



WatchGuard® SSL 2.0 – New Features

For Secure Remote Access, Identity Management, and Network Access Control

Introduction

WatchGuard® SSL 2.0 unifies identity and access management capabilities, with features focused on the integration between the two. WatchGuard SSL 2.0 makes it easier for enterprises to control who has access to what resources at any given time, with powerful integration tools, enhanced security, and reporting technology. This includes:

- Introduction of access client security (WatchGuard SSL ACS)
- Enhanced endpoint security with Java and ActiveX controls
- In-depth graphical reporting tools for increased operational insight
- Introduction of alerts enabling alarm triggers to be set on system events
- Support for federated identities using the SAML standard
- Device-adaptable application portal
- Multi-domain support allowing per domain configuration and customized graphical interfaces
- Mid-point security

WatchGuard SSL Access Client Security (ACS)

WatchGuard SSL 2.0 introduces a feature called WatchGuard SSL access client security (ACS). The ACS consists of three types of controls and is an integrated part of the WatchGuard SSL access client, greatly enhancing security with:

- Network control
- Application control
- End user session notification

Network Control

Network control allows the system administrator to define how incoming and outgoing requests are to be handled. In combination with the enhanced application connectivity and the network control, system administrators can define split-tunneling handling in a number of ways, such as:

- Route all traffic through the WatchGuard SSL access point and WatchGuard SSL access client
- Only route traffic with an internal destination and stop any traffic on other network interfaces – this means that a user can only be connected to resources published by WatchGuard SSL. For example, a user would be able to connect to WatchGuard SSL, but not browse the Internet at the same time.

- Only route traffic with an internal destination through the WatchGuard SSL access point and WatchGuard SSL access client and route other traffic through additional interfaces.

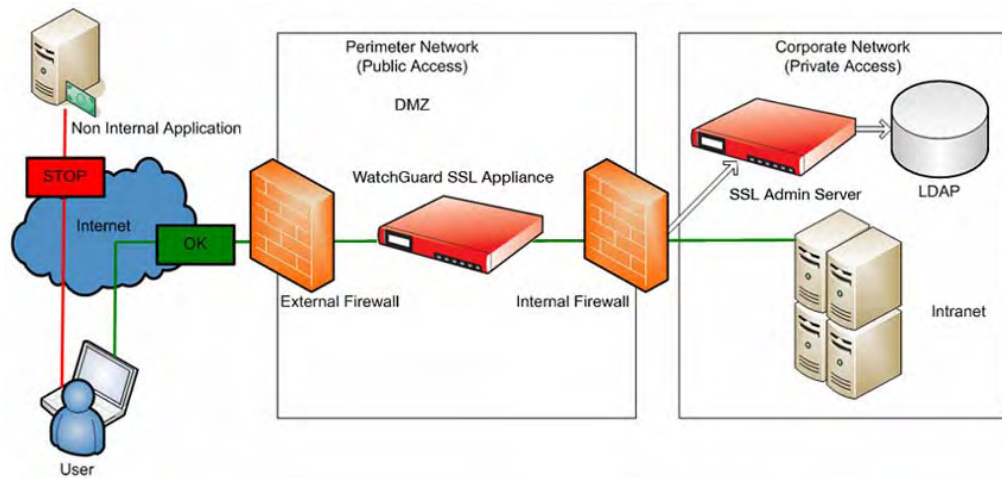


Figure 1: An example where the user is only allowed to reach internal applications and non-internal traffic is blocked.

Application Control

Application control allows the system administrator to define which applications are entitled to use a specific connection. The process includes validation of the application name, location, and checksum. Unauthorized applications are denied access to internal resources.

