Release Notes

SonicOS

SonicOS Enhanced 4.2.1.0 Release Notes

Contents

Platform Compatibility

The SonicOS Enhanced 4.2.1.0 release is supported on the following SonicWALL security appliances:

- SonicWALL TZ 180
- SonicWALL TZ 180 Wireless
- SonicWALL TZ 190
- SonicWALL TZ 190 Wireless
- SonicWALL PRO 2040
- SonicWALL PRO 3060
- SonicWALL PRO 4060
- SonicWALL PRO 4100
- SonicWALL PRO 5060

This release supports the following wireless access points:

- SonicWALL SonicPoint-N
- SonicWALL SonicPoint

This release supports the following Web browsers:

- Microsoft Internet Explorer 6.0 and higher
- Mozilla Firefox 2.0 and higher
- Netscape 9.0 and higher
- Opera 9.10 and higher for Windows
- Safari 2.0 and higher for MacOS

Strong SSL and TLS Encryption Required in Your Browser

The internal SonicWALL Web server only supports SSL version 3.0 and TLS with strong ciphers (128 bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128 bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 roll-back vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.

TIP: By default, Mozilla Firefox 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. SonicWALL recommends using the most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0 and TLS and disable SSL 2.0. In Internet Explorer, go to Tools > Internet Options on the Advanced tab and scroll to the bottom of the Settings menu. In Firefox, go to Tools > Options on the Advanced tab, and then select the Encryption tab.

Known Issues

This section contains a list of known issues in the SonicOS Enhanced 4.2.1.0 release.

Application Firewall

Symptom	Condition / Workaround	Issue
Application Firewall policies configured to disable email attachments and add notification text do not provide notification text and can result in either connection timeout or garbled, duplicated email attachments.	Occurs when the following configurations are used for the Application Firewall policy: 1. Settings for client-server connection timeout: • Application Object: File Extension (Exact Match) • Action: Disable E-Mail Attachment – Add Text • Policy Type: SMTP Client Request / Destination Service = SMTP (Send E-Mail) / Client Side / Outgoing POP3 Server Response / Source Service = POP3 (Retrieve E-Mail) / Server Side / Incoming 2. Settings for garbled, duplicated attachments: • Application Object: File Name (Partial Match) • Action: Disable E-Mail Attachment – Add Text • Policy Type: SMTP Client Request / Destination Service = SMTP (Send E-Mail) / Client Side / Outgoing POP3 Server Response / Source Service = POP3 (Retrieve E-Mail) / Server Side / Incoming	73775

Security Services

Symptom	Condition / Workaround	Issue
SonicWALL CDP firmware patches can be blocked by content filtering. A permanent exception is needed for www.lassopatch.com (used by CDP 3.x and earlier) and Software.sonicwall.com (CDP 5.0 and higher).	Occurs when CFS on a SonicWALL firewall appliance is configured to block category 27.	83171

Users

Symptom	Condition / Workaround	Issue
Users get blocked pages when accessing the Internet because their access is filtered by the default CFS policy instead of the actual policies assigned to the user groups.	Occurs when a Single Sign-On agent reports blank user names when querying work stations for the logged in user information.	65334

Resolved Issues

This section contains a list of issues that are resolved in this SonicOS Enhanced 4.2.1.0 release.

Application Firewall

Symptom	Condition / Workaround	Issue
Application Firewall wizard uses “URL” and “URI” interchangeably.	Occurs when using the wizard to create a Web Access policy to look for access to specific URLs, but the Application Object is created for a URI object.	67037

Bandwidth Management

Symptom	Condition / Workaround	Issue
When throttling bandwidth from any interface, egress bandwidth management does not take effect in certain cases.	Occurs when PPPoE, L2TP, or PPTP is used and bandwidth management is enabled for outbound WAN traffic.	73244

GMS Firmware

Symptom	Condition / Workaround	Issue
The GMS gateway firewall edits the “GMSAgentAddrObj” object, instead of adding a new address object.	Occurs when attempting to add a new address object on the GMS gateway. Rather than creating a new object, the object “GMSAgentAddrObj” is edited. This affects the settings of the access rules and management VPN policies; the existing “GMSAgentAddrObj” is modified to the new object’s settings.	72674

