

SonicOS 7.1

Diagnostics for Classic Mode

Administration Guide

SONICWALL®

# Contents

<b>About SonicOS</b> .....	<b>4</b>
Working with SonicOS .....	4
SonicOS Workflow .....	6
How to Use the SonicOS Administration Guides .....	7
Guide Conventions .....	8
<b>Introduction to Diagnostics for Classic Mode</b> .....	<b>9</b>
<b>Terminal</b> .....	<b>11</b>
<b>Tech Support Report</b> .....	<b>12</b>
Completing a Tech Support Request .....	12
Generating a Tech Support Report .....	13
<b>Check Network Settings</b> .....	<b>15</b>
<b>DNS Name Lookup</b> .....	<b>17</b>
Resolving a System DNS Server .....	18
Resolving a Customized DNS Server .....	19
<b>Network Path</b> .....	<b>20</b>
<b>Ping</b> .....	<b>21</b>
<b>Trace Route</b> .....	<b>22</b>
<b>Real-Time Blacklist</b> .....	<b>23</b>
<b>Reverse Name Lookup</b> .....	<b>24</b>
<b>Connection TopX</b> .....	<b>25</b>
<b>Geo and Botnet</b> .....	<b>26</b>
<b>MX and Banner</b> .....	<b>27</b>
<b>GRID Check</b> .....	<b>29</b>
<b>URL Rating Request</b> .....	<b>30</b>
<b>PMTU Discovery</b> .....	<b>31</b>

<b>Switch Diagnostics</b> .....	<b>32</b>
<b>SonicWall Support</b> .....	<b>33</b>
About This Document .....	34

# About SonicOS

This guide is a part of the SonicOS collection of administrative guides that describes how to administer and monitor the SonicWall family of firewalls. SonicOS provides network administrators the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration by setting objects to secure and protect the network services, to manage traffic, and to provide the desired level of network service. This guide focuses on how to configure the diagnostics settings on the SonicWall security appliances.

## Topics:

- [Working with SonicOS](#)
- [SonicOS Workflow](#)
- [How to Use the SonicOS Administration Guides](#)
- [Guide Conventions](#)

## Working with SonicOS

SonicOS provides a web management interface for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your network. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system.

The SonicOS management interface facilitates:

- Setting up and configuring your firewall
- Configuring external devices like access points or switches
- Configuring networks and external system options that connect to your firewall
- Defining objects and policies for protection
- Monitoring the health and status of the security appliance, network, users, and connections
- Monitoring traffic, users, and threats
- Investigating events

SonicWall offers two different modes of operation in SonicOS; the modes differ mainly in the areas of policy, object configuration and diagnostics.

- *Policy Mode* provides a unified policy configuration work flow. It combines Layer 3 to Layer 7 policy enforcement for security policies and optimizes the work flow for other policy types. This unified policy work flow gathers many security settings into one place, which were previously configured on different pages of the management interface.
- *Classic Mode* is more consistent with earlier releases of SonicOS; you need to develop individual policies and actions for specific security services. The Classic Mode has a redesigned interface.

This table identifies which modes can be used on the different SonicWall firewalls:

Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTTPS bandwidth issues; built-in SD-WAN, and lawful TLS 1.3 decryption support.
NSa Series	yes	no	NSa firewalls provide your mid sized network with enhanced security . They are designed specifically for businesses with 250 and up. it can provide cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, SD-WAN, real-time visualization, and WLAN management.
NSsp 10700, NSsp 11700, NSsp 13700	yes	no	The NSsp platforms high-end firewalls that deliver the advanced threat protection and fast speeds that large enterprises, data centers, and service providers need.
NSsp 15700	no	yes	The NSsp 15700 is designed for large distributed enterprises, data centers, government agencies and services providers. It provides advanced threat protection like Real-Time Deep Memory Inspection, multi-instance firewall configuration, and unified policy creation and modification, with scalability and availability.
NSv Series	yes	yes	The NSv series firewalls offers all the security advantages of a physical firewall with the operational and economic benefits of virtualization. The NSv firewalls can operate in either Policy Mode or Classic Mode. You can switch between modes, but some configuration information from extra interfaces is removed.

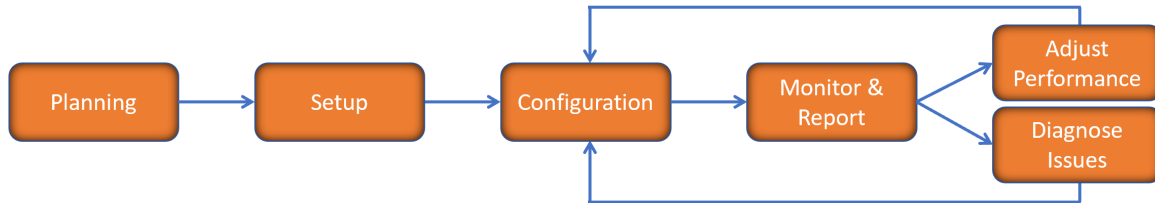
In addition to the management interface, SonicOS also has a full-featured API and a CLI to manage the firewalls. For more information, refer to:

- [SonicOS 7.1 API Reference Guide](#)

- [SonicOS Command Line Interface Reference Guide](#)

# SonicOS Workflow

When working with SonicWall products, you can use the following workflow as a guide for setting up your security solution.

