Release Notes

SonicOS

SonicOS 5.6.0.12 Release Notes

Contents

SonicWALL Analysis of PenTest Vulnerability Reports

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

Analysis: SonicOS Management SessionID Brute Force Vulnerability

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

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

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

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

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

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

Analysis: Preview of Custom Web Page Vulnerability

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

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

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

Analysis: MAC Address Spoofing on Wireless Networks

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

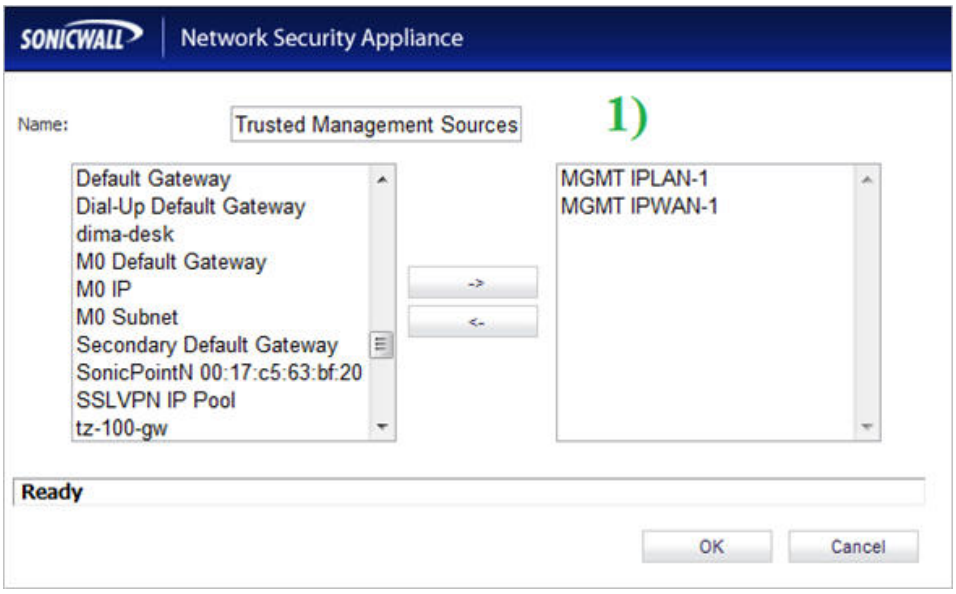
SonicOS Updates

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

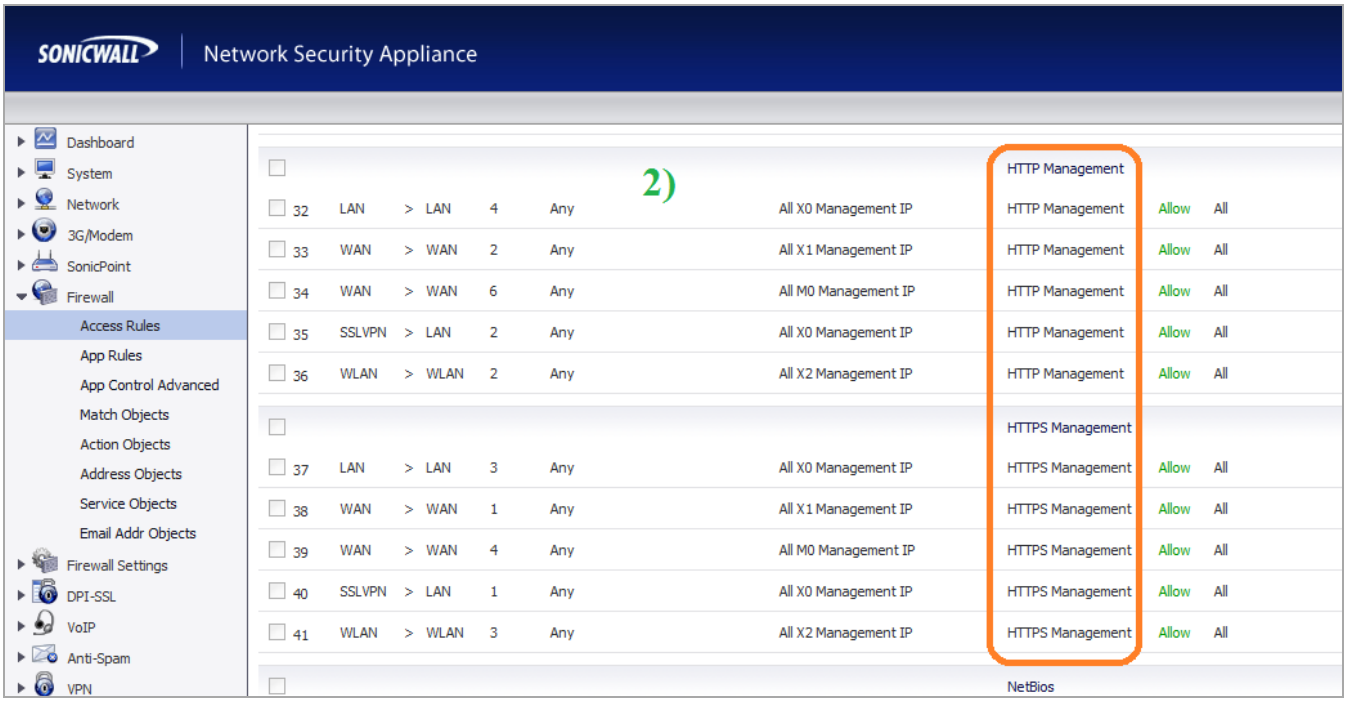
Recommended Best Practice – Limiting SonicOS management access to "Trusted Management Sources"

