Release Notes

| SonicOS | SonicOS 5.8.1.5 Release Notes |

Contents

Platform Compatibility

The SonicOS 5.8.1.5 release is supported on the following SonicWALL Deep Packet Inspection (DPI) security appliances:

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

The SonicWALL WAN Acceleration Appliance Series (WXA 500 Live CD, WXA 5000 Virtual Appliance, WXA 2000/4000 Appliances) are also supported for use with NSA E-Class, NSA, and TZ products running 5.8.1.5. The minimum recommended Firmware version for WXA Series is 1.0.18.

SONICWALL®

Browser Support

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

This release supports the following Web browsers:

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

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

Supported Features by Appliance Model

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

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
Wireless Client Bridge Support			Supported	Supported	Supported
App Flow Monitor	Supported	Supported	Supported		
Real-Time Monitor	Supported	Supported	Supported		
Packet Monitor Enhancements	Supported	Supported	Supported	Supported	Supported
Log > Flow Reporting Enhancements	Supported	Supported	Supported		
App Control Advanced	Supported	Supported	Supported	Supported	Supported
App Rules	Supported	Supported	Supported		
DPI-SSL	Supported	Supported			
Cloud GAV	Supported	Supported	Supported	Supported	Supported
NTP Auth Type	Supported	Supported	Supported	Supported	Supported
Link Aggregation	Supported				
Port Redundancy	Supported				
CFS Enhancements	Supported	Supported	Supported	Supported	Supported
IPFIX & NetFlow Reporting	Supported	Supported	Supported		
VLAN Enhancements (TZ Support)	Supported	Supported	Supported	Supported	Supported
SonicPoint VAPs	Supported	Supported	Supported	Supported	Supported

Feature / Enhancement	NSA E-Class Series	NSA Series	TZ 210 Series	TZ 200 Series	TZ 100 Series
CASS 2.0	Supported	Supported	Supported	Supported	Supported
Enhanced Connection Limit	Supported	Supported	Supported	Supported	Supported
Dynamic WAN Scheduling	Supported	Supported	Supported	Supported	Supported
Browser NTLM Auth	Supported	Supported	Supported	Supported	Supported
User Import from LDAP	Supported	Supported	Supported	Supported	Supported
SSL VPN NetExtender Client Update	Supported	Supported	Supported	Supported	Supported
DHCP Scalability Enhancements	Supported	Supported	Supported	Supported	Supported
SIP Application Layer Enhancements	Supported	Supported	Supported	Supported	Supported
SonicPoint-N DR	Supported	Supported	Supported	Supported	Supported
Accept Multiple VPN Client Proposals.	Supported	Supported	Supported	Supported	Supported
WAN Acceleration Support	Supported	Supported	Supported	Supported	Supported
App Control Policy Configuration via App Flow Monitor	Supported	Supported	Supported	Supported	Supported
Global BWM Ease of Use Enhancements	Supported	Supported	Supported	Supported	Supported
Application Usage and Risk Report	Supported	Supported	Supported		
Geo-IP Filtering and Botnet Command & Control Filtering	Supported	Supported	Supported		
Wire and Tap Mode	Supported	3500 and above			
Customizable Login Page	Supported	Supported	Supported	Supported	Supported
Preservation of Anti-Virus Exclusions After Upgrade	Supported	Supported	Supported	Supported	Supported
Management Traffic Only Option for Network Interfaces	Supported	Supported	Supported	Supported	Supported
Current Users and Detail of Users Options for TSR	Supported	Supported	Supported	Supported	Supported
User Monitor Tool	Supported	Supported	Supported		
Auto-Configuration of URLs to Bypass User Authentication	Supported	Supported	Supported	Supported	Supported

Known Issues

This section contains a list of known issues in the SonicOS 5.8.1.5 release.

