

Intrusion Prevention Service (침입방지 서비스)



WatchGuard® 어플라이언스의 통합 보안 서비스

Intrusion Prevention Service(IPS)는 WatchGuard XTM 솔루션의 응용 프로그램 레이어 콘텐츠 검사와 함께 작동하면서 SQL 주입, 사이트 간 스크립팅, 버퍼 오버플로우 등의 네트워크 위협을 실시간으로 차단해 줍니다.

IPS를 추가해야 하는 이유

IPS는 주기적 업데이트되는 시그니처를 사용하여 주요 프로토콜의 트래픽을 전부 스캔하면서 모든 유형의 위협을 감지하고 차단합니다. IPS는 WatchGuard XTM 보안 어플라이언스와 통합되기 때문에, 하드웨어를 추가로 구입하여 유지 보수하지 않고도 관리하기 쉽고 경제적인 솔루션을 얻는 셈입니다.

보안 솔루션에 IPS (침입방지 서비스)를 추가하는 이유
세 가지는 Cross-site 스크립트 공격, SQL 주입, 버퍼 오버플로우 때문입니다.

IPS로 네트워크 공격 차단

WatchGuard XTM 어플라이언스의 응용 프로그램 레이어 콘텐츠 검사 기능은 스푸핑, 플러드, 서비스 거부 등의 네트워크 공격을 막아 줍니다. Intrusion Prevention Service는 시그니처 기반의 네트워크 침입 탐지를 통해 보호 장막을 하나 더 추가합니다.

네트워크 침입 탐지 및 차단

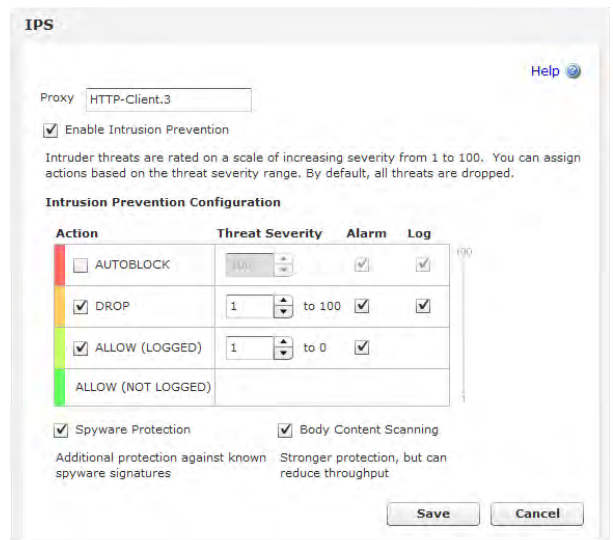
- 응용 프로그램, 데이터베이스, 운영 체제의 여러 가지 알려진 정보 보안 취약 지점과 노출 지점을 종합적으로 보호합니다.
- 15,000개 이상의 시그니처를 바탕으로 SQL 주입, 사이트 간 스크립팅(XSS), 버퍼 오버플로우, 서비스 거부, 원격 파일 포함 등 광범위한 위협을 모두 막아냅니다.
- 시그니처 데이터베이스는 끊임없이 업데이트되므로 시기 적절하고 광범위한 위협 차단이 보장됩니다. 새로운 위협이 등장하는 순간 새로운 시그니처도 공개됩니다.
- HTTP, HTTPS, FTP, TCP, UDP, DNS, SMTP, POP3 등 주요 프로토콜을 전부 스캔하여 네트워크, 응용 프로그램 및 프로토콜 기반의 공격을 차단합니다.
- 웹 서핑 시 지나가는 스파이웨어를 차단하고 호스트에 접속하려고 하는 스파이웨어를 찾아내서 네트워크를 스파이웨어로부터 안전하게 지켜 줍니다.

