



- **Complete unified threat management** protects the network from malicious attacks
- **True zero day protection** proactively blocks new threats
- **New! Built-in SSL VPN**
- **Eight 10/100/1000 Gigabit Ethernet ports** support high-speed connectivity
- **Advanced networking capabilities** control resources, shaping traffic and increasing uptime
- **Easy configuration and centralized management** of all appliances and features
- **Integrated security subscriptions** for more granular protection



Earth-friendly technology



## 10/100/1000 Gigabit Security for Demanding Networks

Firebox® X Peak™ is the highest-performance line of unified threat management (UTM) appliances from WatchGuard®, offering zero day protection out of the box and multi-gigabit-per-second firewall throughput. By integrating powerful security capabilities with advanced networking features, the Firebox X Peak delivers a superior overall solution that meets the needs of the most demanding network environments.

### Complete Unified Threat Management

Firebox X Peak delivers the most comprehensive security in its class. Built-in application proxies, stateful packet firewall, and full-featured VPN combine with optional security subscriptions for powerful multi-layered defenses. Anti-spyware, intrusion prevention, anti-virus, anti-spam with virus outbreak detection, and URL filtering capabilities fully integrate on one robust appliance, greatly reducing the time and costs associated with managing multiple-point solutions.

### True Zero Day Attack Prevention

When security vulnerabilities in software allow new network attacks to be introduced, the proactive defenses of Firebox X Peak ensure your network and users are safe. Sophisticated proxy technologies perform deep application inspection to identify and block emerging threats, providing automatic protection from spyware, trojans, worms, DoS, DDoS, DNS poisoning, buffer overflows, and other attacks.

### High Performance

Offering multi-gigabit firewall and up to 600 Mbps VPN throughput, Firebox X Peak provides the highest performance of any UTM solution in our family of products. With eight 10/100/1000 Gigabit Ethernet ports on all models, it supports high-speed LAN backbone infrastructures, as well as gigabit WAN connections. To maximize port utilization, any of the eight ports can be configured as Internal, External, or Optional.

### Advanced Networking Capabilities

Advanced networking features intelligently manage resources and optimize traffic, while ensuring reliable connectivity to increase network uptime.

- **VLAN support** reduces hardware requirements and provides rich interoperability
- **Multi-WAN load balancing, high availability, and WAN and VPN failover** increase performance, redundancy, and reliability
- **Dynamic routing and traffic shaping** maximize network flexibility and efficiency
- **Policy-based routing** lets you specify the outgoing interface per service to enhance bandwidth management and reduce costs
- **Server load balancing** makes it easy to protect public-facing e-commerce "server farms"

### Intuitive, Centralized Management

WatchGuard® System Manager (WSM) makes centralized management of Firebox X deployments intuitive - regardless of their size. Administrators save time and money using the interface to easily create and deploy configuration changes, monitor real-time data, and generate historical reports.

### Secure Remote Connectivity

Protection for remote workers, no matter where they are, is easier with the Firebox X Peak. It has the broadest range of remote access capabilities in its class, allowing off-site users to safely access the corporate network via:

- IPsec VPN, SSL VPN, and PPTP clients

Includes single sign-on to streamline authentication.

### Integrated Security Capabilities for More Granular Protection

Boost defenses in critical attack areas by adding powerful security subscriptions to your Firebox X. All subscriptions are centrally managed using WSM and continuously updated for the most current protection.

#### WebBlocker

URL filtering increases productivity and decreases security risks by blocking HTTP and HTTPS access to malicious or inappropriate web content

#### spamBlocker with virus outbreak detection

Stops nearly 100% of spam and the viral payloads it carries

#### Gateway AV/IPS with anti-spyware

Stop known spyware, viruses, trojans, and web exploits with signature-based protection

### Full Model Upgradeability and Scalability

As network requirements change, easily increase capacity or add security subscriptions using simple, downloadable software license keys.