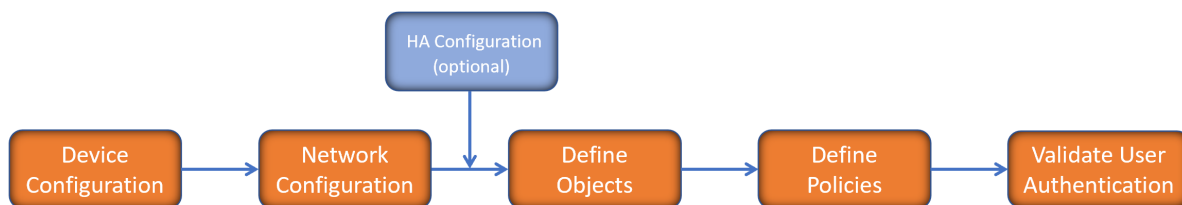


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your network and make recommendations based on the kinds of security services you need. You can learn more about SonicWall products by reviewing [product information](#) and [solutions](#). After selecting the solution, you can schedule your implementation.

After planning and scheduling your solution, you begin setting up the firewalls. The [Getting Started Guides](#) for your products can help you begin setting up the pieces to your solution. The getting started guides are designed to help you install the firewall to a minimal level of operation. Before performing any detailed configuration tasks described in the SonicOS Administration Guides, you should have your firewall set up and basic operation validated.

The configuration block of the workflow refers to the many tasks that combine to define how your firewall is integrated into your security solution and how it behaves when protecting your environment. Depending on the features of your security solution, this task can be quite complex. The System Administration Guides are broken into the key command sets and features. Some documents may be used for all solutions, but others may be used only if you integrated that feature into your solution. For example, High Availability or Wireless Access Points are not necessarily used by all customers. More information about a feature's workflow is presented in the feature administration guide. Refer to the [specific Administration Guide for a SonicOS feature](#) for more information.

Configuration tends to be a one-time activity, although you might make minor adjustments after monitoring performance or after diagnosing an issue. The configuration activity can be broken down into the more detailed flow as the following figure shows. This also mirrors the key functions that are listed across the top of the management interface.

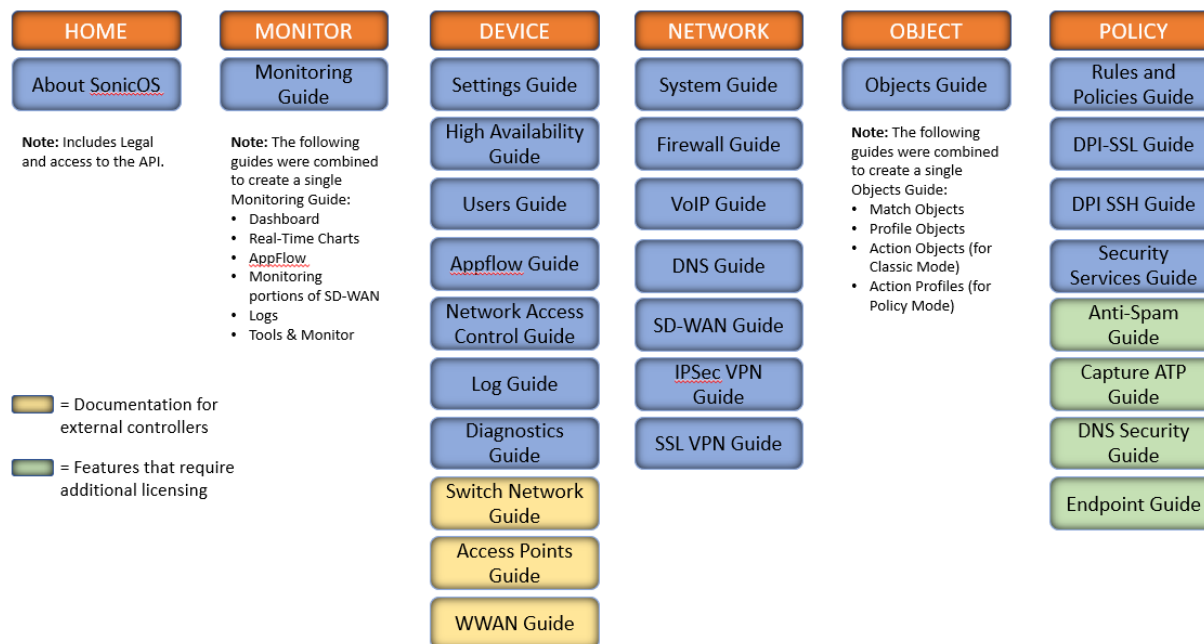


There is some flexibility in the order in which you do things, but this is the general work-flow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement High Availability when done. After your device, network, and system is configured, you should define the objects that you want to monitor. Then you use those objects to define the policies that protect your network. The final step to preparing your setup is to validate the user authentication.

## How to Use the SonicOS Administration Guides

The *SonicOS Administration Guide* is a collection of guides that detail the features represented by each of the main menu items in the management interface. Within each guide, you can find topics covering commands in that menu group, along with procedures and in-depth information. The exceptions are the *SonicOS 7.1 Monitor Guide* and the *SonicOS 7.1 Objects Guide* which combine the topics for each of those functions into a single book.

