

# Gateway AntiVirus

WatchGuard® XTM 어플라이언스의 통합 보안 서비스



## 방어의 최일선은 Gateway AntiVirus

바이러스, 웜, 트로이 목마를 게이트웨이에서 차단

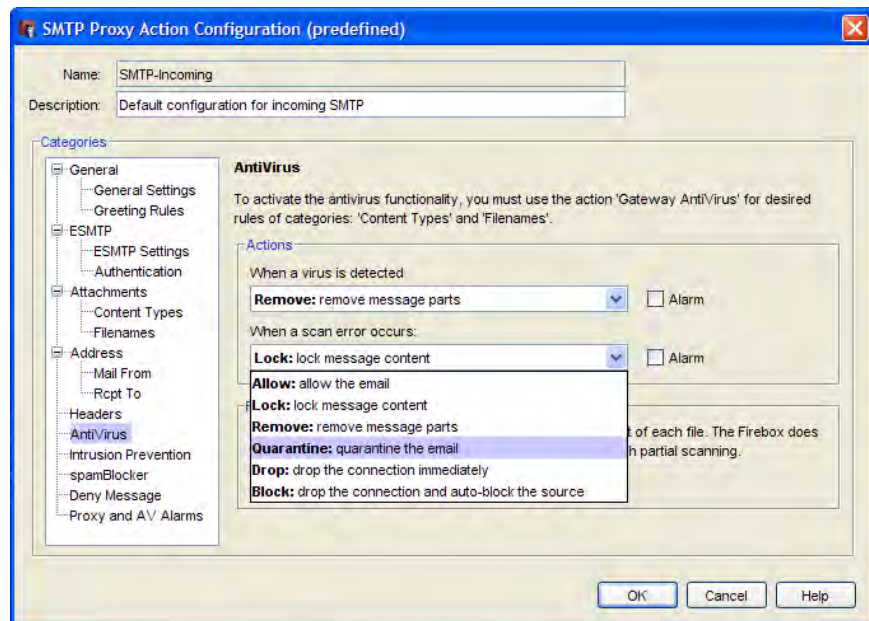
- HTTP, HTTPS, FTP, TCP, UDP, SMTP, POP3 등 주요 프로토콜을 전부 스캔하여 모든 유형의 맬웨어를 차단합니다.
- 전자 메일 트래픽을 게이트웨이에서 스캔하므로 각종 위협이 서버에 접근하여 위험한 작업을 실행하기 전에 막을 수 있습니다.
- 의심되는 전자 메일은 플래그 표시하여 검역소로 보내서 검역한 다음, 관리자가 자동 전자 메일 경보를 통해 사용자의 해당 파일 액세스를 제한하거나 허용할 수 있습니다.
- 악성 코드의 다운로드 및 실행을 차단함으로써 보다 안전한 인터넷 이용을 보장합니다.

## 우수한 스캔 효과

- 업계 최고의 AVG Technologies\*에서 제공하는 고급 스캔 엔진을 사용합니다.
- 매 시간 업데이트를 확인하도록 시그니처 데이터베이스를 구성하면 시기 적절하고 광범위한 위협 차단이 가능합니다.
- 코드 에뮬레이션을 이용한 동적 휴리스틱(heuristic) 분석을 통해 시그니처로는 잡을 수 없는 여러 형태의 바이러스와 위험한 코드를 찾아냅니다.
- 압축 파일 및 인코딩된 파일은 압축 해제 후 검사하며, .zip, .gzip, .tar, .jar, .rar, .chm, .lha, .pdf, XML/HTML 컨테이너, OLE 컨테이너(Microsoft Office 문서), .cab, .arj, .ace, .bz2(Bzip), .swf 등 폭넓은 압축 포맷을 지원합니다.
- 스캔 프로세스에 버퍼를 사용하여 인라인 HTTP 스캔 성능을 극대화합니다.

## 경제적인 바이러스 스캔

- Gateway AV 서비스 하나로 WatchGuard XTM 방화벽 뒤의 모든 사용자를 네트워크 전체에 걸쳐 보호합니다.
- 강력한 보안 서비스 제품으로 구성된 WatchGuard 패키지와 Gateway AV를 번들로 구입할 경우 비용 절감 효과가 더욱 높아집니다.



Gateway AntiVirus(Gateway AV)는 WatchGuard XTM 솔루션의 응용 프로그램 레이어 콘텐츠 검사와 함께 작동하면서 알려진 바이러스와 트로이 목마, 웜, 스파이웨어 및 로그웨어 등을 실시간으로 차단해 줍니다.

### Gateway AV를 추가해야 하는 이유

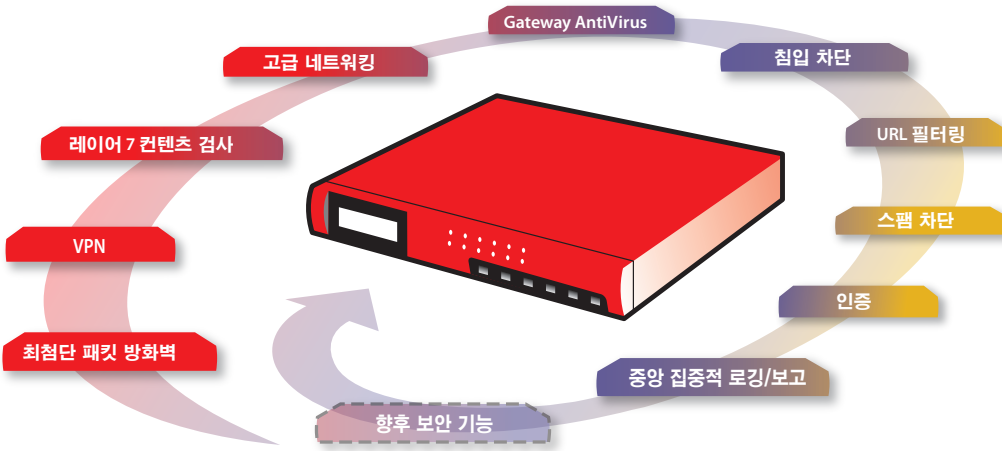
Gateway AV는 끊임없이 업데이트되는 시그니처를 사용하여 주요 프로토콜의 트래픽을 전부 스캔하면서 모든 유형의 맬웨어를 감지하고 차단합니다.

이 바이러스 백신 솔루션을 게이트웨이에서 실행하면 데스크탑 및 서버에서 실행되는 다른 바이러스 백신 제품 앞에 보호 장막을 하나 더 추가하는 셈이 되므로 보다 심층적인 방어가 가능합니다.

## Gateway AntiVirus

서비스를 추가하여 보호가 가장 필요한 부분, 바로 게이트웨이의 보호 수준을 대폭 높일 수 있습니다.

## 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 탐지된 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. Gateway AntiVirus 외의 서비스는 다음과 같습니다.

- WebBlocker** 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.
- Intrusion Prevention Service**는 15,000여 종의 시그니처를 바탕으로 프로토콜 표준에 맞지 않는 악성 위협을 담고 있는 공격을 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 보안 관리를 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.