Release Notes

SonicOS

SonicOS 5.8.1.2 Release Notes

Contents

SonicWALL Analysis of PenTest Vulnerability Reports

Three vulnerabilities (**SonicOS Management SessionID Brute Force Vulnerability**, **Preview of Custom Web Page Vulnerability**, and **MAC Address Spoofing on Wireless Networks**) for SonicOS were reported by PenTest, a penetration testing firm in Spain. SonicWALL has analyzed the reported vulnerabilities and our findings and recommendations are below.

Analysis: SonicOS Management SessionID Brute Force Vulnerability

For Web GUI management, SonicOS creates a unique management SessionID, using a cryptographically random number, which is associated with a legitimate Administrator login (requiring the appropriate username/password authentication) and which is further associated with the specific “management source IP address” used during the initiation and authentication of the Administrator. For all subsequent HTTPS/HTTP management transactions associated with the management session, SonicOS validates both the management SessionID and the specific “management source IP address” used to establish the management session. A management SessionID cannot be utilized with another source IP address, nor can another source IP address be used with the management SessionID.

As SonicOS validates both the management SessionID and the management Source IP address used to establish the management session, any attempt at a brute force attack on the management SessionID can only be originated from the Source IP used by an active session of a legitimate Administrator.

Further, a brute force attack on the management SessionID would need to go undetected from the management source IP while the legitimate management session remains open, and does not logout, from the same source IP address. Further, the legitimate administrator will be notified in the logs, syslogs, and alerts, of each brute force attempt.

The validation by SonicOS, described above, significantly reduces the scope and probability of any successful brute force attack on the management SessionID.

In addition to existing validation measures described above, as further protection against a brute force attack from the source IP of the legitimate administrator (as described above), the SonicOS firmware has been enhanced with a SessionID that is based on a cryptographically random number which is 4 times larger, and which increases the time required for a theoretical attack to 2,697,570,767,701,495,615,277,217,349,632 years, and all SonicOS firmware versions are available with this additional protection.

In addition, please review the section below entitled “**Recommended Best Practice – Limiting SonicOS management access to “Trusted Management Sources”.**

Analysis: Preview of Custom Web Page Vulnerability

The Preview of Customer Web Page vulnerability requires a legitimate administrator to customize some web pages directly from the administrative interface where he/she can put the code and test it via a preview feature. This preview feature will show the page and execute all the JavaScript code inside it in the web admin security context. Incorrect coding by the legitimate administrator can leads to traditional attacks like XSS, session hijacking, etc. This vulnerability requires the authenticated administrator to post malicious JavaScript code into the firewall.

SonicOS firmware is available with additional protections against administrators introducing vulnerabilities into a custom a web page with potentially malicious JavaScript.

SonicWALL strongly recommends reviewing any custom web page, including not posting unverified JavaScript code into the custom web page design fields.

Analysis: MAC Address Spoofing on Wireless Networks

PenTest reported a vulnerability described as "MAC spoofing protection option that can be activated in wireless networks per ESSID basis." SonicWALL is aggressively testing and attempting to confirm this vulnerability. Thus far, the result has not been reproduced by the SonicWALL security verification team. SonicWALL is working with PenTest to determine appropriate status of this report.

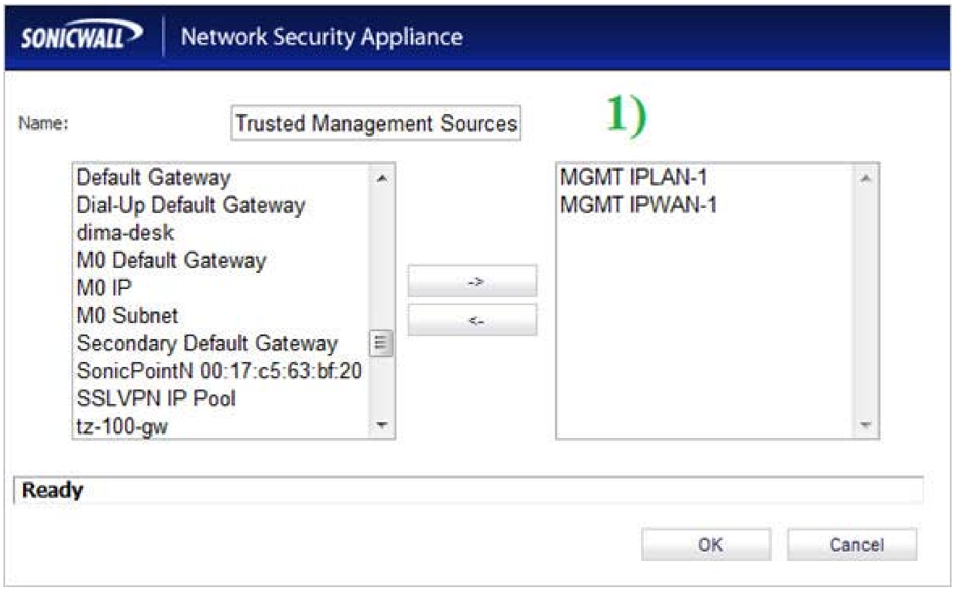
SonicOS Updates

SonicWALL has posed updated firmware to its www.mysonicwall.com firmware download site today and this update is available for free to all users of SonicWALL firewalls regardless of support contract status. All customers are encouraged to review the recommendations above, include best practices, and download the updated SonicOS firmware from www.mysonicwall.com as needed and at your convenience.

Recommended Best Practice – Limiting SonicOS management access to “Trusted Management Sources”

To enhance the security of administrative sessions, SonicWALL advises administrators to adhere to the best practice of limiting SonicOS management access to “Trusted Management Sources” by modifying the existing SonicOS Web Management rules (HTTPS/HTTP Managment) to allow management access only from trusted IP Addresses. Administrators with firewalls under GMS management should push these rule updates to the firewalls through the GMS interface.

