URL 필터링

액세스 제어 규칙을 사용하여 URL 필터링을 구현할 수 있습니다.

URL 필터링 개요

네트워크의 사용자가 액세스할 수 있는 웹사이트를 제어하려면 URL 필터링 기능을 사용합니다.

- 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. 권장 옵션입니다.
- 수동 URL 필터링 - 임의의 라이선스를 사용하여 개별 URL, URL 그룹 및 URL 목록과 피드를 수동으로 지정해 웹 트래픽을 맞춤형 방식으로 더 상세하게 제어할 수 있습니다. 자세한 내용은 수동 URL 필터링, 16 페이지를 참고하십시오.

악성 URL, 도메인 및 IP 주소를 차단하는 비슷하지만 다른 기능인 보안 인텔리전스도 참조하십시오.

카테고리 및 평판을 사용한 URL 필터링 정보

ULR 필터링 라이선스가 있으면 요청한 URL의 범주 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 알려지지 않음(레벨 0) 또는 신뢰할 수 없음(레벨 1)에서 신뢰할 수 있음(레벨 5)까지로 나타냅니다.

카테고리 및 평판 기반 URL 필터링의 이점

URL 범주 및 평판을 사용하면 URL 필터링을 빠르게 구성할 수 있습니다. 예를 들어 액세스 제어를 사용해 Hacking(해킹) 카테고리에서 신뢰할 수 없음 URL을 차단할 수 있습니다. 또는 QoS를 사용해 스트리밍 비디오 범주의 사이트에서 생성되는 트래픽의 속도를 제한할 수 있습니다. 스파이웨어 또는 애드웨어 카테고리 등과 같은 위협 유형 카테고리도 있습니다.

범주 및 평판 데이터를 사용하면 정책 생성 및 관리가 간소화됩니다. 이를 통해 시스템이 웹 트래픽을 정상적으로 제어할 수 있습니다. Cisco에서는 새로운 URL 및 기존 URL에 대한 새 범주와 위험을 포함하여 위협 인텔리전스를 지속적으로 업데이트하므로, 시스템이 최신 정보를 사용하여 요청된 URL을 필터링할 수 있습니다. 보안 위협을 나타내거나 부적절한 콘텐츠를 제공하는 사이트가 나타나고 사라지는 속도는 새 정책을 업데이트하고 구축하는 속도보다 빠를 수 있습니다.

시스템을 조정할 수 있는 방법의 몇 가지 예는 다음과 같습니다.

- 액세스 제어 규칙이 모든 게임 사이트를 차단하는 경우, 새로운 도메인이 게임으로 등록되고 분류되면 시스템은 해당 사이트를 자동으로 차단할 수 있습니다. 마찬가지로 QoS 규칙이 모든 스트리밍 비디오 사이트의 속도를 제한하는 경우 시스템은 새 스트리밍 비디오 사이트로의 트래픽을 자동으로 제한할 수 있습니다.
- 액세스 제어 규칙이 모든 악성코드 사이트를 차단하는 경우, 쇼핑 페이지 하나가 악성코드에 감염되면 시스템은 쇼핑의 URL을 악성코드 사이트로 재분류하고 해당 사이트를 차단할 수 있습니다.
- 액세스 제어 규칙이 신뢰할 수 없음인 소셜 네트워킹 사이트를 차단하고 누군가가 악성 페이로드 링크를 포함하는 프로파일 페이지에 링크를 게시하는 경우, 시스템은 해당 페이지의 평판을 선호 사이트에서 신뢰할 수 없음으로 변경하고 해당 페이지를 차단할 수 있습니다.

SSL 정책 Do Not Decrypt(암호 해독 안 함) 규칙의 범주 기반 필터링 제한 사항

선택적으로 SSL 정책에 범주를 포함하도록 선택할 수 있습니다. *URL* 필터링이라고도 하는 이러한 범주는 Cisco Talos 인텔리전스 그룹에 의해 업데이트됩니다. 업데이트는 웹사이트 대상 및 경우에 따라 호스팅 및 등록 정보에서 검색할 수 있는 콘텐츠에 따라 머신 러닝 및 인적 분석을 기반으로 합니다. 분류는 선언된 회사 범주, 의도 또는 보안을 기반으로 하지 않습니다.

참고 URL 필터링을 애플리케이션 탐지와 혼동하지 마십시오. 웹사이트에서 패킷의 일부를 읽어 패킷의 정체(예: Facebook Message 또는 Salesforce)를 더 구체적으로 확인합니다. 자세한 내용은 애플리케이션 제어 구성 모범 사례을 참고하십시오.

자세한 내용은 URL 필터링에 범주 사용, 8 페이지를 참고하십시오.

URL 카테고리 및 평판 설명

카테고리 설명

각 URL 카테고리에 대한 설명은 https://www.talosintelligence.com/categories에 나와 있습니다.

범주를 보려면 **Threat Categories(**위협 범주**)**를 클릭해야 합니다.

평판 레벨 설명

https://talosintelligence.com/reputation_center/support(으)로 이동해 Common Questions(자주 하는 질문) 섹션에서 확인하십시오.

Cisco Cloud의 URL 필터링 데이터

URL 필터링 라이선스를 추가하면 URL 필터링 기능이 자동으로 활성화됩니다. 이를 통해 웹 사이트의 일반 분류 또는 범주, 위험 수준 또는 평판을 기준으로 트래픽을 처리할 수 있습니다.

URL 필터링 라이선스를 추가하면 URL 필터링 기능이 자동으로 활성화됩니다. 이를 통해 웹 사이트의 일반 분류 또는 범주, 위험 수준 또는 평판을 기준으로 트래픽을 처리할 수 있습니다.

URL 필터링을 활성화(또는 다시 활성화)하면 management center는 Cisco에 URL 데이터를 쿼리하고 데이터 집합을 매니지드 디바이스에 푸시합니다. 이 데이터 집합의 자동 업데이트는 기본적으로 활성화되어 있습니다. 이러한 업데이트는 비활성화하지 않는 것이 좋습니다.

사용자가 웹을 탐색할 때 시스템은 범주 및 평판 정보에 대해 로컬 데이터 집합을 사용합니다. 사용자가 로컬 데이터 세트 또는 이전에 액세스한 웹 사이트의 캐시에 범주 및 평판이 없는 URL을 검색하면 기본적으로 시스템이 위협 인텔리전스 평가를 위해 해당 URL을 클라우드에 제출하고 결과를 캐시에 추가합니다. (이 클라우드 조회를 비활성화할 수 있습니다. URL 필터링 옵션, 11 페이지의 내용을 참조하십시오.)

URL 카테고리 집합은 주기적으로 변경될 수 있습니다. 변경 알림을 받으면 URL 필터링 구성을 검토하여 트래픽이 예상대로 처리되는지 확인합니다. 자세한 내용은 URL 범주 집합이 변경되면 작업 수행, 23 페이지을 참고하십시오.

URL 필터링 모범 사례

URL 필터링을 위한 다음 지침 및 제한 사항을 유념하십시오.

범주 및 평판을 기준으로 필터링

범주 및 평판을 사용한 URL 필터링 설정 방법, 9 페이지의 지침을 따릅니다.

URL을 식별하기 전에 통과해야 하는 패킷을 검사하도록 정책 설정

시스템은 다음 작업을 수행한 후 URL을 필터링할 수 있습니다.

- 클라이언트와 서버 간 모니터링된 연결이 설정됩니다.
- 시스템은 세션에서 DNS, HTTP 또는 HTTPS 애플리케이션을 식별합니다.
- 시스템은 (암호화된 세션의 경우 암호화되지 않은 도메인 이름, ClientHello 메시지 또는 서버 인증서로부터) 요청된 도메인 또는 URL을 식별합니다.

이 식별은 3~5개 패킷 내에서 또는 트래픽이 암호화된 경우 TLS/SSL 핸드셰이크의 서버 인증서 교환 후에 이루어져야 합니다.

중요! 시스템이 통과할 이러한 초기 패킷을 검사하도록 하려면 트래픽이 식별되기 전에 통과하는 패킷 검사 및 하위 주제를 참조하십시오.

초기 트래픽이 기타 모든 규칙 조건과 일치하지만 식별이 불완전한 경우 시스템은 패킷 통과 및 연결 설정 (또는 TLS/SSL 핸드셰이크 완료)을 허용합니다. 시스템은 식별을 완료하면 나머지 세션 트래픽에 적절한 규칙 작업을 적용합니다.

위협 범주 차단

정책은 잘 알려진 악성 사이트를 식별하는 위협 카테고리를 해결해야 합니다. 평판이 불량한 사이트를 차단하는 것 외에 이 작업을 수행합니다.

