Technical FAQ

SSL-VPN | SonicWALL SSL-VPN 200 / 2000 / 4000 FAQ

Introduction

This document provides FAQs for the SonicWALL SSL-VPN 200, 2000, and 4000 platforms. This document contains the following subsections:

- Features
  - 3.0 Firmware Release
  - 2.5 Firmware Release
  - 2.1 Firmware Release
  - 2.0 Firmware Release
  - 1.5 Firmware Release
- Prerequisites
- Certificates and Certificate Authorities
- General
- NetExtender
- Virtual Assist
- Hardware
- Contacting Technical Support

Features

What are the new features available in the 3.0 firmware release for SSL-VPN 2000 and SSL-VPN 4000?

Virtual Assist Enhancements

- Technician Anywhere—Allows the Technician to connect to the SSL VPN appliance without first starting NetExtender. A lightweight application will run on the Technician's computer each time the Technician logs into the SSL VPN appliance prior to servicing customers. The application opens a secure tunnel to the appliance, and runs as a proxy.
- 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. A drop-down menu displays shortcuts when the Technician right-clicks the Virtual Assist taskbar at the top of the display. The Open Task Manager option brings up the Task Manager on the customer's computer, and Send Ctrl+Esc opens the customer's Start menu.
- Optional email notification to Technician—There is now the option to send email to a pre-configured list of Technicians whenever a customer logs into the system. The list must be configured by an administrator in the Virtual Assist > Settings page.
- 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, including the Technician user name, the time of service, customer and Technician system information, the chat dialog, the customer request login, the customer exit prior to servicing, and other information. To view the details of the session click the Ticket from the initial summary page. Reporting enhancements include options in the administrative interface to export, email, or clear log entries, automated log rotation and/or emailing according to a schedule or when full, and an option to send email to a list configured by the Technician or by an administrator. Log data generated by the applications on the customer's and Technician's computers is sent to the SSL VPN appliance. The logs are cycled when full and can then be sent to an external site for longer retention as configured by the administrator.

NetExtender Enhancements

- 64-bit Vista support for Windows NetExtender client—NetExtender now supports 64-bit Windows Vista as well as 32-bit Windows 2000, XP, Server 2003, and Vista. The user experience with NetExtender on 64-bit Vista is exactly same as on the 32-bit version.
- 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 on Mac 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.

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.
- Mouseover tooltips—Tooltips pop up with useful information when the mouse cursor hovers over a checkbox, text field, or radio button in the administrative interface.

Reverse Proxy Enhancements

- HTTP(S) caching—Caching is now supported on the SSL VPN appliance for use when it is acting as a proxy Web server deployed between a remote user and a local Web server. The proxy is allowed to cache HTTP(S) content on the SSL VPN appliance which the internal Web server deems cacheable based on the HTTP(S) protocol specifications. For subsequent requests, the cached content is returned only after ensuring that the user is authenticated with the SSL VPN device and is cleared for access by the access policies. Further enhancements allow the proxy to parse HTML/JavaScript/CSS documents of indefinite length. The administrator can enable or disable caching, flush cached content and set the maximum size for the cache.
- Remote gzip compression—Content received by the SSL VPN from the local Web server is compressed using gzip before sending it over the Internet to the remote client. Compressing content sent from the SSL VPN saves bandwidth and results in higher throughput. Furthermore, only compressed content is cached, saving nearly 40-50% of the required memory. Note that gzip compression is not available on the local (clear text side) of the SSL VPN appliance, or for HTTPS requests from the remote client.
- Per HTTP(S) bookmark SSO support— Administrators and users can now enable, disable, and configure custom Single Sign-on credentials for HTTP(S) bookmarks. Administrators can configure SSO for a user, a group, or a global bookmark. This feature is used to access resources on web servers that need a domain prefix for SSO authentication. Users can log into the SSL VPN as username, and click a customized bookmark to access a server with domain\username.
- Replicon Timesheet support—The Replicon Timesheet application is supported in SSL VPN 3.0. The Timesheet, Reports, and Configuration sections can be accessed through an HTTP(S) Bookmark (Proxy).

Miscellaneous Enhancements

- One Time Password enhancements—In the System > Administration page of the SSL VPN management interface, the administrator can customize the email subject and body text to either include or exclude the One Time Password. The administrator can also select the format (such as characters and numbers) for the One Time Password.
- 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. For instance, you can configure that the log be mailed at midnight every day, or at 4:00 A.M. on Saturday. SMTP

authentication is now supported when sending the log files, in addition to the previously supported POP authentication. The port number can also be configured.

- Port-based policies—Port-based policies are now available for all services including NetExtender and HTTP bookmarks. The administrator can configure a port range (such as 80-443) or a port number (80) on the Network Objects page and in User, Group, or Global policies for IP addresses or IP address ranges. For instance, with this feature you can create a Deny All policy and allow only HTTP bookmarks to reach port 80 of a Web server.
- Remote Desktop Protocol client enhancements—SSL VPN 3.0 introduces new features for RDP5 ActiveX bookmarks and RDP5 Java bookmarks. RDP5 ActiveX bookmarks now support advanced Windows options for resource mapping, with options to 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. Advanced Windows options for RDP5 Java bookmarks include redirect drives, redirect printers, redirect ports, redirect smartCards, redirect clipboard, redirect plug and play devices, dual monitors, display connection bar, automatic reconnection, font smoothing, window dragging, themes, desktop background, desktop composition, menu/window animation, and bitmap caching.

What are the new features available in the 2.5 firmware release for SSL-VPN 2000 and SSL-VPN 4000?

- **SonicWALL Virtual Assist**: SSL VPN 2.5 allows a technician to remotely diagnose and fix issues an off-site computer may be experiencing. The technician can remotely take control of the machine through secure control of mouse and keyboard to repair the problem while the customer is watching. This feature allows IT to support users off-site as if they were physically there.
- **NetExtender for Mac & Linux**: SSL VPN 2.5 has a NetExtender client that is compatible with MacOS and Linux systems. It uses a similar graphical layout and has many of the same basic features as the NetExtender client for Windows for ease of use.
  - Mac Requirements:
    - Mac OS X 10.4+
    - Apple Java 1.4+ (can be installed/upgraded by going to Apple Menu > Software Update; should be pre-installed on OS X 10.4+)
  - Linux Requirements:
    - i386-compatible distribution of Linux
    - Fedora Core and Ubuntu.
    - Sun Java 1.4+
- **NetExtender Windows Client Enhancements:** The NetExtender client for Windows from SSL VPN 2.5 comes with added features and improved functionality including a new log system and log viewer that supports flexible log formats, such as binary log files. The standalone log viewer can filter logs by time and log levels.
- **Reverse-Proxy Enhancements:**
  - Java applet rewriting
  - Flash rewriting
  - URL/Port based policies
  - Variable response size
- **Portal Enhancements:** SSL VPN 2.5 features numerous enhancements to the Portal configuration capabilities such as: the web server can listen on different IP addresses, new management rules that can be set for HTTP, HTTPS, and Ping, Virtual Office portals that can now use customized logos and specify the server certificate used.
- **Per Bookmark Single Sign-On Credentials**: SSL VPN 2.5 supports Single Sign-On for RDP and FTP bookmarks.
- **RDP Enhancements:** SSL VPN 2.5 supports the 'Login as Console' option, the ability to control the number of colors used in RDP sessions, Wake-on-Lan capability, and the 'Execute in Folder' option.

What are the new features available in the 2.1 firmware release for SSL-VPN 2000 and SSL-VPN 4000?

- File Shares Java Applet: The File Shares Java Applet is a Java Virtual Machine (JVM) Web browser plug-in for remote users that provides improved navigation when using File Shares to access to shared network resources. Using the File Shares Java Applet, files and

folders can be moved by drag-and-drop and multiple files and folders can be transferred with a single command. From the SSL-VPN portal, select HTML or Java File Shares application to launch by default.

