

# Release Notes

## Contents

---

Platform Compatibility .....	1
New Features in SonicOS 5.2 .....	2
End of Support for N2H2 .....	2
Known Issues .....	3
Resolved Issues .....	5
Upgrading SonicOS Enhanced Image Procedures .....	7
Related Technical Documentation .....	10

## Platform Compatibility

---

The SonicOS Enhanced 5.2 release is supported on the following SonicWALL security appliances:

- SonicWALL TZ 210
- SonicWALL TZ 210 Wireless-N
- SonicWALL NSA 240
- SonicWALL NSA 2400
- SonicWALL NSA 3500
- SonicWALL NSA 4500
- SonicWALL NSA 5000
- SonicWALL NSA E5500
- SonicWALL NSA E6500
- SonicWALL NSA E7500

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

### 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.

# Release Notes

## New Features in SonicOS 5.2

---

SonicOS Enhanced 5.2 release introduces the following new features:

- **Apple Bonjour Support** – SonicOS Enhanced 5.2 introduces support for Apple's Bonjour protocol (also known as Rendezvous or zero-configuration networking). Bonjour enables automatic discovery of computers, devices, and services on IP networks without the need to enter IP addresses or configure DNS servers.
- **Apple iPhone Support** – SonicOS Enhanced 5.2 supports L2TP termination from the Apple iPhone.
- **Connection Limiting** – To provide an additional layer of security against distributed denial-of-service (DDoS) attacks, the number of connections that can be initiated from or to an individual IP address can be limited.
- **Content Filtering Enhancements** – The following enhancements have been added to SonicWALL Content Filtering Service (CFS):
  - **CFS Policy per IP Address** – Appliances with SonicWALL CFS Premium can now assign specific CFS policies to ranges of IP address ranges. This provides the ability to segment CFS policies within a single zone.
  - **Fully Customizable Block Page** – The web page that is displayed when a user attempts to access a blocked site can now be fully customized. This enables organizations to brand the block page and display any organization-specific information.
  - **Safe Search Enforcement** - Safe Search Enforcement allows you to force Web search sites like Google and Yahoo that have content restriction options always to use their strictest settings.
- **MD5 Certificate Detection and Blocking** – The SSL Control feature now provides the ability to block or log connections that use a certificate signed with an MD5 hash. (SonicWALL security appliances now use SHA1 to sign their self-signed certificates instead of MD5.)
- **New Firmware Auto-Update** – Firmware Auto-Update helps ensure that your SonicWALL security appliance has the latest firmware release. This feature automatically notifies the administrator when a new firmware release is available, and it can optionally download it automatically.
- **Outbound Inspection for Gateway Anti-Virus** – The SonicWALL Gateway Anti-Virus security service now provides outbound inspection for HTTP, FTP, and TCP traffic.
- **SonicPoint 802.11n Support** – SonicOS Enhanced 5.2 supports the new SonicPoint-N, which provides next-generation 802.11n wireless network connectivity.
- **SonicWALL SSL VPN NetExtender Support** – SonicOS Enhanced 5.2 provides support for SonicWALL's SSL VPN NetExtender, which was previously available only on the SonicWALL SSL VPN platforms. SonicWALL NetExtender is a transparent software application for users that enables remote users to securely connect to the remote network.
- **Support Services Page** – The new Support Services page displays a summary of the current status of support services for the SonicWALL security appliance. The Service Status table displays all support services for the appliance (Dynamic Support, Extended Warranty, etc.), their current status, and their expiration date.

## End of Support for N2H2

---

Beginning March 17th, 2009, all E-Class NSA Series, NSA Series, and TZ Series appliances running SonicOS 5.2.0.1 and later will no longer provide software support for the N2H2 Sentian Content Filtering Service. For more information, please see:

[http://www.sonicwall.com/downloads/End\\_of\\_Feature\\_Support\\_Notification\\_N2H2\\_Content\\_Filtering.pdf](http://www.sonicwall.com/downloads/End_of_Feature_Support_Notification_N2H2_Content_Filtering.pdf)

# Release Notes

## Known Issues

This section contains a list of known issues in the SonicOS Enhanced 5.2 release.

