Question/Topic

UTM: Key Features and Enhancements in SonicOS Enhanced (5.1.0 to 5.8.1)

Answer/Article

Key Features and Enhancements in SonicOS Enhanced 5.8.1, 5.8.0, 5.7.0, 5.6.0, 5.5.0, 5.4.0, 5.3.0, 5.2.0, and 5.1.0

This article contains the following sections:

Key Features in SonicOS Enhanced 5.8.1

SonicOS Enhanced 5.8.1 is the most powerful SonicOS operating system for SonicWALL security appliances and include the following key features:

• **App Control Policy Configuration via App Flow Monitor** - The Dashboard > App Flow Monitor page now provides a Create Rule button that allows the administrator to quickly configure App Rule policies for application blocking, bandwidth management, or packet monitoring.

• **Current Users and Detail of Users Options for TSR** - SonicOS 5.8.1.0 provides two new checkboxes, Current users and Detail of users, in the Tech Support Report section of the System > Diagnostics page. These options allow the currently connected users to be omitted from the TSR, included as a simple summary list, or included with full details.

• **Customizable Login Page** - SonicOS 5.8.1.0 provides the ability to customize the language of the login authentication pages that are presented to users. Administrators can translate the login related pages with their own wording and apply the changes so that they take effect without rebooting.

Although the entire SonicOS interface is available in different languages, sometimes the administrator does not want to change the entire UI language to a specific local one. However, if the firewall requires authentication before users can access other networks, or enables external access services (e.g. VPN, SSL-VPN), those login related pages usually should be localized to make them more usable for normal users.

• **Geo-IP & Botnet Filtering** - This feature allows the administrator to block connections to or from a geographic location based on IP address(es), and to or from a BOTNET command and control server. A new Security Services > Geo-IP & BOTNET Filter page has been added to the management interface.

You can look up an IP address to find out the domain, DNS server, and check whether it is part of a Botnet. The Services > Geo-IP & BOTNET Filter page provides this functionality at the bottom of the page. The System > Diagnostics and Dashboard > App Flow Monitor pages also provide this capability.

• **Global BWM Ease of Use Enhancements** - Several enhancements are provided in this release to improve ease of use for Bandwidth Management (BWM) configuration, and also to increase throughput performance of managed packets:

–Support for simple bandwidth management on all interfaces.

–Support for bandwidth management on both ingress and egress.

–Support for specifying bandwidth management priority per firewall rules and app rules.

–Support for default bandwidth management Q for all traffic.

–Support for applying BWM via app flow monitor page.

Global bandwidth management provide 8 priority queues. The Guaranteed rate and Maximum\Burst rate are user configurable. Eight queues are created for each physical interface. As traffic flows through the firewall from interface1 to interface2, BWM is applied on both the interfaces according to the configuration. For example, ingress BWM can be applied based on interface1 settings and egress BWM applied on interface2 settings.

• **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, and SonicOS 5.8.1.0 provides a new attribute setting in the LDAP schema configuration for using this feature.

• **Management Traffic Only Option for Network Interfaces** - SonicOS 5.8.1.0 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 desirable 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.

• **Preservation of Anti-Virus Exclusions After Upgrade** - SonicOS 5.8.1.0 provides an enhancement 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 booting process. There is no message in the SonicOS management interface at login time regarding the conversion.

• **SonicWALL Enforced Client Anti Virus** - SonicOS 5.8.1.0 supports a new SonicWALL Enforced Client Anti-Virus. With Enforced Client, the SonicWALL firewall does not allow clients to connect and access the Internet unless they have client anti-virus installed.

The SonicWALL Enforced Client Beta Release Notes, available with the software on MySonicWALL, provide detailed information about client installation and usage, and describe administrator access to the SonicWALL Enforced Client Anti-Virus Policy and Reporting Server (EPRS). The EPRS system allows administrators to configure policies for clients and client groups, and to view reports showing top hazards and other client status.

