Release Notes

Secure Remote Access | **Dell SonicWALL SRA 7.0**

Contents

Platform Compatibility

The Dell SonicWALL SRA 7.0 release is supported on the following platforms:

- Dell SonicWALL SRA 1200
- Dell SonicWALL SRA 1600
- Dell SonicWALL SRA 4200
- Dell SonicWALL SRA 4600
- Dell SonicWALL SRA Virtual Appliance

Licensing on the SRA Appliances and Virtual Appliance

The Dell SonicWALL SRA 7.0 firmware provides for user-based licensing on Dell SonicWALL SRA appliances and SRA Virtual Appliance. By default, the SRA 4600/4200 comes with a 25-user license and the SRA 1600/1200 and Virtual Appliance come with a 5-user license. On the SRA 4600/4200, extra licenses are added in 10, 25, and 100 user denominations, up to a maximum that allows for 500 concurrent user sessions. On the SRA 1600/1200 and Virtual Appliance, customers can add licenses in 5-user and 10-user denominations, up to a maximum of 50 concurrent user sessions.

Licensing is controlled by the Dell SonicWALL license manager service, and customers can add licenses through their MySonicWALL accounts. Unregistered units support the default license allotment for their model, but the unit must be registered in order to activate additional licensing from MySonicWALL.

License status is displayed in the SRA management interface, on the Licenses & Registration section of the 'System > Status' page. The TSR, generated on the 'System > Diagnostics' page, displays both the total licenses and active user licenses currently available on the appliance.

If a user attempts to log in to the Virtual Office portal and no user licenses are available, the login page displays the error, “No more User Licenses available. Please contact your administrator.” The same error is displayed if a user launches the NetExtender client when all user licenses are in use. These login attempts are logged with a similar message in the log entries, displayed in the 'Log > View' page.

To activate licensing for your appliance or virtual appliance, perform the following steps:

1. Login as admin, and navigate to the System > Licenses page.
2. Click the **Activate, Upgrade or Renew services** link. The MySonicWALL login page is displayed.
3. Type your MySonicWALL account credentials into the fields to login to MySonicWALL. This must be the account to which the appliance is, or will be, registered. If the serial number is already registered through the MySonicWALL web interface, you will still need to login to update the license information on the appliance itself.
4. For the SRA 4600/4200/1600/1200 appliances, MySonicWALL automatically retrieves the serial number and authentication code. For the virtual appliance, you will need to enter this information:
    - Type the serial number of the virtual appliance into the **Serial Number** field. The serial number and authentication code are provided when the software is purchased.
    - Type the authentication code into the **Authentication Code** field.
5. Type a descriptive name for the appliance or virtual appliance into the **Friendly Name** field, and then click **Submit**.
6. Click **Continue** after the registration confirmation is displayed.
7. Optionally upgrade or activate licenses to other services displayed on the System > Licenses page.
8. After activation, view the System > Licenses page to see a cached version of the active licenses.

Important Differences between the SRA Appliances

Although all SRA appliances support major SRA features, not all features are supported on all SRA appliances.

Similarities

The Dell SonicWALL SRA appliances and SRA Virtual Appliance share most major SRA features, including:

- Virtual Office
- NetExtender
- Secure Virtual Assist
- Secure Virtual Access
- Application Offloading
- Web Application Firewall
- End Point Control
- Geo IP & Botnet Filter

Differences

Important differences between the SRA appliances are shown in the table below. An 'X' indicates that the feature is supported on that appliance model.

