Extend access to any application or network resource from anywhere – without compromising security.

Today, mid-sized enterprises 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, blocked access due to firewall traversal issues, and client interoperability problems. Many current SSL VPN solutions suffer from limitations in what applications and protocols can be accessed and are complex to set up and administer. As IT administrator, you need a dependable solution.

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

Dependable, Universal Access
You get two powerful access modes in one solution to extend your network’s reach.

- **Secure Access client mode.** Authorized users connect using an auto-updating, Web-deployed client for an in-office experience, accessing any application or network resource. It also provides client failover capabilities to keep remote connections always up and running.

- **Kiosk mode.** Authorized users can use Web-enabled handhelds, laptops, desktops, and Internet kiosks whose browsers support SSL in Java™ and Microsoft® Windows® environments, to securely access Web applications, Citrix® servers, and other Web-based network resources.

Regardless of the mode used, Firebox SSL Core VPN Gateway traverses any firewall and supports all major operating systems and protocols including TCP, UDP (VoIP), and ICMP.

Unmatched Ease of Use
You get robust, secure access out of the box without additional costs, reconfiguration, development work, or administrative headaches. 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, maintenance, or support is needed – the client is automatically 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

Powerful Security
Firebox SSL Core VPN Gateway provides robust security from the access device to the network, for managed and unmanaged devices, over all protocols.

- Verifies endpoint security status before allowing network access 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 & RC4
- Hides IP addresses of remote network to block worm traversal
- Session timeout protects corporate information from unauthorized users
- Kiosk mode sessions transmit images, not data – no cache cleaning required
- Additional security capabilities, including support for two-factor authentication and authorized digital certificates, alleviate security concerns for extending network access
- Can be deployed with a Firebox X integrated security appliance to add protection from network, application, and content-based attacks

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. You can:

- Assign access policies for users and groups with robust authentication support including LDAP, Radius, Windows® Domain, and RSA SecurID®
- Control which devices gain network access through built-in endpoint security checks
- Use advanced networking functions including IP pooling, optional split tunneling, load balance support, and dynamic or static routing to provide the flexibility needed for evolving network topologies

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 complex 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
- Built-in desktop sharing for SSL-encrypted remote help desk support
- Comprehensive support package delivered by WatchGuard's LiveSecurity® Service experts
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 such as laptops, PDAs, and smart phones
- 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

For more information, visit www.watchguard.com/products/fb_ssl.asp