To help you understand how the books align with the features and commands, the following figure shows the books organized like the SonicWall management interface.



The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the <https://www.sonicwall.com/support/technical-documentation/>.

# Guide Conventions

These text conventions are used in this guide:

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **TIP:** A TIP icon indicates helpful information.

⚠ | **CAUTION:** A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

⚠ | **WARNING:** A WARNING icon indicates a potential for property damage, personal injury, or death.

Convention	Description
<b>Bold text</b>	Used in procedures to identify elements in the management interface like dialog boxes, windows, screen names, messages, and buttons. Also used for file names and text or values you are being instructed to select or type into the interface.
<b>Function   Menu group &gt; Menu item</b>	Indicates a multiple step menu choice on the user interface. For example, <b>NETWORK   System &gt; Interfaces</b> means to select the <b>NETWORK</b> functions at the top of the window, then click on <b>System</b> in the left navigation menu to open the menu group (if needed) and select <b>Interfaces</b> to display the page.
<b>Code</b>	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<b>&lt;Variable&gt;</b>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment <b>serialnumber=&lt;your serial number&gt;</b> , replace the variable and brackets with the serial number from your device, such as <b>serialnumber=2CB8ED000004</b> .
<b>Italics</b>	Indicates the name of a technical manual. Also indicates emphasis on certain words in a sentence, such as the first instance of a significant term or concept.



# Introduction to Diagnostics for Classic Mode

This administration guide provides information about the SonicOS Diagnostics feature for the Classic Mode.

Diagnostic tools allow the administrator to test connectivity by performing a Ping, TCP connection test, DNS lookup, reverse lookup, and trace route for a specific IP address or web site. Other Diagnostics for Classic Mode tools provide a way to view or monitor the Geo and Botnet, the MX Banner, GRID result, PMTU Discovery, and other features.

The following comparison table gives the Diagnostics features available for SonicOS Classic Mode and Policy Mode:

<b>Diagnostic Tools Features</b>	<b>SonicOS 7 Classic Mode</b>	<b>SonicOS 7 Policy Mode</b>
Tech Support Report	Available	Available
Check Network Settings	Available	Available
DNS Name Lookup	Available	Available
Network Path	Available	Available
Ping	Available	Available
Trace Route	Available	Available
Real-Time Blacklist	Available	Available
Reverse Name lookup	Available	Available
Connection TopX	Available	Not Available
Geo and Botnet	Available	Available
MX and Banner	Available	Not Available
GRID Check	Available	Not Available
URL Rating Request	Available	Available
PMTU Discovery	Available	Available
Switch Diagnostics	Available	Available
Policy Lookup	Not Available	Available

The following comparison table gives the platforms supported:

SonicWall Firewall Model	SonicOS 7 Classic Mode	SonicOS 7 Policy Mode
<i>Hardware Firewalls</i>		
TZ Series: TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670	Supported	Not Supported
NSa Series: NSa 2700, NSa 3700, NSa 4700, NSa 5700, and NSa 6700	Supported	Not Supported
NSsp Series: NSsp 10700, NSsp 11700, and NSsp 13700	Supported	Not Supported
NSsp Series: NSsp15700	Not Supported	Supported
<i>Virtual Firewalls</i>		
NSv Series: NSv 270, NSv 470, and NSv 870	Supported	Supported

① **NOTE:** The Terminal option that was available on Diagnostics menu is now moved to the notification center and no longer appears in the Diagnostics menu. For more information, refer to [Terminal](#).

Navigate to **Device > Diagnostics**, the various tools available in Diagnostics menu group includes:

- [Tech Support Report](#)
- [Check Network Settings](#)
- [DNS Name Lookup](#)
- [Network Path](#)
- [Ping](#)
- [Trace Route](#)
- [Real-Time Blacklist](#)
- [Reverse Name Lookup](#)
- [Connection TopX](#)
- [Geo and Botnet](#)
- [MX and Banner](#)
- [GRID Check](#)
- [URL Rating Request](#)
- [PMTU Discovery](#)
- [Switch Diagnostics](#)

For Troubleshooting diagnostics tools, refer to the knowledge base articles [Troubleshooting](#) and to monitor, refer to the [SonicOS 7.1 Monitor Guide](#)

# Terminal

Navigate to notification center, click **Open SSH terminal session** icon to start a SSH Console Window to issue commands directly to the network security appliance.

① | **NOTE:** SSH management must be enabled for the interface of the device before a SSH session can be started successfully.

### ***To enable SSH management of the device:***

1. Navigate to **Network > Interfaces**.
2. Select the interface for which you want to enable SSH management and click the **Edit** icon.
3. In the **Management** section, click the **SSH** toggle to activate SSH management of the device (if it is not already enabled).
4. Click **OK**.

### ***To start a SSH management session:***

1. Navigate to notification center, click **Open SSH terminal session** icon.
2. Click **OK** when the warning displays with the IP address.
3. The SSH session will start by requesting the administrator login credentials on SSH Console Window.  
① | **NOTE:** SSH management must be ON for this interface.