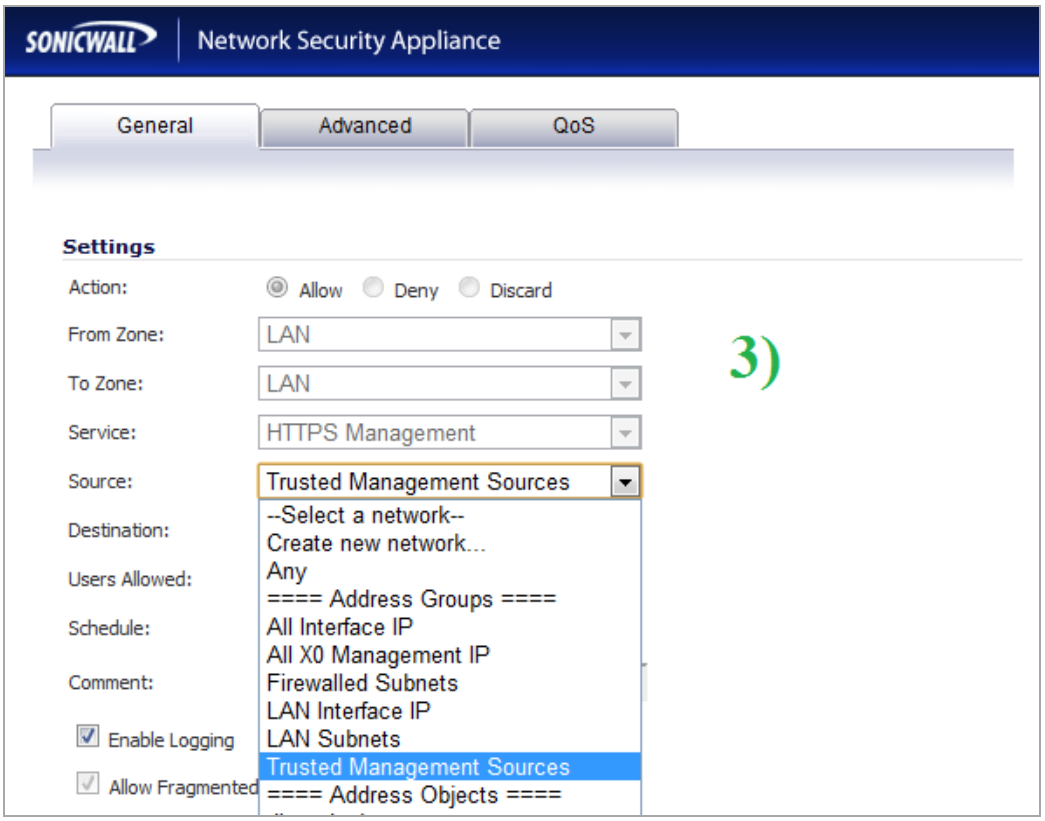
To enhance the security of administrative sessions, SonicWALL advises administrators to adhere to the best practice of limiting SonicOS management access to "Trusted Management Sources" by modifying the existing SonicOS Web Management rules (HTTPS/HTTP Management) to allow management access only from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

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



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





Platform Compatibility and Enhancements

The SonicOS 5.6.0.12 release is supported on the following SonicWALL security appliances:

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

This release supports the following Web browsers:

- Microsoft Internet Explorer 7.0 and higher
- Mozilla Firefox 3.0 and higher
- Chrome 4.0 and higher

Strong SSL and TLS Encryption Required in Your Browser

The internal SonicWALL Web server only supports SSL version 3.0 and TLS with strong ciphers (128 bits or greater) when negotiating HTTPS management sessions. SSL implementations prior to version 3.0 and weak ciphers (symmetric ciphers less than 128 bits) are not supported. This heightened level of HTTPS security protects against potential SSLv2 roll-back vulnerabilities and ensures compliance with the Payment Card Industry (PCI) and other security and risk-management standards.

TIP: By default, Mozilla Firefox 3.0, Microsoft Internet Explorer 8.0, and Google Chrome enable SSL 3.0 and TLS, and disable SSL 2.0. SonicWALL recommends using the most recent Web browser releases. If you are using a previous release of these browsers, you should enable SSL 3.0 and TLS and disable SSL 2.0.

