Release Notes

Secure Remote Access

SonicOS SSL VPN 3.5.0.11 on SSL-VPN 2000/4000

Contents

Platform Compatibility

The SonicOS SSL VPN 3.5.0.11 release is supported on the following platforms:

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

New Features

The following new feature is introduced in the SonicOS SSL VPN 3.5.0.11 release on the SSL-VPN 2000/4000:

- **NetExtender Support for MacOS 10.6** – SonicOS SSL VPN 3.5.0.11 on SSL-VPN 2000/4000 provides NetExtender support for the MacOS 10.6 Snow Leopard release.

Known Issues

The following are known issues in the SonicOS SSL-VPN 2000/4000 3.5.0.11 release:

Java Clients

Symptom	Condition / Workaround	Issue
Using RDP-Java to access a bookmark does not open the Testing Java Compatibility page to show that Java is not installed or enabled in the browser.	Occurs when clicking an RDP-ActiveX bookmark on the portal in an Opera browser with Java disabled. The portal switches to RDP-Java because the browser is not Internet Explorer, but the process halts at the Terminal Services (RDP) Loading page.	80341

ActiveX Client

Symptom	Condition / Workaround	Issue
Full domain name is not resolved by the RDP-ActiveX Client.	Occurs when the user attempts to create and use a bookmark for RDP-ActiveX, giving a full domain name as "exchange2003ad.com" for "Use Custom Credentials". **Workaround**: Use JAVA RDP to log into the backend server full domain name. Remove ".com" from the domain name field to automatically log into the RDP.	78778

NetExtender

Symptom	Condition / Workaround	Issue
NetExtender gets an error when attempting to launch automatically from a portal that is accessed with Internet Explorer 8.	Occurs when a portal is configured to automatically launch NetExtender after a user logs in, and the IE8 browser that is used to log into the portal has Protected Mode enabled in the Internet Options > Security settings.	81025
The NetExtender client for Linux fails to connect with a pppd error.	Occurs when launching NetExtender from a Linux machine, either in the SSL VPN user interface or on the command line.	78674
The NetExtender client only executes the domain logon script when it is named domain.bat; otherwise the Domain Controller will send a SMB response to the NetExtender client indicating a query path info error: STATUS_OBJECT_NAME_NOT_FOUND.	Occurs when the logon script is not named domain.bat or a different script is assigned to the user.	74366

Resolved Issues

The following issues are resolved in the SonicOS SSL-VPN 2000/4000 3.5.0.11 release:

Authentication

Symptom	Condition / Workaround	Issue
One Time Password with Client certificates gives an error when logging into the portal.	Occurs when the Active Directory Authentication domain is set up with Client certificates and One Time Password on SSL-VPN 3.0.0.5. After upgrading to SSL-VPN 3.5.0.0, an OTP error occurs while trying to login.	78843

JavaScript

Symptom	Condition / Workaround	Issue
Users are not able to log in to the management portal or other portal when JavaScript is disabled in the browser, but no error message is displayed.	Occurs when JavaScript is disabled in Opera or Firefox.	80339

NetExtender

Symptom	Condition / Workaround	Issue
NetExtender for Mac fails. The log shows an error like "Pppd is not setuid-root and the invoking user is not root".	Occurs when using NetExtender on Mac OS 10.6 Snow Leopard.	82600
Disabling the 'Display NetExtender' setting for the portal not only prevents the display of the NetExtender button on the portal, but also prevents the use of the NetExtender client.	Occurs when the 'Display NetExtender' setting for the portal is disabled. The resolution includes a new checkbox in the Add/Edit Portal page to control use of the NetExtender client: [ ] Allow NetExtender connections to this portal.	81389

System

Symptom	Condition / Workaround	Issue
The system becomes unresponsive after changing the self-signed certificate's common name field.	Occurs when entering a common name that is greater than 32 characters.	82260

Web Application Firewall

Symptom	Condition / Workaround	Issue
Web Application Firewall Database sync errors appear unexpectedly in the log files.	Occurs when the Web Application Firewall license is expired and the feature is not in use.	81961
Syntax errors in a Web Application Firewall signature database update cause the firmware to revert to the factory default signature database, rather than restoring the last known good update.	Occurs when syntax errors occur during dynamic signature database updates.	81878

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

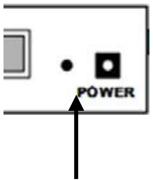
If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings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

