Secure Web Appliance 악성코드 및 스파이웨어 차단 이해

목차

소개

이 문서에서는 Cisco SWA(Secure Web Appliance)의 포괄적인 악성코드 및 스파이웨어 방지 기능에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SWA 관리.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

개요

Cisco SWA는 광범위한 스파이웨어 및 웹 기반 악성코드에 대해 강력하고 포괄적인 게이트웨이 방

어 메커니즘을 제공하도록 설계되었습니다. 네트워크 리소스 소모 및 지원 가능성 문제를 크게 야기하는 것으로 악명 높은 애드웨어, 트로이 목마, 브라우저 하이재커, 브라우저 헬퍼 개체, 피싱, 파밍, 시스템 모니터, 키로거 및 웜과 같은 더 심각한 위협에 이르기까지 다양한 위협을 효율적으로 차단합니다.

SWA의 주요 차별화 요소

통합 L4TM(Layer 4 Traffic Monitor)

L4 트래픽 모니터는 유선 속도로 모든 네트워크 포트(총 65,535개)를 스캔할 수 있으므로 악성코드 및 무단 통신 시도를 포괄적으로 탐지하고 차단할 수 있습니다. 이 기능은 포트 80 및 443과 같은 일반 포트를 우회하려는 악성코드를 효과적으로 차단하고 비인가 P2P(Peer-to-Peer) 및 IRC(Internet Relay Chat) 활동을 억제합니다.

프록시 계층 처리

SWA는 통합 캐싱 및 콘텐츠 가속화 기능을 갖춘 고성능 웹 프록시를 통합합니다. Cisco 전용 AsyncOS를 기반으로 하는 이 웹 프록시는 기존 UNIX 기반 프록시 서버보다 최대 10배 많은 연결을 관리할 수 있습니다. 웹 프록시로서, 웹 기반 악성코드에 대한 정확한 방어에 필수적인 애플리케이션 레이어에서 철저한 콘텐츠 검사를 지원합니다.

웹 신뢰도 필터

업계 선구적인 웹 평판 필터로 추가 방어 레이어를 제공합니다. 이러한 필터는 SenderBase®를 활용하여 50개 이상의 웹 트래픽 및 네트워크 관련 매개변수를 평가하여 URL의 신뢰성을 확인합니다. 고급 보안 모델링 기술을 사용하여 각 매개변수에 개별 가중치를 할당하여 -10에서 +10 범위의 평판 점수를 매깁니다. 관리자가 구성한 정책은 이러한 점수를 기반으로 동적으로 조정됩니다.

DVS(Dynamic Vectoring and Streaming) 엔진

DVS 엔진은 ICAP(Internet Content Adaptation Protocol) 및 멀티 박스(multi-box) 구축을 통해 악성코드를 스캐닝하는 레거시 아키텍처와는 별도로 SWA 내에서 가속화된 시그니처 스캐닝을 도입합니다. 이 최첨단 플랫폼은 정교한 객체 구문 분석, 벡터링 기술, 스트림 스캐닝 및 판정 캐시를 활용하여 1세대 ICAP 기반 솔루션에 비해 스캐닝 처리량을 최대 10배 향상시킵니다.

Cisco Anti-Malware 시스템

이 시스템은 DVS 엔진을 Webroot에서 제공하는 여러 시그니처 유형과 함께 활용하여 다양한 웹 기반 위협에 대해 탁월한 보호 기능을 제공합니다. 위협의 범위에는 애드웨어, 브라우저 납치범, 피싱, 파밍 공격, 트로이 목마, 시스템 모니터, 키로거 등의 악의적인 엔터티가 포함됩니다. SWA는 게이트웨이에서 업계 최대 규모의 악성코드 시그니처 데이터베이스를 자랑하며 포괄적인 보호를 보장

합니다.

따라서 Cisco Web Security Appliance는 광범위한 웹 기반 위협으로부터 네트워크 게이트웨이를 보호하는 데 있어 선도적인 위치를 차지하며 강력한 보호 기능과 고성능 네트워크 처리량을 모두 보장합니다.

관련 정보

- AsyncOS 15.2 for Cisco Secure Web Appliance 사용 설명서

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.