

# Hotsheet



## Hassle-Free, Universal Access – without compromising security

with **CITRIX<sup>®</sup>** Secure Access

### Firebox<sup>®</sup> SSL Core™ VPN Gateway Offers:

- Dependable, secure access to corporate resources from anywhere, anytime
- Universal access to any application, with no network configuration changes, custom application connectors, or complicated development work
- Streamlined deployment and management for the IT administrator, with no clients to manage; unmatched ease of use for the user

### KEY SELLING POINTS

#### Dependable, universal access

Gives users anywhere access by providing two powerful access modes in one solution to extend the network's reach.

- **Secure Access client mode.** Authorized users connect through an auto-updating, Web-deployed client for an in-office user experience, accessing any application or network resource
- **Kiosk mode.** Authorized users can use Web-enabled handhelds, laptops, desktops, or Internet kiosks, whose browsers support SSL in Java™ or Windows<sup>®</sup> environments, to securely access Web and other supported applications\*, Citrix<sup>®</sup> servers, and other Web-based network resources

Regardless of the mode used, Firebox<sup>®</sup> SSL Core™ VPN Gateway traverses any firewall and supports all major operating systems and protocols including UDP (VoIP), TCP, and IP.

#### One box, no additional adapters

Provides robust, secure access out of the box with streamlined deployment and management, so you get up and running fast – and stay that way.

- No additional components, adapters, or special application connectors are required to get universal network and application access
- No client installation or maintenance is needed – client is automatically deployed and updated whenever users connect to the network

#### Unmatched ease of use for the user

With Secure Access client mode, users have an in-office experience from any location without sacrificing security. Users can easily:

- Work with client/server applications, file servers, printer servers, and any other network resource just as they would when connected to a LAN, without learning new user interfaces
- Map network drives as they would when on the LAN to seamlessly access all of the resources they need

In Kiosk mode, users can access Web applications\*, as well as additional supported applications, from any Web-enabled device, such as PDAs and smart phones, no matter where they are.

\*Must support Mozilla

### Designed For:

- Businesses that need to provide secure, always-on connectivity to applications and corporate resources for up to 205 concurrent remote users
- Workers on the go who require reliable, universal access to the corporate network to stay productive wherever they are
- Organizations that want to be able to safely extend select portions of their network to partners, consultants, and customers around the globe

#### Powerful built-in security

Firebox SSL Core VPN Gateway provides robust security from any endpoint to network resources, from managed and unmanaged devices.

- Verifies security status by checking device attributes including: IP address, firewall settings, operating system, patch level, and status of antivirus software
- Encryption: 196-bit TLS supports all OpenSSL cipher including 3DES and RC4
- Hides IP addresses of remote network to block worm traversal
- Session timeout protects corporate information from unauthorized users
- In Kiosk mode, no data is transferred, so no cache cleaning is required
- Additional security capabilities, including support for two-factor authentication and PEM digital certificates, alleviate security concerns for extending network access

#### Strong administrative control

Granular access controls enable IT administrators to easily deploy and manage user and group access from a single centralized location with integrated logging and reporting. IT administrators can:

- Determine level of trust for the user and the endpoint device
- Assign authentication and authorization to give users and groups levels of network and application access
- Enable or disable split-tunneling and split DNS

#### Lower total cost of ownership

Get the best of IPSec and the best of SSL VPN without the limitations of either, in a one-box solution. Organizations realize tremendous cost savings with:

- No additional adapters, application connectors, or network reconfiguration
- No installation or ongoing maintenance of client software
- Intuitive interfaces for IT administrators to greatly reduce time spent configuring and managing access policies
- Robust support package delivered by LiveSecurity<sup>®</sup> Service experts
- A dramatically lower number of support calls from mobile users
- Built-in desktop sharing for remote help desk support

**When is SSL VPN a better choice than IPsec VPN?**

If you require standard site-to-site VPNs, such as between central and branch offices, IPsec is an excellent choice. It's a proven technology with powerful security capabilities. IPsec, however, is not optimized for mobile usage. Mobile user implementations of IPsec present difficulties for users as firewall traversal is unreliable and the user is tied to a specific machine. The IT administrator also has to deploy and maintain the IPsec client software on their users' devices.

SSL VPN is ideally suited for organizations with many mobile users connecting from varied locations. It provides employees and partners with enormous flexibility to access the network from any location and from any Web-enabled devices whose browsers support SSL in Java™ or Windows® environments, such as laptops, PDAs, and smart phones. It also allows you to securely extend portions of your network to partners, consultants, and customers. In addition, the IT administrator doesn't need to maintain client software on the users' devices. With many SSL VPN products, access is limited to a small number of applications. Firebox SSL Core VPN Gateway overcomes this limitation and offers an in-office user experience from any location with its Secure Access client mode. This makes it the smart choice over other SSL VPN products.