# Tech Support Report

The Tech Support Report generates a detailed report of the SonicWall security appliance configuration and status and saves it to the local hard disk using the Download Tech Support Report button. This file can then be emailed to SonicWall Technical Support to help assist with a problem.

① | **NOTE:** You must register your SonicWall security appliance on MySonicWall to receive technical support.

## Topics:

- [Completing a Tech Support Request](#)
- [Generating a Tech Support Report](#)

## Completing a Tech Support Request

Before emailing the Tech Support Report to the SonicWall Technical Support team, complete a Tech Support Request Form at <https://www.mysonicwall.com>. After the form is submitted, a unique case number is returned. Include this case number in all correspondence, as it allows SonicWall Technical Support to provide you with better service.

# Generating a Tech Support Report

**TECH SUPPORT REPORT**

Automatic secure crash analysis reporting

Periodic secure diagnostic reporting for support purposes

Time Interval (minutes)

CSC Reporting Time Interval (minutes)

Include raw flow table data entries when sending diagnostic report

**CONFIGURE**

Sensitive Keys <input type="checkbox"/>	Inactive users <input checked="" type="checkbox"/>	Extra Routing Info <input type="checkbox"/>
ARP Cache <input type="checkbox"/>	Detail of users <input checked="" type="checkbox"/>	Vendor Name Resolution <input type="checkbox"/>
DHCP Bindings <input type="checkbox"/>	IP Stack Info <input type="checkbox"/>	Debug info in report <input checked="" type="checkbox"/>
IKE Info <input type="checkbox"/>	IPv6 NDP <input type="checkbox"/>	IP Report <input type="checkbox"/>
List of current users <input checked="" type="checkbox"/>	IPv6 DHCP <input type="checkbox"/>	ABR Entries <input type="checkbox"/>
DNS Proxy Cache <input type="checkbox"/>	Geo-IP/Botnet Cache <input type="checkbox"/>	Application Signatures <input type="checkbox"/>
Wireless Diagnostics <input type="checkbox"/>	User Name <input checked="" type="checkbox"/>	

Cancel Accept

**ACTIONS**

Download System Logs Download Tech Support Report Download SSO Auth Log Send Diagnostic Reports To Support

## To generate a Tech Support Report (TSR):

1. Navigate to **Device > Diagnostics > Tech Support Report**.
2. In the Tech Support Report section, turn on any of the following report options:
  - **Sensitive Keys** - Saves shared secrets, encryption, and authentication keys to the report.
  - **ARP Cache** - Saves a table relating IP addresses to the corresponding MAC or physical addresses.
  - **DHCP Bindings** - Saves entries from the firewall DHCP server.
  - **IKE Info** - Saves current information about active IKE configurations.
  - **List of current users** - Lists all currently logged in active local and remote users.
  - **Wireless Diagnostics** - Lists log data if the SonicPoint or internal wireless radio experiences a failure and reboots.
  - **DNS Proxy Cache** - This option is not selected by default.
  - **Inactive users** - Lists the users with inactive sessions. Selected by default.
  - **Detail of users** - Lists additional details of user sessions, including timers, privileges, management mode if managing, group memberships, CFS policies, VPN client networks, and other information. The Current users report checkbox must be enabled first to obtain this detailed report.
  - **IP Stack Info** - This option is not selected by default.
  - **IPv6 NDP** - This option is not selected by default.
  - **IPv6 DHCP** - This option is not selected by default.

- **Geo-IP/Botnet Cache** - Saves the currently cached Geo-IP and Botnet information.
  - **User Name** - Shows user name in the report.
  - **Extra Routing Info** - Shows extra routing information in the report.
  - **Capture ATP Cache** - Saves the currently cached Capture information.
  - **Vendor Name Resolution** - This option is not selected by default.
  - **Debug Info in report** - Specifies whether the downloaded TSR is to contain debug information.
  - **IP Report** - This option is not selected by default.
  - **ABR Entries** - This option is not selected by default.
  - **Application Signatures** - Shows application signature information in the report.
3. Click **Accept** to save the changes.
  4. Click **Download Tech Support Report** under the **Actions** section to save the file to your system.
  5. Click **OK** to save the file.
  6. Attach the report to your Tech Support Request email.
  7. To send the TSR, system preferences, and trace log to SonicWall Engineering (not to SonicWall Technical Support), click **Send Diagnostic Reports to Support** under the **Actions** section. The Status indicator at the bottom of the page displays **Please wait!** while the report is sent, and then displays **Diagnostic reports sent successfully**. You would normally do this after talking to Technical Support.
  8. To download the SSO authentication log, click **Download SSO Auth Log** under the **Actions** section .
  9. To download system logs, click **Download System Logs** under the **Actions** section and then click **Confirm**.
  10. To send diagnostic files to SonicWall Tech Support for crash analysis, select the **Automatic secure crash analysis reporting** toggle switch  
**NOTE:** This toggle switch is not applicable for NSsp 15700.
  11. To periodically send the TSR, system preferences, and trace log to MySonicWall for SonicWall Engineering:
    - a. Select the **Periodic secure diagnostic reporting for support purposes** switch.
    - b. Enter the interval in minutes between the periodic reports in the **Time Interval (minutes)** field. The default is 1440 minutes (24 hours).
    - c. Enter the interval in minutes between the periodic reports in the **CSC Reporting Time Interval (minutes)** field. The default is 15 minutes.  
**NOTE:** This toggle switch is not applicable for NSsp 15700.
  12. To include flow table data in the TSR, toggle the switch for **Include raw flow table data entries when sending diagnostic report**.  
**NOTE:** This toggle switch is not applicable for NSsp 15700.