Feature	SRA 4600	SRA 4200	SRA 1600	SRA 1200	SRA Virtual Appliance
Hardware-based SSL Acceleration		X			
Generic SSL Offloading Portals	X	X			X
Application Profiling	X	X			X
High Availability (HA)	X	X			X
Virtual Meeting	X	X			X

Following are examples of the different System > Settings pages on the SRA Virtual Appliance and SRA hardware appliances:

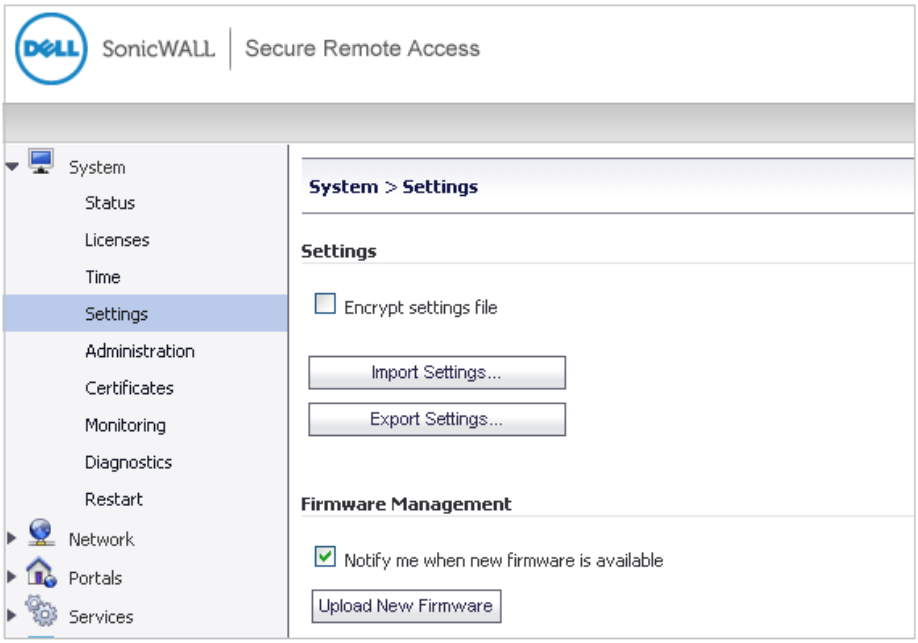

Figure 1 System > Settings page for SRA Virtual Appliance

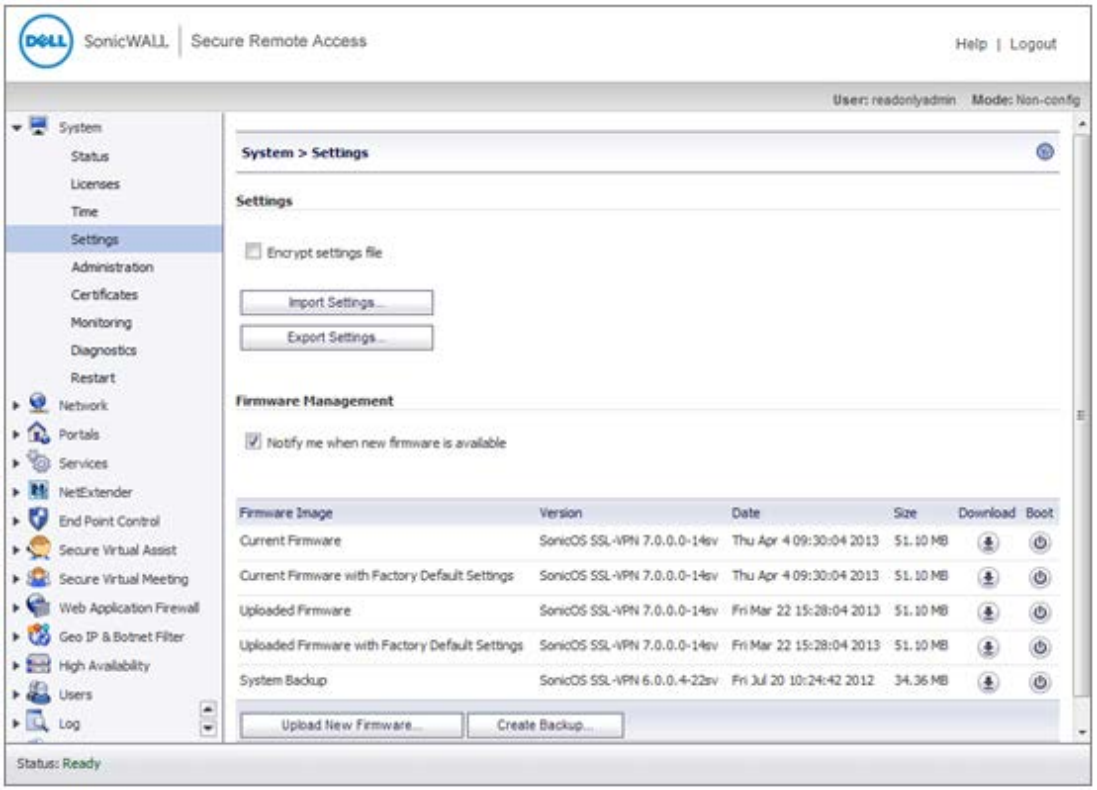

Figure 2 System > Settings page for SRA Hardware Appliances

Feature Enhancements in SRA 7.0

The following enhancements and new features are introduced in the SONICWALL SRA 7.0 Beta release:

For detailed information on these features, see the SRA 7.0 Administrator Guide and the SRA 7.0 User Guide, which can be downloaded from http://www.sonicwall.com/us/en/support/3893.html.

Secure Virtual Meeting

The following enhancements have been added to SRA 7.0 Secure Virtual Meeting for the SRA 4200, 4600, and Virtual Appliance:

- Virtual Meeting now allows multiple Participants to view a desktop.
- A Participant can now point  to objects on the Host's screen and ask the Host to look at it without taking control of the meeting. This feature is enabled in the General Settings tab.
- The meeting Host can share files with selected Participants, who download the file. The Host initiates file sharing from the File menu by clicking the  File Share icon and can publish the file's information to the selected Participants.
- The Host can share a white board with Participants. Text, objects, and highlighting can be added to the white board by using tools accessed through icons displayed at the top of the white board:
- The Host can use Annotation tools to annotate a shared screen. These tools are similar to the white board tools, and the annotations are visible to all meeting Participants.
- The Host can share selected windows or the entire desktop with Participants. To do so, the Host selects Per-App Sharing from the menu bar and then selects the windows to be shared:
