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.

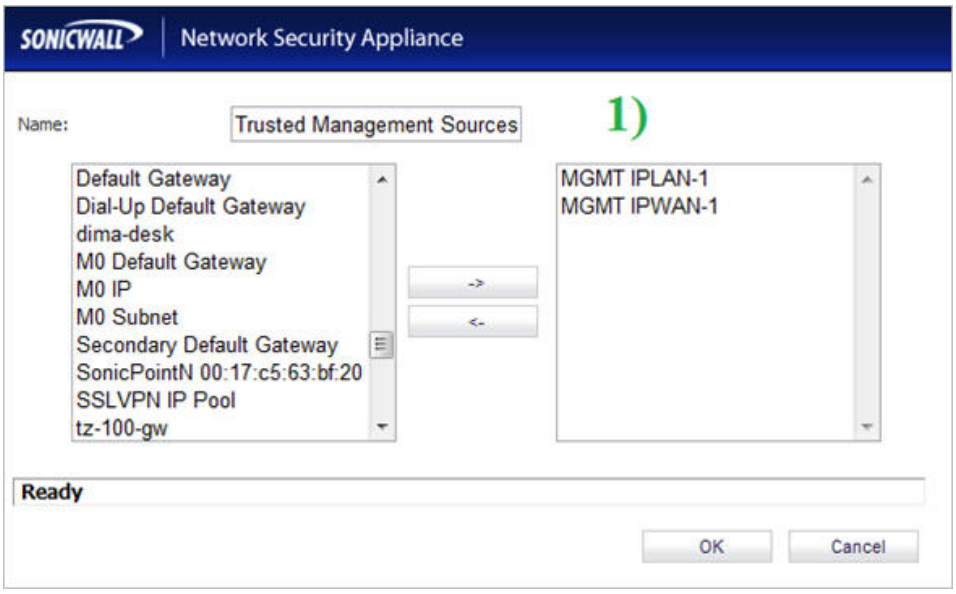
SonicOS Updates

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.

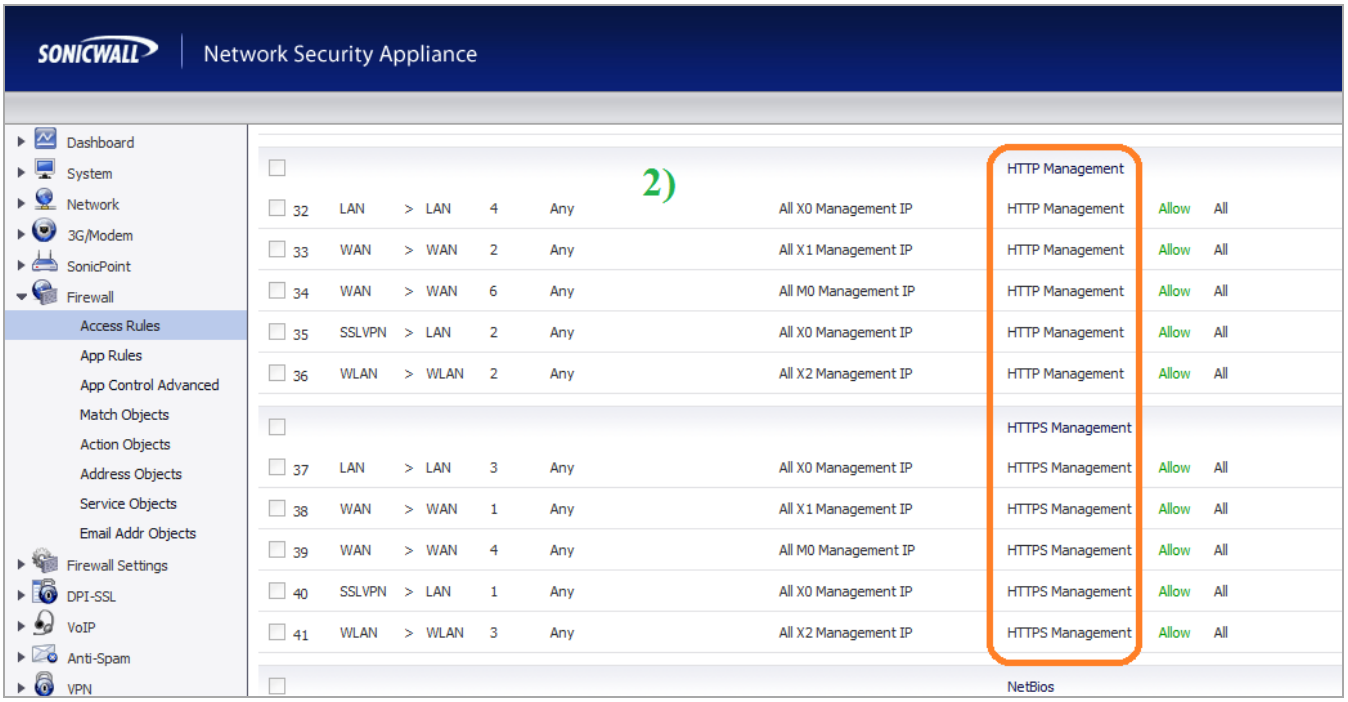
Recommended Best Practice – Limiting SonicOS management access to "Trusted Management Sources"