Application Control

Symptom	Condition / Workaround	Issue
Emails are received with attachments even though an App Rules policy is created to block attachments.	Occurs when creating an App Rules policy to block POP3 incoming emails with .exe attachments, then connecting a PC to a firewall's LAN interface, and sending an email with an .exe attachment.	111851
App Control Advanced policies are applied to traffic from and to the VPN zone, rather than within the WAN zone only.	Occurs when enabling the App Control service on the WAN zone, and then enabling the logging or blocking action for any signature. After traffic is generated from the LAN to the VPN, the App Control Advanced policy is applied to VPN traffic.	107296
App Rules policies remain in effect even when disabled globally.	Occurs when the **Enable App Rules** checkbox is cleared to disable these policies globally, then an App Rules policy is created. When traffic on the WAN interface matches the rule, the configured policy action is applied. **Workaround**: Clear the **Enable App Rules** checkbox and reboot the appliance.	101194
Related traffic configured in an App Rules policy is blocked even though the **Enable App Rules** checkbox is not selected.	Occurs when an App Rules policy is created using the **Create Rule** button on the App Flow Monitor page and the **Enable App Rules** checkbox is not selected, which is the factory default setting. The App Rules policy is created and functions properly, even though the **Enable App Rules** checkbox is disabled. **Workaround**: Clear the **Enable App Rules** checkbox and reboot the appliance.	100120

Bandwidth Management

Symptom	Condition / Workaround	Issue
Traffic is dropped when the ingress or egress values for an interface are modified and traffic is passing through that interface.	Occurs when modifying the ingress or egress interface values while the interface is passing traffic. **Workaround**: Stop traffic on the interface, and then modify the values.	101286
Bandwidth management application rules are sometimes mapped to the wrong global BWM priority queue.	Occurs when creating a bandwidth management rule on the **App Flow Monitor** page and setting the priority to **High**. The **App Flow Monitor** page displays the created rule with a **Medium** priority setting, even though **High** was selected.	100116

DPI-SSL

Symptom	Condition / Workaround	Issue
DPI-SSL interrupts the Remote Desktop Protocol (RDP) traffic passing from a WLAN to a LAN.	Occurs when running Windows 7 and passing traffic from a WLAN to a LAN. The LAN side cannot establish an RDP session with the WLAN as an initiator.	102701

High Availability

Symptom	Condition / Workaround	Issue
The redundant WAN port allows traffic to pass, but the primary WAN interface and all routes to this subnet are marked as down when the primary port stops working.	Occurs when High Availability is enabled with probing and the primary WAN interface is configured with a redundant port. If the link for the active port goes down, Load Balancing (enabled by default) will change the status of the primary WAN interface to "Failover". All routes to the primary WAN subnet will be marked as down and traffic destined to the subnet will fail. However, traffic will still succeed to any destination that is on the far side of the default gateway of the primary WAN interface, by using the redundant port. **Workaround**: Disable Load Balancing or HA probing.	97883

Networking

Symptom	Condition / Workaround	Issue
Intermittent dropped routes for Route Based VPN or Tunnel Interfaces.	Occurs when configuring more than one Route Based VPN (or Tunnel Interface) to remote units with OSPF enabled.	102961
Traffic passing through interfaces paired in Wiremode is unsuccessful.	Occurs when the Wiremode interfaces are configured as Safe and Active/Active UTM is enabled.	101359

Users

Symptom	Condition / Workaround	Issue
The Log page displays the message "UDP Packet Dropped" after pinging a host or accessing a website using a Domain Name.	Occurs when navigating to the Users > Settings page and selecting **SSO Agent** from the **Single Sign On Method** drop-down list, then configuring the TSA agent and setting the default LAN to WAN Access Rule to **Trusted Users**.	111879
The **Policy Access Barred**, **Policy Access Down**, and **Policy Access Unavailable** login page types cannot be saved and error messages might be received.	Occurs when attempting to save changes when these login page types are selected in the **Select Login Page** drop-down list in the Customized Login Pages section of the Users > Settings page.	111814

VPN

Symptom	Condition / Workaround	Issue
Only one VPN tunnel can be active when multiple VPN polices are configured. Negotiations take place for both policies, but only the first policy results in an active tunnel.	Occurs when two or more VPN policies are configured between two firewalls, and each policy is bound to a different WAN interface on one of the firewalls.	110476 103398
Sometimes, the secondary IPSec gateway is unable to establish a tunnel with a peer if the primary gateway is unreachable.	Occurs when an IPsec VPN tunnel is configured between two SonicWALL appliances, one of which provides dual WAN interfaces (X1 and X4). If the primary WAN interface is disconnected, the tunnel cannot be established using the secondary interface.	103935