Key Features

The following key features are supported in all versions of SonicOS 5.6:

- **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 Firewall, Packet Capture and Packet Mirror. DPI-SSL is initially available on SonicWALL NSA models 3500 and above.

- **3G and Modem Support** – SonicOS 5.6 supports 3G and Modem configurations for WAN Load Balancing (WLB). 3G and Modem support is available on all TZ and NSA models except the SonicWALL NSA 2400.

- **Command Line Interface Enhancements** – Provides increased support through the command line interface to configure and modify Network Address Translation (NAT) Policies, Access Rules, Service Objects, and Service Groups.

- **Diagnostic Improvements** – Includes a diagnostic tool which automatically checks the network connectivity and service availability of several pre-defined functional areas of SonicOS. The tool also returns results and attempts to describe causes, if any exceptions are detected.

- **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 WAN Load Balancing to advertise a predictable IP address to the DDNS service.

- **Increased UTM Connection Support** – Provides the ability to increase 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 Intrusion Prevention Service). This feature is intended for high-end (E-Class) customers who 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 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 simplifies complex VPN deployments by enabling dynamic routing to determine the best path that traffic should take over a VPN tunnel.

- **Signature Download through a Proxy Server –** Provides the ability for SonicWALL security appliances to download signatures even when they access the Internet through a proxy server. 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 logged in from a Terminal Services or Citrix server. This transparent authentication enables Application Firewall and CFS policy enforcement in Terminal Services and Citrix environments.

- **SSL VPN Enhancements** – SonicOS 5.6 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 –** Allows network administrators 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.
    - **Separate Port and Certificate Control –** Provides separate port access for SSL VPN and HTTPS management certificate control, allowing administrators to close HTTPS management while leaving SSL VPN open.
    - **Virtual Assist –** 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. It enables a technician to assume control of a customer's PC or laptop for the purpose of providing remote technical assistance.

- **Unbounded Multiple WAN Support –** Provides the ability to enable any number of WAN Ethernet interfaces for WAN Load Balancing and Failover on SonicWALL TZ and NSA appliances.

- **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. Note that VAPs are not supported on SonicPoint or SonicPoint-N devices connected to TZ models.

- **VPN Policy Bound to VLAN Interface** – Allows users to bind a VPN policy to a VLAN interface when configuring a site-to-site VPN.

- **WebCFS Server Failover** – Provides the ability to enable WebCFS server failover, allowing a SonicWALL security appliance to contact another server for URL rating information if the local server is unavailable. This ensures performance continuity for Web navigation and Web content filtering functionality.

- **Wireless Bridging for SonicWALL TZ Wireless Platforms –** 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.

Known Issues

This section contains a list of known issues in the SonicOS 5.6.0.12 release.

Bandwidth Management

Symptom	Condition / Workaround	Issue
Fragmented, non-VPN outbound packets are not accounted for in Bandwidth Management (BWM).	Occurs when the user enables fragmented, non-VPN outbound packets after enabling BWM. Fragmented outbound packets are not being accounted for by BWM.	93951
Bandwidth Management uses the wrong active WAN and BWM settings after WAN Load Balancing (WLB) is disabled.	Occurs when WLB and BWM are enabled for two interfaces (X3, X5) with BWM ingress and egress set to 1 Gbps. BWM is disabled on X1 with the default values unchanged. While WLB is enabled, the active WAN interface is X3. After disabling WLB, the BWM module uses X1 as the default WAN, while the WLB module still uses X3.	93919

CFS

Symptom	Condition / Workaround	Issue
A new custom schedule used by a CFS policy can be deleted.	Occurs after creating and applying a new custom schedule to the CFS policy. A user is then able to delete the new custom schedule.	94007

DPI-SSL

Symptom	Condition / Workaround	Issue
Throughput drops and the firewall cannot be managed with the SonicOS management interface when Client DPI-SSL is enabled while traffic is running through the firewall.	Occurs when Client DPI-SSL is enabled while multi-protocol traffic (HTTP, HTTPS, SMTP, Ping, SSL VPN tunnels, site to site VPN tunnels) is running through the firewall. The management interface becomes inaccessible or very slow to load and throughput drops by a factor of more than 20. **Workaround**: Disable Client DPI-SSL.	93774

High Availability

Symptom	Condition / Workaround	Issue
The wrong interface can be unassigned when removing interfaces from a Load Balancing group.	Occurs when X1 and X3 are configured as WAN interfaces and assigned to the default LB group with X3 having a higher rank. After setting X3 back to unassigned, it remains in the LB group and X1 is removed from the LB group.	94598

Networking

Symptom	Condition / Workaround	Issue
The WAN interface X1 cannot be unassigned from the Interface Ordering Group.	Occurs when assigning the X1 interface from Group Members to the Interface Ordering Group. After performing this task, attempting to un-assign the X1 interface from the Interface Ordering Group does not work.	101101
Modifying the interface IP address may result in issues for the corresponding static DHCP scope entry.	Occurs after changing a dynamic DHCP interface to static, and then back again to dynamic in a different subnet. For the X0 interface, the static DHCP IP range is removed. For another LAN interface, the static DHCP IP range remains unchanged.	94053