### Our Commitment to the Environment

WatchGuard is committed to creating products that are energy efficient and use recyclable appliance and packaging material. We fully comply with EU directives against the use of hazardous substances and have made environmental responsibility an important component of our strategic global business requirements.

## Blocking Web-based Exploits

The Web is one of your most valuable business tools, but it can also be a serious threat to your network. Unmanaged web users can inadvertently or deliberately create weaknesses, introducing bots and spyware that can put sensitive corporate data in jeopardy and dramatically increase helpdesk calls. Vulnerable networks are susceptible to Domain Name Service (DNS) cache poisoning, buffer overflows, and Denial of Service (DoS) attacks.

### What You Need

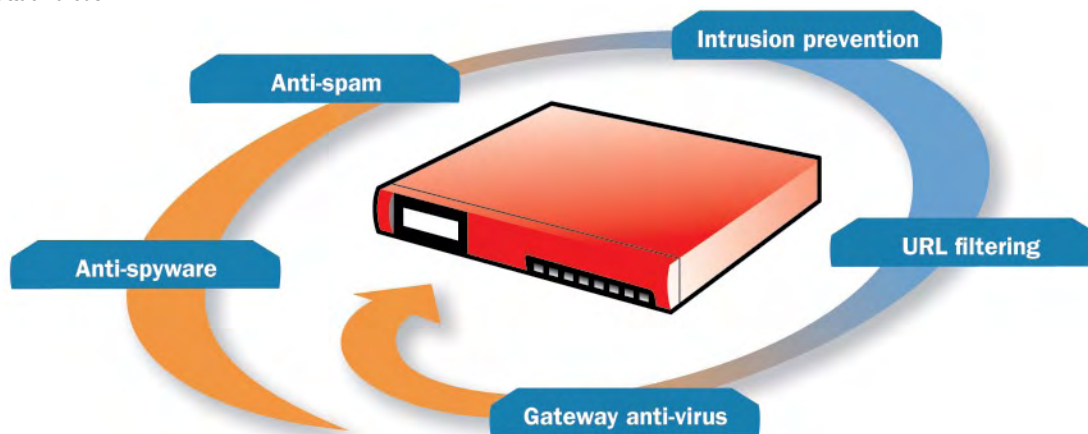
- Start with **Firebox X Peak** for true zero day attack protection and multi-gigabit performance
- Activate subscriptions to **WebBlocker** for control over unauthorized web surfing, and to **Gateway AV/IPS** to block suspicious web traffic and downloaded files in real time

### How the Protection Adds Up

- **True zero day protection** through powerful, built-in application proxy technologies shields your network against unknown threats when vulnerabilities in application software make new kinds of attacks possible

- **Multi-layered anti-spyware capabilities** block access to known spyware sites, stop “drive-by” spyware from entering the network as a result of web surfing, and block spyware attempting to contact its host
- **Gateway anti-virus/IPS with anti-spyware** inspects web traffic for viruses, trojans, bots, and other malware for granular protection from known threats
- **Cloaking your web servers** prevents hackers from using your system information to attack your network
- **WebBlocker** allows you to limit what employees can access on the Web from work to increase productivity and prevent legal liabilities, while protecting the network from malicious sites
- **URL filtering of HTTPS** traffic stops users from slipping through the backdoor for off-limits web surfing
- **Intelligent layered security architecture works with the DNS proxy** to protect against network intrusion, DoS attacks, and DNS cache poisoning
- **Integrated logging, reporting, and alerting** provide detailed insight into network activity, and allow you to take immediate preventive or corrective action

**Integrated security subscriptions** on the Firebox X Peak boost protection in critical attack areas



## Securing Remote Offices and Mobile Users

With more employees telecommuting or working from satellite facilities, the need for reliable and secure remote connections to resources and data is great. Issues such as centralized management and reporting, setting uniform security policies, interoperability with your existing network resources and applications, and reliable remote connectivity should be weighed carefully. And ensuring that remote devices meet your security policies before accessing the network is critical.

