WatchGuard®
PRODUKTDATENBLATT

GepaNet
http://www.gepanet.com

Firebox® X Peak™
e-Series

- **Umfassendes Unified Threat Management:** schützt das Netzwerk vor Angriffen
- **Echter Zero Day Angriffsschutz:** schützt proaktiv gegen neue Bedrohungen
- **Neu! Integriertes SSL VPN**
- **Acht 10/100/1000 Gigabit Ethernet Ports:** sorgen für hochschnelle Verbindungen
- **Moderne Netzwerkfunktionen** bieten Ressourcenverwaltung, Traffic Shaping und damit längere Betriebszeiten
- **Einfache Konfiguration und Verwaltung** aller Appliances und Funktionen
- **Integrierte Sicherheits-abonnements** für umfassenden Schutz

Umweltfreundliche Technologie

10/100/1000 Gigabit-Sicherheit für anspruchsvolle Netzwerke

Mit einem Firewall-Durchsatz von mehreren Gigabit pro Sekunde bietet die Firebox® X Peak™, die absolut hochleistungsfähige Reihe der UTM- (Unified-Threat-Management) Appliances von WatchGuard®, Zero-Day-Angriffsschutz direkt aus der Box. Sie integriert leistungsstarke Sicherheits- mit modernen Netzwerkfunktionen und bietet damit eine beeindruckende Komplettlösung, die selbst den Anforderungen der anspruchsvollsten Netzwerke genügt.

Umfassendes Unified Threat Management

Die Firebox Peak integriert Funktionen wie Anwendungs-Proxies, Stateful Packet Firewall und vollständiges VPN mit optionalen Sicherheitsabonnements für eine mehrschichtige Verteidigung. Zusammen mit Funktionen wie Anti-Spyware, Intrusion Prevention, Antivirus, Anti-Spam mit Viruserkennung und URL-Filtering bietet sie damit nicht nur die umfassendste Sicherheit in ihrer Klasse, sondern im Vergleich zu Mehrfachlösungen auch noch eine eindeutige Zeit- und Kostenersparnis – und das alles in einer einzigen Appliance.

Echter Zero Day Angriffsschutz

Die Sicherheitstechnologie der Firebox X Peak schützt das Netzwerk Ihrer Kunden proaktiv gegen Software-Sicherheitslücken, die neue Formen von Attacken ermöglichen. Durch die auf modernsten Proxy-Technologien basierende Deep Application Inspection, die neue Bedrohungen identifiziert und blockiert, bietet die Firebox X Core automatischen Schutz vor Spyware, Trojanern, Würmern, DoS, DDoS, DNS-Poisoning, Pufferüberläufen und anderen Attacken.

Hochleistungsfähigkeit

Mit einem Durchsatz von mehreren Gigabit für die Firewall bzw. 600 Mbps für VPN bietet die Firebox X Peak die höchste Performance aller UTM-Lösungen in unserem Produktangebot. Alle Modelle der Reihe verfügen über acht 10/100/1000 Gigabit Ethernet Ports zur Unterstützung schneller LAN Backbone-Infrastrukturen sowie von WAN-Gigabit-Verbindungen. Für eine optimale Nutzung kann jeder der acht Ports individuell als Intern, Extern oder Optional konfiguriert werden.

Moderne Netzwerkfunktionen

Die modernen Netzwerkfunktionen der Firebox X Peak ermöglichen die intelligente Verwaltung von Ressourcen, die Optimierung des Netzwerkverkehrs sowie eine Verringerung der Betriebsausfallzeiten durch stabile Konnektivität.

- ***VLAN-Unterstützung*** senkt die Hardwareanforderungen und bietet umfassende Interoperabilität
- ***Multi-WAN Load-Balancing und Hochverfügbarkeit (aktiv/passiv), WAN- und VPN-Failover*** steigern Performance, Redundanz und Zuverlässigkeit
- ***Dynamisches Routing und Traffic Shaping*** maximieren Netzwerkflexibilität und Effizienz
- ***Policy Based Routing*** trägt durch Zuweisung einer Schnittstelle für abgehenden Verkehr je Dienst zur Steigerung der Netzwerkbandbreite und Senkung der Kosten bei
- ***Server Load-Balancing*** vereinfacht den Schutz öffentlich zugänglicher e-commerce „Server Farms“

Intuitive, zentrale Verwaltung

Der WatchGuard® System Manager (WSM) ermöglicht eine intuitive, zentrale und vor allem benutzerfreundliche Verwaltung aller Firebox X Lösungen, einschließlich Konfigurationsänderungen, der Überwachung von Daten in Echtzeit sowie der Erstellung historischer Berichte – und zwar unabhängig vom Umfang des Gerätenetzwerks und mit signifikanten Zeit- und Kosteneinsparungen.