VPN

Symptom	Condition / Workaround	Issue
The IKE Security Association delete request is blocked by the SonicWALL appliance and the VPN Tunnel is still connected.	Occurs when a remote user sends an IKE SA delete request to the SonicWALL appliance. This request should be accepted by the appliance and the VPN Tunnel should be deleted.	100785

Wireless

Symptom	Condition / Workaround	Issue
A performance drop is seen for PC-card 3G interface throughput on the NSA 240.	Occurs when using a wireless 3G PC card on a SonicWALL NSA 240 to download an FTP file or to load Web pages in a browser.	95135

Resolved Issues in SonicOS 5.6.0.12

The following issue is resolved in the SonicOS 5.6.0.12 release.

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

Resolved Issues in SonicOS 5.6.0.11

The following issues are resolved in the SonicOS 5.6.0.11 release:

Content Filtering Service

Symptom	Condition / Workaround	Issue
The error message: “Reason for Restriction: Connection Problem on Firewall” is displayed on the CFS Block page.	Occurs when CFS is set to block the connection and the CFS servers are unavailable for 5 seconds. The description in the error message is incorrect because there is not a connection problem to the firewall.	77568

Firmware

Symptom	Condition / Workaround	Issue
An access rule is not applied to traffic immediately after the firewall is restarted.	Occurs for an access rule that denies traffic from the LAN IP address to a WAN FQDN object when DNS resolution fails for the WAN FQDN object. After DNS resolution occurs, the access rule is applied correctly.	97001
Automatically added VPN Access Rules are not deleted when the related VPN policies are deleted.	Occurs when using a site to site VPN configuration and the auto-added access rules are edited, then the VPN policies are deleted. The access rules cannot be removed.	96233

Graphical User Interface

Symptom	Condition / Workaround	Issue
HTTPS management of SonicOS fails from some public IP addresses, but works fine from others.	Occurs when attempting to connect to the management interface of a remote appliance using HTTPS from behind a SonicWALL NSA 5500.	92438
The user cannot manage remote appliances and the SonicOS login page does not display.	Occurs when attempting to manage a remote appliance from a work appliance using HTTPS. If the firewall is rebooted, the system functions properly for about 24 hours before the error occurs again.	87053

Global VPN Client

Symptom	Condition / Workaround	Issue
The GUI becomes unresponsive and displays the message: “Acquiring IP”. A DHCP address is never obtained.	Occurs when attempting to connect to the appliance with GVC, while the appliance is configured to use layer 2 bridge mode with X1 and any other interface except X0.	94865

High Availability

Symptom	Condition / Workaround	Issue
The secondary WAN is set to “admin down” after a reboot and the error message: “target unavailable” is displayed.	Occurs when upgrading firmware and rebooting the appliance. If the failover settings are reconfigured after the reboot, then the appliance functions properly.	85266

Log

Symptom	Condition / Workaround	Issue
The syslog traffic is being sent through the WAN instead of the VPN Tunnel.	Occurs when sending syslog data through a site-to-site VPN Tunnel with a manually created NAT Policy.	75898

Modem

Symptom	Condition / Workaround	Issue
The Huawei E182 modem is not recognized by the appliance.	Occurs when rebooting the appliance with the Huawei E182 modem connected.	97751

Networking

Symptom	Condition / Workaround	Issue
The traffic being passed from a group within an address range object is incorrectly blocked by the appliance.	Occurs when changing the IP addresses so that traffic is not blocked by Access Rule 22. Access Rule 22 should only block traffic within the group it is applied to. If the IP addresses are changed so they are no longer part of that group, Access Rule 22 should not block traffic being passed from these addresses.	99227
Multiple interfaces stop passing traffic at the same time and the firewall is not accessible, then the firewall resumes normal functions after a few minutes. No failover occurs if High Availability is configured.	Occurs on NSA 2400 appliances when the interfaces are connected to different switches.	99199 / 99176 / 97864
The customer is unable to access new websites with the **connection limit based on source IP** enabled.	Occurs when the **connection limit based on source IP** option is set to a number larger than the current actual connections, but previously the limit was exceeded and this number is not being reset. Any host previously blocked due to feature will remain blocked even if connection cache is emptied.	96591
The error message: 'L2TP Server not responding' is displayed on the client user interface.	Occurs when connecting new iPad L2TP Clients to an NSA appliance. After several iPad Clients are connected, any additional new clients receive an error message and are not connected.	94806
Traffic with Multicast MAC and Unicast IP addresses that are routed through a Microsoft Internet Security and Acceleration (ISA) Server are blocked by the appliance.	Occurs when Microsoft Internet Security and Acceleration Server is configured as the default gateway and placed inline with a Sonicwall appliance.	91867
The auto-added access rules for VPN tunnel interface are not functioning properly.	Occurs after changing the auto-added access rules and attempting to communicate with other appliances through the firewall. The firewall will now block any traffic even if the access rules are set back to auto-adding, until the firewall is rebooted.	87602
Outbound traffic is sent out through interface X1 instead of X3.	Occurs when traffic is sent through the Network Address Translation (NAT) to a web server on a routed subnet. The outbound traffic has the correct IP address but is sent out on the wrong interface.	85125

