



## 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** protects you from malicious network attacks
- **Zero day protection** proactively blocks new threats
- **Doubles the performance** of previous models and has eight 10/100/1000 Gigabit Ethernet ports
- **Manages resources**, shaping traffic and increasing uptime
- **Easy configuration and management** of Firebox X appliances and services
- **Integrated security capabilities** for more granular protection
- **Fully compliant with RoHS/WEEE** and other environmental directives

### Complete Unified Threat Management

Firebox X Peak provides comprehensive security by integrating deep application inspection firewall, VPN, zero day protection, gateway anti-virus, intrusion prevention, anti-spyware, anti-spam, and URL filtering into a single appliance, reducing the time and costs associated with managing multiple-point solutions.

### Zero Day Protection

When security vulnerabilities in software make new kinds of network attacks possible, the built-in proactive defenses of the Firebox X Peak are already working to keep your network safe. Its intelligent layered security architecture is based on sophisticated proxy technologies that can identify and block new threats as they emerge, so you securely carry on with business as usual.

### Highest Performance Firebox X

Offering multi-gigabit firewall and up to 600 Mbps VPN throughput, Firebox X Peak provides the highest performance of any UTM solution in our line. 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

Firebox X Peak advanced networking features intelligently manage resources, optimize traffic, and increase network uptime.

- **VLAN** 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

### Intuitive, Centralized Management

WatchGuard® System Manager (WSM) is an intuitive graphical UI used to centrally manage all capabilities of the Firebox X Peak. Because there's

just one interface to learn in order to manage your security solution, including multi-box deployments, you'll quickly get up and running and stay that way. Comprehensive logging and reporting, drag-and-drop VPN creation, and interactive, real-time monitoring are all included in WSM, with no hidden costs.

### Integrated Security Capabilities for More Granular Protection

Each WatchGuard security service works cooperatively with the built-in zero day attack prevention of the Firebox X Peak for an unbeatable combination of security capabilities. These capabilities are fully integrated within the Firebox so no additional hardware is required. Because subscriptions are priced per appliance, not per user, there are no escalating costs. All security services are continuously updated to give you up-to-the-minute protection, and are centrally managed with WSM for real-time views of all service activities. Services include:

- **WebBlocker**  
Increase productivity and decrease security risks by blocking access to inappropriate and potentially malicious Web content
- **spamBlocker**  
Get the best anti-spam service in the industry, blocking up to 97% of unwanted emails
- **Gateway AV/IPS**  
Rely on robust, signature-based protection at the gateway to stop known viruses, spyware, trojans, and Web-based exploits

### Full Model Upgradeability and Scalability

As your network requirements change, you can easily increase capacity or add any of our security services using simple, downloadable software license keys to avoid costly hardware upgrades.

### 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 European Union 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 Server (DNS) cache poisoning, buffer overflows, and Denial of Service (DoS) attacks.

### What You Need

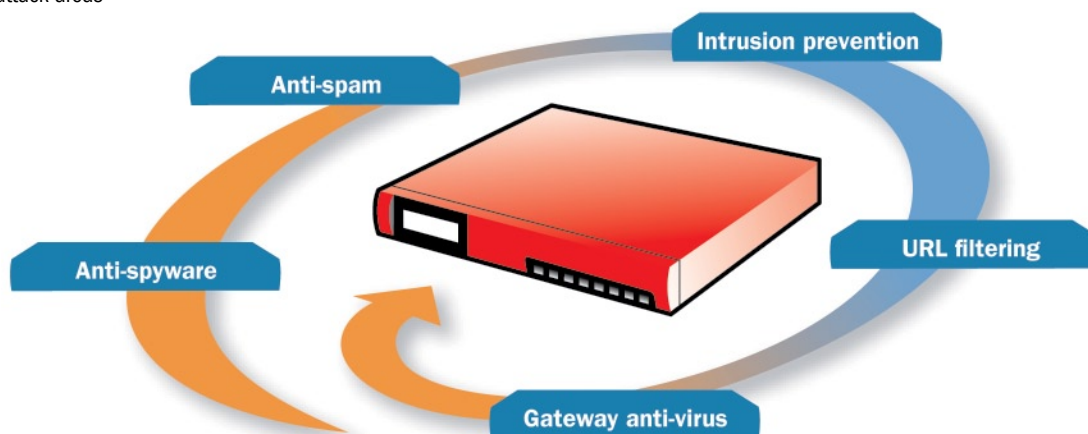
- Start with **Firebox X Peak** for true zero day attack protection and gigabit performance
- Activate subscriptions to **WebBlocker** for control over unauthorized Web surfing, and to **Gateway AV/IPS** to block suspicious Web traffic and downloaded files in real time

### How the Protection Adds Up

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

- **Gateway anti-virus** inspects Web traffic for viruses, trojans, bots, and other malware
- **Cloaked Web servers** prevent hackers from using your system information to attack your network
- **URL filtering** controls users' Web surfing to increase productivity, protect network bandwidth, lower security risks, and decrease legal liability resulting from inappropriate content in the workplace
- **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
- **Intelligent layered security architecture works with the DNS proxy** to protect against network intrusion, DoS attacks, and DNS cache poisoning
- **Robust IPS capabilities** control the use of Instant Messaging (IM) and Peer-to-Peer (P2P) applications - two of the most common vehicles for spyware distribution
- **Integrated logging, reporting, and alerting** provide detailed insight into network activity, and allow you to take immediate preventive or corrective action

