에서 여러 침입 정책을 제공합니다. Cisco Cisco Talos Intelligence Group(Talos)이 제공하는 여러 침입 정책은 Cisco에서 설계하였습니다. Talos는 침입 및 전처리기 규칙 상태와 고급 설정을 설정했습니다. 트래픽을 허용하는 액세스 제어 규칙의 경우 침입 정책을 선택하여 트래픽에서 침입 및 익스플로잇을 검사할 수 있습니다. 침입 정책은 패턴을 기반으로 디코딩된 패킷에서 공격을 검사하며 악의적인 트래픽을 차단하거나 변경할 수 있습니다.

Snort 2를 실행할 때는 이러한 정책만 사용할 수 있으며 수정할 수 없습니다. 그러나 침입 규칙 작업 변경(Snort 2)의 설명대로 특정 규칙에 대해 취할 조치를 변경할 수 있습니다.

Snort 3을 실행할 때 이러한 정책 중 하나를 선택하거나 자체 침입 정책을 생성할 수 있습니다.

침입 검사를 활성화하려면 **Intrusion Policy(**침입 정책**)** > **On(**켜기**)**을 선택하고 원하는 정책을 선택합니다. 각 정책에 대한 설명을 보려면 드롭다운 목록에서 정책의 정보 아이콘을 클릭합니다.

사전 정의된 정책에 대한 자세한 내용은 시스템 정의 네트워크 분석 및 침입 정책의 내용을 참조하십시오.

파일 정책 설정

악성코드 방어를 사용해 악의적인 소프트웨어 또는 악성코드를 탐지하기 위해 파일 정책을 사용합니다. 파일 제어를 수행하는 데에도 파일 정책을 사용할 수 있습니다. 그러면 파일에 악성코드가 있는지와 관계없이 특정 유형의 모든 파일에 대한 제어가 가능합니다.

악성코드 방어는 Secure Malware Analytics Cloud를 사용하여 네트워크 트래픽에서 탐지될 가능성이 있는 악성코드의 상태를 검색하고 로컬 악성코드 분석 및 파일 사전 분류 업데이트를 가져옵니다. 관리 인터페이스에는 Secure Malware Analytics Cloud에 연결하고 악성코드 조회를 수행하기 위한 인터넷으로 연결되는 경로가 있어야 합니다. 디바이스는 적합한 파일을 탐지하면 파일의 SHA-256 해시 값을 사용하여 Secure Malware Analytics Cloud에서 파일의 상태를 쿼리합니다. 가능한 상태는 다음과 같습니다.

- Malware(악성코드) - Secure Malware Analytics Cloud가 파일을 악성코드로 분류했습니다. 아카이브 파일(예: zip 파일)은 해당 파일 내에 악성코드인 파일이 있으면 악성코드로 표시됩니다.
- Clean(정상) - Secure Malware Analytics Cloud가 파일을 악성코드가 포함되어 있지 않은 정상 파일로 분류했습니다. 아카이브 파일은 해당 파일 내의 모든 파일이 정상이면 정상으로 표시됩니다.
- Unknown(알 수 없음) - Secure Malware Analytics Cloud가 파일에 상태를 아직 할당하지 않았습니다. 아카이브 파일은 해당 파일 내에 알 수 없는 상태의 파일이 있으면 알 수 없음으로 표시됩니다.
- Unavailable(사용할 수 없음) - 시스템이 Secure Malware Analytics Cloud를 쿼리하여 파일의 상태를 확인하지 못했음을 나타냅니다. 이 속성을 통해 이벤트의 일부를 확인할 수 있습니다. 이는 예상된 작업입니다. "사용할 수 없음" 이벤트가 연속하여 여러 개 표시되는 경우에는 관리 주소에 대한 인터넷 연결이 정상적으로 작동하는지 확인하십시오.

사용 가능한 파일 정책

다음 파일 정책 중 하나를 선택할 수 있습니다.

- **None(**없음**)** - 전송된 파일에서 악성코드를 평가하지 않으며 파일별 차단을 수행하지 않습니다. 파일 전송을 신뢰할 수 있거나 거의 또는 전혀 수행될 가능성이 없는 규칙 또는 애플리케이션이나 URL 필터링이 네트워크를 적절하게 보호한다고 확신할 수 있는 규칙의 경우 이 옵션을 선택합니다.
- **Block Malware All(**악성코드 모두 차단**)** - 네트워크를 지나는 파일이 악성코드를 포함하는지 확인한 다음 위협이 되는 파일을 차단하기 위해 Secure Malware Analytics Cloud에 쿼리합니다.
- **Cloud Lookup All(**모두 클라우드 조회**)** - 네트워크를 지나는 파일의 전송을 허용하되 그 파일의 속성을 확인하고 로깅하기 위해 Secure Malware Analytics Cloud에 쿼리합니다.
- **(Custom File Policy(**맞춤형 파일 정책**))** - threat defense API filepolicies 리소스 및 기타 FileAndMalwarePolicies 리소스(예: filetypes, filetypecategories, ampcloudconfig, ampservers, 및 ampcloudconnections)를 사용하여 고유한 파일 정책을 생성할 수 있습니다. 정책을 생성하고 변경 사항을 구축한 후에는 device manager에서 액세스 제어 규칙을 수정할 때 정책을 선택할 수 있습니다. 정책 설명은 정책을 선택하면 해당 정책 아래에 표시됩니다.

