



## Comprehensive Unified Threat Management Solution

Firebox® X Core™ Unified Threat Management (UTM) solutions provide the most complete security in their class, integrating stateful packet firewall, VPN, true Zero Day attack prevention, anti-spyware, anti-spam, anti-virus, intrusion prevention, and URL filtering on a single appliance – reducing the time and cost associated with managing multiple-point solutions and significantly increasing protection from blended network attacks.

- **Comprehensive protection** keeps your network safe from malicious threats
- **Zero Day attack prevention** shuts down new and unknown threats before signatures are available
- **Streamlined network security management** saves you time
- **Continually updated anti-virus, anti-spam, anti-spyware, and URL filtering services** provide up-to-the-minute protection
- **Integrated, upgradeable capabilities** mean better value for your dollar
- **Global team of security experts** are there when you need them

### Superior Multi-Layered Security

The Firebox X Core is built on Intelligent Layered Security (ILS). Within this architecture, security layers work together to strengthen overall protection, while cooperative communication between layers reduces and fine tunes the processing. The result – you get the protection you need to stay safe without sacrificing performance.

### True Zero Day Protection

Unlike products that rely solely on signature-based scanning, the Firebox X Core has critical security capabilities built in that defend against classes of attacks and their variants, without the need for signatures. While other networks remain vulnerable to the newest threat until a signature arrives, your network has strong protection from the moment you turn on your Firebox.

### Unified Management with No Hidden Costs

WatchGuard® System Manager (WSM) is the intuitive graphical user interface used to manage all capabilities of Firebox X Core UTM solutions, as well as Firebox X Peak™ and Edge appliances. WSM provides comprehensive logging, drag-and-drop VPN creation, and real-time monitoring out of the box, with no hidden costs or additional purchases required. Because there's just one interface to learn in order to manage all aspects of your security solution, you'll save time as well as money.

### Expert Guidance and Support

The WatchGuard LiveSecurity® Service is the most comprehensive bundled support and maintenance offering in the industry. Our global team of security experts is committed to equipping you to better manage your network security. LiveSecurity Service provides software updates, expert technical support, up-to-the-minute vulnerability warnings, 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.

### 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 Core for an unbeatable combination of security capabilities. Services are fully integrated and 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.

- **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.

- **WebBlocker**

Increase productivity and decrease security risks by blocking access to malicious Web content and managing your users' Web surfing.

### Protecting Your Investment

Consider the cost of deploying, managing, and upgrading multiple security solutions to handle wide-ranging security needs, and it's clear why our Firebox X Core UTM solutions provide better value for your dollar. Fully integrated, multifaceted protection on a single appliance means you save money on every aspect of ownership, from initial purchase to support contracts.

As needs grow, you can easily add new capabilities to boost your organization's security posture. For more throughput and capacity, you can upgrade to a higher model in the line by downloading a simple license key. To meet the needs of more demanding networks, upgrade to Fireware® Pro advanced appliance software for expanded networking features including high availability, traffic management, and dynamic routing. All of this is available without buying new hardware. No other security products on the market protect your security investment in so many ways.

## 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

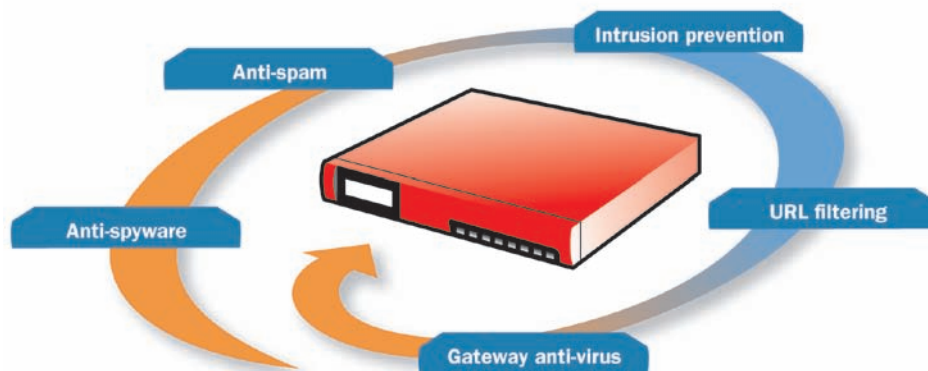
- Start with **Firebox X Core** for true Zero Day attack protection and gigabit performance
- Activate subscriptions to **WebBlocker** for control over unauthorized Web surfing, and to **Gateway AV/IPS** to block suspicious Web traffic and downloaded files in real time

### How the Protection Adds Up

- **Gateway anti-virus** inspects Web traffic for viruses and other malware
- **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



## Stopping Email-borne Threats

Your business relies on email. It has to flow smoothly and reliably, without jeopardizing network security. But email remains the most common vehicle for spreading malicious code in your network. Add the hassle of relentless spam, and your email environment can be one of your greatest IT burdens.

