콘텐츠 제한을 사용하는 액세스 제어

다음 주제에서는 콘텐츠 제한 기능을 사용하도록 액세스 제어 정책을 구성하는 방법을 설명합니다.

콘텐츠 제한 정보

주요 검색 엔진 및 콘텐츠 제공 서비스에서는 검색 결과 및 웹 사이트 콘텐츠를 제한할 수 있는 기능을 제공합니다. 예를 들어 학교에서는 콘텐츠 제한 기능을 사용하여 CIPA(Children's Internet Protection Act)를 준수합니다.

검색 엔진 및 콘텐츠 제공 서비스를 통해 구현한 경우, 개별 브라우저 또는 사용자에 대해서만 콘텐츠 제한 기능을 시행할 수 있습니다. Firepower System을 사용하면 이러한 기능을 전체 네트워크에 확장할 수 있습니다.

이 시스템에서 시행할 수 있는 기능:

- 안전 검색 — 대다수의 주요 검색 엔진에서 지원되는 이 서비스는 기업, 정부기관, 교육 환경에서 유해물로 분류하는 노골적인 성인 콘텐츠를 필터링하여 제외합니다. 이 시스템은 지원되는 검색 엔진의 홈 페이지에 사용자가 액세스할 수 있는 기능을 제한하지 않습니다.
- *YouTube EDU* — 이 서비스는 교육 환경에서 YouTube 콘텐츠를 필터링합니다. 학교에서는 이 서비스를 사용하여 교육 콘텐츠에 대한 액세스를 설정하는 동시에 비교육 콘텐츠에 대한 액세스를 제한할 수 있습니다. YouTube EDU는 YouTube 제한 모드와는 다른 것으로, Google 세이프서치 기능의 일부로서 YouTube 검색 결과를 제한합니다. YouTube 제한 모드는 세이프서치의 하위 기능입니다. YouTube EDU를 활용하면 사용자는 일반적인 YouTube 홈 페이지 대신 YouTube EDU 홈 페이지에 액세스하게 됩니다.

두 가지 방법을 사용하여 다음 기능을 시행하도록 시스템을 구성할 수 있습니다.

방법**:** 액세스 제어 규칙

콘텐츠 제한 기능은 요청 URI의 요소, 연관된 쿠키 또는 맞춤형 HTTP 헤더 요소를 통해 제한된 상태의 검색 또는 콘텐츠 쿼리를 전달합니다. 시스템에서 트래픽을 처리할 때 이러한 요소를 수정하도록 액세스 제어 규칙을 구성할 수 있습니다.

방법**: DNS** 싱크홀

Google 검색의 경우, 트래픽이 Google 세이프서치 VIP(Virtual IP Address)로 리디렉션하도록 구성할 수 있습니다. 이렇게 하면 세이프서치를 위한 필터가 부여됩니다.

아래 표에는 이러한 시행 방법 간의 차이가 설명되어 있습니다.

표 ***1:*** 콘텐츠 제한 방법 비교

Attribute(속성**)**	방법**:** 액세스 제어 규칙	방법**: DNS** 싱크홀
지원되는 장치	모두	Firepower Threat Defense 전용
검색 엔진 지원	규칙 편집기의 **Applications(**애플리케이션**)** 탭에서 `safesearch supported` 태그가 있는 모든 애플리케이션	Google 전용
YouTube 제한 모드 지원	예	예
YouTube EDU 지원	예	아니요
SSL 정책 필요	예	아니요
호스트에서 IPv4를 사용 중이어야 함	아니요	예
연결 이벤트 로깅	예	예

사용할 방법을 결정할 때에는 다음 제한 사항을 고려하십시오.

- 액세스 제어 규칙 방법에는 SSL 정책이 필요하며, 이는 성능에 영향을 미칩니다.
- Google 세이프서치 VIP는 IPv4 트래픽만 지원합니다. Google 검색을 관리하기 위해 DNS 싱크홀을 구성할 경우, 영향을 받는 네트워크의 모든 호스트에서 IPv4를 사용 중이어야 합니다.

