Release Notes

Contents

Platform Compatibility

The SonicOS 5.8.1.2 release is supported on the following SonicWALL Deep Packet Inspection (DPI) security appliances:

- SonicWALL NSA 250M / 250M Wireless
- SonicWALL NSA 220 / 220 Wireless

The SonicWALL WAN Acceleration Appliance Series (WXA 500 Live CD, WXA 2000 appliance, WXA 4000 appliance, WXA 5000 Virtual Appliance) are also supported for use with NSA appliances running 5.8.1.2. The minimum recommended Firmware version for WXA Series is 1.0.12.

Browser Support

SonicOS with Visualization uses advanced browser technologies such as HTML5, which are supported in most recent browsers. SonicWALL recommends using the latest Chrome, Firefox, Internet Explorer, or Safari browsers for administration of SonicOS.

This release supports the following Web browsers:

- Chrome 11.0 and higher (recommended browser for dashboard real-time graphics display)
- Firefox 4.0 and higher
- Internet Explorer 8.0 and higher (do not use compatibility mode)
- Safari 5.0 and higher

Mobile device browsers are not recommended for SonicWALL appliance system administration.

New Features in SonicOS 5.8.1.2

This section describes the new features supported in the SonicOS 5.8.1.2 release.

SonicWALL NSA Module Support

SonicOS 5.8.1.2 introduces support for the following SonicWALL NSA modules on the NSA 250M series appliances:

WARNING: You MUST power down the appliance before installing or replacing the modules.

- **1 Port ADSL (RJ-11) Annex A**– Provides Asymmetric Digital Subscriber Line (ADSL) over plain old telephone service (POTS) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.3 Mbit/s.

- **1 Port ADSL (RJ-45) Annex B**– Provides Asymmetric Digital Subscriber Line (ADSL) over an Integrated Services Digital Network (ISDN) with a downstream rate of 12.0 Mbit/s and an upstream rate of 1.8 Mbit/s.

- **1-port T1/E1 Module** – Provides the connection of a T1 or E1 (digitally multiplexed telecommunications carrier system) circuit to a SonicWALL firewall using a RJ-45 jack.

- **2-port LAN Bypass Module** – Removes a single point of failure so that essential business communication can continue while a network failure is diagnosed and resolved.
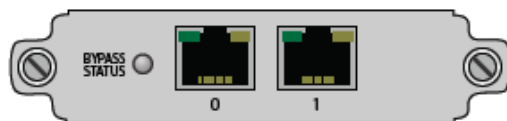
- **2-Port SFP Module –** A small form-factor pluggable (SFP) network interface module.

SonicOS 5.8.1.2 Release Notes for the NSA 220/250M Series Appliances
P/N 232-000648-00 Rev A

2

Supported Features by Appliance Model

The following table lists the key features in the SonicOS 5.8.0.x, 5.8.1.0, 5.8.1.2 releases, and which are supported on the SonicWALL NSA 220 and 250M series appliances.

Features Supported on NSA 220 and NSA 250M Series	Features Not Supported on NSA 220 and NSA 250M Series
DPI-SSL	Link Aggregation
NSA Modules (supported only on NSA 250M Series)	Port Redundancy
Wireless Client Bridge Support	Wire Mode
App Flow Monitor	
Real-Time Monitor	
Top Global Malware	
Log Monitor	
Connection Monitor	
Packet Monitor	
Log > Flow Reporting	
App Control Advanced	
App Rules	
Cloud GAV	
NTP Auth Type	
CFS Enhancements	
IPFIX & NetFlow Reporting	
VLAN	
SonicPoint VAPs	
CASS 2.0	
Enhanced Connection Limit	
Dynamic WAN Scheduling	
Browser NTLM Auth	
SSO Import from LDAP	
SSL VPN NetExtender Update	
DHCP Scalability Enhancements	
SIP Application Layer Gateway Enhancements	
SonicPoint-N DR	
Accept Multiple Proposals for Clients	
WAN Acceleration Support	
App Control Policy Configuration via App Flow Monitor	
Global BWM Ease of Use Enhancements	

Features Supported on NSA 220 and NSA 250M Series	Features Not Supported on NSA 220 and NSA 250M Series
Application Usage and Risk Report	
Geo-IP Filtering and Botnet Command & Control Filtering	
Customizable Login Page	
LDAP Primary Group Attribute	
Preservation of Anti-Virus Exclusions After Upgrade	
Management Traffic Only Option for Network Interfaces	
Current Users and Detail of Users Options for TSR	
User Monitor Tool	
Auto-Configuration of URLs to Bypass User Authentication	

Known Issues

This section contains a list of known issues in the SonicOS 5.8.1.2 release.