Sichere Remote-Konnektivität

Der Schutz von Telearbeitern gestaltet sich mit der Firebox X Core viel einfacher, und zwar unabhängig vom Standort. Mit der größten Vielfalt an Funktionen für den Remote-Zugriff in ihrer Klasse ermöglicht sie die sichere Anbindung an das Firmennetzwerk via:

- IPSec VPN, SSL VPN, PPTP

Mit Single-Sign-On für eine einfachere Authentifizierung.

Integrierte Sicherheitsfunktionen für umfassenderen Schutz

Stärken Sie Ihren Netzwerkschutz für kritische Bereiche mit den Sicherheitsabonnements für Ihre Firebox X. Die zentrale Verwaltung per WSM sorgt dazu für einen stets aktuellen Schutz.

- ***WebBlocker***
  Steigern Sie die Produktivität und verringern Sie das Sicherheitsrisiko durch Blockieren des Zugriffs auf bösartige oder unerwünschte Webinhalte per HTTP und HTTPS
- ***spamBlocker mit Viruserkennung***
  Blockiert fast 100 % aller Spam-Mails mit infizierten Anhängen
- ***Gateway AV/IPS mit Anti-Spyware***
  Vertrauen Sie auf signatur-basierten Schutz gegen bekannte Viren, Spyware-Programme, Trojaner und Webattacken

Vollständiges Modell-Upgrade und Skalierbarkeit

Wenn sich die Netzwerkanforderungen ändern, kann auf einfachste Weise mehr Kapazität oder weitere Sicherheitsabonnements hinzugefügt werden. Dazu muss lediglich ein praktischer Softwarelizenzschlüssel eingespielt werden.

Unser Engagement für die Umwelt

WatchGuard verpflichtet sich zur Herstellung energiesparender Produkte, die in wiederverwendbaren Verpackungsmaterialien vertrieben werden. Wir erkennen die EU-Direktive über gefährliche Substanzen uneingeschränkt an und haben die Nachhaltigkeit zu einem festen Bestandteil unserer weltweit geltenden strategischen Unternehmensgrundsätze gemacht.

Blockieren von Webattacken

Das Internet ist ein überaus wertvolles Werkzeug für Geschäftsabläufe, 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 Service), Pufferüberläufe und DoS-Attacken (Denial of Service).

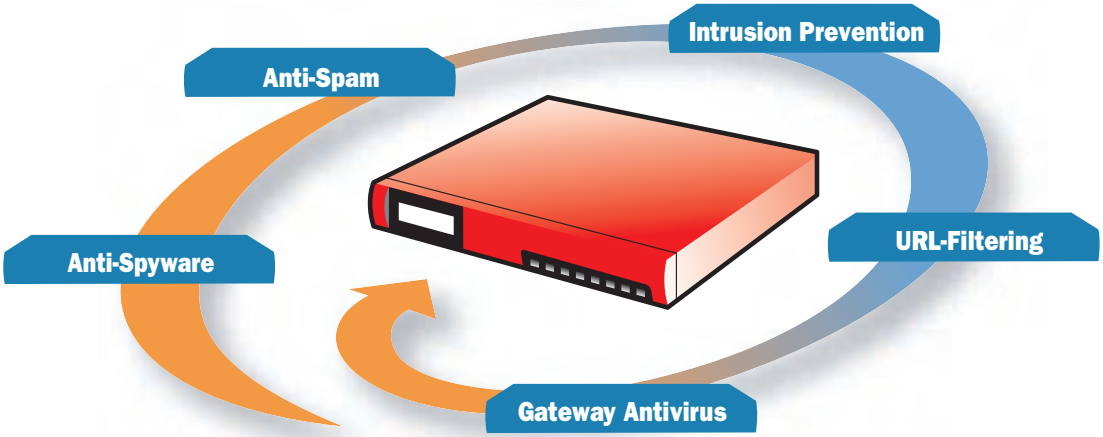
Diese Tools benötigen Sie:

- Eine **Firebox X Peak** für echten Zero Day Angriffsschutz mit Multi--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:

- **Echter Zero Day Angriffsschutz:** schützt Ihr Netzwerk mit leistungsstarken, integrierten Anwendungs-Proxy-Technologien vor vielen neuen und unbekannten Bedrohungen, die durch Sicherheitslücken in verschiedenen Softwareanwendungen ermöglicht werden
- **Mehrschichtiges Spyware-System:** blockiert 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
- **Gateway Antivirus/IPS mit Anti-Spyware:** prüft den Webverkehr auf Viren, Trojaner, Bots und andere Malware und bietet so umfassenden Schutz gegen bekannte Bedrohungen
- **Webserver-Cloaking:** verhindert, dass Hacker Systeminformationen für Angriffe ausnutzen
- **WebBlocker:** ermöglicht Ihnen, das Surfverhalten Ihrer Angestellten einzugrenzen. Sie schützen damit nicht nur Ihr Netzwerk vor Angriffen, sondern steigern auch noch die Produktivität und verringern das Risiko von Haftungsansprüchen
- **URL-Filtering für HTTPS:** blockiert Schlupflöcher für unerlaubtes Websurfing
- **Intelligente mehrschichtige Sicherheitsarchitektur und DNS-Proxy:** schützen gegen Netzwerkbedrohungen, DoS-Attacken sowie DNS-Cache-Poisoning
- **Integrierte Protokollierung, Berichterstattung und Alarme:** bieten einen genauen Einblick in die Netzwerkaktivitäten und ermöglichen sofortige Präventiv- oder Abhilfemaßnahmen

Die integrierten Sicherheitsabonnements der Firebox X Peak schützen besonders empfindliche Bereiche vor Attacken.



Sicherheit für Niederlassungen und mobile Benutzer

Immer mehr Mitarbeiter sind heute als Telearbeiter oder an entfernten Standorten tätig. Damit wächst natürlich auch der Bedarf an zuverlässigen und sicheren Remote-Verbindungen zu Ressourcen und Daten. Dabei sind Aspekte wie zentrale Verwaltung und Berichterstellung, Einrichtung einheitlicher Sicherheitsrichtlinien, Interoperabilität mit bestehenden Netzwerkressourcen und -anwendungen sowie Remote-Konnektivität in Betracht zu ziehen. Und natürlich müssen diese Remote-Geräte zuerst Ihre Sicherheitsrichtlinien erfüllen, bevor Sie Zugriff auf Ihr Netzwerk gewähren.

Diese Tools benötigen Sie:

- **Firebox X Peak** für Unified Threat Management mit Multi-Gigabit-Performance
- **Firebox X Edge** für den bestmöglichen Schutz des Netzwerkrands (verkabelte oder kabellose Konfiguration) bei Remote-Niederlassungen und Zweigstellen sowie den **WatchGuard System Manager** für die zentrale Verwaltung aller Sicherheitsfunktionen

Die verschiedenen Sicherheitsfunktionen sind:

- **Zentrale Richtlinien- und VPN-Verwaltung:** ermöglicht die Durchsetzung einheitlicher Sicherheitsrichtlinien bei allen Standorten und Benutzern
- **Sicherer Remote-Zugriff auf Netzwerkressourcen** für Niederlassungen und mobile Benutzer über verschlüsselte VPN-Tunnel – für mehr Produktivität und Flexibilität auch außerhalb der Firmenzentrale
- **Leistungsstarkes Unified Threat Management** für Remote-Niederlassungen und Telearbeiter: Die Benutzer und das erweiterte Netzwerk sind vor Spyware, Viren, DoS-Attacken und anderen dynamischen Bedrohungen geschützt
- **Einfache VPN-Konfiguration für Niederlassungen per Drag&Drop:** durch drei einfache Konfigurationsschritte ist Ihre Niederlassung sicher ins Netzwerk eingebunden – und das bedeutet äußerst niedrige Betriebskosten
- **Multi-Gigabit-Performance:** bietet Zuverlässigkeit, Redundanz und Flexibilität für die verschiedensten Typen der Netzwerk-Konnektivität und Zukunftssicherheit bei wachsenden Bedürfnissen

