

Overview and FAQ

Announcement Overview: SonicWALL SSL VPN Series Recent News

The SonicWALL SSL VPN Series, featuring the SSL-VPN 200, SSL-VPN 2000 and SSL-VPN 4000, provides organizations of all sizes with affordable, simple and secure clientless remote access and support solutions that require no pre-installed client software. Utilizing only a standard Web browser, users can easily and securely access e-mail, files, intranets, remote desktops (includes both full desktop and individual application access) and other resources on the corporate LAN from any location. SonicWALL Virtual Assist, a licensable add-on module for the SSL-VPN 2000 and 4000 appliances, enables a technician to assume control of a customer's PC or laptop in order to provide assistance. With no need for a pre-installed or "fat" client, administrators are freed from the tasks of deploying, configuring and updating software, reducing maintenance and support costs. SonicWALL SSL VPN Series solutions integrate seamlessly into virtually any network topology to deliver powerful, scalable and affordable remote access to corporate resources.

Recent News

Below a list of enhancements in firmware version 3.0.0.0 release for the SSL-VPN 200, 2000 and 4000 platforms (unless otherwise noted). Detailed descriptions can be found in the release notes.

Admin Portal Enhancements

- **Redesigned Graphical User Interface** — The SSL VPN administrative interface has a new look and feel that is consistent with the updated SonicOS Enhanced 5.0 management interface.
- **Self-Refreshing Status Pages** — The **Users > Status** and **NetExtender > Status** pages now use AJAX to continuously display the most current information.
- **Mouse-Over Tooltips** — Tooltips pop up with useful information when the mouse cursor hovers over a checkbox, text field, or radio button in the administrative interface.

License Manager Enhancements

- **SonicWALL License Manager** — Allows the SonicWALL SSL VPN appliance to communicate directly with the SonicWALL licensing server. The License Manager runs on the SSL VPN appliance and communicates periodically (hourly) with the SonicWALL licensing server to verify the validity of licenses. The License Manager also allows the administrator to purchase licenses directly from MySonicWALL or turn on free trials to preview a product before buying.

Virtual Assist Enhancements *

- **Technician Anywhere Support** — Allows the Technician to connect to the SSL VPN appliance without first starting NetExtender.
- **Customer Status: Active or View Only** — View Only prevents conflicting inputs from both the technician and the customers. Active allows the customer to have control on the session.



Overview and FAQ

- **Customer Hotkeys** — Customers can now use keyboard shortcuts for chatting (Alt+c) and disconnecting (Alt+q).
- **Technician Shortcuts** — Technicians can now use shortcuts for certain operations on the customer's computer including opening the Task Manager and Start Menu on the customer's computer.
- **Customer Computer Specification** — Allows the technician to view the customer's PC information.
- **Optional Email Notification to Technician** — When customers request support, the admin now has the option to send notification emails to a pre-configured list of Technicians.
- **Improved Logging and Reporting** — A new **Virtual Assist > Log** page in the SSL VPN administrative interface is now available, and more fields have been added to the **Virtual Assist > Settings** page. The Technician's activities while servicing the customer are now fully logged.

NetExtender Enhancements

- **64-bit Vista Support for Windows NetExtender Client** — NetExtender now supports 64-bit Windows XP and 64-bit Windows Vista as well as 32-bit Windows 2000, XP, Server 2003, and Vista.
- **OpenSUSE Linux NetExtender Support** — SSL VPN 3.0 supports NetExtender on OpenSUSE in addition to Fedora Core and Ubuntu. An i386-compatible Linux distribution is required, along with Sun Java 1.4+.
- **Setup Enhancements for Mac and Linux NetExtender Clients** — The Virtual Office portal now provides seamless NetExtender installation, connection, and upgrading of Mac and Linux NetExtender clients. A NetExtender RPM package is available for installation on Linux.
- **Usability Improvements for Mac NetExtender Clients** — A Menu Extra is now provided on Mac systems to indicate NetExtender connection status and provide quick access to connect, disconnect, or exit actions.
- **RSA Two-Factor Authentication for Mac and Linux NetExtender Clients** — Mac and Linux clients now support RSA two-factor authentication similar to the Windows NetExtender client and the portal.

