액세스 제어의 모범 사례

액세스 제어의 모범 사례

다음 요구 사항 및 일반적인 모범 사례를 검토합니다.

- 구축에 라이선스를 부여하지 않고 시스템을 구성할 수는 있지만, 대부분의 기능을 사용하려면 구축 전에 적절한 라이선스를 활성화해야 합니다.
- 시스템이 트래픽에 영향을 미치려면 라우팅, 스위칭 또는 투명 인터페이스 또는 인라인 인터페이스 쌍을 사용하여 관련 구성을 매니지드 디바이스에 구축해야 합니다.

  경우에 따라 시스템에서는 탭 모드의 인라인 디바이스를 비롯하여 수동으로 구축된 디바이스에 인라인 구성을 구축하지 못하도록 할 수 있습니다.

  다른 경우에는 정책이 성공적으로 구축될 수 있지만 수동 구축된 디바이스를 사용하여 트래픽을 차단하거나 변경하려고 하면 예상치 못한 결과가 발생할 수 있습니다. 예를 들어, 차단된 연결이 수동 배포에서 실제로 차단되는 것은 아니기 때문에 시스템은 각 차단된 연결에 대한 여러 초기 연결 이벤트를 보고할 수 있습니다.
- URL 필터링, 애플리케이션 탐지, 지능형 애플리케이션 우회를 비롯한 특정 기능은 시스템에서 트래픽을 식별하기 위해 일부 패킷이 통과하도록 허용해야 합니다.

  이러한 패킷이 검사되지 않은 대상에 도달하지 못하도록하려면 트래픽 식별 전에 통과하는 패킷 처리를 위한 모범 사례 및 트래픽 식별 전에 통과하는 패킷을 처리할 정책 지정의 내용을 참조하십시오.
- 액세스 제어 정책의 기본 작업에 의해 처리되는 트래픽에 대해서는 파일 또는 악성코드 검사를 수행할 수 없습니다.
- 일부 기능은 특정 디바이스 모델에서만 사용할 수 있습니다. 경고 아이콘 및 확정 대화 상자는 지원되지 않는 기능을 지정합니다.

- 시스템 로그를 사용하거나 이벤트를 외부에 저장하려는 경우, 정책 및 규칙 이름과 같은 개체 이름에 특수 문자를 사용하지 마십시오. 개체 이름은 수신 애플리케이션에서 구분자로 사용할 수 있는 특수 문자(예: 쉼표)를 포함해서는 안 됩니다.
- 기본 작업으로 처리되는 연결에 대한 로깅은 초기에는 비활성화되어 있지만 활성화할 수는 있습니다.
- 액세스 제어 규칙 생성, 순서 지정 및 구현에 대한 모범 사례는 액세스 제어 규칙 순서에 대한 모범 사례, 2 페이지 및 하위 주제에 자세히 설명되어 있습니다.

액세스 제어 규칙 순서에 대한 모범 사례

효과적인 구축을 위해서는 규칙을 올바르게 구성하고 그 순서를 지정해야 합니다. 다음 주제는 규칙 성능 지침을 요약합니다.

참고 컨피그레이션 변경 사항을 구축할 때 시스템은 모든 규칙을 함께 평가하며, 타겟 디바이스가 네트워크 트래픽을 평가하는 데 사용하는 확장된 기준 집합을 생성합니다. 이러한 기준이 타겟 디바이스의 리소스(물리적 메모리, 프로세서 등)를 초과할 경우, 해당 디바이스에 구축할 수 없습니다.

관련 항목

애플리케이션 제어 모범 사례
URL 필터링 모범 사례

규칙 순서 지정 모범 사례

일반 지침:

- 일반적으로 정책 상단에서 모든 트래픽에 적용되는 최우선 규칙을 지정합니다.
- 구체적인 규칙은 일반적인 규칙보다 먼저 배치해야 합니다(특히, 구체적인 규칙이 일반적인 규칙에 대한 예외인 경우).