- Improved support for external authentication servers: LDAP Multiple Organizational Unit (OU) support, Active Directory Group support, RADIUS Filter-ID Group support, support for changing passwords for LDAP domains, and Added support for the RADIUS Domain authentication based on PAP, CHAP, MSCHAP, MSCHAPV2.
- Support for GMS/ViewPoint Reporting: SonicWALL SSL-VPN will support GMS and ViewPoint 4.1, which will be available later in 2007, by routing Syslog messages to a ViewPoint server for reporting and monitoring.
- NetExtender enhancements: There are numerous enhancements to NetExtender in the SonicWALL SSL-VPN 2.1 release, including:
    - Full compatibility with Windows Vista
    - MSI stand-alone installer that allows NetExtender to be deployed through Windows Active Directory
    - NT domain logon script support in NetExtender standalone client
    - Support for proxy servers using HTTPS and secure proxy server forwarding
    - New administrator/ server level control and configuration options
- Reverse Proxy enhancements: HTTP(S) reverse proxy now supports Windows SharePoint Services 2.0, a Web portal management tool. All features in Windows SharePoint Services are supported except those that require integration with the client program.
- RDP ActiveX enhancements: RDP - ActiveX enhancements include RDP6 support, encryption for sensitive parameters, proxy support that includes HTTPS proxy and automatic use of Internet Explorer proxy settings, and RDP5: ActiveX bookmarks that now work with custom ports.

What were the new features in the 2.0 firmware release for the SSL-VPN 2000 and SSL-VPN 4000?

- **Two-factor authentication support** – Domains can be created for which users are authenticated against the most common third-party two-factor authentication products from RSA Security Inc. and Vasco Data Security International. Both the Virtual Office and the standalone NetExtender client support two-factor authentication.
- **Improved reverse proxy** – Various improvements have been made to the reverse proxy engine, including support for the premium version of Outlook Web Access, Lotus Domino Web Access and BIG5 and multi-byte character sets.
- **Improved bookmark policy options** – The administrator has the ability to control single sign-on at the bookmark, user, group, and global level. In addition, it is also possible to specify whether bookmarks are editable by the remote user, including changing of bookmark names.
- **Citrix Java applet** – A Java applet was added as an alternative to the existing ActiveX client to establish a connection between a Citrix Presentation Server and a client machine. The SSL-VPN appliance automatically pushes the Java component through the Virtual Office. There is no need to have a Citrix ICA client pre-installed on the remote machine. The Citrix Java applet expands Citrix support to Linux and Mac OS X client systems.
- **SSHv2 Java Applet** – To complement the existing SSHv1 support, a Java based SSHv2 Java Applet has been added to enable a proxied connection between a remote machine and any specified SSHv2 server.

What were the new features in the 1.5 firmware release for all models?

- **One-time Passwords (OTP)** - This feature is a form of two-factor authentication. After remote users enter their regular user name and password, the user receives an email with a temporary one-time password that is generated by the SSL-VPN appliance. The one-time password can also be emailed to a mobile appliance. The one-time password is then entered into the Virtual Office login interface, providing additional security.
- **Citrix (ICA) Support** - An ActiveX client has been added to establish a connection between a Citrix Presentation Server and a remote Windows client computer. The SSL-VPN appliance automatically pushes the ActiveX component through the Virtual Office. There is no need to have a Citrix ICA client pre-installed on the remote computer.

- **NetExtender Stand-Alone Client Integration** - The NetExtender client can now be used as a standalone client. Initial distribution still occurs from the Virtual Office Web portal, but after initial installation, NetExtender can be started as regular Windows application from the Start menu.
- **NetExtender Multiple Ranges and Routes** - The administrator now has the ability to assign specific IP addresses or ranges of IP addresses and specific routes to individual NetExtender users and groups. This feature allows for more granular control of who can access what network resources when using NetExtender.
- **Context-Sensitive Help Links** - Icons identified by a question mark are located on the pages of the administrative portal that link directly to the relevant sections of the online Administrator's Guide hosted on a central server by SonicWALL. In addition, several context-specific Help buttons have been added to the Virtual Office to increase usability for remote users.
- **Global Management System Basic Support** - The administrator can now configure the SSL-VPN appliance to send heartbeat messages to a designated SonicWALL Global Management System (GMS). SonicWALL GMS is not included with the SSL-VPN appliance.
- **File Shares Access Policies** - Existing access policies (which are configured for IP addresses, address ranges, and network objects) now also apply to CIFS file shares. This feature enhancement allows file sharing access policies to be configured globally on the SSL-VPN appliance, rather than having to set up permissions per user on each server. Policies can also be set at the server path level, allowing or denying access to specific shares using bookmarks.
- **RDP5 Java Client** - An RDP5 Java applet has been added to establish a connection between a Microsoft Terminal Server and a client machine with a browser that runs SUN JRE 1.3 or higher. The RDP5 Java client replaces the RDP4 Java client that was present in prior versions of firmware.
- **Reverse Proxy Enhancements (HTTP and HTTPS bookmarks)** - The reverse proxy engine, used for HTTP and HTTPS bookmarks, now supports Digest Access Authentication for negotiating credentials between a Web page and a remote user.

What does the SSL-VPN appliance do?

The SonicWALL SSL-VPN appliance provides clientless*, identity-based secure remote access to your protected internal network. Using the Virtual Office portal, SonicWALL SSL-VPN can provide users with secure remote access to your entire private network, or to individual components such as file shares, Web servers, FTP servers, remote desktops, or even individual applications hosted on Microsoft Terminal Servers. These various methods of secure remote access are provided by the following components:

- **NetExtender –** NetExtender can provide remote users with full access to your protected internal network. The experience is virtually identical to that delivered by traditional IPsec VPN clients, but NetExtender does not require any manual client installation. Instead, the NetExtender client is automatically installed on remote user's PC, which instantiates a virtual adapter for SSL-secure point-to-point access to permitted hosts and subnets on the internal network.
- **File Shares –** File Shares provide remote users with a secure Web interface to Microsoft File Shares using the CIFS (Common Internet File System) or SMB (Server Message Block) protocols. Using a Web interface similar in style to Microsoft's familiar "Network Neighborhood" or "My Network Places," File Shares allows users with appropriate permissions to browse network shares, rename, delete, retrieve, and upload files, and to create bookmarks for later recall.
- **Network Resources –** Network Resources are the more finely granular components of a trusted network that can be accessed through the SSL-VPN. Network Resources can be pre-defined by the administrator and assigned to users or groups as bookmarks, or users can define and bookmark their own Network Resources. Network Resources comprise the following remote access capabilities:
    - HTTP (Web) – Proxy access to an HTTP server on the internal network, or any other network segment that can be reached by the SSL-VPN appliance, including the Internet. The remote user communicates with the SSL-VPN appliance by HTTPS and requests a URL which is then retrieved over HTTP by the SSL-VPN, transformed as needed, and returned encrypted to the remote user. Web application session authentication is supported, as are many popular Web applications, including as Microsoft Outlook Web Access.
    - HTTPS (Web) - Proxy access to an HTTPS server on the internal network, or any other network segment that can be reached by the SSL-VPN appliance, including the Internet. The remote user communicates with the SSL-VPN appliance by

HTTPS and requests a URL which is then retrieved over HTTPS by the SSL-VPN, decrypted, transformed as needed, and returned encrypted to the remote user. Web application session authentication is supported, as are many popular Web applications, including as Microsoft Outlook Web Access.

