

# Product Introduction Bulletin

## SonicWALL 4.0 Release

4.0 Release Version (2/22/10 Update)



---

### SonicWALL SSL VPN 4.0 Key Investments

---

The SonicWALL SSL VPN 4.0 release provides a best of need solution that focuses on ease-of-use, flexibility and innovation for SMB customers with the following new features.

1. Virtual Access
2. Web Application Firewall
3. NetExtender Re-architecture
4. SNMP Support
5. Unified Policy

The SonicWALL SSL VPN 4.0 beta release is available for SSL VPN 2000, SSL VPN 4000 and SRA 4200 appliance customers.

---

### Virtual Assist

---

**Virtual Access:** This new Virtual Assist feature allows users the ability to access their personal computers located outside the LAN of the SRA appliance. By installing the application on a Windows PC with Internet access and can also communicate to the SRA appliance, that computer becomes available for users access to view the desktop and have mouse/keyboard control (Windows only). Note that a Virtual Assist license is required to use Virtual Access.

*Benefit:* Provides an easy to use mechanism for remote users to connect to an unattended Windows device, which is great for employees that work outside of the LAN and have the need to connect back to their Windows device on occasion.

#### **Additional Enhancements:**

**Trusted Permission Mode:** Now the default behavior upon connection. Users will not be prompted prior do doing actions such as file transfer when trusted mode is enabled.

**Unattended Mode:** When Unattended Mode permission is granted, technicians may have unrestricted access to the end user's machine. This includes access to the system when the end user is not present. A password set upon starting the mode will restrict access to the system from other technicians.

**Reboot & Reconnect:** Reboot and automatic reconnection of the remote system can now be accomplished without the need for the end user's participation (Windows only).

**Request Help Button:** New portal option makes it very easy to configure the portal with a 'Request Help' button, making it very easy for end users to understand how to request assistance.

---

### Web Application Firewall (WAF)

---

**Licensable Web Application Firewall:** The proliferation of Web 2.0 applications has propelled the Worldwide Web as a critical platform for businesses and consumers. However, its recent popularity has also made it a new threat vector of choice and Web-based attacks are rising at an alarming rate. Web Application Firewall is a new subscription-based service that employs a dynamically updated signature database to protect against modern, web-based threats. With the 4.0 release, the Web Application Firewall moves from a technology preview feature to a fully supported and licensable feature (*Available in the April 2010 price book*).

*Benefit:* Detects and protects Web applications (including the SSL VPN appliance itself) from Web-based attacks, reducing potential losses and adhering to data protection compliance mandates

#### **Additional Enhancements:**

**Automatic Signature Updates:** Allows for real time protection by allowing administrators to select that signatures be updated automatically. Signatures are used to protect Web applications from potential vulnerabilities.

**Cross-Site Request Forgery Protection:** Administrators can enable protection for Web sites against Cross-Site Request Forgery attacks.

# Product Introduction Bulletin

## SonicWALL 4.0 Release



**Information Disclosure Protection:** The Web Application Firewall can be configured to prevent sensitive information from being revealed from Web sites that go through the WAF. Administrators can select keyword or phrases that if detected in the website, access to that site will be blocked.

**WAF Session Management:** The Web Application Firewall can be configured to force the display of the logout Dialog Window for any Web page accessed using the WAF.

**Removed Reboot Requirements:** Administrators no longer need to reboot the SSL VPN appliance after making any changes to the WAF > Settings and WAF > Signatures sections.

**Hiding Threat Information in URL:** The WAF no longer will display any of the threat information in the URL when blocking access. Displaying this information could be considered as a vulnerability.

---

### NetExtender Re-architecture

The Windows NetExtender client has been redesigned with a new look and feel. Moreover, the underlying technology now implements a custom-dialer that allows it to be launched from the Windows "Network Connections" menu. This change allows NetExtender to be connected before the Windows domain login. Additionally, the Mac and Linux NetExtender clients have been redesigned with the same look and feel of the Windows NetExtender client.

*Benefit:* User interface standardization across all SSL VPN clients creates a unified look and feel and the new technology supports domain login scripts

---

### SNMP Support

SonicWALL SSL VPN devices will support Simple Network Management Protocol (SNMP) which will report remote access statistics.

*Benefit:* Facilitates network management for administrators as they can leverage standardized reporting tools

---

### Unified Policy

All granular bookmarks and policies are now displayed single page, providing for a single place to manage all SSL VPN policy.

*Benefit:* This reduces the administrative overhead in configuring and troubleshooting policies in multiple locations.

---

### Additional Features

**Authentication enhancements:** Users can now change their password when they are part of an Active Directory domain. Passwords can be changed before or after expiration. Users will also be notified when their password is about to expire.

Additional authentication enhancements include: Active Directory nested group support and TLS/SSL support for LDAP/AD

**One Time Password (OTP) enhancements:** Administrators can now configure the OTP password length to be anywhere between 4 and 14 characters in length. Administrators can also now configure the email subject and message body, including the ability to use Active Directory based variables in the subject or body of the OTP message.

**Reverse Proxy enhancements:** Backend Web servers using NTLM or Windows Integrated Authentication are now supported, including support for SSO with NTLM. Reverse proxy bookmarks now support HTTP 1.1. protocol and connection persistence.

**External Web Site Bookmarks:** Bookmarks for external public Web sites can now be created, useful for public Web sites frequently accessed by the organization.

**Citrix XenApp Server enhancements:** Support for Citrix XenApp Server 5.0

**IPv6 enhancements:** RDP and VNC bookmark support