



- **Dependable, universal access** extends your network's reach
- **Reliable performance and capacity** ensures connectivity for remote users
- **Unmatched ease of use** saves time for IT administrators and end users
- **Strong administrative control** is provided through a single, flexible Administration Tool
- **Powerful security** lets users connect without compromising the network

## Extend access to applications and network resources from anywhere – without compromising security

Small- to mid-size businesses face a tough choice when looking for secure remote access solutions. IPSec is a headache to deploy and maintain. Support for remote users can be challenging and costly because of unreliable connections, firewall traversal issues, and client interoperability problems. Many SSL VPN solutions suffer from limitations in what applications and protocols can be accessed and are complex to set up and administer.

Firebox® SSL Core™ VPN Gateway is the hassle-free VPN solution that provides universal access to applications and network resources with no connectors, no modules, no client management issues – no extras to buy.

### Dependable, Universal Access

You get powerful, dependable, and secure access in one solution to extend your network's reach.

- **Secure Access client mode** allows authorized users to connect using a Web-deployed, auto-updating client for a true in-office experience. Includes client failover capabilities to keep remote connections always up and running.
- **Supports major operating systems and protocols** and traverses almost any firewall.

### Reliable Performance and Capacity

While some SSL VPN products claim "unlimited" capacity, in reality their users regularly experience unreliable connections and poor performance. The Firebox SSL Core solution ensures secure, universal connectivity to applications and resources for up to 205 concurrent remote users, with 75 Mbps throughput.

### Unmatched Ease of Use

You get robust, secure access out of the box without additional reconfiguration, development work, or administrative headaches.

- No additional components, adapters, or special application connectors are required to get universal network and application access
- Single sign-on support: HTTP Basic Auth and Windows® Domain
- No client administration – the Secure Access client is Web deployed and auto-updated whenever the user connects to the network
- Intuitive interfaces greatly reduce time spent configuring and managing access policies
- With an in-office experience, users can work as productively as they do when connected to the LAN
- Easy-to-use Administration Tool has drag-and-drop object support

### Strong Administrative Control

Easy yet deep access control enables you to quickly set up and manage user and group access from a single centralized location with integrated logging and reporting.

- Assign access policies for users and groups with robust authentication support
- Control which devices gain network access through built-in endpoint security checks and Application White List controls
- Use advanced networking functions including IP pooling, optional split tunneling, load balance support, and dynamic or static routing to provide needed flexibility for evolving network topologies
- Manage multiple Firebox SSL VPN Gateways in your network from the single Administration Tool

### Powerful Security

Firebox SSL VPN provides robust security from the access device to the network, for managed and unmanaged devices, over most protocols.

- Verifies endpoint security status before allowing network access by checking device attributes including IP address, firewall settings, OS, patch level, and status of anti-virus software
- Encryption: 128-bit/168-bit session length, DES, 3DES, RC4 ciphers, MD5/SHA1 Hashes, SSL v3, TLS v1
- Hides IP addresses of remote network to block worm traversal
- Session timeout protects corporate information from unauthorized users
- Authentication methods and supported directories: server- and client-side digital certificates, RADIUS, RSA SecurID®, LDAP, and Windows® Active Directory
- Can be deployed with a Firebox X Unified Threat Management appliance to add protection from network, application, and content-based attacks

**TECHNOLOGY COMPARISON**

Features	IPSec VPN	Other SSL VPNs	Firebox SSL Core VPN Gateway
Complete network access	✓	optional purchase	✓
Most protocols supported	✓		✓
Most applications supported	✓		✓
In-office user experience	✓		✓
Traverses most firewall		✓	✓
Light desktop client for minimal IT support		✓	✓
Prevents worm traversal		✓	✓
Application-level access control		✓	✓
Auto-updated, Web-deployed client**			✓
Always-on capability/persistent connection			✓
Powerful yet easy-to-use Administration Tool			✓
Built-in desktop sharing			✓
Built-in endpoint security out of the box			✓
Reliable performance and capacity			✓

**Specifications**
**Firebox SSL Core VPN Gateway**

Max tunnel throughput	75 Mbps
Max # VPN tunnels – concurrent	205
Secure Access client mode tunnels	205
Kiosk mode tunnels*	3
Processor	1.2 GHz Intel based
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 in inches	H: 1.75", W: 16.75", D: 9.75"
Weight	9.3 lbs.
LiveSecurity® Service	90 days (initial subscription)

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

SSL VPN is ideally suited for organizations with many mobile users connecting from varied locations.

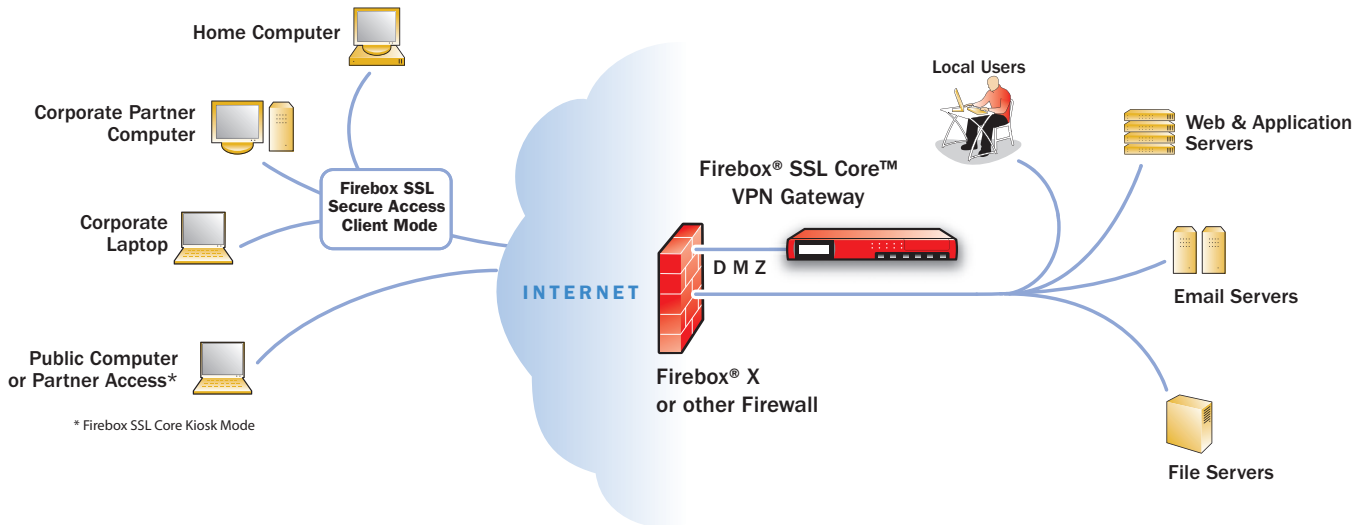
- Provides employees with enormous flexibility to access the network from any location and from Web-enabled devices
- Allows you to securely extend portions of your network to partners, consultants, and customers
- Saves time and money since the IT administrator does not need to maintain client software on the users' devices

\* In Kiosk mode, authorized users have access to Web-based and supported applications from Web-enabled devices running JVM v1.2.4 or higher, whose browsers support SSL in Java® or Windows® environments. 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 using a Web-deployed, auto-updating client to access applications and network resources.

**Firebox® SSL Core Deployment**

Increase secure access – Reduce IT support costs



For more information, visit [www.watchguard.com/appliances](http://www.watchguard.com/appliances)

with **CITRIX** Secure Access

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, LiveSecurity, Core, 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. WGCE66293\_082406