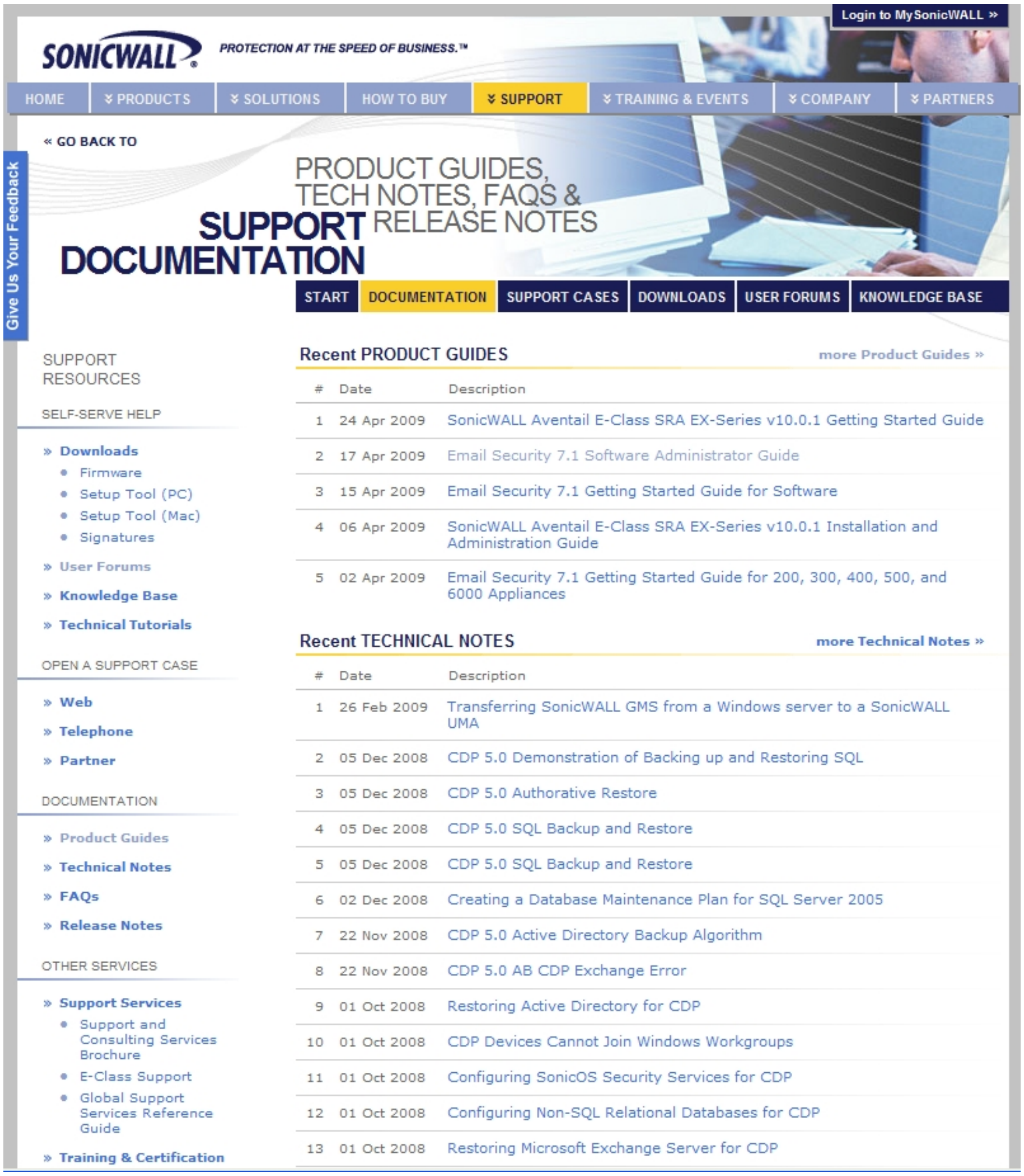
4. Try rebooting the SonicWALL security appliance with your current settings. Click the boot icon in the same line with **Current Firmware**.

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



Recent PRODUCT GUIDES

#	Date	Description
1	24 Apr 2009	SonicWALL Aventail E-Class SRA EX-Series v10.0.1 Getting Started Guide
2	17 Apr 2009	Email Security 7.1 Software Administrator Guide
3	15 Apr 2009	Email Security 7.1 Getting Started Guide for Software
4	06 Apr 2009	SonicWALL Aventail E-Class SRA EX-Series v10.0.1 Installation and Administration Guide
5	02 Apr 2009	Email Security 7.1 Getting Started Guide for 200, 300, 400, 500, and 6000 Appliances

Recent TECHNICAL NOTES

#	Date	Description
1	26 Feb 2009	Transferring SonicWALL GMS from a Windows server to a SonicWALL UMA
2	05 Dec 2008	CDP 5.0 Demonstration of Backing up and Restoring SQL
3	05 Dec 2008	CDP 5.0 Authorative Restore
4	05 Dec 2008	CDP 5.0 SQL Backup and Restore
5	05 Dec 2008	CDP 5.0 SQL Backup and Restore
6	02 Dec 2008	Creating a Database Maintenance Plan for SQL Server 2005
7	22 Nov 2008	CDP 5.0 Active Directory Backup Algorithm
8	22 Nov 2008	CDP 5.0 AB CDP Exchange Error
9	01 Oct 2008	Restoring Active Directory for CDP
10	01 Oct 2008	CDP Devices Cannot Join Windows Workgroups
11	01 Oct 2008	Configuring SonicOS Security Services for CDP
12	01 Oct 2008	Configuring Non-SQL Relational Databases for CDP
13	01 Oct 2008	Restoring Microsoft Exchange Server for CDP

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: 9/10/2009