SSL-VPN

Symptom	Condition / Workaround	Issue
The customer is redirected to use a WAN IP address instead of a domain name address in when using SSL-VPN to login.	Occurs when using the SSL-VPN NetExtender Client and logging into the appliance. After confirming the login by selecting **Click Here for SSL Login** the user is redirected to use a WAN IP address.	88613

Users

Symptom	Condition / Workaround	Issue
Performing a Windows Update causes the user to be redirected to the login page for authentication.	Occurs when running a Windows Update with the access rules set to allow HTTP URLs to bypass authentication. After the access rules are created, the user should be able to run a Windows Update without being authenticated by the appliance.	91282

VPN

Symptom	Condition / Workaround	Issue
The maximum number of concurrent L2TP connections cannot be attained. L2TP connectivity interruptions and L2TP connections can cause the appliance to become unstable.	Occurs when attempting to connect more than approximately 25% of the supported maximum concurrent L2TP clients to a single appliance.	95048

Wireless

Symptom	Condition / Workaround	Issue
Wireless users experience delayed response times.	Occurs after enabling RF Monitoring on a SonicPoint-N appliance.	90534

Resolved Issues in SonicOS 5.6.0.10

This section contains a list of issues resolved in the SonicOS 5.6.0.10 release.

Networking

Symptom	Condition / Workaround	Issue
Deleting a VLAN sub-interface can cause the system to reboot under certain circumstances in SonicOS 5.6.0.9-49o.	Occurs when an interface has a NAT policy attached to it which consists of multi-level nested address object groups.	96539
The active unit of a Stateful High Availability pair can fail with a memory error during stateful synchronization shortly after the firewall becomes active.	Occurs when DHCP Persistance is not enabled, resulting in a low memory allocation for the operating system tDHCP task.	90722

System

Symptom	Condition / Workaround	Issue
The appliance reboots with the error message “Reboot due to task suspension …Task Trace tDhcpRcv.”	Occurs in certain situations when the SonicOS DHCP server processes the DISCOVER message from the clients.	93661

Resolved Issues in SonicOS 5.6.0.9

This section contains a list of issues resolved in the SonicOS 5.6.0.9 release.

CFS

Symptom	Condition / Workaround	Issue
CFS configuration and policies cannot be modified once Client DPI-SSL license expires.	Occurs after enabling IP-based HTTPS filtering alongside Client DPI-SSL, and firmware is upgraded to version 5.6.0.3-40o or later. Once DPI-SSL has expired, CFS configuration and policies can no longer be modified.	93706

High Availability

Symptom	Condition / Workaround	Issue
Directly connected networks are not broadcasting their location in the OSFP environment after a HA failover event.	Occurs in a HA failover to a redundant unit. Remote networks and static routes are advertised while directly connected networks are not acknowledged in an OSPF environment.	93098
Exchanging members in a default WAN Load Balancing group is not allowed and errors are issued.	Occurs when a user attempts to reconfigure and exchange interfaces on a default WLB group consisting of interface X1 as a member, and interface X2 as a final backup.	86088

Networking

Symptom	Condition / Workaround	Issue
Network monitor probing for inbound NAT load balancing only works with destination objects of type Range. Cannot configure probing for target objects containing Host objects. When upgrading, NAT policies with Host objects in the probing destination are disabled.	Occurs when trying to add a NAT policy that has probing configured, when the NAT Translated Destination is set to an address group containing an object of type Host. Also occurs when upgrading from a previous firmware version on an appliance that has such a NAT policy.	91304
Active or Passive FTP do not work as expected with a custom control port instead of the default port, 21.	Occurs when either Active or Passive FTP is configured with a custom control port and the default LAN to WAN access rule is disabled. For Passive FTP, also occurs when the default LAN to WAN access rule is enabled and a custom control port is configured.	89577
Static routes and connected networks with “non-classful” prefix lengths are in specific cases not redistributed by OSPF.	Occurs when OSPF is enabled for networks that have a prefix longer—more restrictive network mask—than other connected networks, and the other networks do not use /8, /16, /24, or /32 subnets. In this scenario, when the connected networks are redistributed, those which do not have /8, /16, /24, or /32 prefixes (subnet mask length) may not be advertised by OSPF.	89382

Symptom	Condition / Workaround	Issue
Packets can be dropped when WAN to LAN inbound rules and NATs are created to allow services on additional WAN public IPs.	Occurs when the WAN interface is L2-bridged with another interface, and port-forwarding to a NAT-enabled network does not work from WAN to LAN when any additional public IP addresses are used from the WAN subnet.	89307
The automatically added NAT policy for a Web proxy disappears after rebooting the appliance.	Occurs when the Web proxy is configured using a FQDN.	84927