Application Control

Symptom	Condition / Workaround	Issue
App Control advanced signatures are applied to traffic from and to the VPN zone, rather than the WAN zone only.	Occurs when enabling the App Control service on the WAN zone, and then enabling the logging or blocking action for any signature. After traffic is generated from the LAN to the VPN, the App control signatures are applied to VPN traffic.	107296
App rules remain in effect even when disabled globally.	Occurs when the Enable App Rules checkbox is cleared to disable these policies globally, then an app rule is created. When traffic on the WAN interface matches the rule, the configured policy action is applied.	101194
Related traffic configured in an application rule is blocked even though the **Enable App Rules** checkbox is not selected.	Occurs when an application rule is created using Create Rule on the App Flow Monitor page and the Enable App Rules checkbox is not selected, which is the factory default setting. The app rule is created and functions properly, even though the **Enable App Rules** checkbox is disabled.	100120

SONICWALL®

SonicOS 5.8.1.2 Release Notes for the NSA 220/250M Series Appliances
P/N 232-000648-00 Rev A

Bandwidth Management

Symptom	Condition / Workaround	Issue
Traffic is dropped when the ingress or egress values for an interface are modified and traffic is passing through that interface.	Occurs when modifying the ingress or egress interface values while the interface is passing traffic. **Workaround**: Stop traffic on the interface, and then modify the values.	101286
Bandwidth management application rules are sometimes mapped to the wrong global BWM priority queue.	Occurs when creating a bandwidth management rule on the **App Flow Monitor** page and setting the priority to **High**. The **App Flow Monitor** page displays the created rule with a **Medium** priority setting, even though **High** was selected.	100116

Firmware

Symptom	Condition / Workaround	Issue
The Botnet Service is incorrectly listed on the Security Services > Summary page and the System > Status page of the SonicWALL TZ 200 wireless appliance, even though the service is not supported on this platform.	Botnet Command & Control Filtering is not supported on the SonicWALL TZ 100 and TZ 200 series appliances (as also reflected in the Supported Features by Appliance Model table of the Release Notes). The Botnet service listing indicating 'Not Licensed' on the System > Status page should be ignored.	108038
An iPad client fails to connect to the L2TP server if MSCHAPv2 authentication is set as the first order authentication method.	Occurs when GroupVPN is enabled and configured for an L2TP. The iPad can successfully connect if PAP authentication is set as the first order authentication method, but fails if MSCHAPv2 is prefered. A Windows XP client can succesfully connect using MSCHAPv2. **Workaround**: Move MSCHAPv2 to the bottom of the authentication protocol list (by clicking on the Down Arrow button).	106801
The error message "This request is blocked by the sonicwall gateway botnet service. Botnet Responder IP: 125.39.127.25" is displayed.	Occurs when navigating to the **Security Services > Geo-IP & Botnet Filter** page and enabling the "Block connections to/from Botnet Command and Control Systems" option. For example, when trying to view the qq.com web site, the site is blocked even though it is not considered a Botnet server.	105889
The Geo-IP and Botnet Exclusion Objects do not take effect, causing DNS query packets to be incorrectly dropped.	Occurs when enabling the checkbox for **Block All Connections to/from Following Countries**, selecting all countries, and entering DNS Servers into the **Exclusion Object**. When a web page is accessed and the packet monitor is used to capture packets, you can see that all DNS query packets are dropped by the Geo-IP filter.	100010

SONICWALL®

High Availability

Symptom	Condition / Workaround	Issue
With Active/Passive High Availability enabled with probing, and the primary WAN interface configured with a redundant port, the primary WAN interface and all routes to this subnet are marked as down when the primary port stops working.	Occurs when HA is enabled with probing and the primary WAN interface is configured with a redundant port. If the link for the active port goes down, Load Balancing (enabled by default) will change the status of the primary WAN interface to "Failover". All routes to the primary WAN subnet will be marked as down and traffic destined to the subnet will fail. However, traffic will still succeed to any destination that is on the far side of the default gateway of the primary WAN interface, by using the redundant port. **Workaround**: Disable Load Balancing or HA probing.	97883

Module

Symptom	Condition / Workaround	Issue
The LAN Bypass module's Bypass Status LED indicates that bypass mode is active during the boot process, then changes to the normal mode in which bypass is ready, but not active.	Occurs when configuring an SFP module in Layer 2 Bridge Mode, then replacing it with a LAN Bypass module.	108416
The ADSL card cannot connect in DHCP mode.	Occurs when configuring an ADSL card with the WAN in DHCP mode. The Status mode, Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP) do not work with this configuration.	106473