Reverse Proxy Enhancements

- **HTTP(S) Caching*** — The reverse proxy is allowed to cache HTTP(S) content on the SSL VPN appliance which an internal Web server deems cacheable based on the HTTP(S) protocol specifications.
- **Remote Gzip Compression**** — Compressing content sent from the SSL VPN saves bandwidth and results in higher throughput.
- **Per HTTP(S) Bookmark SSO Support** — Administrators and users can now enable, disable, and configure custom Single Sign-on credentials for HTTP(S) bookmarks.
- **Replicon Timesheet Support**** — The Timesheet, Reports, and Configuration sections of the Replicon Timesheet application is supported in SSL VPN 3.0 via reverse proxy.

Miscellaneous Enhancements

- **One Time Password Enhancements** — The administrator can customize the email subject and body text.
- **Scheduling and SMTP Authentication for Sending Logs** — In SSL VPN 3.0, the administrator can schedule a day and hour at which to email the event log. SMTP authentication is now supported when sending the log files, in addition to the previously supported POP authentication.
- **Port-Based Policies** — Port-based policies are now available for all services including NetExtender and



Overview and FAQ

HTTP bookmarks.

- **Remote Desktop Protocol Client Enhancements** — SSL VPN 3.0 introduces new options for RDP5 ActiveX and RDP5 Java bookmarks such as redirect drives, redirect printers, redirect ports, and redirect smartcards. RDP5 Java bookmarks will now attempt to run the native Windows mstsc.exe if it exists to give a full-featured RDP experience with Java.

* Only licensable on the SSL-VPN 2000 and 4000 platforms

** Only available on the SSL-VPN 2000 and 4000 platforms



Overview and FAQ

SonicWALL SSL VPN Hardware SKU information:

Product	SonicWALL SKU
SonicWALL SSL-VPN 200	01-SSC-5947
SonicWALL SSL-VPN 2000	01-SSC-5953
SonicWALL SSL-VPN 4000	01-SSC-5961

SonicWALL SSL VPN Support SKU information:

Product	SonicWALL SKU
Dynamic Support 8x5 for SSL-VPN 200 (1 Year)	01-SSC-5642
Dynamic Support 8x5 for SSL-VPN 200 (2 Years)	01-SSC-6244
Dynamic Support 8x5 for SSL-VPN 200 (3 Years)	01-SSC-6245
Dynamic Support 24x7 for SSL-VPN 200 (1 Year)	01-SSC-5643
Dynamic Support 24x7 for SSL-VPN 200 (2 Years)	01-SSC-6246
Dynamic Support 24x7 for SSL-VPN 200 (3 Years)	01-SSC-6247
Dynamic Support 8x5 for SSL-VPN 2000 (1 Year)	01-SSC-5646
Dynamic Support 8x5 for SSL-VPN 2000 (2 Years)	01-SSC-6236
Dynamic Support 8x5 for SSL-VPN 2000 (3 Years)	01-SSC-6237
Dynamic Support 24x7 for SSL-VPN 2000 (1 Year)	01-SSC-5647
Dynamic Support 24x7 for SSL-VPN 2000 (2 Years)	01-SSC-6238
Dynamic Support 24x7 for SSL-VPN 2000 (3 Years)	01-SSC-6239
Dynamic Support 8x5 for SSL-VPN 4000 (1 Year)	01-SSC-6248
Dynamic Support 8x5 for SSL-VPN 4000 (2 Years)	01-SSC-6249
Dynamic Support 8x5 for SSL-VPN 4000 (3 Years)	01-SSC-6250
Dynamic Support 24x7 for SSL-VPN 4000 (1 Year)	01-SSC-6251
Dynamic Support 24x7 for SSL-VPN 4000 (2 Years)	01-SSC-6252
Dynamic Support 24x7 for SSL-VPN 4000 (3 Years)	01-SSC-6253

SonicWALL Virtual Assist SKU information:

Product	SonicWALL SKU
Up to 1 concurrent Technician tunnel	01-SSC-5957
Up to 2 concurrent Technician tunnels	01-SSC-5958
Up to 4 concurrent Technician tunnels	01-SSC-5959
Up to 6 concurrent Technician tunnels	01-SSC-5960
Up to 10 concurrent Technician tunnels	01-SSC-5961
Up to 25 concurrent Technician tunnels	01-SSC-5962

- Please note that maximums of 4 and 25 concurrent technicians can be licensed on the SSL-VPN 2000 and 4000 appliances, respectively.
- Support for SonicWALL Virtual Assist is included with the support purchased for the appliance on which the add-on is enabled

To purchase SonicWALL SSL-VPN solutions, contact a SonicWALL-certified reseller. To find a reseller in your area, please visit <http://www.sonicwall.com/howtobuy/index.html#europe> or call SonicWALL at any of the following numbers:



Overview and FAQ

- Benelux
+32.11.300.615
- UK & Ireland
+800 CALLSNWL
+32.11.300.610
- Nordic Regions
+32.11.300.613
- Germany, Austria & Switzerland
+800 CALLSNWL
+32.11.300.611
- Italy
+32.11.300.616
- France, Spain and Portugal
+800 CALLSNWL
+32.11.300.609

SonicWALL SSL VPN Series Sales Q&A Section:

Q: What are the main differences between the SSL-VPN 200, SSL-VPN 2000 and SSL-VPN 4000?

A: The SSL-VPN 200, SSL-VPN 2000 and SSL-VPN 4000 are very similar remote access solutions with two key differences. First, the SSL-VPN 200 utilizes a compact, desktop form factor whereas the SSL-VPN 2000 and SSL-VPN 4000 are larger 1U rackmount appliances. Second, while all three support any unrestricted number of concurrent user connections, each has a different recommended count. SonicWALL recommends a maximum of 10 concurrent user connections for the SSL-VPN 200, making it an ideal remote access solution for organizations with 50 or fewer employees. Similarly, SonicWALL recommends a maximum of 50 concurrent user connections under typical usage conditions for the SSL-VPN 2000, making it an outstanding remote access solution for organization with 500 or fewer employees. For mid-to-large enterprises, SonicWALL recommends a maximum of 200 concurrent user connections for the SSL-VPN 4000, making it the ideal choice for organizations with more than 500 employees. Unlike the SSL-VPN 200, the SSL-VPN 2000 and SSL-VPN 4000 tout a graphical usage monitoring page and the option to create a system backup on the appliance. In addition, the SSL-VPN 2000 and SSL-VPN 4000 offer a variety of features that are not available on the SSL-VPN 200 including SonicWALL Virtual Assist, Citrix support, Vasco support, multiple IP range support for NetExtender and more.

The following table describes the key differences between SSL-VPN 200, SSL-VPN 2000 and SSL-VPN 4000.

Positioning	SSL-VPN 200	SSL-VPN 2000	SSL-VPN 4000
Target Customer (No. of employees)	Small organizations (less than 50)	Mid-size organizations (less than 500)	Mid-to large enterprises (more than 500)
Recommended maximum number of concurrent users	10	50	200
Concurrent User License	Unrestricted	Unrestricted	Unrestricted
Maximum Number of Virtual Assist Technician Tunnels (requires add-on license)	Not Available	4	25
Hardware			
Chassis Form Factor	Desktop Unit 7.45 x 4.55 x 1.06 in 18.92 x 11.56 x 2.69 cm	1 U rack-mountable 17.00 x 10.00 x 1.75 in 43.18 x 25.40 x 4.45 cm	1 U rack-mountable 17.00 x 13.25 x 1.75 in 43.18 x 33.66 x 4.45 cm



