



THE NEXT-GENERATION SSL VPN:
HASSLE-FREE, UNIVERSAL SECURE REMOTE ACCESS
AUGUST 2005

THE NEXT-GENERATION SSL VPN: HASSLE-FREE, UNIVERSAL SECURE REMOTE ACCESS

OVERVIEW

Virtual Private Networks (VPNs) have revolutionized the way branch offices and business partners connect back to an organization. VPNs leverage low-cost Internet access to build trusted tunnels between the central office and branch offices or partners over untrusted networks. IPSec, the most widely adopted VPN technology, is designed to provide robust security for data moving between two networks. Yet organizations must also solve the general problem of secure remote access for individuals, not just for networks. Employees and business partners, for example, frequently need to access information remotely, from another private or public network, and are potentially behind other security and firewall equipment themselves. Unfortunately, IPSec VPNs are not well-suited for mobile applications. Most current IPSec Mobile User VPN (MUVPN) technologies will not work reliably for traveling users attempting to connect back to their corporate resources while behind a firewall at a customer or partner site. IPSec MUVPNs also bring along administrative headaches and high support and configuration costs resulting from installing and updating the software client which mimics the network-to-network connection that IPSec was designed to support.

Organizations seeking to solve this problem require secure, authenticated access for trusted persons and organizations, protecting their data as it flows over third-party (untrusted) networks. Furthermore, the ideal solution will be easy to manage, will not be hindered by common firewall configurations, will offer full "on the home network" support for all applications and resources, and be transparent to the end user.

WatchGuard Technologies, Inc. in partnership with Citrix Systems, Inc. has developed the WatchGuard Firebox® SSL VPN Gateway with Citrix® Secure Access. This appliance meets these requirements and more, providing dependable, secure, universal access to network resources with unparalleled ease of use for both IT administrators and their users. Unlike most SSL VPN solutions, the Firebox SSL VPN Gateway requires no special connectors or Webification to support applications, delivering significant administrative time and cost savings while ensuring always-on access to specified network resources and applications by any authorized user.

SOLVING THE MOBILE ACCESS VPN PROBLEM

VPNs were created to solve the problem of establishing secure remote access over untrusted networks. Over the years, organizations have deployed different types of solutions such as the following:

IPSec

This VPN type uses a technique known encapsulation. Encapsulation allows packets from network "A" and destined for network "B" to be encapsulated, encrypted, and sent, on a packet-by-packet basis, to a trusted server on network "B" where the packets are unwrapped and forwarded on to their final destination on network "B". The great advantage to the encapsulation approach is that ALL packets from ALL applications are supported across the tunnel without modification. For mobile applications, IPSec VPNs rely on a "thick" client to initiate and maintain the tunnel.

Drawbacks to Mobile IPSec VPN Solutions

1. Thick-client solutions require an organization to assume a significant support burden to aid end users with installation, maintenance, and troubleshooting which introduces administrative headaches and high support costs to an organization.
2. Most firewalls today use "Network Address Translation" (NAT) to manage their IP address space. NAT relies on rewriting source and destination IP addresses on a per packet basis so that computers using private and public IP addresses can communicate. Because the NAT code is changing the tunnel traffic, the traffic often fails validation at the destination and is discarded. In most cases, NAT prevents the casual use of IPSec MUVPNs by individuals who want to remotely connect to a private network from some other organization. This situation leaves many employees with the inability to access their company network from other organizations they may be visiting, limiting their access to information except when in a more unrestricted environment.
3. IPSec MUVPNs do not enable secure access to a private network from public computers such as kiosks. Kiosk machines will not allow loading and configuring an IPSec client necessary for the mobile user VPN to function.

SSL VPN

Secure Socket Layer (SSL) VPN was initially developed to solve the problem of providing secure access to Web servers (such as E-commerce sites) where it was undesirable to deploy and maintain a thick client. SSL VPNs also can be used to address the issues associated with IPSec VPNs, providing the secure access required by remote workers and business partners over networks that are not compatible with IPSec. SSL however, has problems of its own.

SSL VPN solutions leverage HTTPS connections providing Web portal access to a limited number of Web-enabled applications. The SSL VPN appliances (sometimes called concentrators) do this by parsing and reconstructing the Web application in real time as requests are serviced. By reconstructing the navigation paths, the concentrator successfully mimics the functionality of the Web application behind it without requiring a thick client for access. Since SSL VPNs provide a "clientless" way to access applications that are internal to an enterprise or organization's network (the Web browser is the client), they eliminate or reduce the administrative headaches and high support costs of IPSec VPN clients. The limitation of this approach is that only web applications are supported, greatly limiting the usefulness of the solution compared with IPSec MUVPN.