로깅 설정

액세스 규칙의 로깅 설정에 따라 규칙과 일치하는 트래픽에 대해 연결 이벤트가 생성되는지가 결정됩니다. 이벤트 뷰어에서 규칙과 관련된 이벤트를 확인하려면 로깅을 활성화해야 합니다. 또한, 시스템을 모니터링하는 데 사용할 수 있는 여러 대시보드에 일치하는 트래픽을 반영하려는 경우에도 로깅을 활성화해야 합니다.

조직의 보안 및 규정 준수 필요에 따라 연결을 로깅해야 합니다. 사용자가 생성하고 기능을 향상시키는 이벤트의 수를 제한하는 것이 사용자의 목표라면 사용자의 분석에 중요한 연결에 대한 로깅만 사용 설정합니다. 그러나, 자료 수집을 목적으로 사용자의 네트워크 트래픽에 대한 광범위한 견해를 원할 경우, 추가 연결에 대한 로깅을 사용 설정할 수 있습니다.

주의 DoS(서비스 거부) 공격 중에 차단된 TCP 연결을 로깅하는 경우 시스템 성능에 영향을 미칠 수 있으며, 데이터베이스가 유사한 다수의 이벤트로 가득 찰 수 있습니다. 차단 규칙에 대한 로깅을 활성화하기 전에 이 규칙이 인터넷 연결 인터페이스 또는 DoS 공격에 취약한 다른 인터페이스용인지를 고려하십시오.

다음과 같은 로깅 작업을 구성할 수 있습니다.

로그 작업 선택

다음 작업 중 하나를 선택할 수 있습니다.

- 연결 시작 및 종료 시 로깅 - 연결 시작 및 종료 시에 이벤트를 생성합니다. 연결 종료 이벤트는 연결 시작 이벤트에 포함된 모든 항목과 연결 중에 수집되었을 수 있는 모든 정보를 포함하므로 허용하는 트래픽에 대해서는 이 옵션을 선택하지 않는 것이 좋습니다. 두 이벤트를 모두 로깅하면 시스템 성능에 영향을 줄 수 있습니다. 하지만 차단된 트래픽의 경우에는 이 옵션만 사용할 수 있습니다.
- 연결 종료 시 로깅 - 연결 종료 시에 연결 로깅을 활성화하려면 이 옵션을 선택합니다. 허용되는 트래픽이나 신뢰하는 트래픽의 경우 이 옵션을 선택하는 것이 좋습니다.
- 연결 시 로깅하지 않음 - 규칙에 대해 로깅을 비활성화하려면 이 옵션을 선택합니다. 이는 기본값입니다.

참고 액세스 제어 규칙이 호출한 침입 정책이 침입을 탐지하고 침입 이벤트를 생성하면, 시스템은 규칙의 로깅 컨피그레이션에 상관없이 침입이 발생한 연결의 종료를 자동으로 로깅합니다. 침입이 차단된 연결을 위한 연결 로그 내 연결 작업은 **Block(**차단**)**입니다. 그 이유는 **Intrusion Block(**침입 차단**)**이며, 침입 탐지 수행을 위해서라면 반드시 Allow(허용) 규칙을 사용해야 합니다.

파일 이벤트

금지된 파일 또는 악성코드 이벤트 로깅을 활성화하려면 **Log Files(**로그 파일**)**를 선택합니다. 이 옵션을 구성하려면 규칙에서 파일 정책을 선택해야 합니다. 규칙에 대해 파일 정책을 선택하는 경우 기본값으로 이 옵션을 활성화합니다. 이 옵션은 활성화된 상태로 유지하는 것이 좋습니다.

시스템은 금지된 파일을 탐지하면 다음과 같은 유형의 이벤트 중 하나를 자동으로 로깅합니다.

- 파일 이벤트 - 악성코드 파일을 포함하여 탐지되거나 차단된 파일을 나타냅니다.
- 악성코드 이벤트 - 탐지되거나 차단된 악성코드 파일만 나타냅니다.
- 소급 적용되는 악성코드 이벤트 - 이전에 탐지된 파일에 대한 악성코드 상태가 변경되는 경우 생성됩니다.

파일이 차단된 경우의 연결을 위한 연결 로그 내 연결 작업은 **Block(**차단**)**입니다. 파일 또는 악성코드 탐지를 수행하려는 경우에도 Allow(허용) 규칙을 사용해야 합니다. 연결하는 이유는 파일

모니터링(파일 유형 또는 악성코드가 탐지된 경우), 악성코드 차단 또는 파일 차단(파일이 차단된 경우)입니다.