시스템에 로깅되는 연결 이벤트의 **Reason(**이유**)** 필드 값은 방법에 따라 달라집니다.

- 액세스 제어 규칙 — 콘텐츠 제한
- DNS 싱크홀 — `DNS 차단`

콘텐츠 제한 요구 사항 및 사전 요건

모델 지원

Any(모두) 또는 절차에 나와 있는대로.

지원되는 도메인

모든

사용자 역할

- 관리자
- 액세스 관리자
- Network Admin(네트워크 관리자)

액세스 제어 규칙을 사용하여 콘텐츠 제한 시행

주의 규칙 사전 대응을 방지하려면 SSL 및 액세스 제어 정책에서 YouTube EDU 관리 규칙을 안전 검색 관리 규칙 위에 배치합니다. 콘텐츠 제한 규칙 순서 참조.

참고 액세스 제어 규칙에서 안전 검색 또는 YouTube EDU가 활성화되면 인라인 정규화가 자동으로 활성화됩니다. 자세한 내용은 인라인 정상화 전처리기를 참고하십시오.

시작하기 전에

클래식 디바이스의 경우에는 제어 라이선스가 있어야 합니다.

프로시저

단계 **1** SSL 정책을 생성합니다(기본 SSL 정책 생성 참조).

단계 **2** 안전 검색 및 YouTube EDU 트래픽 처리용 SSL 규칙을 추가합니다.

- 규칙에 대한 **Action(**작업**)**으로 **Decrypt - Resign(**암호 해독 - 다시 서명**)**을 선택합니다. 시스템은 콘텐츠 제한 처리를 위한 다른 작업은 지원하지 않습니다.
- **Applications(**애플리케이션**)**에서 **Selected Applications and Filters(**선택한 애플리케이션 및 필터**)** 목록에 선택 항목을 추가합니다.

- YouTube EDU - `YouTube` 및 `YouTube Upload` 애플리케이션을 추가합니다.
- 안전 검색 - `Category: search engine`(카테고리: 검색 엔진) 필터를 추가합니다.

자세한 내용은 애플리케이션 조건(애플리케이션 컨트롤)을 참조해 주십시오.

단계 **3** 추가한 SSL 규칙의 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다.

사전 대응을 방지하기 위해 안전 검색 규칙을 YouTube EDU 규칙 뒤에 배치합니다.

단계 **4** 액세스 제어 정책을 생성 또는 편집하고 SSL 정책을 액세스 제어 정책에 연결합니다.

자세한 내용은 액세스 제어에 다른 정책 연결를 참고하십시오.

단계 **5** 액세스 제어 정책에서 안전 검색 및 YouTube EDU 트래픽 처리를 위한 규칙을 추가합니다.

- 규칙에 대한 **Action(**작업**)**으로 **Allow(**허용**)**를 선택합니다. 콘텐츠 제한 처리를 위해 다른 작업을 수행할 수는 없습니다.
- **Applications(**애플리케이션**)**에서 안전 검색( ) 또는 **YouTube EDU**( )에 대해 흐리게 표시하고 관련 옵션을 설정합니다. 액세스 제어 규칙에 대한 안전 검색 옵션, 5 페이지 및 액세스 제어 규칙에 대한 YouTube EDU 옵션, 5 페이지의 내용을 참조하십시오.

  규칙에 대해 **Allow(**허용**)**가 아닌 **Action(**작업**)**을 선택하면 이러한 옵션은 흐리게 표시되지 않고 비활성화됩니다.

  같은 액세스 제어 규칙에 대해 안전 검색 제한과 YouTube EDU 제한을 둘 다 활성화할 수는 없습니다.
- **Applications(**애플리케이션**)**의 **Selected Applications and Filters(**선택한 애플리케이션 및 필터**)** 목록에서 애플리케이션 선택 항목을 구체화합니다.