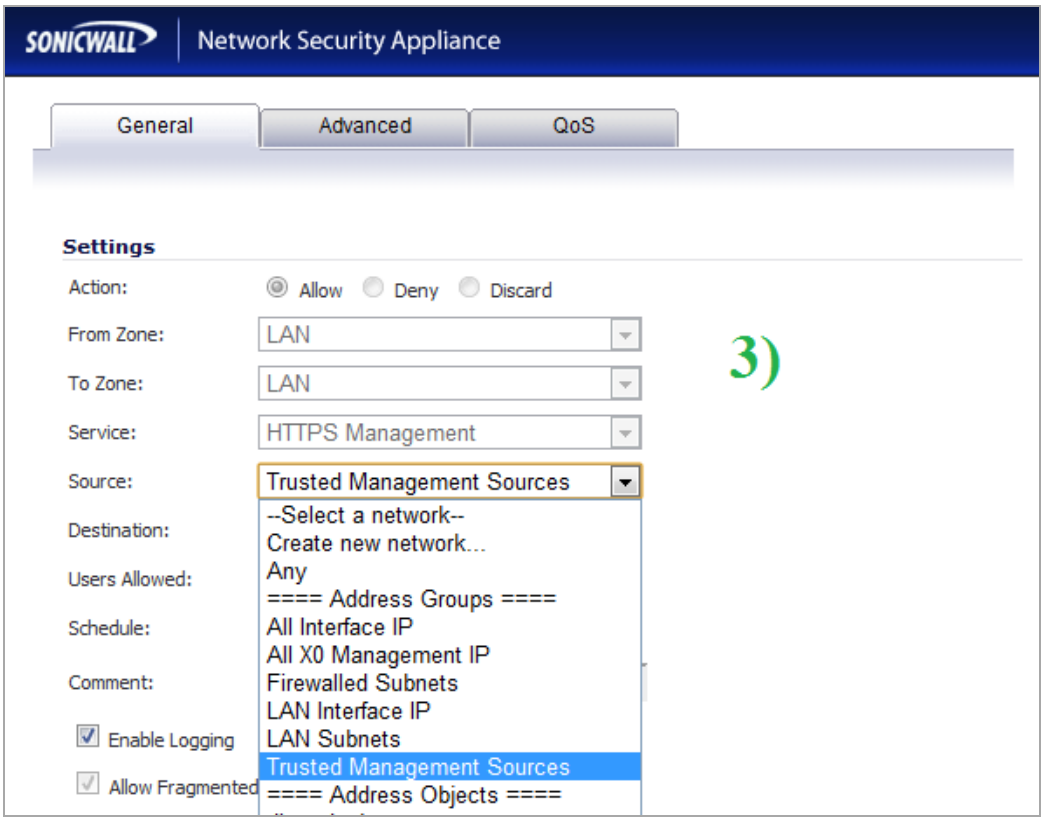
To enhance the security of administrative sessions, SonicWALL advises administrators to adhere to the best practice of limiting SonicOS management access to "Trusted Management Sources" by modifying the existing SonicOS Web Management rules (HTTPS/HTTP Management) to allow management access only from 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



- 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.





Platform Compatibility

The SonicOS 5.8.0.8 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

New Features in SonicOS 5.8.0.8

SonicPoint-N Dual Radio Support

The SonicWALL **SonicPoint-N Dual Radio** appliance (SonicPoint-N DR) is supported by all SonicWALL NSA and TZ platforms when running SonicOS 5.8.0.8.

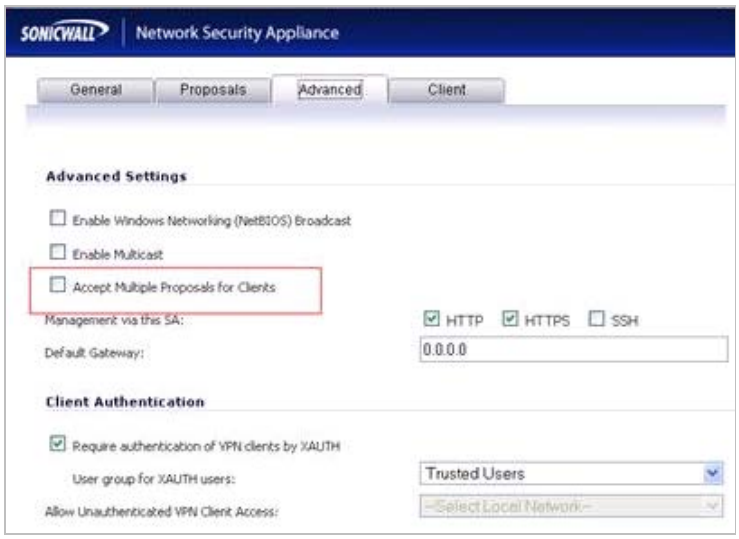
With support for two wireless radios at the same time, you can use **SonicPoint-N DR Clean Wireless** access points to create an enterprise-class secure wireless network. The SonicPoint-N DR uses six antennas to communicate with wireless clients on two frequency ranges: 2.4 GHz and 5 GHz. You can install and configure a SonicPoint-N DR access point in about an hour.

For more information, see the *SonicWALL SonicPoint-N DR Getting Started Guide*, at:
http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=PG&id=444

Accept Multiple Proposals for Clients Option

The new **Accept Multiple Proposals for Clients** checkbox allows multiple VPN or L2TP clients using different security policies to connect to a firewall running SonicOS 5.8.0.8.

The option is on the **Advanced** tab when configuring a GroupVPN policy from the **VPN > Settings** page in SonicOS.



The client policy is still strictly checked against the configured proposal in the Proposals tab, as with clients connecting with SonicWALL GVC. This option has no effect on GVC.

If the **Accept Multiple Proposals for Clients** option is selected, SonicOS will allow connections from other L2TP clients, such as Apple OS, Windows, or Android clients whose offered proposal is different from what is configured on the Proposals tab. The proposal is accepted if it meets the following conditions:

- If the offered algorithm matches one of the possible algorithms available in SonicOS.
- If the offered algorithm is stronger and more secure than the configured algorithm in the SonicOS proposal.

If this option is not selected, SonicOS will require the client to strictly match the configured policy.