Networking

Symptom	Condition / Workaround	Issue
On the X1 interface, 1Gbps traffic sometimes does not reach the WAN. After configuring the link speed, the link status displays the previously configured speed.	Occurs when passing traffic through the X1 interface with a 1Gbps switch and forcing the X1 interface's link speed to 1000Mbps or 100Mbps. **Workaround**: Configure the SonicOS to auto-negotiate link speed.	105890
Configuring more than one remote appliance with a tunnel interface and OSPF could result in dropped routes.	Occurs when an additional remote appliance is configured with a tunnel interface and OSPF is enabled.	102961

SONICWALL®

System

Symptom	Condition / Workaround	Issue
The MO/M1 status LED does not indicate the presence of a module.	Occurs when inserting a module into the appliance and booting the system. The M0/M1 status LED should be on when a valid module is detected in the slot and blink if a module is present but not supported.	107620
The system preferences do not import correctly. The LAN IP address is changed to 192.168.168.168 and the user cannot log in.	Occurs when importing preferences from a TZ 200 appliance into a NSA 250M appliance, then performing a restarting.	107209

Visualization

Symptom	Condition / Workaround	Issue
The NetFlow EndTime timestamp results in 0.00000 for valid and allowed TCP packets.	Occurs when the NetFlow collector's logging is enabled on Applicable Interfaces and Rules, and TCP traffic is sent to the allowed destination. Upon checking the packet capture details, the EndTime timestamp displays as 0.00000.	102961

VPN

Symptom	Condition / Workaround	Issue
Sometimes, the secondary IPSec gateway is unable to establish a tunnel with a peer if the primary gateway is unreachable.	Occurs when there are two SonicWALL devices with VPN configured and the cable from the secondary gateway is unplugged.	103935
Having multiple tunnel interface policies with the same IPSec gateway but different ports configured on the firewall can cause only one tunnel to be active.	Occurs when there are two or more tunnel interface policies using the same IPSec gateway and those interfaces are bound to different ports.	103398

SONICWALL®

Upgrading SonicOS Image Procedures

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

Obtaining the Latest SonicOS Image Version

To obtain a new SonicOS 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 image file to a directory on your management station.

You can update the SonicOS 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 a SonicOS 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 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 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 image version information is listed on the **System** > **Settings** page.

Importing Preferences to SonicOS 5.8

Preferences importing to the SonicWALL UTM appliances is generally supported from the following SonicWALL appliances running SonicOS:

- NSA Series
- NSA E-Class Series
- TZ 210/200/100/190/180/170 Series
- PRO Series

There are certain exceptions to preferences importing on these appliances running the SonicOS 5.8 release. Preferences cannot be imported in the following cases:

- Settings files containing Portshield interfaces created prior to SonicOS 5.x
- Settings files containing VLAN interfaces are not accepted by the TZ 100/200 Series firewalls
- Settings files from a PRO 5060 with optical fiber interfaces where VLAN interfaces have been created

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 maintenance release available on MySonicWALL.

Importing Preferences from SonicOS Standard to SonicOS 5.8 Enhanced

The SonicOS Standard to Enhanced Settings Converter is designed to convert a source Standard Network Settings file to be compatible with a target SonicOS Enhanced appliance. Due to the more advanced nature of SonicOS Enhanced, its Network Settings file is more complex than the one SonicOS Standard uses. They are not compatible. The Settings Converter creates an entirely new target Enhanced Network Settings file based on the network settings found in the source Standard file. This allows for a rapid upgrade from a Standard deployment to an Enhanced one with no time wasted in re-creating network policies. **Note**: SonicWALL recommends deploying the converted target Network Settings file in a testing environment first and always keeping a backup copy of the original source Network Settings file.

The SonicOS Standard to Enhanced Settings Converter is available at:
https://convert.global.sonicwall.com/

If the preferences conversion fails, email your SonicOS Standard configuration file to settings_converter@sonicwall.com with a short description of the problem. In this case, you may also consider manually configuring your SonicWALL appliance.

