

- **Umfassender Datei- und Datenschutz** – blockiert sämtlichen verdächtigen Datenverkehr
- **Blockierung von bekannten Angriffsquellen** und gleich gearteten Attacken
- **Sperrung von infizierten Anhängen** – verhindert die Ausführung bössartiger Dateien
- **Automatische Aktualisierung von Signaturen** – für dauerhaften Schutz
- **Verhinderung der IM- und P2P-Nutzung** – zum Schutz gegen Spyware
- **Block Sites List** – verhindert den Zugriff auf Spyware Sites

Blockierung von bössartigem Verkehr in Echtzeit

Der WatchGuard Gateway AntiVirus/Intrusion Prevention Service (Gateway AV/IPS) mit Anti-Spyware ist ein integrierter, signaturbasierter Sicherheitsdienst für die UTM-Appliances (Unified Threat Management) Firebox® X Core™ und Peak™. Gateway AV/IPS ist in den Zero-Day-Angriffsschutz der Firebox X integriert und bietet unerreichten Echtzeitschutz gegen Spyware, Viren, Trojaner, Pufferüberläufe, SQL-Injektionen, Instant Messaging sowie die P2P-Nutzung. Im Gegensatz zu anderen Lösungen scannt Gateway AV/IPS nur den Verkehr, der die Überprüfung durch die ILS-Architektur (Intelligent Layered Security) erfolgreich bestanden hat. So wird die Leistungsfähigkeit Ihrer Netzwerkressourcen nicht durch überflüssige Wiederholungsaktionen beeinträchtigt.

Gateway AV/IPS wird mit dem WatchGuard System Manager (WSM) verwaltet, der gleichen funktionsreichen und intuitiven Benutzeroberfläche, die für alle Firebox X Core und Peak UTM Appliances verwendet wird. WSM protokolliert, überwacht und berichtet über alle Aktivitäten. Über eine Echtzeitansicht der Antivirus- und Intrusion-Prevention-Aktivitäten behalten Sie stets die Übersicht und Kontrolle.

Umfassender Datei- und Datenschutz

Mithilfe von Signaturen wird ein bekannter bössartiger Code in wichtigen Geschäftsdaten und -dateien identifiziert. Gateway AV/IPS scannt den HTTP-Verkehr, blockiert Malware-Dateien am Netzwerk-Gateway und verhindert so, dass die Sicherheit von Desktops und Servern gefährdet wird. Die mehrschichtige Anti-Spyware-Funktion schützt Ihr Netzwerk vor Sites, die bekanntermaßen Ausgangspunkt für Spyware sind. Je nach Typ, Benutzer/Gruppe, Protokoll und Schweregrad können Sie das Netzwerk mit den Einstellungen „Allow“ (Zulassen), „Block“ (Blockieren) oder „Lock“ (Sperren) konfigurieren.

Blockierung von bekannten Angriffsquellen

Sobald eine IP-Adresse als potenzielle Angriffsquelle identifiziert wurde, werden zukünftige Attacken von dieser Adresse dynamisch und proaktiv blockiert, wodurch Ihr Netzwerk vor bössartigem Verkehr geschützt wird. Gateway AV/IPS bietet zudem konfigurierbare Whitelists, mit denen Sie Ausnahmen definieren können. So bleiben vertrauenswürdige Anwendungen bzw. Sites stets verfügbar und Sie können ungestört Ihrem Tagesgeschäft nachgehen.

Sperrung von infizierten Anhängen

Durch das Sperren verdächtiger Anhänge verhindert Gateway AV/IPS die Ausführung bössartiger Dateien auf dem Desktop. Dieser Schutz ist extrem robust und effektiv, da in den Scanvorgang eine Vielfalt komprimierter und codierter Dateitypen eingeschlossen werden, wie z. B. ZIP, RAR 2.0, TAR, GZIP, ARC und MS CAB.