다음으로 연결 이벤트 보내기

외부 syslog 서버로 이벤트의 복사본을 전송하려는 경우 syslog 서버를 정의하는 서비스 개체를 선택합니다. 필요한 개체가 아직 없으면 **Create New Syslog Server(**새 **Syslog** 서버 생성**)**를 클릭하여 개체를 생성합니다. syslog 서버에 대한 로깅을 비활성화하려면 서버 목록에서 **Any(**모두**)**를 선택합니다.

디바이스의 이벤트 스토리지는 제한되어 있으므로 외부 syslog 서버로 이벤트를 전송하면 더 장기적으로 저장할 수 있으며 이벤트 분석 성능이 개선됩니다.

이 설정은 연결 이벤트에만 적용됩니다. Syslog에 침입 이벤트를 전송하려면 침입 정책 설정에서 서버를 컨피그레이션하십시오. syslog에 파일/악성코드 이벤트를 전송하려면 **Device(**디바이스**)** > **System Settings(**시스템 설정**)** > **Logging Settings(**기록 설정**)**에서 서버를 컨피그레이션하십시오.

액세스 제어 정책 모니터링

다음 주제에서는 액세스 제어 정책을 모니터링하는 방법에 대해 설명합니다.

대시보드에서 액세스 제어 통계 모니터링

모니터링 대시보드에 있는 대부분의 데이터는 액세스 제어 정책과 직접적으로 관련되어 있습니다. 트래픽 및 시스템 대시보드 모니터링의 내용을 참조하십시오.

- **Monitoring(**모니터링**)** > **Access And SI Rules(**액세스 및 **SI** 규칙**)**에는 가장 많이 적중한 액세스 규칙, 보안 인텔리전스 규칙에 상응하는 규칙 및 관련 통계가 표시됩니다.
- 일반적인 통계는 **Network Overview(**네트워크 개요**)**, **Destinations(**대상**)**, **Zones(**영역**)**, 대시보드에서 확인할 수 있습니다.
- URL 필터링 결과는 **URL Categories(URL** 카테고리**)** 및 **Destinations(**대상**)** 대시보드에서 확인할 수 있습니다. **URL Categories(URL** 카테고리**)** 대시보드에서 정보를 확인하려면 하나 이상의 URL 필터링 정책이 있어야 합니다.
- 애플리케이션 필터링 결과는 **Applications(**애플리케이션**)** 및 **Web Applications(**웹 애플리케이션**)** 대시보드에서 확인할 수 있습니다.
- 사용자 기반 통계는 **Users(**사용자**)** 대시보드에서 확인할 수 있습니다. 사용자 정보를 수집하려면 ID 정책을 구현해야 합니다.
- 침입 정책 통계는 **Attackers(**공격자**)** 및 **Targets(**대상**)** 대시보드에서 확인할 수 있습니다. 이러한 대시보드에서 정보를 확인하려면 하나 이상의 액세스 제어 규칙에 침입 정책을 적용해야 합니다.

- 파일 정책 및 악성코드 필터링 통계는 **File Logs(**파일 로그**)** 및 **Malware(**악성코드**)** 대시보드에서 확인할 수 있습니다. 이러한 대시보드에서 정보를 확인하려면 하나 이상의 액세스 제어 규칙에 파일 정책을 적용해야 합니다.
- **Monitoring(**모니터링**)** > **Events(**이벤트**)**에는 액세스 제어 규칙과 관련된 데이터 및 연결에 대한 이벤트도 표시됩니다.

규칙 적중 횟수 검토

각 액세스 제어 규칙에 대한 적중 횟수를 볼 수 있습니다. 적중 횟수는 연결이 규칙과 얼마나 자주 일치했는지 나타냅니다. 이 정보를 사용해 가장 많이 활성화된 규칙과 덜 활성화된 규칙을 식별할 수 있습니다.

리부팅 및 업그레이드 시에도 개수가 유지됩니다.

프로시저

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

단계 **2** **Toggle Hit Counts(**적중 횟수 토글**)** 아이콘()을 클릭합니다.

적중 횟수 열은 규칙에 대한 총 적중 횟수와 최종 적중 날짜 및 시간과 함께 이름 열의 오른쪽에 표시됩니다. 적중 횟수 정보는 토글 버튼을 클릭하면 가져올 수 있습니다.

적중 횟수 정보로 할 수 있는 작업은 다음과 같습니다.

- 버튼 왼쪽에 적중 횟수가 마지막으로 업데이트된 시각에 관한 정보가 표시됩니다. 최신 횟수를 얻으려면 **refresh(**새로고침**)** 아이콘()을 클릭하십시오.
- 특정 규칙에 대한 적중 횟수 자세히 보기를 열려면 테이블에 있는 적중 횟수 번호를 클릭하여 적중 횟수 대화 상자를 여십시오. 적중 횟수 정보에는 적중 횟수와 규칙과 일치한 마지막 연결의 날짜 및 시간이 포함됩니다. 카운터를 0으로 재설정하려면 **Reset(**재설정**)** 링크를 클릭하십시오.