### Logging

Symptom	Condition / Workaround	Issue
A delay occurs before events are logged, and clearing or refreshing the Log > View page has no effect.	Occurs when actions are taken that generate many log messages in a short time. For example, if one hundred or more user guest accounts are automatically created and then pruned within a few minutes, this should generate a log message for every account creation and pruning.	76681

### Networking

Symptom	Condition / Workaround	Issue
The VLAN Filtering Block List fails to block traffic from a VLAN from reaching a host on the WAN zone.	Occurs when using L2 Bridge Mode and a VLAN is added to the VLAN Filtering Block List.	75221
OSPF becomes disabled on the X1 interface if the IP address is changed and the appliance is then rebooted.	Occurs when OSPF is enabled on the X1 interface, the IP address for the X1 interface is changed, and the appliance is then rebooted.	75228
L2 Bridge VLAN filter settings are lost in the management interface and in the TSR.	Occurs when the appliance is restarted after configuring a Layer 2 Bridge between two of the interfaces, with <b>L2 Bridge VLAN Filter</b> configured to block traffic from some VLANs.	75041
A modified access rule is replicated after a reboot of the device. The modified access rule is still present, but the original access rule is recreated.	Occurs when an access rule is modified to or from the WLAN zone such as WLAN > WAN or LAN > WLAN. It is modified by selecting a choice in the <b>Users allowed</b> drop-down list.	74956
Incoming packets through a WAN L2TP tunnel are dropped by the appliance.	Occurs with an active L2TP tunnel on the WAN interface.	74929

### Upgrading

Symptom	Condition / Workaround	Issue
Upgrading to SonicOS Enhanced 5.2 causes the deletion of rules that use service groups with a mix of HTTP/HTTPS/SSH management services and non-management services.	Occurs when upgrading from SonicOS Enhanced 5.1 to SonicOS Enhanced 5.2.	77660
On TZ 210 Series appliances only, upgrading from SonicOS Enhanced 5.1.3.2 to SonicOS Enhanced 5.2.0.1 fails under certain circumstances.	Occurs when a steady flow of traffic is passing through the TZ 210 Series appliance or TZ 210 Series HA pair at the same time that the upgrade is attempted. <b>Workaround:</b> Restart the TZ 210 Series appliance, or both appliances in an HA pair, and then perform the upgrade.	75987

# Release Notes

## VPN

Symptom	Condition / Workaround	Issue
A multicast stream does not pass through a site-to-site VPN tunnel between two SonicWALL security appliances.	Occurs when the site-to-site VPN tunnel is in IKEv2 mode. Multicast traffic can pass when the VPN tunnel is in Main or Aggressive mode.	76639
An appliance configured for a site-to-site VPN drops all incoming packets. Packets can be sent to the remote site.	Occurs when the WAN interface of the appliance is configured in L2TP mode.	74999

## Wireless

Symptom	Condition / Workaround	Issue
Attempting to change the SonicPoint-N setting individually results in the error message "Error: Invalid Country Code".	Occurs when the SonicPoint-N is managed by an international SonicWALL security appliance. <b>Workaround:</b> Change the SonicPoint-N provisioning profile and then re-synchronize the SonicPoint-N configuration from the provisioning profile.	77103

# Release Notes

## Resolved Issues

This section contains a list of issues that are resolved in the SonicOS Enhanced 5.2.0.1 release.

### High Availability

Symptom	Condition / Workaround	Issue
In a WAN Load Balancing configuration, the Primary WAN interface does not return to the Available state after connectivity is restored following a failover.	Occurs when using WLB with Active/Passive selected and Preempt disabled. <b>Workaround:</b> Disable WLB probing.	73399
In a Stateful HA pair, an IKEv1 SA is not synchronized on the Backup unit after failing over and then failing back.	Occurs when IKEv1 and IPsec security associations are configured between the HA pair and a peer, with preempt and physical monitoring enabled on the HA pair. A failover occurs from the Primary to the Backup appliance, then the Primary reboots and preempts the Backup to cause a failback to the Primary as the Active unit. The Backup reboots, after which the IKE SA is no longer synchronized on the Backup unit.	68190

### Networking

Symptom	Condition / Workaround	Issue
The appliance fails to pass LAN to WAN traffic when the WAN interface is connected using PPTP.	Occurs when the WAN interface uses a PPTP connection.	75334
A computer that is connected to the LAN zone of the appliance on a port other than X0 is unreachable by a remote computer over a VPN.	Occurs when the appliance is configured in DHCP over VPN mode. The appliance can send and receive traffic over the VPN tunnel, but computer connected to the LAN on a non-X0 port cannot receive VPN traffic.	75068
A SonicWALL appliance configured to forward IKE and ESP inbound traffic does not pass ESP traffic to an internal VPN gateway.	Occurs when correct inbound rules and NAT policies are configured and NAT traversal is disabled, and when attempting to use Global VPN Client and S2S to pass traffic.	73974
An access rule change is not enforced immediately for a TCP connection over a L2 bridge pair.	Occurs when a L2 bridge pair is configured on the X2 and X3 interfaces and an access rule is added to the X2 to X3 access policy. However, if a rule is added from the LAN zone to another zone and is then assigned to the L2 bridge interface, the rule is enforced immediately.	71001
The source IP address of a DHCP discover packet is changed to the IP Relay address when the request passes through a SonicWALL appliance.	Occurs when DHCP over VPN is enabled and the SonicWALL is acting as a relay agent.	69297
The appliance fails to implement the configured OSPF Router-ID for an interface. Instead it continues to use the IP address of the interface.	Occurs when the <b>OSPF Router-ID</b> field is modified on the <b>Network &gt; Routing</b> page.	67129
The OSPF router ID (such as 10.0.0.2) retains its previous value after being changed.	Occurs when the OSPF authentication mode is "simple password".	66113

