

# Release Notes

## Contents

---

<i>Platform Compatibility</i> .....	1
<i>Browser Support</i> .....	1
<i>Enhancements in SonicOS 5.8.1.7</i> .....	2
<i>Supported Features by Appliance Model</i> .....	2
<i>Key Features in SonicOS 5.8</i> .....	4
<i>Known Issues</i> .....	12
<i>Resolved Issues</i> .....	15
<i>Upgrading SonicOS Image Procedures</i> .....	16
<i>Related Technical Documentation</i> .....	21

## Platform Compatibility

---

The SonicOS 5.8.1.7 release is supported on the following SonicWALL Deep Packet Inspection (DPI) security appliances:

- SonicWALL TZ 105 / 105 Wireless
- SonicWALL TZ 205 / 205 Wireless

The SonicWALL WXA series appliances (WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are also supported for use with SonicWALL NSA E-Class, NSA, and TZ products running 5.8.1.7. The minimum recommended firmware version for the WXA series appliances is 1.1.1.

## Browser Support

---



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

This release supports the following Web browsers:

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

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

# Release Notes

## Enhancements in SonicOS 5.8.1.7

Beginning in SonicOS 5.8.1.7, HTTP access to the SonicOS web-based management interface is disabled by default. When running SonicOS 5.8.1.7 using factory defaults, the administrator can log into the management interface using HTTPS at <https://192.168.168.168>.

HTTP management is still allowed when upgrading from prior firmware versions, when already enabled in the previous configuration settings.

**Note:** HTTP management must be enabled when the firewall is being managed by SonicWALL GMS via a VPN tunnel. This applies when using either a GMS Management Tunnel or an existing VPN tunnel.

The System > Administration page has a new **Allow management via HTTP** checkbox to allow the administrator to enable/disable HTTP management globally.

**Web Management Settings**

Allow management via HTTP

HTTP Port:  Delete cookies

HTTPS Port:  End config. mode

Certificate Selection:

Certificate Common Name:

Default Table Size:  items per page

Auto-updated Table Refresh Interval:  in seconds

Use System Dashboard View as starting page

Enable Tooltip

Form Tooltip Delay:  in msec

Button Tooltip Delay:  in msec

Text Tooltip Delay:  in msec

## 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	TZ 105 Series	TZ 205 Series
Wireless Client Bridge Support	Supported	Supported
App Flow Monitor		
Real-Time Monitor		
Packet Monitor Enhancements	Supported	Supported
Log > Flow Reporting		
App Control Advanced	Supported	Supported
App Rules	Supported	Supported

# Release Notes

Feature / Enhancement	TZ 105 Series	TZ 205 Series
DPI-SSL		
Stateless High Availability		Supported
Cloud GAV	Supported	Supported
NTP Auth Type	Supported	Supported
Link Aggregation		
Port Redundancy		
CFS Enhancements	Supported	Supported
IPFIX & NetFlow Reporting		
VLAN Subinterfaces	Supported	Supported
SonicPoint VAPs	Supported	Supported
CASS 2.0	Supported	Supported
Enhanced Connection Limit	Supported	Supported
Dynamic WAN Scheduling	Supported	Supported
Browser NTLM Auth	Supported	Supported
User Import from LDAP	Supported	Supported
SSL VPN NetExtender Client Update	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported
SIP Application Layer Enhancements	Supported	Supported
SonicPoint-N DR	Supported	Supported
Accept Multiple VPN Client Proposals.	Supported	Supported
WAN Acceleration Support	Supported	Supported
App Control Policy Configuration via App Flow Monitor		
Global BWM Ease of Use Enhancements	Supported	Supported
Application Usage and Risk Report		
Geo-IP Filtering and Botnet Command & Control Filtering		
Wire and Tap Mode		
Customizable Login Page	Supported	Supported
Preservation of Anti-Virus Exclusions After Upgrade	Supported	Supported
Management Traffic Only Option for Network Interfaces	Supported	Supported
Current Users and Detail of Users Options for TSR	Supported	Supported
User Monitor Tool		
Auto-Configuration of URLs to Bypass User Authentication	Supported	Supported

# Release Notes

## Key Features in SonicOS 5.8

The following are the key features introduced in SonicOS 5.8:

- **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 easily create network policy object-based control rules to filter network traffic flows based on:

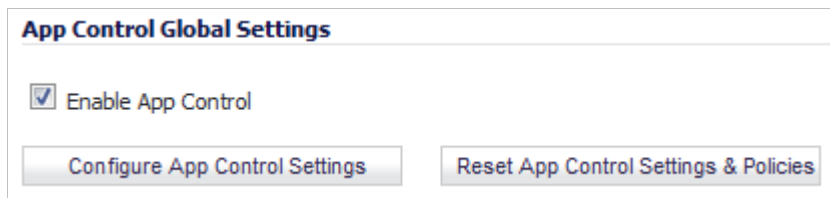
- Blocking signature-matching **Applications**, which are notoriously dangerous and difficult to enforce
- Viewing the real-time network activity of trusted **Users and User Groups** and guest services
- Matching **Content-rated categories**

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, 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.

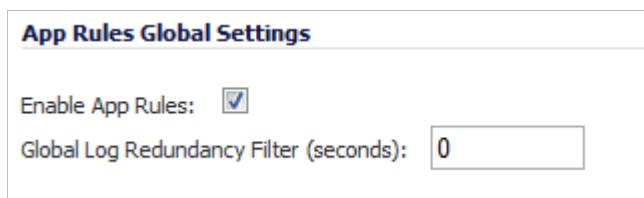
SonicWALL appliances upgrading to SonicOS 5.8 **and** already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) automatically receive a complimentary App Control license, required for creating Application Control policies.

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



The screenshot shows the 'App Control Global Settings' interface. It features a checked checkbox for 'Enable App Control'. Below this are two buttons: 'Configure App Control Settings' and 'Reset App Control Settings & Policies'.

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



The screenshot shows the 'App Rules Global Settings' interface. It features a checked checkbox for 'Enable App Rules'. Below this is a text input field for 'Global Log Redundancy Filter (seconds)' with the value '0'.

# Release Notes

- **Global Bandwidth Management**—Global Bandwidth Management improves ease of use for bandwidth management (BWM) configuration, and increases throughput performance of managed packets for ingress and egress traffic on all interfaces, not just WAN. The new Firewall Settings > BWM page allows network administrators to specify guaranteed minimum bandwidth, maximum bandwidth, and control the number of different priority levels for traffic. These global settings are used in firewall access rules and application control policies. Global BWM provides:
  - Simple bandwidth management on all interfaces.
  - Bandwidth management of both ingress and egress traffic.
  - Support for specifying bandwidth management priority per firewall rules and application control rules.
  - Default bandwidth management queue for all traffic.
  - Support for applying bandwidth management directly from the Dashboard > App Flow Monitor page.

Global bandwidth management provides 8 priority queues, which can be applied to each physical interface.

The new **Firewall Settings > BWM** page is shown below:

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
<b>Total:</b>		<b>100</b>	

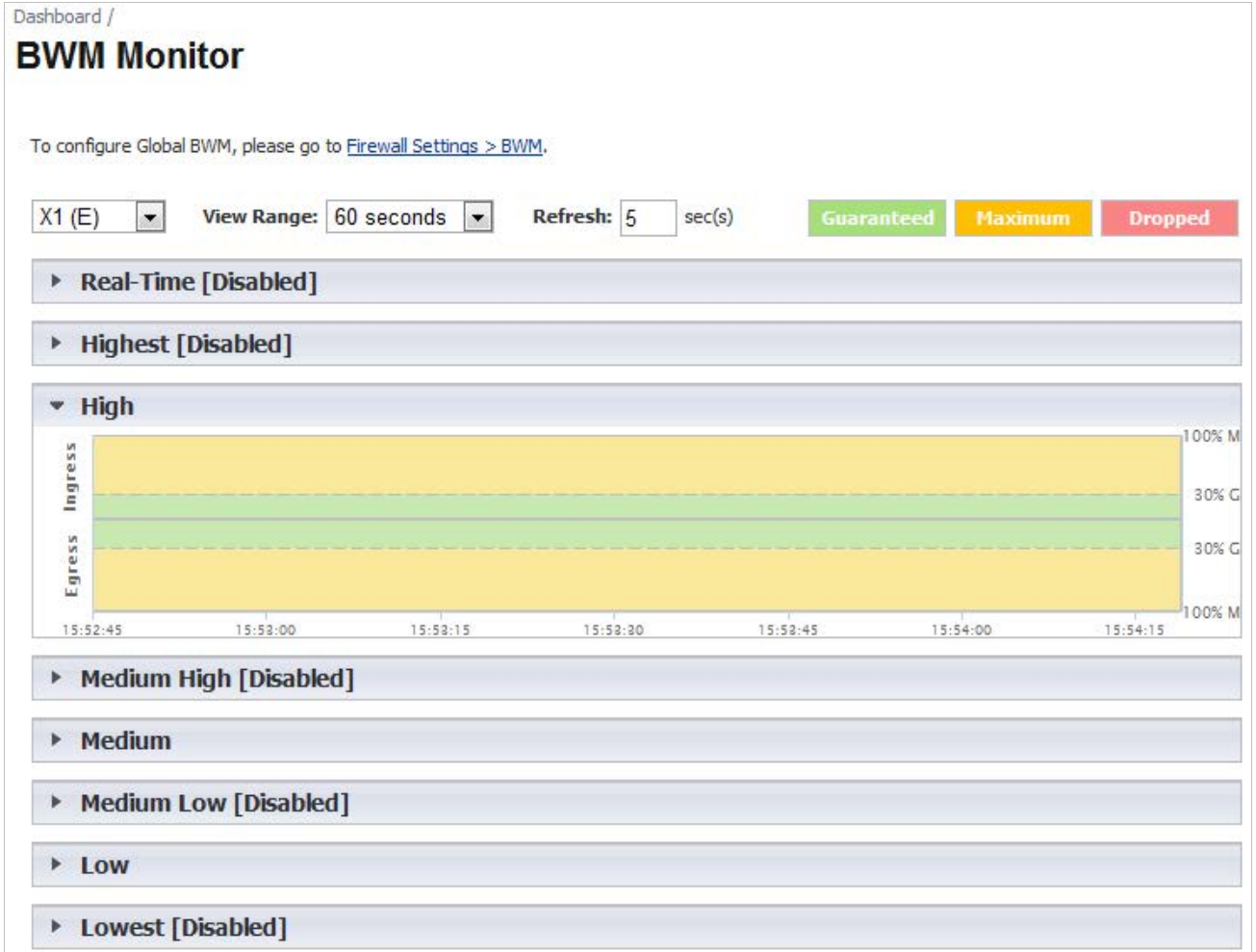
You can select either **WAN** or **Global** as the **Bandwidth Management Type**.

**Note:** When switching between bandwidth management modes, all bandwidth management settings in firewall access rules are set back to defaults and any custom settings must be reconfigured. Default BWM actions in Application Control policies are automatically converted to WAN BWM or Global BWM, using default priority levels.

In the global priority queue table, you can configure the **Guaranteed** and **Maximum\Burst** rates for each **Priority** queue. The rates are specified as a percentage. The actual rate is determined dynamically while applying BWM on an interface. The configured bandwidth on an interface is used in calculating the absolute value. The sum of all guaranteed bandwidth must not exceed 100%, and guaranteed bandwidth must not be greater than maximum bandwidth per queue.