  그렇지 않으면 트래픽이 일반 규칙과 먼저 일치하며 적용 가능한 특정 규칙에 도달하지 않습니다.
- 구체적인 삭제 규칙은 가능한 경우 항상 정책 상위에 둡니다. 이렇게 하면 부적절한 트래픽에 대해 가능한 한 빠른 결정을 내릴 수 있습니다.
- IP 주소, 보안 영역, 포트 번호 등 레이어-3/4 기준만을 기반으로 하여 트래픽을 삭제하는 규칙은 가능한 한 먼저 배치해야 합니다.
- URL 필터링 규칙, 애플리케이션 규칙 및 검사가 필요한 기타 규칙은 레이어 3/4 기준(예: IP 주소, 보안 영역, 포트 번호)만을 바탕으로 트래픽을 삭제하는 규칙 뒤에 와야 하며, 파일 및 침입 정책을 지정하는 규칙 앞에 와야 합니다.

- URL 필터링 규칙을 애플리케이션 규칙 위에 두고, 마이크로 애플리케이션 규칙 및 CIP(Common Industrial Protocol) 하위 분류 애플리케이션 필터링 규칙을 사용하여 애플리케이션 규칙을 따릅니다.
- 파일 정책 및 침입 정책을 지정하는 규칙은 규칙 순서의 맨 아래에 와야 합니다. 이러한 규칙에는 리소스를 많이 사용하는 심층 검사가 필요하며, 심층 검사가 필요한 잠재적인 위협 수를 최소화하려면 성능상의 이유로 먼저 덜 집중적인 방법을 사용하여 최대한 많은 위협을 제거해야 합니다.
- 항상 조직의 요구 사항에 맞게 규칙의 순서를 지정해야 합니다.

위의 지침에 대한 예외 및 추가 사항은 아래 섹션에 나와 있습니다.

규칙 선점

평가 순서에서 앞서는 규칙이 트래픽에 우선 일치하기 때문에 규칙이 트래픽과 일치하지 않는 경우 규칙 선점이 발생합니다. 규칙의 조건은 다른 규칙의 선점 여부를 제어합니다. 다음 예에서는 첫 번째 규칙이 관리 트래픽을 허용하기 때문에 두 번째 규칙이 차단할 수 없습니다.

액세스 제어 규칙 1: 관리자 사용자 허용
액세스 제어 규칙 2: 관리자 사용자 차단

모든 유형의 규칙 조건은 후속 규칙에 사전 대응할 수 있습니다. 첫 번째 SSL 규칙의 VLAN 범위는 VLAN을 두 번째 규칙으로 포함하므로 첫 번째 규칙이 두 번째 규칙보다 사전에 대응합니다.

SSL 규칙 1: VLAN 22-33을 암호화하지 않음
SSL 규칙 2: VLAN 27 차단

다음 예에서는 VLAN이 설정되지 않아 규칙 1이 모든 VLAN과 일치하므로 규칙 1이 VLAN 2에 일치시키려는 규칙 2를 선점합니다.

액세스 제어 규칙 1: 소스 네트워크 10.4.0.0/16 허용
액세스 제어 규칙 2: 소스 네트워크 10.4.0.0/16, VLAN 2 허용

규칙은 또한 선점합니다.

액세스 제어 규칙 1: VLAN 1 URL www.example.com 허용
액세스 제어 규칙 2: VLAN 1 URL www.example.com 허용

후속 규칙은 조건이 다른 경우 사전 대응되지 않습니다.

액세스 제어 규칙 1: VLAN 1 URL www.example.com 허용
액세스 제어 규칙 2: VLAN 2 URL www.example.com 허용

규칙은 모든 설정 조건이 동일한 후속 규칙을 선점합니다.

QoS 규칙 1: VLAN 1 URL www.netflix.com 속도 제한
QoS 규칙 2: VLAN 1 URL www.netflix.com 속도 제한

조건이 다른 경우 후속 규칙의 선점이 발생하지 않습니다.

QoS 규칙 1: VLAN 1 URL www.netflix.com 속도 제한
QoS 규칙 2: VLAN 2 URL www.netflix.com 속도 제한

예: 사전 대응을 방지하기 위해 **SSL** 규칙 순서 지정

예를 들어 신뢰받는 CA(Good CA)에서 악성 엔티티(Bad CA)에 CA 인증서를 잘못 발급했지만 아직 그 인증서를 폐기하지 않았습니다. 신뢰할 수 없는 CA에서 발행한 인증서로 암호화된 트래픽을 차단하지만 신뢰할 수 있는 CA의 신뢰 체인의 트래픽은 허용하는 SSL 정책을 사용하려 합니다. CA 인증서 및 모든 중간 CA 인증서를 업로드한 후 다음 순서에 따라 규칙이 포함된 SSL 정책을 구성합니다.