예를 들어, 악의적인 사이트로부터 네트워크를 보호하려면 모든 위협 범주를 차단해야 합니다. 또한 Talos에서는 불량 범주의 사이트만 차단할 것을 권장합니다. 보안 상태가 적극적인 경우 의심스러운 평판을 차단할 수 있지만, 이로 인해 오탐이 더 많이 발생할 수 있습니다.

자세한 내용은 URL 카테고리 및 평판 설명, 3 페이지의 URL의 위협 범주를 참조하십시오.

URL 조건 및 규칙 순서

- 적중해야 하는 다른 모든 규칙 뒤에 URL 규칙을 배치합니다.
- URL은 여러 카테고리에 속할 수 있습니다. 명시적으로 또는 기본 작업에 의존하여, 특정 웹사이트 범주는 허용하고 다른 범주는 차단할 수도 있습니다. 이 경우 블록 허용 또는 차단 중 무엇을 우선하는 가에 따라, 원하는 효과를 얻을 수 있도록 URL 규칙을 생성하고 순서를 지정해야 합니다.

규칙에 대한 자세한 지침은 액세스 제어 규칙 순서에 대한 모범 사례 주제를 참조하십시오.

미분류 또는 무평판 URL

URL 규칙을 만들 때 일치시키려는 카테고리를 먼저 선택합니다. **Uncategorized(**미분류**)** URL을 명시적으로 선택하면 평판에 따른 추가 제한이 불가능합니다.

신뢰할 수 없음 평판이 있는 미분류 URL은 악성 사이트 카테고리로 처리됩니다. (의심스러움 등의) 다른 평판 수준을 사용해 분류되지 않은 사이트를 차단하려는 경우에는 분류되지 않은 모든 사이트를 차단해야 합니다.

범주 및 평판 레벨을 선택한 후 필요에 따라 **Apply to unknown reputation(**알 수 없는 평판에 적용**)**을 선택할 수 있습니다. 예를 들어, 신뢰할 수 없음, 의심스러움, 알 수 없는 평판의 사이트에 적용되는 규칙을 생성할 수 있습니다.

URL에는 범주와 평판을 수동으로 할당할 수 없지만, 액세스 제어 및 QoS 정책에서는 특정 URL을 수동으로 차단할 수 있습니다. 수동 URL 필터링, 16 페이지의 내용을 참조하십시오. URL 범주 및 평판, 22 페이지도 참조하십시오.

암호화된 웹 트래픽에 대한 **URL** 필터링

암호화된 웹 트래픽에 대해 URL 필터링을 수행할 때 시스템은 다음 작업을 수행합니다.

- (DNS 필터링이 활성화된 경우) 시스템이 이전에 원래 도메인을 파악했는지 또는 도메인이 로컬 평판 데이터베이스에 있는지 확인하고, 있는 경우 도메인의 평판 및 범주를 기반으로 조치를 취합니다. 그렇지 않으면 시스템은 액세스 제어 정책의 고급 설정에서 **Retry URL cache miss lookup(URL** 캐시 누락 조회 다시 시도**)**가 활성화된 경우에도 암호화된 트래픽에 대한 설정에 따라 트래픽을 처리합니다.
- 암호화 프로토콜을 무시합니다. 규칙에 URL 조건은 있지만 프로토콜을 지정하는 애플리케이션 조건이 없는 경우 해당 규칙은 HTTPS 및 HTTP 트래픽 두 가지 모두와 일치합니다.
- URL 목록을 사용하지 않습니다. 그 대신 URL 개체 및 그룹을 사용해야 합니다.
- 트래픽을 암호화하는 데 사용되는 공개 키 인증서의 주체 공통 이름을 기반으로 HTTPS 트래픽과 일치시키며, 암호 해독 후 HTTP URL을 포함하여 트랜잭션 중에 언제든지 표시되는 다른 URL의 평판도 평가합니다.
- 주체 공통 이름 내의 서브도메인을 무시합니다.
- 액세스 제어 규칙이나 기타 컨피그레이션에서 차단한 암호화된 연결에 대해 HTTP 응답 페이지를 표시하지 않습니다(HTTP 대응 페이지의 제한, 18 페이지 참조).

URL 필터링 및 **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 정책 고급 설정은 TLS 서버 ID 검색을 위한 **Early application detection and URL categorization(**초기 애플리케이션 탐지 및 **URL** 분류**)** 옵션을 제공합니다.

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.

자세한 내용은 액세스 제어 정책 고급 설정를 참고하십시오.

HTTP/2

시스템은 TLS 인증서에서 HTTP/2 URL을 추출할 수 있지만 페이로드에서는 추출할 수 없습니다.

수동 URL 필터링

- 사용자 지정 보안 인텔리전스 목록 또는 피드 개체를 사용하여 URL을 지정합니다. URL 개체를 사용하거나 규칙에 URL을 직접 입력하지 마십시오. 자세한 내용은 수동 URL 필터링 옵션, 16 페이지 섹션을 참조해 주십시오.
- URL 개체를 사용하거나 규칙에 URL을 직접 입력하여 특정 URL을 수동으로 필터링하는 경우, 영향을 받을 수 있는 다른 트래픽을 신중하게 고려하십시오. URL 조건이 네트워크 트래픽과 일치하는지 확인하기 위해 시스템은 간단한 부분 문자열 일치를 실행합니다. 요청한 URL은 문자열의 일부분과 일치하는 경우 일치 항목으로 간주됩니다.
- 수동 URL 필터링을 사용하여 다른 규칙에 대한 예외를 생성하는 경우, 예외를 생성하지 않으면 적용될 일반 규칙 위에 예외가 있는 특정 규칙을 배치합니다.

URL 내 검색 쿼리 매개변수

시스템은 URL 조건과 일치하도록 URL에서 검색 쿼리 매개변수를 사용하지 않습니다. 예를 들어, 모든 쇼핑 트래픽을 차단하는 시나리오를 생각해 보십시오. 이 경우, amazon.com을 검색하기 위해 웹 검색을 사용하는 것은 차단되지 않지만 amazon.com 브라우징은 차단됩니다.

고가용성 배포의 URL 필터링

고가용성에 Firepower Management Center를 사용하여 URL을 필터링하는 경우의 지침은 Cisco Secure Firewall Management Center 관리 가이드 의 *URL* 필터링 및 보안 인텔리전스를 참조하십시오.

선택한 디바이스 모델의 메모리 제한

- 메모리가 적은 디바이스 모델은 적은 URL 데이터를 로컬로 저장하며, 따라서 시스템은 클라우드를 더 자주 확인해 로컬 데이터베이스에 없는 사이트의 카테고리와 평판을 확인합니다.

  하위 메모리 디바이스는 다음과 같습니다.

- Firepower 1010
- Threat Defense Virtual, 8GB RAM

위협 방어에서 **TLS** 세션 재개에 대한 **URL** 일치

다음 조건에서 Snort 2와 URL 일치를 사용합니다.

- TLS 세션 재개가 없고 SSL 정책이 활성화되어 있거나 클라이언트 Hello 메시지에 SNI(Server Name Indication) 확장이 포함된 경우.
- TLS 세션 재개가 있고 SSL 정책이 활성화되지 않았거나 클라이언트 Hello 메시지에 SNI 확장이 포함되지 않은 경우.

HTTPS 트래픽 필터링

시스템은 암호화 트래픽을 필터링하기 위해 TLS/SSL 핸드셰이크 중에 전달된 정보(트래픽을 암호화하는 데 사용된 공개 키 인증서의 주체 공용 이름)를 기준으로 요청된 URL을 확인합니다.

HTTP 필터링과 달리, HTTPS 필터링은 주체 공용 이름 내의 서브도메인을 무시합니다. 액세스 제어 또는 QoS 정책에서 HTTPS URL을 수동으로 필터링할 경우, 서브도메인 정보를 포함하지 마십시오. 이를테면 www.example.com 대신 example.com을 사용하십시오.

팁 SSL 정책에서는 고유 이름 SSL 정책 규칙 조건을 정의하여 특정 URL에 대한 트래픽을 처리하고 암호를 해독할 수 있습니다. 인증서의 주체 고유 이름의 공용 이름 속성에는 사이트의 URL이 포함됩니다. HTTPS 트래픽을 암호 해독하면 액세스 제어 규칙이 암호 해독된 세션을 평가할 수 있으므로 URL 필터링 성능이 개선됩니다.

