Release Notes

Contents

Platform Compatibility

The SonicOS SSL VPN 3.0.0.8 release is supported on the following platform:

- **SonicWALL SSL-VPN 200**

Known Issues

The following are known issues in the SonicOS SSL-VPN 200 3.0.0.8 release:

Bookmarks

Symptom	Condition / Workaround	Issue
No validation is provided for name and IP address fields when creating bookmarks.	Occurs when a users logs into the SSL-VPN portal, creates an RDP or other bookmark and enters invalid characters into the name or IP address fields, such as ""!@#$%^&*()".	64014

Java Clients

Symptom	Condition / Workaround	Issue
Connection to multiple terminals fails with Java RDP client, allowing only one RDP session at a time.	Occurs when the user clicks on a terminal services RDP-Java bookmark and logs in, and then this RDP session closes when the user clicks on another terminal services RDP bookmark.	64010

NetExtender

Symptom	Condition / Workaround	Issue
NetExtender does not give any error message nor does it limit the number of retries when incorrect credentials are entered for a proxy server.	Occurs when **Use Proxy Server** is selected in the preferences for standalone NetExtender, but incorrect credentials are entered for the proxy server there. When NetExtender is launched and the same credentials are entered, the user is simply prompted again for the credentials over and over.	64014

Reverse Proxy

Symptom	Condition / Workaround	Issue
Accessing an HTTP bookmark to the URL of a VNC server results in a Java Connection Refused error.	Occurs when a VNC server is listening on port 5801 for use by users without a VNC client where access occurs in a browser using the URL: http://<IPAddress of the server>:5801. The HTTP bookmark is created with this URL, and gives the error when accessed. **Workaround**: Use a VNC bookmark rather than an HTTP bookmark, or use NetExtender.	69742

Resolved Issues

The following issues are resolved in the SonicOS SSL-VPN 200 3.0.0.8 release:

Licensing

Symptom	Condition / Workaround	Issue
The wrong MySonicWALL page appears when accessed from the SSL-VPN management interface.	Occurs when the **Activate, Upgrade, or Renew services** link is clicked on the System > Licenses page.	77104
Resetting the serial number and restarting the appliance does not reflect unregistered status in the System > Status page.	Occurs when using the SonicWALL backend tool to reset the serial number to unregistered status. Fixed when the internal reset tool in the <SSL-VPN IP>/cgi-bin/diag page is used.	74307
The System > Status page shows that the appliance is registered even after the serial number is reset.	Occurs when the serial number is manually reset with a SonicWALL application.	76952

Java Clients

Symptom	Condition / Workaround	Issue
RDP Java cannot determine the correct IP address when connecting to an RDP host name.	Occurs when attempting to connect to an RDP host from an external network. **Workaround**: Connect to the IP address rather than the host name.	76791
All Web-based clients need to be signed with an updated certificate before the current code signing certificate expires.	Occurs when the previous code signing certificate expires on May 13, 2009 for the following components: • RDP ActiveX • RDP Java applet • VNC Java applet • FileShares applet • SSHv2 applet • NetExtender executables • Web Cache Cleaner SonicWALL highly recommends upgrading to the SSL VPN 3.0.0.8 firmware, without which the affected clients will not be able to install and therefore, will not function.	76019

User Policies

Symptom	Condition / Workaround	Issue
User allow policies for file shares are missing after reboot/restart of SSL VPN appliance or Web server.	Occurs when the host field in the policy contains one or more spaces, such as "stat1\SAS Projects\Client FTP Site\tdye".	73722

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.

Release Notes

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 200 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.
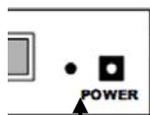
  Reset Button – SSL-VPN

  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 200 appliances can be found in the many reference guides available on the Web site, including the following:

- *SonicWALL SSL-VPN 200 Getting Started Guide*
- *SonicOS SSL VPN 3.0 Administrator's Guide*
- *SonicOS SSL VPN 3.0 User's Guide*
- *Advanced Deployment Technical Notes*

Last updated: 4/30/2009