  한 번에 모든 규칙에 대한 적중 횟수를 재설정하려면 디바이스에 대한 SSH 세션을 열고 **clear rule hits** 명령을 실행하십시오.
- 테이블에서 적중 횟수 열을 제거하려면 **Toggle Hit Counts(**적중 횟수 토글**)** 아이콘()을 다시 클릭합니다.

액세스 제어에 대한 **Syslog** 메시지 모니터링

이벤트 뷰어에서 이벤트를 확인하는 것 외에도 액세스 제어 규칙, 침입 정책, 파일/악성코드 정책 및 보안 인텔리전스 정책을 컨피그레이션하여 syslog 서버로 이벤트를 전송할 수 있습니다. 이벤트에서는 다음 메시지 ID를 사용합니다.

- 430001 — 침입 이벤트

- 430002 — 연결 시작 시 기록된 연결 이벤트
- 430003 — 연결 종료 시 기록된 연결 이벤트
- 430004 — 파일 이벤트
- 430005 — 악성코드 이벤트

CLI에서 액세스 제어 정책 모니터링

CLI 콘솔을 열거나 디바이스 CLI에 로그인한 후에 다음 명령을 사용하여 액세스 제어 정책과 통계에 대한 상세 정보를 가져올 수도 있습니다.

- **show access-control-config** 액세스 제어 규칙에 대한 요약 정보를 규칙별 적중 횟수와 함께 표시합니다.
- **show access-list** 액세스 제어 규칙에서 생성된 ACL(Access Control Lists)을 표시합니다. ACL은 초기 필터를 제공하며 가능한 경우 항상 빠른 결정 제공을 시도하므로, 삭제해야 하는 연결을 검사할 필요가 없어 리소스가 불필요하게 사용되지 않습니다. 이 정보에는 적중 횟수가 포함됩니다.
- **show rule hits**에서는 **show access-control-config** 및 **show access-list**와 함께 표시된 횟수보다 더 정확한 통합 적중 횟수를 표시합니다. 적중 횟수를 재설정하려는 경우, **clear rule hits** 명령을 사용하십시오.
- **show snort statistics** 기본 검사기인 Snort 검사 엔진에 대한 정보를 표시합니다. Snort는 애플리케이션 필터링, URL 필터링, 침입 차단, 파일 및 악성코드 필터링을 구현합니다.
- **show conn** 인터페이스를 통해 현재 설정되어 있는 연결에 대한 정보를 표시합니다.
- **show traffic** 각 인터페이스를 통과하는 트래픽에 대한 통계를 표시합니다.
- **show ipv6 traffic** 디바이스를 통과하는 IPv6 트래픽에 대한 통계를 표시합니다.

액세스 제어의 예시

사용 사례 장에는 액세스 제어 규칙을 구현하는 몇 가지 예시가 포함되어 있습니다. 다음 예시를 참조하십시오.

- 네트워크 트래픽을 파악하는 방법. 이 예시는 전반적인 연결 및 사용자 정보 수집을 위한 몇 가지 기본적인 개념을 보여줍니다.
- 위협을 차단하는 방법. 이 예시는 침입 정책을 적용하는 방법을 보여줍니다.
- 악성코드를 차단하는 방법. 이 예시는 파일 정책을 적용하는 방법을 보여줍니다.
- 사용 제한 정책(URL 필터링)을 구현하는 방법. 이 예시는 URL 필터링을 수행하는 방법을 보여줍니다.

- 애플리케이션 사용량을 제어하는 방법. 이 예시는 애플리케이션 필터링을 수행하는 방법을 보여줍니다.
- 서브넷을 추가하는 방법. 이 예시는 트래픽 플로우를 허용하는 데 필요한 액세스 규칙을 비롯하여 전체 네트워크에 새 서브넷을 통합하는 방법을 보여줍니다.
- 네트워크에서 트래픽을 능동적으로 모니터링하는 방법

추가 예는 다음과 같습니다.

TrustSec SGT(Security Group Tag)를 사용하여 네트워크 액세스를 제어하는 방법

Cisco ISE(Identity Services Engine)를 사용하여 Cisco TrustSec 네트워크에서 트래픽을 분류하기 위해 SGT(Security Group Tag)를 정의하고 사용하는 경우, SGT를 일치 기준으로 사용하는 액세스 제어 규칙을 작성할 수 있습니다. 따라서 IP 주소가 아니라 보안 그룹 멤버십을 기준으로 직접 액세스를 차단하거나 허용할 수 있습니다.