Caution: Before installing SonicWALL Enforced Client on your client systems, Kaspersky Anti-Virus must be licensed on your SonicWALL appliance. To do this, email the serial number of the appliance to the beta alias (secbeta@sonicwall.com). After the general release, if you are running a firmware version prior to 5.8.1 and currently licensed for McAfee Anti-Virus, the McAfee AV license must expire or be expired before you can license Kaspersky AV. Please note that SonicWALL cannot reinstate your McAfee licensing if it is prematurely expired on customer request.Please do NOT contact SonicWALL technical support with any requests about the Enforced Client beta program. All questions and feedback should go to the above beta alias.

• **User Monitor Tool** - The User Monitor tool provides a quick and easy method to monitor the number of active users on the SonicWALL security appliance. To view the User Monitor tool, navigate to the **Dashboard > User Monitor** page. The tool provides several options for setting the scale of time over which user activity is displayed. The tool can display all users, only users who logged in through the web portal, or only users who logged in remotely through GVC or L2TP.

• **WAN Optimization** - SonicOS 5.8.1.0 supports the use of WAN Optimization devices with SonicWALL firewalls to optimize traffic traversing a WAN connection. For example, the diagram below shows a WANOPT deployment between a data center and remote office. In such a deployment, the SonicWALL gateway may be providing services such as attack prevention, VPN, routing and anti-spam.

WAN connections such as T1/E1 or xDSL typically have a round trip time of greater 25ms and less than 100ms. This latency causes some applications to perform less than expected or poorly. The typical remedy is to purchase a higher quality service or larger provision of bandwidth. WAN optimization can delay or postpone the expenditure and provide an increase in application performance response time.

● **Wire/Tap Mode** - Wire Mode is a deployment option where the SonicWALL appliance can be deployed as a "Bump in the Wire." It provides a least-intrusive way to deploy the appliance in a network. Wire Mode is very well suited for deploying behind a pre-existing Stateful Packet Inspection (SPI) Firewall.

Wire Mode is a simplified form of Layer 2 Bridge Mode. A Wire Mode interface does not take any IP address and it is typically configured as a bridge between a pair of interfaces. None of the packets received on a Wire Mode interface are destined to the firewall, but are only bridged to the other interface.

Wire Mode operates in any one these 4 different modes:

–**Bypass Mode** - Bypass Mode can be configured between a pair of interfaces. All traffic received is bridged to the paired interface. There is no SPI or Deep Packet Inspection (DPI) processing of traffic in this mode. There is no Application Visibility or Control in Bypass Mode.

–**Tap Mode** - Tap Mode can be configured between a pair of interfaces. All traffic received is bridged to the paired interface; in addition, the firewall does SPI and DPI processing of traffic. There is full Application Visibility, but no Application Control in Tap Mode.

–**Secure Mode** - Secure Mode can be configured between a pair of interfaces. All traffic received is fully processed by the firewall. There is full Application Visibility and Control in Secure Mode.

–**Sniffer Mode** - Sniffer Mode can be configured for a single interface. All traffic received is never sent out of the firewall, but the firewall performs full SPI and DPI processing. There is full Application Visibility, but no Application Control in Sniffer Mode. Typically, a mirror port is set up on the switch to mirror the network traffic to the firewall.

Wire Mode is supported on the following SonicWALL appliance models:

–NSA E8500

–NSA E7500

–NSA E6500

–NSA E5500

–NSA 5000

–NSA 4500

–NSA 3500

Key Features in SonicOS Enhanced 5.8

SonicOS Enhanced 5.8 and higher releases include the following key features:

● **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.

SonicWALL appliances running SonicOS 5.8.0.0 or higher and already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) will receive a complimentary license for the Real-Time Visualization Dashboard (App Visualization). Note that appliances running earlier versions of SonicOS and/or appliances not licensed for GAV/IPS/AS, Total Secure, or CGSS will receive a 30-day free trial

Appliances newly registered and upgraded to SonicOS 5.8.0.0 or higher will receive a 30-day free trial license of App Visualization by default.

Navigate to the Log > Flow Reporting page to manually Enable Flow Reporting and Visualization 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:

–Report to App Flow Collector

–Report to EXTERNAL Flow Collector

● **Application Intelligence + Control**

- This feature has two components for more network security:

–Identification: Identify applications and track user network behaviors in real-time.