## Check Network Settings

Check Network Settings is a diagnostic feature that automatically checks the network connectivity and service availability of several pre-defined functional areas of SonicOS, returns the results, and attempts to describe the causes if any exceptions are detected.

SERVER	IP ADDRESS	TEST RESULTS	NOTES	TIMESTAMP	PROGRESS
<input type="checkbox"/> Default Gateway (X1)	→ 10.203.28.1				
<input type="checkbox"/> DNS Server 1	→ 8.8.8.8				
Total: 2 item(s)					

SERVER	IP ADDRESS	TEST RESULTS	NOTES	TIMESTAMP	PROGRESS
<input type="checkbox"/> My SonicWall	→ www.mysonicwall.com				
<input type="checkbox"/> License Manager	→ lm2.sonicwall.com				
Total: 2 item(s)					

This tool helps you locate the problem area when users encounter a network problem. The feature lists both IPv4 and IPv6 network settings in different tabs.

Specifically, Check Network Settings automatically tests the following functions:

- Default Gateway settings
- DNS settings
- MySonicWall server connectivity
- License Manager server connectivity
- Content Filter server connectivity

The return data consists of two parts:

- Test Results – Provides a summary of the test outcome
- Notes – Provides details to help determine the cause if any problems exist

The **Check Network Settings** feature is dependent on the **Network Monitor** feature available under **Network | Network Monitor** view. Whenever the Check Network Settings tool is being executed (except during the Content Filter test), a corresponding Network Monitor Policy appears on the **Network | Network Monitor** page, with a special diagnostic tool policy name in the form:

```
diagTestPolicyAuto_<IP_address/Domain_name>_0
```

Navigate to **Device > Diagnostics > Check Network Settings**. to use the Check Network Settings tool, first select it in the Diagnostic Tools drop-down list and then click the Test button in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red X indicates that there is a problem.

To test multiple items at the same time, check the box for each desired item and then click **TEST ALL SELECTED**.



## DNS Name Lookup

The DNS lookup tool returns the IPv4 and IPv6 IP address of a URL. If you enter an IPv4 and/or IPv6 IP address, the tool returns the domain name for that address. If you enter a domain name, the tool returns the DNS server used and the resolved address.

Navigate to **Device > Diagnostics > DNS Name Lookup**, with the **DNS Server** radio buttons, you can select either a **System** or **Customized** DNS server. The options change, depending on which you choose.

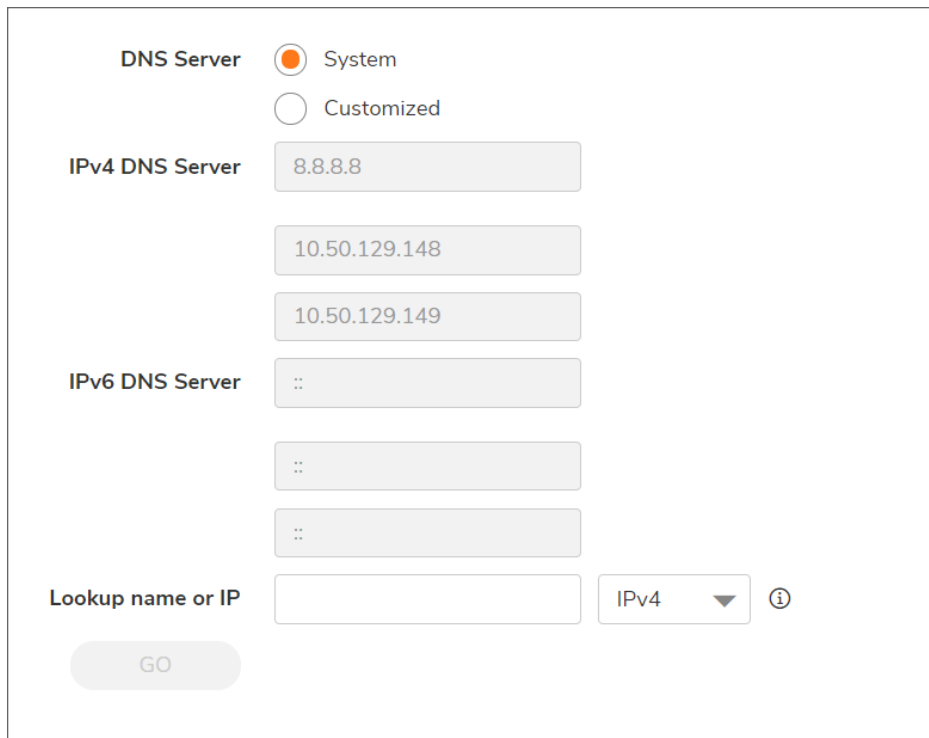
The **IPv4/IPv6 DNS Server** fields display the IP addresses of the DNS Servers configured on the firewall. If there is no IP address (0.0.0.0 for IPv4 or :: for IPv6) in the fields, you must configure them on the **Network > DNS** page.