SGT(Security Group Tag) 정보

Cisco ISE(Identity Services Engine)에서는 SGT(Security Group Tag)를 생성하고 각 태그에 호스트 또는 네트워크 IP 주소를 할당할 수 있습니다. 또한 사용자 어카운트에 SGT를 할당할 수 있으며, SGT는 사용자의 트래픽에 할당됩니다. 네트워크의 스위치와 라우터가 이 작업을 수행하도록 구성된 경우, 이러한 태그는 ISE, Cisco TrustSec 클라우드로 제어되는 네트워크에 진입할 때 패킷에 할당됩니다.

device manager에서 ISE ID 소스를 구성하면 threat defense 시스템에서는 ISE에서 SGT 목록을 자동으로 다운로드합니다. 그러면 액세스 제어 규칙에서 SGT를 트래픽 일치 조건으로 사용할 수 있습니다.

예를 들어, 프로덕션 사용자 태그를 생성하고 192.168.7.0/24 네트워크를 태그에 연결할 수 있습니다. 이는 노트북 컴퓨터, Wi-Fi 클라이언트 등의 사용자 엔드포인트에 해당 네트워크를 사용하는 경우에 적합합니다. 프로덕션 서버에 대한 별도의 태그를 생성하고 관련 서버 또는 서브넷의 IP 주소를 태그에 할당할 수 있습니다. 그런 다음에는, threat defense에서 태그를 기반으로 사용자 네트워크에서 프로덕션 서버로의 액세스를 허용하거나 차단할 수 있습니다. 나중에 ISE의 태그와 연결된 호스트 또는 네트워크 주소를 변경하는 경우에는 threat defense 디바이스에 대해 정의된 액세스 제어 규칙을 변경할 필요가 없습니다.

threat defense에서는 SGT를 액세스 제어 규칙에 대한 트래픽 일치 기준으로 평가하는 경우, 다음 우선순위를 사용합니다.

1. 패킷에 정의된 소스 SGT 태그(있는 경우). SGT 태그를 패킷에 포함하려면 네트워크의 스위치와 라우터를 추가하도록 구성해야 합니다. 이 메서드를 구현하는 방법에 대한 자세한 내용은 ISE 설명서를 참조하십시오.
2. ISE 세션 디렉토리에서 다운로드된 대로 사용자 세션에 할당된 SGT. 이러한 유형의 SGT 일치에 대한 세션 디렉토리 정보를 수신 대기하려면 해당 옵션을 활성화해야 합니다. 그러나 이 옵션은 처음에 ISE ID 소스를 생성할 때 기본적으로 켜집니다. SGT는 소스 또는 대상과 일치할 수 있습니다. 필수 사항은 아니지만 일반적으로 사용자 ID 정보를 수집하기 위해 AD 영역과 함께 ISE ID 소스를 사용하여 패시브 인증 ID 규칙도 설정합니다.

3. SXP를 사용하여 다운로드한 SGT-IP 주소 매핑. IP 주소가 SGT 범위 내에 있는 경우 트래픽은 SGT를 사용하는 액세스 제어 규칙과 일치합니다. SGT는 소스 또는 대상과 일치할 수 있습니다.

   ISE에서는 SXP(Security-group eXchange Protocol)를 사용하여 IP-SGT 매핑 데이터베이스를 네트워크 디바이스에 전파합니다. ISE 서버를 사용하도록 threat defense 디바이스를 구성하는 경우 ISE에서 SXP 항목을 수신 대기하려면 해당 옵션을 켜야 합니다. 따라서 threat defense 디바이스에서는 ISE에서 바로 SGT(Security Group Tag) 및 매핑에 대해 학습하며, ISE에서 업데이트된 SGT(Security Group Tag) 및 매핑을 게시할 때마다 알림을 받습니다. 이렇게 하면 SGT(Security Group Tag) 및 매핑 목록이 디바이스에서 최신 상태로 유지되므로 threat defense에서 ISE에 정의된 정책을 효과적으로 적용할 수 있습니다.

SGT(Security Group Tag)를 기반으로 액세스 제어 구성

SGT(Security Group Tag)를 일치 기준으로 사용하는 액세스 제어 규칙을 구성하려면 먼저 ISE 서버에서 SGT 매핑을 가져오도록 디바이스를 구성해야 합니다.

다음 절차에서는 SXP를 통해 게시된 SGT-IP 주소 매핑을 비롯하여 ISE에 정의되어 있는 모든 매핑을 가져오려고 한다는 가정 하에 엔드 투 엔드 프로세스에 대해 설명합니다. 다른 방법은 다음과 같습니다.

- 패킷에서만 SGT 정보를 사용하고 ISE에서 다운로드한 매핑을 사용하지 않으려면 SGT 그룹 동적 개체를 간단하게 생성하여 액세스 제어 규칙에서 소스 SGT 기준으로 사용하면 됩니다. 이 경우에는 SGT 태그를 소스 조건으로만 사용할 수 있으며 이러한 태그는 대상 기준과 일치하지 않습니다.
- 패킷에 있는 SGT를 사용자 세션 SGT 매핑하고만 사용하려는 경우 ISE ID 소스의 SXP 항목을 구독하도록 옵션을 설정할 필요가 없으며 SXP 매핑을 게시하도록 ISE를 구성할 필요도 없습니다. 소스 및 대상 일치 조건 둘 다에 이 정보를 사용할 수 있습니다.