To convert a Standard Network Settings file to an Enhanced one:
1. Log in to the management interface of your SonicOS Standard appliance, navigate to **System > Settings**, and save your network settings to a file on your management computer.
2. On the management computer, point your browser to https://convert.global.sonicwall.com/.
3. Click the **Settings Converter** button.
4. Log in using your MySonicWALL credentials and agree to the security statement.
   The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that SonicWALL will retain a copy of their network settings after the conversion process is complete.
5. Upload the source Standard Network Settings file:
   - Click **Browse**.
   - Navigate to and select the source SonicOS Standard Settings file.
   - Click **Upload**.
   - Click the right arrow to proceed.
6. Review the source SonicOS Standard Settings Summary page.
   This page displays useful network settings information contained in the uploaded source Network Settings file. For testing purposes, the LAN IP and subnet mask of the appliance can be changed on this page in order to deploy it in a testing environment.
   - (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.
   - Click the right arrow to proceed.
7. Select the target SonicWALL appliance for the Enhanced deployment from the available list.
   SonicOS Enhanced is configured differently on various SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.
8. Complete the conversion by clicking the right arrow to proceed.
9. Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.
10. Click the **Download** button, select Save to Disk, and click OK to save the new target SonicOS Enhanced Network Settings file to your management computer.
11. Log in to the management interface for your SonicWALL appliance.
12. Navigate to **System > Settings**, and click the **Import Settings** button to import the converted settings to your appliance.

Support Matrix for Importing Preferences

DESTINATION FIREWALLS

SOURCE FIREWALLS	TZ100/ TZ200	TZ100w/ TZ200w	TZ210	TZ210w	TZ170	TZ170w	TZ170SP	TZ170SPw	TZ180	TZ180w	TZ190	TZ190w	PRO 1260	PRO 2040	PRO 3060	PRO 4060	PRO 4100	PRO 5060	NSA 240	NSA 2400	NSA 3500	NSA 4500	NSA 5000	NSA E5500	NSA E6500	NSA E7500	NSA E8500
TZ100/TZ200	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
TZ100W/TZ200W	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
TZ210	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
TZ210W	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
TZ170	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
TZ170W	B,C,D	B,D	B,C,D	B,D	C	✓	✓	✓	C	✓	C	✓	✓	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
TZ170SP	B,C,D	B,C,D	B,C,D	B,D	C	C	✓	✓	C	C	✓	C	C	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
TZ170SPW	C,D	B,C,D	B,C,D	B,D	C	C	C	✓	C	C	C	✓	C	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
TZ180	C,D	C,D	C,D	C,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗	✗
TZ180W	C,D	C,D	C,D	C,D	C	✓	C	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
TZ190	C,D	C,D	C,D	C,D	C	C	✓	✓	C	C	✓	✓	C	✗	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗	✗
TZ190W	C,D	C,D	C,D	C,D	C	✓	C	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
PRO 1260	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗	✗
PRO 2040	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	C	✓	✓	✓	✓	✓	✓	✓	✓
PRO 3060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✓	✓	✓	C	✓	✓	✓	✓	✓	✓	✓	✓
PRO 4060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✓	✓	✓	C	✓	✓	✓	✓	✓	✓	✓	✓
PRO 4100	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	✓	C	C	C	C	C	C	C	C	C	C
PRO 5060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C,E	✓	C,E	C,E	C,E	C,E	C,E	C,E	C,E	C,E	C,E
NSA 240	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
NSA 2400	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✓	✓	✓	✓	✓	✓	✓
NSA 3500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	✓	✓	✓	✓	✓	✓	✓
NSA 4500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	✓	✓	✓	✓	✓	✓	✓
NSA 5000	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	✓	✓	✓	✓	✓
NSA E5500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	C	✓	✓	✓	✓
NSA E6500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	C	✓	✓	✓	✓
NSA E7500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	C	✓	✓	✓	✓
NSA E8500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	C	C	C	C	✓	✓	✓	✓

Notes:

A - When VLANs are present, the settings file will not be accepted

B - Portshield interfaces prior to SonicOS 5.x is not supported.

C - Configuration information from extra interfaces will be removed. NAT policies/Firewall access rules and other interface-dependent configuration will also be removed

D - When importing from non-SonicOS5.x devices, the X2 interface will be configured in the DMZ zone.

E - VLANs created as sub-interfaces of the fiber interfaces will be renamed.

✓	Supported
✗	Unsupported. While importing the settings file may be successful, firewall limitations may result in the removal of items such as DHCP scopes, VPN settings, etc.

Upgrading a SonicOS 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 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 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 Setup Wizard, with a link to the login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware

The SafeMode procedure uses a reset button in a small pinhole, whose location varies: on the NSA models, the button is near the USB ports on the front; on the TZ models, the button is next to the power cord on the back. 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.
   - 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 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 Website.

_____

Last updated: 11/14/2011

Free Manuals Download Website

http://myh66.com

http://usermanuals.us

http://www.somanuals.com

http://www.4manuals.cc

http://www.manual-lib.com

http://www.404manual.com

http://www.luxmanual.com

http://aubethermostatmanual.com

Golf course search by state

http://golfingnear.com

Email search by domain

http://emailbydomain.com

Auto manuals search

http://auto.somanuals.com

TV manuals search

http://tv.somanuals.com