Client/Server Applications and SSL VPNs

Although SSL VPNs primarily work with Web-based applications, a few SSL VPN vendors have written custom connectors to support a limited number of client/server applications. Custom connectors that are sold by SSL VPN vendors are normally for applications that have a standard (non-customizable) client, such as Microsoft® Outlook®. Since the Outlook 2000 Service Pack 3 (SP3) client is the same for all organizations, it's economical for SSL VPN vendors to develop a custom connector for this application, which can be resold to customers as an add-on. For applications that have a standardized client (such as Outlook), the custom connector approach uses the client that is on the users' PC and creates a protocol-mapping scheme that proxies data exchanges between the client and server. This protocol mapping scheme is specific to the version of software client, and requires that the IT department adapt the network environment, and each laptop to accommodate the proxy and fool the

application. This approach provides the same general level of connectivity for that application as IPsec does, but imposes a performance penalty and requires a management burden equivalent to or greater than that of an IPsec solution.

Other common business applications, such as Sales Force Automation (SFA) tools, Customer Relationship Management (CRM) systems, and Enterprise Resource Planning (ERP) applications, as well as other applications from companies such as Siebel, Oracle, Remedy, Clarify, and SAP, do not have a standard client. Clients for these applications are customized for a particular customer. A Siebel implementation at company A is much different than a Siebel implementation at company B, or at any other company.

For applications that are customized for a specific organization, the SSL VPN vendor can bring in their Professional Services team to create a custom connector or to “Webify” the product. Since the applications are customized for a particular organization, the Webification or creation of a custom connector would also be specific to each customer. The cost of this type of custom programming is significant.

Web-Enabled Applications and SSL VPNs

Many SFA, CRM, and ERP vendors provide a native Web-enabled interface, and it seems attractive to expose this to remote users, bypassing the restrictions on SSL VPNs mentioned previously.

SSL VPNs are essentially a proxy technology, and as such, have to parse and rewrite links to provide access to internal Web applications. This means SSL VPNs can only work with Web components which can be read and rewritten on the fly as needed. Java applets, ActiveX, Flash, and other common Web components are executable binary code, and therefore cannot be rewritten. Unfortunately, many of the stock Web interfaces from SFA, CRM, and ERP vendors contain these structures, preventing them from being accessed through an SSL VPN. Moreover, for the Web applications that *can* be used with an SSL VPN, there is a significant performance degradation due to the computationally intensive process of parsing the Web page, identifying URLs, rewriting and mapping the navigation paths to externally accessible URLs, and then reconstructing all the Web pages for the end user.

DRAWBACKS TO STANDARD SSL VPNS

1. **Split DNS entries** – When connecting to an internal resource, the PC client is looking for an IP address or server name which cannot be seen outside the firewall (SSL VPNs do not provide transparent access like IPsec VPNs); therefore the IT administrator has to set up split DNS entries either on the host or on a DNS server.

For example, an Outlook client is normally set up to look for the Exchange server by name. This server can be easily found and connected to by name if the PC is inside the network. However, for an outside client, this server’s DNS name cannot be resolved as typically there is no externally published DNS entry for internal servers. Even if the entry was published by the enterprise’s public DNS server, the client would not be able to find a route to the private server since, in most cases, the Exchange server would be using a private or unroutable IP address.

SSL VPN vendors solve this issue by requiring an IT administrator to set up split DNS entries where, if the PC

is on the home network, it is routed to the Exchange server. However, if it is not on the home network, it is routed to the SSL VPN loopback address that is running on the PC (they accomplish this by specifying a loopback address like 127.0.0.1 as the IP address for the Exchange server).

Alternatively, some SSL VPN vendors will avoid loopback connectors by pointing PCs outside the private network directly at the SSL VPN server, however this also requires a split DNS entry (namely for PCs outside the network to resolve to the public SSL VPN server).

Each PC that uses the SSL VPN to access the application will have to change the server name on the client to point to the new, split DNS entry (at the time of SSL VPN configuration) or to the application connector, which is part of the SSL VPN Server.