Resolved Issues

The following issues were resolved in the SonicOS 5.8.1.5 release:

Content Filtering System

Symptom	Condition / Workaround	Issue
Only the first 100 domains are filtered by the Content Filtering System (CFS), even though the Allowed List is set to 100+ domains.	Occurs when creating a custom CFS policy, setting the allowed domains to "Per Policy", and adding 100+ domains to the Allow List. **Resolution**: The user is now warned when 100 domains are exceeded, and a note has been added in the management interface to inform the user that the domain limit is 100.	107969

DPI-SSL

Symptom	Condition / Workaround	Issue
Newly added Common Name Exclusions are not populated in the DPI-SSL Common Name Exclusions list, or existing exclusions are lost.	Occurs when adding or editing URLs in the DPI-SSL Common Name Exclusions list.	98536

Networking

Symptom	Condition / Workaround	Issue
The **Network > NAT Policies** page in the management interface can display duplicate policies and extra characters on some policy names.	Occurs when enabling the Web Proxy feature with an IP on the WAN, then restarting the appliance.	110091

Users

Symptom	Condition / Workaround	Issue
The redirect for forced authorization by SonicWALL does not work with Internet Explorer 8 or 9.	Occurs when using a User Level Authentication (ULA) rule to force authorization by SonicWALL on an interface in Layer 2 Bridge Mode.	109762

Visualization

Symptom	Condition / Workaround	Issue
The NetFlow EndTime timestamp results in 0.00000 for valid and allowed TCP packets.	Occurs when the NetFlow collector's logging is enabled on Applicable Interfaces and Rules, and TCP traffic is sent to the allowed destination. Upon checking the packet capture details, the EndTime timestamp displays as 0.00000.	107239

WAN Acceleration

Symptom	Condition / Workaround	Issue
WFS Acceleration cannot be enabled and the error message "An error has occurred saving the hostname" displays.	Occurs when disabling WFS Acceleration, upgrading or downgrading the WXA firmware version, then re-enabling WFS Acceleration. WXA hostnames were allowed to be edited after WFS Acceleration was disabled, causing the error message when trying to re-enable WFS Acceleration.	110377

Wireless

Symptom	Condition / Workaround	Issue
The SonicPoint Ne becomes unresponsive during an Intrusion Detection Services (IDS) scan.	Occurs when configuring a SonicPoint Ne to an interface on the WLAN zone, then performing a manual IDS scan. This may also occur on boot up, when the appliance performs an initial scan.	111914

The following issues were resolved in the SonicOS 5.8.1.4 release:

Bandwidth Management

Symptom	Condition / Workaround	Issue
The ingress/egress rate per interface is not accurately controlled by the bandwidth management settings.	Occurs when Global BWM is enabled and 400 Mbps of UDP traffic (1518 bytes) is passing from the X5 (DMZ) interface to X0 (LAN). With no BWM rate configured on X5, the received rate on X0 is the full 400 Mbps. When a 200, 300, or 400 Mbps ingress rate is configured on X5, the received rate on X0 is 135, 140, or 146 Mbps.	108199

Content Filtering System

Symptom	Condition / Workaround	Issue
The SonicWALL CFS block page does not display when a blocked page is accessed, but the user sees a "page cannot be displayed" message instead.	Occurs when users are connecting via Layer 2 Tunneling Protocol and the L2TP server is configured in route-all mode, and a user browses to a website that is blocked by the CFS policy.	92539

Dashboard

Symptom	Condition / Workaround	Issue
The Bandwidth Management icon does not display anything after clicking it.	Occurs when navigating to the **Firewall Settings > BWM** page, then clicking the BWM icon.	109663
Changing the View Style, Vertical Access, or Show options on the **Dashboard > Use Monitor** page does not work.	Occurs when navigating to **Dashboard > Use Monitor**, then clicking the icon next to **Use Monitor**. A separate Dashboard > Use Monitor tab is displayed in the browser. Changing the View Style, Vertical Axis, or Show options does not work. Refresh the browser page and the options still do not work.	109634