–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.

SonicWALL appliances running SonicOS 5.8.0.0 or higher and already licensed for GAV/IPS/AS, Total Secure, or Comprehensive Gateway Security Suite (CGSS) will receive a complimentary license for Application Intelligence and Control (App Control). Note that appliances running earlier versions of SonicOS and/or appliances not licensed for GAV/IPS/AS, Total Secure, or CGSS will receive a 30-day free trial

Appliances newly registered and upgraded to SonicOS 5.8.0.0 or higher will receive a 30-day free trial license of App Control by default.

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** - 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.

SonicOS 5.8.0.0 supports Static Link Aggregation with the ability to aggregate up to 4 ports into a single link. 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 and IPFIX. The data exported through IPFIX 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.

● **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 Schedule** - SonicOS 5.8.0.0 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.

● **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** - SonicOS 5.8.0.0 provides SIP operational and scalability enhancements. 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.

Key Features in SonicOS Enhanced 5.7

SonicOS Enhanced 5.7 release include the following key features:

Please Note: SonicOS Enhanced 5.7 release is available for NSA 2400MX only.

● **Switching on the SonicWALL NSA 2400MX appliance** - The SonicWALL NSA 2400MX appliance is a Unified Threat Management (UTM) security appliance that integrates the WAN flexibility of a router with 24 built-in Ethernet switch ports. The functionality supports the following switching features:

> **–VLAN Trunking** – Provides the ability to trunk different VLANs between multiple switches.
>
> **–Rapid Spanning Tree Protocol** – Prevents loops from being formed when switches or bridges are interconnected via multiple paths and provides for network convergence after a topology change.
>
> **–Layer 2 Network Discovery** – Uses IEEE 802.1AB (LLDP) and Microsoft LLTD protocols and switch forwarding table to discover devices visible from a port.
>
> **–Link Aggregation** – Provides the ability to aggregate ports for increased performance and redundancy.

–**Port Mirroring** – Allows the administrator to assign mirror ports to mirror ingress, egress or bidirectional packets coming from a group of ports.

–**Layer 2 Quality of Service** – On a per port basis, allows configuration to trust Cost of Service (CoS) (802.1p) or trust DSCP marking and treat the frames appropriately.

–**Rate Control / Flow Control** – On a per port basis, the bandwidth of ingress frames can be tuned in four modes by limiting all/flooded unicast/multicast /broadcast frames. Rate limiting for egress frames can be enabled or disabled.

–**Port Security** – Provides the ability to bind a MAC address or multiple MAC addresses to a specific port interface.

● **Expansion Modules for the SonicWALL NSA 2400MX appliance** - The SonicWALL NSA 2400MX appliance supports the following expansion modules:

–**LAN Bypass Module** – The SonicWALL LAN Bypass Gigabit Ethernet Module provides a failsafe open-state switch for the NSA Series firewalls. It provides a modular slot that, if an unrecoverable firewall error occurs, allows network traffic to continue to flow, without firewall services. This is useful in cases where a network shutdown is unacceptable, such as in inline L2 Bridge deployments.

–**2-Port SFP and 4-Port Gigabit Ethernet Expansion Packs** – The SonicWALL expansion pack modules provide extra ports for your SonicWALL appliance.

Key Features in SonicOS Enhanced 5.6

SonicOS Enhanced 5.6 and higher releases include the following key features:

● **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 and non-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 Firewall, Packet Capture and Packet Mirror. DPI-SSL is initially available on NSA-3500 and above hardware platforms.

● **Dynamic DNS per Interface** - Provides the ability to assign a Dynamic DNS (DDNS) profile to a specific WAN interface. This allows administrators who are configuring multiple WAN load balancing to advertise a predictable IP address to the DDNS service.

● **Increased UTM Connection Support** - Provides the ability to increases the number of simultaneous connections on which SonicWALL security appliances can apply Unified Threat Management (UTM) services (Application Firewall, Anti-Spyware, Gateway Anti-Virus, and IPS engine). This feature is intended for high-end (E-Class) customers who have a need to support a large number of concurrent connections. (Note: There is a slight performance decrease when this option is enabled.)