**TECHNOLOGY COMPARISON**

Features	IPsec VPN	Other SSL VPNs	Firebox SSL Core VPN Gateway
Complete network access	✓	limited and costly	✓
All protocols supported	✓		✓
All applications supported	✓		✓
In-office user experience	✓		✓
Traverses any firewall		✓	✓
Clientless access from anywhere*		✓	✓
Prevents worm traversal		✓	✓
Application-level access control		✓	✓
Auto-updated, Web-deployed client**			✓
Always-on capability/persistent connection			✓
Leaves no information behind on public kiosks		optional purchase	✓
Built-in desktop sharing			✓
Built-in endpoint security out of the box			✓
Supports & optimizes UDP traffic, including VoIP			✓

\*In Kiosk mode, authorized users have access to Web-based and supported applications from Web-enabled devices running JVM v 1.2.4 or higher, whose browsers support SSL in Java or Windows environments, such as PDAs and smart phones. Such applications include Citrix® ICA, Remote Desktop, SSH, Telnet 3270 emulator, and VNC clients. Web applications must support Mozilla.

\*\*In Secure Access client mode, authorized users connect through an auto-updating, Web-deployed client to access any application or network resource.

Item Description	SKU
Firebox SSL VPN Gateway Core	WGSSL05
Firebox SSL VPN Gateway 5 Tunnel Pack†	WG018010
Firebox SSL VPN Gateway 10 Tunnel Pack†	WG018011
Firebox SSL VPN Gateway 20 Tunnel Pack†	WG018012
Firebox SSL VPN Gateway 50 Tunnel Pack†	WG018013
Firebox SSL VPN Core 9-Month LiveSecurity Renewal	WG018014
Firebox SSL VPN Core 1-Year LiveSecurity Renewal††	WG018015
Firebox SSL VPN Core 2-Year LiveSecurity Renewal	WG018016
Firebox SSL Core 1-Year LiveSecurity Gold Upgrade	WG018017
LiveSecurity Reinstatement - Firebox SSL VPN Core	WG018018

† Tunnel packs are stackable, maximum 205 concurrent tunnels per appliance  
 †† Refer to WatchGuard's price list for complete LiveSecurity® Service renewal SKUs

Specifications	Firebox SSL Core VPN Gateway
Max tunnel throughput	75 Mbps
Max # VPN tunnels - concurrent	205
Secure Access client mode tunnels/Kiosk mode tunnels	205/3
Processor	1.2 GHz Intel based
Security co-processor	SafeNet SafeXcel-1141
Memory - Compact Flash	64 MB
Memory - RAM	256 MB
Active network interfaces	2 x 10/100
Serial ports	1 DB9
Hard drive included	40 GB
Power supply	100-240 VAC Auto-sensing
Dimensions (height, width, depth) in inches	H: 1.75", W: 16.75", D: 9.75"
Weight	9.3 lbs.
LiveSecurity® Service initial subscription	90 days

**Other products your customers may be interested in**

**Firebox® X Peak™** – Our highest-performance line of integrated security appliances. Capable of gigabit throughput, it has the reliability, redundancy, traffic management, and port density that demanding, high-speed networks require. Optional gateway antivirus, intrusion prevention, and Web content filtering can be added with the activation of a simple license key.

**Firebox® X Core™** – Our best-selling Firebox® X Core™ line of integrated security appliances provides the strongest protection available out of the box for businesses requiring integrated security, ease of use, and the capacity to extend and scale to meet growing needs. Integrated security services like gateway antivirus, intrusion prevention, spam blocking, and Web content filtering provide even greater protection.

**Firebox® X Edge** – Our line of firewall and VPN endpoint security appliances delivers exceptional network protection to small businesses, remote offices, and telecommuters. Optional Web content filtering is available. Firebox X Edge is the ideal endpoint for Firebox X Peak and Core.

**For more information on Firebox SSL Core VPN Gateway visit: [www.watchguard.com/products/fb\\_ssl.asp](http://www.watchguard.com/products/fb_ssl.asp)**

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.

© 2005 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, LiveSecurity, Core, and Peak 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. WGCE66286\_0705



**ADDRESS:**  
 505 Fifth Avenue South,  
 Suite 500  
 Seattle, WA 98104

**E-MAIL:**  
[information@watchguard.com](mailto:information@watchguard.com)  
**WEB:**  
[www.watchguard.com](http://www.watchguard.com)

**US SALES:**  
 1.800.734.9905

**INTERNATIONAL SALES:**  
 +1.206.613.0895

**FAX:**  
 1.206.521.8342