암호화 프로토콜을 통해 트래픽 제어

시스템은 액세스 제어 또는 QoS 정책에서 URL 필터링을 수행할 때 암호화 프로토콜(HTTP 또는 HTTPS)을 무시합니다. 이는 수동 및 평판 기반 URL 조건 모두에 해당됩니다. 즉, URL 필터링에서는 다음 웹 사이트에 대한 트래픽을 동일하게 처리합니다.

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

HTTP 또는 HTTPS 트래픽에만 일치하는 규칙을 구성하려면 규칙에 애플리케이션 조건을 추가합니다. 예를 들어 각각 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)
애플리케이션: HTTPS
URL: example.com

두 번째 규칙은 동일한 웹 사이트에 대한 HTTP 액세스를 차단합니다.

작업: Block(차단)
애플리케이션: HTTP
URL: example.com

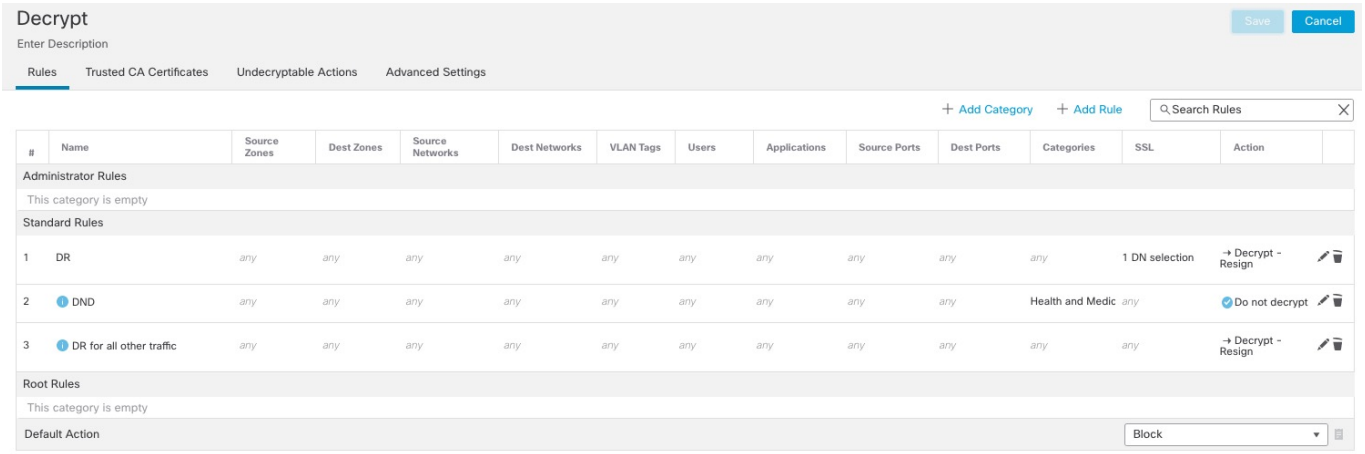
URL 필터링에 범주 사용

Do Not Decrypt(암호 해독 안 함) 규칙의 범주 제한 사항

선택적으로 SSL 정책에 범주를 포함하도록 선택할 수 있습니다. *URL* 필터링이라고도 하는 이러한 범주는 Cisco Talos 인텔리전스 그룹에 의해 업데이트됩니다. 업데이트는 웹사이트 대상 및 경우에 따라 호스팅 및 등록 정보에서 검색할 수 있는 콘텐츠에 따라 머신 러닝 및 인적 분석을 기반으로 합니다. 분류는 선언된 회사 범주, 의도 또는 보안을 기반으로 하지 않습니다. Cisco에서는 URL 필터링 범주를 지속적으로 업데이트하고 개선하기 위해 노력하고 있지만, 이는 정확한 과학이 아닙니다. 일부 웹사이트는 전혀 분류되지 않으며, 일부 웹사이트는 잘못 분류되었을 수 있습니다.

Do not decrypt(암호 해독 안 함) 규칙에서 범주를 남용하지 마십시오. 예를 들어 Health and Medicine(건강 및 의료) 범주에는 환자의 프라이버시를 위협하지 않는 WebMD 웹사이트가 포함됩니다.

다음은 Health and Medicine(건강 및 의료) 범주의 웹사이트에 대한 암호 해독을 방지할 수 있지만 WebMD 및 기타 모든 항목에 대한 암호 해독을 허용하는 샘플 암호 해독 정책입니다. 암호 해독 규칙에 대한 일반 정보는 TLS/SSL 암호 해독 사용 지침에서 확인할 수 있습니다.



참고 URL 필터링을 애플리케이션 탐지와 혼동하지 마십시오. 웹사이트에서 패킷의 일부를 읽어 패킷의 정체(예: Facebook Message 또는 Salesforce)를 더 구체적으로 확인합니다. 자세한 내용은 애플리케이션 제어 구성 모범 사례을 참고하십시오.

URL 필터링의 라이선스 요건

Threat Defense 라이선스

- 범주 및 평판 필터링 -URL 필터링
- 수동 필터링 - 추가 라이선스가 없습니다.

기본 라이선스

- 범주 및 평판 필터링 -URL 필터링
- 수동 필터링 - 추가 라이선스가 없습니다.

Threat Defense 디바이스의 **URL** 필터링 라이선스

Cisco Secure Firewall Management Center 관리 가이드의 라이선스 장에서 *URL* 라이선스를 참조하십시오.

URL 필터링을 위한 요구 사항 및 사전 요건

모델 지원

Any(모든)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

범주 및 평판을 사용한 URL 필터링 설정 방법

	수행해야 할 작업	추가 정보
1단계	올바른 라이선스가 있는지 확인합니다.	URL을 필터링할 관리되는 각 디바이스에 URL 필터링 라이선스를 할당합니다.

	수행해야 할 작업	추가 정보
2단계	Firepower Management Center가 클라우드와 통신하여 URL 필터링 데이터를 가져올 수 있는지 확인합니다.	Cisco Secure Firewall Management Center 관리 가이드의 인터넷 액세스 요구 사항 및 통신 포트 요구 사항
3단계	제한 사항과 지침을 이해하고 필요한 조치를 취합니다.	URL 필터링 모범 사례, 3 페이지
4단계	URL 필터링 기능을 활성화합니다.	범주 및 평판을 사용한 URL 필터링 활성화, 11 페이지
5단계	범주 및 평판을 기준으로 URL을 필터링하는 규칙을 설정합니다.	URL 조건 설정, 12 페이지 악의적인 사이트로부터 최상의 보호를 받으려면 평판으로 사이트를 차단하고 모든 위협 범주에서 URL을 차단해야 합니다. (선택사항) 범주 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의, 17 페이지
6단계	(선택 사항) 사용자가 경고 페이지에서 클릭하면 웹사이트 차단을 우회할 수 있게 합니다.	HTTP 응답 페이지 및 인터랙티브 차단
7단계	트래픽이 주요 규칙에 먼저 적중하도록 규칙 순서를 정합니다.	URL 규칙 순서
8단계	(선택 사항) URL 필터링과 관련된 고급 옵션을 수정합니다.	일반적으로 기본값을 변경해야 하는 특별한 이유가 없는 한 기본값을 사용합니다. 다음을 비롯한 고급 옵션에 대한 자세한 내용은 액세스 제어 정책 고급 설정의 내용을 참조하십시오. • 연결 이벤트에 저장하고자 하는 최대 **URL** 문자 • 인터랙티브 차단을 허용하여 다음 시간**(**초**)** 동안 차단 바이패스 • **URL** 캐시 누락 조회 다시 시도 • **DNS** 트래픽에 대한 평판 시행 활성화
9단계	변경 사항을 배포합니다.	구성 변경 사항 구축
10단계	시스템이 예상대로 향후 URL 데이터 업데이트를 수신하는지 확인합니다.	URL 필터링 상태 모니터 설정, 22 페이지

	수행해야 할 작업	추가 정보
11단계	악성 사이트로부터 네트워크를 보호하는 다른 기능을 활성화했는지 확인하십시오.	보안 인텔리전스의 내용을 참조하십시오.

범주 및 평판을 사용한 URL 필터링 활성화

이 작업을 수행하려면 관리자 사용자여야 합니다.

시작하기 전에

범주 및 평판을 사용한 URL 필터링 설정 방법, 9 페이지에 설명된 사전 요건을 완료합니다.

프로시저

단계 **1** **Integration(**통합**)** > **Other Integrations(**기타 통합**)**를 선택합니다.

단계 **2** 클라우드 서비스 버튼을 클릭합니다.

단계 **3** URL 필터링 옵션, 11 페이지를 구성합니다.

단계 **4** **Save(**저장**)**를 클릭합니다.

