Secure Remote Access
Give users “in office” remote access—anytime, anywhere

June 2008

Introduction

As organizations strive to increase productivity, secure remote access to network resources becomes increasingly important. It is an ideal way to ensure your employees remain connected and productive wherever they may be. WatchGuard® SSL provides secure remote access that delivers an “in-office” experience from any location. The benefits this can provide your organization include:

• Access to real-time or up-to-the-minute information for better decision making
• Increased responsiveness to customers and business issues
• Increased productivity
• Ability to offer flexible working hours and telecommuting

Figure 1: WatchGuard® SSL gives users access to business applications and mission-critical data—anytime, anywhere
Entry-to-Exit Security for Users

WatchGuard SSL enables businesses that are interested in opening up their systems for remote access, but not sure where to start or how to proceed. WatchGuard SSL uses a six-step process to ensure workers are connecting securely and safely, thus protecting the organization as well as the individual. These six steps include:

1. Assessment of end user devices
2. Authentication of identity
3. Authorization to access applications
4. Access through an encrypted connection
5. Audit of user activity and history
6. Abolishment of user session data

Figure 2: The 6 A’s of entry-to-exit security; the major capabilities necessary for secure application access

Assessment of End User Devices

In order to prevent the introduction of malware to the corporate network, remote end-user devices must be checked for integrity to ensure health and policy compliance. As threats to devices increase, this is a crucial step in providing in-depth security. WatchGuard SSL device assessment includes the following:

Deep Device Examination – Pre-connection scanning of every device (e.g., laptop or PDA) to ensure policy compliance. Attributes can include network interface information, application, file or operating system requirements. For example: is up-to-date anti-virus installed on the user’s endpoint?

Access Client Security (Application Control) – Only approved applications are granted access to the network. This results in tighter control over user activities on the network.

Figure 3: Application control enforces policy to regulate which applications are allowed to participate on the network
Access Client Security (Network Control) – Allows administrators to specify and regulate how traffic is routed during a session, thus protecting against external connections through the device into the corporate network. For example:

- Allow traffic to the WatchGuard SSL Access Point and block all other traffic
- Allow traffic to the WatchGuard SSL Access Point and to other destinations
- Allow traffic to the WatchGuard SSL Access Point on a selected network interface, while routing other traffic through other interfaces

Real-Time Scanning – Continuous scanning of the device throughout a session protects against remote devices that become non-compliant or violate policy during a session.

Heterogeneous – ActiveX and Java support means examination of a broad range of devices.

Authentication of Identity

Identities can be faked or stolen, which is why organizations must have bullet-proof authentication in place to ensure sensitive data is not compromised. WatchGuard SSL provides strong authentication with the following benefits:

Mobile Two-Factor Authentication – By using a consumer device the user already owns, such as a mobile phone, PDA, or BlackBerry, users can generate a unique one-time password (OTP). Deploying two-factor authentication becomes convenient and fast. This also lowers costs by removing the need to acquire specialized proprietary hardware.

![Figure 4: By using mobile devices (phones, PDAs, BlackBerrys), organizations can save money on deployment costs and optimize ease of use](image)

Web-based Key Pad Authentication – Unique one-factor authentication protects the user and organization from trojans and spyware.

Reduced Sign-On – Access to resources without having to re-authenticate improves the user experience.

3rd Party Authentication Support – WatchGuard SSL supports up to 14 different authentication methods including token-based solutions from RSA, Vasco, and VeriSign. WatchGuard SSL makes it easy to leverage the investment you’ve made in an existing authentication mechanism.

Federated Identity – By using the SAML (Security Assertion Mark-up Language) 2.0 standard, one digital identity can be used to access multiple domains without the need for extra and costly user enrolment. This is ideal for business-to-business partnerships, as well as mergers and acquisitions.

Authorization to Access Applications

WatchGuard SSL features a sophisticated policy engine and authorization model. Access decisions can be more sophisticated than simple allow or deny entry policies. Access can be granted based on a number of different characteristics including:

- **User Device** – Grant access based on device type (PDA, Laptop, PC, etc.).
- **Authentication Level** – Grant access based on authentication level (two-factor or one-factor).
• **User Role** – Grant access based on who the user is (e.g., marketing, sales, engineering, or finance; employee, partner, or customer).