- Add a "Trusted Management Sources" address object group containing trusted management IP addresses



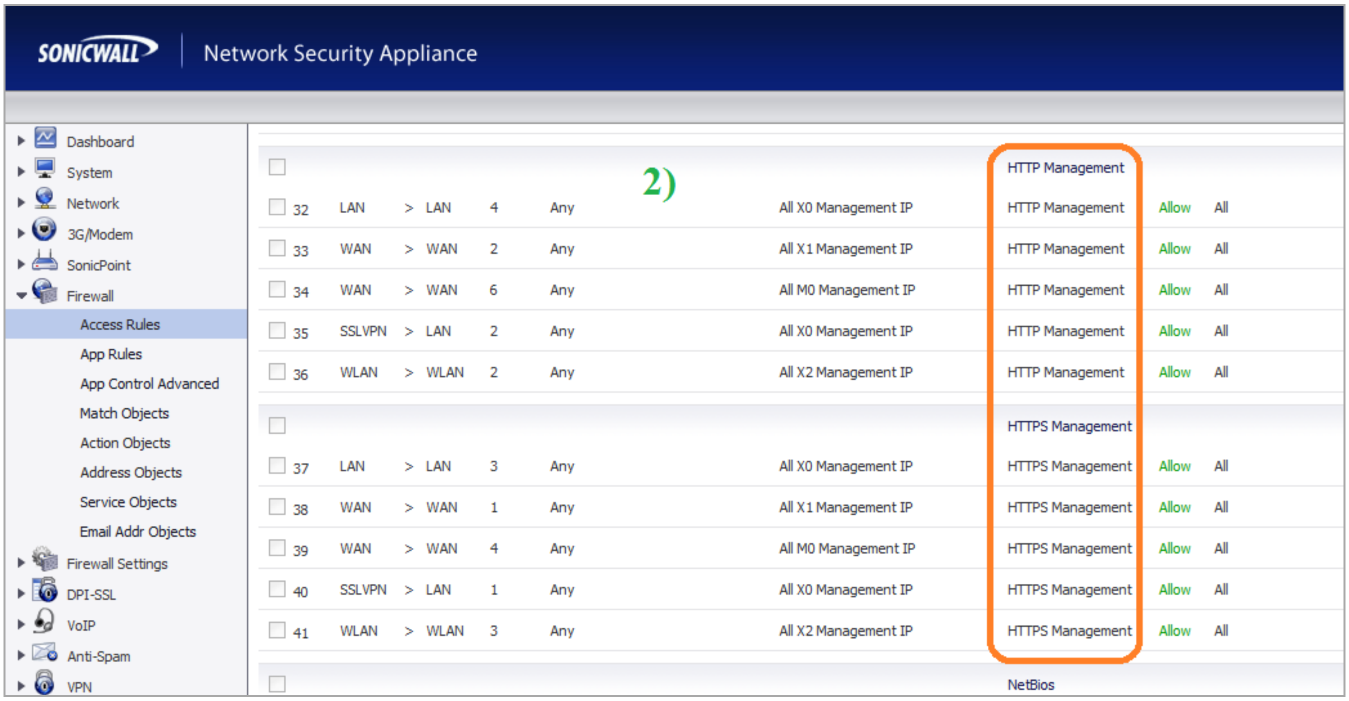
Name: Trusted Management Sources

Default Gateway
Dial-Up Default Gateway
dima-desk
M0 Default Gateway
M0 IP
M0 Subnet
Secondary Default Gateway
SonicPointN 00:17:c5:63:bf:20
SSLVPN IP Pool
tz-100-gw