URL 필터링 옵션

URL 필터링 라이선스를 추가하면 URL 필터링 기능이 자동으로 활성화됩니다. 이를 통해 웹 사이트의 일반 분류 또는 범주, 위험 수준 또는 평판을 기준으로 트래픽을 처리할 수 있습니다.

URL 필터링을 활성화(또는 다시 활성화)하면 management center는 자동으로 Cisco에 URL 데이터를 쿼리하고 데이터 집합을 매니지드 디바이스에 푸시합니다. 이 프로세스는 시간이 걸릴 수 있습니다.

SSL 규칙을 사용하여 암호화 트래픽을 처리하는 경우, TLS/SSL 규칙 지침 및 제한 사항도 참조하십시오.

자동 업데이트 활성화

Enable Automatic Updates(자동 업데이트 활성화**)**(기본값)를 선택한 경우 management center는 클라우드에서 업데이트를 30분마다 확인합니다. 시스템이 외부 리소스와 접촉하는 시기를 엄격히 제어해야 하는 경우, 이 페이지의 자동 업데이트를 비활성화하고 대신 스케줄러를 사용하여 반복 작업을 생성합니다. Cisco Secure Firewall Management Center 관리 가이드 에서 예약된 작업을 통해 *URL* 필터링 업데이트 자동화를 참조하십시오.

지금 업데이트

일회성, 온디맨드 URL 데이터 업데이트를 수행하려면 **Update Now(**지금 업데이트**)**를 클릭합니다. 업데이트가 이미 진행 중인 경우, 온디맨드 업데이트를 시작할 수 없습니다. 일일 업데이트 용량은

작지만 마지막 업데이트 후 5일 이상이 경과했다면 대역폭에 따라 새 URL 데이터를 다운로드하는 데 20분 이상이 소요될 수 있습니다. 그런 다음 업데이트 자체를 수행하는 데 30분이 걸릴 수 있습니다.

알 수 없는 **URL**에 대한 **Cisco** 클라우드 쿼리

로컬 데이터베이스에 카테고리와 평판이 없는 웹사이트를 사용자가 탐색하는 경우, 위협 인텔리전스 평가를 위해 시스템이 클라우드에 URL을 제출하도록 허용합니다. 이 옵션은 기본적으로 활성화되어 있습니다. 예를 들어 사생활 보호를 위해 미분류 URL을 제출하기를 원치 않는 경우, 이 옵션을 비활성화하십시오. 그러나 미분류 URL에 대한 연결은 카테고리 또는 평판 기반 URL 규칙과 일치하지 않습니다. URL에 카테고리 또는 평판을 수동으로 할당할 수 없습니다.

캐시된 **URL** 만료

카테고리 및 평판 데이터를 캐싱하면 웹 브라우징 속도가 빨라집니다. 가장 빠른 성능을 위해 캐시된 URL 데이터는 기본적으로 만료되지 않습니다.

오래된 데이터에서 URL 일치 인스턴스를 최소화하려면 캐시의 URL이 만료되도록 설정할 수 있습니다. 위협 데이터의 정확성과 유효 기간을 높이려면 더 짧은 만료 기간을 선택하십시오. 캐시된 URL은 지정된 시간이 경과한 후 네트워크의 사용자가 처음 해당 URL에 액세스한 후 새로 고침됩니다. 첫 번째 사용자는 새로 고침된 결과를 볼 수 없지만 이 URL을 방문하는 다음 사용자는 새로 고침된 결과를 볼 수 있습니다.

URL 조건 설정

URL 범주 및 평판을 기반으로 사이트에 대한 액세스를 제어하여 네트워크를 보호합니다.

프로시저

단계 **1** 규칙 편집기에서 URL 조건에 대해 다음을 클릭합니다.

- 액세스 제어 또는 QoS - **URLs**를 클릭합니다. 새 액세스 제어 UI의 Destinations and Applications(대상 및 애플리케이션) 열에서 이 옵션을 선택합니다.
- SSL - **Category(**범주**)**를 클릭합니다.

단계 **2** 제어할 URL 범주를 찾아 선택합니다.

액세스 제어 또는 QoS 규칙에서 **Category(**범주**)**를 클릭합니다.

악성 사이트로부터 효과적으로 보호하려면 모든 위협 범주에서 URL을 차단해야 합니다. 또한 Talos에서는 불량 범주의 사이트만 차단할 것을 권장합니다. 보안 상태가 적극적인 경우 의심스러운 평판을 차단할 수 있지만, 이로 인해 오탐이 더 많이 발생할 수 있습니다. 위협 범주 목록은 URL 카테고리 및 평판 설명, 3 페이지의 내용을 참조하십시오.

사용 가능한 모든 범주를 보려면 목록 하단에 있는 화살표를 클릭해야 합니다.

단계 **3** (선택 사항) **Reputations(**평판**)**를 선택하여 URL 카테고리를 제한합니다.

Uncategorized(미분류**)** URL을 명시적으로 일치시키면 평판에 따른 추가 제한이 불가능합니다. 평판 레벨을 선택하면 규칙 작업에 따라 선택하는 레벨보다 더 심각하거나 덜 심각한 평판도 포함됩니다.

- 덜 심각한 평판을 포함 - 규칙이 웹 트래픽을 허용하거나 신뢰하는 경우. 예를 들어 선호 사이트(레벨 4)를 허용하는 액세스 제어 규칙을 구성한다면, 신뢰할 수 있음(레벨 5) 사이트도 자동으로 허용합니다.
- 더 심각한 평판을 포함 - 규칙이 웹 트래픽을 속도 제한, 해독, 차단 또는 모니터링하는 경우. 예를 들어 수상한 사이트(레벨 2)를 차단하는 액세스 제어 규칙을 구성하면 해당 규칙은 신뢰할 수 없음(레벨 1) 사이트도 차단합니다.

규칙 작업을 변경하면 시스템은 URL 조건의 평간 레벨을 자동으로 변경합니다.

필요에 따라 **Apply to unknown reputation(**알 수 없는 평판에 적용**)**을 선택합니다.

단계 **4** **Add to Rule(**규칙에 추가**)**을 클릭하거나 끌어서 놓습니다. 새 액세스 제어 UI에서 **Add URL(URL** 추가**)**을 클릭합니다.

단계 **5** (선택 사항) 사전 정의된 URL 개체 또는 액세스 제어 또는 QoS 규칙의 URL 목록 및 피드를 선택하려면 **URL**을 클릭하고 개체를 선택한 후 대상에 추가합니다.

이러한 개체는 범주 기반 필터링이 아닌 수동 URL 필터링을 구현합니다.

단계 **6** 규칙을 저장하거나 계속 수정합니다.

예**:** 액세스 제어 규칙의 **URL** 조건

다음 그림은 모든 악성코드 사이트, 모든 신뢰할 수 없음 사이트 및 평판 수준이 보통 이하인 모든 소셜 네트워킹 사이트를 차단하는 액세스 제어 규칙의 URL 조건을 보여줍니다.

다음 표에는 조건을 만드는 방법이 요약되어 있습니다.

차단된 **URL**	카테고리	평판
평판과 상관없이 악성코드 사이트	Malware Sites(악성코드 사이트)	Any(모든)
모든 신뢰할 수 없는 URL(레벨 1)	Any(모든)	1 - 신뢰할 수 없음
평판 수준이 보통 이하인(레벨 1부터 3까지의) 소셜 네트워킹 사이트	소셜 네트워크	3 - 보통

URL 조건이 포함된 규칙

아래 표에는 URL 조건을 지원하는 규칙과 각 규칙 유형이 지원하는 필터링 유형이 나와 있습니다.

규칙 유형	카테고리 및 평판 필터링을 지원합니까?	수동 필터링 지원 여부
액세스 제어	예	예
SSL 정책	예	아닙니다. 대신 고유 이름 조건을 사용합니다.
QoS	예	예

Do Not Decrypt(암호 해독 안 함**)** 규칙 조건이 있는 SSL 정책 정책에서 URL 필터링을 사용하려면 URL 필터링에 범주 사용, 8 페이지 섹션을 참조하십시오.

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.

DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별

Enable reputation enforcement on DNS traffic(DNS 트래픽에 대한 평판 시행 활성화**)** 옵션은 각 새 액세스 제어 정책의 **Advanced(**고급**)** 탭에서 기본적으로 활성화됩니다. 이 옵션은 URL 필터링 동작을 약간 수정하며 URL 필터링이 활성화 및 설정된 경우에만 적용 가능합니다.

이 옵션이 활성화된 경우:

- 브라우저가 도메인 이름을 조회하여 IP 주소를 가져올 때 시스템은 URL 트랜잭션 초기에 도메인 범주 및 평판을 평가합니다.
- 암호화된 트래픽의 범주 및 평판은 암호 해독 없이 확인할 수 있는 경우가 많습니다.