### What You Need

- Start with **Firebox X Peak** for unified threat management and multi-gigabit performance
- Add **Firebox X Edge** appliances to get exceptional wired or wireless network perimeter protection for remote and branch offices, and centrally manage all security capabilities with the easy-to-use **WatchGuard System Manager (WSM)**

### How the Protection Adds Up

- **Centralized policy and VPN management** lets you uniformly enforce security policies across all locations and users
- **Secure remote access to network resources** over encrypted branch office and mobile user VPN tunnels increases productivity and flexibility for employees outside the main office
- **Powerful unified threat management** for your remote offices and telecommuters means your users and extended network are protected from spyware, viruses, DoS attacks, and other dynamic threats
- **Easy drag-and-drop Branch Office VPN configuration** gets remote office connectivity up and running in 3 clicks, and keeps IT costs low
- **Multi-gigabit performance** supports reliability, redundancy, and flexibility for varied network-connectivity environments and future network growth needs

Specifications	<b>Firebox® X5500e</b> WG55500 X5500e UTM Bundle WG55503	<b>Firebox® X6500e</b> WG56500 X6500e UTM Bundle WG56503	<b>Firebox® X8500e</b> WG58500 X8500e UTM Bundle WG58503	<b>Firebox® X8500e-F</b> WG58510 X8500e-F UTM Bundle WG58513
<b>Firewall Throughput*</b>	2.0+ Gbps	2.3 Gbps	2.3 Gbps	2.3 Gbps
<b>VPN Throughput*</b>	400 Mbps	600 Mbps	600 Mbps	600 Mbps
<b>AV Throughput*</b>	140 Mbps	170 Mbps	200 Mbps	200 Mbps
<b>Gateway AV/IPS</b> with anti-spyware	Optional	Optional	Optional	Optional
<b>URL Filtering</b> for HTTP and HTTPS	Optional	Optional	Optional	Optional
<b>Spam Blocking</b> with virus outbreak detection	Optional	Optional	Optional	Optional
<b>Interfaces 10/100/1000</b>	8	8	8	8 (4 copper/4 fiber)
<b>Serial Port</b>	1	1	1	1
<b>VLAN Support</b>	75	75	75	75
<b>Security Zones</b> (incl.)	8	8	8	4 RJ45, 4 SFP GBIC
<b>Concurrent Sessions</b>	500,000	750,000	1,000,000	1,000,000
<b>Nodes Supported</b> (LAN IPs)	Unlimited	Unlimited	Unlimited	Unlimited
<b>Branch Office VPN Tunnels</b> (incl./max.)	750/750	750/750	750/750	750/750
<b>Mobile VPN Tunnels - IPSec</b> (incl./max.)	600/600	600/600	600/600	600/600
<b>Mobile VPN Tunnels - SSL</b> (incl./max.)	1000/1000	4000/4000	6000/6000	6000/6000
<b>Local User Authentication DB Limit</b>	5,000	6,000	8,000	8,000
<b>Model Upgradeable</b>	Yes	Yes	No	No

\*Throughput rates will vary depending on environment and configuration

## Features

### Security Features

- Stateful Packet Firewall
- Deep Application Inspection Firewall
- Application Proxies - HTTP, SMTP, FTP, DNS, TCP, POP3
- Spyware Blocking
- DoS and DDoS Prevention
- Progressive DDoS Prevention
- Protocol Anomaly Detection
- Behavioral Analysis
- Pattern Matching
- Fragmented Packet Reassembly Protection
- Malformed Packet Protection
- Static and Dynamic Blocked Sources List
- Time-based Rules
- Instant Messaging and P2P Allow/Deny

### Virtual Private Networks

- VPN
  - Encryption (DES, 3DES, AES 128-, 192-, 256-bit)
  - IPSec
    - SHA-1, MD5
    - IKE Pre-Shared Key, Firebox 3rd Party Cert.
  - SSL
    - Thin Client, Web Exchange
- PPTP Server
- PPTP Passthrough
- Dead Peer Detection (RFC 3706)
- Hardware-based Encryption
- Drag-and-Drop VPN Tunnels