This option allows SonicWALL to support heterogeneous environments for Apple, Windows, and Android clients. Using this option, SonicOS can work with these clients if their proposal includes a combination of algorithms which are supported in SonicOS, but are not configured in the policy to prevent other clients like GVC from failing.

Supported Features by Appliance Model

The following table lists the key features in SonicOS 5.8 and shows which appliance models support them.

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
App Flow Monitor	Supported	Supported	Supported		
Real-Time Monitor	Supported	Supported	Supported		
Top Global Malware	Supported	Supported	Supported	Supported	Supported
Log Monitor	Supported	Supported	Supported	Supported	Supported
Connection Monitor	Supported	Supported	Supported	Supported	Supported
Packet Monitor	Supported	Supported	Supported	Supported	Supported
Log > Flow Reporting	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	Supported	Supported	Supported	Supported	Supported
SonicPoint VAPs	Supported	Supported	Supported	Supported	Supported
CASS 2.0	Supported	Supported	Supported	Supported	Supported
Enhanced Connection Limiting	Supported	Supported	Supported	Supported	Supported
Dynamic WAN Scheduling	Supported	Supported	Supported	Supported	Supported
Browser NTLM Auth	Supported	Supported	Supported	Supported	Supported
SSO Import from LDAP	Supported	Supported	Supported	Supported	Supported
SSL VPN NetExtender Update	Supported	Supported	Supported	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported	Supported	Supported	Supported
SIP Application Layer Gateway Enhancements	Supported	Supported	Supported	Supported	Supported
SonicPoint-N DR	Supported	Supported	Supported	Supported	Supported
Accept Multiple Proposals for Clients	Supported	Supported	Supported	Supported	Supported

Key Features in SonicOS 5.8

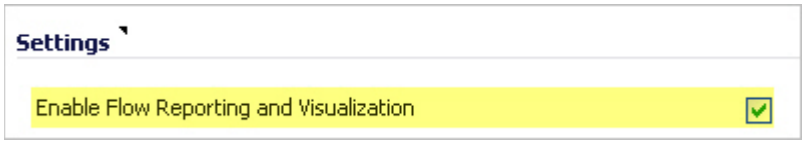
The following are the key features introduced in SonicOS 5.8:

- **Real-Time Visualization Dashboard**—With the new visualization dashboard monitoring improvements, administrators are able to respond more quickly to network security vulnerabilities and network bandwidth issues. Administrators can see what websites their employees are accessing, what applications and services are being used in their networks and to what extent, in order to police content transmitted in and out of their organizations.

New appliances running SonicOS 5.8 receive an automatic 30-day free trial for App Visualization upon registration.

SonicWALL appliances upgrading to SonicOS 5.8 ***and*** already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) automatically receive a complimentary App Visualization license for the Real-Time Visualization Dashboard.

Navigate to the Log > Flow Reporting page to manually select the **Enable Flow Reporting and Visualization** checkbox to activate the feature. You can then view real-time application traffic on the Dashboard > Real-Time Monitor page and application activity in other Dashboard pages for the configured flows from the SonicWALL application signature database.



If you plan to use both internal ***and*** external flow reporting, SonicWALL recommends enabling the following (located in the Log > Flow Reporting screen) after successfully registering and licensing your appliance to avoid multiple restarts:

- Enable Flow Reporting and Visualization
- Report to EXTERNAL Flow Collector

- **Application Intelligence + Control**—This feature has two components for more network security:

  (a) **Identification**: Identify applications and track user network behaviors in real-time.
  (b) **Control**: Allow/deny application and user traffic based on bandwidth limiting policies.

  Administrators can now more easily create network policy object-based control rules to filter network traffic flows based on:

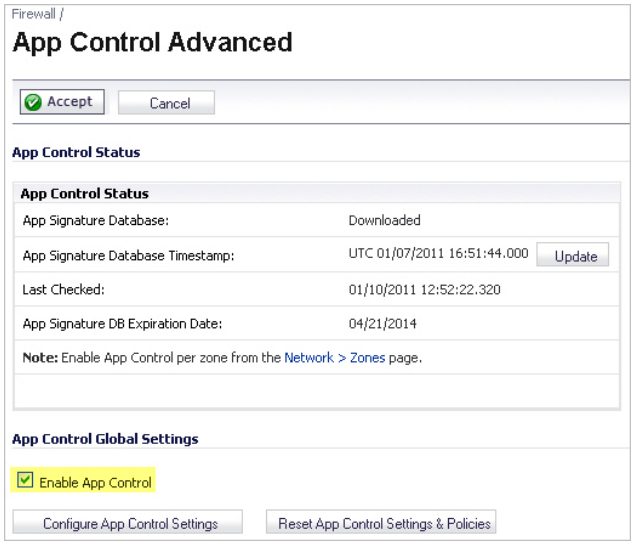
  - Blocking signature-matching **Applications**, which are notoriously dangerous and difficult to enforce
  - Viewing the real-time network activity of trusted **Users and User Groups** and guest services
  - Matching **Content-rated categories**

  Network security administrators now have application-level, user-level, and content-level real-time visibility into the traffic flowing through their networks. Administrators can take immediate action to re-traffic engineer their networks, and quickly identify Web usage abuse, and protect their organizations from infiltration by malware. Administrators can limit access to bandwidth-hogging websites and applications, reserve higher priority to critical applications and services, and prevent sensitive data from escaping the SonicWALL secured networks.