SSL 규칙 1: 발급자 차단 CN=www.badca.com
SSL 규칙 2: 발급자 암호 해독 안 함 CN=www.goodca.com

규칙을 반대로 설정할 경우 불량 CA가 신뢰하는 트래픽을 포함해 우수한 CA가 신뢰하는 모든 트래픽을 우선 일치시킵니다. 어떤 트래픽도 이후의 불량 CA 규칙에 일치시키지 않으므로 악성 트래픽이 차단되지 않고 허용될 수 있습니다.

규칙 작업 및 규칙 순서

규칙의 작업은 시스템에서 일치하는 트래픽을 처리하는 방법을 결정합니다. 추가로 트래픽 처리를 수행하거나 확인하여 리소스를 많이 소모하는 규칙 앞에 그렇지 않은 규칙을 배치하면 성능이 향상됩니다. 시스템은 검사 대상이었던 트래픽으로 전환할 수 있습니다.

다음 예는 여러 정책에서 중요 규칙이 없고 사전 대응이 문제가 되지 않는 규칙 집합 중 규칙 순서를 정하는 방법을 나타냅니다.

규칙이 애플리케이션 조건을 포함하는 경우에도 애플리케이션 제어 구성 모범 사례의 내용을 참조하십시오.

최적의 순서: **SSL** 규칙

암호 해독뿐 아니라 암호 해독된 트래픽의 추가 분석에도 리소스를 필요로 합니다. 트래픽의 암호를 해독하는 SSL 규칙을 나중에 배치하십시오.

1. 모니터링 - 일치하는 연결을 기록하지만 트래픽에 다른 작업을 수행하지 않는 규칙
2. 차단, 재설정과 함께 차단 - 추가 검사 없이 트래픽을 차단하는 규칙입니다.
3. 암호 해독 안 함 - 암호화된 트래픽의 암호를 해독하지 않고 암호화된 세션을 액세스 제어 규칙에 전달하는 규칙 이런 세션의 페이로드는 심층 검사 대상이 아닙니다.
4. 암호 해독 - 알려진 키 - 확인된 개인 키로 수신 트래픽을 암호 해독하는 규칙
5. 암호 해독 - 다시 서명 - 서버 인증서에 다시 서명을 하여 발신 트래픽을 암호 해독하는 규칙

최적의 순서: 액세스 제어 규칙

특히 여러 사용자 정의 침입 정책과 변수 집합을 사용하는 경우 침입, 파일, 악성코드 검사 시 리소스를 사용합니다. 심층 검사를 마지막으로 호출하는 액세스 제어 규칙을 배치합니다.

1. 모니터링 - 일치하는 연결을 기록하지만 트래픽에 다른 작업을 수행하지 않는 규칙 (액세스 제어 규칙 모니터 작업에서 중요 예외 및 주의 사항을 확인하십시오.)

2. 신뢰, 차단, 재설정과 함께 차단 - 추가 검사 없이 트래픽을 처리하는 규칙 신뢰할 수 있는 트래픽에는 ID 정책에 적용된 인증 요건 및 속도 제한이 적용됩니다.
3. 허용, 상호 작용 차단(심층 검사 없음) - 트래픽을 추가로 검사하지 않지만 검색을 허용하는 규칙 허용된 트래픽에는 ID 정책에 적용된 인증 요건 및 속도 제한이 적용됩니다.
4. 허용, 상호 작용 차단(심층 검사) - 금지된 파일, 악성코드, 익스플로잇에 대해 심층 검사를 수행하는 파일 또는 침입 정책과 관련된 규칙

콘텐츠 제한 규칙 순서

SSL 및 액세스 제어 정책 둘 다에서 규칙 사전 대응을 방지하려면 YouTube 제한 관리 규칙을 안전 검색 제한 관리 규칙 위에 배치합니다.