Automatische Aktualisierung von Signaturen

Signaturen werden ohne Unterbrechung aktualisiert, damit Ihr Netzwerk auch jederzeit rundum geschützt ist. Mit Tausenden von Virussignaturen, darunter WildList- und „Zoo“-Viren, bietet unsere Datenbank den bestmöglichen Schutz für Ihr Netzwerk. Unsere auf die aktivsten Bedrohungen vollständig geprüfte Datenbank garantiert, dass Sie höchste Genauigkeit mit nur wenigen „false positives“ (E-Mails, die zu Unrecht geblockt wurden) erhalten.

Verhinderung der IM- und P2P-Nutzung

Gateway AV/IPS ermöglicht die Aktivierung/Deaktivierung von so beliebten Anwendungen wie Instant Messaging (IM) und Peer-to-Peer (P2P), zwei der am häufigsten verwendeten Träger zur Verbreitung von Spyware.

Liste blockierter Sites

Die Liste mit den blockierten Sites wird fortlaufend aktualisiert und garantiert so dauerhaften Netzwerkschutz. Die mehrschichtige Anti-Spyware-Funktion blockiert bekannte Spyware-Sites, so genannte „Driveby“-Downloads, durch die Spyware beim Surfen im Internet ins Netzwerk eingeschleust wird, sowie Spyware, die versucht, mit ihrer Host-Site Kontakt aufzunehmen. Alle Aktionen werden protokolliert und in Berichtsform bereitgestellt.

Mehrschichtiger Spyware-Schutz blockiert bössartigen Verkehr wie:

- | | | |
|---------------------------|---------------------|-------------------|
| ✓ Spyware | ✓ Viren | ✓ SQL-Injektionen |
| ✓ Trojaner | ✓ Pufferüberläufe | ✓ Würmer |
| ✓ Blended Threats | ✓ DoS/DDoS-Attacken | ✓ Bots |
| ✓ Richtlinienverletzungen | ✓ Internetattacken | |

Umfassendes Unified-Threat-Management (UTM)

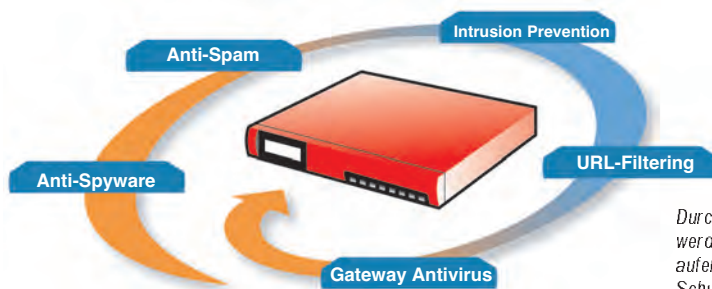
Netzwerkattacken kosten Unternehmen enorm viel Geld und Zeit. Hacker lancieren täglich immer ausgeklügeltere Attacken und kein Protokoll ist gegen solche Bedrohungen absolut immun. Angesichts der vielen Netzwerkbedrohungen nutzen immer mehr Unternehmen jeder Größenordnung die mehrschichtigen UTM-Lösungen zum Schutz Ihrer Systeme. Die Firebox X Familie der Security Appliances von WatchGuard bietet umfassendes Unified Threat Management (von Hardware- bis hin zu Softwarediensten) für voll integrierten, vielschichtigen Netzwerkschutz vor Spyware, Spam, Viren, Würmern, Trojanern, Internetattacken und anderen Blended Threats.

Neben Gateway AV/IPS gehören zu unseren integrierten Sicherheitsdiensten u. a.:

- **spamBlocker:** Der beste Dienst der Branche für die Unterscheidung zwischen legitimer Kommunikation und Spam-Attacken. Bis zu 97 % aller unerwünschten E-Mails werden blockiert.

- **WebBlocker:** Durch Blockierung von bösartigen Webinhalten und die Verwaltung des Surfverhaltens Ihrer Benutzer steigern Sie die Produktivität und verringern Sie das Sicherheitsrisiko.