Technische Daten	**Firebox® X5500e** WG55500 X5500e UTM Bundle WG55503	**Firebox® X6500e** WG56500 X6500e UTM Bundle WG56503	**Firebox® X8500e** WG58500 X8500e UTM Bundle WG58503	**Firebox® X8500e-F** WG58510 X8500e-F UTM Bundle WG58513
Firewall-Durchsatz*	2.0+ Gbps	2.3 Gbps	2.3 Gbps	2.3 Gbps
VPN-Durchsatz*	400 Mbps	600 Mbps	600 Mbps	600 Mbps
AV-Durchsatz*	140 Mbps	170 Mbps	200 Mbps	200 Mbps
Gateway AV/IPS mit Anti-Spyware	Optional	Optional	Optional	Optional
URL Filtering für HTTP und HTTPS	Optional	Optional	Optional	Optional
Spam-Blocking mit Viruserkennung	Optional	Optional	Optional	Optional
Schnittstellen 10/100/1000	8	8	8	8 (4 Kupfer/4 Glasfaser)
Serielle Ports	1	1	1	1
VLAN-Unterstützung	75	75	75	75
Enthaltene Sicherheitszonen	8	8	8	4 RJ45, 4 SFP GBIC
Gleichzeitige Sitzungen	500.000	750.000	1.000.000	1.000.000
Unterstützte Knoten (LAN IPs)	Unbegrenzt	Unbegrenzt	Unbegrenzt	Unbegrenzt
VPN-Tunnel für Niederlassungen (inkl./max.)	750/750	750/750	750/750	750/750
Mobile VPN-Tunnel – IPSec (inkl./max.)	600/600	600/600	600/600	600/600
Mobile VPN-Tunnel – SSL (inkl./max.)	600/600	600/600	600/600	600/600
Obergrenze für lokale Authentifizierungs-DB	5.000	6.000	8.000	8.000
Modell-Upgrades	Ja	Ja	Nein	Nein

*Durchsatzraten variieren je nach Umgebung und Konfiguration

Funktionen

Sicherheitsfunktionen
- Stateful Packet Fireware
- Deep Application Inspection Firewall
- Anwendungs-Proxies – HTTP, SMTP, FTP, DNS, TCP, POP3
- Spyware-Blocking
- DoS- und DDoS-Schutz
- Progressiver DDoS-Schutz
- Erkennung von Protokollanomalien
- Verhaltensanalyse
- Pattern-Matching
- Fragmented Packet Reassembly-Schutz
- Malformed Packet-Schutz
- Liste statisch und dynamisch blockierter Sites
- Zeitbasierte Regeln
- Instant Messaging und P2P Allow/Deny

Virtual Private Networks
- VPN
  - Verschlüsselung (DES, 3DES, AES 128-, 192-, 256-bit)
  - IPSec
    - SHA-1, MD5
    - IKE – Pre-Shared Key, Firebox Zertifikat
  - SSL
    - Thin Client, Web Exchange
- PPTP-Server
- PPTP-Passthrough
- Dead Peer Detection (RFC 3706)
- Hardware-basierte Verschlüsselung
- Drag-and-Drop-VPN-Tunnel

Benutzerauthentifizierung
- Transparente Active Directory Authentifizierung (Single-Sign-on)
- XAUTH
  - RADIUS®, LDAP, Windows® Active Directory
- VASCO
- RSA SecurID®
- Web-basiert
- Lokale Authentifizierung

IP-Adresszuweisung
- Statisch
- PPPoE-Client
- DHCP-Server, Client, Relay
- Dynamischer DNS-Client

X8500e-F Glasfaserschnittstelle
- Multi-mode Fiber (MMF)
- 1000 Base SX
- 850 nm
- LC-Stecker

Hochverfügbarkeit
- HA Aktiv/Passiv
- Konfigurationssynchronisierung
- Sitzungssynchronisierung
- VPN-Tunnel-Synchronisierung

WAN-Failover
- VPN-Failover
- WAN-Modi
  - Spill-over
  - Round Robin, Weight Round Robin
  - Failover
  - ECMP

Traffic Shaping
- Quality of Service
  - 8 Prioritäts-Warteschlangen
  - Diffserve
  - Modified Strict Queuing

Routing
- Statisches Routing
- Dynamisches Routing
  - BGP4, OSPF, RIPv1 und v2
- Policy-based Routing

Networking
- Porttrennung
- VLAN
  - Bridging, Tagging, Routed Mode
- Server Load-Balancing
- Unterstützung für VoIP- und Video-Conferencing

Sicherheitsabonnements
- spamBlocker
  - Quarantäne für Spam-, Bulk- und verdächtige Mail
  - Viruserkennung
- Gateway AntiVirus/IPS mit Anti-Spyware
  - Unbegrenztes AV-Datei-Scanning
- WebBlocker

Betriebsmodi
- Transparenter/Drop-in-Modus (Layer 2)
- Routed-Modus (Layer 3)

Network Address Translation (NAT)
- Statische NAT (Port-Forwarding)
- Dynamische NAT
- Eins-zu-Eins-NAT
- IPSec NAT Traversal
- Richtlinienbasierte NAT
- Virtuelle IP für Server Load-Balancing

Protokollierung/Berichterstattung
- Protokollzusammenfassung für mehrere Appliances
- WebTrends®-kompatible Berichte (WELF)
- HTML- und PDF-Berichte
- SQL-Protokolldatenbank
- Verschlüsselter Protokollkanal
- Syslog
- SNMP v2 und v3