Upgrading Firmware or Services

Symptom	Condition / Workaround	Issue
"Not enough memory to upload image" error causes firmware upgrade to fail on SonicWALL TZ 210/200/100 series and NSA 240 models.	Occurs when trying to upgrade firmware from any previous version of SonicOS 5.x.x.x to 5.6.0.9-46o on any of these TZ series and NSA 240 models. **Workaround**: Restart the SonicWALL immediately prior to upgrade.	93382
After importing appliance settings from a PRO 3060 to an NSA E6500, VPN tunnels do not pass traffic after the upgrade.	Occurs when automatically added VPN rules are added in the firewall rules table during settings import, but the inbound rules are not linked to the VPN policy due to look up failure. The lookup fails due to a service object mismatch for inbound automatic rules that were modified to allow only specific services. **Workaround**: Toggle the "Suppress automatic Access Rules creation for VPN Policy" for each VPN policy.	89935
A firewall running a version of SonicOS firmware that supports Comprehensive Anti-Spam Service, version 1, reboots periodically when a different CASS version is enabled.	Occurs when the CASS version 2 Junk Store with enhanced messaging is deployed on the firewall.	87563

Users and Clients

Symptom	Condition / Workaround	Issue
The appliance log shows errors reported by the Single Sign-On Agent with the wrong user IP address or 0.0.0.0 in the destination IP address field, which should be the IP address of the user.	Occurs when the log entry records the first user IP address from the list of addresses sent in a multi-user polling request. The address is sometimes 0.0.0.0 if the appliance has received a reply for it and has zeroed it.	89727
Global VPN Client (GVC) with DHCP experiences connectivity issues to WAN GroupVPN.	Occurs when an IP address fails to renew after DHCP request is sent from the client to the re-established GVC connection. Connectivity issues occur with TZ, NSA 240, and NSA 2400 devices.	89344
A connected Global VPN Client user is not visible on the active user session page.	Occurs when an IP address is manually configured for the Virtual NIC.	88870
The appliance may restart if certain static routes are configured and Terminal Services Agents are used.	Occurs when one or more LAN-side routes are using a group address object as their destination. Workaround: Configure these routes individually, each with a single address object as the destination.	87697

VPN

Symptom	Condition / Workaround	Issue
In site-to-site VPN, the wrong proposed networks from the initiator are logged. The log entry includes a correct network proposed as a remote by the initiator (which matches the responder's local network objects), not the wrong local network proposed by the initiator (which does not match the responder's remote network objects).	Occurs in site-to-site VPN, when the initiator is erroneously proposing the wrong local network objects in its VPN Policy for a peer gateway device (which do not match the responder's remote network objects).	93806
Static routes are removed from the routing tables after the unit reboots.	Occurs when static routes are created that utilize VPN tunnel interfaces. Routes operate correctly but disappear from the routing tables after the unit reboots.	91910
Idle Dead Peer Detection does not work with IKEv2 VPN policies. The remote firewall does not automatically renegotiate VPN policies after the initiator firewall is restarted.	Occurs when all hosts on the local initiator side of the VPN policy stop sending pings or communicating with a remote, responder host. Idle Dead Peer Detection is enabled only on the remote initiator side. Regular Dead Peer Detection is enabled on both sides, and both sides are configured with split tunnel IKEv2 VPN policies (LAN subnet to LAN subnet).	91875
A SonicWALL NSA has IKEv2 VPN stability issues in which VPN security associations start dropping randomly after a period of time, "IKEv2 Out of memory" events appear in the logs and the firewall exhibits unusual rebooting issues.	Occurs when the firewall has been up for a number of days and is getting more than 50 IKE requests per second from some of the sites, and thousands of incomplete IKE security associations accumulate.	88548
On a High Availability pair, DHCP over VPN tables are not synchronized if a failover occurs during lease renewal.	Occurs when reassigning an IP address to the client after the lease period expires. If a failover occurs while reassigning the IP, the idle Primary unit will not have any entries in the DHCP over VPN table.	88177
With IKEv2, a wrong network is proposed in the IPSec re-key, and the responder sends a "Traffic Selectors Unacceptable" message to the initiator.	Occurs when a continuous ping is running from the initiator to the responder in an IKEv2 tunnel between two NSA firewalls. When the initiator starts the IPSec re-key, it proposes a wrong network. The responder's log shows that the proposed network is 0.0.0.0-0.0.0.0. This wrong proposal lasts for a short period of time and then the correct re-key proposal occurs and the IKEv2 re-key succeeds, and traffic never fails on the IKEv2 VPN.	88005