액세스 제어 규칙에 대해 Safe Search를 활성화하면 시스템은 선택된 애플리케이션 및 필터 목록에 `검색 엔진` 카테고리를 추가합니다. 이 애플리케이션 카테고리에는 YouTube가 포함됩니다. 그러므로 평가 우선 순위가 더 높은 규칙에서 YouTube EDU를 활성화하는 경우가 아니면 YouTube 트래픽은 안전 검색 규칙과 일치하게 됩니다.

`safesearch supported` 필터가 포함된 SSL 규칙을 평가 순서에서 특정 YouTube 애플리케이션 조건이 포함된 SSL 규칙보다 상위 위치에 배치하는 경우 이와 유사한 규칙 사전 대응이 수행됩니다.

애플리케이션 규칙 순서

애플리케이션 조건이 포함된 규칙은 목록에서 낮은 순서로 이동할 경우 트래픽과 일치할 가능성이 높습니다.

특정 조건(예: 네트워크 및 IP 주소)을 사용하는 액세스 제어 규칙은 일반 조건(예: 애플리케이션)을 사용하는 규칙보다 앞에 배치합니다. OSI(Open Systems Interconnect) 모델에 익숙하다면 컨셉이 유사한 번호를 사용합니다. 계층 1, 2 및 3(물리적, 데이터 링크 및 네트워크)에 대한 조건이 있는 규칙은 액세스 제어 규칙의 앞부분에 배치합니다. 계층 5, 6 및 7(세션, 프레젠테이션 및 애플리케이션)에 대한 조건은 액세스 제어 규칙의 뒷부분에 배치합니다. OSI 모델에 대한 자세한 내용은 이 위키피디아 문서를 참조하십시오.

자세한 정보와 예시는 애플리케이션 제어 구성 모범 사례 및 애플리케이션 제어 모범 사례의 내용을 참조하십시오.

SSL 규칙 순서

일반적으로 특정 조건(IP 주소 및 네트워크 등)을 사용하는 규칙은 일반 조건(애플리케이션 등)을 사용하는 규칙 앞에 배치합니다.

인증서 고정 사이트의 트래픽을 허용

일부 애플리케이션이 *TLS/SSL* 피닝또는 인증서 피닝이라는 기법을 사용하는데 이 기법에서는 원본 서버 인증서 지문이 애플리케이션 자체에 내장됩니다. 따라서 TLS/SSL 규칙을 **Decrypt - Resign(**암호 해독 - 재서명**)** 작업으로 구성하는 경우, 애플리케이션이 매니지드 디바이스로부터 재서명된 인증서를 수신할 때 확인이 실패하고 연결이 중단됩니다.

TLS/SSL 피닝이 발생하고 있는지 확인하려면, Facebook 같은 모바일 애플리케이션에 로그인을 시도합니다. 네트워크 연결 오류가 표시되는 경우, 웹 브라우저를 사용하여 로그인 합니다. (예를 들어, Facebook 모바일 애플리케이션에는 로그인이 불가능하더라도 Safari나 Chrome을 사용하여 Facebook에 로그인할 수 있습니다.) Firepower Management Center 연결 이벤트를 TLS/SSL 피닝의 추가 증거로 사용할 수 있습니다.

참고 TLS/SSL 피닝은 모바일 애플리케이션에 국한되지 않습니다.

이 트래픽을 허용하려면 암호 해독 안 함 작업을 사용해 SSL 규칙이 서버 인증서 공통 이름 또는 고유 이름과 일치하도록 설정합니다. SSL 정책에서 트래픽과 일치하는 모든 암호 해독 - 다시 서명 규칙 앞에 배치합니다. 웹사이트에 정상적으로 연결한 후 클라이언트 브라우저에서 고정된 인증서를 검색할 수 있습니다. 연결의 성공/실패 여부와 관계없이 기록된 연결 이벤트에서도 인증서를 확인할 수 있습니다.

SSL 정책이 우회되는 상황

액세스 컨트롤 규칙이 신뢰, 차단 또는 리셋과 함께 차단 동작과 일치하는 연결인 경우 SSL 정책이 우회됩니다.

