Secure Web Appliance에서 알 수 없는 애플리케이션을 차단하는 방법

목차

소개

이 문서에서는 Cisco Secure Web Appliance에서 알 수 없는 애플리케이션을 차단하는 몇 가지 방법에 대해 설명합니다.

알 수 없는 응용 프로그램을 차단하는 방법

이러한 방법을 단독으로 또는 조합하여 사용할 수 있습니다.

> **참고:** 이 기술 자료 문서는 Cisco에서 유지 관리하거나 지원하지 않는 소프트웨어를 참조합니다. 이 정보는 귀하의 편의를 위해 제공됩니다. 자세한 내용은 소프트웨어 공급업체에 문의하십시오.

사용자 에이전트 문자열을 기반으로 애플리케이션 차단

첫 번째 방어는 사용자 에이전트 문자열을 사용하여 알 수 없는 애플리케이션을 차단하는 것입니다.

- 사용자 에이전트 추가 **Web Security Manager** > **Access Policies** > **Protocols and User Agents** 열 <필수 액세스 정책용>
- 아래에 사용자 에이전트 문자열 추가 **Block Custom User Agents** (한 줄에 하나씩)

> **참고:** Reference(참조)에 제공된 링크를 사용하여 User Agents(사용자 에이전트)를 검색할 수 있습니다.

애플리케이션 가시성 제어를 기반으로 애플리케이션 차단

AVC(Application Visibility Controls)가 활성화된 경우 **GUI > Security Services > Web Reputation and Anti-Malware**)를 클릭한 다음 프록시, 파일 공유, 인터넷 유틸리티 등과 같은 애플리케이션 유형에 따라 액세스를 차단할 수 있습니다. 이 작업은 **Web Security Manager > Access Policies > Applications** 열 <필수 액세스 정책용>

MIME 유형을 기반으로 애플리케이션 차단

사용자 에이전트가 없으면 MIME(Multipurpose Internet Mail Extensions) 유형을 추가하려고 시도할 수 있습니다.

- 아래에 MIME 유형 추가 **Web Security Manager** > **Web Access Policies** > **Objects** 열 <필수 액세스 정책용 >
- 개체/MIME 유형을 **Block Custom MIME Types** 섹션(한 줄에 하나씩). 예를 들어 BitTorrent 애플리케이션을 차단하려면 application/x-bittorrent.

  참고: Reference(참조)에 제공된 링크를 사용하여 MIME 유형을 검색할 수 있습니다.

액세스 정책에서 URL 범주 차단

필터 방지, 불법 활동, 불법 다운로드 등의 범주가 액세스 정책에서 차단되었는지 확인합니다. 일부 응용 프로그램에서 연결에 알려진 URL 또는 IP 주소를 사용하는 경우, 해당 IP 주소, FQDN(Fully Qualified Domain Name) 또는 도메인과 일치하는 regex를 사용하여 관련 사전 정의된 URL 카테고리를 차단하거나 차단된 사용자 지정 URL 카테고리에서 구성할 수 있습니다. 이 작업은 **Web Security Manager > Access Policies > URL Categories** 열.

액세스 정책에서 HTTP CONNECT 포트 컨피그레이션 제한

일부 응용 프로그램에서는 HTTP CONNECT 메서드를 사용하여 다른 포트에 연결할 수 있습니다. HTTP CONNECT 포트 컨피그레이션 도메인의 사용자 환경에 필요한 알려진 포트 또는 특정 포트만 허용합니다.

- HTTP CONNECT는 **Web Security Manager** > **Access Policies** > **Protocols and User Agents** 열 <필수 액세스 정책용>
- 아래에 허용되는 포트 추가 **HTTP CONNECT Ports**.

특정 IP 주소에 대한 액세스 차단

액세스 중인 대상 IP 주소만 알고 있는 애플리케이션의 경우 L4 트래픽 모니터 기능을 사용하여 특정 IP 주소에 대한 액세스를 차단할 수 있습니다. 아래의 대상 IP를 추가할 수 있습니다. **Web Security Manager > L4 Traffic Monitor > Additional Suspected Malware Addresses**.

응용 프로그램에서 사용하는 사용자 에이전트 또는 MIME 유형을 찾는 방법

특정 애플리케이션에서 어떤 사용자 에이전트 또는 MIME 유형을 사용하고 있는지 모르는 경우 다음 단계 중 하나를 수행하여 이 정보를 찾을 수 있습니다.

- 클라이언트의 시스템에서 WireShark(Ethereal)로 패킷 캡처를 실행하고 'http' 프로토콜에 대한

필터를 실행합니다.
- Secure Web Appliance에서 캡처 실행 **Support and Help** > **Packet Capture**)에 대해 필터링됩니다.

참조

참고: 여기에 나열된 외부 웹 사이트는 참조용으로만 제공됩니다. 링크 및 콘텐츠는 Cisco에서 제어하지 않으며 변경될 수 있습니다.

사용자 에이전트 목록

사용자 에이전트 String.Com(useragentstring.com)

MIME 유형 목록

- 일반 MIME 유형(mozilla.org)
- MIME 유형: 전체 MIME 유형 목록(w3cub.com)
- MIME 유형 전체 목록(sitepoint.com)