- The Host can share voice communication with Participants by clicking the  voice icon in the meeting lobby. Only the Host can be heard. An icon appears next to the host name on the Meeting Members window when voice communication is active.
- The Host and Participants can record a meeting in a wmv media file. Display the Record Control window by clicking the  Record button on the Float Bar.
- The client now verifies the server certificate when connecting to the Virtual Meeting appliance. If it is not issued by authorized organization or does not seem valid, an alert message is displayed and you can choose the next action.

Secure Virtual Assist

The following enhancements have been added to SRA 7.0 Secure Virtual Assist:

- The Technician can wake a client running Virtual Assist on the LAN if both are in the same subnet. The client can be recovered when powered off, in Sleep state, or in Hibernate state. This feature is invisible to the Technician and is enabled/disabled on the Secure Virtual Assist > Settings page.
- Virtual Assist can be installed as a web application by request or automatically. This feature is enabled/disabled on the Virtual Assist > Settings page and configured for the portal on the Portals > Portals > Edit > Virtual Office page.
- Customers can specify a specific Technician when requesting assistance.
- Technicians can click the 

button to record a service session in a .wmv video that can be shared with other users experiencing the same issue.

High Availability (HA) Enhancements

The following enhancements have been added to SRA 7.0 High Availability for the SRA 4200, 4600, and Virtual Appliance:

- The High Availability interface is now configurable on the High Availability > Settings page. The HA interface can only be set when the unit is in the HA unconnected mode, and both units must be set to the same interface.
- Management of the idle unit can now be enabled on the High Availability > Settings page, so the management interface and IP address can be set.
- High Availability is now supported on the SRA Virtual Appliance with the following limitations:
    - High Availability cannot be used on a virtual appliance in Single Network Interface mode.
    - The Synchronize Firmware function is not supported for a virtual appliance.