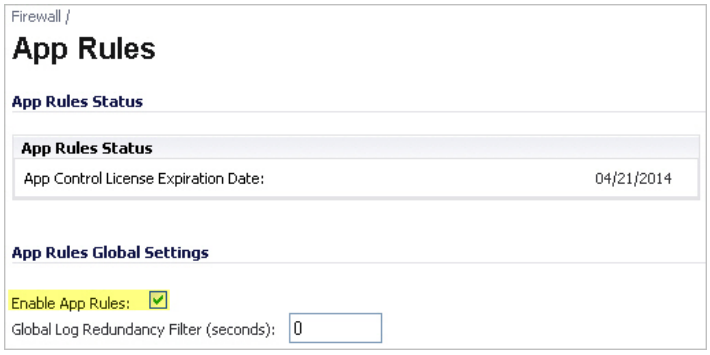
  New appliances running SonicOS 5.8 receive an automatic 30-day free trial for App Control upon registration.

  SonicWALL appliances upgrading to SonicOS 5.8 ***and*** already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) automatically receive a complimentary App Control license, required for creating Application Control policies.

  Select the **Enable App Control** option on the Firewall > App Control Advanced page to begin using the App Control feature.



  To create policies using App Rules (included with the App Control license), select **Enable App Rules** on the Firewall > App Rules page.



- **Deep Packet Inspection of SSL encrypted data (DPI-SSL)**—Provides the ability to transparently decrypt HTTPS and other SSL-based traffic, scan it for threats using SonicWALL's Deep Packet Inspection technology, then re-encrypt (or optionally SSL-offload) the traffic and send it to its destination if no threats or vulnerabilities are found. This feature works for both client and server deployments. It provides additional security, application control, and data leakage prevention functionality for analyzing encrypted HTTPS and other SSL-based traffic. The following security services and features are capable of utilizing DPI-SSL: Gateway Anti-Virus, Gateway Anti-Spyware, Intrusion Prevention, Content Filtering, Application Control, Packet Monitor and Packet Mirror. DPI-SSL is supported on SonicWALL NSA models 240 and higher.
- **Gateway Anti-Virus Enhancements (Cloud GAV)**—The Cloud Gateway Anti-Virus feature introduces an advanced malware scanning solution that compliments and extends the existing Gateway AV scanning mechanisms present on SonicWALL firewalls to counter the continued growth in the number of malware samples in the wild. Cloud Gateway Anti-Virus expands the Reassembly Free Deep Packet Inspection engine capabilities by consulting with the data center based malware analysis servers. This approach keeps the foundation of RFDPI-based malware detection by providing a low-latency, real-time solution that is capable of scanning unlimited numbers of files of unlimited size on all protocols that are presently supported without adding any significant incremental processing overhead to the appliances themselves. With this additional layer of security, SonicWALL's Next Generation Firewalls are able to extend their current protection to cover multiple millions of pieces of malware.
- **NTP Authentication Type**—When adding a Network Time Protocol server, the Add NTP Server dialog box provides a field to specify the NTP authentication type, such as MD5. Fields are also available to specify the trust key ID, the key number and the password.
- **Link Aggregation**—Link Aggregation provides the ability to group multiple Ethernet interfaces to form a trunk which looks and acts like a single physical interface. This feature is useful for high end deployments requiring more than 1 Gbps throughput for traffic flowing between two interfaces. This functionality is available on all NSA E-Class platforms.

  Static Link Aggregation with the ability to aggregate up to 4 ports into a single link is supported on SonicOS 5.8. A round-robin algorithm is used for load balancing traffic across the interfaces in an aggregated link.
- **Port Redundancy**—Port Redundancy provides the ability to configure a redundant physical interface for any Ethernet interface in order to provide a failover path in case a link goes down. Port Redundancy is available on all NSA E-Class platforms.

  When the primary interface is active, it handles all traffic from/to the interface. When the primary interface goes down, the backup interface takes over and handles all outgoing/incoming traffic. When the primary interface comes up again, it takes over all the traffic handling duties from the backup interface.

  When Port Redundancy, High Availability and WAN Load Balancing are used together, Port Redundancy takes precedence followed by High Availability, then followed by WAN Load Balancing.
- **Content Filtering Enhancements**—The CFS enhancements provide policy management of network traffic based on Application usage, User activity, and Content type. Administrators are now able to create multiple CFS policies per user group and set restrictive 'Bandwidth Management Policies' based on CFS categories.
- **IPFIX and NetFlow Reporting**—This feature enables administrators to gain visibility into traffic flows and volume through their networks, helping them with tracking, auditing and billing operations. This feature provides standards-based support for NetFlow Reporting, IPFIX, and IPFIX with extensions. The data exported through IPFIX with extensions contains information about network flows such as applications, users, and URLs extracted through Application Intelligence, along with standard attributes such as source/destination IP address (includes support for IPv6 networks), source/destination port, IP protocol, ingress/egress interface, sequence number, timestamp, number of bytes/packets, and more.
- **VLAN Support for TZ Series**—SonicOS 5.8 provides VLAN support for SonicWALL TZ 210/200/100 Series appliances, including wireless models. The TZ 210 and 200 Series support up to 10 VLANs, the TZ 100 Series supports up to 5 VLANs.