Overview and FAQ

Interfaces	(5) 10/100 Ethernet	(4) 10/100 Ethernet, (1) Serial port	(6) 10/100 Ethernet, (1) Serial port
Processor	SonicWALL security processor, cryptographic accelerator	x86 main processor, cryptographic accelerator	P4 Celeron main processor, cryptographic accelerator
Memory (RAM)	128 MB	512 MB	1 GB
Flash Memory	16 Mb	128 Mb	128 Mb
Power Supply	20W, 12VDC, 1.66A	Internal	Internal
WEED Weight	2.0 lbs 0.91 kg	8.8 lbs 3.99 kg	13.0 lbs 5.90 kg
Total Weight	3.0 lbs 1.36 kg	14.8 lbs 6.71 kg	18.5 lbs 8.39kg
MTBF	9 years	11.2 years	9.2 years
Key Features*			
Standalone NetExtender client and MSI Installer	x	x	x
NetExtender domain suffix, proxy server and NT domain logon script support	x	x	x
Mac/Linux NetExtender Clients	x	x	x
NetExtender Comprehensive Log System	x	x	x
NetExtender Standalone Upgrade Feature	x	x	x
Reverse Proxy: Windows Sharepoint 2.0 support*	x	x	x
Single sign-on bookmark policy options	x	x	x
Email log capability	x	x	x
LDAP Multiple OU support	x	x	x
Support for changing passwords for LDAP domains	x	x	x
Multiple RADIUS server and group support	x	x	x
RADIUS CHAP, MSCHAP, MSCHAPv2 support	x	x	x
SSHv2 support	x	x	x
RDP ActiveX RDP6 support and proxy support	x	x	x
Variable Bookmark Entries based on user name	x	x	x
Reverse Proxy support for URL/Port-based Policies	x	x	x
Reverse Proxy Variable Response Size support	x	x	x
ViewPoint/ GMS Reporting support**	x	x	x
Tokenless two-factor authentication	x	x	x
Vasco support	x	x	x
Port-based policies	x	x	x
RSA support	-	x	x
Citrix (ICA) support	-	x	x



Overview and FAQ

NetExtender: support for multiple IP ranges and routes	-	X	X
Optional client certificate support	-	X	X
Graphical usage monitoring	-	X	X
Option to create system backup	-	X	X
Reverse Proxy: OWA premium version and Lotus Domino Web Access 7.0	-	X	X
RADIUS test function	-	X	X
Active Directory Groups support	-	X	X
Virtual Host/ Domain Name support	-	X	X
FileShares Java Applet	-	X	X
Diagnostics: DNS lookup and Traceroute	-	X	X
SonicWALL Virtual Assist	-	X	X
Reverse Proxy support for Java applets and Flash	-	X	X
Multiple IP addresses support for Web Server	-	X	X
Customizable Logo per Portal	-	X	X
HTTP(S) caching	-	X	X
Remote GZIP compression	-	X	X

Note: includes v3.0 firmware update on SSL-VPN 200, SSL-VPN 2000 and SSL-VPN 4000

* Only limited support for Sharepoint-compatible application integration. Microsoft Outlook is supported.

** Requires ViewPoint/GMS 4.1

Q: When should I sell the SSL-VPN-200 versus SSL-VPN-2000 or SSL-VPN 4000?

A: The following table summarizes when to sell the SSL-VPN 200 versus the SSL-VPN 2000 or SSL-VPN 4000.

Target Customer	What to recommend	Why
Small organizations with 50 or fewer employees	SSL-VPN 200	Supporting a maximum of 10 concurrent users and offered at an affordable price, it provides a cost effective alternative to traditional remote access products for small sized organizations.
Mid-size organizations with 500 or fewer employees	SSL-VPN 2000	Supporting a maximum of 50 concurrent user connections, it provides an easy-to-use, affordable secure remote access solution for mid-sized organizations.
Mid-to-large enterprises with 500 or more employees	SSL-VPN 4000	Supporting a maximum of up to 200 concurrent user connections, it provides rock-solid enterprise-class remote access for mid-to-large enterprises.

Q: Does the end-user need to download and install a client on their laptop?

A: No. SonicWALL SSL VPN appliances do not require the administrator or end-user to download and install a software client for secure remote access. With no need for a pre-installed or "fat" VPN client, administrators are freed from the



Overview and FAQ

tasks of deploying, configuring and updating software, thus reducing maintenance and support costs.

Q: Does every user have a personalized portal?

A: Yes. SonicWALL SSL VPN appliances feature a customizable Web interface that provides each user with a personalized portal experience, displaying only those resources that are available to the user based on company policy.