EPC Enhancements

EPC Profiles for Linux/Mac

The Administrator can create EPC profiles for Linux and Mac OS using the End Point Control > Device Profiles page and force NetExtender login from the Linux and Mac portal using the Users > Local Users page. The method used to set up Mac and Linux clients is the same as for Windows except selecting Mac or Linux on the End Point Control > Device Profiles page:

EPC Check for Portal Login

EPC is checked when users log into the web portal from a web browser, which blocks any access to the private network from untrusted sites. EPC portal checking uses the NetExtender browser plug-in, so NetExtender must be installed. This feature is available on Windows only.

Bookmark Enhancements for Mobile Connect

SRA 7.0 integrates bookmarks and the Mobile Connect for Apple iOS and Android 2.0 release. This allows Mobile Connect users to seamlessly access bookmarks from the Mobile Connect Connection screen. A **Display Bookmark to Mobile Connect clients** check box has been added to the Bookmarks page, which allows the Administrator to designate which bookmarks will be displayed to Mobile Connect 2.0 or higher clients upon connection.

In addition, a new Mobile Connect bookmark type has been added, which can be used to define URL schemes that launch directly from the bookmark. This bookmark type is only available for edit from standard browsers and is intended for use only on mobile browsers. Third party applications must be able to handle these URL schemes.

Note: Bookmarks require third party apps that must be installed on the mobile device. Dell SonicWALL is not responsible for any third party apps. Full details on the Mobile Connect 2.0 are provided in the Mobile Connect 2.0 Release Notes at:

Mobile Connect for Android 2.0 Release Notes
http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=RN&id=470

Mobile Connect for Apple iOS 2.0 Release Notes
http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=RN&id=471

WAF Enhancements

Delete URL Profiles

URL profiles can now be deleted from the list shown on the Web Application Firewall > Rules page when URLs are profiled. To delete a URL, select the URL(s) to be deleted and click the  button at the top right of the pane.

Rule Chain Enhancements

Rules in the Web Application Firewall > Rules page can be divided into pages and filtered by searching for a key word. To display only rules containing a key word in all fields or a specific field, type the key word in the Search field, select All Fields or a specific field to search, and click **Search**. Or, click **Exclude** to display only rules that do not contain the key word. Click **Reset** to display all rules. All matches are highlighted. The default is 50 rules per page.

Signature Enhancements

The paging and searching functionality for Signatures are the same as for Rule Chains, with an additional sorting option. The list can be sorted by the contents of any column in ascending or descending order by clicking the column heading.

Application Offloading Enhancements

The **Auto (HTTP/HTTPS)** option has been added to the Scheme drop-down list on the Offloading tab of the Portals > Portals > Offload Web Application page. This new feature allows the end user to determine the actual scheme used to talk to the backend server when accessing an offloading portal.

*Note: Auto (HTTP/HTTPS) Scheme can operate only if HTTP is enabled for the Virtual Host and authentication is disabled, which may be insecure. Therefore, you will be prompted to click **OK** to enable HTTP for Virtual Host and enable Anonymous access.*

Local User Login

An **Only allow users listed locally** check box has been added to the Portals > Domains > Add Domain page. When this feature is enabled, domain users are allowed to login only if listed in the local user database.

Local User Password Expiration

The Administrator can force local domain users to change their password the next time they login or at set intervals. Use the Portals > Domains page for Local User Database authentication type to force all users in a local user database to change their passwords, set the password expiration interval, and set how many days before expiration that users receive notifications.

To force a specific user to change their password, use the General tab of the Users > Local Users > Edit page.

When configured, users and Administrators receive notifications that their password will expire in *x* days, with the maximum number of days the notification is displayed specified by the Administrator. Notifications also include a link to a screen where the password can be changed.