  대부분의 경우 안전 검색 또는 YouTube EDU를 활성화하면 **Selected Applications and Filters(**선택한 애플리케이션 및 필터**)** 목록에 적절한 값이 입력됩니다. 이 기능을 활성화할 때 안전 검색 또는 YouTube 애플리케이션이 목록에 이미 있으면 값이 목록에 자동으로 입력되지 않습니다. 애플리케이션이 자동으로 입력되지 않으면 다음과 같이 수동으로 추가합니다.

  - YouTube EDU - `YouTube` 및 `YouTube Upload` 애플리케이션을 추가합니다.
  - 안전 검색 - `Category: search engine`(카테고리: 검색 엔진) 필터를 추가합니다.

자세한 정보는 애플리케이션 조건 및 필터 구성의 내용을 참고하십시오.

단계 **6** 추가한 액세스 제어 규칙의 규칙 위치를 설정합니다. 이렇게 하려면 규칙을 클릭하여 끌거나 오른쪽 클릭 메뉴를 사용하여 잘라내고 붙여넣습니다.

사전 대응을 방지하기 위해 안전 검색 규칙을 YouTube EDU 규칙 뒤에 배치합니다.

단계 **7** 제한된 콘텐츠가 차단될 때 표시되는 HTTP 응답 페이지)를 구성합니다(HTTP 응답 페이지 선택 참조).

단계 **8** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.

액세스 제어 규칙에 대한 안전 검색 옵션

Firepower System은 특정 검색 엔진에 대해서만 안전 검색 필터링을 지원합니다. 지원되는 검색 엔진 목록을 확인하려면 액세스 제어 규칙 편집기의 **Applications(**애플리케이션**)** 탭에서 `safesearch supported` 태그가 지정된 애플리케이션을 참고하십시오. 지원되지 않는 검색 엔진 목록을 확인하려면 `safesearch unsupported` 태그가 지정된 애플리케이션을 참고하십시오.

액세스 제어 규칙에 대해 안전 검색을 활성화할 때는 다음 파라미터를 설정합니다.

안전 검색 활성화
: 이 규칙과 일치하는 트래픽에 대해 안전 검색 필터링을 활성화합니다.

Unsupported Search Traffic(지원되지 않는 검색 트래픽**)**
: 지원되지 않는 검색 엔진의 트래픽을 처리할 때 시스템에서 수행하도록 할 작업을 지정합니다. **Block(**차단**)** 또는 **Block with Reset(**차단 후 재설정**)**을 선택하는 경우에는 제한된 콘텐츠가 차단될 때 시스템에 표시되는 HTTP 응답 페이지도 구성해야 합니다(HTTP 응답 페이지 선택 참조).

액세스 제어 규칙에 대한 **YouTube EDU** 옵션

액세스 제어 규칙에 대해 YouTube EDU를 활성화할 때는 다음 파라미터를 설정합니다.

Enable YouTube EDU(YouTube EDU 활성화**)**
: 이 규칙과 일치하는 트래픽에 대해 YouTube EDU 필터링을 활성화합니다.

맞춤형 **ID**
: YouTube EDU 이니셔티브에서 학교나 지역 네트워크를 고유하게 식별하는 값을 지정합니다. YouTube에서는 학교나 지역에서 YouTube EDU 계정을 등록하면 이 ID를 제공합니다.

참고 **Enable YouTube EDU(YouTube EDU** 활성화**)**를 선택하는 경우 **Custom ID(**맞춤형 **ID)**를 입력해야 합니다. 이 ID는 YouTube가 외부에서 정의합니다. YouTube 시스템에 대해 입력하는 내용은 검증되지 않습니다. 잘못된 ID를 입력하면 YouTube EDU 제한이 올바르게 수행되지 않을 수 있습니다.

DNS 싱크홀을 사용하여 콘텐츠 제한 적용

일반적으로 DNS 싱크홀은 특정 대상에서 멀리 트래픽을 전송합니다. 이 절차에서는 Google 및 YouTube 검색 결과에 콘텐츠 필터를 적용하는 Google SafeSearch Virtual IP Address(VIP)로 트래픽을 재전송하도록 DNS 싱크홀을 구성하는 방법을 설명합니다.