2. **Application performance** - When a PC client is accessing the server application over an SSL VPN, the performance of the application is significantly reduced. This is due to the protocol conversions that have to take place between the PC client and the SSL VPN client and then between the SSL VPN server and the application. Of course, the opposite protocol conversions have to happen on the return trip of information from the application to the application client.

For example, an Outlook client would normally use a MAPI protocol to communicate with an Exchange server. When an SSL VPN is introduced, the Outlook client still communicates via MAPI to the SSL VPN client. The SSL VPN client converts this information into a custom protocol that it uses to communicate with the SSL VPN server. The SSL VPN server then has to convert this custom protocol back into a MAPI protocol that the Exchange server is expecting. The reverse set of protocol conversions happen on the return trip of information from the Exchange server to the Outlook client.

3. **Application upgrades** - Most upgrades to an application require a corresponding upgrade to the SSL VPN. SSL VPNs are sensitive to changes in client server communications protocols. When an application upgrade brings a change in how that application communicates, the SSL VPN that provides access to remote users must adapt to that change.

Returning to the Outlook example: If an organization upgrades the Exchange server from version 5.5 to 2000, the MAPI protocol used between the Outlook client and the Exchange server changes. Since the SSL VPN client and server convert this specific MAPI protocol to the proprietary SSL VPN protocol, the corresponding protocol conversion of the SSL VPN server has to be upgraded. Furthermore, if the MAPI protocol between Outlook and the Exchange server is changed during a Service Pack upgrade (such as SP3 to SP4); the SSL VPN will also have to be upgraded.

4. **Long implementation time and high cost** - Webification is a professional services exercise to provide browser access to a client/server application just so it can be accessed through an SSL VPN.

An SSL VPN Professional Services organization will create an ActiveX, Java applet, or HTML representation of the application that runs in the PC's Web browser. This process will require an implementation of a Web

service that is able to translate the application server's protocol and data to a Web-friendly front-end.

If this Webification takes ten days at a Professional Services rate of \$2000 per day, it would amount to a total of \$20,000 over and above the cost of the product, plus travel and expense costs.

5. **User interface changes** - Employees grow accustomed to existing user interfaces. Developing unnatural browser interfaces for native applications will most likely change the look and feel of the application. This can require organizations to spend significant amounts of time reeducating unhappy users.
6. **Inhibited protocol functionality (such as SMB)** - Just as an unnatural user interface can have an affect on the efficiency of an employee using a Webified application, the same can apply for some of the basic protocol conversions that may come with an SSL VPN.

One example is the SMB (Server Message Block) Protocol. If a user is at his or her desk, mapped network drives are available for accessing or saving files right from even simple applications like Microsoft Word, Microsoft PowerPoint, Microsoft Excel, etc.

Forcing a user that is remote and using an SSL VPN to have to use a Webified file-sharing protocol instead decreases the efficiency of that user, especially if he or she is not a power user.

7. **Real-time traffic (voice or video) is unsupported** - SSL VPNs cannot support real-time traffic such as voice or video, which means users cannot take advantage of soft phones on their PCs or on-line or real-time video training sessions.
8. **Kiosk modes can leave temporary files and cookies** - The way an SSL VPN deals with kiosks is to run a clean-up script at the end of the session to delete any temporary files that may have been opened in e-mail and to delete any cookies.

The problem with this approach is that it fails if the browser happens to crash during the session. If the browser crashes during the session, the clean-up script will not have a chance to work and all the proprietary information that was opened during the session is stored on the kiosk.

9. **Deployment time can be inaccurately represented** - SSL VPN vendors tout a significant reduction in the amount of time it takes to deploy an SSL VPN solution when compared to an IPSec solution. This, however, assumes that there is no customization or professional services work for the SSL VPN vendor to do. Even when using custom connectors, there are issues with split DNS entries that increase the deployment time with both the application and the client.

Webification of an application increases the deployment time even more. In other words, this large reduction in deployment time will be the case when the SSL VPN can be installed with no application or client modification or professional services.

SSL VPNs Summarized

SSL VPN solutions will work from most computers, even behind various firewall configurations. However, they do have drawbacks:

1. SSL VPNs are not a complete remote access solution. They only work for certain types of Web applications, and fail on advanced Web applications that use binary object technology, such as Java applets and ActiveX controls. They are incompatible with client/server applications without using custom connectors or high-cost Webification.
2. SSL VPNs are slow for the limited number of client/server applications they support
3. SSL VPNs are slow for Web applications; the server-side logic involves parsing and rewriting Web applications.
4. SSL VPNs do not allow for peer-to-peer or real-time applications, where two applications need to open separate IP connections with each other to establish data paths so as to allow the peer-to-peer, or even client/server, protocol to work.
5. SSL VPNs provide “unnatural” access to limited applications, instead of access that is similar to what employees experience when at their desk.