Terminal Services Enhancements

A bookmark can be used to launch a terminal service farm. A terminal service bookmark requires the client to have a compatible client installed to connect to the terminal server. Use the **Server is TS Farm** check box on the Services > Bookmarks > Add Bookmark page to create a terminal service farm bookmark. The bookmark will then be displayed in the list of bookmarks on the portal:

Geo IP & Botnet Filter

The Geo IP & Botnet Filter feature enforces a strong and anti-evasive defense against rogue activity from Botnets using Geo IP and a dynamically updated database maintained by Dell SonicWALL. Selecting Geo IP & Botnet Filter from the navigation pane displays Status, Settings, Log, and Licensing. These features are disabled by default.

Status

The Status page has two tabs of information: General Status and Botnet Status. The General Status tab displays general filter information. The Botnet Status tab displays statistics for traffic from Botnet IPs during the last monitoring period.

Settings

The Geo IP & Botnet Filter > Settings page contains three tabs: General Settings, Cache Management, and Access Policies. Use the General Settings tab to globally enable or disable the Geo IP & Botnet filter and/or logs.

Use Cache Management to govern how Geo IP and Botnet data is managed: Offline Mode or Maximum Cache Lifetime. The Offline Mode uses, the most recent cached Geo IP & Botnet data filter whenever the Dell SonicWALL backend Server cannot be reached. Maximum Cache Lifetime sets the maximum hours that cached Geo IP & Botnet data will be retained.

Use Access Policies to create a Geo IP policy that allows or denies traffic from specified countries or a Botnet policy, which allows or denies access from a specified IPv4 IP address or IP address range. Each policy has a different priority with 1 being the highest priority. A policy's priority determines the order of enforcement, which is identified by the order they are listed on the Settings page.

Log

The Geo IP & Botnet Filter > Log page displays all Geo IP and the Botnet filter. The Log can be filtered, searched, exported, emailed, and cleared.

Licensing

The Geo IP & Botnet Filter > Licensing page identifies whether Geo IP & Botnet Filter feature is licensed. A preview license is included with SRA 7.0 until April 2014.

Other Changes

A Location column, which can be searched and excluded, has been added to logs on the Web Application Firewall > Log and Log > View pages. Also, a Location column has been added to the NetExtender > Status, Virtual Assist > Status, Virtual Meeting > Status, and User > Status pages to identify where the user is located.

Other Enhancements

- OESIS library version 3.6.4746.2 support
- Auto-scheme for Application Offloading.
- NetExtender Client DNS Registration support
- Chrome store extensions (Download the NetExtender plug-in from www.play.google.com.)
- Mobile Connect bookmark Integration
- Windows 8 support
- IPV6 Improvement for NetExtender

Known Issues

This section contains a list of known issues in the SRA 7.0 release.

NetExtender

Symptom	Condition / Workaround	Issue
Connections cannot be made with NetExtender 6.0.191.	Occurs when using both Windows 7 and Windows 8 clients with Net Extender 6.0.191 and OTP RADIUS token. **Workaround**: Use Windows 7 with NetExtender client 6.0.181. (Use MSI install to avoid auto update.)	127790

SharePoint

Symptom	Condition / Workaround	Issue
Office 2010 documents cannot be opened.	Occurs when opening Office 2010 documents on SRA offloaded portals using Sharepoint 2010 because SharePoint 2010 does not support Client Integration. **Workaround**: Enable Client Integration on SharePoint 2010, right-click the document, and save it locally. The saved document can then be opened with the applicable Office program.	124215

Resolved Issues

The following issues are resolved in the SRA 7.0 release:

Application Offloading

Symptom	Condition / Workaround	Issue
Selecting a link on an offloaded application page displays a *We Couldn't Find That Page (404 Error)* message and the URL changes to */cgi-bin/welcome?...sessionExpired*.	Occurs when a URL starts with /go (for example, /government/)	124160

Authentication

Symptom	Condition / Workaround	Issue
Users are able to login with a valid certificate.	Occurs when client certificate enforcement is enabled and a user who is not defined in the SRA appliance logs in the first time.	123910

Certificates

Symptom	Condition / Workaround	Issue
Subject Alternative Name (SAN) cannot be used instead of FQDN when generating a CSR.	Occurs when creating a Certificate Signing Request (CSR) using OpenSSL.	97776

