Release Notes

Secure Remote Access | SonicOS SSL VPN 3.5.0.0 on SSL-VPN 2000/4000

Contents

Platform Compatibility

The SonicOS SSL VPN 3.5 release is supported on the following platforms:

- **SonicWALL SSL-VPN 2000**
- **SonicWALL SSL-VPN 4000**

New Features in SonicOS SSL VPN 3.5 Release

The following new features are introduced in the SonicWALL SSL VPN 3.5 release:

- **Application Offloading** - This new Portal feature enables secure access to a specified web application through the configured portal. Administrators can require user authentication, or they can provide unauthenticated access for public e-commerce applications. For both cases, Web Application Firewall can be enabled to prevent Web-based attacks on these internal servers. Such functionality can be critical in adhering to corporate data compliance policies.
- **IPv6 Support** - SonicWALL SSL VPN 3.5 Release provides IPv6 support for the following areas:
  - Interfaces, routes and network objects
  - NetExtender
  - Virtual Assist
  - FTP, Telnet, SSH, SSHv2, HTTP, HTTPS, and Citrix Bookmarks and services
  - Access and login policy rules
- **NetExtender Command Line Interface** – SonicWALL NetExtender for Windows platforms now includes a command line interface (CLI) that allows users to control most functions of the application using the Windows Command Prompt interface.
- **NetExtender Windows Mobile** – SonicWALL currently offer Windows, Mac and Linux support for all SonicWALL SSL VPN platforms. With the proliferation of mobile computing, there is a growing need to support mobile devices. NetExtender Mobile provides access to your entire intranet from your Windows mobile device.
- **Redesigned Dynamic Virtual Office** - The SonicWALL SSL VPN Virtual Office (the user portal) has been completely redesigned to implement web 2.0 technologies. The streamlined design increases ease-of-use

by allowing for better customization, icon-based look and feel, dynamic page updates, and advanced user help features.

- **Reverse-Proxy Enhancements** - SonicWALL SSL VPN 3.5 release provides reverse proxy support for SharePoint 3.0 and Lotus Domino Web-Access 7.0.
- **Web Application Firewall (WAF)** - A new subscription-based service that employs a dynamically updated signature database to protect against modern, web-based threats. The proliferation of Web 2.0 applications has propelled the Worldwide Web as a critical platform for businesses and consumers. However, its recent popularity has also made it a new threat vector of choice and Web-based attacks are rising at an alarming rate. WAF is being offered as a free, technology preview in the beta for firmware version 3.5 but will not be available for purchase.
- **Virtual Assist Mac Support** - Virtual Assist technicians can now assist customers who are using MacOS.
- **Virtual Assist Standalone Client** - A new standalone Virtual Assist client facilitates a number of advanced features including, multiple customer support, dual monitor support, and the ability to reboot and reconnect a client's computer.

NetExtender for Windows Mobile Platform Support

Hardware Support

NetExtender for Windows Mobile is supported on ARM CPU-based devices.

Software Support

Window Mobile 5 or higher is required. The following specific platforms are supported:

- Windows Mobile 5 PocketPC
- Windows Mobile 6 Professional
- Windows Mobile 6 Classic

NetExtender for Windows Mobile Installation instructions

To install NetExtender for Windows Mobile, perform the following tasks:

1. Log in to http://mySonicWALL.com.
2. Click on **Downloads**.
3. In the **Software Type** pulldown menu, select either **SSL-VPN 2000 firmware** or **SSL-VPN 4000 firmware**.
4. Click on the **SSLVPN 2000/4000 NetExtender (Windows Mobile)** link.
5. Save the .cab file onto your Windows Mobile device.
6. Double-click on the .cab file to install NetExtender.
7. Go to your Programs folder to launch NetExtender.

Potential Proxy Issue for AT&T Customers

Some Windows Mobile phones using AT&T may encounter problems with accessing Intranet sites over NetExtender. This is caused by the phones being pre-configured with a proxy to wireless.cingular.com for web browsers. When using Mobile Internet Explorer, you will see a "502 Proxy Error" message. When using Opera 9 Mobile, you will see a "Could not connect remote server."