- Telnet (Java) – A Java-based telnet client delivered through the remote user's Web browser. The remote user can specify the IP address of any accessible telnet server; the SSL-VPN will make a connection to the server, and will then proxy the communications between the user over SSL and the server using native telnet.
- SSHv1 and SSHv2 (Java) - A Java-based SSHv1/SSHv2 client delivered through the remote user's Web browser. The remote user can specify the IP address of any accessible SSHv1/SSHV2 server; the SSL-VPN will make a connection to the server, and will then proxy the communications between the user over SSL and the server using natively encrypted SSHv1/SSHv2.
- FTP (Web) - Proxy access to an HTTP server on the internal network, or any other network segment that can be reached by the SSL-VPN appliance, including the Internet. The remote user communicates with the SSL-VPN appliance by HTTPS and requests a URL that is then retrieved over HTTP by the SSL-VPN, transformed as needed, and returned encrypted to the remote user.
- Remote Desktop – Remote Desktop provides remote users with access to RDP (Remote Desktop Protocol) and VNC (Virtual Network Computing) capable workstations and servers on the internal network to approximate the experience of being at the computer. Most modern Microsoft workstations and server have RDP server capabilities that can easily be enabled for remote access, and there are a number of freely available VNC server options that can be easily obtained and installed on most operating systems. The RDP and VNC clients are automatically delivered to authorized remote users through their Web browser in the following formats:
  - RDP5 (Java) – The Java-based RDP5 client can be used to provide access to internal resources to non-Windows clients. Firmware versions 2.0 and below cannot support full-screen mode, and does not support sound-mapping, drive-mapping, serial-port mapping, or printer-mapping in the RDP session. At present, only one Java-based RDP5 session can be open. This will be corrected in a future firmware release.
  - RDP5 (ActiveX) – RDP5 is the current version of Microsoft's Remote Desktop Protocol, and because of its richer set of capabilities (such as session sound and full-screen mode), is only available in an ActiveX client. If the appliance is running 1.5 firmware or newer, it is possible to have multiple RDP5 sessions open.
  - VNC (Java) – VNC was originally developed by AT&T, but is today widely available as open source. Any one of the many variants of VNC server available can be installed on most any workstation or server for remote access. The VNC client to connect to those servers is delivered to remote users through the Web browser as a Java client.
- Applications – Applications are RDP sessions to a specific application rather than to the entire desktop. This allows administrators and users to define access to an individual application, such as CRM or accounting software, without the need for the remote user to navigate the entire desktop. When the application is closed, the session closes.
  - RDP5 (Java) - Uses the Java-based RDP5 client to connect to the terminal server, and to automatically invoke an application at the specified path (for example, "C:\program files\microsoft office\office11\winword.exe")
  - RDP5 (ActiveX) - Uses the ActiveX-based RDP5 client to connect to the terminal server, and to automatically invoke an application at the specified path (for example, "C:\program files\ethereal\ethereal.exe")

*The "clientless" notion of SSL-VPN refers to the lack of need for users or administrators to manually install a client component to access private network resources. For most functions of SSL-VPN, a client is installed, but the installation process is automated through the Web browser. The specific type of client used for each component is listed parenthetically in the section above.

Which SSL-VPN appliance do I need for my network?

For environments with fewer than 10 simultaneous users, SonicWALL recommends the SSL-VPN 200 appliance. The 200 is a low-end appliance designed for very small sites where usage is minimal. For environments with up to 50 simultaneous users, SonicWALL recommends the SSL-VPN 2000 appliance. For environments with up to 200 users, SonicWALL recommends the SSL-VPN 4000 appliance.

Is the 3.0 SSL-VPN firmware update available on all SSL-VPN platforms?

The 3.0 firmware is available for the 2000 & 4000 platforms as of mid-May 2008.
The 3.0 firmware is available for the 200 platform as of mid-September 2008.
The 2.5 firmware is available on all platforms as of Q1 2007.

Are there any feature differences between the SSL-VPN 200 and the SSL-VPN 2000/4000 appliances?

Yes. The SSL-VPN 200 appliance does not support the following features found on the 2000/4000 appliances:

- Virtual Assist
- Citrix ICA Support
- FileShares Java Applet
- Portal Virtual Host Features
- Multiple Custom Logos
- Client certificate support
- Backup/snapshot images of the firmware/settings.
- Per User and Per Group settings for NetExtender Range/Route/Client Controls
- RSA Two-Factor Authentication
- Reverse-Proxy HTTP/HTTPS Bookmark support for OWA Premium more, Flash & Java applet rewriting, Caching, Gzip Compression

Is the SonicWALL SSL-VPN appliance a true reverse proxy?

Yes, the HTTP, HTTPS, CIFS, FTP are Web-based proxies, where the native Web browser itself is the client. VNC, RDP, SSHv1, SSHv2, Citrix, and Telnet use browser-delivered Java or ActiveX clients. NetExtender uses a browser-delivered ActiveX client to IE browsers and a standalone installer to other Windows-based browsers (in firmware 1.5 and newer). Virtual Assist uses a browser-delivered thin client for both customers and technicians.

Prerequisites

What browser and version do I need to successfully connect to the SSL-VPN appliance?

- Microsoft Internet Explorer 5.01 or newer, recommend Internet Explorer 6.0SP1 (If using IE7 please upgrade firmware to 2.0.0.2 or newer)
- Mozilla 1.7.1 and newer
- Firefox 2 and newer
- Opera 9 and newer
- Safari 2 and newer

What needs to be activated on the browser for me to successfully connect to the SSL-VPN appliance?

- SSLv3 or TLS 1.0
- Enable cookies
- Enable pop-ups for the site
- Enable Java
- Enable Javascript
- Enable ActiveX

What operating systems are supported?

- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP Home SP1 and Professional SP1
- Microsoft Vista (please see NetExtender section, also note you will need firmware 2.0.0.2 or newer)
- Apple OSX 10.4 and newer
- Linux kernel 2.4.x and newer

What version of Java do I need?

You need to install Sun JRE 1.4.2 or newer (available at http://www.java.com) to use some of the features on the SSL-VPN appliance, but SonicWALL recommends using version 1.5 and newer (please note Sun now calls this 5.0). If you are experiencing problems with the RDP5 Java component, upgrade to the newest Java version.

Why can't I launch any of the RDP5 connectors, or NetExtender from my Web browser?

If your SSL-VPN appliance is running 1.0 firmware, NetExtender and the RDP5 connector are ActiveX-based, so you will need to check to see if your version of Microsoft Internet Explorer is 5.01 or newer, although SonicWALL recommends using IE 6.0SP1. Also check your browser settings to see if ActiveX is enabled (this can be found by navigating to **Tools > Internet Options > Security > Custom Level** in IE). If your SSL-VPN appliance is running firmware 1.5 or newer, you should also check to see if you have the most current version of Java installed (see below). The SSL-VPN appliances running firmware 1.5 or newer can deliver NetExtender as a standalone installer to Firefox browsers.

Why can't I open more than one RDP5 session at once?

You need to upgrade your SSL-VPN appliance to firmware 1.5 or newer if you need users to be able to each launch multiple concurrent RDP5 sessions through a SSL-VPN appliance (to clarify, this is a scenario where a single user needs to be able to do this). The 1.5 and newer firmware release only supports concurrent ActiveX-based RDP5 sessions. Support for concurrent Java-based RDP5 sessions is not currently supported.

How do I license my Windows Terminal Server to work with the SSL-VPN Appliance?

The SSL-VPN appliance functions as a fully transparent proxy, so you can choose to license your terminal server for either per appliance licensing or per user licensing. Once that is set you must purchase the appropriate number of per-user licenses or per-user licenses to support your environment. It's also advised that your SSL-VPN appliance be updated to firmware 2.0.0.2 or newer, as it resolves a number of prior issues with RDP (RDP4 support was non-compliant and removed, and support for RDP6 was added).

Why doesn't the File Shares component recognize my server names?

If you cannot reach your server by its NetBIOS name, there might be a problem with name resolution. Future firmware updates will make the name resolution process more reliable across different environments. In the meantime, check your DNS and WINS settings on the SSL-VPN appliance. You might also try manually specifying the NetBIOS name to IP mapping in the **Network > Host Resolution** section, or you can manually specify the IP address in the UNC path, for example, \\192.168.100.100\sharefolder.

Why does the SSL-VPN 200 have four 10/100 ports all marked "X1"?

The SSL-VPN 200 is based upon the TZ150 chassis and is built with a 4-port 10/100 Ethernet switch. Any of these ports can be used if you are deploying the appliance in two-port mode, although as noted the appliance is more commonly deployed in one-port mode using the "X0" port.

Does the SSL-VPN appliance have a SPI firewall?

No, it only has basic filtering capabilities. It must be combined with a SonicWALL security appliance or other third-party firewall/VPN appliance.

When will the SonicWALL security appliance line of products (TZ-series, PRO-series) have support for NetExtender?

The UTM product line is scheduled to introduce NetExtender support with SonicOS 5.1 firmware.

Can I access the SSL-VPN appliance using HTTP?
No, it requires HTTPS. HTTP connections are immediately redirected to HTTPS. You may wish to open both ports 80 and 443, as many people forget to type “https://” and instead type “http://”. If you block port 80, they will not be redirected.

What is the most common deployment of the SSL-VPN appliances?
One-port mode, where only the X0 interface is utilized, and the appliance is placed in a separated, protected “DMZ” network/interface of a SonicWALL security appliance, such as the SonicWALL TZ 170, or the SonicWALL PRO 2040.