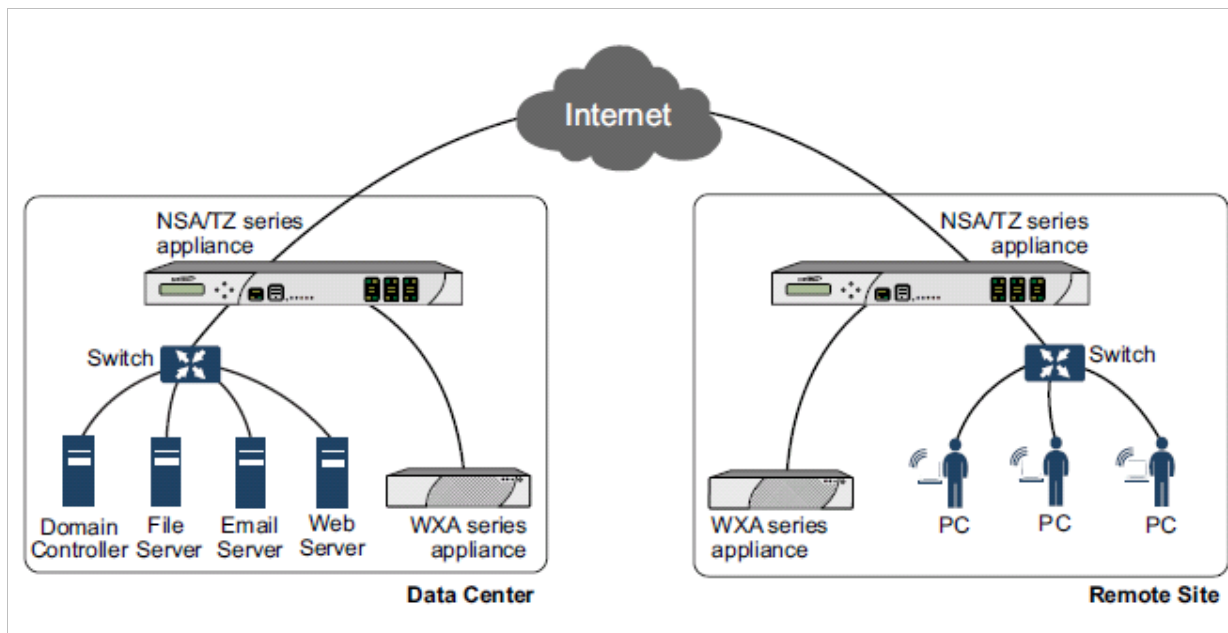
# Release Notes

- **Bandwidth Management Monitor Page**—The new BWM Monitor page displays per-interface bandwidth management for ingress and egress network traffic. The BWM monitor graphs are available for real-time, highest, high, medium high, medium, medium low, low and lowest policy settings. The view range is configurable in 60 seconds, 2 minutes, 5 minutes, and 10 minutes (default). The refresh interval rate is configurable from 3 to 30 seconds. The bandwidth management priority is depicted by guaranteed, maximum, and dropped.



# Release Notes

- **WAN Acceleration**—SonicOS 5.8.1.7 provides support for the SonicWALL WXA series appliances which are deployed in one-arm mode with SonicWALL firewalls. WAN Acceleration appliances employ techniques such as TCP acceleration and Windows File Sharing (WFS) acceleration to optimize WAN traffic between multiple locations connected by VPN or dedicated links. In this deployment, the SonicWALL appliance provides networking and security services, such as application control, intrusion prevention, anti-malware protection, VPN, routing, anti-spam, and content filtering while the WAN acceleration appliance eliminates redundant traffic and eliminates protocol latency. The following diagram illustrates the basic network topology for the SonicWALL WXA series appliances and the SonicWALL network security appliances.



WAN acceleration using a SonicWALL WXA series appliance can provide an increase in application performance response time without purchasing a higher quality service or larger provision of bandwidth. This is especially noticeable on WAN connections such with high latency, which causes some applications to perform poorly.

- **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 5.8.0.3 or higher.

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.

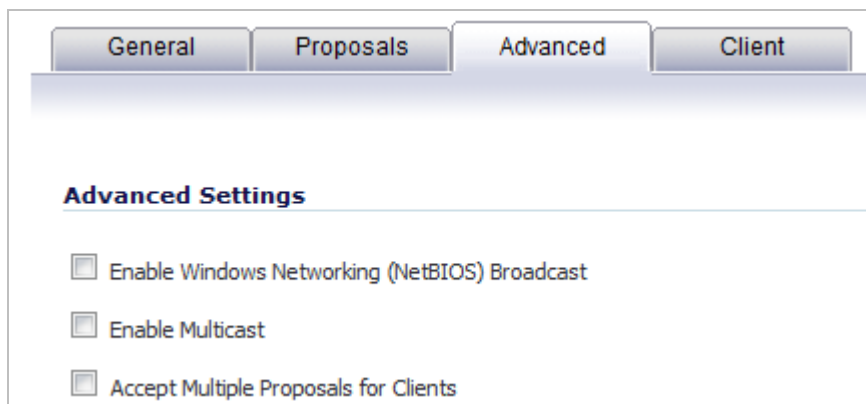
**Note:** The SonicPoint-N DR cannot broadcast the same Service Set Identifiers (SSID) when using Virtual Access Points (VAP) on 2.4 and 5 GHz frequency ranges.