- **SonicPoint Virtual Access Point Support for TZ Series**—Virtual Access Points (VAPs) are now supported when one or more SonicWALL SonicPoints are connected to a SonicWALL TZ 210/200/100 Series appliance. The TZ 210 and 200 Series support up to 8 VAPs, the TZ 100 Series supports up to 5 VAPs.
- **Comprehensive Anti-Spam Service (CASS) 2.0**—The Comprehensive Anti-Spam Service (CASS) feature provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your SonicWALL security appliance. This feature increases the efficiency of your SonicWALL security appliance by providing you the ability to configure user view settings and filter junk messages before users see it in their inboxes. The following enhancements are now available with CASS 2.0:
    - The Email Security Junk Store application can now reside outside the Exchange Server system. Unlike in version 1.0, Junk Store can now be installed on another remote server.
    - Dynamic discovery of Junk Store user interface pages has been added. This feature allows the Junk Store to inform SonicOS of a list of pages to display under Anti-Spam in the SonicOS left hand navigation pane. For example, the pane might show Junk Box View, Junk Box Settings, Junk Summary, User View Setup, and/or Address Books.
    - User-defined Allow and Deny Lists can now be configured with FQDN and Range address objects in addition to Host objects.
    - A GRID IP Check tool has been added in the Anti-Spam > Status page. The SonicWALL administrator can specify (on-demand) an IP address to check against the SonicWALL GRID IP server. The result will either be LISTED or UNLISTED. Connections from a LISTED host will be blocked by the SonicWALL security appliance running CASS (unless overridden in the Allow List).
    - A parameter to specify the Probe Response Timeout is added in the Anti-Spam > Settings page Advanced Options section. There are deployment scenarios where a longer timeout is needed to prevent a target from frequently being marked as Unavailable. The default value is 30 seconds.
- **Enhanced Connection Limiting**—Connection Limiting enhancements expand the original Connection Limiting feature which provided global control of the number of connections for each IP address. This enhancement is designed to increase the granularity of this kind of control so that the SonicWALL administrator can configure connection limitation more flexibly. Connection Limiting uses Firewall Access Rules and Policies to allow the administrator to choose which IP address, which service, and which traffic direction when configuring connection limiting.
- **Dynamic WAN Scheduling**—SonicOS 5.8 supports scheduling to control when Dynamic WAN clients can connect. A Dynamic WAN client connects to the WAN interface and obtains an IP address with the PPPoE, L2TP, or PPTP. This enhancement allows the administrator to bind a schedule object to Dynamic WAN clients so that they can connect when the schedule allows it and they are disconnected at the end of the configured schedule. In the SonicOS management interface, a Schedule option is available on the WAN interface configuration screen when one of the above protocols is selected for IP Assignment. Once a schedule is applied, a log event is recorded upon start and stop of the schedule.
- **NTLM Authentication with Mozilla Browsers**—As an enhancement to Single Sign-On, SonicOS can now use NTLM authentication to identify users who are browsing using Mozilla-based browsers (including Internet Explorer, Firefox, Chrome and Safari). NTLM is part of a browser authentication suite known as “Integrated Windows Security” and should be supported by all Mozilla-based browsers. It allows a direct authentication request from the SonicWALL appliance to the browser with no SSO agent involvement. NTLM authentication works with browsers on Windows, Linux and Mac PCs, and provides a mechanism to achieve Single Sign-On with Linux and Mac PCs that are not able to interoperate with the SSO agent.
- **Single Sign-On Import Users from LDAP Option**—A new **Import from LDAP** button on the Users > Local Users page allows you to configure local users on the SonicWALL by retrieving the user names from your LDAP server. This allows SonicWALL user privileges to be granted upon successful LDAP authentication. For ease of use, options are provided to reduce the list to a manageable size and then select the users to import.

- **SSL VPN NetExtender Update**—This enhancement supports password change capability for SSL VPN users, along with various fixes. When the password expires, the user is prompted to change it when logging in via the NetExtender client or SSL VPN portal. It is supported for both local users and remote users (RADIUS and LDAP).
- **DHCP Scalability Enhancements**—The DHCP server in SonicWALL appliances has been enhanced to provide between 2 to 4 times the number of leases previously supported. To enhance the security of the DHCP infrastructure, the SonicOS DHCP server now provides server side conflict detection to ensure that no other device on the network is using the assigned IP address. Conflict detection is performed asynchronously to avoid delays when obtaining an address.
- **SIP Application Layer Gateway Enhancements**—SIP operational and scalability enhancements are provided in SonicOS 5.8. The SIP feature-set remains equivalent to previous SonicOS releases, but provides drastically improved reliability and performance. The **SIP Settings** section under the **VoIP > Settings** page is unchanged.

  SIP ALG support has existed within SonicOS firmware since very early versions on legacy platforms. Changes to SIP ALG have been added over time to support optimized media between phones, SIP Back-to-Back User Agent (B2BUA), additional equipment vendors, and operation on a multi-core system.

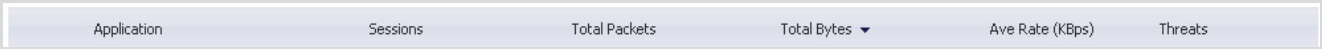
  The SIP protocol is now in a position of business critical importance – protecting the voice infrastructure, including VoIP. To accommodate the demands of this modern voice infrastructure, SIP ALG enhancements include the following:
  - **SIP Endpoint Information Database** – The algorithm for maintaining the state information for known endpoints is redesigned to use a database for improved performance and scalability. Endpoint information is no longer tied to the user ID, allowing multiple user IDs to be associated with a single endpoint. Endpoint database access is flexible and efficient, with indexing by NAT policy as well as by endpoint IP address and port.
  - **Automatically Added SIP Endpoints** – User-configured endpoints are automatically added to the database based on user-configured NAT policies, providing improved performance and ensuring correct mappings, as these endpoints are pre-populated rather than “learnt.”
  - **SIP Call Database** – A call database for maintaining information about calls in progress is implemented, providing improved performance and scalability to allow SonicOS to handle a much greater number of simultaneous calls. Call database entries can be associated with multiple calls.
  - **B2BUA Support Enhancements** – SIP Back-to-Back User Agent support is more efficient with various algorithm improvements.
  - **Connection Cache Improvements** – Much of the data previously held in the connection cache is offloaded to either the endpoint database or the call database, resulting in more efficient data access and corollary performance increase.
  - **Graceful Shutdown** – Allows SIP Transformations to be disabled without requiring the firewall to be restarted or waiting for existing SIP endpoint and call state information to time out.