시작하기 전에

이 섹션에서는 네트워크에서 이미 Cisco TrustSec을 구성했으며 단순하게 정책 적용 시점으로 threat defense 디바이스를 추가하는 것으로 가정합니다. Cisco TrustSec을 구축하지 않은 경우 ISE로 시작하여 네트워크를 구성한 다음, 이 절차로 돌아오십시오. Cisco TrustSec에 대한 설명은 이 문서에 포함되어 있지 않습니다.

프로시저

단계 **1** SGT가 정의되었는지, ISE가 SXP 주제를 게시하도록 올바르게 구성되었는지, 필요한 정적 매핑이 있는지 확인합니다.

ISE에서 보안 그룹 및 SXP 게시 구성, 37 페이지의 내용을 참조하십시오.

단계 **2** SXP 주제를 수신하도록 Identity Services Engine 개체를 업데이트합니다.

ISE를 사용하여 사용자 세션 SGT 매핑, SXP를 통한 정적 SGT-IP 주소 매핑 또는 둘 다를 가져올 수 있습니다. 기본적으로 ISE ID 소스를 구성하면 사용자 세션 매핑만 가져오게 됩니다. ISE에서 SXP 항목을 수신 대기하려면 해당 옵션을 켜야 합니다.

a) **Objects(**개체**)** > **Identity Sources(ID** 소스**)**를 선택합니다.
b) ISE 개체를 수정합니다. 아직 이를 구성하지 않은 경우 **+** > **Identity Services Engine**을 클릭하여 ISE(Identity Services Engine) 구성를 확인합니다.
c) **Subscribe To(**구독 대상**)**에서 **SXP Topic(SXP** 주제**)**을 선택합니다.

패시브 인증을 사용하거나 user-to-SGT 매핑을 원하는 경우 **Session Directory Topic(**세션 디렉토리 주제**)**도 선택했는지 확인합니다.

d) **OK(**확인**)**를 클릭합니다.

단계 **3** 변경 사항을 구축하고 시스템이 ISE에서 태그 및 매핑을 다운로드할 때까지 기다립니다.

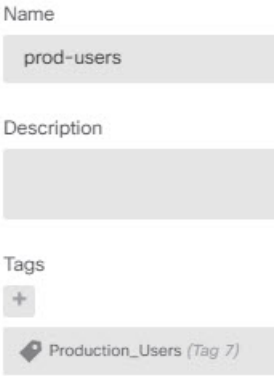
ISE ID 소스를 구성하고 변경 사항을 구축하고 나면 시스템에서는 ISE 서버에서 SGT(Security Group Tag) 정보를 검색합니다. 변경 사항을 구축할 때까지는 다운로드가 수행되지 않습니다.

단계 **4** 액세스 제어 규칙에 필요한 SGT 그룹 개체를 생성합니다.

ISE에서 검색된 정보는 액세스 제어 규칙에서 바로 사용할 수 없습니다. 대신, 다운로드한 SGT 정보를 참조하는 SGT 그룹을 생성해야 합니다. SGT 그룹에서는 둘 이상의 SGT를 참조할 수 있으므로 적절한 경우 관련된 태그 컬렉션을 기준으로 정책을 적용할 수 있습니다.

개체의 수와 내용은 작성하려는 액세스 제어 규칙에 따라 달라집니다. 필요한 모든 개체를 생성하려면 다음 프로세스를 반복합니다.

a) **Objects(**개체**)** > **SGT Group(SGT** 그룹**)**을 선택합니다.
b) **+**를 클릭하여 새 개체를 추가하거나 기존 개체를 수정합니다.
c) 새 개체의 이름을 입력하고 필요한 경우 설명을 입력합니다.
d) **Tags(**태그**)**에서 **+**를 클릭하고 그룹에 포함해야 하는 모든 태그를 선택합니다.



e) **OK(**확인**)**를 클릭합니다.

단계 **5** SGT 그룹 개체를 사용하는 액세스 제어 규칙을 생성합니다.

예를 들면, 아래의 규칙에서는 프로덕션 사용자에게서 프로덕션 서버로 향하는 트래픽을 허용합니다. 이 규칙은 전적으로 SGT에 달려 있으며, 소스/대상 인터페이스 또는 기타 기준으로 제한되지 않습니다. 따라서 규칙은 서로 다른 인터페이스에서 오는 경우 및 ISE에서 보안 그룹 멤버십을 변경하

는 경우 트래픽에 동적으로 적용됩니다. 패킷에 소스 SGT가 명시적으로 포함되지 않은 경우, 소스/대상 일치는 사용자 세션 정보 또는 SXP에서 게시된 매핑에서 가져온 SGT-IP 주소 매핑과 비교하여 패킷 IP 주소를 기반으로 합니다.