Why is it recommended to install the SSL-VPN appliance in one-port mode with a SonicWALL security appliance?
This method of deployment offers additional layers of security control plus the ability to use SonicWALL’s Unified Threat Management (UTM) services, including Gateway Anti-Virus, Anti-Spyware, Content Filtering and Intrusion Prevention, to scan all incoming and outgoing NetExtender traffic.

Is there an installation scenario that uses more than one interface or two-port mode?
Yes, when it would be necessary to bypass a firewall/VPN appliance that may not have an available third interface, or an appliance where integrating the SSL-VPN appliance may be difficult or impossible.

Can I cascade multiple SSL-VPN appliances to support more concurrent connections?
No, this is not supported, although you can use a third-party load balancer or content switch in front of multiple SSL-VPN appliances to do so.

Can the SSL-VPN appliance pull its configuration from the head-end SonicWALL as the SonicPoint does?
No, this is not supported and there are no plans to support this in the future.

I can’t log into the management interface of the SSL-VPN appliance – what do I do?
The default IP address of the appliance is 192.168.200.1 on the X0 interface. If you cannot reach the appliance, try cross-connecting a system to the X0 port, assigning it a temporary IP address of 192.168.200.100, and attempt to log into the SSL-VPN appliance at https://192.168.200.1.

I can’t seem to print to my local printer through the Citrix ICA Client – why?
When using the Java applet, the local printers are available in the Citrix client. However, under some circumstances it might be necessary to change the Universal Printer Driver to PCL mode

Certificate and Certificate Authorities

Do I have to purchase an SSL certificate? They are really expensive.
No, your can simply ignore the security warnings, which are a message to users that the certificate is not trusted or contains mismatched information. Accepting a non-trusted certificate does not have anything to do with the level of encryption negotiated during the SSL handshake. However, SonicWALL tested digital certificates from www.rapidssl.com, which are inexpensive, work fine in the SonicWALL SSL-VPN appliance, and do not require the background check that other Certificate Authorities require during the purchase process. You can find a whitepaper on how to purchase and install a certificate online at: http://www.sonicwall.com/us/support/3165.html.

What format is used for the digital certificates?
X509v3.

What CA’s certificates can I use with the SSL-VPN appliance?

Verisign, Thawte, Baltimore, and RSA. However, any should work if they are X509v3 format. To use Thawte certificates with the SSL-VPN appliances, you will need to upgrade to firmware 1.0.0.9 or newer.

Does the SSL-VPN appliance support chained certificates?

Yes, they do. On the **System > Certificates** page, do the following:

1. Under "Server Certificates", click **Import Certificate** and upload the SSL server certificate and key together in a .zip file. The certificate should be named 'server.crt'. The private key should be named 'server.key'.
2. Under "Additional CA Certificates", click **Import Certificate** button and upload the intermediate CA certificate(s). The certificate should be PEM encoded in a text file.

After uploading any intermediate CA certificates, the system should be restarted. The web server needs to be restarted with the new certificate included in the CA certificate bundle.

Any other tips when I purchase the certificate for the SSL-VPN appliance?

We recommend you purchase a multi-year certificate to avoid the hassle of renewing each year (most people forget and when the cert expires it can create an administrative nightmare). It is also good practice to have all users that will connect to the SSL-VPN appliance run Windows Update (also known as Microsoft Update) and install the 'Root Certificates' update.

Can I use certificates generated from a Microsoft Certificate Server?

Yes, but to avoid a browser warning, you will need to install the Microsoft CA's root cert into the appliance and all Web browsers that will connect to the appliance.

Why can't I import my new certificate and private key?

The certificate and private key must be named 'server.crt' and 'server.key', and then both placed into a .zip file in order to be successfully imported. If these three steps are not followed, the import will fail.

Why do I see the message "pending" after I import a new certificate and private key?

Click the **Configure** icon next to the new certificate and enter password you specified when creating the Certificate Signing Request (CSR) to finalize the import of the certificate. Once this is done you can successfully activate the certificate on the SSL-VPN appliance.

Can I have more than one certificate active if I have multiple virtual hosts?

Prior to 2.5 firmware: No, only one can be active, other virtual sites with names that do not match the name embedded on the SSL-VPN appliance's certificate will show security warnings to any Web browser connecting to them.

With 2.5 firmware or later, it is possible to select a certificate for each Portal under the Portals > Portals: Edit Portal - Virtual Host tab. The portal Virtual Host Settings fields allow you to specify separate IP address, and certificate per portal.

I imported the CSR into my CA's online registration site but it's asking me to tell them what kind of Webserver it's for. What do I do?

Select 'Apache'.

Can I store the key and cert?

Yes, the key is exported with the CSR during the CSR generation process. It's strongly recommended that you can keep this in a safe place with the certificate you receive from the CA. This way, if the SSL-VPN appliance ever needs replacement or suffers a failure, you can reload the key and cert.

Are PKCS#7 (chained certs) or PKCS#12 (key and cert PFX container) supported on the SSL-VPN appliance?

No, neither one is currently supported. SonicWALL is investigating supporting these in a future release.

Does the SSL-VPN appliance support client-side digital certificates?

Yes, client certificates can be required for individual users on the Users > Local Users: Edit User – Login Policies tab. Enable the 'User require client cert to login' checkbox for that user. The client certificate must be loaded into the client's browser and the CN field in the certificate subject must be the same as the user's login name. In the following examples, the user's login name should be 'username':

MS Certificate Server 2003:

/DC=local/DC=swenglabone/CN=Users/CN=username/emailAddress=username@sonicwall.com

OpenLDAP:
/C=US/ST=California/L=Sunnyvale/O=Engineering/OU=SSLVPN/CN=username/emailAddress=username@sonicwall.com

Also, remember that any certificates in the trust chain of the client certificates must be installed onto the SSL-VPN appliance.

When client authentication is required my clients cannot connect even though a CA certificate has been loaded?

After a CA certificate has been loaded the SSL-VPN must be rebooted before it is used for client authentication. Failures to validate the client certificate will also cause failures to logon. Among the most common are certificate is not yet valid, certificate has expired, login name does not match common name of the certificate, certificate not sent.

General

Can I create site-to-site VPN tunnels with the SSL-VPN appliance?

No, it is only a client-access appliance. If you require this, you will need a SonicWALL TZ-series or PRO-series or NSA-series security appliance.

Can the SonicWALL Global VPN Client (or any other third-party VPN client) connect to the SSL-VPN appliance?

No, they can not. Only NetExtender and proxy sessions are supported.

Can I connect to the SSL-VPN appliance over a modem connection?

Yes, although performance will be slow, even over a 56K connection it is usable. NetExtender may have issues connecting over a slow or high-latency line (for example, it may disconnect immediately upon launch) if using the original 1.x firmware; update to firmware 1.5.0.3 or newer to resolve this issue.

Should I be using SSL-VPN or standard IKE/IPSec VPN?

Use SSL-VPN if:
You need remote users to gain secure remote access.

Use IKE/IPSec if:
Must connect two or more network segments together.

When I log in to the SSL-VPN appliance, my browser displays an error – what should I do?

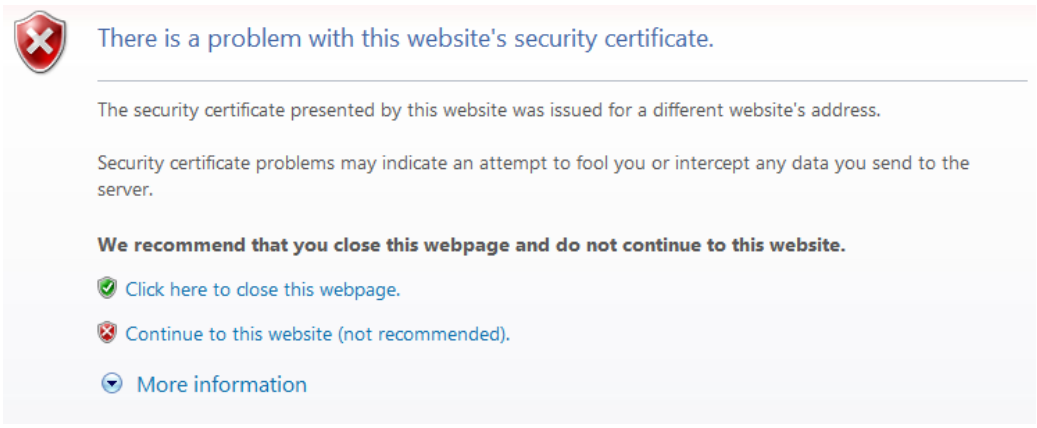
This error (see next page) can be caused by any combination of the following three factors:

1. The certificate in the SSL-VPN appliance is not trusted by the browser
2. The certificate in the SSL-VPN appliance may be expired
3. The site requested by the client Web browser does not match the site name embedded in the certificate

Web browsers are programmed to issue a warning if these three conditions are not met precisely. This security mechanism is intended to ensure end-to-end security, but often confuses people into thinking something is broken. If you are using the default self-signed certificate, this error will appear every time a Web browser connects to the SSL-VPN appliance. However, it is just a warning and can be safely ignored, as it does not affect the security negotiated during the SSL handshake. If you do not want this error to happen, you will need to purchase and install a trusted SSL certificate onto the SSL-VPN appliance.