User Interface Enhancements in SonicOS 5.8.0.1

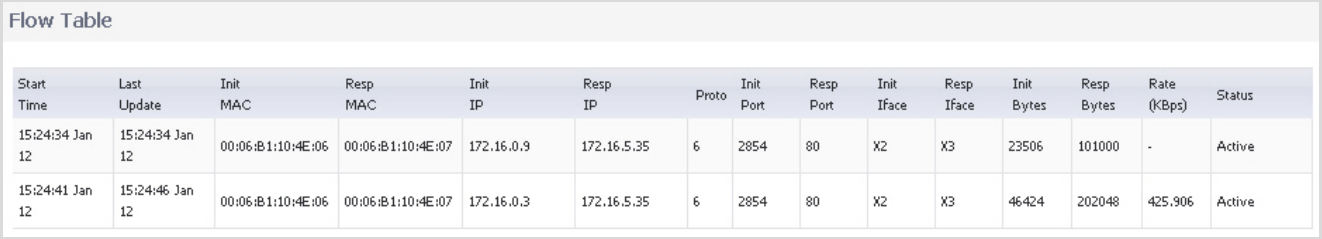
SonicOS 5.8.0.1 included several UI enhancements to the Visualization Dashboard screen to ensure efficient navigation through this feature. These enhancements include the following:

Dashboard > App Flow Monitor

- **App Flow Monitor Toolbar**—The toolbar categories for Packets, Bytes, and Rate has changed to Total Packets, Total Bytes, and Average Rate, providing the user with a more specific view of data being transferred.



- **Sessions Flow Table**—By clicking on the number specified under the Sessions category of any Application, a Flow Table displays with Application-specific data, including the Rate in KBps.

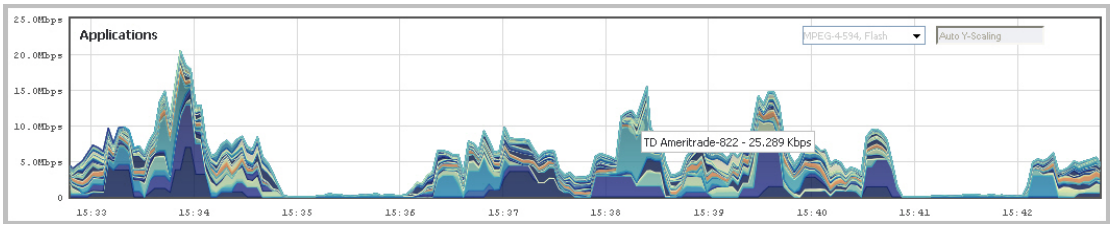


Dashboard > Real-Time Monitor

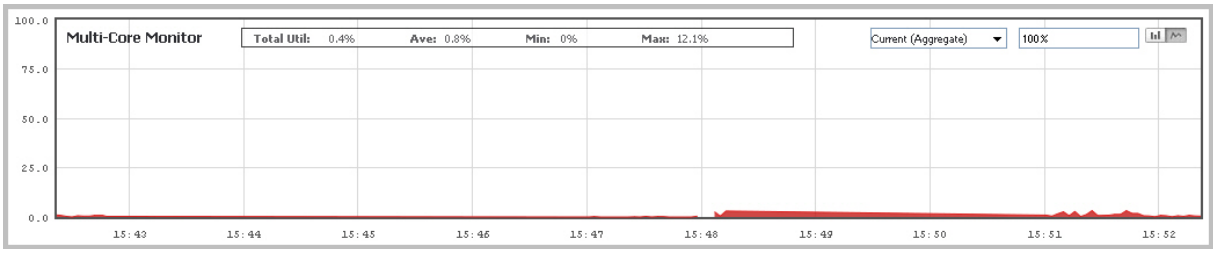
- **Real-Time Monitor Applications**—All application legends are now hidden by default from the Application Chart.

  To view the legends, click the Settings icon. Clear the option to **Hide Legends in Application Chart**. Then, click **Save**.

  To view individual application information, hover the mouse over the real-time visualization; a pop-up displays.



- **Multi-Core Monitor—**By default, the Multi-Core Monitor now displays as a stack chart, rather than as a bar graph, to easily show its relation to the other charts on this screen.



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 5.8.0.8 release.

Anti-Spam

Symptom	Condition / Workaround	Issue
Email containing a definite virus remains in the Inbox, rather than being deleted, when the Junk Store is not available.	Occurs when the **Store in Junk Box** option is selected for **Definite Virus**, and the **Emails when SonicWALL Junk Store is unavailable** option is set to **Delete**.	96866

Application Control

Symptom	Condition / Workaround	Issue
With an App Rules policy that uses a Bandwidth Management action, SonicOS does not display any usage statistics to indicate that traffic is being throttled.	Occurs when Bandwidth Management is enabled and an App Rules policy is configured to limit P2P traffic. The traffic is actually throttled.	96923
A user cannot login from the LAN although a policy is configured to allow the user to log in.	Occurs when CFS is enabled and an App Rules policy (of type CFS, IPS Content, or App Control) is configured and the user is selected for the Included Users/Groups list.	90394

App Flow Monitor

Symptom	Condition / Workaround	Issue
App Flow Monitor does not display active user sessions or traffic generated from the SonicOS SSL VPN portal.	Occurs when attempting to view SonicOS SSL VPN portal sessions. **Workaround**: Use NetExtender.	97466
App Flow Monitor incorrectly categorizes Web sites from one country as being from another.	Occurs when viewing App Flow Monitor after the country database IP address cannot be resolved.	96974

