



Die umfassende Unified-Threat-Management-Lösung

Firebox® X Core™ UTM-Lösungen (Unified Threat Management) bieten die umfassendste Sicherheit in ihrer Klasse mit Funktionen wie Stateful Packet Firewall, VPN, echtem Zero-Day-Angriffsschutz, Anti-Spyware, Anti-Spam, Antivirus, Intrusion Prevention und URL-Filtering über eine einzige Appliance. Damit entfällt der Zeit- und Kostenmehraufwand für Mehrfachlösungen und es wird ein wesentlich besserer Schutz vor „Blended Threats“ (kombinierten Angriffen) geboten.

Unerreichte mehrschichtige Sicherheit

Herzstück der Firebox X Core ist die ILS-Architektur (Intelligent Layered Security), deren Schichten zusammenwirken und damit umfassenden Schutz bieten. Durch die Kommunikation zwischen den verschiedenen Ebenen werden die Aufgaben der Sicherheitsfunktionen optimal aufeinander abgestimmt. Dadurch erhalten Sie den Schutz, den Sie brauchen und das ohne jegliche Leistungseinbußen.

Echte Zero-Day-Protection

Im Gegensatz zu anderen Produkten, die von Signaturen abhängig sind, bietet die Firebox X Core wichtige integrierte Sicherheitsfunktionen, die gegen Attackenklassen und ihre Varianten schützen – und alles ohne Signaturen. Während andere Netzwerke so lange gefährdet sind, bis eine entsprechende Signatur entwickelt ist, wird Ihr Netzwerk von dem Moment an geschützt, wo Sie Ihre Firebox einschalten.

Unified Management ohne versteckte Kosten

WatchGuard® System Manager (WSM) ist die intuitive Benutzeroberfläche, mit der alle Funktionen der Firebox X Core UTM-Lösungen sowie der Firebox X Peak® und Edge Appliances verwaltet werden. WSM bietet eine umfassende Protokollierung, VPN-Erstellung per Drag&Drop sowie Echtzeitüberwachung direkt aus der Box – und zwar ohne versteckte Kosten oder zusätzliche Produktkäufe. Und da Sie zur Verwaltung aller Aspekte Ihrer Sicherheitslösung lediglich eine Benutzeroberfläche erlernen müssen, sparen Sie dazu noch Zeit und Geld.

Beratung und Support durch Experten

Unser LiveSecurity® Service ist das umfassendste Support- und Wartungspaket der Branche. Ein globales Team aus Sicherheitsexperten bietet Ihnen jegliche Unterstützung für eine bessere Verwaltung Ihrer Netzwerksicherheit. Zum Leistungsumfang des LiveSecurity® Service gehören Softwareupdates, technischer Support durch unsere Experten, aktuelle Sicherheitswarnungen, vorzeitiger Hardwareaustausch sowie Selbsthilfe-Ressourcen wie Schulungen, Zertifizierungen und Lernprogramme. Unternehmen mit geschäftskritischen Internetanforderungen können zudem unseren Premium Service in Anspruch nehmen.

Integrierte Sicherheitsfunktionen für umfassenderen Schutz

Alle WatchGuard Sicherheitsdienste lassen sich mit dem Zero-Day-Angriffsschutz der Firebox X Peak integrieren und bieten so

eine unschlagbare Kombination – und das ohne zusätzliche Hardware. Außerdem gelten alle Abonnements pro Appliance und nicht pro Benutzer, so dass die Kosten nicht eskalieren. Darüber hinaus werden alle Sicherheitsdienste fortlaufend aktualisiert, wodurch Sie jederzeit Rundum-Schutz genießen. Die zentrale Verwaltung erfolgt über WSM mit seinen Echtzeitansichten aller Dienstaktivitäten.

■ *spamBlocker*

Holen Sie sich den besten Anti-Spam-Dienst der Branche für die Blockierung von bis zu 97 % aller unerwünschten E-Mails.

■ *Gateway AV/IPS*

Vertrauen Sie auf robusten, signatur-basierten Schutz am Gateway gegen bekannte Viren, Spyware-Programme, Trojaner und Webattacks.