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](http://www.sonicwall.com/app/projects/file_downloader/document_lib.php?t=PG&id=444)



# Release Notes

- **Accept Multiple Proposals for Clients Option**—The **Accept Multiple Proposals for Clients** checkbox allows multiple VPN or L2TP clients using different security policies to connect to a firewall running SonicOS 5.8.0.3 or higher  
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.

- **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.



# Release Notes

- **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.
- **Content Filtering Enhancements**—The CFS enhancements provide policy management of network traffic based on Application usage, User activity, and Content type. Administrators can create multiple CFS policies per user group and set restrictive 'Bandwidth Management Policies' based on CFS categories.
- **VLAN Support for TZ Series**—SonicOS 5.8 provides VLAN support for SonicWALL TZ 105/205 Series appliances, including wireless models.
- **SonicPoint Virtual Access Point Support for TZ Series**—Virtual Access Points (VAPs) are supported when one or more SonicWALL SonicPoints are connected to a SonicWALL TZ 105/205 Series appliance.
- **LDAP Primary Group Attribute**—To allow Domain Users to be used when configuring policies, membership of the Domain Users group can be looked up via an LDAP "Primary group" attribute. SonicOS 5.8.1.7 provides an attribute setting in the LDAP schema configuration for using this feature.
- **Preservation of Anti-Virus Exclusions After Upgrade**—SonicOS 5.8.1.7 includes the ability to detect if the starting IP address in an existing range configured for exclusion from anti-virus enforcement belongs to either LAN, WAN, DMZ or WLAN zones. After upgrading to a newer firmware version, SonicOS applies the IP range to a newly created address object. Detecting addresses for other zones not listed above, including custom zones, is not supported.

Anti-virus exclusions which existed before the upgrade and which apply to hosts residing in custom zones will not be detected. IP address ranges not falling into the supported zones will default to the LAN zone. Conversion to the LAN zone occurs during the restart process. There is no message in the SonicOS management interface at login time regarding the conversion.

- **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 capabilities are available with CASS 2.0:
  - The Email Security Junk Store application can reside outside the Exchange Server system, such as on a remote server.
  - Dynamic discovery of Junk Store user interface pages 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 be configured with FQDN and Range address objects in addition to Host objects.
  - A GRID IP Check tool is available 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 available in the Anti-Spam > Settings page Advanced Options section. This option supports deployment scenarios where a longer timeout is needed to prevent a target from frequently being marked as Unavailable. The default value is 30 seconds.

# Release Notes

- **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**—An **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.

# Release Notes

- **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.
- **Management Traffic Only Option for Network Interfaces**—SonicOS 5.8.1.7 provides a **Management Traffic Only** option on the **Advanced** tab of the interface configuration window, when configuring an interface from the **Network > Interfaces** page. When selected, this option prioritizes all traffic arriving on that interface. The administrator should enable this option **ONLY** on interfaces intended to be used exclusively for management purposes. If this option is enabled on a regular interface, it will still prioritize the traffic, but that may not be the desired result. It is up to the administrator to limit the traffic to just management; the firmware does not have the ability to prevent pass-through traffic.

The purpose of this option is to provide the ability to access the SonicOS management interface even when the appliance is running at 100% utilization.
- **Auto-Configuration of URLs to Bypass User Authentication**—SonicOS 5.8.1.7 includes a new auto-configuration utility to temporarily allow traffic from a single, specified IP address to bypass authentication. The destinations that traffic accesses are then recorded and used to allow that traffic to bypass authentication. Typically this is used to allow traffic such as anti-virus updates and Windows updates. To use this feature, navigate to **Users > Settings** and click the **Auto-configure** button in the Other Global User Settings section.

# Release Notes

## Known Issues

This section contains a list of known issues in the SonicOS 5.8.1.7 release.