Alarme/Benachrichtigungen
- SNMP
- E-Mail
- Management System Alert

Management-Software
- WatchGuard System Manager (WSM)

Zertifizierungen
- Common Criteria EAL4
- ICSA IPSec und ICSA Firewall
- West Coast Labs Checkmark Zertifikat

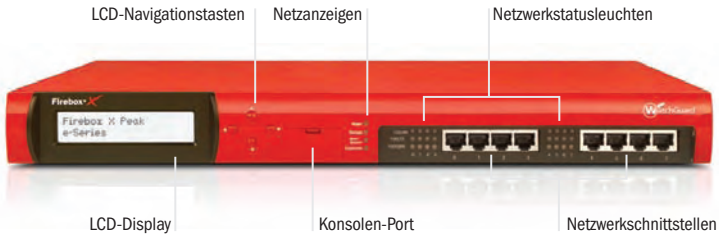
Support und Wartung
- 1 Jahr Hardware-Garantie
- 90-Tage- oder 1-Jahres-Erstabonnement für den LiveSecurity® Service

Abmessungen/Leistungswerte

Abmessungen Appliance	4,5 x 42,6 x 36,2 cm
Abmessungen Verpackung	18,4 x 54,6 x 48,2 cm
Gewicht Appliance	5,62 kg
Gesamtgewicht	6,25 kg
WEEE-Gewicht	4,81 kg
Wechselspannung	100-240 VAC Autoumschaltung
Stromverbrauch	USA: 80 Watt Restliche Welt: 1146 Kal/min oder 273 BTU/Std.
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 (Ruhezustand)	7 – 28 Hz 0,001 bis 0,01 G2 pro Hz
Akustisches Rauschen	54 dB bei 20 - 25° C
Mechanischer Schock (Betrieb)	20 G mit 11 Ms Dauer 1/2 Sinuswelle
WEEE/RoHS-konform	Ja



Netzwerkschnittstellen – 8 Kupfer-Ports für das Modell X8500e
Modell X8500e-F auch mit je 4 Kupfer- und Glasfaser-Ports erhältlich

Beratung und Support durch Experten

Der LiveSecurity® Service von WatchGuard 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:

- Hardware-Garantie mit Vorabaustausch
- Softwareupdates
- Technischer Support durch unser Rapid-Response-Team
- Topaktuelle Sicherheitshinweise mit klaren Anweisungen zum Umgang mit neuen Bedrohungen und praktische Links zu Händler-Patches
- Innovative Fortbildungsressourcen, darunter Videos, Podcasts und praktische Sicherheitsschulungen für Endbenutzer

Beim Erwerb einer Firebox X Peak Appliance können Sie zwischen einem 90-Tage- und einem 1-Jahres-Erstabonnement für den Live Security Service wählen. Unternehmen mit geschäftskritischen Internetanforderungen können zudem unseren Premium Service in Anspruch nehmen.

Peak™ UTM Bundle – Eine Lösung. Eine Lizenz: ein toller Preis

Die neue Firebox X Peak bietet jetzt in einem einzigen hochwertigen Paket alles, was Sie für ein umfassendes Unified Threat Management auf einer hochleistungsfähigen Security Appliance benötigen. Im Einzelnen sind das:

- Firebox X Peak e-Series Security Appliance
- WebBlocker*
- spamBlocker mit Viruserkennung*
- Gateway AV/IPS mit Anti-Spyware*
- LiveSecurity® Service*

Ab der Erstinstallation bietet das Firebox X Peak e-Series UTM Bundle ein effizientes und fortlaufendes Sicherheitsmanagement für Ihr Netzwerk. Sie bekommen damit nicht nur die beste UTM Lösung auf dem Markt, sondern realisieren auch noch zusätzliche Einsparungen gegenüber dem Kauf einzelner Komponenten!

*1-Jahres-Abonnement

GepaNet
http://www.gepanet.com

GepaNet
88142 Wasserburg
Wiesenstraße 12
Tel +49 8382 9479825
Fax +49 8382 9479826
Mail: info@gepanet.com
WEB: www.gepanet.com

KOSTENLOSE! 30-Tage-Demos

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

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

ADRESSE: Watchguard Technologies, IOM Business Center, Humboldt Str. 12, 85609 Aschheim-Dornach, Germany · WEB: www.watchguard.de
E-MAIL: GermanySales@watchguard.com · GERMANY SALES: +49 700 92229333

Firewall Level 1 · *VPN* · *Web Filtering* · *Intrusion Prevention* · *Anti-Spam* · *IPSec* · *Firewall* · COMMON CRITERIA EAL4+ CERTIFIED

WatchGuard™