



- **Complete Unified Threat Management** protects you from malicious network threats
- **Zero Day protection** proactively blocks new and unknown attacks without signatures
- **Doubles the performance** of previous models and has eight 10/100/1000 Gigabit Ethernet ports
- **Manages resources**, optimizing traffic and increasing uptime
- **Easy configuration and management** of Firebox X appliances and services
- **Integrated security capabilities** for more granular protection

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 true Zero Day protection out of the box, with up to gigabit-per-second firewall throughput. 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 provides comprehensive security by integrating stateful packet firewall, VPN, true Zero Day attack prevention, 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.

True Zero Day Protection

The Intelligent Layered Security (ILS) in Firebox X Peak offers true Zero Day protection right out of the box. It protects against new and unknown threats before the vulnerability is discovered and the exploit is created and launched. Many vendors only provide signature-based protection that requires a separate license fee. These reactive solutions actually leave their customers exposed to new types of threats.

Highest Performance Firebox X

Offering up to 2.0 Gbps firewall and up to 600 Mbps VPN, Firebox X Peak provides the highest performance and best scalability of any UTM solution in our line. Firebox X Peak has eight 10/100/1000 Gigabit Ethernet ports on all models to support 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. Multi-WAN load sharing and interface failover increase performance and reliability, while dynamic routing, and traffic management and prioritization deliver superior network capabilities for mission-critical data and communication throughout your network.

Easy, Intuitive Management

WatchGuard System Manager (WSM), included in your Firebox X Peak, streamlines your network security administration. With a graphical user interface, quick configuration wizards, and smart defaults, WSM simplifies the installation process. Comprehensive logging and reporting; interactive, real-time

monitoring; and drag-and-drop VPN creation 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 with the Firebox, so no additional hardware is required. Subscriptions are priced per appliance, not per user, so 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:

- **spamBlocker**
Get the best anti-spam service in the industry, blocking up to 97% of unwanted e-mails.
- **Gateway AV/IPS**
Rely on robust, signature-based protection at the gateway against known viruses, spyware, trojans, and Web-based exploits.
- **WebBlocker**
Increase productivity and decrease security risks by blocking access to malicious Web content and managing your users' Web surfing.

Full Model Upgradeability and Scalability

As your network security requirements change, you can easily extend and protect your security investment. Increase capacity and firewall or VPN throughput, or add any of our security capabilities with no hardware replacement required.

- The only truly model upgradeable UTM security appliance on the market today, Firebox X Peak lets you easily increase performance, capacity, networking, and security capabilities as your needs grow.
- Firebox X Peak can be upgraded to support growing business requirements with a simple license key. No forklift upgrades.



Stronger Security, Simply Done™

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

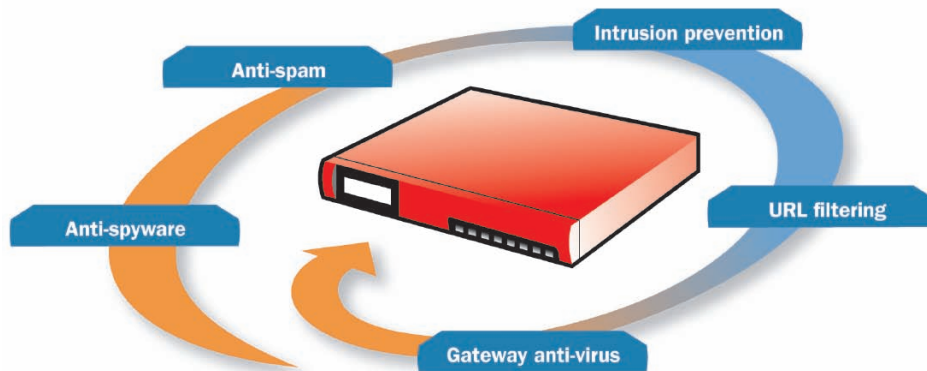
- Start with **Firebox X Peak** for true Zero Day attack protection and gigabit performance
- Activate subscriptions to **WebBlocker** for control over unauthorized Web surfing, and to **Gateway AV/IPS** to block suspicious Web traffic and downloaded files in real time

How the Protection Adds Up

- **Gateway anti-virus** inspects Web traffic for viruses and other malware surfing, and blocks spyware attempts
- **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
- **True Zero Day protection** shields your network against many new or unknown threats before the vulnerability is discovered and the exploit is created and launched
- **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 working with the DNS proxy** protects 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