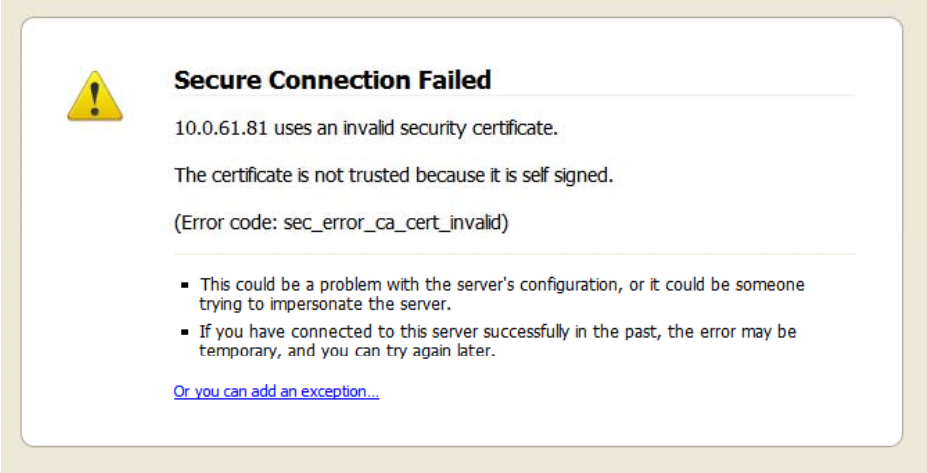
I get this message below when I log into my SSL-VPN appliance – what do I do?

It's the same problem as noted in the previous topic, but this is the new "improved" security warning screen in Microsoft Internet Explorer 7.0, which was released in late October 2006 to the Microsoft Update Website. Whereas before IE5.x and IE6.x presented a pop-up that listed the reasons why the certificate is not trusted, IE7.0 simply returns a generic error page which recommends that the user close the page. The user is not presented with a direct 'Yes' option to proceed, and instead has to click on the embedded 'Continue to this Website (not recommended)' link. For these reasons, it is strongly recommended that all SonicWALL SSL-VPN appliances, going forward, have a trusted digital certificate installed.

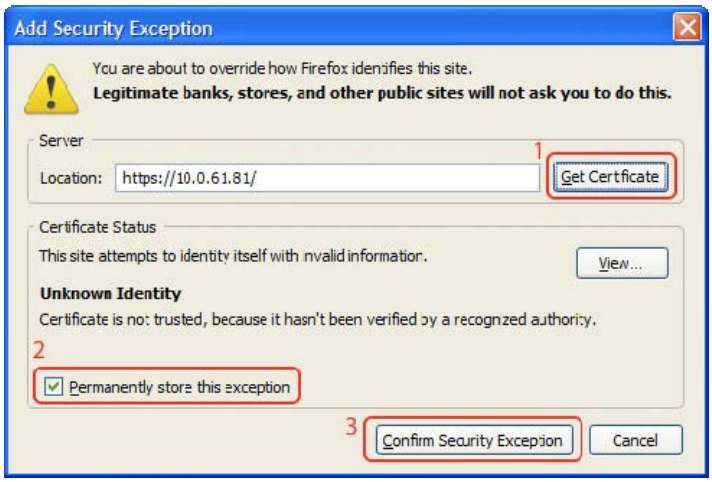


I get this message below when I log into my SSL-VPN appliance using Firefox 3 – what do I do?

Much like the errors shown above for Internet Explorer, Firefox 3 has a unique error message when any certificate problem is detected. The conditions for this error are the same as for the above Internet Explorer errors.



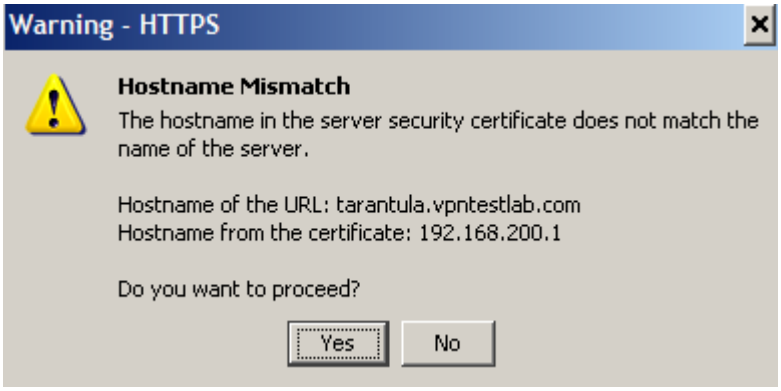
To get past this screen, click the 'Or you can add an exception…' link at the bottom, then click the 'Add Exception…' button that appears. This will open an 'Add Security Exception' window. In this window, click the 'Get Certificate' button, ensure that 'Permanently store this exception' is checked, and finally click the 'Confirm Security Exception' button. See below:



To avoid this inconvenience, it is strongly recommended that all SonicWALL SSL-VPN appliances, going forward, have a trusted digital certificate installed.

When I launch any of the Java components it gives me an error – what should I do?

See the previous section. This occurs when the certificate is not trusted by the Web browser, or the site name requested by the browser does not match the name embedded in the site certificate presented by the SSL-VPN appliance during the SSL handshake process. This error can be safely ignored. See the top of the next page for an example.



I see a 'Critical Error' message when accessing one of the SSL-VPN components – what do I do?
Reboot the system. If it does not go away, contact SonicWALL technical support. Details on how to contact SonicWALL's technical support department can be found at the end of this FAQ.

How does the strength of encryption compare to my 3DES or AES IPSec VPN?
Many newer browsers can use 3DES and AES during SSL session negotiation. It is far more important to note that RSA-RC4-SHA1 has not been compromised to date and that most banking and financial systems use RC4-SHA1 for HTTPS transactions.

Is AES supported in SSL-VPN?
Yes, if the browser supports it.

Can I expect similar performance (speed, latency, and throughput) as my IPSec VPN?
Yes, actually you may see better performance as NetExtender uses multiplexed PPP connections and runs compression over the connections to improve performance.

Does performance change when using NetExtender vs. proxy?
Yes, absolutely. NetExtender connections put minimal load on the SSL-VPN appliances, whereas many proxy-based connections may put substantial strain on the SSL-VPN appliance.

Is 2-factor authentication (RSA SecurID, etc) supported?
Yes, this is supported in the 2.0 firmware release and newer. This feature is only supported on the 2000 and

4000 platforms. It will not be supported on the 200 platform.

SSL-VPN is application dependent. How can I address non-standard applications?
You can use NetExtender to provide access for any application that cannot be accessed using internal proxy mechanisms - HTTP, HTTPS, FTP, RDP4 (firmware 1.0 only), ActiveX-based RDP5, Java-based RDP5 (firmware 1.5 and newer),Telnet, and SSHv1.

Speaking of SSH, is SSHv2 supported?
Yes, this is supported in firmware 2.0 and newer.

I understand there will be Javascript downloaded on my system. Is this safe?
Yes.

Does the SSL-VPN appliance support VoIP?
Yes, over NetExtender connections.

Are SNMP and Syslog supported?
Syslog forwarding to up to two external servers is supported in the current software release. SNMP is not currently supported but may be planned for a future software release.