  DNS 필터링에서 암호화된 트래픽의 URL을 확인할 수 없는 경우, 해당 트래픽은 암호화된 트래픽에 대한 설정을 사용하여 처리됩니다.

도메인 조회 중 URL을 식별하도록 DNS 필터링 활성화

DNS 필터링은 새 액세스 제어 정책에서 기본적으로 활성화됩니다. 그러나 이 설정을 적용하려면 추가 구성이 필요할 수 있습니다.

시작하기 전에

- 범주 및 평판을 사용하는 URL 필터링은 라이선스가 부여되고 활성화 및 설정되어야 합니다.

  (DNS 필터링은 URL 탭인 URL 그룹, URL 개체, URL 목록 및 피드, "Enter URL(URL 입력)" 텍스트 상자에 입력한 URL에서 다음 설정을 사용하지 않습니다.)

- DNS 필터링 제한, 15 페이지의 제한 사항을 참조하십시오.

프로시저

단계 **1** 액세스 제어 정책의 **Enable reputation enforcement on DNS traffic(DNS** 트래픽에 대한 평판 시행 활성화**)**을 선택합니다.

단계 **2** 동일한 정책에서 URL 범주 및 평판 차단이 설정된 각 액세스 제어 규칙에 대해 다음을 수행합니다.

- 애플리케이션 조건 - 애플리케이션 조건이 **any**(또는 비어 있음)가 아닌 경우 해당 목록에 **DNS**를 추가합니다. 다른 DNS 관련 옵션은 이 목적과 관련이 없습니다.
- 포트 조건 — 포트/프로토콜 조건이 **any**(또는 비어 있음)가 아닌 경우 **DNS_over_TCP** 및 **DNS_over_UDP**를 추가합니다.

단계 **3** 변경 내용을 저장합니다.

다음에 수행할 작업

변경이 완료되면, 구성 변경 사항 구축.

DNS 필터링 제한

Block with reset(차단 후 재설정**)**, **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)** 작업이 있는 규칙과 일치하는 트래픽은 규칙 작업이 차단인 것처럼 처리됩니다.

차단된 URL에 액세스하려는 최종 사용자는 설명할 수 없는 페이지 연결 불가능을 경험하게 됩니다. 연결이 끊긴 다음 시간이 초과됩니다.

DNS 필터링 및 이벤트

DNS 필터링에 의해 생성된 연결 이벤트는 DNS 쿼리, URL 범주, URL 평판 및 대상 포트 필드를 사용하여 로깅됩니다. DNS 쿼리 필드에는 도메인 이름이 있습니다. DNS 필터링 일치의 경우 URL 필드가 비어 있습니다. 대상 포트는 53입니다.

또한:

- 액세스 제어 규칙 작업이 **Allow(**허용**)** 또는 **Trust(**신뢰**)**인 경우, 동일한 트래픽에 대해 두 개의 연결 이벤트가 생성됩니다. 하나는 DNS 필터링(**DNS** 쿼리 필드 입력) 및 하나는 URL 필터링(**URL** 필드 입력)입니다.

- 시스템에서 특정 URL을 처음 발견하면 해당 단일 세션에 대해 2개의 이벤트가 표시됩니다. 하나는 DNS 쿼리에 대해 분류되지 않았거나 평판이 없음을 표시하는 이벤트이고, 다른 하나는 DNS 쿼리 중에 검색된 URL의 실제 범주 및 평판을 표시하며 표준 URL 필터링을 사용하여 처리하는 동안 해당 세션에 적용됩니다.

수동 URL 필터링

액세스 제어 및 QoS 규칙에서는 개별 URL, URL 그룹 또는 URL 목록과 피드를 수동으로 필터링하여 카테고리 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의할 수 있습니다.

예를 들어 액세스 제어를 사용하여 조직에 적합하지 않은 웹 사이트 범주를 차단할 수 있습니다. 그러나 해당 범주에 액세스 권한을 제공하려는 적절한 웹 사이트가 포함된 경우에는 해당 사이트용으로 수동 허용 규칙을 생성한 다음 범주에 대한 차단 규칙 앞에 배치할 수 있습니다.

이러한 유형의 URL 필터링을 수행하는 데는 특별한 라이선스가 필요하지 않습니다.

수동 URL 필터링은 SSL 규칙에서는 지원되지 않습니다. SSL 규칙에서는 고유 이름 조건을 대신 사용해야 합니다.

⚠

주의 수동 URL 필터링을 구현하는 방법에 따라 URL 일치가 의도한 것과 다를 수 있습니다. 수동 URL 필터링 옵션, 16 페이지의 내용을 참조하십시오.

수동 URL 필터링 옵션

수동 URL 필터링을 위해 URL을 지정하는 방법에는 여러 가지가 있습니다.

옵션	설명
(모범 사례) 사용자 지정 보안 인텔리전스 URL 목록 또는 피드 개체를 사용합니다.	이는 수동 URL 필터링에 권장되는 방법입니다. 새 목록 또는 피드를 생성하거나 액세스 제어 또는 QoS 규칙에서 기존 목록 또는 피드를 선택할 수 있습니다. 자세한 내용은 사용자 지정 보안 인텔리전스 목록 및 피드 및 하위 항목을 참조하십시오.

옵션	설명
URL 개체를 개별적으로 또는 그룹으로 사용합니다. URL 개체는 URL에 설명되어 있습니다. 또는 액세스 제어 규칙에 URL을 직접 입력합니다. (웹 인터페이스의 규칙 페이지에 있는 **Enter URL(URL 입력)** 옵션)	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. **Enter URL(URL 입력)** 옵션은 와일드카드를 지원하지 않습니다.

범주 및 평판 기반 URL 필터링을 보완하거나 선택적으로 재정의

액세스 제어 또는 QoS 규칙에서 보안 인텔리전스 URL 목록 및 피드를 사용하여 범주 및 평판 기반 URL 필터링 규칙을 보완하거나 예외를 지정할 수 있습니다.

중요! 이 절차에서 설정 중인 목록 또는 피드에 범주 또는 평판 기반 규칙에 대한 예외가 포함된 경우, 규칙 순서에서 이 규칙 위에 해당 규칙을 추가합니다.

SSL 규칙에서 고유 이름 조건을 사용하여 병렬 동작을 설정합니다.

시작하기 전에

- 범주 및 평판을 사용하여 URL 필터링을 설정합니다. URL 조건 설정, 12 페이지의 내용을 참조하십시오.
- 수동 URL 필터링에 대한 중요한 모범 사례를 이해합니다. URL 필터링 모범 사례, 3 페이지 및 수동 URL 필터링 옵션, 16 페이지를 참조하십시오.
- 수동 필터링에 사용할 URL이 포함된 하나 이상의 보안 인텔리전스 개체(목록 또는 피드)를 설정합니다. 사용자 지정 보안 인텔리전스 목록 및 피드의 내용을 참조하십시오.

프로시저

단계 **1** 규칙을 정의할 액세스 제어 또는 QoS 정책으로 이동합니다.

단계 **2** 새 조건을 추가할 규칙을 생성하거나 편집합니다.

- 범주 또는 평판 기반 URL 필터링 규칙을 보완하는 경우, 기존 규칙을 편집합니다.

- 범주 또는 평판 기반 URL 필터링 규칙에 대한 예외를 재정의하거나 생성하는 경우, 새 규칙을 생성합니다.

단계 **3** 생성한 목록 또는 피드를 대상 URL 기준으로 선택합니다.

단계 **4** 규칙을 저장합니다.

HTTP 응답 페이지 구성

액세스 제어의 일환으로 액세스 제어 규칙 또는 액세스 제어 정책 기본 작업을 사용하여 시스템이 웹 요청을 차단할 때 표시할 *HTTP* 응답 페이지를 구성할 수 있습니다.

표시되는 응답 페이지는 세션을 차단하는 방법에 따라 달라집니다.

- 응답 페이지 차단: 연결이 거부되었음을 설명하는 기본 브라우저 또는 서버 페이지를 재정의합니다.
- 응답 페이지 인터랙티브 차단: 사용자에게 경고하지만 사용자가 버튼을 클릭하거나 페이지를 새로 고쳐 원래 요청한 사이트를 로드하도록 허용합니다. 사용자는 로드하지 않은 페이지 요소를 로드하기 위해 응답 페이지를 우회한 후 새로 고침해야 할 수 있습니다.

응답 페이지를 선택하지 않으면 상호작용 또는 설명 없이 세션이 차단됩니다.