High Availability

Symptom	Condition / Workaround	Issue
While sending traffic over a VPN tunnel from a Stateful HA pair to a peer firewall, with physical monitoring enabled on the WAN, a responder drops ESP packets and reports IPSec Replay and a wrong sequence number in the packets.	Occurs when the HA pair has a failover, a failback, and a second failover within a short time.	76301

Intrusion Prevention

Symptom	Condition / Workaround	Issue
Access to Google email is possible even when IPS is configured to block it.	Occurs when IPS is enabled with low priority blocking for Google email signatures, and access to https://gmail.com is attempted several times. Occurs on Firefox more than on Internet Explorer.	75084

Log

Symptom	Condition / Workaround	Issue
PRO systems get a page fault error and reboot.	Occurs when **Apply Filter** is clicked after configuring 255.255.255.255 as the destination interface in the filter settings on the Log > View page.	83157

Multicast

Symptom	Condition / Workaround	Issue
The multicast group address 224.0.0.0-224.0.0.255 is unexpectedly registered to the firewall, and the multicast traffic to these addresses is forwarded, but should not be.	Occurs when multicast is enabled on X0 and X1 interfaces, IGMP traffic is allowed from the WAN zone to the Multicast zone, and multicast traffic is sent from the WAN zone to any multicast address between 224.0.0.0-224.0.0.255.	83355

Networking

Symptom	Condition / Workaround	Issue
The SonicWALL L2TP Client does not connect to the Windows 2000/Cisco L2TP Server.	Occurs when attempting to connect a SonicWALL L2TP Client to a Cisco router configured as L2TP Server or Windows 2000 L2TP Server.	83331
Layer 2 VLAN filtering settings are lost after a firewall restart.	Occurs when the firewall is restarted after configuring a Layer 2 bridge pair with VLAN filtering settings, including selecting “Allowed Listed VLANs.”	82333
When using a SonicWALL PRO 4060, the WAN interface is unable to pass traffic when dialed into a Cisco L2TP server.	Occurs when the WAN interface uses the Layer 2 Tunneling Protocol (L2TP) client IP address received from the Cisco L2TP server, as the firewall did not support the L2TP shared secret feature.	78868
Layer 2 bridge mode negates the ability to pull DHCP leases from the internal server for WAN GroupVPN.	Occurs when configuring a WAN GroupVPN with XAuth, DHCP, and DHCP Over VPN with Internal Server used for GVC, and then attempting to connect with the L2 bridge mode enabled on any interface. **Workaround:** Configure downstream DHCP server and DHCP over VPN accordingly to allow a DHCP lease to be obtained.	50765

Security Services

Symptom	Condition / Workaround	Issue
HTML pages can experience long delays in loading.	Occurs when Content Filtering with Websense is enabled and Websense server is not available. The resolution enables detection of the availability of the Websense server before sending a request.	77560
Custom client AntiVirus configuration settings, such as the IP address Exclusion/Inclusion list, are cleared unexpectedly.	Occurs when Security Services licensing information is temporarily lost or reset.	74618
Gateway Anti-Virus displays a False Positive alert.	Occurs when attempting to pass traffic from a Linux system receiving mail on X3 to an Exchange server on X0. **Workaround:** Add the IP of the Linux box to the GAV exclusion list.	80546

System

Symptom	Condition / Workaround	Issue
SonicOS should disable TLS renegotiation for additional security within existing TLS connections .	Occurs when a client and server generate new keys and attempt TLS renegotiation for HTTPS management and SSL-VPN access.	85724
SSL Control blocks Go Daddy (wild card) certificates for forum.sonicwall.com as unidentified CA.	Occurs when enabling SSL control and selecting “Detect Certificate signed by an Untrusted CA.” **Workaround:** Add the blocked sites so the allowed list.	80913
A TZ 180W appliance reboots due to a problem with the flash writer task.	Occurs when the flash writer task refers to an un-initialized pointer in the code and frees memory that has not been allocated.	77689
A PRO 2040 appliance reboots due to a deadlock and task suspension.	Occurs when the policy callback runs from the NSM thread during a PBR route add/delete, instead of from the timer-scheduler task.	77079
The last object from the “Default ACL Deny Group” or the “Default ACL Allow Group” cannot be deleted.	Occurs when attempting to remove the last object in either group, leaving the group empty. **Workaround:** Create a dummy object as the last member of the group.	68393