Clearly, SSL VPN remote access technology falls short of being able to address all remote access needs.

Prevailing Technologies Fail to Meet the Challenge

IPSec can encapsulate just about any sort of traffic and forward it on to the destination host, giving the user the illusion that they are on the home network. However, it is complicated and costly to deploy and maintain, and is notoriously unreliable when passing through NAT devices, firewalls, and even some ISP networks. SSL on the other hand passes gracefully through almost any network environment by leveraging the ubiquity of Web access, and in many cases requires no additional client-side installation, since most people already have a Web browser. Because of its reliance on Web technology however, SSL presents some serious limitations as well. Performance is a problem due to the need to re-write Web sites on the fly, and Web applications which use binary technologies like Java and Microsoft ActiveX® can't be translated at all. Client/server applications like Microsoft Outlook, CRM Implementations, and databases must all either be Webified or have custom connectors written for them in order to work over the SSL VPN—all at significant cost to the organization.

What is needed is a solution which combines the strengths of each approach while not indulging in the weaknesses of either. While many organizations meet this challenge by using both technologies where they are most appropriate, this approach necessitates parallel infrastructures and inflated support costs, while still not providing seamless access under all circumstances.

THE WATCHGUARD® SOLUTION: THE STRENGTHS OF IPSEC AND SSL WITHOUT THE DRAWBACKS

The WatchGuard® Firebox® SSL Core™ VPN Gateway uses Citrix® Secure Access technology which, while based on SSL VPN technology, combines all of the benefits of IPSec in terms of network connectivity with the SSL VPN ability to gain access from almost any network regardless of firewall or NAT configuration.

A Review of the Needs

A typical end user might state their needs as: "The ability to securely access any protected resource from anywhere" That's a tall order. In the event that the mobile user is borrowing a computer or on a kiosk, the VPN solution must not depend on the ability to install software, as the user may not have permissions on the machine to do so. When the session is over, the solution cannot leave a trace of the end user's presence or activities for someone else to discover. A network administrator would add to this list of requirements that users should be allowed to access no more than they need to. Management would require that the solution not be costly to deploy or maintain. In short, mobile users require a secure, robust, flexible, economical means of accessing the home network while away.

SECURE ACCESS CLIENT: HASSLE-FREE, UNIVERSAL ACCESS

The WatchGuard Firebox SSL VPN Gateway controls connections between end users in the field and the home network. Network traffic destined for the home network is encapsulated in SSL by the Citrix® Secure Access client, a lightweight client automatically downloaded to the end user's browser after authentication. Since the traffic is encapsulated, no special Webification or custom connectors are required to support full network access. Since the traffic is SSL, it's not susceptible to being disrupted by NAT devices or other measures that sabotage IPSec connections. Authentication functions and the Citrix® Secure Access client distribution mechanism are hosted on the Firebox SSL VPN Gateway's secure external Web site.

Gaining Remote Access

First time end users obtain remote access by simply accessing a secure Web URL with their browser. Once connected, clients are prompted for their user name and password over HTTP 401 Basic, Digest, or NTLM authentication. The Gateway then authenticates these credentials with the organization's logon server (such as Microsoft Active Directory, LDAP, or RADIUS), and if the credentials are correct, offers the user the choice of connecting from "my own computer", or "a public computer". If "my own computer" is selected, the Citrix® Secure Access client is downloaded to the end users machine and the connection with the client PC is established. For subsequent connections, the Citrix® Secure Access client is run from the desktop and the authentication performed and connection established without requiring access to the secure Web URL. If "a public computer" is selected, the user is given limited access to the organizations corporate network via Kiosk Mode. This mode is discussed in a later section.

Establishing the Secure Tunnel

Completing the authentication sequence establishes a secure tunnel over HTTPS (port 443 or any other configured port on the gateway) using SSL. Once the tunnel is established, the Gateway sends configuration information to the Citrix® Secure Access client describing the networks that can be reached over the secure connection.

