WatchGuard®
PRODUCT DATASHEET

Firebox® X Core™
e-Series

- **Comprehensive protection** keeps your network safe from malicious attacks
- **True zero day attack prevention** proactively blocks new threats
- **New! Built-in SSL VPN**
- **Streamlined network security management** saves you time
- **Continually updated security subscriptions** 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

Earth-friendly technology

Comprehensive Unified Threat Management Solution

Firebox® X Core™ unified threat management (UTM) solutions provide the most complete security in their class, protecting the network from spyware, spam, viruses, trojans, web-based exploits, and other malware. Robust multi-layered protection greatly reduces the time and cost associated with managing multiple-point solutions and significantly increases protection from blended threats. At the same time, advanced networking capabilities managed through an intuitive UI ensure fast, secure business data connectivity in a single, easy-to-use appliance.

Reliable, Multi-Layered Security

The Firebox X Core is built on an intelligent layered 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 Attack Prevention

When security vulnerabilities in software allow new network attacks to be introduced, the proactive defenses of Firebox X Core 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.

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.

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.

- ***Gateway AV/IPS with anti-spyware***
  Stop known spyware, trojans, viruses, and web-based exploits with robust, signature-based protection at the gateway
- ***spamBlocker with virus outbreak protection***
  Get the best anti-spam and email security solution in the industry. Blocks nearly 100% of unwanted email and provides real-time protection against virus outbreaks
- ***WebBlocker***
  Increase productivity and decrease security risks by blocking HTTP and HTTPS access to malicious or inappropriate web content

Secure Remote Connectivity

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

- IPSec
- SSL VPN
- PPTP

Includes single sign-on to streamline authentication.

Expert Guidance and Support

WatchGuard LiveSecurity® Service puts a global team of security experts behind you to help make the complex job of IT management easier. Your LiveSecurity subscription includes a hardware warranty with advance hardware replacement, software updates, rapid-response technical support, up-to-the-minute vulnerability warnings, and innovative educational resources.

Protecting Your Investment

Consider the cost of deploying, managing, and upgrading multiple security solutions, and it's clear why Firebox X UTM solutions provide better value for your dollar. Fully integrated, multifaceted protection on one appliance saves you money on every aspect of ownership, from initial purchase to support contracts.

As needs grow, easily add new capabilities to enhance security. For more capacity, upgrade to a higher model in the line with a simple license key. To meet the needs of more demanding networks, upgrade from Fireware® to Fireware® Pro for expanded networking features including VLAN, high availability, and QoS. All of this is available without buying new hardware. No other products on the market protect your network security investment in so many ways.

Our Commitment to the Environment

WatchGuard creates products that are energy efficient and use recyclable appliance and packaging material. We fully comply with international directives against the use of hazardous substances and have made environmental responsibility an important component of our strategic 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.

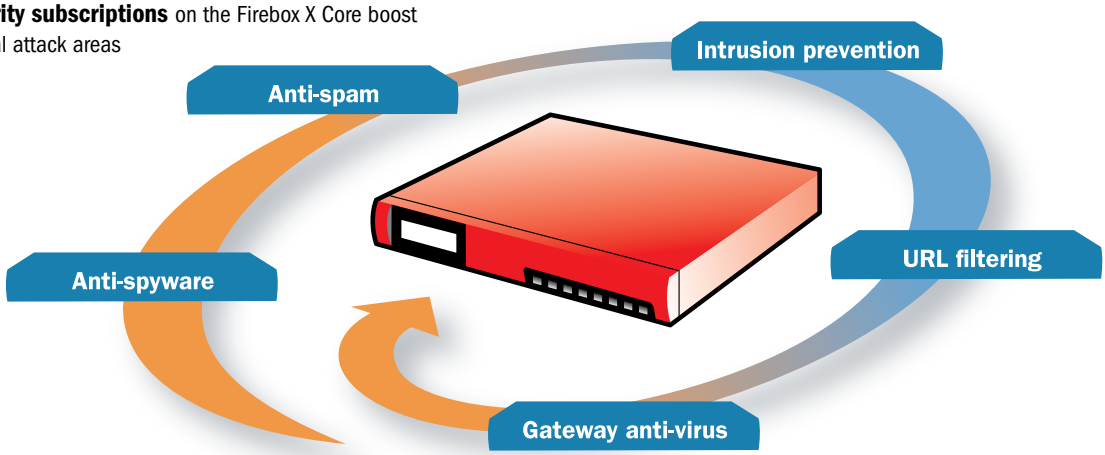
What You Need

- Start with **Firebox X Core** for true zero day attack protection
- 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 AV/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 Core boost protection in critical attack areas



Stopping Email-borne Threats

Your business relies on email. It has to flow smoothly and reliably, without jeopardizing network security. Meanwhile, 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 spyware, worms, viruses, trojans, and other malware
- Enable a **spamBlocker** subscription, the best solution in the industry at distinguishing legitimate email from spam outbreaks in real time. spamBlocker includes a powerful layer of anti-virus protection that can recognize and block email-borne viruses with near 100% accuracy.