Does the SSL-VPN appliance have a CLI?
No, it does not. The console ports on the SSL-VPN 2000 and SSL-VPN 4000 appliance are disabled and cannot be accessed. The SSL-VPN 200 appliance does not have a console port.

Can I Telnet or SSH into the SSL-VPN appliance?
No, neither Telnet or SSH are supported in the current release of the SSL-VPN appliance software as a means of management (this is not to be confused with the Telnet and SSH proxies, which the appliance does support).

When controlling user access, can I apply permissions on both a domain as well as a Forest basis?
Yes, using the LDAP connector.

What does the Web cache cleaner do?
The Web cache cleaner is an ActiveX-based applet that removes all temporary files generated during the session, removes any history bookmarks, and removes all cookies generated during the session. It will only run on Internet Explorer 5.0.1 or newer.

Why didn't the Web cache cleaner work when I exited the Web browser?
In order for the Web cache cleaner to run, you must click on the **Logout** button. If you close the Web browser using any other means, the Web cache cleaner cannot run.

What does the 'encrypt settings file' checkbox do?
This setting will encrypt the settings file so that if it is exported it cannot be read by unauthorized sources. Although it is encrypted, it can be loaded back onto the SSL-VPN appliance (or a replacement appliance) and decrypted. If this box is not selected, the exported settings file is clear-text and can be read by anyone.

What does the 'store settings' button do?
By default, the settings are automatically stored on a SSL-VPN appliance any time a change to programming is made, but this can be shut off if desired. If it is shut off, all unsaved changes to the appliance will be lost unless this button is clicked. This feature is most useful when you are unsure of making a change that may result in the box locking up or dropping off the network. If the setting is not immediately saved, you can simply power-cycle the appliance and it will return to the previous state before the change was made.

What does the 'create backup' button do?
This feature allows you to create a backup snapshot of the firmware and settings into a special file that can be reverted to from the management interface or from SafeMode. SonicWALL

strongly recommends creating system backup right before loading new software, or making significant changes to the programming of the appliance. This feature is available only on the SSL-VPN 2000 appliance, and is not available on the SSL-VPN 200 appliance.

What is 'SafeMode'?

SafeMode is a feature of the SSL-VPN appliance that allows administrators to switch between software image builds and revert to known-good versions in case a new software image turns out to cause issues. In cases of software image corruption, the appliance will boot into a special GUI mode that allows the administrator to choose which version to boot, or load a new version of software image.

How do I access the SafeMode menu?

In emergency situations, you can access the SafeMode menu by holding in the Reset button on the back of the SSL-VPN appliance (the small pinhole button located on the front of the SSL-VPN 2000 or 4000, and on the back of the SSL-VPN 200) for 12-14 seconds until the 'Test' light begins quickly flashing yellow. Once the SonicWALL has booted into the SafeMode menu, assign a workstation a temporary IP address of '192.168.200.100 and attach it to the X0 interface on the SSL-VPN appliance. Then, using a modern Web browser (Microsoft IE6.x, Mozilla 1.4+), access the special SafeMode GUI using the appliance's default IP address of 192.168.200.1. You will be able to boot the appliance using a previously saved backup snapshot, or you can upload a new version of software with the **Upload New Software image** button.

Can I change the colors of the portal pages?

This is not supported in the current releases, but is planned for a future software release.

What authentication methods are supported?

Local database, RADIUS, Active Directory, NT4, and LDAP.

I configured my SSL-VPN appliance to use Active Directory as the authentication method, but it fails with a very strange error message – any idea why?

Yes, the appliances must be precisely time-synchronized with each other or the authentication process will fail. Ensure that the SSL-VPN appliance and the Active Directory server are both using NTP to keep their internal clocks synchronized.

My Windows XPSP2 system cannot use the RDP5-based connectors – why?

You will need to download and install a patch from Microsoft for this to work correctly. The patch can be found at the following site: http://www.microsoft.com/downloads/details.aspx?FamilyID=17d997d2-5034-4bbb-b74d-ad8430a1f7c8&DisplayLang=en. You will need to reboot your system after installing the patch.

I created a FTP bookmark, but when I access it, the filenames are garbled – why?

If you are using a Windows-based FTP server, you will need to change the directory listing style to 'UNIX' instead of 'MS-DOS'.

Where can I get a VNC client?

SonicWALL has done extensive testing with RealVNC. It can be downloaded here: http://www.realvnc.com/download.html

Are the SSL-VPN 200/2000/4000 fully supported by GMS or ViewPoint?

With 2.0 firmware, you can configure it to send heartbeat and syslog messages to a designated SonicWALL Global Management System.

Does the SSL-VPN appliance support printer mapping?

Yes, this is supported with the ActiveX-based RDP5 client only. The Microsoft Terminal Server RDP5 connector must be enabled first for this to work. You may need to install the correct printer driver software on the Terminal Server you are accessing.

Can I integrate SSL-VPN with wireless?

Yes, please refer to pages 117-141 of this guide: http://www.sonicwall.com/downloads/swisg.pdf.

Can I manage the appliance on any interface IP address of the SSL-VPN appliance?
Prior to 2.5 firmware: No, the appliance can only by managed using the X0's IP address.
With 2.5 firmware and later, yes, you can manage on any of the interface IP addresses.

How do you associate different portals with domains and user groups?
This is a complex topic. For information, refer to the SSL-VPN Administrator's Guide.

What about binding multiple domains to global portal layout?
This is a complex topic. For information, refer to the SSL-VPN Administrator's Guide.

Can I only allow certain Active Directory users access to logging into the SSL-VPN appliance?
Use LDAP, or use local accounts.

Does the HTTP(S) proxy support the full version of Outlook Web Access (OWA Premium)?
Yes, but this only is supported on the 2000 and 4000 appliances running firmware 2.0 or newer.

Why are my RDP sessions dropping frequently?
Try adjusting the session and connection timeouts on both the SSL-VPN appliance and any appliance that sits between the endpoint client and the destination server. If the SSL-VPN appliance is behind a firewall, adjust the TCP timeout upwards and enable fragmentation.

Can I create my own services for bookmarks rather than the services provided in the bookmarks section?
This is not supported in the current release of software but may be supported in a future software release.

Why can't I see all the servers on my network with the File Shares component?
The CIFS browsing protocol is limited by the server's buffer size for browse lists. These browse lists contain the names of the hosts in a workgroup or the shares exported by a host. The buffer size depends on the server software. Windows personal firewall has been known to cause some issues with file sharing even when it is stated to allow such access. If possible, try disabling such software on either side and then test again.

What port is the SSL-VPN appliance using for the Radius traffic?
It uses port 1812.

My SSL-VPN appliance is reporting the wrong time, but its set for NTP with the correct timezone – how can I fix this?
This is fixed in firmware release 2.1 and newer.

NetExtender

Does NetExtender work on other operating systems than Windows?
Yes. Version 2.5 firmware added support for Mac and Linux platforms.

Mac Requirements:
- Mac OS X 10.4+
- Apple Java 1.4+ (can be installed/upgraded by going to Apple Menu > Software Update; should be pre-installed on OS X 10.4+)

Linux Requirements:
- i386-compatible distribution of Linux
- Fedora Core, Ubuntu, and OpenSUSE (version 10.3 or higher).

- Sun Java 1.4+

Separate NetExtender installation packages are downloadable from mysonicwall.com for each release.

I tried to run NetExtender but it says I must have admin rights – why?

If your SSL-VPN appliance is running 1.0 firmware, then on Windows 2000, XP, 2003 and Vista systems the logged-in user must have administrative rights to be able to install ActiveX-based components such as NetExtender, and it will not be possible to run NetExtender on systems where you do not have administrative rights (this often is seen in kiosk or public computer environments, where the OS is locked down to prevent this sort of behavior). If your SSL-VPN appliance is running firmware 1.5 firmware or newer, a user can run NetExtender provided that a user with administrative rights previously installed NetExtender onto the system.

Can I block communication between NetExtender clients?

Yes, this can be achieved with the User/Group/Global Policies by adding a 'deny' policy for the NetExtender IP range.

Can NetExtender run as a service?

The Windows version of NetExtender found in the 1.5 firmware release and newer can be installed and configured to run as a Windows service, which will allow systems to login to domains across the NetExtender client.

What range do I use for NetExtender IP client address range?