a) **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 선택합니다.
b) 새 규칙을 생성하거나 기존 규칙을 수정하려면 **+**를 클릭합니다.
c) 규칙 이름을 입력하고 작업으로 **Allow(**허용**)**를 선택합니다.
d) **Source/Destination(**소스/대상**)** 탭에서 **Source(**소스**)** > **SGT Groups(SGT** 그룹**)**아래에서 **+**를 클릭하고 프로덕션 사용자 용으로 생성한 개체를 선택합니다.
e) **Source/Destination(**소스/대상**)** 탭의 **Destination(**대상**)** > **SGT Groups(SGT** 그룹**)**아래에서 **+**를 클릭하고 프로덕션 서버용으로 생성한 개체를 선택합니다.
f) 필요에 따라 다른 옵션을 구성합니다. 예를 들어 로깅을 활성화하고 침입 정책을 적용할 수 있습니다.
g) **OK(**확인**)**를 클릭합니다.

단계 **6** 컨피그레이션을 구축합니다.

ISE에서 보안 그룹 및 SXP 게시 구성

TrustSec 정책 및 SGT(Security Group Tag)를 생성하려면 Cisco ISE(Identity Services Engine)에서 수행해야 할 구성이 많이 있습니다. TrustSec을 구현하는 방법에 대한 더 자세한 내용은 ISE 설명서를 참조하십시오.

다음 절차에서는 ISE에서 threat defense 디바이스에 대해 구성해야 하는 핵심 설정의 중요 사항을 골라서 설명하므로 이를 따라 정적 SGT-IP 주소 매핑을 다운로드하고 적용할 수 있습니다. 그러면 이 매핑을 액세스 제어 규칙에서 소스 및 대상 SGT 일치에 사용할 수 있습니다. 자세한 내용은 ISE 설명서를 참조하십시오.

이 절차의 스크린 샷은 ISE 2.4를 기준으로 합니다. 이러한 기능에 대한 정확한 경로는 이후 릴리스에서 변경될 수 있지만 개념 및 요구 사항은 동일합니다. ISE 2.4 이상 및 2.6 이상 버전이 권장되더라도 구성은 ISE 2.2 패치 1부터 작동해야 합니다.

시작하기 전에

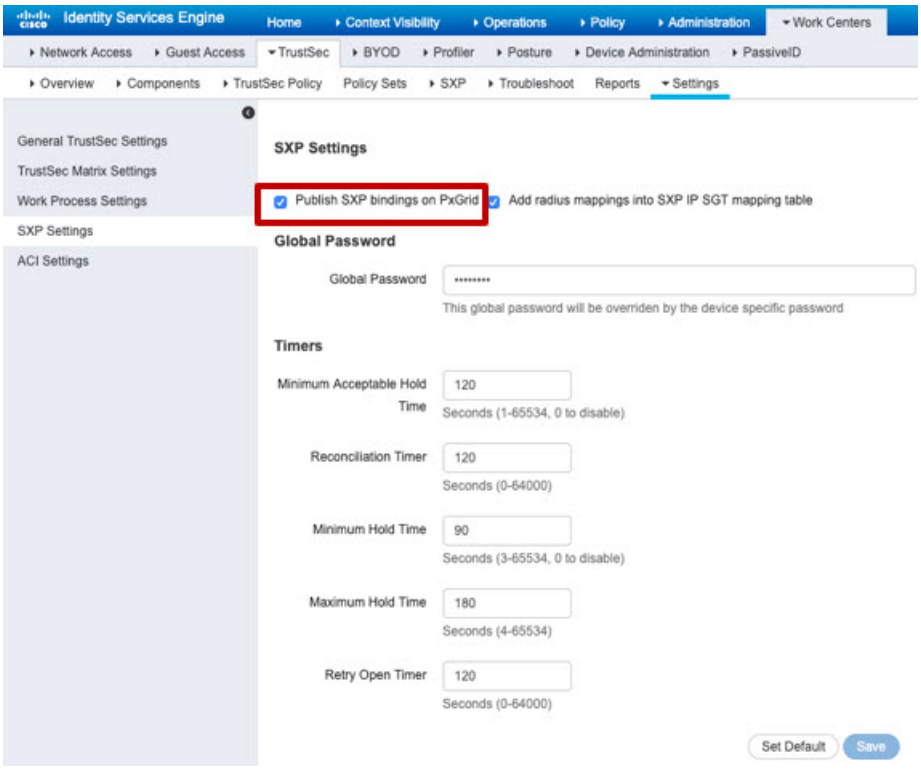
SGT-IP 주소 정적 매핑을 게시하고, 사용자 세션-SGT 매핑을 가져와 threat defense 디바이스가 이를 수신할 수 있도록 하려면 ISE Plus 라이선스가 있어야 합니다.

프로시저

단계 **1** **Work Center(**작업 센터**)** > **TrustSec** > **Settings(**설정**)** > **SXP Settings(SXP** 설정**)**를 선택하고 **Publish SXP Bindings on PxGrid(PxGrid**에서 **SXP** 바인딩 게시**)** 옵션을 선택합니다.