Citrix

Symptom	Condition / Workaround	Issue
Citrix 4.5 client detection page goes into a continuous loop.	Occurs when using NetExtender and accessing a Citrix bookmark to a XenApp 4.5 server.	126285

NetExtender

Symptom	Condition / Workaround	Issue
NetExtender client can login even when the server's certificate is invalid.	Occurs when using Mac and Linux clients	125726

Policies

Symptom	Condition / Workaround	Issue
A user is able to login even though a policy blocks the user's login.	Occurs when a user is in two Active Directories and only one is blocked by a policy.	128307

Remote Desktop

Symptom	Condition / Workaround	Issue
A custom port cannot be used for Remote Desktop	Occurs when the destination port is 3389 instead of 3390.	124639
TS farm server advanced features are not available.	Occurs because pure Java applet is limited in functionality. **Workaround**: Use NetExtender with a native RDP client for full functionality.	109574

Secure Virtual Meeting

Symptom	Condition / Workaround	Issue
Meeting coordinator cannot start a meeting and, therefore, cannot share his desktop.	Occurs when users log into a meeting using the host name. **Workaround**: Access the meeting by using the IP address.	127872

Security

Symptom	Condition / Workaround	Issue
Security guidelines require 2048-bit certificates and SHA-256.	Occurs before some customers are allowed to use a security appliance, which include the Dell SonicWALL SRA, SSL VPN WorkPlace portal, and NetExtender, and Mobile Connect.	119919

Vulnerability

Symptom	Condition / Workaround	Issue
Man-in-the-middle attacker can recover text from a TLS/DTLS connection.	Occurs when using CBC-mode encryption with TLS 1.1/1.2, DTLS 1.0/1.2 and SSL 3.0 with TLS 1.0.	126877

Upgrading SRA Image Procedures

The following procedures are for upgrading an existing SRA firmware image or Virtual Appliance software image to a newer version:

Obtaining the Latest SRA Image Version

To obtain a new SRA firmware image file for your Dell SonicWALL security appliance:

1. Connect to your mysonicwall.com account at http://www.mysonicwall.com.

   Note: If you have already registered your Dell SonicWALL SRA 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 SRA image file to a directory on your management station.

   For the Dell SonicWALL SRA 4600/4200/1600/1200 appliance, this is a file such as:
   sw_sslvpnsra4600_eng_7.0.0.0_tip_4sv_506137.sig

   For the Dell SonicWALL Virtual Appliance, this is a file such as:
   sw_sslvpnsra-vm_eng_7.0.0.0_tip_4sv_506137.sig

   Note: For SRA Virtual Appliances, image files for new deployments have an .ova file extension, and image files for upgrades have a .sig file extension.

Exporting a Copy of Your Configuration Settings

Before beginning the update process, export a copy of your Dell SonicWALL SRA appliance configuration settings to your local machine. The Export Settings feature saves a copy of your current configuration settings on your Dell SonicWALL SRA 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 Dell SonicWALL SRA image from which you are exporting the settings.

Uploading a New SRA Image

Note: *Dell SonicWALL SRA 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 Dell SonicWALL SRA 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 SRA 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 SRA 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 Dell SonicWALL SRA appliance with the new SRA 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 Dell SonicWALL SRA 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 Dell SonicWALL SRA appliance, the login screen is displayed. The updated image information is displayed on the **System > Settings** page.

Resetting the Dell SonicWALL SRA Appliances Using SafeMode

If you are unable to connect to the Dell SonicWALL security appliance's management interface, you can restart the Dell 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 Dell SonicWALL security appliance, perform the following steps:

1. Connect your management station to a LAN port on the Dell 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 Dell 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 pen tip, to press and hold the reset button on the security appliance for five to ten seconds. The reset button is on the front panel in a small hole to the right of the USB connectors.