Mit dem WatchGuard Security Manager lassen sich die Dienste kinderleicht aktivieren und verwalten. Da sie nahtlos in die Intelligent Layered Security der Firebox X integriert sind, bieten sie leistungsstarke Sicherheit bei niedrigen Betriebskosten und hoher Produktivität.



Durch die Kommunikation zwischen den Sicherheitsebenen werden die Aufgaben der einzelnen Funktionen optimal aufeinander abgestimmt. Dadurch erhalten Sie genau den Schutz, den Sie brauchen, und das ohne jegliche Leistungseinbußen.

Gateway AV/IPS für die Firebox® X Core™

Firebox X550e	
Gateway AV/IPS 1-Jahres-Abonnement	WG017317
Firebox X500*	
Gateway AV/IPS 1-Jahres-Abonnement	WG017238
Firebox X750e	
Gateway AV/IPS 1-Jahres-Abonnement	WG017318
Firebox X700*	
Gateway AV/IPS 1-Jahres-Abonnement	WG017241
Firebox X1250e	
Gateway AV/IPS 1-Jahres-Abonnement	WG017319
Firebox X1000*	
Gateway AV/IPS 1-Jahres-Abonnement	WG017244
Firebox X2500*	
Gateway AV/IPS 1-Jahres-Abonnement	WG017247

*Erfordert Fireware® Pro Appliance-Software

Systemanforderungen

- WatchGuard Firebox X Peak oder Core mit Fireware® Appliance-Software 8.2 oder eine neuere Version
- Microsoft® Windows® 2000, Windows NT oder XP für WatchGuard System Manager 8.2 oder eine neuere Version
- SMTP-Server
- Aktives LiveSecurity® Service Abonnement zum Herunterladen der neuesten Funktionen

Gateway AV/IPS für die Firebox® X Peak™

Firebox X5500e	
Gateway AV/IPS 1-Jahres-Abonnement	WG017320
Firebox X5000	
Gateway AV/IPS 1-Jahres-Abonnement	WG017250
Firebox X6500e	
Gateway AV/IPS 1-Jahres-Abonnement	WG017321
Firebox X6000	
Gateway AV/IPS 1-Jahres-Abonnement	WG017252
Firebox X8500e	
Gateway AV/IPS 1-Jahres-Abonnement	WG017322
Firebox X8000	
Gateway AV/IPS 1-Jahres-Abonnement	WG017254
Firebox X8500e-F	
Gateway AV/IPS 1-Jahres-Abonnement	WG017323

KOSTENLOSE 30-Tage-Demos

Beim Kauf einer Firebox Core oder Peak erhalten Sie eine kostenlose 30-Tage-Demo für **Gateway AntiVirus/Intrusion Prevention Service, spamBlocker** und **WebBlocker**. Weitere Informationen erhalten Sie bei Ihrem Händler.

Weitere Informationen zu spamBlocker erhalten Sie unter www.watchguard.com/services

ADRESSE: Watchguard Technologies Schellerdamm 16 21079 Hamburg Germany · WEB: www.watchguard.com · E-MAIL: germany@watchguard.com · GERMANY SALES: +49 40 689876 10 · FAX: +49 40 689876 76

Für die Richtigkeit/Aktualität der hierin enthaltenen Informationen (die jederzeit geändert werden können) wird weder eine ausdrückliche noch eine konkludente Garantie übernommen. Zukünftige Produkte oder Funktionen werden zum gegebenen Zeitpunkt zur Verfügung gestellt. ©2006 WatchGuard Technologies, Inc. Alle Rechte vorbehalten. WatchGuard, das WatchGuard Logo, Firebox, Fireware, LiveSecurity, Core, Peak und Stronger Security, Simply Done sind in den USA und/oder anderen Ländern entweder Markenzeichen oder eingetragene Markenzeichen von WatchGuard Technologies, Inc. Alle anderen Markenzeichen oder Markennamen sind Eigentum ihrer jeweiligen Besitzer. Teilnr. WGCE66238_0506