■ *WebBlocker*

Steigern Sie Ihre Produktivität und verringern Sie das Sicherheitsrisiko durch das Blockieren von böswilligen Webinhalten und die Verwaltung des Surfverhaltens Ihrer Nutzer.

Schutz Ihrer Investitionen

In Anbetracht der Kosten, die bei mehreren Sicherheitslösungen für Implementierung, Verwaltung und spätere Upgrades anfallen, um eine breite Palette an Sicherheitsbedürfnissen abzudecken, wird klar, warum unsere Firebox X Core UTM-Lösungen einen eindeutigen Mehrwert bieten. Dank des voll integrierten, mehrschichtigen Schutzes einer einzelnen Appliance sparen Sie in jeder Hinsicht Geld, vom Erstkauf bis hin zu den Supportverträgen.

Indem Sie bei wachsenden Bedürfnissen einfach neue Funktionen hinzufügen, sind Sie mit Ihrem Unternehmen sicherheitstechnisch immer auf dem neuesten Stand. Wenn Sie einen höheren Durchsatz und mehr Kapazität benötigen, führen Sie ein Upgrade auf ein höherwertiges Modell durch. Dazu müssen Sie nur einen einfachen Lizenzschlüssel herunterladen. Wenn Sie anspruchsvolle Netzwerke betreiben, kommt für Sie vielleicht ein Upgrade auf die moderne Fireware® Pro Appliance-Software in Frage, die zusätzliche Netzwerkfunktionen wie Hochverfügbarkeit, Verkehrsverwaltung sowie dynamisches Routing bietet. Und all das, ohne dass Sie neue Hardware kaufen müssen. Keine anderen Sicherheitsprodukte auf dem Markt schützen Ihre Investitionen auf so vielfältige Weise.

- **Umfassender Schutz:** Macht Ihr Netzwerk immun gegen Bedrohungen.
- **Zero-Day-Angriffsschutz:** Stoppt neue und unbekannte Bedrohungen, sogar noch bevor entsprechende Signaturen verfügbar sind.
- **Rationelles Netzwerksicherheitsmanagement:** Bietet Zeitersparnis.
- **Kontinuierlich aktualisierte Antivirus-, Anti-Spam- und Webfiltering-Dienste:** Bieten dauerhaften Schutz.
- **Integrierte, upgradefähige Funktionen:** Bieten ein besseres Preis-/Leistungsverhältnis.
- **Globales Team aus Sicherheitsexperten:** Bietet Unterstützung bei Bedarf.

Blockieren von Webattacken

Das Internet ist ein überaus wertvolles Geschäftstool, kann sich aber auch als ernsthafte Bedrohung für Ihr Netzwerk erweisen. Durch unbeaufsichtigtes Surfverhalten können absichtlich oder unabsichtlich Schwachstellen entstehen, die von Bots und Spyware ausgenutzt werden und Ihre wichtigen Geschäftsdaten gefährden bzw. zu einem enormen Zeit- und Kostenaufwand im Helpdesk-Bereich führen. Anfällige Netzwerke sind leichte Beute für DNS-Cache-Poisoning (Domain Name Server), Pufferüberläufe und DoS-Attacken (Denial of Service).

Diese Tools benötigen Sie:

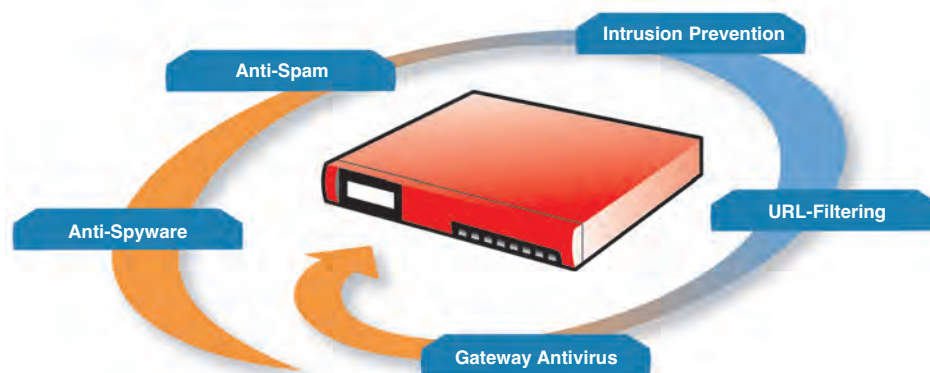
- Eine **Firebox X Core** für echten Zero-Day-Angriffsschutz mit Gigabit-Performance
- Gültige Abonnements für **WebBlocker** zur Überwachung von nicht autorisiertem Surfen im Web sowie **Gateway AV/IPS** zur Echtzeit-Blockierung von verdächtigem Internetverkehr und heruntergeladenen Dateien