세분화된 위협 대처 관리

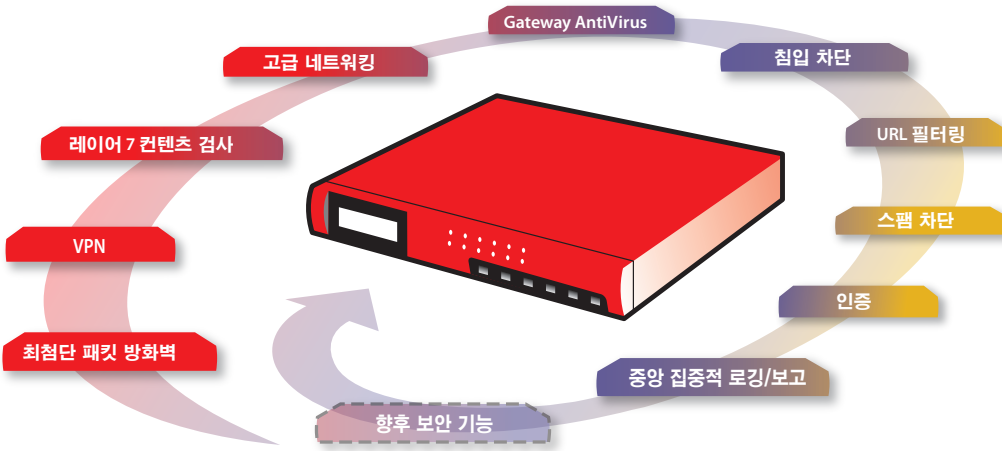
- 위협 수준에 따라 구체적인 조치를 지정합니다. 시그니처마다 심각도가 정해져 있습니다.
- 공격자로 파악된 IP 주소를 자동으로 차단하여 악성 트래픽이 더 이상 네트워크로 진입하지 못하게 할 수 있습니다.
- 차단된 사이트 목록을 작성하고, 일단 공격자로 확인된 IP 주소에서 향후 공격이 개시되면 동적으로 차단합니다.
- 특정 시그니처를 제외할 수 있습니다. 공통 취약 지점 및 노출 지점(CVE)이 있으면 그 이름을 알려서 각종 네트워크 보안 도구 간에 보다 쉽게 데이터를 공유할 수 있습니다.

경제적 침입 방지

- IPS 서비스 하나로 WatchGuard XTM 방화벽 뒤의 모든 사용자를 네트워크 전체에 걸쳐 보호합니다.
- 비용 절감 효과를 더 높이려면 WebBlocker, spamBlocker, Gateway AntiVirus, LiveSecurity Service(기술 지원 포함) 등 강력한 보안 서비스 패키지와 함께 묶인 IPS 번들을 구입하십시오.



완벽히 통합된 보안으로 종합적 보호



올인원 보안 솔루션

WatchGuard XTM 어플라이언스와 강력한 보안 서비스 기능을 결합하면 맬웨어를 포괄적으로 차단할 수 있습니다. 직관적인 콘솔 하나에서 모든 보안 기능을 관리하고, 로그 및 보고 기능은 중앙에서 실행하므로 항상 네트워크의 최신 보안 상황을 확인할 수 있습니다.

위협 상황은 끊임없이 변화하기 때문에, 보안 서비스를 통해 새로운 네트워크 방어 기능을 손쉽게 추가할 수 있도록 WatchGuard XTM 솔루션을 설계했습니다. 따라서 비용이 많이 드는 하드웨어 업그레이드는 필요 없습니다.

간편한 보안 서비스 관리

Gateway AntiVirus를 비롯하여 WatchGuard XTM 솔루션의 보안 기능은 모두 직관적인 콘솔 하나에서 관리할 수 있으므로 효율과 편의성이 극대화됩니다.

- Gateway AV에 탑재된 보안 활동은 로그 및 저장 과정을 거쳐 간단히 보고되므로 즉각 예방 또는 정정 조치를 취할 수 있습니다.
- IT 관리자는 의심스러운 트래픽의 유형, 사용자/그룹, 프로토콜 등을 기준으로 네트워크에서 해당 트래픽 허용, 차단, 검역, 잠금 등 맬웨어 탐지 시 취할 조치를 융통성 있게 정의할 수 있습니다.
- WatchGuard XTM 어플라이언스를 구입하시면 다양한 보고 및 모니터링 등의 관리 도구도 모두 기본 제공됩니다. 하드웨어나 소프트웨어를 추가로 구입할 필요가 없습니다.

