



Firebox® X Core™ e-Series Competitive Selling Guide

Firebox® X Core™ delivers the most comprehensive network security in its class. It integrates zero day protection, application proxy firewall and VPN capabilities, anti-spyware, anti-spam, anti-virus, intrusion prevention, and URL filtering for a complete unified threat management (UTM) solution.

KEY SELLING POINTS

- **Stronger security with true zero day protection**
 - What differentiates our security is the comprehensive, proactive approach. WatchGuard 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 with virus outbreak detection, and Gateway AV/IPS with anti-spyware.
- **Unmatched ease of use**
 - Easy to set up and manage, Firebox X Core 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 Upgrade**
 - Easily upgrade to Fireware® Pro, the advanced appliance software with additional networking features including traffic shaping, high availability, VLAN, and dynamic routing.
- **Scalable and model-upgradeable**
 - Get more capacity and security capabilities by applying a simple license key – no hardware to buy.
- **Best support package in the industry**
 - Hardware warranty, threat alerts, technical support, software updates, innovative training, and more!

COMPETITIVE POSITIONING

CISCO ASA 5500 SERIES

- **Poor Integration:**
 - Can't do IPS and AV at same time
 - ASA 5510 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

- **Limited functionality:** IPS module scans only packet headers, not data content, so malicious payloads may not be blocked

FORTINET FortiGate 100A, 200A, 300A

- **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 thru 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

ASTARO ASG 220, 320

- **Limited Proxies:** Astaro is one of the few proxy-based competitors; however, its proxies are missing key functionality such as command limiting, pattern matching, and protocol anomaly detection. Astaro also does not include a DNS proxy.
 - Limited UTM Functionality: Astaro's UTM services have some serious shortcomings:
 - Anti-spam relies on non real-time technologies, easily subject to evasion via new spamming techniques
 - Anti-spyware is limited to an anti-spyware checkbox in its URL filtering. By contrast, WatchGuard protects against spyware in three distinct ways (URL filtering, IPS signatures, and proxy actions)
- **Limited Centralized Management:** Astaro's Command Center looks impressive, but lacks features:
 - No interactive real-time monitoring
 - No drag-and-drop VPN tunnel creation
 - No one-touch configuration or firmware updates for VPN endpoints

JUNIPER SSG 140

- **Reactive, costlier security:** Juniper's deep application inspection is signature-based. Not well integrated
- **Limited expandability:** Slow CPU and small Flash/RAM may not be able to support additional services/features
- **Weaker management:**
 - Web-based management is not as robust as WatchGuard System Manager (WSM)
 - Reporting costs extra and does not provide level of rich and insightful information that WSM provides with the base product purchase
- **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 2040, 3060, 4060

- **Weaker security:**

- Basic stateful packet filter and signature-based AV and IDS do not provide enough security; new application firewall features cost extra (enhanced OS).
- 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 true UTM solution:** no integrated anti-spam.
- **Logging/reporting cost extra**

TARGET CUSTOMERS

Firebox X550e Ideal for small business stand-alone site that requires affordable, integrated security — or use it to securely connect small branch office to HQ site. Profile: DSL or T1 Connection, possibly direct Internet access, local Internet servers, need proxies and services, locally or remotely administered.

Firebox X750e The right appliance for an SME site that wants a solution that easily scales as business needs grow. Profile: Basic BOVPN needs, standard remote access, public Internet servers (mail, Web, etc), needs proxy protection for servers as well as clients; needs AV, anti-spyware, anti-spam, web filtering. 3 to 10 Mb connection.

Firebox X1250e Good choice for larger SME site with the need for higher performance. Profile: Greater performance needs. May serve as branch office VPN HQ site, remote access hub for >10 users. 3 to 10 Mb connection.

FEATURE COMPARISON AT A GLANCE[†]

Product	Firebox X Core 550e 750e 1250e	Astaro 220 320	Cisco ASA 5510 Bun K9 5510 AIP 10 Mod	Juniper /NS SSG 140	FortiGate 100A 200A 300A	SonicWALL 2040 3060 4060
Zero Day Protection	Yes	Limited	Limited	No	No	No
Email Virus outbreak detection	Yes	No	No	No	No	No
URL Filtering available	Yes	Yes	Yes	Yes	Yes	Yes
Real-Time Spam Blocking available	Yes	No	Incl. with URL filtering	Not real-time	Not real-time	Separate appliance
Gateway AV/IPS available	Yes	Yes	Choose AV or IPS – not both	Yes	Yes	Yes
Firewall Throughput (Mbps)	300+ 750 1,500	260 420	300 300	350	100 150 300	200 300+ 300+
VPN Throughput (Mbps)	35 50 100	150 200	170 170	100	40 70 120	50 75 190
AV Throughput (Mbps)	50 70 100	Not Published	Not Published	Not Published	20 30 70	Not Published
Concurrent Sessions	25,000 75,000 200,000	400,000 550,000	50,000 50,000 (130,000 w/Sec+ license)	32,000	200,000 400,000 400,000	32,000 128,000 500,000
Ports 10/100 (incl/max)	4/4 8/8 0/0	8/8 4/8	3/3 3/3 (5 w/Sec + license)	8	8/8 8/8 4/4	3/4 3/6 6/6
Ports: Gig E Standard 10/100/1000 (incl/max)	0/0 0/0 8/8	0/0 4/8	0/0 0/0 0/0	2	0/0 0/0 2/2	0/0 0/0 0/0
Branch Office VPN Tunnels (incl/max)	35/45 100/100 600/600	unrestricted	250 shared 250 shared	125/125	80/80 200/200 1500/1500	50/50 700/1000 3,000/3,000
Mobile User VPN Tunnels (incl/max)	5/75 50/100 400/400	unrestricted	250 shared 250 shared	50/100 shared 150/400 shared 500/1000 shared	80/80 200/200 1500/1500	10/100 25/500 1,000/3,000

[†]Not all competitor product models are available in all regions worldwide