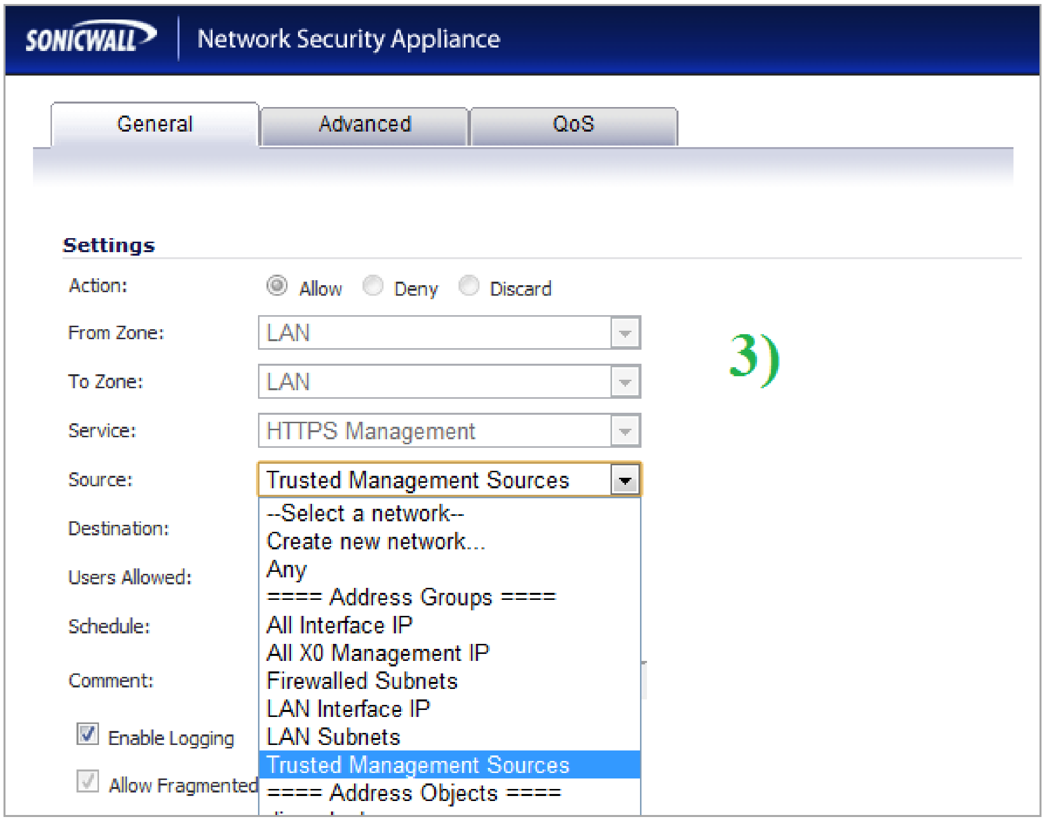
MGMT IPLAN-1
MGMT IPWAN-1

Ready

- In the access rules screen, modify the existing management HTTP/HTTPs rules for each zone by adding the "Trusted Management Sources" address object for the appropriate zone to the "Source" field, to block access from non-trusted sources.



□								HTTP Management		
□	32	LAN	>	LAN	4	Any	All X0 Management IP	HTTP Management	Allow	All
□	33	WAN	>	WAN	2	Any	All X1 Management IP	HTTP Management	Allow	All
□	34	WAN	>	WAN	6	Any	All M0 Management IP	HTTP Management	Allow	All
□	35	SSLVPN	>	LAN	2	Any	All X0 Management IP	HTTP Management	Allow	All
□	36	WLAN	>	WLAN	2	Any	All X2 Management IP	HTTP Management	Allow	All
□								HTTPS Management		
□	37	LAN	>	LAN	3	Any	All X0 Management IP	HTTPS Management	Allow	All
□	38	WAN	>	WAN	1	Any	All X1 Management IP	HTTPS Management	Allow	All
□	39	WAN	>	WAN	4	Any	All M0 Management IP	HTTPS Management	Allow	All
□	40	SSLVPN	>	LAN	1	Any	All X0 Management IP	HTTPS Management	Allow	All
□	41	WLAN	>	WLAN	3	Any	All X2 Management IP	HTTPS Management	Allow	All
□								NetBios		



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: LAN

To Zone: LAN

Service: HTTPS Management

Source: Trusted Management Sources

Destination:

Users Allowed:

Schedule:

Comment:

☑ Enable Logging

☑ Allow Fragmented

Platform Compatibility

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

- SonicWALL NSA E8500
- SonicWALL NSA E7500
- SonicWALL NSA E6500
- SonicWALL NSA E5500
- SonicWALL NSA 5000
- SonicWALL NSA 4500
- SonicWALL NSA 3500
- SonicWALL NSA 2400
- SonicWALL NSA 240
- SonicWALL TZ 210 / 210 Wireless
- SonicWALL TZ 200 / 200 Wireless
- SonicWALL TZ 100 / 100 Wireless

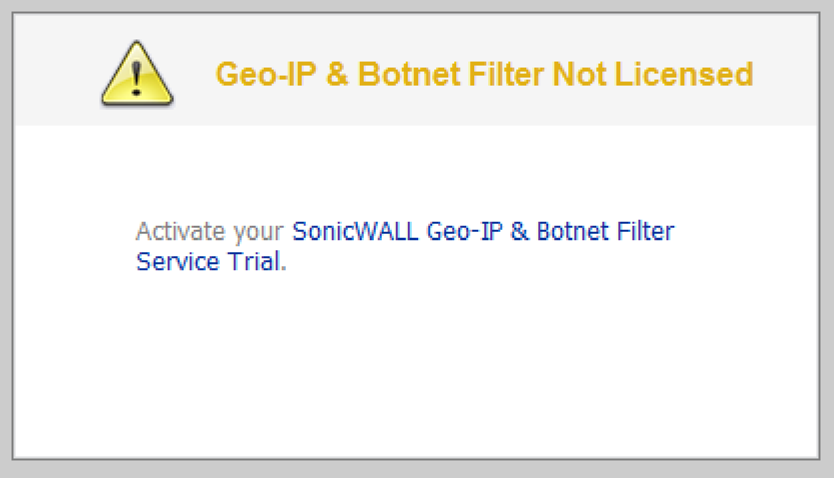
The SonicWALL WAN Acceleration Appliance Series (WXA 500 Live CD/WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are also supported for use with NSA E-Class, NSA, and TZ products running 5.8.1.2. The minimum recommended Firmware version for WXA Series is 1.0.12.

Geo-IP and Botnet Filter are Now Licensed Services

In SonicOS 5.8.1.1, the Geo-IP and Botnet Filter features are now licensed services, although these features are currently available on a free trial license basis. You simply need to click on the link to activate the trial license with your mysonicwall.com account.

Note: App Visualization must also be both licensed and enabled to enable Geo-IP and Botnet Filter.