# Release Notes

## VPN

Symptom	Condition / Workaround	Issue
A SPD/SADB mismatch occurs in a hub and spoke VPN topology causing all VPN traffic to be sent to the wrong destination.	Occurs when a SonicWALL NSA 240 appliance has two VPN policies, such as one with a SonicWALL NSA 2400 and the other with a SonicWALL Pro 4060. Both policies on the NSA 240 have the same local network, and the policies on the NSA 2400 and PRO 4060 have overlapped local networks.	76705
SonicWALL Global VPN Client connections cause S2S VPNs to begin dropping TCP sessions (e.g., RDP connections).	Occurs when overlapping VPN and routes are configured on different interfaces, a TCP session is created via the tunnel, and then a GVC user connects causing the addition of a route which forces a route re-lookup for the TCP session. The re-lookup finds the overlapping route and assumes the connection moved from one interface to another and closes the session.	74076
VPN traffic does not pass through a SonicWALL NSA unit when the VPN gateway is behind the SonicWALL.	Occurs when NAT traversal is used to forward IKE traffic inbound to the internal gateway device from the X1 IP address of the SonicWALL, and the VPN gateway private IP address is mapped to the SonicWALL WAN interface IP address.	73100
Traffic from the LAN side of a SonicWALL NSA appliance bound for a VPN'd network behind a SonicWALL TZ 190W is dropped at the NSA appliance with the following error: "SA not found on lookup by SPI for outbound pkt."	Occurs when there are multiple failovers on the SonicWALL TZ190W from PPPoE WAN to WWAN and back.	70256

# Release Notes

## 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 .....	7
Saving a Backup Copy of Your Configuration Preferences .....	7
Importing Preferences to SonicOS Enhanced 5.2 on SonicWALL TZ 210 Series.....	7
Importing Preferences from SonicOS Enhanced 4.0 to SonicOS Enhanced 5.2 on SonicWALL NSA Series.....	8
Upgrading a SonicOS Enhanced Image with Current Preferences .....	8
Upgrading a SonicOS Enhanced Image with Factory Defaults .....	9
Using SafeMode to Upgrade Firmware.....	9

### **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.

### **Importing Preferences to SonicOS Enhanced 5.2 on SonicWALL TZ 210 Series**

Preferences importing to the SonicWALL TZ 210 Series appliances is generally supported from the following SonicWALL appliances running SonicOS Enhanced:

- NSA Series
- NSA E-Class Series
- TZ 190/180/170 Series
- PRO Series

There are certain exceptions to preferences importing on TZ 210 Series appliances running SonicOS Enhanced 5.2. Preferences cannot be imported in the following cases:

- From a PRO 5060 with optical fiber interfaces where VLAN interfaces have been created
- From wireless SonicWALL appliances to the TZ 210 (non-wireless)

Full support for preferences importing from these appliances is targeted for a future release. At that time, you will need to upgrade your firmware to the latest SonicOS Enhanced maintenance release available on MySonicWALL.

# Release Notes

## **Importing Preferences from SonicOS Enhanced 4.0 to SonicOS Enhanced 5.2 on SonicWALL NSA Series**

You can import the preferences from most SonicWALL PRO appliances running SonicOS Enhanced 4.0 or higher into a SonicWALL NSA appliance running SonicOS Enhanced 5.2. Preference importing is supported from the following appliances:

- SonicWALL PRO 2040
- SonicWALL PRO 3060
- SonicWALL PRO 4060
- SonicWALL PRO 4100
- SonicWALL PRO 5060



**Note:** Importing preferences from units running SonicOS Standard is *not* supported.

Perform the following steps to import preferences from an appliance running SonicOS Enhanced 4.0 or higher:

1. Verify that the target SonicWALL security appliance is correctly registered and licensed.
2. If the original unit has High Availability (HA) enabled, disable HA.
3. If the original unit is a SonicWALL PRO 4100, navigate to the **Network > Interfaces** screen and configure the **Zone** setting to **Unassigned** for the following interfaces:
  - If the target system is a SonicWALL NSA E7500, E6500, or E5500 - Interfaces X8 and X9
  - If the target system is a SonicWALL NSA 5000, 4500, or 3500 - Interfaces X6, X7, X8 and X9This is necessary because the SonicWALL E-Class NSA appliances have 8 interfaces rather than 10 as on the SonicWALL PRO 4100, and the SonicWALL NSA 5000/4500/3500 appliances have 6 interfaces. Settings associated with the affected interfaces are not maintained after the upgrade.
4. Export the preferences file from the original unit.
5. Import the preferences file into the target product.
6. If HA was originally enabled, do the following:
  - Connect the new HA pair together with a cable between the designated HA ports on each appliance.
  - In the management interface, re-enable HA and change the **Serial Number** field for the Backup SonicWALL to correspond to the new backup unit.