To fix this issue for Mobile Internet Explorer, run the **Disable Proxy** application, which is located in the **Start\Programs\Tools\Proxy Manager** directory.

To fix this issue for Opera 9 Mobile, go to the **Windows\Opera9** directory and open the **opera.ini** file. Remove the following lines:

```
Code:
[Proxy]
Use Proxy On Local Names Check=1
HTTP Server=wireless.cingular.com
HTTPS server=wireless.cingular.com
Use HTTP=1
Use HTTPS=1
Enable HTTP 1.1 for proxy=1
```

Known Issues

The following are known issues in the SonicOS SSL VPN 3.5.0.0 release:

Bookmarks

Symptom	Condition / Workaround	Issue
An RDP Java bookmark fails to connect.	Occurs when the RDP Java bookmark uses a hostname (not an IP address) and the user is connecting from an external network.	76791
When accessing SharePoint through a Virtual Office bookmark, users are unable to create a document in the document library, upload multiple documents, or use the site action combo box.	Occurs when attempting to use a SharePoint bookmark to create a document in the document library, upload multiple documents, or use the site action combo box.	74320
Virtual Office bookmarks do not properly display content encoded in the UTF-16 format.	Occurs when attempting to access UTF-16 content.	75313
An ActiveX bookmark fails to open an application specified in the **Application and Path** field.	Occurs when using a Windows 2008 server and an application is specified in an ActiveX bookmark's **Application and Path** field.	71984
A user sees DNS and NetBios errors when attempting to access a file share bookmark.	Occurs on both HTML and Java file share bookmarks.	70520

IPv6

Symptom	Condition / Workaround	Issue
An internal error message displays when attempting access a Citrix server using an IPv6 address.	Occurs when attempting to access a Citrix server using an IPv6 address.	76180

MacOS

Symptom	Condition / Workaround	Issue
A technician is unable to restart the Virtual Assist service after a customer is re-queued.	Occurs when the customer is using a Mac.	76294
NetExtender on a Mac fails to connect.	Occurs on a Core 2 Duo Mac system running OS X 10.4 using the NetExtender version 3.5.620 client. **Workaround**: Downgrade to 3.5.619 client.	76554

Virtual Assist

Symptom	Condition / Workaround	Issue
A technician is unable to restart the Virtual Assist service after a customer is re-queued.	Occurs when the customer is using a Mac.	76294

Resolved Known Issues

The following known issues are resolved in the SonicOS SSL VPN 3.5.0.0 release:

Bookmarks

Symptom	Condition / Workaround	Issue
Remote Desktop sessions fail when the **Login as console session** option is enabled.	Occurred when using RDP version 6.1 with a computer running Windows Server 2008.	68019

System

Symptom	Condition / Workaround	Issue
SSL VPN, SSH, and Linux do not properly process non-ASCII encoded content (such as Japanese characters).	Occurs when attempting to access non-ASCII content. **Workaround**: Connect with NetExtender and then launch an SSH client that can properly handle the encoding.	51600

Users

Symptom	Condition / Workaround	Issue
Users are able to log in to the SSL VPN even when all LDAP attributes are not matched for their accounts.	Occurs when a user has logged in once while matching all LDAP attributes, and then an attribute is changed after the user logs out.	63959

Virtual Assist

Symptom	Condition / Workaround	Issue
Technicians cannot fully remove a customer from the support queue.	Occurs when a technician has cause to remove a customer from the queue (such as when customers cannot remove themselves or if they are abusing the system).	67323

Upgrading SonicOS SSL VPN Firmware Procedures

The following procedures are for upgrading an existing SonicOS SSL VPN image to a newer version.

Obtaining the Latest SonicOS SSL VPN Image Version

1. To obtain a new SonicOS SSL VPN image file for your SonicWALL security appliance, connect to your mysonicwall.com account at <http://www.mysonicwall.com>.