### What You Need

- Start with the **Firebox X Core** with true Zero Day protection
- Add a **Gateway AV/IPS** subscription that scans email traffic to block known worms, viruses, trojans, and other malware
- Enable a **spamBlocker** subscription, the best service in the industry at distinguishing legitimate email from spam outbreaks in real time

### How the Protection Adds Up

- **spamBlocker** uses real-time spam detection so you get immediate protection, with up to 97% of unwanted email blocked regardless of message content, language, or format
- **Built-in Zero Day protection** proactively blocks file types that commonly carry malware payloads via email
- **Cloaked SMTP servers** prevent hackers from using your system information to attack your network
- **Integrated Gateway AV** gives you more granular file and attachment protection, stopping viruses, worms, and other malware before they can penetrate the network and disable your desktop security applications
- **Outbound email AV scanning** prevents your company from sending viruses, worms, and trojans to partners, customers, and other recipients outside your network

Specifications	Firebox® X550e WG50550	Firebox® X750e WG50750	Firebox® X1250e WG51250
Firewall Throughput*	125 Mbps	200 Mbps	300+ Mbps
VPN Throughput*	20 Mbps	50 Mbps	100 Mbps
Gateway AV/IPS	Optional	Optional	Optional
URL Filtering	Optional	Optional	Optional
Spam Blocking	Optional	Optional	Optional
Serial Port	1	1	1
Interfaces 10/100	4	8	0
Interfaces 10/100/1000	0	0	8
Security Zones (incl.)	4	8	8
Concurrent Sessions	25,000	75,000	200,000
Nodes Supported (LAN IPs)	Unlimited	Unlimited	Unlimited
Branch Office VPN Tunnels (incl./max.)	1/10	100/100	400/400
Mobile User VPN Tunnels (incl./max.)	5/10	50/100	400/400
Local User Authentication DB Limit	250	1,000	5,000
Model Upgradeable	No	Yes	No
Fireware® Pro Advanced Appliance Software	Optional	Optional	Optional

\*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, Firebox Certificate
- 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

### IP Address Assignment

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

### 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
- Traffic Prioritization/QoS\*
  - 2 Prioritization Levels

### 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/Notifications

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

### Management Software

- WatchGuard System Manager (WSM)

### Certifications

- EAL-4 - Pending

### Support & Maintenance

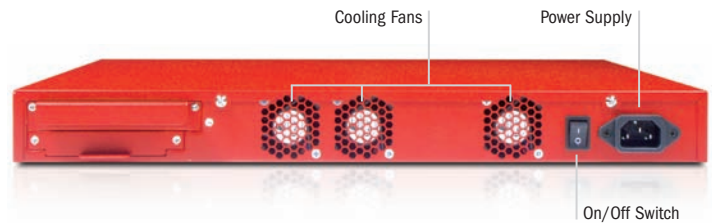
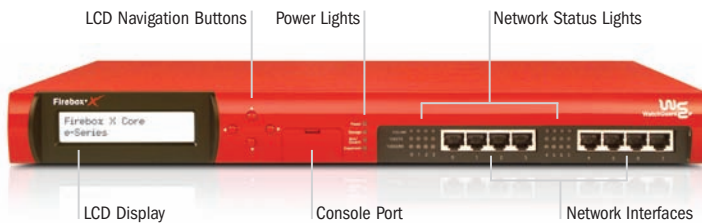
- 1-Year Hardware Warranty
- 90-Day LiveSecurity® Service Subscription

**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 48.3 cm)
Appliance Weight	9.68 lbs (4.39 Kg)
Total Weight	13.7 lbs (6.21 Kg)
WEEE Weight	10.6 lbs (4.81 Kg)
AC Power	100-240 VAC Autosensing
Power Consumption	U.S. 60 Watts Rest of World: 860 Cal/min or 205 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


**Ready to upgrade to Fireware® Pro advanced appliance software?**

As network needs grow, upgrade your Firebox X Core from Fireware to Fireware Pro, WatchGuard's advanced appliance software for more demanding networks. Move up to Fireware Pro for:

- **Traffic Management and Prioritization** - Ensures business-critical applications get the bandwidth they need
- **Dynamic Routing (BGP, OSPF)** - Maximizes network flexibility, redundancy, and efficiency by dynamically updating routing tables
- **High Availability (Active/Passive)** - Offers hardware redundancy to a standby appliance

Contact your reseller for details.

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

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

**One solution, one license, one great price**

Get everything you need for comprehensive Unified Threat Management in one convenient package with the Firebox X Core e-Series UTM bundle. An exceptional value, each package includes:

- **Firebox X Core e-Series X550e, X750e, or X1250e security appliance**
- **Gateway AntiVirus/Intrusion Prevention Service\***
- **spamBlocker\***
- **WebBlocker\***
- **LiveSecurity® Service\***

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

Contact your reseller for details.

\*One-year subscription

For more information on Firebox X Core, 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. ©2006 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, Fireware, LiveSecurity, Core, 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. WGCE66360\_072606