



## Firebox® X Peak™ e-Series Competitive Selling Guide

Firebox® X Peak™, the highest performance line of products from WatchGuard®, delivers the most comprehensive network security in its class. It integrates zero day attack prevention through application proxies, stateful packet firewall and VPN capabilities, anti-spyware, anti-spam with quarantine, anti-virus, intrusion prevention, and URL filtering for a complete unified threat management (UTM) solution. Plus, you get 8 GigE ports and up to 2.3 Gbps firewall throughput!

### KEY SELLING POINTS

- **Stronger security with true zero day protection**
  - What differentiates our security is the comprehensive, proactive approach. Our application proxy technology protects against unknown threats by *only allowing traffic proven clean*. Compare this to the security capabilities of competing products that only partially examine packets, or rely mainly on signatures to protect the network. With Firebox X, you're ready for any attack.
  - Behavioral analysis, protocol anomaly detection (PAD), pattern matching, and other proxy actions deliver proactive protection, greatly limiting vulnerability to many types of attacks.
  - Powerful, fully integrated security subscriptions include WebBlocker, spamBlocker, and Gateway AV/IPS with anti-spyware.
- **Unmatched ease of use**
  - Easy to set up and manage, Firebox X Peak has an intuitive user interface to streamline administration. Includes smart defaults, wizards, and drag-and-drop VPN. No competitor offers drag-and-drop VPN!
- **Centralized management**
  - All security capabilities are controlled from one management console, WatchGuard® System Manager, at no additional cost. Includes flexible policy management and comprehensive reporting.
- **Advanced Networking Features**
  - Fireware® Pro includes advanced networking features to give you the flexibility, redundancy, and reliability required by complex networks.
  - Features include traffic shaping/QoS, high availability (active/passive), multi-WAN failover, VLAN, load balancing, dynamic routing, and SSL VPN.
- **Scalable and upgradeable**
  - Get more performance and security capabilities by applying a simple license key – no hardware to buy.
  - More memory than most competitors; allows plenty of room for feature and capacity growth – unlike many competitors.
- **Best support package in the industry**
  - Hardware warranty with advance hardware replacement, threat alerts, expert advice, technical support, software updates, training, and more!

### COMPETITIVE POSITIONING

#### CISCO ASA 5520

- **Poor Integration:**
  - Can't do IPS and AV at same time
  - ASA 5520 can't have IPS or AV when using 10/100/1000 module
  - ASA product line offers Firewall, IPS, and VPN from three different products. Not well integrated, with separate config and management application for IPS
- **Difficult to use:** Hard to set up and manage – most functions configured through a command line interface
- **Limited functionality:** IPS module scans only packet headers, not data content, so malicious payloads may not be blocked
- **Limited Ports:** The ASA 5520 has only 4 10/100/1000 ports. The Peak appliances have 8 and an option for fiber

#### FORTINET FortiGate 400A, 500A, 800, 1000A

- **No real zero day protection:** Signature-only solution only offers protection against *previously identified* attacks. So, a lapse exists between the time a virus is discovered and a signature deployed. Not proactive, not true zero day protection
- **Weaker management:** Thin management capability through Web-based GUI. Additional multi-box management package is expensive. No interactive, real-time monitoring; no drag-and-drop VPN tunnel creation
- **Performance degradation:** Drops significantly when gateway AV is turned on along with Firewall and VPN; also when other services are enabled

#### JUNIPER SSG 300, 500 Series

- **Reactive, costlier security:** Juniper's Deep Application Inspection is signature-based. Not well integrated
- **Weaker management:**
  - Web-based management is not as robust as WatchGuard System Manager
  - Reporting costs extra and does not provide level of rich and insightful information that WatchGuard System Manager provides with the base product purchase
  - NetScreen Security Manager not included
- **Inferior UTM solution:**
  - UTM features require high memory option
  - Spam protection is not real time
- **"Deep Inspection" limitations:** Not a proxy. Protects against a limited set of *known* attacks
  - No signature updates; most PAD signatures are simplistic bounds-checking

## COMPETITIVE POSITIONING (continued)

### SONICWALL 4100, 5060c

- **Weaker security:**
  - Basic stateful packet filter, signature-based AV and IDS, RBL-based spam blocking
  - No true zero day protection; signatures only protect against previously identified attacks – a lapse occurs
- **Not model upgradeable:** Low port density and no opportunity to grow appliance in the future
- **Not a comprehensive UTM solution:** No integrated spam
- **No integrated SSL** for mobile users

## TARGET CUSTOMERS

**Firebox X5500e** For small businesses/branch offices requiring an integrated security appliance that grows with their needs, along with high performance and advanced networking. Ideal as hub site for larger branch office VPN (BOVPN) and mobile user VPN (MUVPN) installations. Profile: Good for a central location box that hosts SMTP/HTTP/FTP and domain controllers. ~500-850 users.

**Firebox X6500e** For medium businesses requiring multi-layered security, high performance (2.3 Gbps), advanced networking, and centralized management. Profile: Businesses that have multiple SMTP/HTTP/FTP and domain controllers and a larger number of client PCs: ~750-1250 users.

**Firebox X8500e** For medium or distributed enterprises requiring multi-layered security, high performance (2.3 Gbps), advanced networking, centralized management, and remote connectivity. Profile: Larger offices that are hosting webfarms and numerous SMTP servers. Best suited for a NOC for a medium enterprise. ~1200+ users.

## FEATURE COMPARISON AT A GLANCE<sup>†</sup>

Product	Firebox X Peak 5500e 6500e 8500e, 8500e-F	Cisco ASA 5520 Bun K9 5520 AIP 10 Mod 5540	FortiGate 400A 500A 800 1000A	Juniper /NS SSG-320 SSG-350 SSG-520 SSG-550	SonicWALL 4100 5060c
Zero Day Protection	Yes	Limited	No	No	No
Email Virus Outbreak Detection	Yes	No	No	No	No
Real-Time Spam Blocking available	Yes	Included with URL filtering	Yes	Not real time	Separate email appliance
Gateway AV/IPS available	Yes	Choose AV or IPS – not both	Yes	Yes	Yes
Firewall Throughput (Mbps)	2,000+ 2,300 2,300	450 450 650	500 600 1,000 2,000	450 550 650 1,000+	700 2,800
VPN Throughput (Mbps)	400 600 600	225 225 325	140 150 200 400	175 225 300 500	350 700
AV Throughput (Mbps)	140 170 200	Not Published	100 120 150 200	Not Published	Not Published
Concurrent Sessions	500,000 750,000 1,000,000	280,000 280,000 400,000	400,000 400,000 400,000 600,000	48,000 48,000 64,000 128,000	600,000 750,000
Ports 10/100 (incl/max)	0/0 0/0 0/0	1/1 1/1 1/1	4 8 4 0	0/0 0/0 0/0 0/0	0/0 0/0
Ports: Gig E Standard 10/100/1000 (incl/max)	8/8 8/8 8/8	4/4 4/4 4/4	2 2 4 10	4/28 4/44 4/52 4/52	10/10 6/6
Branch Office VPN Tunnels (incl/max)	750/750 750/750 750/750	750 shared 750 shared 5000 shared	2,000 3,000 3,000 10,000	250 shared 350 shared 500 shared 1,000 shared	3,500/3,500 4,000/4,000
Mobile User VPN Tunnels (incl/max)	600/600 600/600 600/600	750 shared 750 shared 5000 shared	2,000 3,000 3,000 10,000	250 shared 350 shared 500 shared 1,000 shared	1,500/4,500 2,000/6,000

<sup>†</sup> Not all competitor product models are available in all regions worldwide