기타 WatchGuard 보안 서비스

WatchGuard는 주요 공격 영역의 보호 수준을 대폭 높여 주는 완벽한 보안 서비스 패키지를 제공합니다. IPS 외의 서비스는 다음과 같습니다.

- WebBlocker** URL 및 콘텐츠 필터링(HTTP 및 HTTPS 검사 포함) 서비스는 문제가 될 만한 자료를 담고 있는 사이트나 알려진 스파이웨어 및 피싱 사이트 등 네트워크 보안에 위협이 되는 사이트에 대한 액세스를 제어할 수 있습니다.
- spamBlocker** 서비스는 원치 않는 전자 메일이 내부 메일 서버나 클라이언트까지 도달하기 전에 실시간으로 거의 100% 차단할 수 있습니다. 네트워크에 바이러스 확산 방지 장막이 하나 더 추가되며 완벽한 스팸 검역 기능도 갖추고 있습니다.
- Gateway AntiVirus**는 알려진 바이러스, 트로이 목마, 웜, 스파이웨어 및 로그웨어를 실시간으로 차단해 줍니다.

번들 구매로 한 번에 해결!

WatchGuard의 보안 번들을 구매하시면 방화벽, VPN, 보안 서비스, 기술 지원 등을 담은 편리한 패키지 하나로 완벽한 위협 관리에 필요한 모든 것이 제공됩니다.

모든 보안 번들에는 다음이 포함됩니다.

- WatchGuard XTM 어플라이언스 1종(8 시리즈 또는 10 시리즈)
- spamBlocker
- WebBlocker
- Gateway AntiVirus
- Intrusion Prevention Service
- LiveSecurity® Service의 기술 지원, 하드웨어 보증, 소프트웨어 업데이트 및 위협 경보

이 번들을 처음 구입하는 순간부터 지속적 보안을 통해 보다 쉽고 효율적인 네트워크 보안이 보장됩니다. 별도의 비용 부담이나 계약서 또는 추가 하드웨어 없이 놀라운 가격에 완벽한 솔루션을 구입할 기회입니다.

기존 사용자라면 보안 소프트웨어 패키지 구입*

이미 사용 중인 WatchGuard XTM 어플라이언스에 보안 소프트웨어 패키지를 추가하여 완벽한 위협 관리 솔루션으로 탈바꿈할 수 있습니다. 이 패키지에는 위에서 설명한 모든 보안 서비스와 함께 최고의 안내자 겸 지원자 역할을 하는 LiveSecurity가 포함되어 있습니다. 한꺼번에 구입할 경우 놀라운 비용 절감 효과를 보실 수 있습니다.

*어플라이언스는 보안 소프트웨어 패키지에 들어 있지 않습니다.

보안 번들 및 소프트웨어 보안 패키지에 대해 1년, 2년, 3년간 서비스 패키지를 이용하실 수 있습니다.

주소: 18 층 경양 빌딩 서울 특별시 강남구 삼성동 157-27 • 웹: www.watchguardutm.co.kr • 전화: (02) 557 7833 • 이메일: inquiry.korea@watchguard.com

이 문서는 명시적 또는 묵시적 보증을 제공하지 않습니다. 모든 사양은 변경될 수 있으며 향후 예정된 제품, 기능 또는 특징은 가능한 상황 및 시기에 제공될 것입니다. © 2009 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, WatchGuard 로고, LiveSecurity는 미국 및/또는 기타 국가에서 WatchGuard Technologies, Inc.의 상표 또는 등록 상표입니다. 그 밖의 모든 상표는 해당 소유권자의 재산입니다. Part No. WGCE66652_101609