Tunneling Destination Private Address Traffic Over SSL

Once authenticated and properly configured, either all network traffic, or just that network traffic destined for the networks behind the Gateway, is captured and redirected over the secure tunnel to the Gateway's public-facing interface (This option is known as split tunneling and is configurable on the Gateway). All IP packets, regardless of protocol, are captured in this manner and transmitted over the secure link just like an IPSec client would, however

because network routes are not advertised on the client machine, worms cannot use this tunnel to propagate from the client machine back into the corporate network. This is what provides "in office experience" in the WatchGuard Firebox SSL VPN solution.

Terminating the Secure Tunnel and Regenerating Packets on the Private Network

The Firebox SSL terminates the SSL tunnel and accepts any incoming packets destined for the private network. If the traffic meets the authorization and access control criteria, it is first re-written (IP headers are regenerated to appear from the Firebox SSL's private network IP address range, or the client-assigned private IP), then passed into the private network. For circuit-oriented connections, the Gateway maintains a port-mapped NAT table, so that connections can be matched and packets can be sent back over the tunnel to the client with the correct port numbers so they make it to the correct application.

SECURE ACCESS CLIENT: STRONG SECURITY

Configurable "Always-On" Functionality

When the laptop or PC is disconnected from the network, the Citrix® Secure Access client continues to run in memory. This advanced "Always-On" functionality provides user benefits like auto-reconnect (the VPN connection is automatically restored when the network connection returns), remote voice connectivity, remote control of user PCs by the IT department, etc. This mode provides a powerful way to always ensure security over 802.11 networks without having to deploy and maintain a WEP or WPA/PSK environment. This functionality is not currently available in either IPsec or other SSL VPNs.

Integrated Endpoint Security

Integrated Endpoint Security provides continuous, real-time monitoring of items such as file, checksum, and registry checks, as well as whether the endpoint is an approved corporate asset. Access to the corporate network is only allowed if the security policy for the client computer is met and continues to be met during the SSL VPN session. Competing implementations rely on third-party products to provide this functionality, leading to additional costs and integration challenges. Of the few SSL VPNs that can do limited checks as part of the product, the check still occurs only once, and only when accessing their portal of Webified applications. Endpoint Assurance is included with the WatchGuard Firebox SSL VPN Gateway.

Worm Traversal Blocking

Because the network routing information is not propagated onto the client machine from the network over the SSL VPN tunnel, worms cannot use the SSL VPN tunnel to traverse from the client machine back into the corporate network, providing inherently better security.

Remote Control

Integrated remote control eliminates the time and expense of third-party applications such as Microsoft NetMeeting®, Virtual Network Computing, or expensive Web conferencing software in order to access, assess, and repair remote computers. In addition to providing IT and network administrators with improved troubleshooting options, remote control can be used by employees as an on-the-fly collaboration tool. Employees can now share

any desktop application by simply right-clicking on the Firebox SSL Secure Access icon and selecting the person with whom they want to collaborate.

Operation Through NAT Firewalls and Proxies

The Firebox SSL VPN Gateway tunnel is established using HTTPS, Proxied HTTPS, or SOCKS. This makes it firewall friendly and thus allows computers to reliably access private networks from behind another organization's firewalls without requiring reconfiguration of the network or client.

Encryption Algorithms

The Firebox SSL VPN Gateway tunnel is encrypted with SSL/TLS. Whole data streams are encrypted, including any header information, such as the IP header. The Firebox SSL VPN Gateway supports 196-bit encryption, as well as higher or lower bit values set in the certificate. The Firebox SSL VPN Gateway also supports all OpenSSL ciphers: CAST, CAST5, DES, Triple-DES, IDEA, RC2, RC4, and RC5.

Handling Bi-Directional Protocols

FTP and many real-time voice applications require the client to establish a connection with the server, which in turn creates a new connection with the client. For these applications, the Citrix® Secure Access client is able to provide the local application a private IP address which the WatchGuard Firebox SSL VPN Gateway will use on the internal network to maintain bi-directional communications between the client and the server.

Performance and Real-time Traffic

Many applications, such as voice and video, are real-time, and therefore implemented over UDP. With these applications, it is more important to deliver packets in real time than to ensure that all packets are delivered. However, with any tunneling technology over TCP, such real-time performance requirements cannot be met.

The WatchGuard Firebox SSL VPN Gateway overcomes this issue by routing UDP packets over the secure tunnel as custom IP packets that do not require TCP acknowledgements. Even if the packets get lost in the network, there is no attempt made by either the client or the server applications to regenerate them, so real-time (UDP-like) performance is achieved over a secure, TCP-based tunnel.

