Release Notes

SonicOS

SonicOS Enhanced 5.1.0.2 Release Notes

Contents

Platform Compatibility

The SonicOS Enhanced 5.1.0.2 release is supported on the following SonicWALL Network Security Appliance (NSA) appliances:

- SonicWALL NSA E7500
- SonicWALL NSA E6500
- SonicWALL NSA E5500
- SonicWALL NSA 5000
- SonicWALL NSA 4500
- SonicWALL NSA 3500
- SonicWALL NSA 2400

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.

Key Features

Application Firewall Enhancements: SonicOS Enhanced 5.1 includes several enhancements that allow Application Firewall to be used to apply SonicWALL Intrusion Prevention Service (IPS). IPS can still be configured using the Security Services > Intrusion Prevention page. But configuring IPS through Application Firewall allows for granular control over the configuration and actions that can be applied to IPS signatures.

The Application Firewall enhancements include two new application object types:

- **Signature List Objects** – Application objects consisting of an individual IPS signature or a list of multiple IPS signatures. Current IPS signatures are grouped into a number of categories (such as Backdoor, Virus, SMTP, etc.).
- **Signature Category Objects** – Application objects consisting of categories of IPS signatures (such as Backdoor, Virus, SMTP, etc.). Multiple categories can be combined into a single application object.

A new **Dynamic Content** application policy is used to apply these signature-based application objects. These dynamic policies have all of the granular control options available in application firewall, but they dynamically update to include the latest IPS signatures that are added to the Extensive Signature Database.

Known Issues

This section contains a list of known issues in the SonicOS Enhanced 5.1.0.2 release.

High Availability

Symptom	Condition / Workaround	Issue
The appliance responds to pings on its monitoring interface IP using a Virtual MAC address instead of its actual MAC address.	Occurs when the appliance is part of a High Availability pair.	52413
In an HA Pair, changes made from the LCD on the front of the primary unit are not synchronized to the backup unit.	Occurs when a setting such as the IP address of a DNS server is changed in the LCD of the primary unit rather than in the Web-based management interface.	53215
Changes made to a backup appliance are not forwarded to the primary appliance during a High Availability failover. The Sync-Prefs command fails.	Occurs when the changes made to the backup appliance are done through the CLI. **Workaround**: Use the GUI to make any changes. Ideally, do not use the backup appliance to do customization, instead wait until the primary appliance comes back online.	64821
A primary appliance may lose its clients' DHCP leases during a High Availability (HA) failover.	Occurs when using Stateful HA with preempt mode on. The backup appliance assumes the clients' DHCP leases correctly, but once the primary appliance regains control, it no longer has the leases.	67296
A high availability pair cannot upgrade to a new firmware version when the devices are passing a large amount of traffic.	Occurs on a SonicWALL NSA 4500 high availability pair. **Workaround**: Stop the traffic and perform the firmware update.	67898
IKE SAs are not synchronized after failback occurs on a high availability pair.	Occurs on a high availability pair configured for an IKEv1 site-to-site tunnel. After the primary fails, the backup becomes active, and the primary then becomes active again, the backup unit does not have the IKE SAs.	68190

Log

Symptom	Condition / Workaround	Issue
Log messages are not displayed.	Occurs on a SonicWALL NSA 2400 under certain load conditions.	67819

Networking

Symptom	Condition / Workaround	Issue
LAN > WAN access rules cannot be edited, and adding a new LAN > WAN access rule overwrites an existing rule.	Occurs when the WAN zone is configured as a VLAN sub-interface. **Workaround**: Reboot the appliance with factory defaults.	66124
Routes remain active in the routing table after their interfaces become disconnected.	Occurs when interfaces with active routes are disconnected.	66820

A route on a disconnected interface becomes active after the device is rebooted, even though the interface remains disconnected.	Occurs when a policy-based route is configured with the **Disable route when interface is disconnected** option, the interface is disconnected, and the device is rebooted.	70104
IP Helper does not pass NetBOIS traffic from the X0 LAN subnet to the X3 LAN subnet.	Occurs when a GVC client connects to the X0 LAN and attempts to send traffic to a PC on the X3 LAN subnet. Windows NetBOIS broadcast is configured for the WAN GroupVPN and IP Helper is configured for NetBOIS from the X0 LAN subnet to the X3 LAN subnet.	70467

System

Symptom	Condition / Workaround	Issue
Blind Transfer SIP call requests cannot be completed.	Occurs when the phones are registered to a SIP Proxy server in the LAN or in the DMZ behind a SonicWALL NSA.	52286
While downloading the TSR, the status bar displays “Dynamic update connection failure detected.”	Occurs when attempting to download the TSR when the Diagnostic Tool is set to “Multi-Core Monitor”. **Workaround**: Prior to the TSR download, set the Diagnostic Tool to an option other than the default “Multi-Core Monitor”.	53636
Under certain conditions, restoring a SonicWALL NSA to factory defaults does not reset the administrator’s password to the default credentials.	Occurs when using the appliance’s front bezel LCD interface to reboot the appliance to factory defaults.	64833
The firewall may be sending heartbeat messages at inconsistent intervals to the GMS server, resulting in false-positive alerts of unit failures.	Can occur in certain high traffic environments.	67104