HTTP 대응 페이지의 제한

응답 페이지는 액세스 제어 규칙**/**기본 작업에 한정

시스템은 액세스 제어 규칙 또는 액세스 제어 정책 기본 작업을 통해 차단되거나 인터랙티브 차단된 암호화되지 않은 연결 또는 암호 해독된 연결에 대해서만 응답 페이지를 표시합니다. 다른 정책 또는 메커니즘에 의해 차단되거나 차단 목록에 추가된 연결에 대한 응답 페이지는 표시되지 않습니다.

응답 페이지를 표시하면 연결 재설정 비활성화

연결이 재설정되면 시스템이 응답 페이지를 표시할 수 없습니다(RST 패킷 전송). 응답 페이지를 활성화하면 시스템은 해당 구성에 우선 순위를 둡니다. **Block with reset(**차단 후 재설정**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)**을 규칙 작업으로 선택하는 경우, 시스템은 응답 페이지를 표시하고 일치하는 웹 연결을 재설정하지 않습니다. 차단된 해당 웹 연결을 재설정하려면 응답 페이지를 비활성화해야 합니다.

규칙과 일치하는 모든 비 웹 트래픽은 차단 후 재설정됩니다.

암호화된 연결의 응답 페이지 없음**(**암호 해독해야 함**)**

시스템은 액세스 제어 규칙 또는 그 밖의 구성에 의해 차단된 암호화된 연결의 응답 페이지를 표시하지 않습니다. 액세스 제어 규칙은 SSL 정책을 구성하지 않았거나 SSL 정책이 암호화된 트래픽을 통과시키는 경우 암호화된 연결을 평가합니다.

예를 들어 시스템은 HTTP/2 또는 SPDY 세션을 암호 해독할 수 없습니다. 이러한 프로토콜 중 하나를 사용하여 암호화한 웹 트래픽이 액세스 제어 규칙 평가 단계에 도달하는 경우 세션이 차단되면 시스템은 응답 페이지를 표시하지 않습니다.

하지만 시스템은 SSL 정책을 통해 암호 해독된 다음 액세스 제어 규칙 또는 액세스 제어 정책 기본 작업을 통해 차단되거나 인터랙티브 차단된 연결에 대해 응답 페이지를 표시합니다. 이러한 경우 시스템은 응답 페이지를 암호화하여 다시 암호화된 SSL 스트림의 종단에서 전송합니다.

'승격된' 연결의 응답 페이지 없음

승격된 액세스 제어 규칙(단순한 네트워크 조건만 사용하여 초기에 배치된 차단 규칙)으로 인해 웹 트래픽이 차단될 때는 시스템에서 응답 페이지를 표시하지 않습니다.

리디렉트된 특정 연결의 응답 페이지 없음

'http' 또는 'https'를 지정하지 않고 URL을 입력했으며, 브라우저가 포트 80에서 연결을 시작했고, 사용자가 응답 페이지를 클릭하고, 이후 연결이 포트 443으로 리디렉트된다면, 사용자는 두 번째 인터랙티브 페이지를 볼 수 없습니다. 이 URL에 대한 응답이 이미 캐시되었기 때문입니다.

URL 식별 전 응답 페이지 없음

시스템에서 요청된 URL을 식별하기 전에 웹 트래픽이 차단되면 시스템은 응답 페이지를 표시하지 않습니다. URL 필터링 모범 사례, 3 페이지를 참조하십시오.

HTTP 응답 페이지 요구 사항 및 사전 요건

모델 지원

Any(모든)

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- 네트워크 관리자

HTTP 응답 페이지 선택

HTTP 응답 페이지의 안정적 표시 여부는 네트워크 구성, 트래픽 로드, 페이지 크기에 따라 달라집니다. 페이지 크기가 작을수록 성공적으로 표시될 가능성이 높습니다.

프로시저

단계 **1** 액세스 제어 정책 편집기에서 **HTTP Responses(HTTP** 응답**)**를 클릭합니다. 새 UI에서 패킷 플로우 라인의 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 이 옵션을 선택합니다.

컨트롤이 흐리게 표시되는 경우에는 상위 정책에서 설정이 상속되거나 컨피그레이션을 수정할 권한이 없는 것입니다. 구성이 잠금 해제되어 있으면 **Inherit from base policy(**기본 정책에서 상속**)**의 선택을 취소하여 수정을 활성화합니다.

단계 **2** **Block Response Page(**차단 응답 페이지**)** 및 **Interactive Block Resposne Page(**인터랙티브 차단 응답 페이지**)**를 선택합니다.

- System-provided(시스템 제공) - 일반 응답을 표시합니다. **View(**보기**)** ( )를 클릭하면 이 페이지의 코드를 확인할 수 있습니다.
- Custom(맞춤형) - 맞춤형 응답 페이지를 생성합니다. **Edit(**수정**)** ( )을 클릭하면 교체 또는 수정할 수 있는 시스템 제공 코드가 미리 채워진 팝업 창이 나타납니다. 사용한 문자 수가 카운터에 표시됩니다.
- None(없음) - 응답 페이지를 비활성화하고 상호작용 또는 설명 없이 세션을 차단합니다. 전체 액세스 제어 정책에서 인터랙티브 차단을 빠르게 비활성화하려면 이 옵션을 선택하십시오.

단계 **3** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

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

HTTP 응답 페이지를 사용한 인터랙티브 차단 구성

인터랙티브 차단을 설정하면 사용자는 경고를 읽은 후 원래 요청된 사이트를 로드할 수 있습니다. 사용자는 로드하지 않은 페이지 요소를 로드하기 위해 응답 페이지를 우회한 후 새로 고침해야 할 수 있습니다.

팁 전체 액세스 제어 정책에서 인터랙티브 차단을 빠르게 비활성화하려면 시스템 제공 페이지나 맞춤형 페이지를 표시하지 마십시오. 그러면 시스템은 상호작용 없이 모든 연결을 차단합니다.

사용자가 인터랙티브 차단을 우회하지 않는 경우, 일치하는 트래픽은 추가 검사 없이 거부됩니다. 사용자가 인터랙티브 차단을 우회하는 경우, 액세스 제어 규칙은 트래픽을 허용하지만 해당 트래픽은 계속 심층 검사 및 차단 대상이 될 수 있습니다.

기본적으로 사용자 우회는 후속 방문 시 경고 페이지 표시 없이 10분(600초) 동안 유효합니다. 이 기간은 최대 1년까지 설정할 수 있으며, 사용자가 매번 차단을 강제로 우회하도록 할 수도 있습니다. 이러한 제한은 정책에서 모든 Interactive Block(인터랙티브 차단) 규칙을 적용합니다. 규칙별 제한은 설정할 수 없습니다.

인터랙티브 차단된 트래픽에 대한 로깅 옵션은 허용된 트래픽의 옵션과 동일하지만 사용자가 인터랙티브 차단을 우회하지 않는 경우, 시스템은 연결 시작 이벤트만 로깅할 수 있습니다. 시스템은 사용자에게 처음 경고할 때 인터랙티브 차단 또는 인터랙티브 차단 후 재설정 작업과 함께 로깅된 모든 연결 시작 이벤트를 표시합니다. 사용자가 차단을 우회하는 경우, 세션에 대해 로깅된 추가 연결 이벤트에는 `Allow(허용)` 작업이 있습니다.

인터랙티브 차단 설정

다음 절차에서는 사용자가 URL 필터링 규칙을 우회하도록 허용하는 방법을 설명합니다.

프로시저

단계 **1** 액세스 제어의 일부로 웹 트래픽과 일치하는 액세스 제어 규칙을 구성하십시오. 액세스 제어 규칙 생성 및 수정의 내용을 참조하십시오.

- 작업 - 규칙 작업을 **Interactive Block(**인터랙티브 차단**)** 또는 **Interactive Block with reset(**인터랙티브 차단 후 재설정**)**으로 설정하십시오. 액세스 제어 규칙 인터랙티브 차단 작업의 내용을 참조하십시오.
- 조건 - URL 조건을 사용하여 인터랙티브 차단할 웹 트래픽을 지정합니다. URL 조건(URL 필터링)의 내용을 참조하십시오.
- 로깅 - 사용자가 차단을 우회할 것이라고 가정하고 그에 따라 로깅 옵션을 선택합니다.
- 검사 - 사용자가 차단을 우회할 것이라고 가정하고 그에 따라 심층 검사 옵션을 선택합니다. 액세스 제어 개요의 내용을 참조하십시오.

단계 **2** (선택 사항) 액세스 제어 정책 **HTTP Responses(HTTP** 응답**)**에서 맞춤형 인터랙티브 차단 HTTP 응답 페이지를 선택합니다. HTTP 응답 페이지 선택, 19 페이지의 내용을 참조하십시오.