The Secure Access Client Approach

The WatchGuard Firebox SSL VPN Gateway provides secure remote network-level access to an organization's networks and all applications, over SSL/TLS. This application is appropriate for employees accessing the organization remotely and for intranet access from restricted LANs such as wireless networks and client sites.

With the WatchGuard Firebox SSL VPN, features such as Always-On roaming, integrated endpoint security, and remote control are integrated into the product, instead of requiring point product purchases for these requirements.

KIOSK MODE

The Kiosk Mode is designed to provide access to corporate resources from public computers such as those found in Internet café's or libraries in addition a range of other devices such as PDA's which can support a Java Virtual Machine.

Application Support

In Kiosk mode, the Firebox SSL provides access to Citrix ICA, Remote Desktop, SSH, Telnet 3270 emulation, VNC servers and one-click access to shared network drives. Access can be controlled on a per-group basis.

Gaining Remote Access

End users obtain remote access by simply accessing a secure Web URL with their browser. Once connected, clients are prompted for their user name and password over HTTP 401 Basic, Digest, or NTLM. The Firebox SSL then authenticates these credentials with the organization's logon server (such as Microsoft Active Directory, LDAP, or RADIUS), and if the credentials are correct, offers the user the choice of connecting from "my own computer", or "a public computer". If "a public computer" is selected, the user is given limited access to the organizations corporate network via Kiosk Mode.

Operation

In Kiosk mode, the Firebox SSL opens a Virtual Network Computing (VNC) like connection in a window. The Firebox SSL sends images only (no data) over the VPN connection. As a result, there is no risk of leaving temporary files or cookies on the public computer

- For computers running Windows 2000 and above, kiosk operation is available through the Access Portal. The kiosk link can be removed from the Access Portal on a group basis.
- For computers running a JVM 1.4.2 or higher (such as Macintosh or Windows 95/98 computers), kiosk operation is available through a Java applet.
- For Macintosh, Safari is the supported browser.

SUMMARY

IPSec and SSL VPNs each have inherent advantages and disadvantages. To meet the challenge of economical, secure, mobile remote access, organizations need the advantages of both these types of products, with none of their disadvantages. The WatchGuard Firebox SSL VPN Gateway with Citrix® Secure Access provides enterprises and organizations with the advantages of both IPSec VPNs and SSL VPNs, without the shortcomings—replacing the need for pure IPSec or SSL VPN solutions.

Where IPSec VPN solutions provide network-layer access and encryption, and SSL VPNs provide application-layer access and encryption, WatchGuard combines network-layer access with application-level encryption in a hybrid technology. This dramatically improves the end user experience, while significantly reducing the IT security administrator's support overhead and security.

THE NEXT-GENERATION SSL VPN: HASSLE-FREE UNIVERSAL SECURE REMOTE ACCESS

The WatchGuard Firebox SSL VPN Gateway offers:

- Hassle-free universal secure access for all applications, including real-time & VoIP
- Unmatched ease of use
- Strong Security and Administrative control
- The lowest TCO in its class

Freedom and Productivity

IPSec and SSL VPNs both have inherent advantages and disadvantages, but the WatchGuard Firebox SSL VPN Gateway with Citrix® Secure Access provides organizations with the best of both worlds. By providing the combined advantages of IPSec and SSL into a single product that is easy to install and maintain, the Firebox SSL VPN Gateway keeps business moving with an unmatched secure remote access solution, with absolutely no need for any additional connectors or Webification.

For more information about WatchGuard Security Solutions, visit us at www.watchguard.com, or contact your reseller.

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

E-MAIL:

information@watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.521.8340

FAX:

+1.206.521.8342

ABOUT WATCHGUARD

Since 1996, WatchGuard® Technologies has provided award-winning network security solutions to customers worldwide. Our Firebox® X family of integrated security appliances delivers the industry's best combination of strong security, ease of use, and expert guidance and support, while our Firebox SSL VPN Gateway provides dependable, universal, secure access to corporate resources from anywhere, at any time. LiveSecurity® Service, the most comprehensive bundled support offering in the industry, offers up-to-the-minute security warnings, software updates, technical support, advance hardware replacement, training and tutorials, and self-help resources. Our commitment to performance and value gives our customers enterprise-grade protection in a cost-effective, expandable solution.

FOR MORE INFORMATION

Please visit us on the Web at www.watchguard.com or contact your reseller for more information.

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, Core, and LiveSecurity are either registered trademarks or 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. WGCE66307_0805