Die verschiedenen Sicherheitsfunktionen sind:

- **Gateway Antivirus:** Prüft den Webverkehr auf Viren und andere Malware.
- **Webserver-Cloaking:** Verhindert, dass Hacker Systeminformationen für Angriffe ausnutzen.

- **URL-Filtering:** Steuert das Surfverhalten und sorgt so für mehr Produktivität, Netzwerkbandbreite, ein geringeres Sicherheitsrisiko und weniger Haftungsansprüche, die aus der Verwendung unerwünschter Inhalte am Arbeitsplatz entstehen.
- **Echter Zero-Day-Angriffsschutz:** Schützt Ihr Netzwerk vor vielen neuen und unbekanntem Bedrohungen, noch bevor Sicherheitslücken entdeckt und entsprechende Attacken entwickelt und lanciert werden.
- **Mehrschichtige Spyware-Funktionen:** Blockieren den Zugang zu bekannten Spyware-Sites, so genannten „Driveby“-Downloads, durch die Spyware beim Surfen im Internet ins Netzwerk eingeschleust wird, sowie Spyware, die versucht, mit Ihrer Host-Site Kontakt aufzunehmen.
- **HTTP-Proxies:** Schützen gegen Netzwerkbedrohungen, DoS-Attacken sowie DNS-Cache-Poisoning.
- **Robuste IPS-Funktionen:** Steuern die Verwendung von Instant Messaging (IM) und Peer-to-Peer (P2P) Anwendungen, zwei der am häufigsten verwendeten Kanäle für die Verbreitung von Spyware.
- **Integrierte Protokollierung, Berichterstattung und Alarmer:** Bieten einen genauen Einblick in die Netzwerkaktivitäten und ermöglichen sofortige Präventiv- oder Abhilfemaßnahmen.

Firebox X: Integrierte Sicherheit



Maßnahmen gegen E-Mail-Bedrohungen

Da Ihr Geschäft vom E-Mail-Verkehr abhängig ist, muss die Kommunikation reibungslos ablaufen, aber ohne dabei die Netzwerksicherheit zu gefährden. Allerdings ist und bleibt E-Mail das am häufigsten verwendete Kommunikationsinstrument für die Verbreitung bössartiger Codes im Netzwerk. Wenn man dann noch die zusätzliche Belastung durch Massen-Spam bedenkt, kann die E-Mail-Umgebung zu einem Ihrer größten Probleme werden.

Diese Tools benötigen Sie:

- Eine **Firebox X Core** für echten Zero-Day-Angriffsschutz
- Ein **Gateway AV/IPS** Abonnement für das Scannen von E-Mail-Verkehr und die Blockierung bekannter Würmer, Trojaner und anderer Malware
- Ein aktives **spamBlocker**-Abonnement, den besten Dienst der Branche bei der Unterscheidung zwischen legitimer E-Mail-Kommunikation und Spam-Nachrichten in Echtzeit

Die verschiedenen Sicherheitsfunktionen sind:

- **spamBlocker:** Nutzt die Spam-Erkennung in Echtzeit, damit Sie jederzeitigen Rundum-Schutz genießen; blockiert bis zu 97 % des unerwünschten E-Mail-Verkehrs, und zwar unabhängig von Inhalt, Sprache oder Format.
- **Integrierter Zero-Day-Angriffsschutz:** Für die proaktive Blockierung von Dateitypen, die häufig Malware enthalten
- **SMTP-Server Cloaking:** Verhindert, dass Hacker Systeminformationen für Angriffe ausnutzen.
- **Integrierter Gateway AV:** Bietet umfassenden Schutz vor Dateien und ihren Anhängen für eine effiziente Blockierung von Viren, Würmern und anderer Malware, bevor diese ins Netzwerk eindringen und Ihre Desktop-Sicherheitsanwendungen deaktivieren können.
- **AV-Scanning abgehender E-Mail-Nachrichten:** Schützt Ihr Unternehmen davor, selbst Viren, Würmer und Trojaner an Partner, Kunden und andere Empfänger außerhalb des Netzwerks zu verbreiten.