High Availability

Symptom	Condition / Workaround	Issue
After failover on a stateless High Availability pair that is configured for OSPF advanced routing over a VPN tunnel, the Backup unit sends traffic without encryption and VPN traffic is dropped.	Occurs after the Backup unit has learned the dynamic routes, after which traffic should be encrypted, but the unit keeps sending it in the clear. **Workaround**: Add a Drop_TunnelIf route policy on the High Availability pair.	96279
When an interface is removed from the Default Weighted Load Balancing group, the default 0.0.0.0 route lists the primary failover WLB interface as its next hop interface, but should use the currently active WLB interface.	Occurs when the Default WLB group is configured with five WAN interfaces. When one of the interfaces is removed, the default 0.0.0.0 route's next hop is modified. **Workaround**: Reboot the firewall.	92153

Licensing

Symptom	Condition / Workaround	Issue
Enabling the **Signature download through a proxy server** option causes license synchronization issues.	Occurs when enabling the option without configuring values for it, then registering the system on MySonicWALL. **Workaround**: Clear the flag to synchronize the unit's licenses.	93051

Logging

Symptom	Condition / Workaround	Issue
When a packet capture is completed, the firewall doesn't send out IPFIX Log template (ID 269) to the external collector.	Occurs when starting a packet capture and then selecting "Generate All Templates". After the packet capture has completed, the flow reporting statistics indicate there were 21 templates sent, however the packet capture consisted of 22 templates.	98341

Networking

Symptom	Condition / Workaround	Issue
When high availability is enabled with Active/Passive mode, the firewall will not switch to the redundant port if the primary port fails.	Occurs when the primary port X1 fails and high availability is enabled with active/passive mode. The firewall should switch to the redundant port to resume proper operation.	97883
Settings configured for Connection Limiting in SonicOS 5.5 and 5.6 do not stay saved when upgrading to SonicOS 5.8.	Occurs when enabling Connection Limiting in the **Firewall** > **Advanced** screen, and then upgrading to SonicOS 5.8. Values configured and saved for the Source and Destination IP addresses in the earlier SonicOS version are not applied to firewall rules or global settings.	97371
When new preferences are loaded and the firewall is rebooted, a number of critical messages are displayed on the console. The messages are related to automatically added policies with the Multicast source zone disabled.	Occurs when new preferences are loaded and the firewall is rebooted. The policies referenced in the messages are automatically added and are not typically used, so having them disabled should not cause any issues.	94641

Packet Monitor

Symptom	Condition / Workaround	Issue
Packet Monitor fails to capture packets after the firewall is restarted, after functioning properly before the restart.	Occurs when the **Enable filter based on the firewall rule** option is enabled and an access rule is configured. After the restart, traffic that triggers the access rule is not captured.	97000

Signatures / Detection

Symptom	Condition / Workaround	Issue
Real Time Monitor does not recognize sub-H323 and voice related protocols.	Occurs when playing a *pcap* file from LAN to WAN while viewing the Real Time Monitor. The display shows H323, but should also show H225, H245, RTP (Voice) and RTCP protocols.	92747

VPN

Symptom	Condition / Workaround	Issue
A VPN tunnel cannot be created after changing the IKE (Phase 1) Proposal Exchange mode in the VPN Policy configuration. A reboot is required before the VPN tunnel can be created.	Occurs when a site-to-site VPN policy is added using Main Mode or Aggressive Mode in the IKE (Phase 1) Proposal **Exchange** field, and then the **Exchange** field is changed to IKEv2 Mode.	101332
Multicast traffic is not forwarded through a VPN tunnel after the security association is renegotiated using Quick Mode.	Occurs when the administrator clicks the **Renegotiate** button on a firewall at either end of the VPN tunnel to renegotiate the IPSec security association while multicast traffic is streaming through the tunnel. **Workaround**: Restart the client that is receiving the multicast traffic to make it send a Membership Report message.	96901

Wireless / 3G

Symptom	Condition / Workaround	Issue
The 3G card does not connect during Wireless WAN failover after the Ethernet WAN connection is lost.	Occurs when the 3G profile is set to Connect-on-Data mode. When in Persistent mode, it works correctly.	96069
A 3G card cannot reconnect and causes a fatal error on the firewall.	Occurs when using a Cingular Option GT MAX card for WAN Load Balancing. The 3G card functions correctly during a failover after the WAN interface is disconnected, and handles fail back correctly, but causes the error when trying to reconnect after the Default LB group is changed to allow only the M0 interface.	96068
After a reboot, the 3G U0 interface fails to reconnect and get an IP address.	Occurs with a Huawei E1750 3G card. The U0 interface initially connects successfully, but after a reboot, it is unable to reconnect.	92870

Resolved Issues

The following issue is resolved in the SonicOS 5.8.0.8 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 5.8.0.4 release.

Content Filtering System

Symptom	Condition / Workaround	Issue
The “Safesearch” option on Bing.com is not being re-enabled.	Occurs when navigating to Bing.com and disabling the Safesearch option before the Safesearch Enforcement option is enabled.	97206

High Availability

Symptom	Condition / Workaround	Issue
The appliance may experience vulnerability issues causing it to restart.	Occurs when running a Qualys vulnerability scan with a high availability pair configuration.	105129

Modem

Symptom	Condition / Workaround	Issue
For Verizon customers, 3G does not work with a Novatel U760 modem.	Occurs when using a Novatel U760 modem. Verizon no longer supports the Novatel U760. **Workaround:** Use a UMW190 modem for 3G support with SonicOS 5.8.0.4.	105457
The U0/U1 interface is incorrectly displayed in the Statistics section of the **Network** > **Failover & LB** page.	Occurs when configuring a 3G card on the U0/U1 interface, then removing the 3G card and restarting the appliance.	93874