● **FairNet for SonicPoint-N** - Provides the ability to create policies that equally distribute bandwidth for all wireless users connected to a SonicPoint-N.

● **MAC-IP Anti-Spoof Detection and Prevention** - Provides additional protection against MAC address and IP address based spoofing attacks (such as Man-in-the-Middle attacks) through configurable Layer 2 and Layer 3 admission control.

● **Packet Mirroring** - Provides the ability to capture copies of specified network packets from other ports. This is commonly used for network appliances that require monitoring of network traffic, such as an intrusion-detection system. Customers can now gather data from one of the other ports on a SonicWALL to look for threats and vulnerabilities and help aid with diagnostics and troubleshooting.

● **Route-based VPN with Dynamic Routing Support** - Extends support for advanced routing (either OSPF or RIP) to VPN networks. This can be used to simplify complex VPN deployments by enabling dynamic routing to determine the best path traffic should take over a VPN tunnel.

● **Signature Download through a Proxy Server** - Provides the ability for SonicWALL security appliances that operate in networks where they must access the Internet through a proxy server to download signatures. This feature also allows for registration of SonicWALL security appliances through a proxy server without compromising privacy.

● **Single Sign-on for Terminal Services and Citrix** - Provides support for transparent authentication of users running Terminal Services or Citrix. This transparent authentication enables Application Firewall and CFS policy enforcement in Terminal Services and Citrix environments.

● **SSL-VPN Enhancements** - SonicOS Enhanced 5.6.0.0 provides a number of SSL-VPN enhancements:

–**Bookmarks for SSH and RDP** - Provides support for users to create bookmarks on the SSL -VPN Virtual Office to access systems using SSH, RDP, VNC, and telnet services.

–**Granular User Controls** - Provides network administrators with the ability to configure different levels of policy access for NetExtender users based on user ID.

–**One-Time Password** - Provides additional security by requiring users to enter a randomly generated, single-use password in addition to the standard user name and password credentials.

–**Virtual Assist** - A provides a remote assistance tool to SonicWALL security appliance users. SonicWALL Virtual Assist is a thin client remote support tool provisioned via a Web browser that enables a technician to assume control of a customer's PC or laptop for the purpose of providing remote technical assistance. Note: The SonicOS Virtual Assist client is currently not supported on Windows 7 and Windows Vista platforms.

● **Virtual Access Points for SonicWALL TZ Wireless Platforms** - The SonicWALL TZ 100w, TZ 200w and TZ 210w platforms now support Virtual Access Points (VAPs). VAPs enable users to segment different wireless groups by creating logical segmentation on a single wireless radio.

● **Wireless Bridging for SonicWALL TZ Wireless Platform**s - The SonicWALL TZ 100w, TZ 200w and TZ 210w platforms now support Wireless Bridging, which provides the ability to extend a single wireless network across multiple SonicWALL wireless security appliances.

Key Features in SonicOS Enhanced 5.5

SonicOS Enhanced 5.5 and higher releases include the following key features:

● **Wireless Layer 2 Bridge Mode** - Security and ease of use continue to integrate with the addition of Layer 2 bridging between wired and wireless network segments. Wireless clients can now share the same subnet and DHCP pool as their wired counterparts.

● **Guest Services for Wired Clients** - SonicWALL User Guest Services has long provided network administrators with an easy solution for creating wireless guest passes and locked-down Internet-only network access. With SonicOS 5.5, this functionality can be extended to wired users on the LAN, DMZ, or public/semi-public zone of your choice.

Key Features in SonicOS Enhanced 5.4

SonicOS Enhanced 5.4 and higher releases include the following key features:

●**Anti-Spam** - SonicOS Enhanced 5.4 provides support for the anti-spam and anti-phishing capabilities that are available in SonicWALL Email Security.