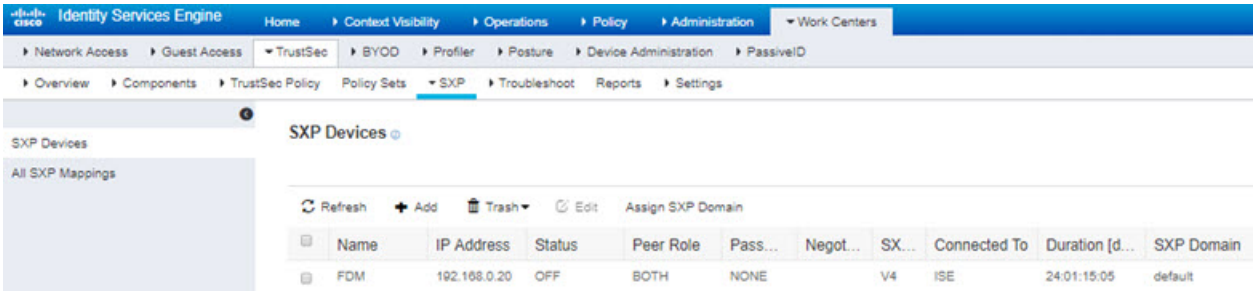
이 옵션을 선택하면 ISE에서 SXP를 사용하여 SGT 매핑을 전송합니다. threat defense 디바이스에서 SXP 항목에 대한 목록의 내용을 "수신 대기"하도록 설정하려면 이 옵션을 선택해야 합니다. 정적 SGT-IP 주소 매핑에 대한 정보를 가져오려면 threat defense 디바이스에 대해 이 옵션을 선택해야 합니

다. 단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 옵션이 필수 사항이 아닙니다.

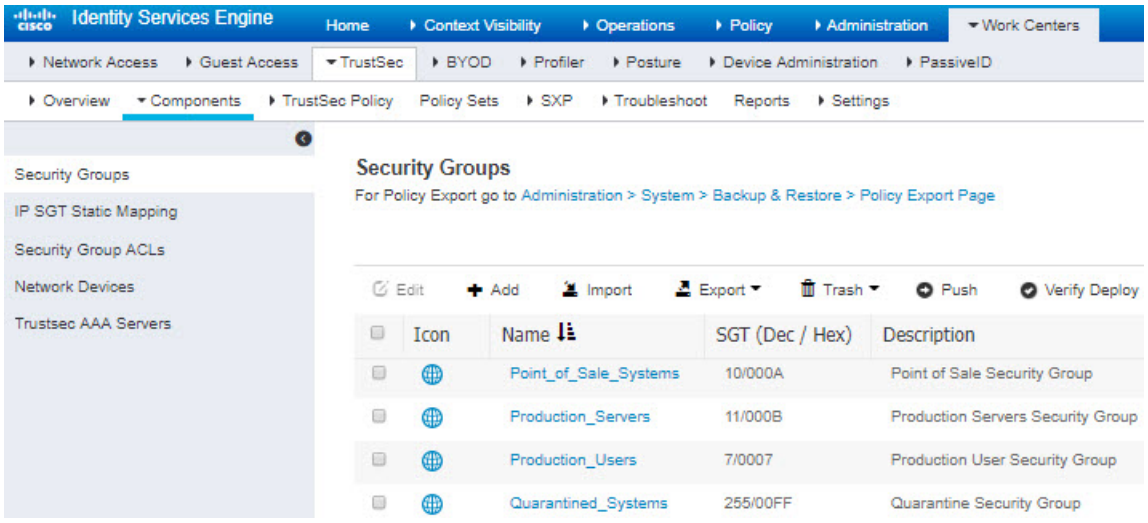


단계 **2** **Work Centers(**작업 센터**)** > **TrustSec** > **SXP** > **SXP Devices(SXP** 디바이스**)**를 선택하고 디바이스를 추가합니다.

이 디바이스가 실제 디바이스일 필요는 없으며, threat defense 디바이스의 관리 IP 주소를 사용할 수도 있습니다. 이 표에는 ISE에서 정적 SGT-IP 주소 매핑을 게시하도록 유도하는 디바이스가 하나 이상 필요합니다. 단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 단계가 필수 사항이 아닙니다.



단계 **3** **Work Centers(**작업 센터**)** > **TrustSec** > **Components(**구성 요소**)** > **Security Groups(**보안 그룹**)**를 선택하고 SGT(Security Group Tag)가 정의되어 있는지 확인합니다. 필요에 따라 새로 생성합니다.



단계 **4** **Work Centers(**작업 센터**)** > **TrustSec** > **Components(**구성 요소**)** > **IPSGT Static Mapping(IPSGT** 정적 매핑**)**을 선택하고 호스트 및 네트워크 IP 주소를 SGT(Security Group Tag)에 매핑합니다.

단순히 패킷에 정의된 SGT 태그 또는 사용자 세션에 할당된 SGT를 사용하려는 경우에는 이 단계가 필수 사항이 아닙니다.