This range is the pool that incoming NetExtender clients will be assigned – NetExtender clients actually appear as though they are on the internal network – much like the Virtual Adapter capability found in SonicWALL's Global VPN Client. You will need to dedicate one IP address for each active NetExtender session, so if you expect 20 simultaneous NetExtender sessions to be the maximum, create a range of 20 open IP addresses. Make sure that these IP addresses are open and are not used by other network appliances or are contained within the scope of other DHCP servers. For example, if your SSL-VPN appliance is in one-port mode on the X0 interface using the default IP address of 192.168.200.1, create a pool of addresses from 192.168.200.151 to 192.168.200.171. In the 1.5 firmware release, you can create multiple unique pools on a per-group or per-user basis.

What do I enter for NetExtender client routes?

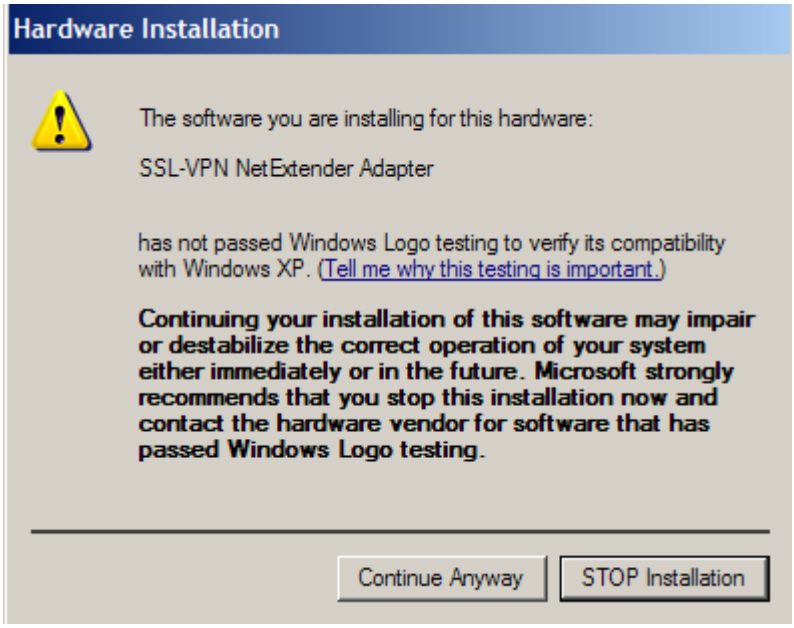
These are the networks that will be sent to remote NetExtender clients and should contain all networks that you wish to give your NetExtender clients access to. For example, if your SSL-VPN appliance was in one-port mode, attached to a SonicWALL PRO 2040 appliance on a DMZ using 192.168.200.0/24 as the subnet for that DMZ, and the PRO 2040 had two LAN subnets of 192.168.168.0/24 and 192.168.170.0/24, you would enter those two LAN subnets as the client routes to provide NetExtender clients access to network resources on both of those LAN subnets.

What does the 'Tunnel All Mode' button do?

Activating this feature will cause the SSL-VPN appliance to push down two default routes that tell the active NetExtender client to send *all* traffic through the SSL-VPN appliance. This feature is useful in environments where the SSL-VPN appliance is deployed in tandem with a SonicWALL security appliance running all UTM services, as it will allow you to scan all incoming and outgoing NetExtender user traffic for viruses, spyware, intrusion attempts, and content filtering.

Why do I get an error message when NetExtender installs?

SonicWALL has not yet completed the certification process with Microsoft, and so the NetExtender component is not currently signed by Microsoft. Because of this, the Microsoft operating system will display a warning error when you attempt to install NetExtender the first time. The error message (below) can be safely ignored.



Is there any way to see what routes the SSL-VPN is sending NetExtender?

Yes, right-click on the NetExtender icon in the taskbar and select **route information**. You can also get status and connection information from this same menu.

Once I install the NetExtender is it uninstalled when I leave my session?

By default, when NetExtender is installed for the first time it stays resident on the system, although this can be controlled by selecting the **Uninstall On Browser Exit > Yes** option from the NetExtender icon in the taskbar while it is running. If this option is checked, NetExtender will remove itself when it is closed. It can also be uninstalled from the "Add/Remove Program Files" in Control Panel. NetExtender remains on the system by default to speed up subsequent login times.

How do I get new versions of NetExtender?

New versions of NetExtender are included in patch releases of the SSL-VPN software and have version control information contained within. If the SSL-VPN appliance has been upgraded with new software, and a connection is made from a system using a previous, older version of NetExtender, it will automatically be upgraded to the new version.

How is NetExtender different from a traditional IPSec VPN client, such as SonicWALL's Global VPN Client (GVC)?

NetExtender is designed as an extremely lightweight client that is installed using a Web browser connection, and utilizes the security transforms of the browser to create a secure, encrypted tunnel between the client and the SSL-VPN appliance. While it does not have anywhere near the feature set of GVC, it is useful in most environments where basic network connectivity is required.

Is NetExtender encrypted?

Yes, it uses whatever the Internet Explorer has negotiated with the SSL-VPN appliance at connection (usually RSA-RC4-SHA1).

Is there a way to secure clear text traffic between the SSL-VPN appliance and the server?

Yes, you can configure the Microsoft Terminal Server to use encrypted RDP5-based sessions, and use HTTPS reverse proxy.

What is the PPP adapter that is installed when I use the NetExtender?
This is the transport method NetExtender uses. It also uses compression (MPPC). You can elect to have it removed during disconnection by selecting this from the NetExtender menu.

What are the advantages of using the Net Extender instead of a Proxy Application?
NetExtender allows full connectivity over an encrypted, compressed PPP connection allowing the user to directly to connect to internal network resources. For example, a remote user could launch NetExtender to directly connect to file shares on a corporate network.

Why is it required that an ActiveX component be installed?
NetExtender is installed via an ActiveX-based plug-in from Internet Explorer. Users using Firefox browsers may install NetExtender via an XPI installer.

Does NetExtender support desktop security enforcement, such as AV signature file checking, or windows registry checking?
Not at present, although these sorts of features are planned for future releases of NetExtender.

Does NetExtender work with the 64-bit version of Microsoft Windows?
Yes, starting with 3.0 firmware, NetExtender supports 64-bit Windows Vista and XP.

Does NetExtender support client-side certificates?
Users need to authenticate to the SSL-VPN portal and then launch NetExtender. This feature is not available from the stand-alone NetExtender client and is planned for a future release.

Do the SSL-VPN appliances support the ability for the same user account to login simultaneously?
Yes, this is supported on 1.5 and newer firmware releases. On the portal layout, you can enable or disable 'Enforce login uniqueness' option. If this box is unchecked, users can log in simultaneously with the same username and password.

Why do Java Services, such as Telnet or SSH, not work through a proxy server?
When the Java Service is started it does not use the proxy server. Transactions are done directly to the SSL-VPN.

The SSH client will not connect to my SSH server?
Check the version of SSH you have enabled on your server, and check the firmware release on the SSL-VPN appliance. SSHv2 support was not added until firmware 2.0 and newer. It's possible that there is a mismatch between the two.

How are the F1-F12 keys handled in the Java-based SSHv1 and Telnet proxies?
The Telnet server must support function keys. If it does, the keyboard used is relevant. Currently, the Telnet proxy uses vt320 and the SSHv1 proxy uses vt100 key codes. This is the default and the SSL-VPN appliance does not support other types such as SCO-ANSI yet. This may be supported in a future firmware release.

When I try to access a site that has Java applets using the SSL VPN 200 all I see is a box with an 'x' in it -- why?
Proxying of Java applets through the reverse proxy is not supported on the SSL VPN 200 platform.

Why can't I define access policies for file shares?
This is supported in the 1.5 and newer firmware releases.

Why am I asked to authenticate several times when browsing the Network with File Shares?
This happens behind the scenes when using Windows Network Places but the credentials are cached. This type of caching is being considered for future versions.

Why is my firewall dropping NetExtender connections from my SSL-VPN as being spoofs?
If the NetExtender addresses are on a different subnet than the X0 interface, a rule needs to be created for the firewall to know that these addresses are coming from the SSL-VPN.

There is no port option for the service bookmarks – what if these are on a different port than the default?
You can specify in the IP address box an 'IPaddress:portid' pair for HTTP, HTTPS, Telnet, Java, and VNC.