Key Features in SonicOS Enhanced 5.3

SonicOS Enhanced 5.3 and higher releases include the following key features:

●**3G Support for Wireless WAN** - SonicOS Enhanced 5.3 expands support for WAN over 3G (Third Generation) cellular connections.

Key Features in SonicOS Enhanced 5.2

SonicOS Enhanced 5.2 and higher releases include the following key features:

● **Apple Bonjour Support** - SonicOS Enhanced 5.2 introduces support for Apple's Bonjour protocol (also known as Rendevous or zero-configuration networking). Bonjour enables automatic discovery of computers, devices, and services on IP networks without the need to enter IP addresses or configure DNS servers.

● **Apple iPhone Support** - SonicOS Enhanced 5.2 supports L2TP termination from the Apple iPhone.

● **Content Filtering Enhancements** - The following enhancements have been added to SonicWALL Content Filtering Service (CFS):

> **–CFS Policy per IP Address** - Appliances with SonicWALL CFS Premium can now assign specific CFS policies to ranges of IP address ranges. This provides the ability to segment CFS policies within a single zone.
>
> **–Fully Customizable Block Page** - The web page that is displayed when a user attempts to access a blocked site can now be fully customized. This enables organizations to brand the block page and display any organization-specific information.
>
> **–Safe Search Enforcement** - Safe Search Enforcement allows you to force Web search sites like Google and Yahoo that have content restriction options always to use their strictest settings.

● **New Firmware Auto-Update** - Firmware Auto-Update helps ensure that your SonicWALL security appliance has the latest firmware release. This feature automatically notifies the administrator when a new firmware release is available, and it can optionally download it automatically.

● **Outbound Inspection for Gateway Anti-Virus** - The SonicWALL Gateway Anti-Virus security service now provides outbound inspection for HTTP, FTP, and TCP traffic.

● **SonicPoint 802.11n Support** - SonicOS Enhanced 5.2 supports the new SonicPoint-N, which provides next-generation 802.11n wireless network connectivity.

● **SonicWALL SSL VPN NetExtender Support** - SonicOS Enhanced 5.2 provides support for SonicWALL's SSL VPN NetExtender, which was previously available only on the SonicWALL SSL VPN platforms. SonicWALL NetExtender is a transparent software application for users that enables remote users to securely connect to the remote network.

● **Support Services Page** - The new Support Services page displays a summary of the current status of support services for the SonicWALL security appliance. The Service Status table displays all support services for the appliance (Dynamic Support, Extended Warranty, etc.), their current status, and their expiration date.

Key Features in SonicOS Enhanced 5.1

SonicOS Enhanced 5.1 and higher releases include the following key features:

● **Strong SSL and TLS Encryption** - The internal SonicWALL Web server now 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 rollback vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards. **Tip** By default, Mozilla Firefox 2.0 and Microsoft Internet Explorer 7.0 enable SSL 3.0 and TLS, and disable SSL 2.0. SonicWALL recommends using these most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0 and TLS and disable SSL 2.0. In Internet Explorer, go to **Tools > Internet Options**, click on the **Advanced** tab, and scroll to the bottom of the **Settings** menu. In Firefox, go to **Tools > Options**, click on the **Advanced** tab, and then click on the **Encryption** tab.

● **Single Sign-On User Authentication** - Single Sign-On User Authentication provides privileged access to multiple network resources with a single workstation login. Single Sign-On uses the SonicWALL SSO Agent to identify user activity based on workstation IP addresses. Access to resources is based on policy for the group to which the user belongs.

● **Stateful High Availability** - Stateful High Availability provides improved failover performance. With Stateful High Availability, the primary and backup security appliances are continuously synchronized so that the backup can seamlessly assume all network responsibilities if the primary appliance fails, with no interruptions to existing network connections. Once the primary and backup appliances have been associated as a high availability pair on mysonicwall.com, you can enable this feature by selecting Enable Stateful Synchronization in the **High Availability > Advanced** page.

● **Application Firewall** - Application Firewall provides a way to create application-specific policies to regulate Web browsing, file transfer, email, and email attachments. Application Firewall enables application layer bandwidth management, and also allows you to create custom policies for any protocol. It gives you granular control over network traffic on the level of users, email users, and IP subnets.