Wireless

Symptom	Condition / Workaround	Issue
Verizon and Sprint 3G devices become non-functional after a reset.	Occurs when using the USB reset function to reset the 3G device. Specifically, from diag.html, click on the "Restart Dial-up Devices" button.	94546
Users cannot browse on the Internet after the second failover to a 3G Wireless WAN connection.	Occurs when a second failover from the WAN to a USB 3G WWAN connection takes place, causing the maximum transmission unit (MTU) size to change to a small number of bytes, less than 200. Ping still works, but LAN users cannot browse the Internet through the 3G WWAN connection.	91339
External authentication page fails to redirect after a reboot when using a FQDN.	Occurs after a device reboot when the External Authentication Server group shows the correct IP, but displays the zone assignment as WLAN or LAN.	90574
Certain models of the 3G USB Huawei modem are not detected when connected to a SonicWALL appliance, although included in the supported list.	Occurs when connecting the 3G USB Modem Huawei 176 G to a SonicWALL appliance using the 5.6.0.0 firmware.	88023
The Pass Networks option for Wireless Guest Services allows only HTTP/HTTPS traffic to pass through the WLAN zone. ICMP, FTP, or other traffic is not allowed.	Occurs when attempting to allow users to access network resources from the wireless zone without logging in to guest services.	86539

Upgrading SonicOS Image Procedures

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

Obtaining the Latest SonicOS Image Version

To obtain a new SonicOS firmware image file for your SonicWALL security appliance:

1. Connect to your mysonicwall.com account at http://www.mysonicwall.com.
2. Copy the new SonicOS image file to a directory on your management station.

You can update the SonicOS image on a SonicWALL security appliance remotely if the LAN interface or the WAN interface is configured for management access.

Saving a Backup Copy of Your Configuration Preferences

Before beginning the update process, make a system backup of your SonicWALL security appliance configuration settings. The backup feature saves a copy of your current configuration settings on your SonicWALL security appliance, protecting all your existing settings in the event that it becomes necessary to return to a previous configuration state.

In addition to using the backup feature to save your current configuration settings to the SonicWALL security appliance, you can export the configuration preferences file to a directory on your local management station. This file serves as an external backup of the configuration preferences, and can be imported back into the SonicWALL security appliance.

Perform the following steps to save a backup of your configuration settings and export them to a file on your local management station:

1. On the System > Settings page, click **Create Backup**. Your configuration preferences are saved. The System Backup entry is displayed in the Firmware Management table.
2. To export your settings to a local file, click **Export Settings**. A popup window displays the name of the saved file.

Upgrading a SonicOS Image with Current Preferences

Perform the following steps to upload new firmware to your SonicWALL appliance and use your current configuration settings upon startup:

1. Download the SonicOS firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.

   NOTE: If the firmware upload fails with a “Not enough memory to upload image” error, restart the appliance on the System > Restart page and then upload the firmware.
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 5.6

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

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

There are certain exceptions to preferences importing on these appliances running the SonicOS 5.6 release. Preferences cannot be imported in the following cases:

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

Full support for preferences importing from these appliances is targeted for a future release. At that time, you will need to upgrade your firmware to the latest SonicOS maintenance release available on MySonicWALL.

Importing Preferences from SonicOS Standard to SonicOS 5.6

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

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

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

To convert a Standard Network Settings file to an Enhanced one:

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

   The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that SonicWALL will retain a copy of their network settings after the conversion process is complete.
5. Upload the source Standard Network Settings file:
   - Click **Browse**.
   - Navigate to and select the source SonicOS Standard Settings file.
   - Click **Upload**.
   - Click the right arrow to proceed.

6. Review the source SonicOS Standard Settings Summary page.

   This page displays useful network settings information contained in the uploaded source Network Settings file. For testing purposes, the LAN IP and subnet mask of the appliance can be changed on this page in order to deploy it in a testing environment.

   - (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.
   - Click the right arrow to proceed.

7. Select the target SonicWALL appliance for the Enhanced deployment from the available list.

   SonicOS Enhanced is configured differently on various SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.

8. Complete the conversion by clicking the right arrow to proceed.
9. Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.
10. Click the **Download** button, select Save to Disk, and click OK to save the new target SonicOS Enhanced Network Settings file to your management computer.
11. Log in to the management interface for your SonicWALL appliance.
12. Navigate to **System > Settings**, and click the **Import Settings** button to import the converted settings to your appliance.

Support Matrix for Importing Preferences

DESTINATION FIREWALLS

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

Notes:

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

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

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

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

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

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

Upgrading a SonicOS Image with Factory Defaults

Perform the following steps to upload new firmware to your SonicWALL appliance and start it up using the default configuration:

1. Download the SonicOS firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Create Backup**.
3. Click **Upload New Firmware**.
4. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.
5. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware with Factory Default Settings**.
6. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
7. Enter the default user name and password (admin / password) to access the SonicWALL management interface.

Using SafeMode to Upgrade Firmware

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. The reset button is in a small hole next to the USB ports.
   - Use the LCD control buttons on the front bezel to set the appliance to Safe Mode. Once selected, the LCD displays a confirmation prompt. Select **Y** and press the **Right** button to confirm. The SonicWALL security appliance changes to SafeMode.