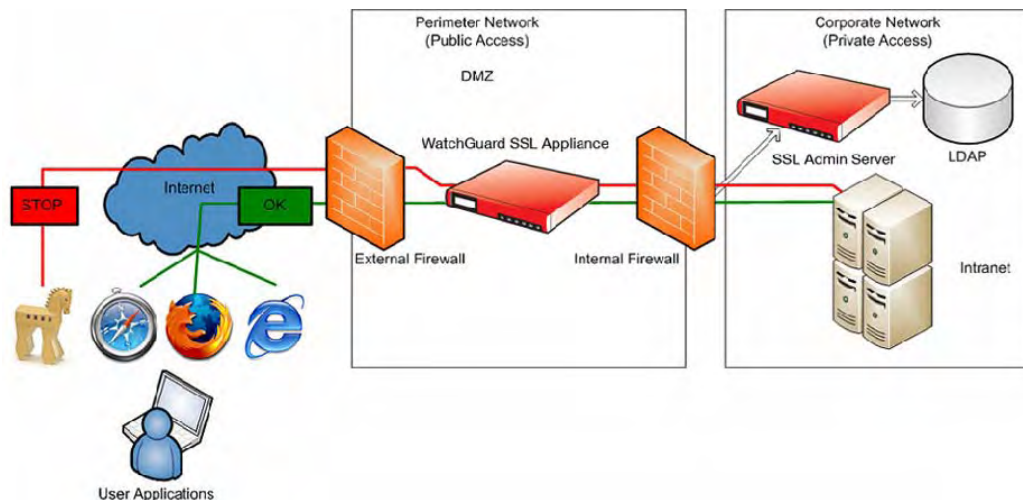


Figure 2: Using application control makes it easy to allow only certain applications access, for example Internet Explorer, Safari, and Firefox, while trojans trying to initiate a connection are stopped.

End User Session Notification

The system administrator can further increase the security by turning on end user session notification. When end user session notification is turned on the user will be forced to accept each new connection that the WatchGuard SSL access client initiates, similar to how personal firewalls work.

Enhanced Endpoint Security

WatchGuard SSL 2.0 includes many endpoint security options including:

- Cross-platform support (ActiveX and Java)
- Separation of device assessment and session clean-up
- Real-time session scanning for continuous security
- New plug-in architecture to support dynamic extensions

Cross-Platform Support

The endpoint security option in WatchGuard SSL 2.0 includes support for more browsers on more platforms than any other product in its class. WatchGuard SSL 2.0 endpoint security supports the following web browsers:

- Internet Explorer
- Firefox
- Opera
- Safari
- Netscape

WatchGuard SSL 2.0 endpoint security supports the following operating systems:

- Windows 2000, Windows XP, Windows 2003, Windows Vista
- Linux
- Mac OS X

WatchGuard SSL 2.0 supports both ActiveX and Java loaders to invoke the endpoint security control on the client, which ensures that Windows users who are not allowed to run ActiveX can still perform an endpoint security scan for optimal protection. This means that device assessment and session clean-up can still be performed on devices with restrictions.

Separation of Assessment and Abolishment

In WatchGuard SSL 2.0 the assessment piece (endpoint security policy decision) and abolishment (session clean-up) are separated modules allowing better policy enforcement. In WatchGuard SSL 2.0, it is also possible to use abolishment as a policy decision on a per application/resource basis.

Real-Time Scan

The assessment phase in WatchGuard SSL 2.0 can be configured to run continually while a user is connected to the application portal, thus making real-time security scans at intervals throughout the session possible. This is important for protection against policy violations that occur after the initial assessment has been performed.

Plug-in Architecture to Support Dynamic Extensions

Extensibility in endpoint security is very important and WatchGuard SSL 2.0 features an architecture allowing for dynamic extensions to both client and server modules, making the possibilities endless. On the server side, modules are often policy validation-focused, such as technology that checks whether or not a range of anti-virus software is updated and running on the client. On the client side, plug-ins are used to expand the gathering of detailed data and extend client platform support.

Graphical Reporting

WatchGuard SSL 2.0 delivers extensive built-in graphical reporting tools that are easily accessed through the WatchGuard SSL administration service. Reports offer another level of insight into who, what, where, and when the system has been used. This is critical for regulatory compliance and corporate governance.