● **HTTPS Filtering** - HTTPS Filtering allows administrators to control user access to Web sites when using the encrypted HTTPS protocol. HTTPS Filtering is based on the ratings of Web sites, such as Gambling, Online Banking, Online Brokerage and Trading, Shopping, and Hacking/Proxy Avoidance.

NoteHTTPS Filtering is IP-based, so IP addresses must be used rather than domain names in the Allowed or Forbidden lists. You can use the **nslookup** command in a DOS cmd window to convert a domain name to its IP address(es). There may be more than one IP address associated with a domain, and if so, all must be added to the Allowed or Forbidden list.

● **SSL Control** - SSL Control is a system that provides visibility into the handshake of Secure Socket Layer (SSL) sessions, and a method for configuring policies to control the establishment of SSL sessions.

● **Certificate Blocking** - The certificate blocking feature provides a way to specify which HTTPS certificates to block. This feature is closely integrated with SSL Control.

● **Inbound NAT Load Balancing with Server Monitoring** - Inbound NAT Load Balancing with Server Monitoring detects when a server is unavailable and stops forwarding requests to it. Inbound NAT Load Balancing spreads the load across two or more servers. When Stateful High Availability (Stateful High Availability) is configured, during a failover, SonicOS forwards all requests to the alternate server(s) until it detects that the offline server is back online. Inbound NAT Load Balancing also works with SonicWALL SSL VPN appliances.

● **Top Global Malware Report Page** - The Top Global Malware page in the user interface displays a summary of threats stopped by the SonicWALL security appliance. The Security shows two types of reports:

> –A Global Report that displays a summary of threat data received from all SonicWALL security appliances worldwide.
>
> –An Individual Appliance Report that displays a summary of attacks detected by the local SonicWALL security appliance.

● **Registration & License Wizard** - As part of the Top Global Malware page, SonicOS Enhanced provides a License Wizard for both firewall registration and the purchase of security service licenses. The available security services are the same as those that enable Global Reports by providing threat data from SonicWALL devices around the world.

● **Multiple SSH Support** - SonicOS Enhanced provides support for multiple concurrent SSH sessions on the SonicWALL security appliance. When connected over SSH, you can run command line interface (CLI) commands to monitor and manage the device. The number of concurrent SSH sessions is determined by device capacity. Note that only one session at a time can configure the SonicWALL, whether the session is on the GUI or the CLI (SSH or serial console). For instance, if a CLI session goes to the config level, it will ask you if you want to preempt an administrator who is at config level in the GUI or an SSH session.

● **Multiple and Read-only Administrator Login** - Multiple Administrator Login provides a way for multiple users to be given administration rights, either full or read-only, for the SonicOS security appliance. Additionally, SonicOS Enhanced allows multiple users to concurrently manage the appliance, but only one user at a time can be in config mode with the ability to change configuration settings. This feature applies to both the graphical user interface (GUI) and the command line interface (CLI).

● **IP-Based Connection Limit** - SonicOS Enhanced provides a way to limit the number of connections on a per-source or per-destination IP address basis. This feature protects against worms on the LAN side that initiate large numbers of connections in denial of service attacks.

● **IKEv2 Secondary Gateway Support** - IKEv2 Secondary Gateway Support provides a way to configure a secondary VPN gateway to act as an alternative tunnel end-point if the primary gateway becomes unreachable. While using the secondary gateway, SonicOS can periodically check for availability of the primary gateway and revert to it, if configured to do so. Configuration for the secondary VPN gateway is available under **VPN > Settings > Add Policy** in the management interface.

● **IKEv2 Dynamic Client Support** - IKEv2 Dynamic Client Support provides a way to configure the Internet Key Exchange (IKE) attributes rather than using the default settings. Previously, only the default settings were supported: Diffie-Hellman (DH) Group 2, the 3DES encryption algorithm, and the SHA1 authentication method. SonicOS now allows the following IKE Proposal settings:

> –DH Group: 1, 2, or 5
>
> –Encryption: DES, 3DES, AES-128, AES-192, AES-256

–Authentication: MD5, SHA1

These settings are available by pressing the Configure button in the **VPN > Advanced** screen of the management interface. However, if a VPN Policy with IKEv2 exchange mode and a 0.0.0.0 IPsec gateway is defined, you cannot configure these IKE Proposal settings on an individual policy basis.