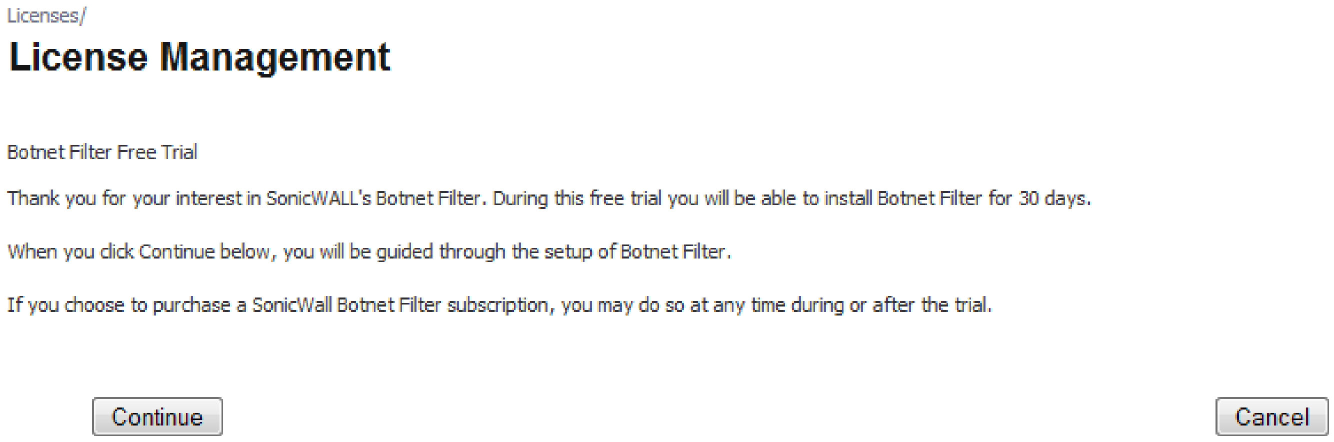
When you initially navigate to the **Security Services > Geo-IP & Botnet Filter** page, you will be prompted to click a link to activate the free trial license, as shown below.



Geo-IP & Botnet Filter Not Licensed

Activate your SonicWALL Geo-IP & Botnet Filter Service Trial.

Clicking the link will redirect to the **Licenses > License Management** page. Click **Continue** to activate the trial license.



Licenses/

License Management

Botnet Filter Free Trial

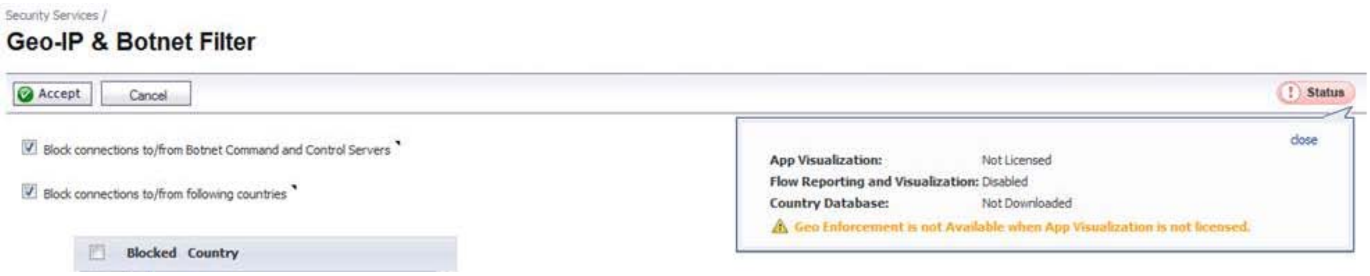
Thank you for your interest in SonicWALL's Botnet Filter. During this free trial you will be able to install Botnet Filter for 30 days.

When you click Continue below, you will be guided through the setup of Botnet Filter.

If you choose to purchase a SonicWall Botnet Filter subscription, you may do so at any time during or after the trial.

The **Security Services > Geo-IP & Botnet Filter** page will now be available.

Note: If Application Visualization is not licensed and enabled, the Status icon at the top left of the page will appear red with an exclamation point.



Geo-IP & Botnet Filter

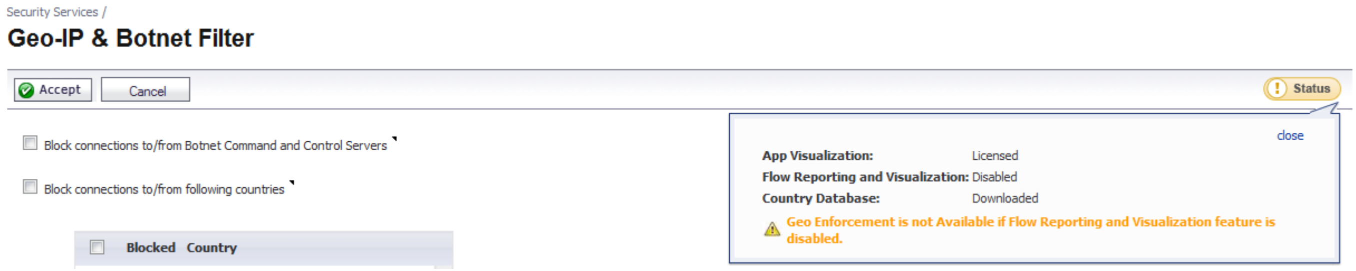
☑ Block connections to/from Botnet Command and Control Servers

☑ Block connections to/from following countries

□ Blocked	Country

App Visualization: Not Licensed
Flow Reporting and Visualization: Disabled
Country Database: Not Downloaded
⚠ Geo Enforcement is not Available when App Visualization is not licensed.

To use the Geo-IP and Botnet Filter features, first active the Application CGSS license bundle, which is part of the CGSS license bundle. If Application Visualization is licensed but not enabled, the Status icon appears orange.