   Note: *If you have already registered your SonicWALL SSL VPN appliance, and you selected **Notify me when new firmware is available** on the **System > Settings** page, you are automatically notified of any updates available for your model.*

2. Copy the new SonicOS SSL VPN image file to a directory on your management station.

Exporting a Copy of Your Configuration Settings

Before beginning the update process, export a copy of your SonicWALL SSL VPN appliance configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your SonicWALL SSL VPN appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

Perform the following procedures to save a copy of your configuration settings and export them to a file on your local management station:

1. Click the **Export Settings . . .** button on the **System > Settings** page and save the settings file to your local machine. The default settings file is named *sslvpnSettings.zip*.

   Tip: To more easily restore settings in the future, rename the .zip file to include the version of the SonicWALL SSL VPN image from which you are exporting the settings.

Uploading a New SonicOS SSL VPN Image

Note: *SonicWALL SSL VPN appliances do not support downgrading an image and using the configuration settings file from a higher version. If you are downgrading to a previous version of a SonicOS SSL VPN image, you must select **Uploaded Firmware with Factory Defaults – New!** . You can then import a settings file saved from the previous version or reconfigure manually.*

1. Download the SonicOS SSL VPN image file from www.mysonicwall.com and save it to a location on your local computer.
2. Select **Upload New Firmware** from the **System > Settings** page. Browse to the location where you saved the SonicOS SSL VPN image file, select the file, and click the **Upload** button. The upload process can take up to one minute.

3. When the upload is complete, you are ready to reboot your SonicWALL SSL VPN appliance with the new SonicOS SSL VPN image. Do one of the following:
   - To reboot the image with current preference, click the boot icon for the following entry: **Uploaded Firmware – New!**
   - To reboot the image with factory default settings, click the boot icon for the following entry: **Uploaded Firmware with Factory Defaults – New!**

   Note: *Be sure to save a backup of your current configuration settings to your local machine before rebooting the SonicWALL SSL VPN appliance with factory default settings, as described in the previous "Saving a Backup Copy of Your Configuration Settings" section.*
4. A warning message dialog is displayed saying **Are you sure you wish to boot this firmware? Click OK to proceed**. After clicking **OK**, do not power off the device while the image is being uploaded to the flash memory.
5. After successfully uploading the image to your SonicWALL SSL VPN appliance, the login screen is displayed. The updated image information is displayed on the **System > Settings** page.

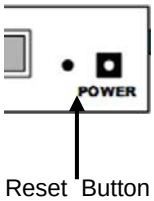
Resetting the SonicWALL SSL-VPN 2000 or 4000 Using SafeMode

If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** page.

To reset the SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the SonicWALL security appliance and configure your management station IP address with an address on the 192.168.200.0/24 subnet, such as 192.168.200.20.

   Note: *The SonicWALL security appliance can also respond to the last configured LAN IP address in SafeMode. This is useful for remote management recovery or hands off recovery in a datacenter.*
2. Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the security appliance for five to ten seconds. The reset button is in a small hole next to the power supply.



Reset Button – SSL VPN

   Tip: *If this procedure does not work while the power is on, turn the unit off and on while holding the reset button until the Test light starts blinking.*

   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.
3. Connect to the management interface by pointing the Web browser on your management station to **http://192.168.200.1**. The SafeMode management interface displays.
4. Try rebooting the SonicWALL security appliance with your current settings. Click the boot icon in the same line with **Current Firmware**.
5. After the SonicWALL security appliance has rebooted, try to open the management interface again. If you still cannot open the management interface, use the reset button to restart the appliance in SafeMode again. In SafeMode, restart the SonicOS SSL VPN image with the factory default settings. Click the boot icon in the same line with **Current Firmware with Factory Default Settings**.

Related Technical Documentation

This section contains a list of technical documentation available on the SonicWALL Technical Documentation Online Library located at:

http://www.sonicwall.com/us/Support.html

Information about the SonicWALL SSL-VPN 2000 and 4000 appliances can be found in the many reference guides available on the Web site, including the following:

- *SonicWALL SSL-VPN 2000 Getting Started Guide*
- *SonicWALL SSL-VPN 4000 Getting Started Guide*
- *SonicOS SSL VPN 3.5 Administrator's Guide*
- *SonicOS SSL VPN 3.5 User's Guide*
- *Advanced Deployment Technical Notes*

Last updated: 2/25/2009