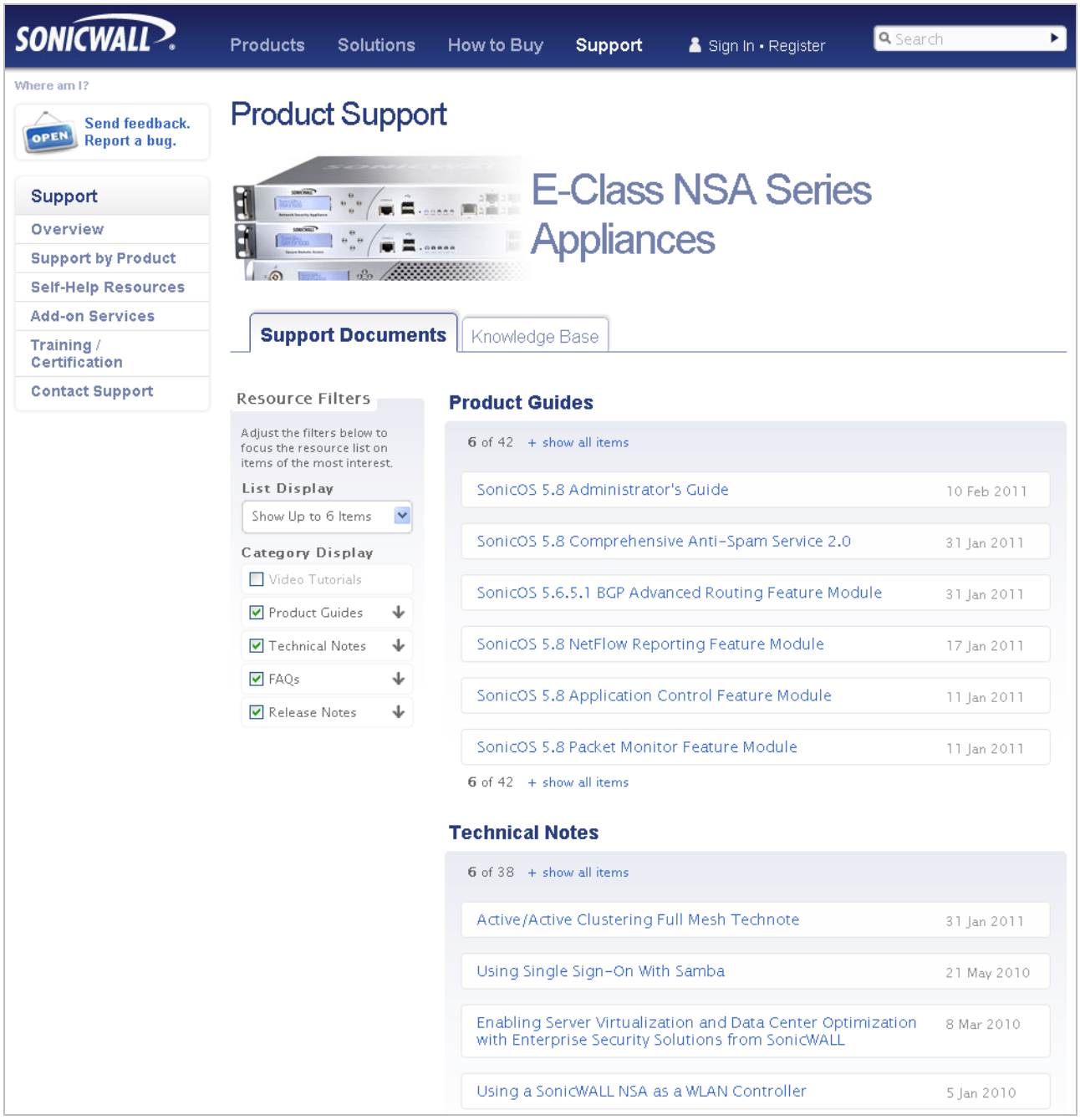
   The **Test** light starts blinking when the SonicWALL security appliance has rebooted into SafeMode.

   Note: *Holding the reset button for two seconds will send a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.*
3. Point the Web browser on your computer to **192.168.168.168**. The SafeMode management interface displays.
4. If you have made any configuration changes to the security appliance, select the **Create Backup On Next Boot** checkbox to make a backup copy of your current settings. Your settings will be saved when the appliance restarts.
5. Click **Upload New Firmware**, and then browse to the location where you saved the SonicOS firmware image, select the file, and click **Upload**.
6. Select the boot icon in the row for one of the following:
   - **Uploaded Firmware – New!**
     Use this option to restart the appliance with your current configuration settings.
   - **Uploaded Firmware with Factory Defaults – New!**
     Use this option to restart the appliance with default configuration settings.
7. In the confirmation dialog box, click **OK** to proceed.
8. After successfully booting the firmware, the login screen is displayed. If you booted with factory default settings, enter the default user name and password (admin / password) to access the SonicWALL management interface.

Related Technical Documentation

SonicWALL reference documentation and user guides are 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 Web site.



Last updated: 10/12/2011