Geo-IP & Botnet Filter

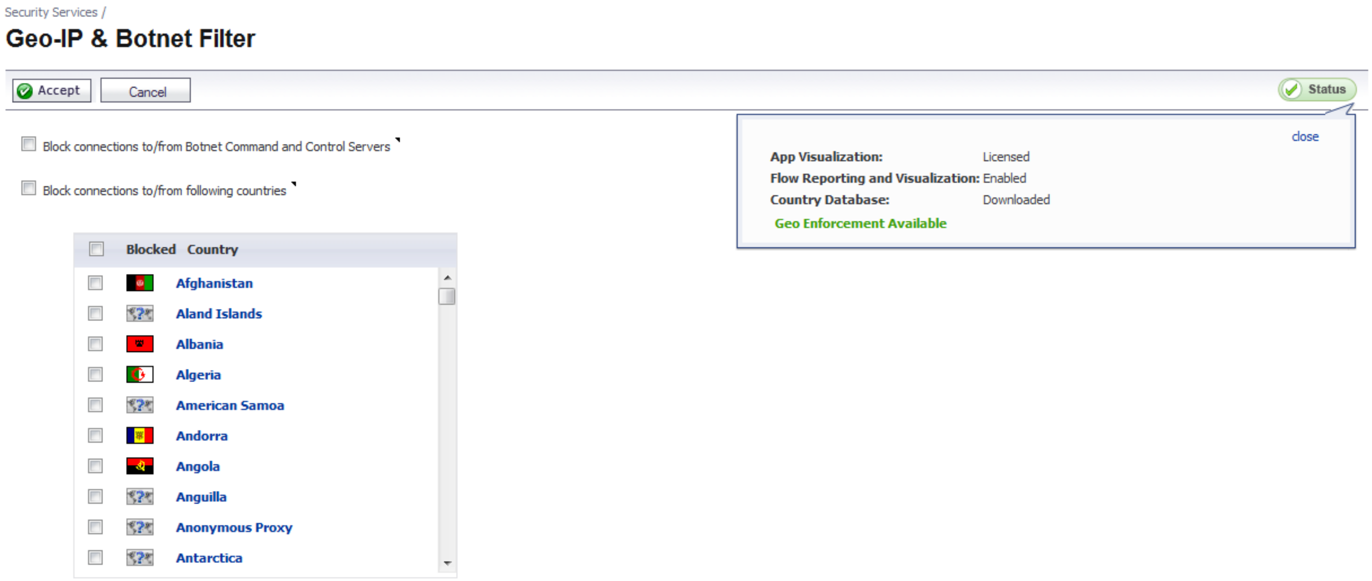
□ Block connections to/from Botnet Command and Control Servers

□ Block connections to/from following countries

□ Blocked	Country

App Visualization: Licensed
Flow Reporting and Visualization: Disabled
Country Database: Downloaded
⚠ Geo Enforcement is not Available if Flow Reporting and Visualization feature is disabled.

After Application Visualization is licensed, go to the **Log > Flow Reporting** page and enable Flow Reporting and Visualization. You must then restart the appliance. The appliance will then download the country database (which may take up to five minutes). Geo-IP and Botnet Filter will then be ready to use.



Geo-IP & Botnet Filter

□ Block connections to/from Botnet Command and Control Servers

□ Block connections to/from following countries

□ Blocked	Country
□	Afghanistan
□	Aland Islands
□	Albania
□	Algeria
□	American Samoa
□	Andorra
□	Angola
□	Anguilla
□	Anonymous Proxy
□	Antarctica

App Visualization: Licensed
Flow Reporting and Visualization: Enabled
Country Database: Downloaded
Geo Enforcement Available

Supported Features by Appliance Model

The following table lists the key features in the SonicOS 5.8.0.x, 5.8.1.0, and 5.8.1.2 releases, and shows which appliance models support them.

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
Wireless Client Bridge Support			Supported	Supported	Supported
App Flow Monitor	Supported	Supported	Supported		
Real-Time Monitor	Supported	Supported	Supported		
Packet Monitor Enhancements	Supported	Supported	Supported	Supported	Supported
Log > Flow Reporting Enhancements	Supported	Supported	Supported		
App Control Advanced	Supported	Supported	Supported	Supported	Supported
App Rules	Supported	Supported	Supported		
DPI-SSL	Supported	Supported			
Cloud GAV	Supported	Supported	Supported	Supported	Supported
NTP Auth Type	Supported	Supported	Supported	Supported	Supported
Link Aggregation	Supported				
Port Redundancy	Supported				
CFS Enhancements	Supported	Supported	Supported	Supported	Supported
IPFIX & NetFlow Reporting	Supported	Supported	Supported		
VLAN Enhancements (TZ Support)	Supported	Supported	Supported	Supported	Supported
SonicPoint VAPs	Supported	Supported	Supported	Supported	Supported
CAS 2.0	Supported	Supported	Supported	Supported	Supported
Enhanced Connection Limit	Supported	Supported	Supported	Supported	Supported
Dynamic WAN Scheduling	Supported	Supported	Supported	Supported	Supported
Browser NTLM Auth	Supported	Supported	Supported	Supported	Supported
User Import from LDAP	Supported	Supported	Supported	Supported	Supported
SSL VPN NetExtender Client Update	Supported	Supported	Supported	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported	Supported	Supported	Supported
SIP Application Layer Enhancements	Supported	Supported	Supported	Supported	Supported
SonicPoint-N DR	Supported	Supported	Supported	Supported	Supported

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
Accept Multiple VPN Client Proposals.	Supported	Supported	Supported	Supported	Supported
WAN Acceleration Support	Supported	Supported	Supported	Supported	Supported
App Control Policy Configuration via App Flow Monitor	Supported	Supported	Supported	Supported	Supported
Global BWM Ease of Use Enhancements	Supported	Supported	Supported	Supported	Supported
Application Usage and Risk Report	Supported	Supported	Supported		
Geo-IP Filtering and Botnet Command & Control Filtering	Supported	Supported	Supported		
Wire and Tap Mode	Supported	3500 and above			
Customizable Login Page	Supported	Supported	Supported	Supported	Supported
Preservation of Anti-Virus Exclusions After Upgrade	Supported	Supported	Supported	Supported	Supported
Management Traffic Only Option for Network Interfaces	Supported	Supported	Supported	Supported	Supported
Current Users and Detail of Users Options for TSR	Supported	Supported	Supported	Supported	Supported
User Monitor Tool	Supported	Supported	Supported		
Auto-Configuration of URLs to Bypass User Authentication	Supported	Supported	Supported	Supported	Supported

Browser Support

SonicOS 5.8 with Visualization uses advanced browser technologies such as HTML5 which are only supported in the latest browsers. SonicWALL therefore recommends using Google Chrome or Mozilla Firefox browsers for administration of SonicOS 5.8.