### User Authentication

- Transparent Active Directory Authentication (Single Sign-on)
- XAUTH
  - RADIUS®, LDAP, Windows® Active Directory
- VASCO
- RSA SecurID®
- Web-based
- Local Authentication

### IP Address Assignment

- Static
- PPPoE Client
- DHCP Server, Client, Relay
- Dynamic DNS Client

### X8500e-F Fiber Interface

- Multi-mode Fiber (MMF)
- 1000 Base SX
- 850 nm
- LC Connectors

### High Availability

- HA Active/Passive
- Configuration Synchronization
- Session Synchronization
- VPN Tunnel Synchronization

### WAN Failover

- VPN Failover
- WAN Modes
  - Spill-over
  - Round Robin, Weighted Round Robin
  - Failover
  - ECMP

### Traffic Shaping

- Quality of Service
  - 8 Priority Queues
  - DiffServ
  - Modified Strict Queuing

### Routing

- Static Routes
- Dynamic Routing
  - BGP4, OSPF, RIP v1 and v2
- Policy-based Routing

### Networking

- Port Independence
- VLAN
  - Bridging, Tagging, Routed Mode
- Server Load Balancing
- VoIP and Video Conferencing Support

### Security Subscriptions

- spamBlocker
  - Quarantine for spam, bulk, and suspect mail
  - Virus Outbreak Detection

- Gateway AntiVirus/IPS with anti-spyware
  - Unlimited AV file size scanning
- WebBlocker

### Modes of Operation

- Transparent/Drop-in Mode (Layer 2)
- Routed Mode (Layer 3)

### Network Address Translation

- Static NAT (Port Forwarding)
- Dynamic NAT
- One-to-One NAT
- IPSec NAT Traversal
- Policy-based NAT
- Virtual IP for Server Load Balancing

### Logging/Reporting

- Multi-appliance Log Aggregation
- WebTrends® Compatible Reports (WELF)
- HTML and PDF Reports
- SQL Log Database
- Encrypted Log Channel
- Syslog
- SNMP v2 and v3

### Alarms/Notifications

- SNMP
- Email
- Management System Alert

### Management Software

- WatchGuard System Manager (WSM)

### Certifications

- Common Criteria EAL4
- ICASA IPSec and ICASA Firewall
- West Coast Labs Checkmark

### Support & Maintenance

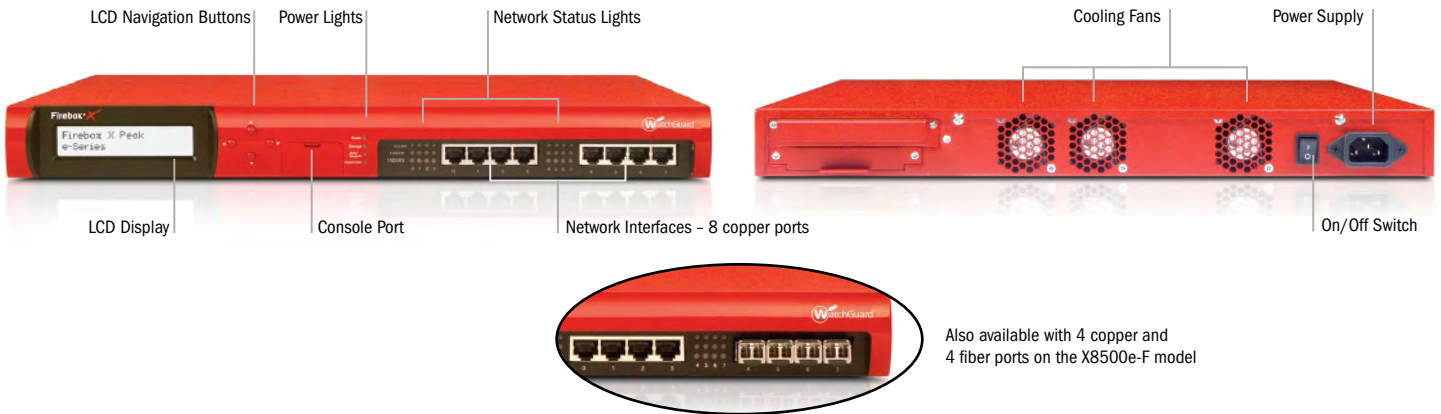
- 1-Year Hardware Warranty
- Initial 90-Day or 1-Year LiveSecurity® Service Subscription