Q: Will the appliances work in non-SonicWALL environments? Are there added benefits if placed behind a SonicWALL firewall?

A: SonicWALL SSL VPN appliances integrate seamlessly into any network topology and can be easily deployed alongside virtually any third-party firewall as a secure remote access solution. This enables IT administrators to leverage the existing network infrastructure without the need to purchase additional hardware. Additionally, when deployed with a SonicWALL TZ or PRO Series Internet security appliance running the SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service¹, the SSL VPN Solutions provide enhanced network integration and security benefits. Incoming HTTPS traffic is seamlessly forwarded by a TZ or PRO Series security appliance to the SSL VPN appliance. Operating in single-arm mode, the SSL VPN appliance takes on the burden of decrypting and authenticating network traffic. Depending on specific policies, the SSL VPN appliance either denies or authorizes the user to gain access to critical resources, adding a new level of security. Allowed traffic is forwarded back to the PRO or TZ Series security appliance where it is fully inspected for viruses, worms, Trojans, spyware, malicious mobile code (MMC) and other sophisticated threats by the SonicWALL deep packet inspection engine and then forwarded to its final destination on the network. By deploying SonicWALL NetExtender and Network Anti-Virus plus Anti-Spyware¹ on managed remote client machines, administrators can configure policies that require and enforce that every computer accessing the network has the most recent version of anti-virus and anti-spyware software installed and active.

Q: What is Tokenless two-factor authentication (One-time passwords) and how does it work?

A: One-Time Passwords (OTP) provide additional security for user authentication by protecting against identity thefts caused by key loggers. This feature, a form of two factor authentication, requires the use of a one-time password in addition to a user's default credentials for login. After a remote user enters his or her regular user name and password, the user receives via email to a PC or mobile phone, a temporary one time password that is generated by the SSL VPN appliance. This one-time password needs to be entered into the Virtual Office login interface for additional security before the user can gain full access to all the applications behind the corporate network.

Q: What is SonicWALL NetExtender technology?

A: The SonicWALL SSL VPN Series make remote access incredibly simple. Remote users require only a standard browser to launch a personalized Web portal that is unique to that user. From this portal, the user has access to e-mail, files, applications and internal Web sites. For more powerful capabilities such as seamless, secure access to any resource on the corporate network including servers and complex or home-grown applications, the appliances transparently push a downloadable thin client called NetExtender to the user's desktop or laptop. NetExtender technology provides enhanced capabilities such as support for legacy applications; remote desktops, services and any TCP/IP based applications on the corporate network.

Q: Where can I find more information on the SonicWALL SSL VPN Series?

Additional information on the SonicWALL SSL VPN Series is available at: <http://www.sonicwall.com>

Q: What form of support is included with my SonicWALL SSL VPN Series appliance?