Firmware

Symptom	Condition / Workaround	Issue
The Botnet Service is incorrectly listed on the Security Services > Summary page and the System > Status page of the SonicWALL TZ 200 wireless appliance, even though the service is not supported on this platform.	Botnet Command & Control Filtering is not supported on the SonicWALL TZ 100 and TZ 200 series appliances (as also reflected in the Supported Features by Appliance Model table of the Release Notes). The Botnet service listing indicating 'Not Licensed' on the System > Status page should be ignored.	108038
An iPad client fails to connect to the L2TP server if MSCHAPv2 authentication is set as the first order authentication method.	Occurs when GroupVPN is enabled and configured for an L2TP. The iPad can successfully connect if PAP authentication is set as the first order authentication method, but fails if MSCHAPv2 is preferred. A Windows XP client can successfully connect using MSCHAPv2. **Workaround**: Move MSCHAPv2 to the bottom of the authentication protocol list (by clicking on the Down Arrow button).	106801

Log

Symptom	Condition / Workaround	Issue
Syslog messages are sent with a source IP address of 0.0.0.0 out the wrong interface.	Occurs when attempting to send syslog messages to an internal Viewpoint server, but they are sent out the WAN interface with the source IP of 0.0.0.0 instead.	106271

Networking

Symptom	Condition / Workaround	Issue
SonicOS drops fragmented packets when Kerberos authentication is based on UDP.	Occurs when the firewall is configured in Routed Mode between a Cisco MPLS Router and the LAN at the remote locations and LAN users are trying to access remote computers over the MPLS link with Kerberos authentication. The SonicWALL drops the fragmented return traffic from the Cisco MPLS router.	108049
The Dynamic DNS agent does not automatically update dynamic DNS records, although the new IP address is reflected in the online status and the WAN interface IP address.	Occurs when using a DynDNS.com free account with a TTL set to 60 seconds, and the Dynamic DNS profile is added to the firewall and bound to the WAN interface using DSL/PPPoE and service type Dynamic, and then renewal of the dynamic WAN IP address is triggered by disconnecting and reconnecting the WAN PPPoE interface, by restarting, or by upgrading the firewall.	104539
The information displayed by the MIB Browser on a SNMPc server is not accurate for the interfaces of the connected SonicWALL appliance.	Occurs when an SNMPc server is connected to the secondary WAN interface on a SonicWALL NSA appliance and configured with read/write access using SNMPv2. SNMP management is enabled on the connected interface.	89533

System

Symptom	Condition / Workaround	Issue
Automatic adjustment for daylight savings time does not occur for Australian time zones.	Occurs when the SonicWALL appliance is set to use the Sydney/Melbourne (GMT +10:00) time zone and the "Automatically adjust clock for daylight saving time" checkbox is selected, and then the date of the time change arrives.	95748

Users

Symptom	Condition / Workaround	Issue
The NT LAN Manager (NTLM) cannot be enabled until RADIUS is enabled, but RADIUS cannot be enabled until NTLM is enabled.	Occurs when setting the authentication method to LDAP, the single-sign-on method to SSO Agent, and then enabling NTLM and RADUIS.	109247

User Interface

Symptom	Condition / Workaround	Issue
HTTP(S) management login or user login on the LAN is not possible and an error message is displayed: "Sorry, but either the maximum number of users are already logged in, or too many users are simultaneously trying to log in. Try again shortly or contact your firewall administrator." Login via SSH is still possible.	Occurs when more than 210 HTTP(S) connections to the appliance are opened, but then stop in the middle of the connection process, possibly to wait for something from the browser.	100106

VoIP

Symptom	Condition / Workaround	Issue
Inbound SIP audio cannot be heard after answering a call placed on hold.	Occurs when the existing SIP media connection being re-used, rather than re-negotiated, after coming off hold.	108339