Google SafeSearch는 VIP에 단일 IPv4 주소를 사용하므로 호스트는 IPv4 주소 지정을 사용해야 합니다.

주의 네트워크에 프록시 서버가 포함된 경우, 이 콘텐츠 제한 방법은 Firepower Threat Defense 디바이스를 프록시 서버와 인터넷 사이에 배치하지 않는 한 효과가 없습니다.

이 절차에서는 Google 검색에 콘텐츠 제한을 적용하는 방법만 설명합니다. 다른 검색 엔진에 콘텐츠 제한을 적용하려면 액세스 제어 규칙을 사용하여 콘텐츠 제한 시행, 3 페이지를 참조하십시오.

시작하기 전에

이 절차는 Firepower Threat Defense에만 적용되며 위협 라이선스가 필요합니다.

프로시저

단계 **1** 다음 URL을 통해 지원되는 Google 도메인 목록을 얻을 수 있습니다(https://www.google.com/supported_domains).

단계 **2** 로컬 컴퓨터에서 맞춤형 DNS 목록을 생성하고 다음 항목을 추가합니다.

- Google SafeSearch를 적용하려면 지원되는 Google 도메인마다 항목을 추가합니다.
- YouTube 제한 모드를 적용하려면 "youtube.com" 항목을 추가합니다.

맞춤형 DNS 목록은 텍스트 파일(.txt) 형식이어야 합니다. 텍스트 파일의 각 행은 앞에 마침표 없이 개별 도메인 이름을 지정해야 합니다. 예를 들어 지원되는 도메인 ".google.com"은 "google.com"으로 표시되어야 합니다.

단계 **3** 맞춤형 DNS 목록을 Firepower Management Center에 업로드합니다(새 보안 인텔리전스 목록을 다음에 업로드 Firepower Management Center 참조).

단계 **4** Google SafeSearch VIP의 IPv4 주소를 결정합니다. 예를 들어 forcesafesearch.google.com에서 `nslookup`을 실행합니다.

단계 **5** SafeSearch VIP에 대한 싱크홀 개체를 생성합니다(싱크홀 개체 생성 참조).

이 개체에 다음 값을 사용합니다.

- IPv4 Address(IPv4 주소) - SafeSearch VIP 주소를 입력합니다.
- IPv6 Address(IPv6 주소) - IPv6 루프백 주소(`::1`)를 입력합니다.
- Log Connections to Sinkhole(싱크 홀에 대한 로그 연결)-Log Connections(로그 연결)
- Type(유형) - **None(**없음**)**을 선택합니다.

단계 **6** 기본 DNS 정책을 생성합니다(기본 DNS 정책 생성 참조).

단계 **7** 싱크홀의 DNS 규칙을 추가합니다(DNS 규칙 생성 및 편집 참조).

이 규칙에서:

- **Enable(**활성화**)** 확인란을 선택합니다.
- **Action(**작업**)** 드롭다운 목록에서 `Sinkhole(싱크홀)`을 선택합니다.

- **Sinkhole(**싱크홀**)** 드롭다운 목록에서 생성한 싱크홀 개체를 선택합니다.
- 생성한 맞춤형 DNS 목록을 **DNS**에서 **Selected Items(**선택한 항목**)** 목록에 추가합니다.
- (선택 사항) 콘텐츠 제한을 특정 사용자로 제한하려면 **Networks(**네트워크**)**에서 네트워크를 선택합니다. 예를 들어 콘텐츠 제한을 학생 사용자로 제한하려면 학생들을 교직원과 다른 서브넷에 할당하고 이 규칙에서 해당 서브넷을 지정하십시오.

단계 **8** DNS 정책을 액세스 제어 정책에 연결합니다(액세스 제어에 다른 정책 연결 참조).

단계 **9** 구성 변경사항을 구축합니다. 컨피그레이션 변경 사항 구축의 내용을 참조하십시오.