Users

Symptom	Condition / Workaround	Issue
The SonicWALL appliance freezes with a buffer pool error when SSO is enabled.	Occurs when the SonicWALL appliance is configured with the SSO server IP address and shared key and then Apply is clicked.	81914
The SSO Agent causes the SonicWALL appliance to reboot when it is enabled.	Occurs when the SSO Agent and LDAP are both enabled on the firewall. When the SSO Agent is enabled, the SonicWALL appliance will go down, and then reboot.	79187
When importing LDAP user groups from Windows Active Directory, user groups are not populated in the Web management interface. The NSA E5500 has problems reading groups from the LDAP server.	Occurs when the user groups contain newline characters and '&' characters in their names.	63501

VPN

Symptom	Condition / Workaround	Issue
After a DHCP client gets a lease through DHCP over VPN, it cannot pass traffic to the WAN or the central VPN subnet.	Occurs on the central VPN subnet when the client pings a host on the central gateway and the reply is not forwarded to the interface to which the DHCP lease is bound. Occurs on the WAN when the source address of the ICMP packet is not translated to the WAN interface before it is forwarded to X1 interface, but it is sent out with the unchanged private IP address.	84604
After negotiation fails with the primary IPsec gateway at the remote site, the central site does not auto-negotiate with the secondary IPsec gateway, and the tunnel is not set up.	Occurs when the primary and secondary gateways are behind NAT in the remote site, Keep Alive is enabled, and the primary SA is expired.	83794
An excessively large local L2TP IP address pool causes the appliance to become unavailable.	Occurs when the L2TP server is enabled on the VPN > L2TP page, and the local L2TP IP pool is configured with a start and end address that causes the message: "This IP range has 167772160 IPs, seems too large, do you want to continue?" to be displayed. After clicking **OK**, the appliance becomes unresponsive after awhile.	82937
When a secondary WAN is disconnected, the VPN re-negotiates when established on the primary WAN.	Occurs when a secondary WAN is disconnected and a site-to-site VPN is established to a remote SonicWALL on the primary WAN interface.	82499
A tIkeUdpTask page fault occurs on a SonicWALL PRO remote unit.	Occurs when system traffic using more than 300 VPN tunnels is sustained on the remote unit for two days or more.	81602
DHCP clients cannot obtain an address from a DHCP server connected by site-to-site VPN.	Occurs when the client is connected to the LAN of a SonicWALL appliance, the LAN zone of this appliance is connected with a site-to-site VPN to a Trusted zone on the X3 interface of a second SonicWALL, and the DHCP server and address pool are enabled on the Trusted zone. This issue occurs with or without a configured IP relay address. **Workaround**: Enable the DHCP server and address pool on the LAN zone (X0) of the second SonicWALL.	73319/ 75888
A TZ 190 with 15 VPN Security Associations only shows 10 VPN SA policies after upgrading to SonicOS Enhanced 4.0.1.0, and no more than 10 VPN SA policies can be created.	Occurs when upgrading the firewall from SonicOS Enhanced 3.9.0.1 to 4.0.1.0.	72052

