Cisco WSA(Web Security Appliance)에서 악성코드/스파이웨어 차단 기능을 제공합니까?

목차

질문

Cisco WSA(Web Security Appliance)에서 악성코드/스파이웨어 차단 기능을 제공합니까?

Cisco WSA(Web Security Appliance)는 스파이웨어 및 웹 기반 악성코드에 대해 업계에서 가장 포괄적인 게이트웨이 방어 기능을 제공합니다.여기에는 애드웨어(가장 지원 가능한 문제를 야기하며 상당한 네트워크 리소스를 소모함)부터 트로이 목마, 브라우저 하이재커, 브라우저 헬퍼 객체, 피싱, 파밍, 시스템 모니터, 키로거, 벌레 등과 같은 더 악의적인 위협에 이르기까지 모든 것이 포함됩니다.

Cisco Web Security 솔루션의 주요 차별화 요소는 다음과 같습니다.

1. 통합 레이어 4(L4) 트래픽 모니터는 모든 포트를 유선 속도로 스캔하여 악성코드 및 Phone-Home 활동을 탐지 및 차단합니다.L4 Traffic Monitor는 65,535개의 모든 네트워크 포트를 추적하여 포트 80을 우회하려는 악성코드를 효과적으로 차단하고 비인가 P2P 및 IRC 관련 활동을 방지합니다.
2. 프록시 레이어 처리:Cisco Web Security Appliance는 또한 통합 캐싱 및 콘텐츠 가속화 기능과 함께 매우 높은 성능의 웹 프록시를 포함합니다.Cisco 전용 운영 체제인 AsyncOS를 기반으로 하는 Cisco Web Proxy 어플라이언스는 기존 UNIX 기반 프록시 서버보다 최대 10만 개의 동시 연결을 지원할 수 있습니다.웹 프록시를 사용하면 애플리케이션 레이어에서 포괄적인 콘텐츠 검사를 수행할 수 있습니다. 이는 웹 기반 악성코드에 대한 정확성을 보장하기 위한 중요한 요구 사항입니다.
3. 업계 최초의 웹 평판 필터는 강력한 외부 방어 레이어를 제공합니다.SenderBase®를 활용하는 Cisco Web Reputation Filter는 50개 이상의 다양한 웹 트래픽 및 네트워크 관련 매개변수를 분석하여 URL의 신뢰성을 정확하게 평가합니다.정교한 보안 모델링 기술을 사용하여 각 매개변수를 개별적으로 측정하고 -10 ~ +10 범위의 단일 점수를 생성합니다. 관리자가 구성한 정책은 평판 점수를 기반으로 동적으로 적용됩니다.
4. DVS 엔진(Dynamic Vectoring & Streaming Engine)을 사용하여 서명 스캐닝을 가속화합니다. ICAP와 멀티 박스 구축을 통해 악성코드 스캐닝을 보장하는 레거시 아키텍처 솔루션과 달리, Cisco WSA는 통합 온박스(on-box) 스캔 솔루션용 DVS 엔진을 도입했습니다.이 혁신적인 플랫폼은 스트림 스캐닝 및 판정 캐싱과 함께 정교한 개체 구문 분석 및 벡터링 기술을 적용하여 1세대 ICAP 기반 솔루션에 비해 최대 10배 증가한 스캔 처리량을 제공합니다.
5. 업계 최고의 Cisco Anti-Malware System은 Webroot의 DVS 엔진 및 여러 시그니처 유형을 활용하여 가장 광범위한 웹 기반 위협에 대해 동급 최고의 보호를 제공합니다.이러한 위협은 애드웨어, 브라우저 공중 납치범, 피싱 및 파밍 공격에서부터 트로이 목마, 시스템 모니터, 키로거 같은 더 많은 악의적인 위협에 이르기까지 다양합니다.WSA는 게이트웨이에서 업계 최대

의 악성코드 시그니처 데이터베이스를 제공합니다.