Under **Lookup name or IP**, enter the URL and select, IPv4, IPv6, or All and click **GO**.

# Resolving a System DNS Server

*To resolve a system DNS Server:*

1. Select **System** for the DNS Server.



The screenshot shows a configuration window for DNS settings. At the top, under 'DNS Server', the 'System' radio button is selected, and the 'Customized' radio button is unselected. Below this, there are three input fields for 'IPv4 DNS Server' containing the addresses 8.8.8.8, 10.50.129.148, and 10.50.129.149. There are three input fields for 'IPv6 DNS Server', each containing '::'. At the bottom, there is a 'Lookup name or IP' text field, a dropdown menu currently set to 'IPv4', and an information icon. A 'GO' button is located at the bottom left of the form area.

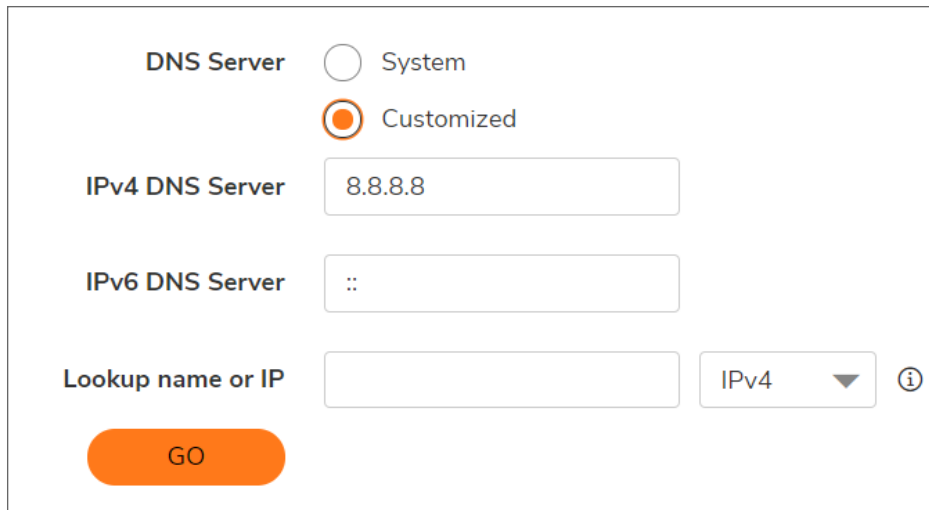
2. In the **Lookup name or IP** field, enter either the domain name or the IP address.
3. Select the type of IP address from the drop-down menu:
  - IPv4 (default)
  - IPv6
  - All
4. Click **GO**. The firewall returns the matching pair of addresses and domain names.

**IMPORTANT:** When specifying a domain name, do not add http or https to the name.

# Resolving a Customized DNS Server

*To resolve a Customized DNS Server:*

1. Select **Customized** under DNS Server.



The screenshot shows a configuration panel for DNS resolution. At the top, under 'DNS Server', there are two radio buttons: 'System' (unselected) and 'Customized' (selected). Below this, there are three input fields: 'IPv4 DNS Server' with the value '8.8.8.8', 'IPv6 DNS Server' with the value '::', and 'Lookup name or IP' which is empty. To the right of the 'Lookup name or IP' field is a dropdown menu currently showing 'IPv4' and an information icon. At the bottom left of the panel is an orange 'GO' button.

2. If the DNS Server IP address is not populated, enter it in the IPv4 or IPv6 field.
3. In the **Lookup name or IP** field, enter either the domain name or the IP address.
4. Select the type of IP address from the drop-down menu:
  - IPv4 (default)
  - IPv6
  - All
5. Click **GO**.

## Network Path

Enter an IP address to determine the network path of it. The Network Path feature finds if the IP is located on a specific network interface, if it reached a router gateway IP address, and if it reached through an Ethernet address.

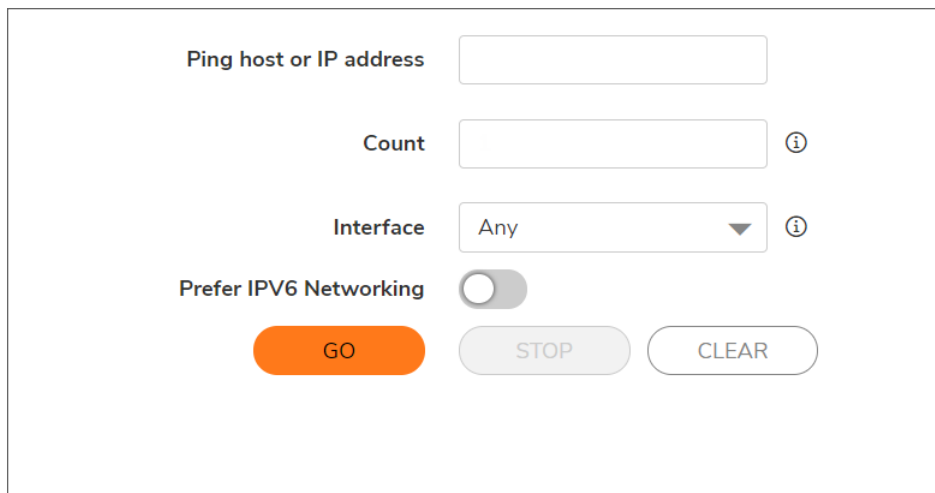
Find location of this IP address

***To find network path of an IP address:***

1. Navigate to **Device > Diagnostics > Network Path**.
2. Enter the IP address of the network.
3. Click **GO**.

# Ping

The Ping test sends a packet off a machine on the Internet and returns it to the sender. This test shows if the firewall is able to contact the remote host. If users on the LAN are having problems accessing services on the Internet, try pinging the DNS server, or another machine at the ISP location. If the test is unsuccessful, try pinging devices outside of the ISP. If you can ping devices outside of the ISP, then the problem lies with the ISP connection.