¹ Sold separately



Overview and FAQ

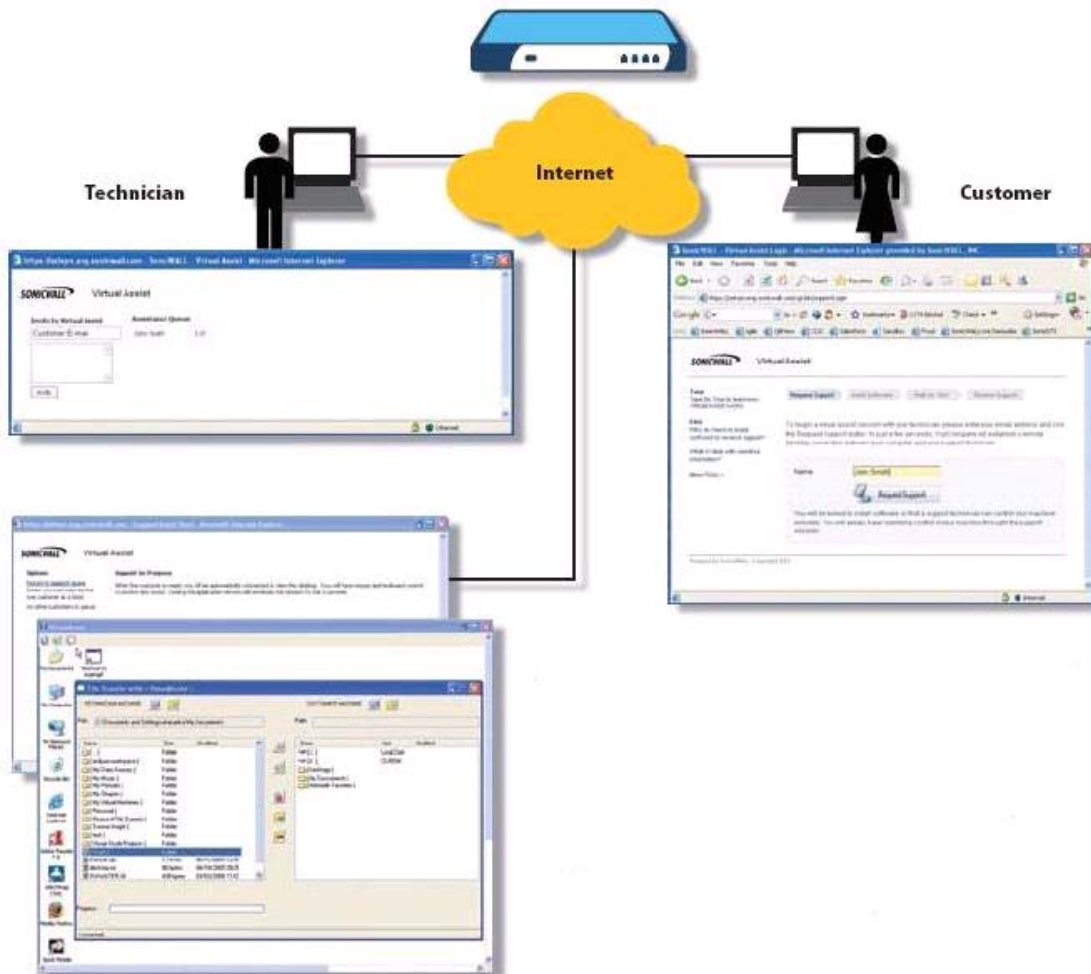
A: All SonicWALL SSL VPN appliances come with a standard warranty, which includes 1-year advanced hardware replacement (return to factory), 90-day email and telephone support, and 90 days of software updates. Extended support contracts are available in 8x5 and 24x7 (local time) and include advanced hardware replacement and software updates. (Note: 8x5 support available in US, Canada, Europe and Japan. 24x7 support available in US, Canada and Europe only). Extended support contracts can be purchased for a one, two, or three time period.

Q: How does SSL VPN compare with IPSec VPN for remote access?

A: With an SSL VPN, end-user access is restricted unless authorized. With IPSec VPNs, users are authorized unless restricted. Combining the restrictive access and clientless convenience, SSL VPN can secure all data streams between the user and network, while IPSec VPN remains a proven solution to protect data streams from network to network. SSL VPN can be considered a complimentary solution to IPSec VPN, rather than a competing one.

IPSec VPN is best suited for site-to-site VPNs - sharing all network resources with trusted branch offices whereas SSL VPN is suited for a diverse community of users – employees, telecommuters, partners, customers etc. with varying degrees of access. SSL VPN also represents the lowest support cost option for remote access as it does not require the need to pre-install and pre-configure a client on the remote machines.

Q: How does SonicWALL Virtual Assist work to provide clientless remote support?



Overview and FAQ

1. Technician Logs in to support Web portal to monitor queue or invite a specific customer via e-mail.
2. Customer logs on to portal and requests help or accepts the e-mail invitation.
3. Meanwhile, the thin client is pushed seamlessly through the browser to the Technician and Customer via a Java launcher. This install can also be done manually in the absence of a JRE.
4. Technician sees Customer in queue and requests access to computer.
5. Customer gives permission and remote support session begins. The Technician now actively controls the remote computer. The Customer is able to see what the Technician does on the screen.
6. The Technician or Customer may end this session at any point in time by clicking the “End Virtual Assist” button.