NoteThe VPN policy on the remote gateway must also be configured with the same settings.

● **Wireless IDS Rogue Detection** - SonicOS Enhanced supports wireless intrusion detection on SonicPoint devices. Wireless IDS Rogue Detection allows you to configure a set of authorized access points, defined by address object groups. If contact is attempted from an unauthorized access point, SonicOS generates an alert.

● **RF Management** - Radio Frequency Management on SonicPoint devices provides detection of eleven types of wireless threats:

–Long duration attack

–Management frame flood

–Null probe request

–Broadcasting de-authentication

–Valid station with invalid SSID

–Ad-Hoc station

–Unassociated station

–Wellenreiter attack

–NetStumbler attack

–EAPOL packet flood

–Weak WEP IV

● **SMTP Authentication** - SonicOS Enhanced supports RFC 2554, which defines an SMTP service extension that allows the SMTP client to indicate an authentication method to the server, perform an authentication protocol exchange, and optionally negotiate a security layer for subsequent protocol interactions. This feature helps prevent viruses that attack the SMTP server on port 25.

● **Generic DHCP Option Support** - SonicOS Enhanced supports generic DHCP configuration, which allows vendor-specific DHCP options in DHCP server leases.

● **DHCP Server Lease Cross-Reboot Persistence** - DHCP Server Lease Cross-Reboot Persistence provides the ability to record and return to DHCP server lease bindings across power cycles. The SonicWALL security appliance does not have to depend on dynamic network responses to regain its IP address after a reboot or power cycle.

● **Custom IP Type Service Objects** - SonicOS Enhanced supports Custom IP Type Service Objects, allowing administrators to augment the predefined set of Service Objects.

● **Dynamic Address Objects** - SonicOS Enhanced supports two changes to Address Objects:

–MAC - SonicOS Enhanced will resolve MAC AOs to an IP address by referring to the ARP cache on the SonicWALL.

–FQDN - Fully Qualified Domain Names (FQDN), such as 'www.sonicwall.com', will be resolved to their IP address (or IP addresses) using the DNS server configured on the SonicWALL. Wildcard entries are supported through the gleaning of responses to queries sent to the sanctioned DNS servers.

● **Virtual Access Points** - A "Virtual Access Point" (VAP) is a multiplexed instantiation of a single physical Access Point (AP) so that it presents itself as multiple discrete Access Points. To wireless LAN clients, each Virtual AP appears to be an independent physical AP, when there is actually only a single physical AP. Before Virtual AP feature support, wireless networks were relegated to a One-to-One relationship between physical Access Points and wireless network security characteristics, such as authentication and encryption. For example, an Access Point providing WPA-PSK security could not simultaneously offer Open or WPA-EAP connectivity to clients. If Open or WPA-EAP were required, they would need to have been provided by a separate, distinctly configured APs. This forced WLAN network administrators to find a solution to scale their existing wireless LAN infrastructure to provide differentiated levels of service. With the Virtual APs (VAP) feature, multiple VAPs can exist within a single physical AP in compliance with the IEEE 802.11 standard for the media access control (MAC) protocol layer that includes a unique Basic Service Set Identifier (BSSID) and Service Set Identified (SSID). This allows segmenting wireless network services within a single radio frequency footprint of a single physical access point device.

VAPs allow the network administrator to control wireless user access and security settings by setting up multiple custom configurations on a single physical interface. Each of these custom configurations acts as a separate (virtual) access point, and can be grouped and enforced on single or multiple physical SonicPoint access points simultaneously. You can configure up to eight VAPs per SonicPoint access point.