**Integrated security services** on Firebox X 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 gigabit performance
- Add **Firebox SSL VPN Gateway** for secure, universal access for mobile workers and telecommuters, **Firebox X Edge** to get exceptional wired or wireless network perimeter protection for remote and branch offices, and manage it all with **WatchGuard System Manager**

### How the Protection Adds Up

- **Centralized policy and VPN management** lets you uniformly enforce security policies across all locations and users
- **Secure remote access** with end-point security checks gives mobile users and telecommuters reliable remote access to network resources, and ensures that their devices are secure before accessing the network
- **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
- **Gigabit performance** provides reliability, redundancy, and flexibility for varied network-connectivity environments and future network growth needs

Specifications	Firebox® X5500e WG55500	Firebox® X6500e WG56500	Firebox® X8500e WG58500	Firebox® X8500e-F WG58510
<b>Firewall Throughput*</b>	2.0 Gbps	2.0 Gbps	2.0 Gbps	2.0 Gbps
<b>VPN Throughput*</b>	400 Mbps	600 Mbps	600 Mbps	600 Mbps
<b>Gateway AV/IPS</b>	Optional	Optional	Optional	Optional
<b>URL Filtering</b>	Optional	Optional	Optional	Optional
<b>Spam Blocking</b>	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</b>	75	75	75	75
<b>Security Zones (incl.)</b>	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 (LAN IPs)</b>	Unlimited	Unlimited	Unlimited	Unlimited
<b>Branch Office VPN Tunnels (incl./max.)</b>	400/400	400/400	400/400	400/400
<b>Mobile User VPN Tunnels (incl./max.)</b>	400/400	400/400	400/400	400/400
<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
- Spyware Blocking
- Application Proxies - HTTP, SMTP, FTP, DNS, TCP
- DoS and DDoS Prevention
- Progressive DDoS Prevention
- Protocol Anomaly Detection
- Behavioral Analysis
- Pattern Matching
- Fragmented Packet Reassembly Protection
- Malformed Packet Protection
- Static Blocked Sources List
- Dynamic Blocked Sources List
- Time-based Rules
- Instant Messaging and P2P Allow/Deny

### Virtualization

- VLAN
  - Bridging
  - Tagging
  - Routed Mode
- VPN
  - Encryption (DES, 3DES, AES 128-, 192-, 256-bit)
  - IPSec
    - SHA-1, MD5
    - IKE Pre-Shared Key, Firebox 3rd Party Cert.
- PPTP Server
- PPTP Passthrough
- Dead Peer Detection (RFC 3706)
- Hardware-based Encryption
- Drag-and-Drop Tunnels with Fireware Rules

### User Authentication

- XAUTH
  - RADIUS®
  - LDAP
  - Windows® Active Directory
- RSA SecurID®
- Web-based
- Local Authentication

### X8500e-F Fiber Interface

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

### IP Address Assignment

- Port Independence
- Static
- PPPoE Client
- DHCP Server
- DHCP Client
- DHCP Relay
- Dynamic DNS Client

### High Availability

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

### WAN Failover

- VPN Failover
- WAN Modes
  - Spill-over
  - Round Robin
  - Failover
  - ECMP
  - Weight Round Robin

### Traffic Shaping

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

### Routing

- Static Routes
- RIPv1, v2
- Dynamic Routing
  - BGP4
  - OSPF
- Policy-based Routing

### Modes of Operation

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

### Network Address Translation

- Static NAT (Port Translation)
- Dynamic NAT
- One-to-One NAT
- IPSec NAT Traversal
- Policy-based NAT

### Logging/Reporting

- Multi-appliance Log Aggregation
- WebTrends® Compatible Reports (WELF)
- HTML Reports
- XML Log Format
- Encrypted Log Channel
- Syslog
- SNMP

### Alarms/Notifications

- SNMP
- Email
- Management System Alert

### Management Software

- WatchGuard System Manager (WSM)

### Certifications

- EAL4+
- West Coast Labs Checkmark
  - Firewall Level 1, VPN, Web Filtering, Intrusion Prevention, Anti-Spam

### Support & Maintenance

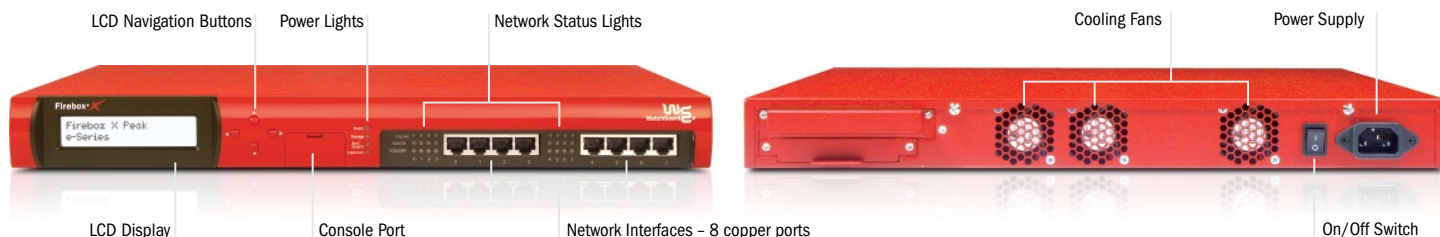
- 1-Year Hardware Warranty
- 90-Day LiveSecurity® Service Subscription

**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

Premium support service is available for companies with mission-critical Internet requirements.

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

**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.

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. ©2007 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, Fireware, LiveSecurity, Peak, Core, and Stronger Security, Simply Done 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. WGC66358\_032707



Firewall Level 1



VPN



Web Filtering



Intrusion Prevention



Anti-Spam