The screenshot shows a configuration panel for the Ping test. It includes the following elements:

- Ping host or IP address:** A text input field.
- Count:** A text input field with an information icon (i) to its right.
- Interface:** A dropdown menu currently set to "Any" with an information icon (i) to its right.
- Prefer IPV6 Networking:** A toggle switch that is currently turned off.
- Buttons:** Three buttons at the bottom: "GO" (orange), "STOP" (grey), and "CLEAR" (grey).

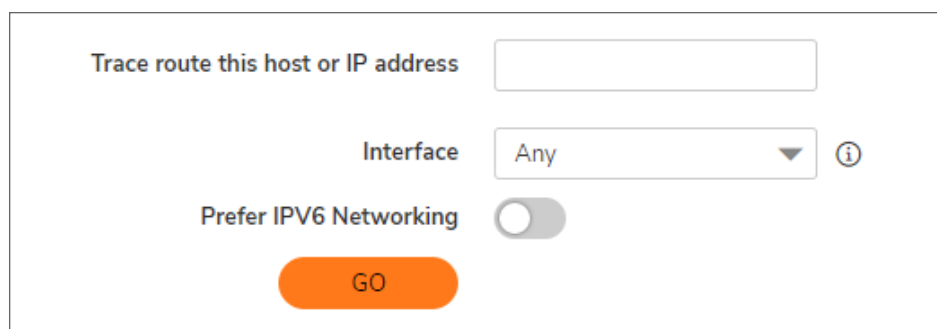
### To ping an IP address:

1. Navigate to **Device > Diagnostics > Ping**
2. Specify the **Ping host or IP address** of the target device.
3. Specify the **Count**.
4. In the **Interface** drop-down menu, select which WAN interface you want to test the ping from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the drop-down.
5. Toggle **Prefer IPv6 Networking** switch if you prefer pinging to an IPv6 address.
6. Click **GO**.

## Trace Route

Trace Route is a diagnostic utility that assists in diagnosing and troubleshooting router connections on the Internet. By using Internet UDP packets similar to Ping packets, Trace Route can test interconnectivity with routers and other hosts that are spread along the network path until the connection fails or until the remote host responds.

Trace Route tool includes a IPv6 networking option. When testing interconnectivity with routers and other hosts, SonicOS uses the first IP address that is returned and shows the actual Trace Route address. If both IPv4 and IPv6 addresses are returned, by default, the firewall checks the IPv4 address. If the **Prefer IPv6 Networking** option is enabled, the check only IPv6 address.



Trace route this host or IP address

Interface  ▼ ⓘ

Prefer IPv6 Networking

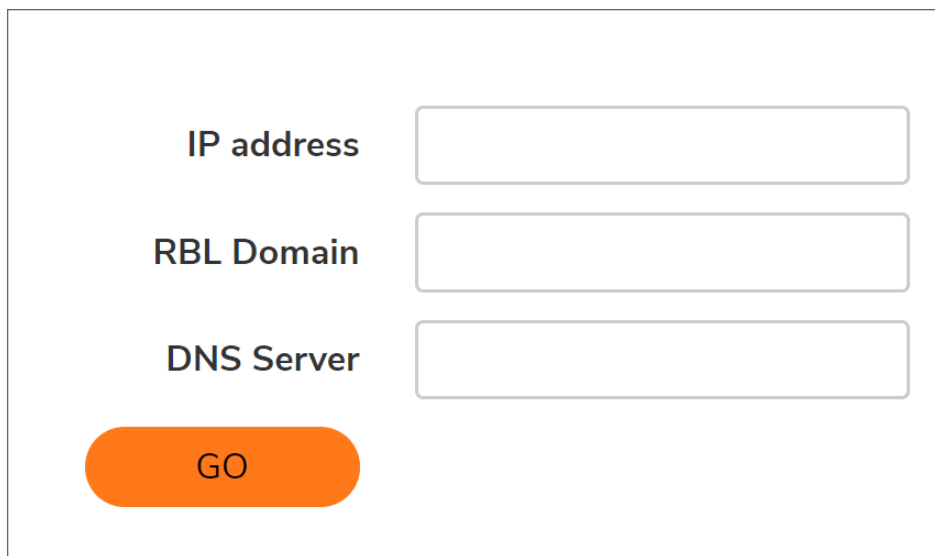
**GO**

### **To troubleshoot with Trace Route:**

1. Navigate to **Device > Diagnostics > Trace Route**.
2. Type the IP address or domain name of the destination host in the **TraceRoute this host or IP address** field.
3. In the **Interface** drop-down menu, select which WAN-specific interface you want to test the trace route from. Selecting ANY, the default, allows the firewall to choose among all interfaces—including those not listed in the drop-down menu.
4. To TraceRoute for IPv6, select the **Prefer IPv6 Networking** checkbox.
5. Click **GO**. Depending on the route, this may take a few minutes. A popup table displays with each hop to the destination host. By following the route, you can diagnose where the connection fails between the firewall and its destination.