To import preferences from SonicWALL appliances running a version of SonicOS Enhanced prior to 4.0, you must contact the SonicWALL Customer Support Technical Assistance Center (TAC). SonicWALL TAC will assist you in converting your preferences file to SonicOS Enhanced 4.0.

## **Upgrading a SonicOS Enhanced Image with Current Preferences**

Perform the following steps to upload new firmware to your SonicWALL appliance and use your current configuration settings upon startup:

1. Download the SonicOS Enhanced firmware image file from [mysonicwall.com](http://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**.
5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password. Your new SonicOS Enhanced image version information is listed on the System > Settings page.

# Release Notes

## **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](http://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 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.
2. Do one of the following to restart the appliance in SafeMode:
  - 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 USB ports.
  - Use the LCD control buttons on the front bezel to set the appliance to Safe Mode. Once selected, the LCD displays a confirmation prompt. Select **Y** and press the **Right** button to confirm. The SonicWALL security appliance changes to SafeMode.

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

**Note:** Holding the reset button for two seconds will send a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.

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, select the **Create Backup On Next Boot** checkbox to make a backup copy of your current settings. Your settings will be saved when the appliance restarts.
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.

# Release Notes

## 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.

**SONICWALL** PROTECTION AT THE SPEED OF BUSINESS.™

HOME PRODUCTS SOLUTIONS HOW TO BUY SUPPORT TRAINING & EVENTS COMPANY PARTNERS

« GO BACK TO

### PRODUCT APPLIANCE SUPPORT

NSA E7500 APPLIANCE

Give Us Your Feedback

Support Resources

SELF-SERVE HELP

- » Downloads
  - Firmware
  - Setup Tool (PC)
  - Setup Tool (Mac)
  - Signatures
- » User Forums
- » Knowledge Portal

OPEN A SUPPORT CASE

- » Web
- » Telephone
- » Partner

REFERENCE LIBRARY

- » Product Guides
- » Technical Notes
- » FAQs
- » Release Notes

OTHER SERVICES

- » Support Services
  - Support and Consulting Services Brochure
  - E-Class Support
  - Global Support Services Reference Guide
- » Training & Certification

STAY IN TOUCH

- » Email Newsletters

#### Recent PRODUCT GUIDES

#	Date	Description
1	16 Oct 2008	SonicOS Enhanced 5.1 Administrator's Guide
2	19 Aug 2008	SonicOS Enhanced 5.1 Application Firewall Feature Module
3	13 Jun 2008	SonicOS Enhanced 5.0 Single Sign-On Feature Module
4	13 Jun 2008	SonicOS Enhanced 5.0 Administrator's Guide
5	20 May 2008	NSA 5.0.2.0 Documents Zip File

[view all Product Guides »](#)

#### Recent TECHNICAL NOTES

#	Date	Description
1	04 Aug 2008	Integrating SonicWALL SonicOS Enhanced PRO-Series/ E-Class UTM Appliances with HP ProCurve Manager Plus/ Network Immunity Manager
2	11 Jun 2008	Cisco Catalyst Switch Configuration for SonicWALL Devices
3	01 Feb 2008	VPN Consortium Interoperability for SonicOS Enhanced
4	11 Jan 2008	SonicWALL Clean VPN
5	16 Nov 2007	Configuring ViewPoint 4 With MS SQL Server 2005

[view all Technical Notes »](#)

#### Recent SERVICE BULLETINS

#	Date	Description
---	------	-------------

[view all Service Bulletins »](#)

#### Recent FAQs

#	Date	Description
1	21 Mar 2008	SonicWALL E-Class NSA FAQ

[view all FAQs »](#)

#### Recent RELEASE NOTES

#	Date	Description
1	04 Nov 2008	SonicOS Enhanced 5.1.0.8 Release Notes
2	02 Sep 2008	SonicOS Enhanced 5.1.0.4 Release Notes
3	07 Aug 2008	SonicOS Enhanced 5.1.0.2 Release Notes

[more Release Notes »](#)

Last updated: 7/27/2010