Authentication Requests

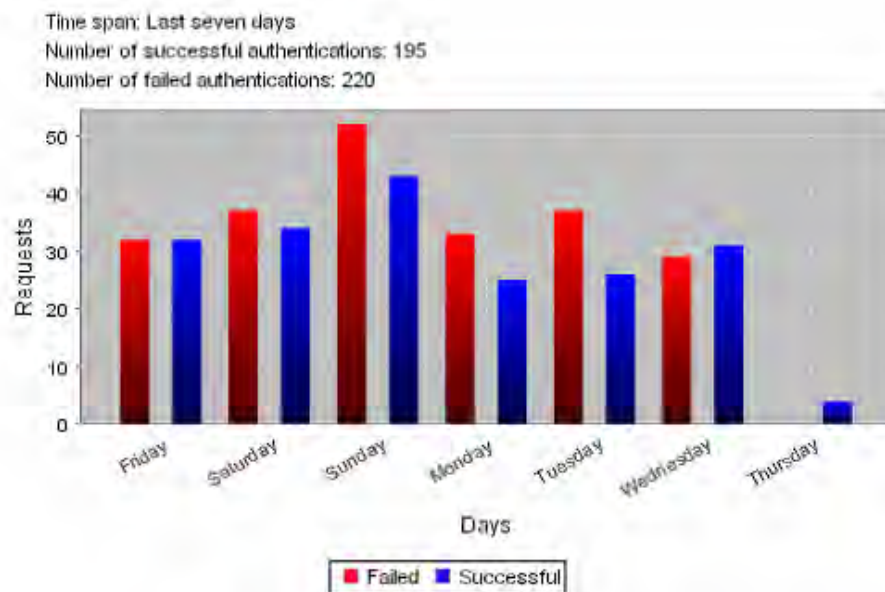


Figure 3: Reporting tools provide the electronic evidence corporations need to show due diligence in compliance efforts.

Granular filters can be applied that enable administrators to create customized reports in both real time or over a historical period for trend analysis. Real-time reports are useful for immediate corrective action, while historical reports are useful for future planning.

Seven Categories of Reports

WatchGuard SSL 2.0 includes seven standard categories of reports:

- **Assessment Reports** - Provides reports on assessments (endpoint security checks) that have been performed.

- **Authentication Reports** - Provides detailed reports on the use of authentication methods.
- **Authorization Reports** - Provides reports on access decisions that have been made by the WatchGuard SSL policy service.
- **Access Reports** - Provides reports on application access and the use of the WatchGuard SSL platform by end users. Filters can be applied to find out how many individuals are using a specific application.
- **Audit Reports** - Provides in-depth reports on who, what, when, and how access was granted.
- **Abolish Reports** - Provides reports on any session clean-up actions that have taken place.
- **System Health and Performance Reports** - Provides reports on system-specific events and statistics.

Alerts

Alerts can be set on system events so administrators can be notified if something occurs, making problem resolution easier and less time-consuming. This tool enables administrators and help desk personnel to work proactively and more quickly respond to incidents.

Alerts can be distributed using either SMS (mobile text message) or email.

The following alerts can be set in the system:

User Accounts

- Account locked for access (User id and reason)
- Account unlocked for access (User id and reason)
- Account locked for authentication (User id and reason)
- Account unlocked for authentication (User id and reason)
- Account Time-lock locked (User id, reason, and time-locked limit value)
- Account Time-lock unlocked (User id and reason)

Resources

- Resource host unreachable (Resource host and reason)
- Resource host reachable (Resource host and reason)

System

- Lost connection to service in WatchGuard SSL network (Display name and reason)
- Connection to service in WatchGuard SSL network restored (Display name and reason)
- Lost connection to Directory Service (Reason)
- Connection to Directory Service restored (Reason)
- Lost connection to Authentication Method Server (Server host and reason)
- Connection to Authentication Method Server restored (Server host and reason)
- Security Issues (Security issue)

Alerting Example

Juan is trying to access the WatchGuard SSL portal, but his password is rejected. Juan tries to login several times, but each time the password is rejected.

1. Juan's account is locked.
2. WatchGuard SSL sends an alert to the system administrator that Juan's account has been locked.
3. The system administrator unlocks the account and resets his password.
4. The system administrator calls Juan to tell him that his account is active and his password has been reset.
5. Juan successfully logs in.