This release supports the following Web browsers:

- Chrome 4.0 and higher (recommended browser for dashboard video streaming)
- Mozilla 3.0 and higher
- Internet Explorer 8.0 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 3.0, Microsoft Internet Explorer 8.0, and Google Chrome 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.

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. **Workaround**: Uncheck Enable App Rules and the reboot the appliance.	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. **Workaround**: Uncheck Enable App Rules and the reboot the appliance.	100120

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

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

Networking

Symptom	Condition / Workaround	Issue
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

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

Resolved Issues

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

Symptom	Condition / Workaround	Issue
SonicOS management SessionID brute force vulnerability. If brute force succeeds, the following alert notifies the administrator: “Login from another browser session”.	Occurs when an undetected brute force attack is launched from the same Source workstation against an active management session. The management session would also need to remain open throughout the duration of the attack.	108138

This section contains a list of resolved issues in the SonicOS 5.8.1.1 release.

Firmware

Symptom	Condition / Workaround	Issue
After LDAP has been successfully configured, the LDAP test page begins to authenticate all users, regardless if their passwords are correct. This issue is encountered intermittently.	Occurs after LDAP is successfully configured, and subsequent changes are then made to the LDAP configuration--such as changing the Schema or enabling TLS.	107745
Open Directory LDAP authentication fails after upgrading to SonicOS 5.8.1.0 or 5.8.1.1.	Occurs when Open Directory LDAP authentication has been successfully configured, and the firmware on the appliance is upgraded from 5.8.0.3 to either 5.8.1.0 or 5.8.1.1	107744
Users cannot login on the SSL VPN portal if the user is a member of an LDAP group. An error message displays "Login failed - User login denied - LDAP communication or configuration error."	Occurs for users that are member of an LDAP group that uses openLDAP. Testing the username on the LDAP configuration page succeeds and returns the correct group membership.	107301

Symptom	Condition / Workaround	Issue
Uploading a large PKCS #12 file causes memory error.	Occurs when uploading a PKCS #12 file containing a certificate, a private key, and optional CA certificates. The PKCS #12 file processes successfully, but memory errors still occur, even after rebooting the system.	106687
Open Shortest Path First (OSPF) does not display connected networks to its OSPF peers after a firmware upgrade.	Occurs when loading customer preferences and attempting an upgrade test from SonicOS 5.8.0.2 to 5.8.1.1.	105987
The Deep Packet Inspection of Secure Socket Layer (DPI-SSL) and Application Firewall services are blocked with SonicOS 5.8.1.0-30o firmware.	Occurs after enabling DPI-SSL, Server SSL, and Application Firewall on the appliance running SonicOS 5.8.1.0-30o.	105444
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

High Availability

Symptom	Condition / Workaround	Issue
When the Active/Active DPI configuration is enabled, the connection cache fails to connect to the backup unit.	Occurs when the active/active configuration is enabled. When the primary unit begins to receive a heavy load of connections, it is unable to connect to the backup unit until active/active is disabled.	102489

Modem

Symptom	Condition / Workaround	Issue
For Verizon customers, 3G does not work with a Novatel U760 modem.	Occurs when using a Novatel U760 modem with a 3G wireless network. Verizon no longer supports the Novatel U760. **Workaround**: Use the UMW190 modem for 3G support.	105457

Networking

Symptom	Condition / Workaround	Issue
The Point-to-Point Protocol over Ethernet (PPPoE) replies with a 50 byte length AC cookie when a 72 byte AC cookie is required, causing difficulty when connecting to the Internet.	Occurs when attempting to connect to the Internet. The PPPoE server resets the connection when there is an AC cookie length mismatch.	105971
When the WAN is down, the routes appear greyed out in the Route list. However, the Routing Information Protocol (RIP) still displays these disabled routes.	Occurs when the WAN is down. Because these routes are still displaying as active, traffic is forwarded to one of the disabled routes. **Workaround:** Manually add static routes to redirect traffic when the WAN is down.	103974
The checkbox for “Fragment non-VPN outbound packets larger than this Interface's MTU” is disabled by default.	Occurs when assigning an unused interface to the WAN zone. In the Advanced tab, the checkbox for “Fragment non-VPN outbound packets larger than this Interface's MTU” should be enabled by default.	102795
The Point-to-Point Protocol over Ethernet (PPPoE) does not parse incoming Open Shortest Path First (OSPF) messages.	Occurs when creating a route based Virtual Private Network (VPN) between a PPPoE WAN and a fixed WAN or DHCP WAN.	102625

SSL-VPN

Symptom	Condition / Workaround	Issue
A second user behind the same public IP address can access the SSL portal without authentication.	Occurs when the login uniqueness is disabled, allowing two users to use the same login name. The first user is logged in, and a second user can login using the same login name without authentication. **Workaround:** Enable login uniqueness.	98028

System

Symptom	Condition / Workaround	Issue
The Global VPN Client (GVC) begins establishing new Phase 2 tunnels without completely removing the old ones.	Occurs when using the GVC to connect. The TSR report shows a large number of expired IPSec Security Associations (SA) for the WAN Group IKE SA.	105204

Users

Symptom	Condition / Workaround	Issue
User is unable to login to the SSL VPN portal if a member of an LDAP group.	Occurs when attempting to login to the SSL VPN portal. An error message displays: “Login failed – User login denied – LDAP communication or configuration error.”	107301
The firewall management interface is not accessible.	Occurs when the DNS server is not reachable and you configure the single sign on agent with a local domain name.	103934
When using RADIUS for user authentication, the administrator is given the option to test the configuration using one of four methods, including PAP and MSCHAP. If the RADIUS server is set to accept only MSCHAP / MSCHAPv2 requests, attempts to login to the SonicWALL appliance or the SonicWALL SSL Portal are rejected. The server then automatically attempts to authenticate using PAP.	Occurs when attempting to login to the SonicWALL appliance or the SonicWALL SSL Portal using MSCHAP / MSCHAPv2. **Workaround:** Select PAP only to login to the SonicWALL appliance or SSL Portal, or Create local user accounts on the appliance, using the Local L2TP IP pool.	83508