- 보안 영역, 네트워크, 지리위치 및 포트를 트래픽 일치 기준으로만 사용하는 경우.
- 검사가 필요한 다른 규칙(예: 애플리케이션이나 URL을 기준으로 하는 연결과 일치하는 규칙) 앞에 오거나 침입 또는 파일 검사를 적용하는 규칙을 허용하는 경우.

URL 규칙 순서

가장 효과적인 URL 일치를 위해 특히 URL 규칙이 차단 규칙이고 다른 규칙이 다음 조건을 모두 만족하는 경우 다른 규칙 전에 URL 조건을 포함하는 규칙을 배치합니다.

- 애플리케이션 조건을 포함합니다.
- 검사할 트래픽은 암호화되어야 합니다.

규칙에 대해 예외를 설정하는 경우 다른 규칙 위에 예외를 배치합니다.

규칙 간소화 및 집중모범 사례

간소화**:** 과잉 구성하지 않습니다**.**

하나의 조건이 처리하려는 트래픽과 일치시키는 데 충분하다면 두 조건을 사용하지 마십시오.

개별 규칙 기준을 최소화합니다. 규칙 조건에 최소한의 개별 요소를 사용합니다. 예를 들어 네트워크 조건에서 개별 IP 주소 대신 IP 주소 블록을 사용합니다.

요소를 개체에 결합하는 것은 성능을 개선하지 않습니다. 예를 들어, 50개의 개별적인 IP 주소를 포함하는 네트워크 개체를 사용하면 사용자가 얻을 수 있는 이점은 성능에 관한 것이 아닌 구성적인 것에 한정되며, 조건에 해당 IP 주소를 개별적으로 포함하는 것입니다.

애플리케이션 탐지와 관련한 권장 사항은 애플리케이션 제어 구성 모범 사례을 참조하십시오.

집중: 특히 인터페이스에서 리소스를 많이 사용하는 규칙을 구체적으로 제한

규칙 조건을 최대한 사용하여 리소스를 많이 사용하는 규칙을 트래픽을 구체적으로 정의합니다. 폭넓은 조건을 가진 규칙이 여러 유형의 트래픽에 일치하며 추후 더 많은 특정 규칙에 사전 정의될 수 있기 때문에 집중 규칙이 중요합니다. 리소스를 많이 사용하는 규칙은 다음과 같습니다.

- 트래픽의 암호를 해독하는 SSL 규칙 - 암호 해독뿐 아니라 암호 해독된 트래픽의 추가 분석에도 리소스가 필요합니다. 집중하여 가능한 곳에서 암호화된 트래픽을 해독하지 않도록 선택 또는 차단합니다.
- 심화 검사를 호출하는 액세스 제어 규칙 - 특히 여러 사용자 정의 침입 정책 및 변수 세트를 사용하는 경우 침입, 파일, 악성코드 검사에 리소스를 사용합니다. 필요한 경우에만 심화 검사를 호출합니다.

최대 성능 향상을 위해 인터페이스로 규칙을 제한합니다. 규칙이 모든 디바이스의 인터페이스를 제외할 경우, 해당 규칙은 해당 디바이스의 성능에 영향을 미치지 않습니다.

최대 액세스 제어 규칙 및 침입 정책 개수

대상 디바이스에서 지원하는 최대 액세스 제어 규칙 또는 침입 정책 수는 정책 복잡성, 물리적 메모리 및 디바이스의 프로세서 수 등 여러 요인에 따라 달라집니다.

장치에서 지원되는 최대 한도를 초과하면 액세스 제어 정책을 구축할 수 없으며 재평가가 필요합니다.

침입 정책에 대한 지침:

액세스 제어 정책에서는 하나의 침입 정책을 각 허용 및 인터랙티브 차단 규칙 및 기본 작업과 연결할 수 있습니다. 모든 고유한 침입 정책 및 변수 집합의 쌍은 하나의 정책으로 계산됩니다.

침입 정책 또는 변수 집합을 통합하여 단일한 침입 정책 변수 집합 쌍을 여러 개의 액세스 제어 규칙과 연결할 수 있습니다. 일부 디바이스에서 모든 침입 정책에 단일 변수 집합만 사용할 수 있거나 전체 디바이스에 단일 침입 정책-변수 집합 쌍을 사용할 수 있습니다.