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

5. After the Dell 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 SRA 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 Dell SonicWALL Technical Documentation Online Library located at:

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

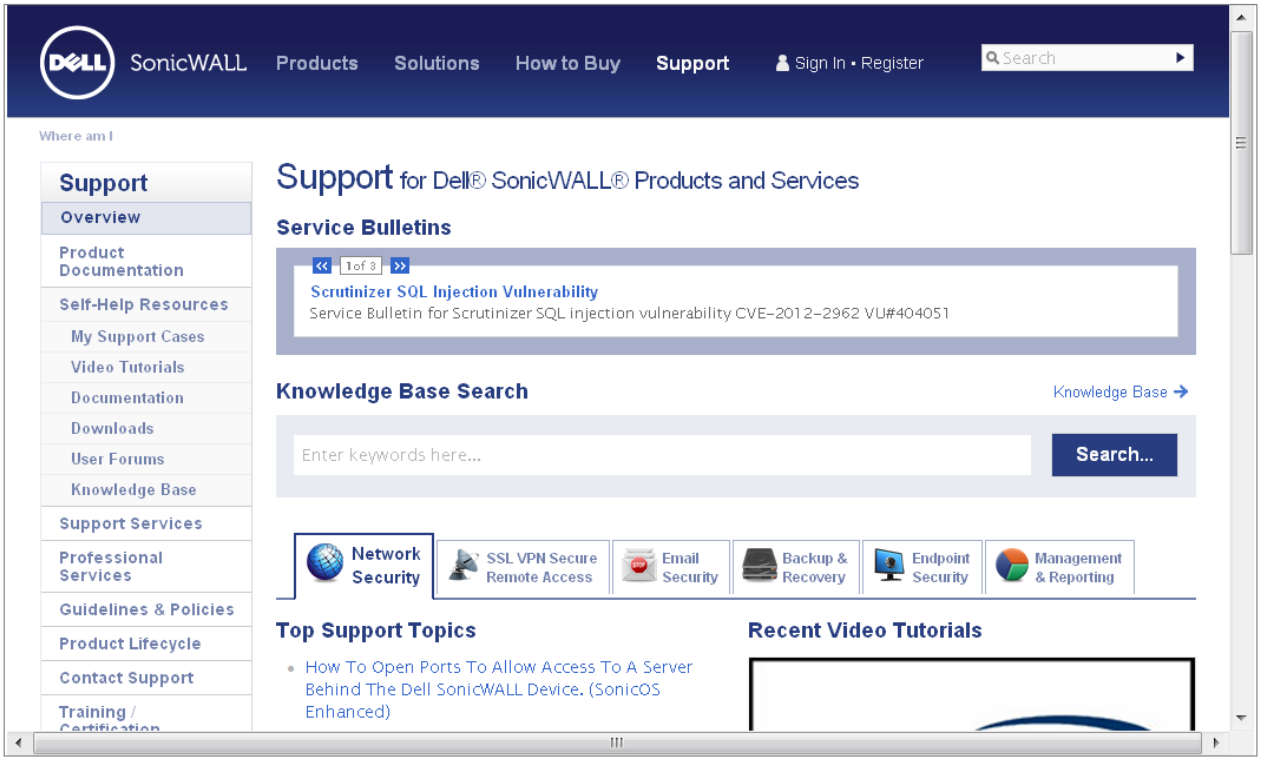

Figure 3 Dell SonicWALL Technical Documentation Online Library

Information about Dell SonicWALL SRA is found in the many reference guides available on the Web site, including the following:

- *Dell SonicWALL SRA Administrator's Guide*
- *Dell SonicWALL SRA User's Guide*
- *Dell SonicWALL SRA NetExtender Feature Module*
- *Dell SonicWALL SRA Citrix Access Feature Module*
- *Dell SonicWALL SRA Web Application Firewall Feature Module*
- *Dell SonicWALL SRA Application Offloading and HTTP(S) Bookmarks Feature Module*
- *Dell SonicWALL SRA Geo IP & Botnet Filter Feature Module*

Last updated: 4/4/2013