Technische Daten

	Firebox® X550e WG50550	Firebox® X750e WG50750	Firebox® X1250e WG51250
Firewall-Durchsatz*	125 Mbps	200 Mbps	300+ Mbps
VPN-Durchsatz*	20 Mbps	50 Mbps	100 Mbps
Gateway AV/IPS	Optional	Optional	Optional
URL-Filtering	Optional	Optional	Optional
Spam-Blocking	Optional	Optional	Optional
Serielle Ports	1	1	1
Schnittstellen 10/100	4	8	0
Schnittstellen 10/100/1000		0	0 8
Enthalten Sicherheitszonen	4	8	8
Gleichzeitige Sitzungen	25.000	75.000	200.000
Unterstützte Knoten (LAN IPs)	Unbegrenzt	Unbegrenzt	Unbegrenzt
VPN-Tunnel für Niederlassungen (inkl./max.)	1/10	100/100	400/400
VPN-Tunnel für mobile Benutzer (inkl./max.)	5/10	50/100	400/400
Obergrenze für die Lokale Authentifizierungs-DB	250	1.000	5.000
Modell-Upgrades	Nein	Ja	Nein
Fireware® Pro Appliance-Software	Optional	Optional	Optional

*Durchsatzraten variieren je nach Umgebung und Konfiguration

Funktionen
Sicherheitsfunktionen

- Stateful Packet Firewall
- Deep Application Inspection Firewall
- Anwendungs-Proxies - HTTP, SMTP, FTP, DNS, TCP
- DoS- und DDoS-Schutz
- Progressiver DDoS-Schutz
- Erkennung von Protokollanomalien
- Verhaltensanalyse
- Pattern Matching
- Fragmented Packet Reassembly-Schutz
- Malformed Packet-Schutz
- Liste statisch blockierter Sites
- Liste dynamisch blockierter Sites
- Zeitbasierte Regeln

VPN

- Verschlüsselung (DES, 3DES, AES 128-, 192-, 256-bit)
- IPSec
 - SHA-1, MD5
 - IKE - Preshared Key, Firebox Zertifikat
- PPTP-Server
- PPTP-Passthrough
- Dead Peer Detection (RFC 3706)
- Hardware-basierte Verschlüsselung

Benutzerauthentifizierung

- XAUTH
 - RADIUS®
 - LDAP
 - Windows® Active Directory
- RSA SecurID®
- Web-basiert
- Lokale Authentifizierung

IP-Adresszuweisung

- Porttrennung
- Statisch
- PPPoE-Client
- DHCP-Server
- DHCP-Client
- DHCP-Relay
- Dynamischer DNS-Client

Redundanzfunktionen

- Hochverfügbarkeit*
 - HA Aktiv/Passiv
 - Konfigurationssynchronisierung
 - Sitzungssynchronisierung
 - VPN-Tunnel-Synchronisierung
- Multi-WAN Failover
 - WAN Failover Ports - 4
 - WAN Failover Modi (Aktiv/Passiv)

Lastverteilung

- Round Robin-Lastverteilung
- Bis zu 4 Ports

Verkehrsverwaltung und -priorisierung

- Maximale Bandbreite
- Maximale Verbindungen/Sekunde
- Verkehrspriorisierung/QoS*
 - 2 Prioritätsebenen

Routing

- Statisches Routing
- RIPv1, v2
- BGP4*
- OSPF*

Betriebsmodi

- Transparenter/Drop-In-Modus (Layer 2)
- Routed-Modus (Layer 3)

Adressübersetzung

- Statische NAT (Portübersetzung)
- Dynamische NAT
- Eins-zu-Eins-NAT
- IPSec NAT Traversal
- Richtlinien-basierte NAT