Wireless

Symptom	Condition / Workaround	Issue
In the management interface, the SonicPointN status displays “unknown”.	Occurs when configuring a SonicPointN appliance with your firewall, then checking the status. Initially the status displays “operational”, but once the firewall is restarted the status displays “unknown”.	101181
The SonicPointN appliance is operating on a different channel than the channel displayed in the management interface.	Occurs when manually configuring a channel on the SonicPointN appliance.	97238

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:

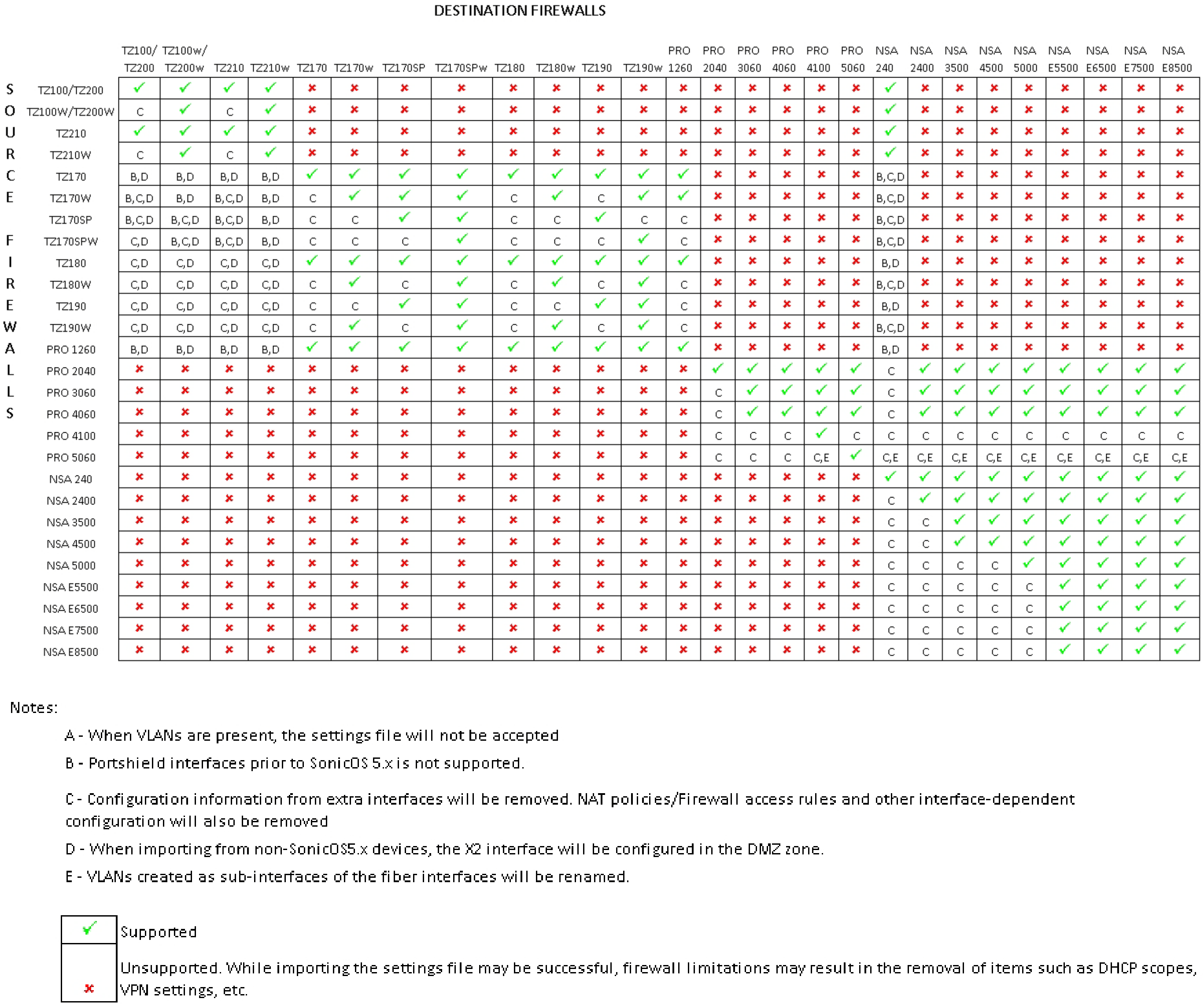
1. Log in to the management interface of your SonicOS Standard appliance, navigate to **System > Settings**, and save your network settings to a file on your management computer.
2. On the management computer, point your browser to https://convert.global.sonicwall.com/.
3. Click the **Settings Converter** 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

		TZ100/	TZ100w/											PRO	PRO	PRO	PRO	PRO	PRO	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA	NSA
		TZ200	TZ200w	TZ210	TZ210w	TZ170	TZ170w	TZ170SP	TZ170SPw	TZ180	TZ180w	TZ190	TZ190w	1260	2040	3060	4060	4100	5060	240	2400	3500	4500	5000	E5500	E6500	E7500	E8500
S	TZ100/TZ200	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
O	TZ100W/TZ200W	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
U	TZ210	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
R	TZ210W	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗
C	TZ170	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
E	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	✗	✗	✗	✗	✗	✗	✗	✗
F	TZ170SPW	C,D	B,C,D	B,C,D	B,D	C	C	C	✓	C	C	C	✓	C	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
I	TZ180	C,D	C,D	C,D	C,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗	✗
R	TZ180W	C,D	C,D	C,D	C,D	C	✓	C	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
E	TZ190	C,D	C,D	C,D	C,D	C	C	✓	✓	C	C	✓	✓	C	✗	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗	✗
W	TZ190W	C,D	C,D	C,D	C,D	C	✓	C	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗
A	PRO 1260	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗	✗
L	PRO 2040	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	C	✓	✓	✓	✓	✓	✓	✓	✓
L	PRO 3060	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✓	✓	✓	C	✓	✓	✓	✓	✓	✓	✓	✓
S	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.