### Application Control

Symptom	Condition / Workaround	Issue
Emails are received with attachments even though an App Rules policy is created to block attachments.	Occurs when creating an App Rules policy to block POP3 incoming emails with .exe attachments, then connecting a PC to a firewall's LAN interface, and sending an email with an .exe attachment.	111851
App Control Advanced policies are applied to traffic from and to the VPN zone, rather than within 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 Advanced policy is applied to VPN traffic.	107296
App Rules policies remain in effect even when disabled globally.	Occurs when the Enable App Rules checkbox is cleared to disable these policies globally, then an App Rules policy is created. When traffic on the WAN interface matches the rule, the configured policy action is applied. Workaround: Clear the Enable App Rules checkbox and reboot the appliance.	101194

### 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. <b>Workaround:</b> 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

### High Availability

Symptom	Condition / Workaround	Issue
WAN failover and failback can cause Internet connectivity problems.	Occurs when using WAN load balancing and probing fails on a NAT static IP address using ICMP or TCP for probing.	112783

# Release Notes

## Log

Symptom	Condition / Workaround	Issue
No user name is generated by the SonicWALL in some syslog messages for connections from a terminal server. ViewPoint reporting therefore does not include the user names.	Occurs when syslog messages are sent for traffic from a terminal server after users connect to it, but before the user identification information for the connection is received from the TS agent.	89488

## Networking

Symptom	Condition / Workaround	Issue
Intermittent dropped routes for Route Based VPN or Tunnel Interfaces.	Occurs when configuring more than one Route Based VPN (or Tunnel Interface) to remote units with OSPF enabled.	102961

## Security Services

Symptom	Condition / Workaround	Issue
Some versions of UltraSurf are not blocked by the SonicOS Intrusion Prevention Service, although log messages state that the connection is blocked.	Occurs when UltraSurf 11.03 or 11.04 are being used to bypass the firewall policies. <b>Workaround:</b> Enable DPI-SSL and block all UDP traffic (via an access rule) to the 65.49.14.0/24 subnet.	111716
The Anti-Virus enforcement list is not correct after upgrading from SonicOS 5.6.0.x to 5.8.x.	Occurs when Kaspersky Anti-Virus was licensed on SonicOS 5.6.0.x, with AV enforcement enabled for the zone and an AV enforcement list configured on the Security Services page.	110845

## System

Symptom	Condition / Workaround	Issue
After adding a VLAN interface, the firewall stops forwarding interesting, allowed traffic.	Occurs when a VLAN sub-interface is added; occurs on two different NSA 4500 appliances. Packets are dropped due to an enforced firewall rule. <b>Workaround:</b> After adding the VLAN interface, disable and then enable the Allow policy that allows the interesting traffic.	114206

## Users

Symptom	Condition / Workaround	Issue
The Log page displays the message "UDP Packet Dropped" after pinging a host or accessing a website using a Domain Name.	Occurs when navigating to the Users > Settings page and selecting <b>SSO Agent</b> from the <b>Single Sign On Method</b> drop-down list, then configuring the TSA agent and setting the default LAN to WAN Access Rule to <b>Trusted Users</b> .	111879

# Release Notes

## **User Interface**

Symptom	Condition / Workaround	Issue
A JavaScript error is sometimes displayed when editing DHCP settings.	Occurs when editing a DHCP option group or when editing interface settings and changing the DHCP scope.	110087

## **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 an IPsec VPN tunnel is configured between two SonicWALL appliances, one of which provides dual WAN interfaces (X1 and X4). If the primary WAN interface is disconnected, the tunnel cannot be established using the secondary interface.	103935

# Release Notes

## Resolved Issues

The following issues were resolved in the SonicOS 5.8.1.7 release:

### Content Filtering System

Symptom	Condition / Workaround	Issue
Attempting to delete an entry on the Security Services > Content Filter page fails and displays an error message on the Status line, "Bad value, script-like text found."	Occurs when attempting to delete an entry from the <b>Trusted Domains</b> list or the <b>CFS Policy per IP Address Range</b> list on the Security Services > Content Filter page, when the <b>Web Page to Display when Blocking</b> text box contains HTML text. <b>Workaround:</b> Delete all text in the <b>Web Page to Display when Blocking</b> text box (saving it elsewhere), delete the policy entry, and then add the block message text back in again.	115129

### Firmware

Symptom	Condition / Workaround	Issue
Cannot login to the firewall's management interface with a previously customized Login Authentication page.	Occurs when running SonicOS 5.8.1.6 firmware and logging into the management interface using a custom Login Authentication page created in SonicOS 5.8.1.5 or earlier. <b>Workaround:</b> Use "defauth.html" to login, if your current Login Authentication page does not allow you to access the management interface. Navigate to the <b>Users &gt; Settings</b> page and click the <b>Default</b> button in the <b>Customized Login Pages</b> section. Use this template to customize the management interface Login Authentication page, then click the <b>Accept</b> button.	114699
Stability improvements are needed when using tunnel interface VPN policies.	Occurs when OSPF is enabled on X0 and approximately 130 VPN security associations of Tunnel Interface type are in use.	113886
The firewall may randomly restart in standalone mode or with a high availability pair configuration.	Occurs after upgrading SonicOS firmware on a SonicWALL NSA 2400 security appliance.	113445