Shared Identities across Domains with Federation

Single sign-on across domains and enterprises are considered by many organizations to be the holy grail of IT because it simplifies the user experience, while maintaining high levels of security. With the introduction of the Secure Assertion Mark-up Language (SAML) there is now no obstacle to sharing identities and achieving seamless single sign-on for users.

WatchGuard SSL 2.0 provides support for the SAML 2.0 standard supporting both ID-producer and ID-consumer mode, allowing internal users to access external services and external users to access internal applications without any additional sign-on or enrolment requirements.



Figure 5: Federated identity allows a single digital identity to be used to access multiple departments, or even businesses, without the need for extra and costly user enrolment. Ideal for sharing identities in B2B partnerships

The promises of federated identities across systems include:

- Scalable and global single sign-on for convenience and reduced administration
- Eliminated user enrolment and enrolment automation for low-cost management
- Enhanced security with high usability

Adaptive Portal

The WatchGuard SSL 2.0 application portal has the ability to adapt to screen resolutions of different devices which improves the usability for individuals with handheld devices. By auto-detecting the type of device the user has, WatchGuard SSL 2.0 automatically adapts the application portal to match the form factor and screen resolution of the device.

Enhanced Multi-Domain Support

WatchGuard SSL 2.0 delivers enhanced support for deployments where multiple domains are in use (i.e., different URLs). With WatchGuard SSL 2.0 it is possible to apply different graphical interfaces depending on the domain the user requests. This is ideal for service providers and enterprises seeking to offer different interfaces to different services and audiences, such as intranet and extranet access.



Mid-Point Integrity

In the early stages of wireless networks security was not the primary concern for network connectivity, but because of widespread adoption it has become increasingly important as security threats like Evil Twin threatens the usability of users and enterprises. WEP is commonly used as one security enforcement method but has proven to be insufficient. Neither hidden SSIDs, nor MAC filtering has proven sufficient for securing wireless environments.

WatchGuard SSL 2.0 introduces support for WPA (Wi-Fi Protected Access) authentication by using the RADIUS PEAP-MSCHAPv2 authentication protocol, which is supported by many operating systems, wireless access points and platforms. By using PEAP-MSCHAPv2 it is possible to mutually authenticate the wireless access point and the Wireless Client.

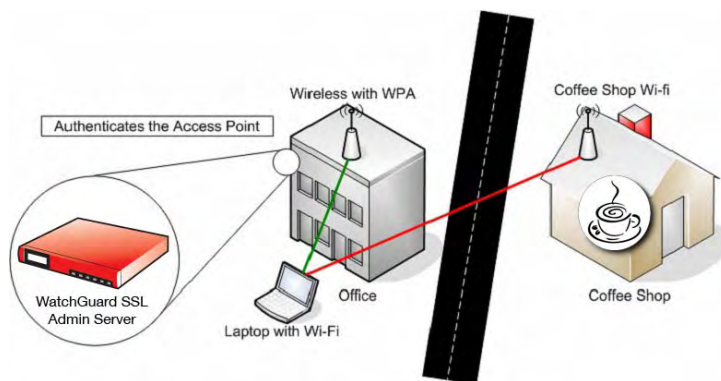


Figure 6: The WatchGuard SSL implementation of WPA uses server-side certificates to allow the client to authenticate the Wireless Access Point and WatchGuard SSL Authentication Service, but does not require deployment of certificates at the client side. Instead the standard WatchGuard SSL Mobile ID can be used to authenticate the end user.



Summary

WatchGuard SSL makes it easy for enterprises to maximize security, while minimizing risk and costs. Whether you deal with internal employees, partners, or customers, you need to provide security that is easy to use and comprehensive. WatchGuard SSL 2.0 delivers the most advanced features to secure your enterprise, so you can feel safe in all your transactions.

More Information

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

ADDRESS:

505 Fifth Avenue South
Suite 500
Seattle, WA 98104

WEB:

www.watchguard.com

U.S. SALES:

+1.800.734.9905

INTERNATIONAL SALES:

+1.206.613.0895

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. WGCE66561_062408