How the Protection Adds Up

- **Built-in zero day protection** relies on powerful application proxy technologies to proactively block file types that commonly carry malware payloads via email
- **spamBlocker** uses real-time spam detection so you get immediate protection, stopping unwanted email regardless of message content, language, or format – including image-based spam
- **Spam and AV quarantine** keep spam and suspect email out of your network while providing administrator and users tools to review it
- **Cloaking SMTP** servers prevents hackers from using your system information to attack your network
- **Integrated Gateway AV** gives you more granular file and attachment protection, stopping spyware, viruses, worms, and other malware before they can penetrate the network and disable desktop security applications
- **Outbound email AV scanning** prevents your company from sending spyware, viruses, worms, and trojans to partners, customers, and other recipients outside your network

Specifications

	Firebox® X550e WG50550 X550e UTM Bundle WG50553	Firebox® X750e WG50750 X750e UTM Bundle WG50753	Firebox® X1250e WG51250 X1250e UTM Bundle WG51253
Firewall Throughput†	300+ Mbps	750 Mbps	1.5 Gbps
VPN Throughput†	35 Mbps	50 Mbps	100 Mbps
AV Throughput†	50 Mbps	70 Mbps	100 Mbps
Gateway AV/IPS with anti-spyware	Optional	Optional	Optional
URL Filtering for HTTP and HTTPS	Optional	Optional	Optional
Spam Blocking with virus outbreak detection	Optional	Optional	Optional
Interfaces 10/100	4	8	0
Interfaces 10/100/1000	0	0	8
Serial Port	1	1	1
VLAN Support*	25	25	25
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.)	35/45	100/100	600/600
Mobile VPN Tunnels - IPSec (incl./max.)	5/75	50/100	400/400
Mobile VPN Tunnels - SSL (incl./max.)	1/75	1/300	1/500
Local User Authentication DB Limit	250	1,000	5,000
Model Upgradeable	Yes	Yes	No
Fireware® Pro Advanced Appliance Software	Optional	Optional	Optional

†Throughput rates will vary depending on environment and configuration *Available with Fireware Pro advanced appliance software upgrade

Features

Security Features

- Stateful Packet Firewall
- Deep Application Inspection Firewall
- Application Proxies - HTTP, SMTP, FTP, DNS, TCP, POP3
- Spyware Blocking
- DoS, DDoS, and Progressive DDoS Prevention
- Protocol Anomaly Detection
- Behavioral Analysis
- Pattern Matching
- Fragmented Packet Reassembly Protection
- Malformed Packet Protection
- Static and Dynamic Blocked Sources Lists
- 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 and 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

High Availability**

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

WAN Failover

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

Traffic Shaping**

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

Routing

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

Networking**

- Port Independence
- VLAN
  - Bridging, Tagging, Routed Mode
- Multi-WAN and 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
- 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, v3

Alarms/Notifications

- SNMP
- Email
- Management System Alert

Management Software††

- WatchGuard System Manager (WSM)

Certifications

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

Support & Maintenance

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

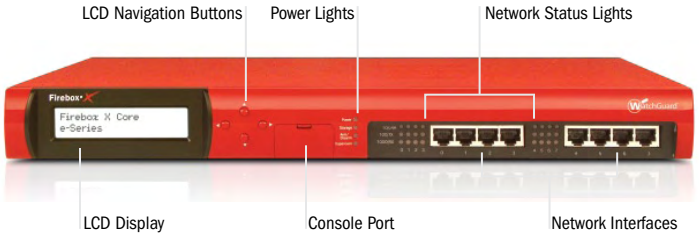
**Available with Fireware Pro advanced appliance software upgrade
††Firebox X 550e comes with a single-node WSM license. To create drag-and-drop tunnels or to centrally manage multiple Firebox X Edge appliances from an X550e, optional WSM upgrade licenses are required.

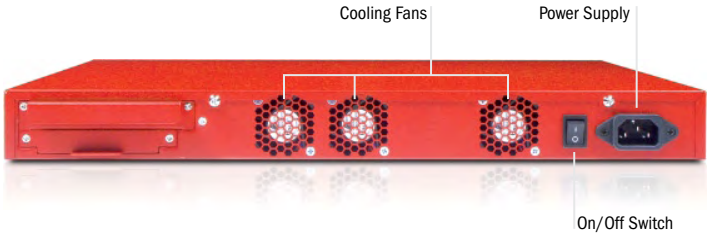
Dimensions and Power

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?

As network needs grow, upgrade your Firebox X Core from Fireware to Fireware Pro advanced appliance software for more demanding networks. Now more powerful than ever, Fireware Pro 10 provides:

- **Traffic Shaping** – 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, plus WAN failover and VPN failover
- **VLAN Support** – Creates logical rather than physical network configurations that reduce hardware requirements, increase control over multiple traffic types, provide richer interoperability, and make it easy to create subnets
- **Multi-WAN Load Balancing** – Distributes and load-balances outgoing traffic across multiple ISPs for greater network efficiency
- **Policy-based Routing** – Allows you to specify outgoing interface per service to enhance network bandwidth management and reduce costs
- **Server Load Balancing** – Makes it easy to protect public-facing e-commerce "server farms"
- **SSL VPN** – Increases the number of SSL VPN tunnels to the maximum available per model

Core™ UTM Bundle – 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 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 Core e-Series 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 Core. Contact your reseller for details.

For more information, 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

COMMON CRITERIA EAL4 CERTIFIED

IPSec *Firewall* *Firewall Level 1* *VPN* *Web Filtering* *Intrusion Prevention* *Anti-Spam*

WatchGuard™