**Dimensions and Power**

<b>Appliance Dimensions</b>	1.75" x 16.75" x 14.25" (4.5 x 42.6 x 36.2 cm)
<b>Packaging Dimensions</b>	7.25" x 21.75" x 19" (18.4 x 54.6 x 48.2 cm)
<b>Appliance Weight</b>	12.4 lbs (5.62 Kg)
<b>Total Weight</b>	13.8 lbs (6.25 Kg)
<b>WEEE Weight</b>	10.6 lbs (4.81 Kg)
<b>AC Power</b>	100-240 VAC Autosensing
<b>Power Consumption</b>	U.S. 80 Watts Rest of World: 1146 Cal/min or 273 BTU/hr
<b>Rack Mountable</b>	Yes

**Environmental**

<b>Operating Temperature</b>	32 - 113° F (0 - 45° C)
<b>Non-operating Temperature</b>	-40 - 158° F (-40 - 70° C)
<b>Operating Humidity</b>	10 - 85%
<b>Non-operating Humidity</b>	10 - 95% Non-condensing at 131° F (55° C)
<b>Non-operating Random Vibration</b>	7 - 28 Hz 0.001 to 0.01 G2 per Hz
<b>Acoustic Noise</b>	54 dBA at 20 - 25° C
<b>Operating Mechanical Shock</b>	20 G with 11 Msec duration 1/2 sine wave
<b>WEEE/RoHS Compliant</b>	Yes



Also available with 4 copper and 4 fiber ports on the X8500e-F model

**Expert Guidance and Support**

LiveSecurity® Service from WatchGuard is the most comprehensive support and maintenance offering in the industry, putting a global team of security experts behind you to make the complex job of IT management easier. LiveSecurity Service provides:

- Hardware warranty with advance hardware replacement
- Software updates
- Rapid-response technical support
- Up-to-the-minute security alerts with clear instructions on how to deal with new threats and direct links to vendor patches to save time
- Innovative education resources, including videos, podcasts, and handy security-training modules for end users

You have your choice of an initial 90-day or 1-year subscription to LiveSecurity Service when you purchase a Firebox X Peak appliance. Premium support service is available for companies with mission-critical Internet requirements.

**Peak™ UTM Bundle – One solution, one license, one great price**

Everything you need for comprehensive unified threat management on a high-performance security appliance is now in one convenient package. An exceptional value, each bundle includes:

- Firebox X Peak e-Series security appliance
- WebBlocker\*
- spamBlocker with virus outbreak detection\*
- Gateway AV/IPS with anti-spyware\*
- LiveSecurity® Service\*

From initial purchase through ongoing security management, a Firebox X Peak e-Series UTM Bundle streamlines network security management while providing the best UTM solution in its class. Buy together and save!

\*One-year subscription

**FREE!** **30-day trials**

Get free 30-day trials of **Gateway AV/IPS**, **spamBlocker**, and **WebBlocker** with the purchase of a Firebox X Peak. Contact your reseller for details.

For more information on Firebox X Peak, visit [www.watchguard.com/appliances](http://www.watchguard.com/appliances)

ADDRESS: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 · WEB: [www.watchguard.com](http://www.watchguard.com) · U.S. SALES: 1.800.734.9905 · INTERNATIONAL SALES: +1.206.613.0895

No express or implied warranties are provided for herein. All specifications are subject to change and any expected future products, features or functionality will be provided on an if and when available basis. ©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, Firewall, LiveSecurity, Peak, and Core are either trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other trademarks and tradenames are the property of their respective owners. Part No. WGCE66358\_011008