단계 **3** (선택 사항) 액세스 제어 정책 **Advanced(**고급**)** 설정에서 사용자 우회 시간 제한을 변경합니다. 차단된 웹사이트의 사용자 우회 시간 제한 설정, 21 페이지의 내용을 참조하십시오.

사용자가 차단을 우회한 후 시스템은 시간 제한 기간이 경과할 때까지 사용자가 해당 페이지를 탐색하는 것을 경고 없이 허용합니다.

단계 **4** 액세스 제어 정책을 저장합니다.

단계 **5** Deploy configuration changes(구성 변경 사항 구축)참조.

차단된 웹사이트의 사용자 우회 시간 제한 설정

다음 절차에서는 사용자가 URL 필터링 차단을 우회한 후 검색에 허용되는 시간을 설정하는 방법을 설명합니다. 시간 제한이 만료되면 사용자는 차단을 다시 우회해야 합니다.

프로시저

단계 **1** **Policies(**정책**)** > **Access Control(**액세스 제어**)**을 클릭하고 정책을 편집합니다.

단계 **2** **Advanced(**고급**)**를 클릭합니다. 새 UI의 패킷 플로우 라인 끝에 있는 **More(**더 보기**)** 드롭다운 화살표에서 **Advanced Settings(**고급 설정**)**를 선택합니다.

단계 **3** General Settings(일반 설정) 옆의 **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 **4** **Allow an Interactive Block to bypass blocking for (seconds)((**초**)** 동안 차단 우회를 위한 인터랙티브 차단 허용**)** 필드에 사용자 우회가 만료되기 전에 경과해야 하는 시간(초)을 입력합니다.

이 값을 0으로 설정하면 인터랙티브 차단 응답이 한 번 표시되고 사용자 우회가 만료되지 않습니다.

단계 **5** **OK(**확인**)**를 클릭합니다.

단계 **6** **Save**를 클릭하여 정책을 저장합니다.

다음에 수행할 작업

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

URL 필터링 상태 모니터 설정

다음 상태 정책은 URL 카테고리 및 평판 데이터를 가져오거나 업데이트하는 데 문제가 발생하는 경우 알려줍니다.

- URL 필터링 모니터
- 디바이스에서 위협 데이터 업데이트

이러한 모듈이 원하는 방식으로 구성되었는지 확인하려면 Cisco Secure Firewall Management Center 관리 가이드의 상태 모듈 및 상태 모니터링 구성을 참조하십시오.

URL 범주 및 평판

Talos에 의해 할당된 카테고리 또는 평판에 이의가 있는 경우, 재평가 요청을 제출할 수 있습니다.

시작하기 전에

Cisco 계정 자격 증명이 필요합니다.

프로시저

단계 **1** Firepower Management Center 웹 인터페이스에서 다음 중 하나를 수행합니다.

분쟁 위치 옵션	분쟁 경로 옵션
클라우드 서비스 설정 페이지	a. **System(**시스템**) > Integration(**통합**) > Cloud Services(**클라우드 서비스**)** 페이지로 이동합니다. b. **Dispute URL categories and reputations(URL** 카테고리 및 평판 이의 제기**)**를 선택합니다.
수동 URL 조회 페이지	a. 수동 URL 조회 페이지: **Analysis(**분석**) > Advanced(**고급**) > URL**로 이동합니다. b. 해당 URL을 조회합니다. c. 테이블 행 끝에서 **Disupte(**이의 제기**)**를 보려면 결과 목록에서 관련 항목 위에 마우스 커서를 올려놓은 다음 Disupte(이의 제기)를 클릭합니다.
URL 연결 이벤트	a. **Analysis(**분석**) > Connections(**연결**)** 메뉴에서 URL이 포함된 테이블이 있는 페이지로 이동합니다. b. **URL Category(URL** 카테고리**)** 또는 **URL Reputation(URL** 평판**)** 열에 있는 항목을 마우스 오른쪽 버튼으로 클릭하고(필요할 경우 숨겨진 열 표시) 옵션을 선택합니다.

별도의 브라우저 창에 Talos 웹사이트가 열립니다.

단계 **2** Cisco 자격 증명으로 Talos 사이트에 로그인합니다.

단계 **3** 정보를 검토하고 Talos 페이지의 지침을 따릅니다.

단계 **4** 제출된 이의 제기를 처리하는 방법과 예상할 수 있는 응답(있는 경우)에 대한 정보를 Talos 사이트에서 찾습니다.

이의 제기 프로세스는 Firepower 제품과 독립적입니다.

URL 범주 집합이 변경되면 작업 수행

새로운 웹 동향과 발전하는 사용 패턴을 수용하기 위해 URL 필터링 카테고리 집합이 때때로 변경될 수 있습니다.

이러한 변경은 정책과 이벤트 모두에 영향을 미칩니다.

URL 범주 변경이 발생하기 직전에 발생하고, 발생한 후에는 변경의 영향을 받는 모든 액세스 제어, SSL 및 QoS 정책에서 규칙 목록에 알림이 표시되며, 사용자가 수정하는 규칙의 URL 또는 범주에서 알림이 표시됩니다.

이러한 알림이 표시되면 조치를 취해야 합니다.

참고 이 주제에서 설명하는 URL 카테고리 집합 업데이트는 단순히 새 URL을 기존 범주에 추가하고 잘못 분류된 URL을 다시 분류하는 변경 작업과는 다릅니다. 이 주제는 개별 URL의 카테고리 변경에는 적용되지 않습니다.

프로시저

단계 **1** 액세스 제어 정책에서 규칙 옆에 경고가 표시된다면, 알림 위에 마우스 커서를 올려 상세정보를 확인합니다.

단계 **2** 경고에서 URL 범주 변경 사항을 언급한다면, 규칙을 편집하여 상세정보를 확인합니다.

단계 **3** 규칙 대화상자의 URL 또는 Category(범주) 위에 마우스 커서를 올려 변경 유형에 대한 일반 정보를 확인합니다.

단계 **4** 범주 옆에 알림이 표시된다면 알림을 클릭하여 상세정보를 확인합니다.

단계 **5** 변경 사항 설명에 'More information(추가 정보)' 링크가 표시된다면, 링크를 클릭해 Talos 웹사이트에서 범주 관련 정보를 확인합니다.

대신 URL 카테고리 및 평판 설명, 3 페이지에 있는 링크에서 모든 범주 목록과 설명을 확인해도 됩니다.

단계 **6** 변경 유형에 따라 적절한 조치를 취합니다.

카테고리 변경 유형	시스템이 수행할 작업	사용자가 수행해야 할 작업
기존 카테고리 사용은 조만간 중단됩니다.	아직은 적용되지 않습니다. 영향받는 규칙을 몇 주 안에 변경해야 합니다. 이 기간에 조치를 취하지 않으면, 시스템에서 정책을 재구축할 수 없게 됩니다.	이 범주를 포함하는 모든 규칙에서 이 범주를 제거합니다. 비슷한 새 범주가 있다면, 해당 범주를 사용하는 것도 고려해 보십시오.
새 카테고리가 추가됨	기본적으로 시스템에서는 새로 추가된 카테고리를 사용하지 않습니다.	새 카테고리에 대한 새 규칙을 생성하는 것이 좋습니다.
기존 카테고리가 삭제됨	해당 카테고리는 규칙에서 취소선 텍스트로 표시됩니다(즉 카테고리 이름에 취소선이 그어집니다).	구축하기 전에 사용하지 않는 카테고리를 규칙에서 삭제해야 합니다.

단계 **7** 이러한 변경 사항에 대한 SSL 규칙(Category(범주))을 확인하고 필요에 따라 조치를 취합니다.

단계 **8** 이러한 변경 사항에 대한 QoS 규칙(URL)을 확인하고 필요에 따라 조치를 취합니다.

다음에 수행할 작업

Deploy configuration changes(구성 변경 사항 구축)참조.

URL 카테고리 및 평판 변경: 이벤트에 미치는 영향

- URL 카테고리가 변경되면 카테고리 변경 전에 시스템에서 처리한 이벤트는 원래 카테고리 이름과 연결되고 **Legacy** 레이블이 지정됩니다. 카테고리 변경 후 시스템에서 처리하는 이벤트는 새 카테고리에 연결됩니다.

  그보다 오래된 레거시 이벤트는 시간이 지나면 시스템에서 삭제됩니다.

- URL이 처리될 때 평판이 없었다면 이벤트 뷰어의 URL 평판 열이 비어 있게 됩니다.