Wireless

Symptom	Condition / Workaround	Issue
A client laptop cannot associate to a SonicPointN when using WPA-EAP authentication, and no EAP authentication related packets can be captured.	Occurs when the SonicPointN is configured with WPA-EAP authentication type, and the first RADIUS server fields are left empty, while correct RADIUS information is provided in the secondary server fields.	85168
A wireless guest account cannot be repeatedly used to login.	Occurs when the system time of the device changes while a wireless guest is logged in.	83388
The SonicPoint A radio cannot be configured to 802.11a Turbo mode.	Occurs when connecting a SonicPoint with both a and g radios. After the SonicPoint is operational, attempting to configure the a radio to 108 Mbps – 802.11a Turbo mode fails.	83218
On TZ 180 appliances, an operational SonicPoint-N cannot be disabled with the checkbox.	Occurs when a SonicPoint-N is connected to a WLAN interface, and then the **Enable** checkbox is cleared and the **Apply** button is clicked to disable it after it is operational.	83185
“Enable MAC Address Filtering” setting for the Allow List does not work.	Occurs when attempting to enable the MAC Address Filtering option. Other MAC addresses that are not in the Allow List are still able to connect with the radio.	79741
Hiding the SSID for one of the Virtual Access Points (VAPs) causes the VAP to not function properly, as well as interfere with its connectivity to other VAPs.	Occurs after including two VAPs in a Group, and suppressing the SSID for one of the VAPs. The existing client associations to the suppressed SSID are affected, thus it disconnects the VAP.	79740
A SonicPoint stops accepting wireless client associations after a few hours or days.	Occurs when using SonicPoint b, g, or N, when using WPA2 authentication.	78311
When Wireless is enabled on the firewall, the appliance randomly locks up, and also displays multiple critical warnings.	Occurs randomly. There are no steps to reproduce.	77653
Access Point starts rejecting client associations with the status code 17.	Occurs when many clients access the system and there is heavy download traffic. **Workaround:** Reboot the box. You can also increase the max allowed client associations from 32 to a higher number. Another workaround is to reduce the cleanup interval for the aged out associations.	74908
WiFiSec can be bypassed by a IPSec Client passing through with a Route All policy, allowing unauthorized Internet access.	Occurs when launching a GVC connection to a third firewall on the Internet, which has a Route All VPN policy for the GVC user.	73075
Authenticating using the third-party option through WGS settings does not populate the USR field in syslog.	Occurs when configuring your appliance with a SonicPoint to support WGS with third-party authentication. **Workaround:** Use Local Users.	72664

Upgrading SonicOS Enhanced Image Procedures

The following procedures are for upgrading an existing SonicOS Enhanced image to a newer version:

Obtaining the Latest SonicOS Enhanced Image Version

To obtain a new SonicOS Enhanced firmware image file for your SonicWALL security appliance:

1. Connect to your mysonicwall.com account at http://www.mysonicwall.com.
2. Copy the new SonicOS Enhanced image file to a directory on your management station.

You can update the SonicOS Enhanced image on a SonicWALL security appliance remotely if the LAN interface or the WAN interface is configured for management access.

Saving a Backup Copy of Your Configuration Preferences

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of your current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

In addition to using the backup feature to save your current configuration settings to the SonicWALL security appliance, you can export the configuration preferences file to a directory on your local management station. This file serves as an external backup of the configuration preferences, and can be imported back into the SonicWALL security appliance.

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

1. On the System > Settings page, click **Create Backup**. Your configuration preferences are saved. The System Backup entry is displayed in the Firmware Management table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.

Upgrading to a SonicOS Enhanced Image with Current Preferences

Note: *SonicWALL security appliances do not support downgrading to a SonicOS Standard/Enhanced image and using the configuration preferences file from a higher version. If you are downgrading to a lower version of a SonicOS Standard/Enhanced image, you must select* ***Uploaded Firmware with Factory Defaults – New!*** *. You can import a preferences file previously saved from the downgrade version or reconfigure manually.*

1. Download the SonicOS Enhanced image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS Enhanced firmware image file, select the file, and click **Upload**.
4. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware – New!**
5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password to access the SonicWALL management interface. Your new SonicOS Enhanced image version information is listed on the **System > Settings** page.

Upgrading a SonicOS Enhanced Image with Factory Defaults

Perform the following steps to upload new firmware to your SonicWALL appliance and start it up using the default configuration:

1. Download the SonicOS Enhanced firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Create Backup**.
3. Click **Upload New Firmware**.
4. Browse to the location where you saved the SonicOS Enhanced firmware image file, select the file, and click **Upload**.
5. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware with Factory Default Settings**.
6. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware

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 use SafeMode to upgrade firmware on the SonicWALL security appliance, perform the following steps:

1. Connect your computer to the X0 / LAN port on the SonicWALL appliance and configure your IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.