Networking

Symptom	Condition / Workaround	Issue
The phrase “Recommended” should be used instead of “Least Connections” in the management interface.	Occurs when the phrase “Least Connections” is displayed in the **Firewall Settings > Advanced** page under the Connections section.	106818
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
The firewall displays the server status as “online” even though the server’s HTTP service is offline and the Transmission Control Protocol (TCP) probe is not working.	Occurs when configuring Network Address Translation (NAT) – Load Balancing (LB) on two HTTP servers, selecting the Sticky IP method, and enabling probing with TCP.	90900

Signatures / Detection

Symptom	Condition / Workaround	Issue
When Application Control is configured to block Webmail, it fails to block the webmail site http://mail.163.com.	Occurs when the Application Control service is enforced on the LAN zone to block Webmail.	90260

Users

Symptom	Condition / Workaround	Issue
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
The access rules "users allowed" field is not enforced for a TSA user who is already logged in.	Occurs when a TSA user attempts to access an IP address with access rules set to block TSA users. The first attempt functions properly and is blocked. The second attempt allows access.	101970
During SSO Agent configuration on TZ 200 and TZ 100 series appliances, the **Test** tab page is blank.	Occurs when “SonicWALL SSO Agent” is selected as the **Single-sign-on method** on the Users > Settings page, and then the configuration window is opened by clicking the **Configure** button. When the **Test** tab is selected, the page appears blank.	101652

Vulnerability Protection

Symptom	Condition / Workaround	Issue
The File Transfer Protocol (FTP) traffic going from the WAN to the LAN FTP server does not complete.	Occurs when enabling the “Always proxy WAN client connections” option on the **Firewall > TCP Settings** page.	51071

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
The Technical Support Report (TSR) does not include the Extensible Authentication Protocol Over LAN (EAPOL) version information.	Occurs when running internal wireless in bridge mode with Wi-Fi Protected Access (WPA) type security.	93548

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.

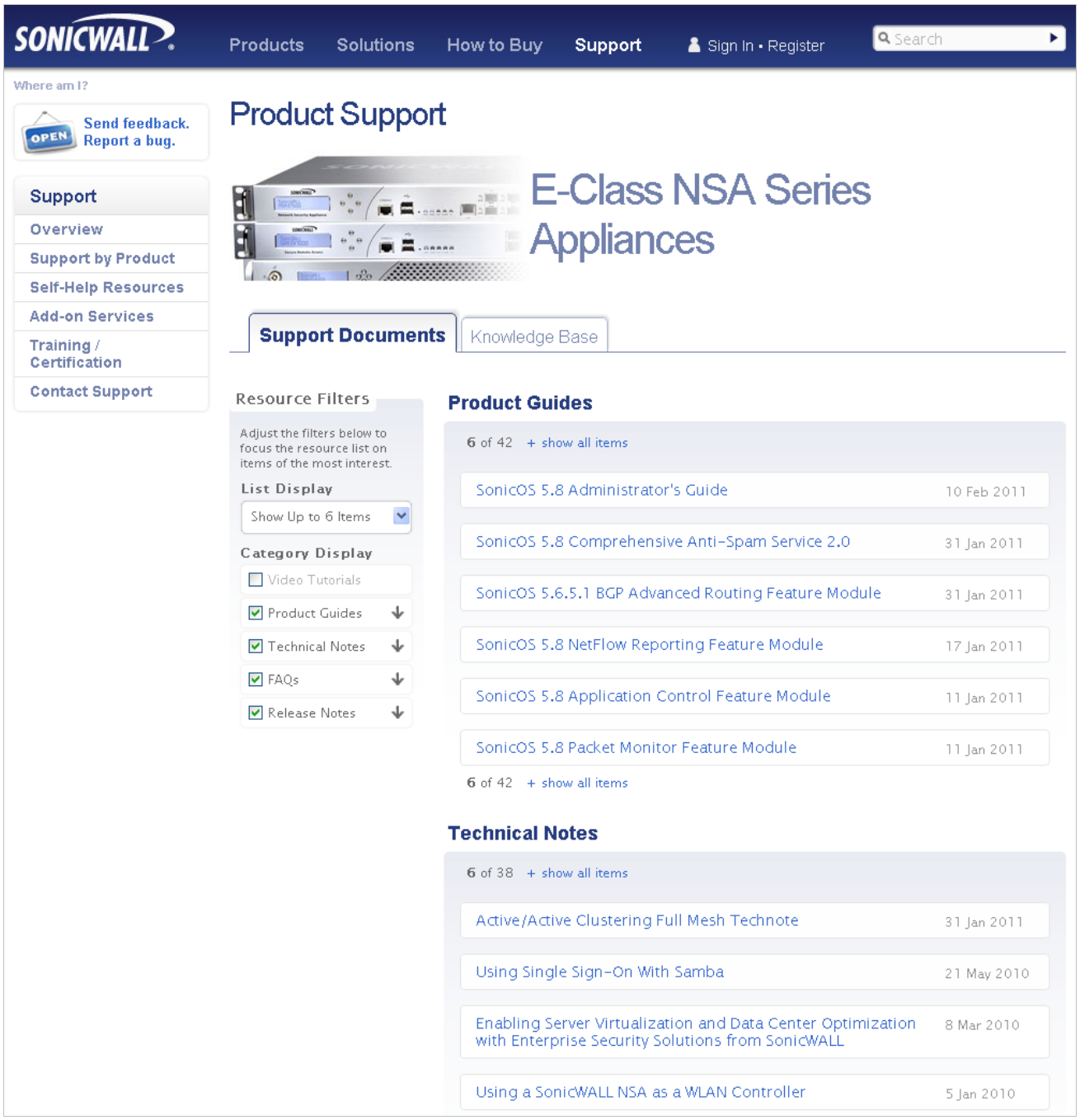
   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

   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: 10/11/2011