What if I want a bookmark to point to a directory on a Web server?
Simply add the path in the IP address box: IP/mydirectory/.

When I access Microsoft Telnet Server using a telnet bookmark it does not allow me to enter a user name -- why?
This is not currently supported on the appliance.

When I click on the 'Import Certificate' button, nothing happens - why?
At present this only works if you are using Microsoft Internet Explorer Web browser on Windows 2000 & XP. Starting with the 3.0 firmware, the Import Certificate is only displayed on Internet Explorer Windows 2000 and XP clients. Other web browsers need to follow their respective steps to import the certificate.

What versions of Citrix are supported?
Presentation Server 4 and MetaFrameXP Feature Release 3.

Does the SSL-VPN appliance support NTLM Authentication?
No, it does not support NTLM authentication. As a work around, the administrator can turn on basic or digest authentication. Basic authentication specifies the username and password in clear text, the security outside the intranet is not compromised, because the SSL VPN uses HTTPS. However, the intranet is required to be "trusted." Digest authentication works better in this case, because the password is not sent in clear text and only a MD5 checksum that incorporates the password is sent.

I cannot connect to a web server when Windows Authentication is enabled. I get the following error message when I try that: 'It appears that the target web server is using an unsupported HTTP(S) authentication scheme through the SSL VPN, which currently supports only basic and digest authentication schemes. Please contact the administrator for further assistance.' - why?
The HTTP and HTTPS services do not support Windows Authentication (formerly called NTLM). Only anonymous, basic or digest authentication schemes are supported.

Hardware

What are the hardware specs for the SSL-VPN 200/2000/4000?

Interfaces
SSL-VPN 200: (5) 10/100 Ethernet (WAN, 4-port LAN)
SSL-VPN 2000: (4) 10/100 Ethernet, (1) Serial port
SSL-VPN 4000: (6) 10/100 Ethernet, (1) Serial port

Processors
SSL-VPN 200: SonicWALL security processor, cryptographic accelerator
SSL-VPN 2000: 800 MHz x86 main processor, cryptographic accelerator
SSL-VPN 4000: P4 Celeron main processor, cryptographic accelerator

Memory (RAM)
SSL-VPN 200: 128 MB
SSL-VPN 2000: 512 MB
SSL-VPN 4000: 1 GB

Flash Memory
SSL-VPN 200: 16 MB
SSL-VPN 2000: 128 MB
SSL-VPN 4000: 128 MB

Power Supply
SSL-VPN 200: External 20W, 12VDC, 1.66A
SSL-VPN 2000: Internal
SSL-VPN 4000: Internal

Max Power Consumption
SSL-VPN 200: 10.4 W
SSL-VPN 2000: 48 W
SSL-VPN 4000: 108 W

Total Heat Dissipation
SSL-VPN 200: 35.6 BTU
SSL-VPN 2000: 163.7 BTU
SSL-VPN 4000: 368.3 BTU

Dimensions
SSL-VPN 200: 7.45 x 4.55 x 1.06 in (18.92 x 11.56 x 2.69 cm)
SSL-VPN 2000: 17.00 x 10.00 x 1.75 in (43.18 x 25.40 x 4.45 cm)
SSL-VPN 4000: 17.00 x 13.75 x1.75 in (43.18 x 33.66 x 4.45 cm)

Weight
SSL-VPN 200: 1.25 lbs (0.57 kg)
SSL-VPN 2000: 8.50 lbs (3.86 kg)
SSL-VPN 4000: 13 lbs (8.39 kg)

Major Regulatory Compliance (both models)
FCC Class A, ICES Class A, CE, C-Tick, VCCI, Class A, MIC, NOM, UL, cUL, TUV/GS, CBEnvironment 40-105¢ª F, 5-40¢ª C
Humidity 10-90% non-condensing

MTBF
SSL-VPN 200: 9.0 years
SSL-VPN 2000: 11.2 years
SSL-VPN 4000: 9.2 years

Do the SSL-VPN appliances have hardware-based SSL acceleration onboard?
Yes, all models have hardware-based SSL accelerators onboard…even the SSL-VPN 200 model.

What are the main differences between the discontinued SonicWALL SSL-RX Accelerator from that of the SSL-VPN 200 and SSL-VPN 2000 appliances?
They are not even remotely similar. The discontinued SSL-RX Accelerator was a purpose-built appliance used to offload cryptographic processes from burdened servers. The SSL-VPN 200 and SSL-VPN 2000 are designed to provide easy-to-use, lightweight, clientless access to internal network resources using a Web browser. The SSL-VPN 200 and SSL-VPN 2000 appliances cannot be used as SSL Accelerators – if you require this sort of appliance you will need to find a third-party company that manufactures such appliances, as SonicWALL no longer markets or sells them.

What operating systems do the SSL-VPN 200 and the SSL-VPN 2000 appliances run?
The SSL-VPN appliance is SonicWALL's own hardened Linux distribution.

Can I put multiple SSL-VPN appliances behind a load-balancer?
Yes, this should work fine as long as the load-balancer or content-switch is capable of tracking sessions based upon SSL Session ID persistence, or cookie-based persistence.

SSL-VPN 200/2000/4000 Max Count Table

TYPE	MAX SUPPORTED ON 200	MAX SUPPORTED ON 2000	MAX SUPPORTED ON 4000
Portal entries	**16**	**32**	32
Domain entries	**10**	**32**	32
Group entries	**32**	**64**	64
User entries	**100**	**1,000**	2,000
NetExtender global client routes	**32**	**32**	32
NetExtender group client routes	**N/A**	**12**	12
NetExtender user client routes	**N/A**	**12**	12
Recommended Concurrent users	**10**	**50**	200
Maximum Concurrent users	**50**	**512**	1024
Maximum Concurrent Nx tunnels	**30**	**125**	300
Route entries	**32**	**32**	32
Host entries	**32**	**32**	32
Bookmark entries	**32**	**32**	32
Policy entries	**12**	**12**	12
Policy address entries	**32**	**32**	32
Network Objects	**64**	**64**	64
'Address' Network Objects	**16**	**16**	16
'Network' Network Objects	**32**	**32**	32
'Service' Network Objects	**32**	**32**	32
SMB shares	**1,024**	**1,024**	1,024
SMB nodes	**1,024**	**1,024**	1,024
SMB workgroups	**8**	**8**	8
Concurrent FTP sessions	**8**	**8**	8
Log size	250 KB	250 KB	250 KB

Feature Support by appliance: SSL-VPN 200/2000/4000, Firmware 2.1 and newer

FEATURE	SSL-VPN 200	SSL-VPN 2000	SSL-VPN 4000
Seamless integration behind any firewall	●	●	●
Clientless connectivity	●	●	●
Unrestricted concurrent user tunnels	●	●	●
Enhanced layered security	●	●	●
NetExtender technology	●	●	●
Granular policy configuration controls	●	●	●
Personalized portal	●	●	●

File shares access policies	●	●	●
Standalone NetExtender client	●	●	●
RDP 5 Java client	●	●	●
Context-sensitive help	●	●	●
Citrix (ICA) support		●	●
NetExtender: Support for multiple IP ranges and routes		●	●
Tokenless two-factor authentication	●	●	●
RSA support		●	●
Vasco support	●	●	●
Optional client certificate support		●	●
Graphical usage monitoring		●	●
Option to create system backup		●	●
OWA premium version and Lotus Domino Access		●	●
Single sign-on bookmark policy options	●	●	●
Email log capability	●	●	●
Multiple RADIUS server support	●	●	●
RADIUS test function		●	●
NetExtender domain suffix support	●	●	●
SSHv2 support	●	●	●
Virtual Host/Domain Name support		●	●

Contacting Technical Support

If the above sections do not adequately describe the issue you are experiencing, or if you have tried all steps above and are still experiencing problems, SonicWALL offers a wide range of support options, including online support documentation, real-time Web-based support, online user discussion forums, and phone-based support. These options are available to you using the site listed below.

http://www.sonicwall.com/us/support/contact.html

Support is available for 90 days upon registration for SonicWALL SSL-VPN 200 and SSL-VPN 2000 appliances. Support is also available for customers with current and valid service & support contracts.

Created: 09/01/2005
Updated: 08/15/2008
Version 3.0
Maintained by: sslvpndev_sv@sonicwall.com