• **Network** – Grant access based on whether or not the network is trusted or unknown.

• **Point of Entry** – Grant access based on which WatchGuard SSL Access Point is used (e.g., London, New York, Tokyo).

• **Wireless Connection** – Grant access based on wired or wireless network.

WatchGuard SSL can use one or more of these access decisions to grant a user access, allowing for very granular policies.

---

**Figure 5:** Granular policies allow you to grant users access to the resources they need

---

**Access through an Encrypted Connection**

Securing the communication between your remote users’ devices and the applications or data they access is critical in ensuring a secure and productive working environment. WatchGuard SSL helps optimize the user experience with the following:

• **Clientless SSL VPN** – WatchGuard SSL removes the need to install proprietary software on remote devices and uses standard web browsers (e.g., Internet Explorer, Firefox, Safari) for access. This results in users having access from any location and any device. Users still have access to all applications and data through an encrypted connection. WatchGuard SSL deployment and ongoing support are made easier by eliminating the requirement to install software on remote devices.

• **Strong Encryption** – WatchGuard SSL utilizes industry standard encryption to ensure users’ communications are safe from eavesdropping hackers.

• **User-Friendly Portal** – WatchGuard SSL creates a device friendly portal to present a user’s applications and resources. Reduced sign-on allows the user to log on once and have access to everything in the portal. The portal auto-detects the device being used and adapts the browser-based portal accordingly.
Figure 6: The look and feel of the WatchGuard SSL portal can be customized. This provides users an easy way to access applications and resources – all with the click of a mouse

- **Broad Application Side** – WatchGuard SSL supports all applications including Web-based, client/server, mainframe, terminal server, and file servers.

- **Built-in Business Continuity/High Availability** – Each WatchGuard SSL Access Point can be mirrored at no additional cost. This guarantees 24x7 access.

**Audit of User Activity and History**

and corporate governance it is imperative that you know who did what, when and where. WatchGuard SSL includes an array features that help organizations meet compliance regulations, including:

- **Consolidated audit** – WatchGuard SSL collects all identity and access activity (user or system-based) in a central repository for easy access. This results in quick and in-depth insight into the activities across the organization. WatchGuard SSL is fully compliant with Sarbanes-Oxley, Gramm-Leach-Bliley, HIPAA, Basel II, and 21 CFR Part 11, among many others.

- **Comprehensive audit** – In-depth audit of device assessments, authentication, and access collected in a secure, central location. Find out exactly who did what, when, where, and how.

- **Graphical reports** – All information in the WatchGuard SSL audit logs can be shown in many different graphical formats (pie charts, line charts, 3D charts, bar charts, etc.) in both real-time and over a historical period. Reports can be run in these different categories:
  - Assessment
  - Authentication
  - Authorization
  - Access

- **Audit**
- **Abolish**
- **System health**
- **Performance**

- **Exportable reports** – For further data mining and asset management, WatchGuard SSL can export audit data to Excel or Crystal Reports.
Abolishment of User Session Data

Session clean-up must be performed to protect remote users’ devices. It is a critical step in ensuring entry-to-exit security, and keeping any malicious threats from entering the enterprise. WatchGuard SSL ensures devices are completely protected by removing the following upon session completion:

- Cookies
- URL history
- Cached pages
- Registry entries
- Downloadable components
- Downloaded files

More Information
For more information about WatchGuard and the WatchGuard SSL solution, visit www.watchguard.com.

ABOUT WATCHGUARD

Since 1996, WatchGuard Technologies has provided reliable, easy to manage security appliances to hundreds of thousands of businesses worldwide. Our Firebox X family of unified threat management (UTM) solutions provides the best combination of strong, reliable, multi-layered security with the best ease of use in its class. Our newest product line – the WatchGuard SSL – makes secure remote access easy and affordable, regardless of the size of your network. All products are backed by LiveSecurity Service, a ground-breaking support and maintenance program. WatchGuard is a privately owned company, headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. For more information, please visit www.watchguard.com.

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.

©2008 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard Logo, Firebox, 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. WGCE66559_062308