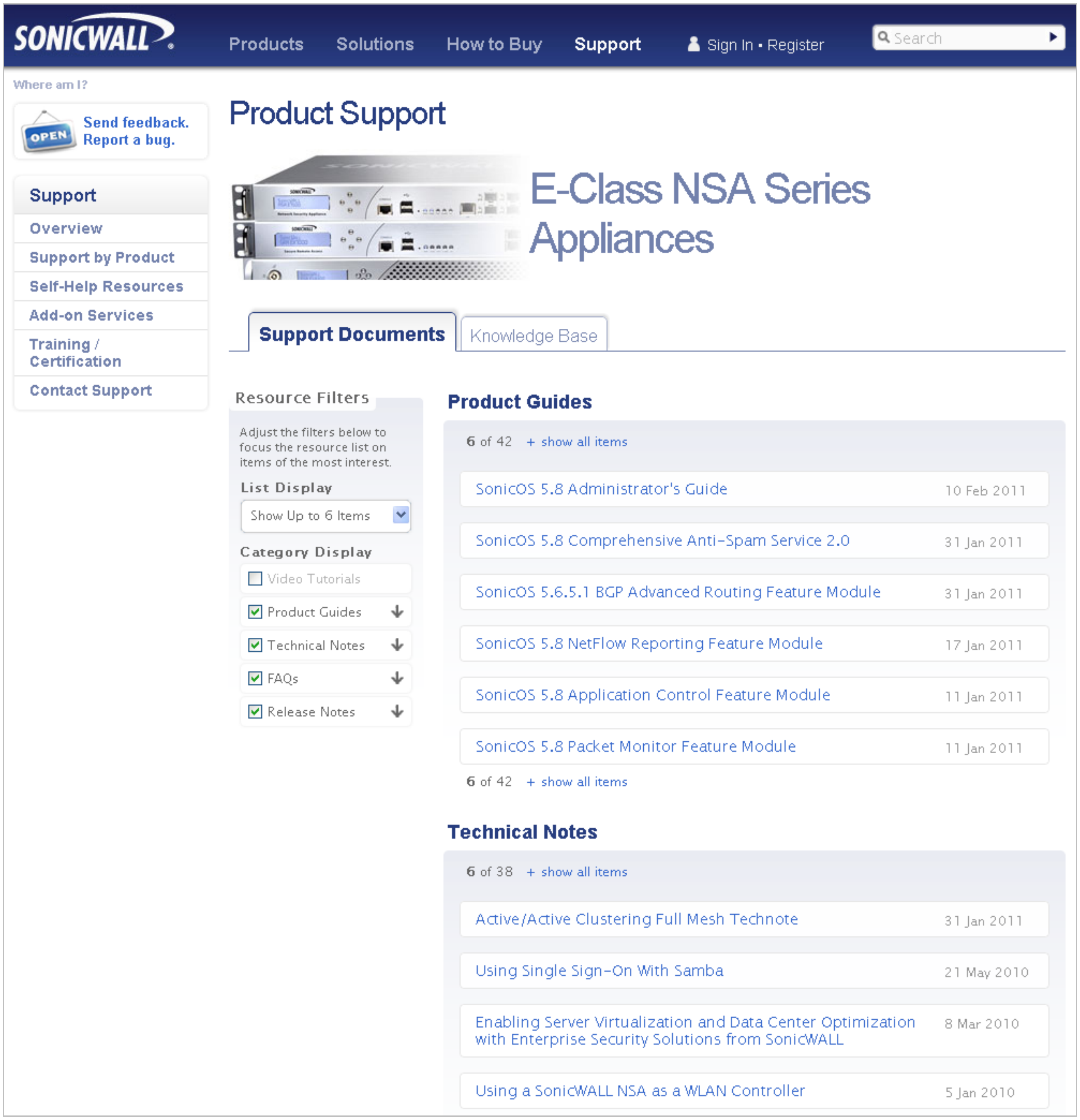
   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

   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.



Product Support

E-Class NSA Series Appliances

Resource Filters

Adjust the filters below to focus the resource list on items of the most interest.

List Display

Show Up to 6 Items

Category Display

☐ Video Tutorials
☑ Product Guides
☑ Technical Notes
☑ FAQs
☑ Release Notes

Product Guides

6 of 42 + show all items

SonicOS 5.8 Administrator's Guide	10 Feb 2011
SonicOS 5.8 Comprehensive Anti-Spam Service 2.0	31 Jan 2011
SonicOS 5.6.5.1 BGP Advanced Routing Feature Module	31 Jan 2011
SonicOS 5.8 NetFlow Reporting Feature Module	17 Jan 2011
SonicOS 5.8 Application Control Feature Module	11 Jan 2011
SonicOS 5.8 Packet Monitor Feature Module	11 Jan 2011

6 of 42 + show all items

Technical Notes

6 of 38 + show all items

Active/Active Clustering Full Mesh Technote	31 Jan 2011
Using Single Sign-On With Samba	21 May 2010
Enabling Server Virtualization and Data Center Optimization with Enterprise Security Solutions from SonicWALL	8 Mar 2010
Using a SonicWALL NSA as a WLAN Controller	5 Jan 2010

Last updated: 10/10/2011