Firebox X: Integrated Security



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
Firewall Throughput*	900 Mbps	1.5 Gbps	2.0 Gbps	2.0 Gbps
VPN Throughput*	400 Mbps	600 Mbps	600 Mbps	600 Mbps
Gateway AV/IPS	Optional	Optional	Optional	Optional
URL Filtering	Optional	Optional	Optional	Optional
Spam Blocking	Optional	Optional	Optional	Optional
Interfaces 10/100/1000	8	8	8	8 (4 copper/4 fiber)
Serial Port	1	1	1	1
Security Zones (incl.)	8	8	8	4 RJ45, 4 SFP GBIC
Concurrent Sessions	500,000	750,000	1,000,000	1,000,000
Nodes Supported (LAN IPs)	Unlimited	Unlimited	Unlimited	Unlimited
Branch Office VPN Tunnels (incl./max.)	400/400	400/400	400/400	400/400
Mobile User VPN Tunnels (incl./max.)	1,200/4,000	1,600/5,000	2,000/10,000	2,000/10,000
Local User Authentication DB Limit	5,000	6,000	8,000	8,000
Model Upgradeable	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
- 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

VPN

- Encryption (DES, 3DES, AES 128-, 192-, 256-bit)
- IPsec
 - SHA-1, MD5
 - IKE - Pre-Shared Key
- PPTP Server
- PPTP Passthrough
- Dead Peer Detection (RFC 3706)
- Hardware-based Encryption

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
- Dynamic DNS Client
- DHCP Server
- DHCP Client
- DHCP Relay

Redundancy Features

- High Availability
 - HA Active/Passive
 - Configuration Synchronization
 - Session Synchronization
 - VPN Tunnel Synchronization
- Multi-WAN Failover
 - WAN Failover Ports - 4
 - WAN Failover Modes (Active/Passive)

Load Sharing

- Round Robin Load Sharing
- Up to 4 Ports

Traffic Management and Prioritization

- Maximum Bandwidth
- Maximum Connections/Second
- Policy-based Traffic Prioritization
- Quality of Service
 - 2 Prioritization

Routing

- Static Routes
- RIPv1, v2
- BGP4
- OSPF

Modes of Operation

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

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/Notification

- SNMP
- E-mail
- Management System Alert
- Custom Program Alert
- Offline Configuration w/GUI

Management Software

- WatchGuard System Manager (WSM)

Certifications

- EAL-4 - Pending

Support & Maintenance

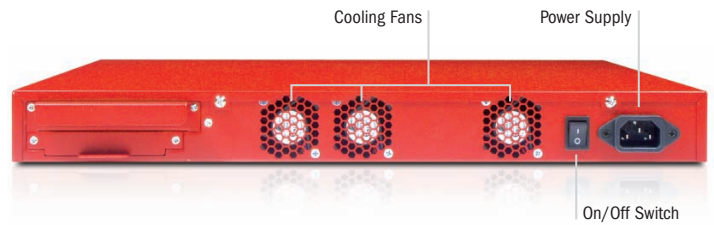
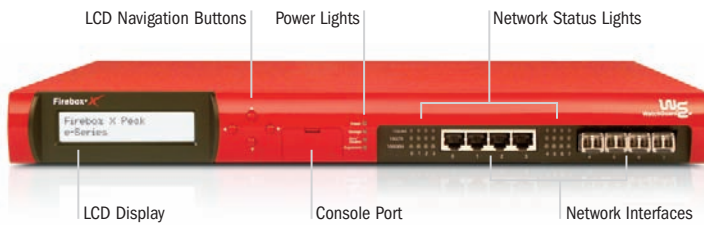
- 1-Year Hardware Warranty
- 90-Day LiveSecurity® Service Subscription

Dimensions and Power

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

Environmental

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


Expert Guidance and Support

The WatchGuard LiveSecurity Service is the most comprehensive bundled support and maintenance offering in the industry. Our expert team will equip you to better manage your network security. LiveSecurity Service offers software updates, expert technical support, up-to-the-minute security warning broadcasts, advance hardware replacement, and self-help resources such as training, certification, and tutorial programs. Premium support service is available for companies with mission-critical Internet requirements.

FREE!
30-day trials

Get free 30-day trials of **spamBlocker**, **WebBlocker**, and **Gateway AV/IPS** 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

ADDRESS: 505 Fifth Avenue South, Suite 500, Seattle, WA 98104 · WEB: 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. ©2006 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, LiveSecurity, Peak, 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. WGCE66358_072006