VPN

Symptom	Condition / Workaround	Issue
A site-to-site VPN tunnel drops large-sized packets.	Occurs when the WAN MTU size is changed from the default 1500 to a smaller value, such as 700. **Workaround**: Set the WAN MTU size to 1500 or larger.	67082
Traffic is only passed in one direction on a VPN tunnel to a SonicWALL NSA 2400.	Occurs about half of the time on all VPN tunnels configured on the SonicWALL NSA 2400.	68804

Wireless

Symptom	Condition / Workaround	Issue
The default GroupVPN policy which was created by the ‘Allow Unauthenticated VPN Client Access’ option is unexpectedly deleted.	Occurs when the parent VLAN subnet that created the GroupVPN policy is deleted, and the policy does not use any other subnets. **Workaround**: Reboot the appliance. The deleted GroupVPN policy is restored after the reboot.	65299
Client Anti-Virus Enforcement blocks rather	Occurs when the client is on the WLAN zone and	65692

than redirecting some clients that do not meet AV requirements.	does not meet the AV requirements. Such clients should be directed to update their Anti-Virus software to be compliant with AV Enforcement.	
The DHCP client gets a lease from the local DHCP server rather than from the DHCP server available via the VPN tunnel.	Occurs when the VPN policy specifies that clients should obtain IP addresses through the VPN tunnel, but a DHCP server exists on the client's local network.	66100
Some user-created LAN-to-WAN Access Rules cannot be changed.	Occurs when the WAN connection is set up on a sub-interface while the main interface is still unassigned.	66124

Resolved Known Issues

This section contains a list of resolved issues in the SonicOS Enhanced 5.1.0.2 release.

Application Firewall

Symptom	Condition	Issue
Application Firewall adds incorrect text to emails that have attachments.	Occurs when an Application Firewall policy is configured to delete email attachments and add text.	64951
A web browser script error occurs when deleting Application Firewall objects and actions.	Occurs when deleting objects and actions in Application Firewall.	67798
Application Firewall policies fail and display a long error message.	Occurs when using Application Firewall policies with objects that contain keywords longer than 48 characters hexadecimal or longer than 24 characters non-hexadecimal do not work.	68269

Log

Symptom	Condition	Issue
Some IP addresses are not resolved to domain names on the **Log > Name Resolution** page.	Occurs when the Name Resolution Method is set to **DNS** or **DNS then NetBIOS**.	67267

High Availability / Stateful High Availability

Symptom	Condition	Issue
The NAT policies that control WAN Load Balancing (WLB) traffic flow between a High Availability (HA) pair may fail after a failover.	Occurs after a failback to the primary device when WLB is enabled.	67372
Attempting to delete a VLAN interface that had been configured for high availability logical monitoring causes the appliance to reboot.	Occurs when stateful High Availability is enabled and the administrator attempts to delete a VLAN interface that was configured for logical monitoring, and the interface had passed traffic.	67493

System

Symptom	Condition	Issue
Yahoo messenger and MSN automatically log off on an administrator's local computer.	Occurs when the administrator logs out of the SonicWALL management interface. Issue occurs even when the administrator is automatically logged out due to inactivity.	66828
The SonicWALL security appliance does not send an SNMP trap (OID 646) when an interface regains connectivity.	Occurs when an interface goes down and then regains connectivity.	69661

Wireless

Symptom	Condition	Issue
A VLAN sub-interface can not be assigned to a WAN interface.	Occurs in the current version of SonicOS Enhanced.	51791
FTP clients sometimes timeout while doing virus checking.	Occurs when the file being transferred does indeed contain a virus. The file is blocked by the security services, but the FTP connection is not reset on the LAN side. The LAN side ends up waiting for the file until the connection times out.	65335
Pull-down menus on the SonicOS UI do not display all of the items in the menu when a wireless guest user with admin privileges accesses them.	Occurs when using the Firefox browser as a wireless guest user with admin privileges. The UI functions properly when using Internet Explorer.	68128
A SonicPoint fails to detect a Toshiba TDP-TW100U projector when a client is using the Toshiba Data Projector utility to attempt to connect to the projector.	Occurs when the client and the projector are connected to a single SonicPoint. The utility functions properly if the client and projector are connected to separate SonicPoints.	68510

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.

Importing Preferences from SonicOS Enhanced 4.0 to SonicOS Enhanced 5.1

You can import the preferences from most SonicWALL PRO appliances running SonicOS Enhanced 4.0 or higher into a SonicWALL E-Class NSA appliance running SonicOS Enhanced 5.1. 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 X9

   This 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 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.

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 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 one second. 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.
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.

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: 8/1/2008