URL 필터링 문제 해결

예상 **URL** 범주가 범주 목록에 없습니다**.**

URL 필터링 기능은 보안 인텔리전스 기능과 다른 범주 집합을 사용합니다. 표시되는 범주는 보안 인텔리전스 범주일 수 있습니다. 이러한 범주를 보려면 액세스 제어 정책에서 **Security Intelligence(**보안 인텔리전스**)** 탭의 **URL** 탭을 확인하십시오.

초기 패킷이 검사되지 않고 통과됨

트래픽이 식별되기 전에 통과하는 패킷 검사 및 하위 항목을 참조하십시오.

DNS 필터링: DNS 조회 중 URL 평판 및 범주 식별, 14 페이지도 참조하십시오.

상태 알림**: 'URL Filtering registration failue(URL** 필터링 등록 실패**)'**

management center와 프록시가 Cisco Cloud에 연결할 수 있는지 확인합니다. Cisco Secure Firewall Management Center 관리 가이드의 주제 인터넷 액세스 요구 사항 및 통신 포트 요구 사항에 있는 URL 필터링 및 URL 범주 관련 정보가 필요할 수 있습니다.

특정 **URL**의 카테고리와 평판을 어떻게 찾을 수 있습니까**?**

수동 조회를 수행합니다. Cisco Secure Firewall Management Center 관리 가이드에서 *URL* 범주 및 평판 찾기를 참조하십시오.

수동 조회를 시도하는 동안 오류**: 'Cloud Lookup Failure for <URL>(<URL>**에 대한 클라우드 조회 실패**)'**

기능이 올바르게 활성화되어 있는지 확인합니다. Cisco Secure Firewall Management Center 관리 가이드에서 *URL* 범주 및 평판 찾기의 사전 요건을 참조하십시오.

URL이 **URL** 카테고리 및 평판에 따라 잘못 처리되는 것 같습니다

문제**:**시스템이 올바르게는 URL 카테고리 및 평판에 따라 URL을 올바로 처리하지 않습니다.

솔루션:

- URL에 연결된 URL 카테고리 및 평판이 사용자가 생각하는 카테고리 및 평판인지 확인하십시오. Cisco Secure Firewall Management Center 관리 가이드에서 *URL* 범주 및 평판 찾기를 참조하십시오.
- 다음 문제는 범주 및 평판을 사용한 URL 필터링 활성화, 11 페이지을(를) 사용하여 액세스할 수 있는 URL 필터링 옵션, 11 페이지에 설명된 설정으로 해결할 수 있습니다.
  - URL 캐시에 오래된 정보가 있을 수 있습니다. URL 필터링 옵션, 11 페이지에서 **Cached URLs Expire(**캐시된 **URL** 만료**)** 설정 관련 정보를 참조하십시오.
  - 로컬 데이터 집합이 클라우드의 최신 정보로 업데이트되지 않았을 수 있습니다. URL 필터링 옵션, 11 페이지에서 **Enable Automatic Updates(**자동 업데이트 활성화**)** 설정에 대한 정보를 참조하십시오.
  - 클라우드에서 최신 데이터를 확인하지 않도록 시스템이 구성되었을 수 있습니다. URL 필터링 옵션, 11 페이지에서 **Query Cisco cloud for unknown URLs(Cisco Cloud**에서 알 수 없는 **URL** 쿼리**)** 설정에 대한 정보를 참조하십시오.
- 클라우드를 확인하지 않고 URL로 트래픽을 전달하도록 액세스 제어 정책이 구성되었을 수 있습니다. 액세스 제어 정책 고급 설정에서 **Retry URL cache miss lookup(URL** 캐시 누락 조회 재시도**)** 설정에 대한 정보를 참조하십시오.
- URL 필터링 모범 사례, 3 페이지도 참조하십시오.
- SSL 규칙을 사용하여 URL이 처리되는 경우, TLS/SSL 규칙 지침 및 제한 사항 및 SSL 규칙 순서의 내용을 참조하십시오.
- 사용자가 생각하는 액세스 제어 규칙을 사용하여 URL이 처리되고 있고 사용자가 생각하는 작업을 규칙이 수행하는지 확인하십시오. 규칙 순서를 고려해야 합니다.
- management center의 로컬 URL 카테고리 및 평판 데이터베이스가 클라우드에서 성공적으로 업데이트되고 매니지드 디바이스가 management center에서 성공적으로 업데이트되는지 확인하십시오.

  이러한 프로세스의 상태는 **URL Filtering Monitor(URL** 필터링 모니터**)** 모듈과 **Threat Data Updates on Devices(**디바이스에서 위협 데이터 업데이트**)** 모듈의 Health Monitor(상태 모니터)에서 보고됩니다. 자세한 내용은 Cisco Secure Firewall Management Center 관리 가이드 의 상태를 참조하십시오.

로컬 URL 카테고리 및 평판 데이터베이스를 즉시 업데이트하려면 **Integration(**통합**)** > **Other Integrations(**기타 통합**)**로 가서 클라우드 서비스을 클릭한 다음 **Update Now(**지금 업데이트**)**를 클릭합니다. 자세한 내용은 URL 필터링 옵션, 11 페이지를 참고하십시오.

URL 범주 또는 평판이 올바르지 않습니다

액세스 제어 또는 QoS 규칙의 경우: 수동 필터링을 사용하며, 규칙 순서를 주의해야 합니다. 수동 URL 필터링, 16 페이지 및 URL 조건 설정, 12 페이지를 참조하십시오.

SSL 규칙의 경우: 수동 필터링은 지원되지 않습니다. 대신 고유 이름 조건을 사용합니다.

URL 범주 및 평판, 22 페이지 섹션도 참조하십시오.

웹 페이지가 느리게 로드됩니다

보안 및 성능은 상충 관계에 있습니다. 몇 가지 옵션:

- **Cached URLs Expire(**캐시된 **URL** 만료**)** 설정을 수정해 보십시오. **Integration(**통합**)** > **Other Integrations(**기타 통합**)**을 클릭한 다음 클라우드 서비스를 선택합니다. 자세한 내용은 URL 필터링 옵션, 11 페이지를 참조하십시오.
- 액세스 제어 정책 고급 설정에서 **Retry URL cache miss lookup(URL** 캐시 누락 조회 재시도**)** 설정의 선택을 취소해 보십시오.

이벤트는 **URL** 카테고리 및 평판은 포함하지 않습니다**.**

- 액세스 제어 정책에 적용 가능한 URL 규칙을 포함했는지, 규칙이 활성 상태인지, 정책이 관련 디바이스에 구축되었는지를 확인하십시오.
- URL 범주 및 평판은 URL 규칙과 매칭되기 전에 연결이 처리되면 이벤트에 표시되지 않습니다.
- URL 범주 및 평판에 대해 연결을 처리하는 규칙을 구성해야 합니다.
- SSL 규칙의 Categories(범주) 탭에서 URL 범주를 구성한 경우에도 액세스 제어 정책의 규칙에서 URL 탭을 구성해야 합니다.

DNS 필터링이 작동하지 않습니다**.**

도메인 조회 중 URL을 식별하도록 DNS 필터링 활성화 , 14 페이지에서 모든 사전 요건과 단계를 완료했는지 확인합니다.

최종 사용자가 차단된 **URL**에 액세스하려고 시도하고 페이지가 회전 및 시간 초과됨

DNS 필터링이 활성화되어 있고 최종 사용자가 차단된 URL에 액세스하면 페이지가 회전하지만 로드되지는 않습니다. 최종 사용자에게 페이지가 차단되었다는 알림이 표시되지 않습니다. 이는 현재 DNS 필터링이 활성화된 경우의 제한 사항입니다.

DNS 필터링 제한, 15 페이지의 내용을 참조하십시오.

이벤트에 **URL** 범주 및 평판이 포함되어 있지만 **URL** 필드가 비어 있음

DNS Query(DNS 쿼리) 필드가 채워져 있고 URL 필드가 비어있는 경우, 이는 DNS 필터링 기능이 활성화될 때 나타납니다.

DNS 필터링 및 이벤트, 15 페이지의 내용을 참조하십시오.

단일 트랜잭션에 대해 여러 이벤트가 생성됨

단일 웹 트랜잭션에서 두 개의 연결 이벤트를 생성하는 경우가 있습니다. 하나는 DNS 필터링이고 다른 하나는 URL 필터링입니다. 이는 DNS 필터링이 활성화되고 다음과 같은 경우에 발생합니다.

- 트래픽에 대한 액세스 제어 규칙 작업이 Allow(허용) 또는 Trust(신뢰)인 경우

- 시스템에서 처음으로 URL을 발견하는 경우

DNS 필터링 및 이벤트, 15 페이지의 내용을 참조하십시오.