   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 front of the security appliance for more than 20 seconds. The reset button is in a small hole next to the Console port.

   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

   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.*

3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. If you have made any configuration changes to the security appliance, make a backup copy of your current settings. Click **Create Backup Settings**.
5. Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS Enhanced firmware image, select the file, and click **Upload**.
6. Select the boot icon in the row for one of the following:
   - **Uploaded Firmware – New!**
     Use this option to restart the appliance with your current configuration settings.
   - **Uploaded Firmware with Factory Defaults – New!**
     Use this option to restart the appliance with default configuration settings.
7. In the confirmation dialog box, click **OK** to proceed.
8. After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicWALL management interface.

Upgrading Firmware on PRO Appliances with Older ROM Versions

This section describes how to upgrade to SonicOS Enhanced 4.2.1.0 on SonicWALL PRO 2040, 3060 and 4060 appliances with ROM versions 2.0, 2.1, and 2.5. In most cases, you must use SafeMode or SonicWALL GMS to perform a successful upgrade.

The following table shows the recommended methods of upgrading firmware on appliances with these 2.x ROM versions and the newer 3.1.0.2 ROM version. Selections marked with **Yes** are recommended, while those marked with **No** are not supported.

The "special firmware" refers to firmware that is ONLY used to upgrade the ROM from a very low version, such as 2.x.x.x, to a higher version, such as 3.x.x.x. This ROM upgrade firmware is uploaded to the PRO appliance in the same way that SonicOS Enhanced firmware is uploaded.

Platform	ROM Version	Upgrading firmware				
		From 2.x.x.x to 4.2.1.0 (LAN/WAN/ HTTP/HTTPS)	From 3.1.0.8 to 4.2.1.0 (LAN/WAN/ HTTP/HTTPS)	From 4.1.0.0 to 4.2.1.0 (LAN/WAN/ HTTP/HTTPS)	From SafeMode (LAN/HTTP)	From GMS (Management tunnel at group level)
Pro 2040	2.1.0.0	No	No	No	**Yes**	**Yes** (with Special Firmware)
	3.1.0.2	No	**Yes**	**Yes**	**Yes**	**Yes**
Pro 3060	2.0.1.3	No	No	**Yes**	**Yes**	**Yes**
	3.1.0.2	No	**Yes**			
Pro 4060	2.5.0.0a1	No	No	No	**Yes**	**Yes** (with Special Firmware)
	3.1.0.2	No	**Yes**	**Yes**	**Yes**	**Yes**

To upgrade from SafeMode:

This method is supported for all PRO appliances running any ROM version.

See the Using SafeMode to Upgrade Firmware section for instructions.

To upgrade from the LAN or WAN interface, using HTTP or HTTPS:

This method is supported for SonicWALL PRO series appliances running ROM version 2.x.x.x, when upgrading from SonicOS Enhanced 3.1.0.8 or newer. The special ROM upgrade firmware is required for appliances with ROM version 2.x.x.x.

1. Log in to the PRO management interface from the LAN or WAN interface.
2. Navigate to the System > Settings page.
3. Load the PRO with the special ROM upgrade firmware and wait while the PRO reboots twice.
4. After the PRO is booted up, load it with the latest SonicOS Enhanced 4.2.1.0 firmware from the LAN or WAN interface.
5. Wait while the PRO reboots with the SonicOS Enhanced 4.2.1.0 firmware.

To upgrade from SonicWALL GMS:

This method is supported for all SonicWALL PRO appliances running any ROM version, but requires the special ROM upgrade firmware for appliances with ROM version 2.x.x.x.