VPN

Symptom	Condition / Workaround	Issue
A misconfigured VPN policy allows a phase 2 tunnel to be established instead of logging an error for the mismatched proposal.	Occurs when two VPN policies are configured on the local firewall and one VPN policy is configured on the remote firewall to match one of the local policies. When the remote firewall starts the tunnel negotiation, it establishes phase 1 to the matching policy, but if the phase 2 proposal matches the other policy, it establishes a tunnel with that policy rather than logging an error for the mismatched proposal.	107806
The Layer 2 Tunneling Protocol (L2TP) allows iOS / MAC users to connect without authentication (only using a pre-shared key).	Occurs when enabling the RSA SecureID option, then authenticating with an invalid username and a pre-shared key. The firewall should require proper authentication and not allow remote clients which have RSA SecureID enabled to connect to L2TP with only the pre-shared key.	107803
A user on a remote DHCP client machine cannot connect to the central firewall using HTTP.	Occurs when the remote and central gateways are configured to allow the remote network to obtain IP addresses via DHCP through the VPN tunnel, which automatically adds access rules on the central gateway. After these access rules are edited via the Firewall > Access Rules page to set the Users Allowed field to Everyone, and the IP address is renewed for the DHCP client on the remote network, the user cannot connect from that client machine.	107637
DHCP (unicast) packets are dropped on the central gateway as IP spoofed packets.	Occurs when IP Helper is enabled on the remote site in the DHCP policy, and the DHCP server is enabled on the central site, and IP Helper sends DHCP relay packets over the VPN tunnel interface.	105924

WAN Acceleration

Symptom	Condition / Workaround	Issue
The TCP Acceleration Service Object configuration is lost after rebooting the SonicWALL WXA. The field is reverted back to the default value of "HTTP" after the reboot.	Occurs when the TCP Acceleration Service Object field on the WAN Acceleration > TCP Acceleration configuration page in SonicOS is set to a non-default value, the configuration is saved, and then the WXA appliance is rebooted.	108197
SonicOS retains the previous IP address for a SonicWALL WXA even after the WXA appliance is replaced by another one.	Occurs when a SonicWALL WXA is connected to the SonicWALL firewall and is configured to use a static DHCP lease for the IP address, and then the WXA appliance is replaced by another WXA.	107384

Wireless

Symptom	Condition / Workaround	Issue
After being redirected to the Policy page and clicking **Accept**, the Android device's stock browser displays a browser error message, but the user can still access the Internet.	Occurs when enabling the guest service's **Policy Page Without Authentication** feature, clicking **Accept** on the Policy page, and then connecting to the web using the Android's stock browser.	108398

The following issue was resolved in the SonicOS 5.8.1.3 release:

Gateway Anti-Virus (GAV)

Symptom	Condition / Workaround	Issue
GAV does not detect malware in zip archives in rare cases with specific combinations of files.	Occurs when the zip contains a combination of at least FTP, NetBIOS and TCP stream files.	109653

The following issue was resolved in the SonicOS 5.8.1.2 release:

System

Symptom	Condition / Workaround	Issue
SonicOS management SessionID brute force vulnerability when attempted from the same source IP as a legitimate administrator's active management session.	Occurs when the brute force attacker finds the legitimate SessionID, which is valid for use only from the source IP of the legitimate administrator during an active session, from one of 4,294,967,296 possible SessionIDs (a session is active between the time legitimate administrator logs on and off). The SessionID security enhancement requires the attacker to guess the legitimate SessionID from one of 340,282,366,920,938,463,463,374,607,431,768,211,456 possible SessionIDs, and therefore requiring an attack on an active administrative session, from the same source IP of the administrator, to last 2,697,570,767,701,495,615,277,217,349,632 years. Please see this document for further analysis: SonicWALL Analysis of PenTest Vulnerability Reports	108138

The following issues were resolved in the SonicOS 5.8.1.1 release:

Firmware

Symptom	Condition / Workaround	Issue
After LDAP has been successfully configured, the LDAP test page begins to authenticate all users, regardless if their passwords are correct. This issue is encountered intermittently.	Occurs after LDAP is successfully configured, and subsequent changes are then made to the LDAP configuration--such as changing the Schema or enabling TLS.	107745
Open Directory LDAP authentication fails after upgrading to SonicOS 5.8.1.0 or 5.8.1.1.	Occurs when Open Directory LDAP authentication has been successfully configured, and the firmware on the appliance is upgraded from 5.8.0.3 to either 5.8.1.0 or 5.8.1.1	107744
Users cannot login on the SSL VPN portal if the user is a member of an LDAP group. An error message displays "Login failed - User login denied - LDAP communication or configuration error."	Occurs for users that are member of an LDAP group that uses openLDAP. Testing the username on the LDAP configuration page succeeds and returns the correct group membership.	107301
Uploading a large PKCS #12 file causes memory error.	Occurs when uploading a PKCS #12 file containing a certificate, a private key, and optional CA certificates. The PKCS #12 file processes successfully, but memory errors still occur, even after rebooting the system.	106687
Open Shortest Path First (OSPF) does not display connected networks to its OSPF peers after a firmware upgrade.	Occurs when loading customer preferences and attempting an upgrade test from SonicOS 5.8.0.2 to 5.8.1.1.	105987
The Deep Packet Inspection of Secure Socket Layer (DPI-SSL) and Application Firewall services are blocked with SonicOS 5.8.1.0-30o firmware.	Occurs after enabling DPI-SSL, Server SSL, and Application Firewall on the appliance running SonicOS 5.8.1.0-30o.	105444
The Geo-IP and Botnet Exclusion Objects do not take effect, causing DNS query packets to be incorrectly dropped.	Occurs when enabling the checkbox for **Block All Connections to/from Following Countries**, selecting all countries, and entering DNS Servers into the **Exclusion Object**. When a web page is accessed and the packet monitor is used to capture packets, you can see that all DNS query packets are dropped by the Geo-IP filter.	100010

High Availability

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

Modem

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

Networking

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

SSL VPN

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

System

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

Users

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

Wireless

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

Upgrading SonicOS Image Procedures

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

Obtaining the Latest SonicOS Image Version

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

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

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

Saving a Backup Copy of Your Configuration Preferences

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

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

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

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

Upgrading a SonicOS Image with Current Preferences

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

1. Download the SonicOS firmware image file from mysonicwall.com and save it to a location on your local computer.
2. On the System > Settings page, click **Upload New Firmware**.
3. Browse to the location where you saved the SonicOS firmware image file, select the file, and click **Upload**.
4. On the System > Settings page, click the **Boot** icon in the row for **Uploaded Firmware**.
5. In the confirmation dialog box, click **OK**. The SonicWALL restarts and then displays the login page.
6. Enter your user name and password. Your new SonicOS image version information is listed on the **System** > **Settings** page.

Importing Preferences to SonicOS 5.8

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

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

There are certain exceptions to preferences importing on these appliances running the SonicOS 5.8 release. Preferences cannot be imported in the following cases:

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

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

Importing Preferences from SonicOS Standard to SonicOS 5.8 Enhanced

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

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

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

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

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

   The source Standard Network Setting file must be uploaded to MySonicWALL as part of the conversion process. The Setting Conversion tool uses MySonicWALL authentication to secure private network settings. Users should be aware that SonicWALL will retain a copy of their network settings after the conversion process is complete.
5. Upload the source Standard Network Settings file:

   - Click **Browse**.
   - Navigate to and select the source SonicOS Standard Settings file.
   - Click **Upload**.
   - Click the right arrow to proceed.
6. Review the source SonicOS Standard Settings Summary page.

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

   - (Optional) Change the LAN IP address and subnet mask of the source appliance to that of the target appliance.
   - Click the right arrow to proceed.
7. Select the target SonicWALL appliance for the Enhanced deployment from the available list.

   SonicOS Enhanced is configured differently on various SonicWALL appliances, mostly to support different interface numbers. As such, the converted Enhanced Network Settings file must be customized to the appliance targeted for deployment.
8. Complete the conversion by clicking the right arrow to proceed.
9. Optionally click the **Warnings** link to view any differences in the settings created for the target appliance.
10. Click the **Download** button, select Save to Disk, and click OK to save the new target SonicOS Enhanced Network Settings file to your management computer.
11. Log in to the management interface for your SonicWALL appliance.
12. Navigate to **System > Settings**, and click the **Import Settings** button to import the converted settings to your appliance.