● **Layer 2 Bridge Mode** - SonicOS Enhanced supports Layer 2 (L2) Bridge Mode, a new method of unobtrusively integrating a SonicWALL security appliance into any Ethernet network. L2 Bridge Mode is similar to the SonicOS Enhanced Transparent Mode in that it enables a SonicWALL security appliance to share a common subnet across two interfaces, and to perform stateful and deep-packet inspection on all traversing IP traffic, but it is functionally more versatile.

L2 Bridge Mode employs a secure learning bridge architecture, enabling it to pass and inspect traffic types that cannot be handled by many other methods of transparent security appliance integration. Using L2 Bridge Mode, a SonicWALL security appliance can be non-disruptively added to any Ethernet network to provide in-line deep-packet inspection for all traversing IPv4 TCP and UDP traffic. Unlike other transparent solutions, L2 Bridge Mode can pass all traffic types, including IEEE 802.1Q VLANs, Spanning Tree Protocol, multicast, broadcast, and IPv6, ensuring that all network communications will continue uninterrupted.

L2 Bridge Mode provides an ideal solution for networks that already have an existing firewall, and do not have immediate plans to replace their existing firewall but wish to add the security of SonicWALL Unified Threat Management (UTM) deep-packet inspection, such as Intrusion Prevention Services, Gateway Anti-Virus, and Gateway Anti Spyware. The following feature enhancements are included in SonicOS Enhanced 5.0 and higher:

● **Enhanced Packet Capture** - Enhanced Packet Capture contains improvements in both functionality and flexibility, including the following:

–Capture control mechanism with improved granularity for custom filtering

–Display filter settings independent from capture filter settings

–Packet status indicating dropped, forwarded, generated, or consumed

–Three-window output in the user interface that provides the packet list, decoded output of selected packet, and hexadecimal dump of selected packet

–Export capabilities that include text, HTML, hex dump, and CAP file format

–Automatic buffer export to FTP server when full

–Bidirectional packet capture based on IP address and port

–Configurable wrap-around of capture buffer when full

● **User Authentication** - There are a number of enhancements to user authentication, including optional case-sensitive user names, optional enforcement of unique login names, support for MSCHAP version 2, and support for VPN and L2TP clients changing expired passwords (when that is supported by the back-end authentication server and protocols used). Note that for this purpose there is a new setting on the **VPN > Advanced** page to cause RADIUS to be used in MSCHAP mode when authenticating VPN client users.

● **IP Helper Scalability** - The IP Helper architecture is enhanced to support large networks. Improvements include changes to DHCP relay and Net-BIOS functionality. DHCP relay over VPN is now fully integrated.

● **Diagnostics Page Tool Tips** - Self-documenting mouseover descriptions are provided for diagnostic controls in the graphical user interface.

● **BWM Rate Limiting** - The Bandwidth Management feature is enhanced to provide rate limiting functionality. You can now create traffic policies that specify maximum rates for Layer 2, 3, or 4 network traffic. This enables bandwidth management in cases where the primary WAN link fails over to a secondary connection that cannot handle as much traffic.

● **DHCP Client Reboot Behavior Control** - In SonicOS Enhanced 5.0 and higher, you can configure the WAN DHCP client to perform a DHCP RENEW or a DHCP DISCOVERY query when attempting to obtain a lease. The previous behavior was to always perform a RENEW, which caused lease failures on some networks, particularly certain cable modem service providers. The new behavior it to perform a DISCOVERY, but it is configurable. A checkbox has been added to the **Network > Interfaces > WAN >DHCP Client** page:

–Enabled: when the appliance reboots, the DHCP client performs a DHCP RENEW query.

–Disabled: (Default) when the appliance reboots, the DHCP client performs a DHCP DISCOVERY query.

● **Dynamic Route Metric Recalculation Based on Interface Availability** - To better support redundant or multiple path Advanced Routing configurations, when a default-route's interface is unavailable (due to no-link or negative WAN LB probe response), that default route's metric will be changed to 255, and the route will be instantly disabled. When a default-route's interface is again determined to be available, its metric will be changed back to 20, and the route will be non-disruptively enabled.

KBID	8958
Date Modified	7/12/2011
Date Created	7/5/2011