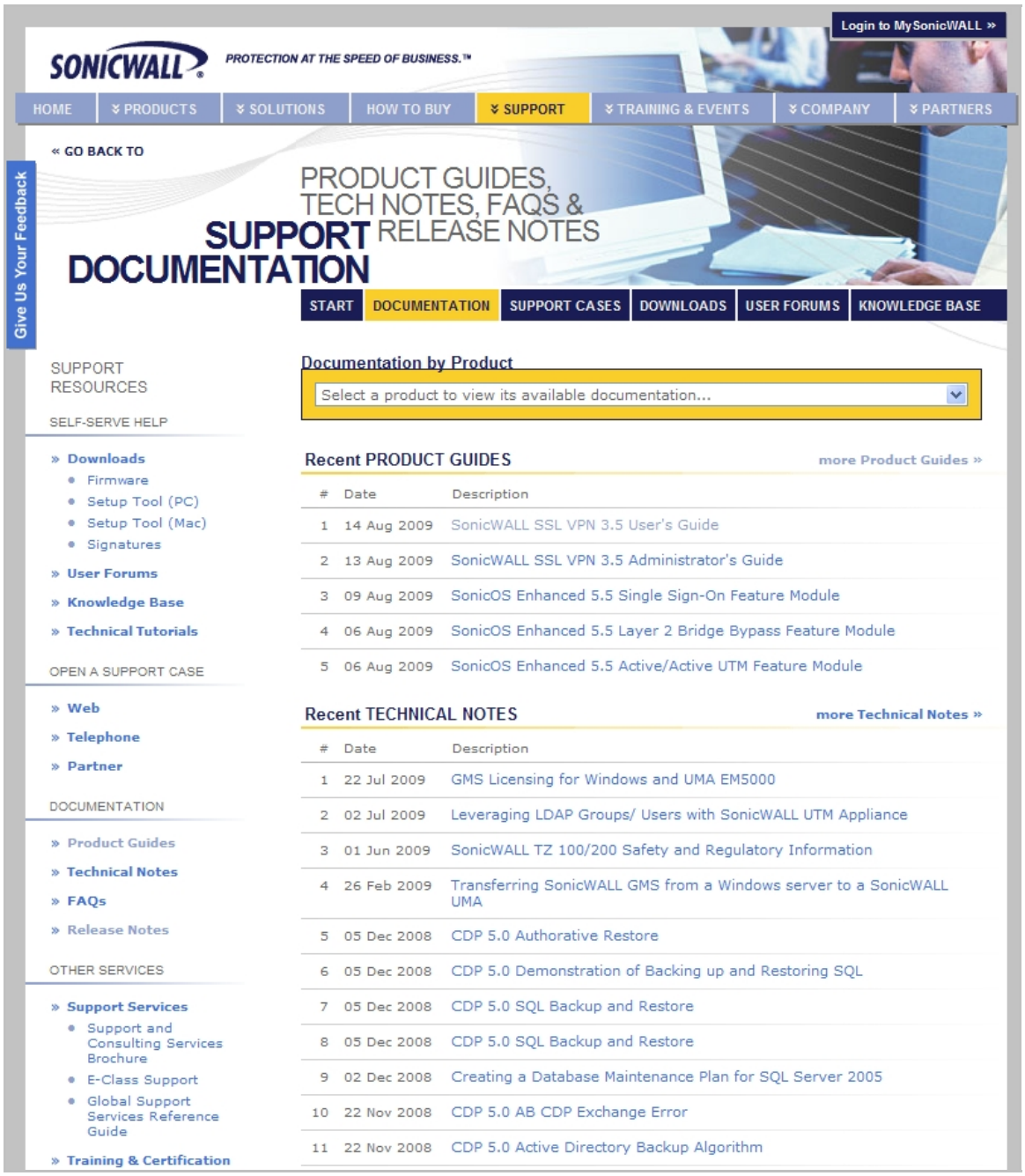
1. Use SonicWALL GMS to manage the PRO appliance.
2. Navigate to the System > Settings page from GMS.
3. Load the PRO with the special ROM upgrade firmware and wait while the PRO reboots twice.
4. After the PRO is booted up, load it with the latest SonicOS Enhanced 4.2.1.0 firmware through GMS.
5. Wait while the PRO reboots with the SonicOS Enhanced 4.2.1.0 firmware.

Related Technical Documentation

SonicWALL user guides and reference documentation is available at the SonicWALL Technical Documentation Online Library:

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

For basic and advanced deployment examples, refer to SonicOS Guides and SonicOS TechNotes available on the Web site.



Last updated: 12/16/2009