### Networking

Symptom	Condition / Workaround	Issue
A NAT policy lookup can generate an invalid message.	Occurs when the lookup generates messages containing "CRITICAL - Informational: natPolicyRemap:1282:".	114478

# Release Notes

## Upgrading SonicOS Image Procedures

---

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

<i>Obtaining the Latest SonicOS Image Version</i> .....	16
<i>Saving a Backup Copy of Your Configuration Preferences</i> .....	16
<i>Upgrading a SonicOS Image with Current Preferences</i> .....	17
<i>Importing Preferences to SonicOS 5.8</i> .....	17
<i>Importing Preferences from SonicOS Standard to SonicOS 5.8 Enhanced</i> .....	18
<i>Support Matrix for Importing Preferences</i> .....	19
<i>Upgrading a SonicOS Image with Factory Defaults</i> .....	20
<i>Using SafeMode to Upgrade Firmware</i> .....	20

### **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.
3. On the System > Diagnostics page, under Tech Support Report, select the following checkboxes and then click the **Download Report** button:
  - VPN Keys
  - ARP Cache
  - DHCP Bindings
  - IKE Info
  - SonicPointN Diagnostics
  - Current users
  - Detail of users

The information is saved to a "techSupport\_" file on your management computer.



# Release Notes

---

## ***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](http://mysonicwall.com) and save it to a location on your local computer.
2. On the System > Settings page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS 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 network security appliances is generally supported from the following SonicWALL appliances running SonicOS:

- NSA Series
- NSA E-Class Series
- TZ 215/210/205/200/100/105/190/180/170 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.

# Release Notes

## **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](mailto: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.



# Release Notes

## **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](http://mysonicwall.com) and save it to a location on your local computer.
2. On the System > Settings page, click **Create Backup**.
3. Click **Upload New Firmware**.
4. Browse to the location where you saved the SonicOS 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.

# Release Notes

## Related Technical Documentation

SonicWALL user guides and reference documentation is available at the SonicWALL Technical Documentation Online Library: <http://www.sonicwall.com/us/Support.html>

For basic and advanced deployment examples, refer to SonicOS Guides and SonicOS TechNotes available on the Website.

The screenshot shows the SonicWALL website's Product Support section for TZ Series Appliances. The page features a navigation menu on the left with categories like Support, Product Documentation, Network Security, and TZ Series. The main content area is titled 'Product Support' and 'TZ Series Appliances'. It includes a search bar, a navigation bar with 'Support Documents' and 'Knowledge Base', and three main sections: 'List View Options', 'Product Guides', and 'Technical Notes'. The 'List View Options' section allows users to filter resources by categories such as Video Tutorials, Product Guides, Technical Notes, FAQs, and Release Notes. The 'Product Guides' section displays a list of documents, including 'SonicOS 5.8.1 Rev E Administrator's Guide' and 'Safety and Regulatory Information for SonicWALL TZ 105 Wireless Appliances'. The 'Technical Notes' section shows documents like 'Integrating Agilink with SonicOS 5.8.1.5'.

**Support Documents** Knowledge Base

**Product Guides**

6 of 68 more items | all items

SonicOS 5.8.1 Rev E Administrator's Guide	19 Apr 2012
Safety and Regulatory Information for SonicWALL TZ 105 Wireless Appliances	16 Apr 2012
SonicWALL TZ 205 Series Quick Start Poster	16 Apr 2012
SonicWALL TZ 105 Series Quick Start Poster	16 Apr 2012
Safety and Regulatory Information for SonicWALL TZ 105 Appliances	16 Apr 2012
Safety and Regulatory Information for SonicWALL TZ 205 Appliances	16 Apr 2012

6 of 68 more items | all items

**Technical Notes**

6 of 20 more items | all items

Integrating Agilink with SonicOS 5.8.1.5	3 Mar 2012
Integrating CradlePoint with SonicOS 5.8.1.5	3 Mar 2012

Last updated: 4/27/2012