Protokollierung/Berichterstattung

- Protokollzusammenfassung für mehrere Appliances
- WebTrends®-kompatible Berichte (WELF)
- HTML-Berichte
- XML-Protokollformat
- Verschlüsselter Protokollkanal
- Syslog
- SNMP

Alarme/Benachrichtigungen

- SNMP
- E-mail
- Management System Alert
- Benutzerdefinierter Programmalarm
- Offline-Konfiguration mit Benutzeroberfläche

Management-Software

- WatchGuard System Manager (WSM)

Zertifizierungen

- EAL-4 - Anstehend

Support und Wartung

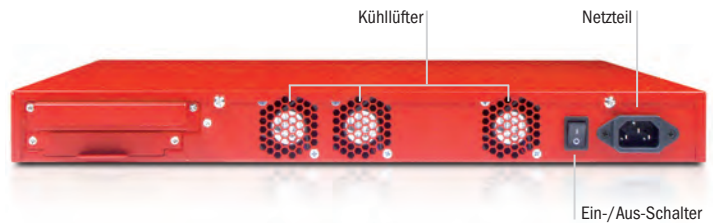
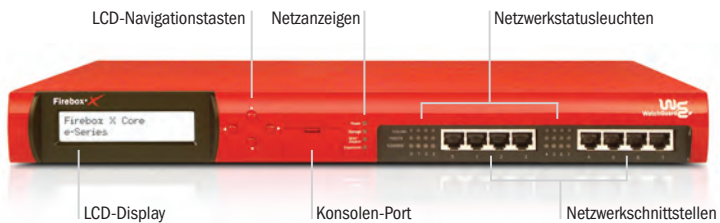
- 1 Jahr Hardware-Garantie
- 90 Tage LiveSecurity® Service Abonnement

Abmessungen/Leistungswerte

Abmessungen Appliance	4,5 x 42,6 x 36,2 cm
Abmessungen Verpackung	18,4 x 54,6 x 48,3 cm
Gewicht Appliance	4,39 kg
Gesamtgewicht	6,21 Kg
WEEE-Gewicht	4,81 Kg
Wechselspannung	100-240 VAC Autoumschaltung
Stromverbrauch	USA: 60 Watt Restliche Welt: 52 Kal/min oder 205 BTU/min
Rack-fähig	Ja

Umgebung

Betriebstemperatur	0 - 45° C
Ruhetemperatur	-40 - 70° C
Betriebsfeuchte	10 - 85%
Ruhefeuchte	10 - 95% nicht kondensierend bei 55° C
Nicht periodische Schwingungen	7 - 28 Hz 0,001 bis 0,01 G2 pro Hz
(Ruhezustand) Akustisches Rauschen	54 dB bei 20 - 25° C
Mechanischer Schock (Betrieb)	20 G mit 11 Ms Dauer 1/2 Sinuswelle
WEEE/RoHS-konform	Ja


Sind Sie bereit für ein Upgrade auf die Fireware® Pro Advanced Appliance Software?

Wenn Ihre Netzwerkbedürfnisse wachsen, können Sie Ihre Firebox X Core von Fireware auf Fireware Pro aufrüsten, die moderne Appliance-Software von WatchGuard für anspruchsvolle Netzwerke. Zu ihren Funktionen gehören:

- **Verkehrsverwaltung und -priorisierung:** Damit geschäftskritische Anwendungen auch die jeweils erforderliche Bandbreite bekommen.
- **Dynamisches Routing (BGP, OSPF):** Ermöglicht eine optimale Netzwerkflexibilität, Redundanz und Effizienz durch dynamische Aktualisierung der Routing-Tabellen.
- **Hochverfügbarkeit (Aktiv/Passiv):** Bietet Hardwareredundanz für eine Standby-Appliance.

Genauere Informationen erhalten Sie bei Ihrem Händler.

KOSTENLOSE
30-Tage-Demos

Beim Kauf einer Firebox Core erhalten Sie kostenlose 30-Tage-Demos für **Gateway AV/PS**, **spamBlocker** und **WebBlocker**. Weitere Informationen erhalten Sie bei Ihrem Händler.

Weitere Informationen zur Firebox X Core erhalten Sie unter www.watchguard.com/appliances.

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. WGCE66360_0506