SONICWALL ®

Support Matrix for Importing Preferences

DESTINATION FIREWALLS

(Legend: ✓ = 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. Letter codes refer to Notes below.)

Source firewalls are listed down the left (labelled vertically "SOURCE FIREWALLS").

Source \ Dest	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 220	NSA 220W	NSA 240	NSA 250M	NSA 250MW	NSA 2400	NSA 3500	NSA 4500	NSA 5000	NSA E5500	NSA E6500	NSA E7500	NSA E8500	NSA E8510
TZ100/TZ200	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ100W/TZ200MW	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 210	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 210W	C	✓	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 170	B,D	B,D	B,D	B,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 170W	B,C,D	B,D	B,C,D	B,D	C	✓	✓	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 170SP	B,C,D	B,C,D	B,C,D	B,D	C	C	✓	✓	C	C	✓	C	C	✗	✗	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 170SPW	C,D	B,C,D	B,C,D	B,D	C	C	C	✓	C	C	C	✓	C	✗	✗	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 180	C,D	C,D	C,D	C,D	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 180W	C,D	C,D	C,D	C,D	C	✓	C	✓	C	✓	C	✓	C	✗	✗	✗	✗	✗	✗	✗	B,C,D	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 190	C,D	C,D	C,D	C,D	C	C	✓	✓	C	C	✓	C	C	✗	✗	✗	✗	✗	✗	✗	B,D	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
TZ 190W	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	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	C,E
NSA 220	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
NSA 220W	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
NSA 240	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
NSA 250M	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
NSA 250MW	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗
NSA 2400	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✗	C	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
NSA 3500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✗	C	✗	✗	C	✓	✓	✓	✓	✓	✓	✓	✓
NSA 4500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✗	C	✗	✗	C	C	✓	✓	✓	✓	✓	✓	✓
NSA 5000	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✗	C	✗	✗	C	C	C	✓	✓	✓	✓	✓	✓
NSA E5500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✗	C	✗	✗	C	C	C	C	✓	✓	✓	✓	C
NSA E6500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✗	C	✗	✗	C	C	C	C	✓	✓	✓	✓	C
NSA E7500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✗	C	✗	✗	C	C	C	C	✓	✓	✓	✓	C
NSA E8500	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	C	✗	C	✗	✗	C	C	C	C	✓	✓	✓	✓	C
NSA E8510	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	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 are 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-SonicOS 5.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.

SONICWALL®

Upgrading a SonicOS Image with Factory Defaults

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

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

Using SafeMode to Upgrade Firmware

The SafeMode procedure uses a reset button in a small pinhole, whose location varies: on the NSA models, the button is near the USB ports on the front; on the TZ models, the button is next to the power cord on the back. If you are unable to connect to the SonicWALL security appliance's management interface, you can restart the SonicWALL security appliance in SafeMode. The SafeMode feature allows you to quickly recover from uncertain configuration states with a simplified management interface that includes the same settings available on the System > Settings page.

To use SafeMode to upgrade firmware on the SonicWALL security appliance, perform the following steps:

1. Connect your computer to the X0 port on the SonicWALL appliance and configure your IP address with an address on the 192.168.168.0/24 subnet, such as 192.168.168.20.
2. Do one of the following to restart the appliance in SafeMode:
    - Use a narrow, straight object, like a straightened paper clip or a toothpick, to press and hold the reset button on the front of the security appliance for more than 20 seconds.
    - Use the LCD control buttons on the front bezel to set the appliance to Safe Mode. Once selected, the LCD displays a confirmation prompt. Select **Y** and press the **Right** button to confirm. The SonicWALL security appliance changes to SafeMode.

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

    Note: *Holding the reset button for two seconds will send a diagnostic snapshot to the console. Holding the reset button for six to eight seconds will reboot the appliance in regular mode.*

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

Related Technical Documentation

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

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

Last updated: 1/26/2012