## Real-Time Blacklist

The Real-Time Blacklist feature allows you to blacklist SMTP IP addresses, RBL services, and DNS servers.



The screenshot shows a configuration interface for the Real-Time Blacklist feature. It consists of three text input fields stacked vertically, each with a label to its left: 'IP address', 'RBL Domain', and 'DNS Server'. Below the input fields is a prominent orange button with the text 'GO' in white capital letters.

**To blacklist an IP address, RBL domain, or a DNS server:**

1. Navigate to **Device > Diagnostics > Real-Time Blacklist**.
2. Enter an IP address in the **IP address** field, a FQDN for the RBL in the **RBL Domain** field, or DNS server information in the **DNS Server** field.
3. Click **GO**.

## Reverse Name Lookup

The Reverse Name Lookup feature returns the DNS server name for a given IP address. The Log Resolution DNS server 1, 2, and 3 shows the DNS servers configured for the firewall. You can manually configure the DNS servers from **Network > DNS**.

Log Resolution DNS Server 1	<input type="text" value="10.65.1.51"/>
Log Resolution DNS Server 2	<input type="text" value="10.50.129.148"/>
Log Resolution DNS Server 3	<input type="text" value="0.0.0.0"/>
Reverse Lookup the IP Address	<input type="text"/>
<input type="button" value="GO"/>	

*To look up an IP address:*

1. Navigate to **Device > Diagnostics > Reverse Name Lookup**.
2. Enter the IP address in the **Reverse Lookup the IP Address** field.
3. Click **GO**.



## Connection TopX

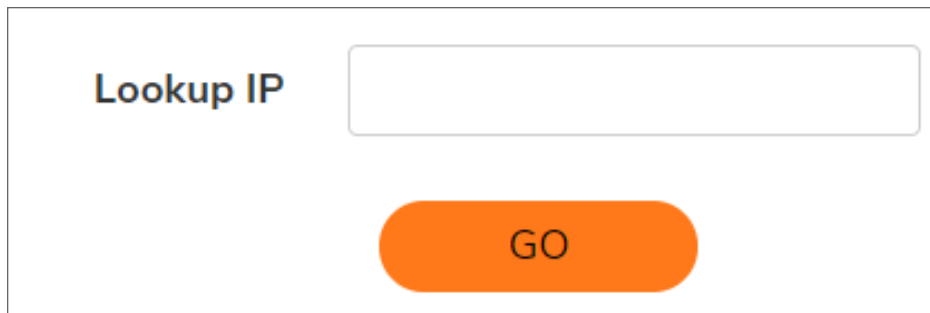
Navigate to **Device > Diagnostics > Connection TopX**. The Connection TopX feature lists the top 10 connections by the source and destination IP addresses. Before you can use this tool, you must enable source IP address connection limiting and /or destination IP address connection limiting for your appliance. If these are not enabled, the page displays a message to tell you where you can enable them.

#	FROM	TO	PRIORITY	SOURCE	DESTINATION	SERVICE	USER INCLUDED	USER EXCLUDED	COMMENT
No Data									
Total: 0 Item(s)									

NOTE: Access Rules listed here are those policies that are enabled and on which source or destination IP address connection limit is enabled.

## Geo and Botnet

The Geo and Botnet Lookup feature allows you to look up the connections to or from a geographic location based on IP address and to or from Botnet command and control servers.



The image shows a user interface for a lookup feature. On the left, the text "Lookup IP" is displayed. To its right is a rectangular text input field. Below the input field is a prominent orange button with the word "GO" written in white capital letters.

***To troubleshoot with GEO Location and BOTNET Server Lookup:***

1. Navigate to **Device > Diagnostics > Geo and Botnet**.
2. Type the IP address or domain name of the destination host in the **Lookup IP** field.
3. Click **GO**. The result displays underneath the Lookup IP field.

## MX and Banner

In the MX Record Lookup and Banner Check section, you can perform:

- An MX Record lookup for a given domain name.
- A connection check to the resulting host server or supplied IP address to retrieve the SMTP banner.

<b>DNS Server 1</b>	<input type="text" value="10.50.129.148"/>
<b>DNS Server 2</b>	<input type="text" value="8.8.8.8"/>
<b>DNS Server 3</b>	<input type="text" value="4.2.2.2"/>
<b>Lookup name or IP</b>	<input type="text"/>
<b>SMTP Port</b>	<input type="text" value="25"/>
<input type="button" value="GO"/>	

The DNS servers are displayed by default in the **DNS Server 1/2/3** fields. The SMTP port is displayed in the **SMTP Port** field.

When you enter a domain name or IP address, the Comprehensive Anti-Spam service attempts to connect to that server and retrieve the SMTP banner. This feature allows you to verify that an email sender is not spoofing an address to appear more legitimate.

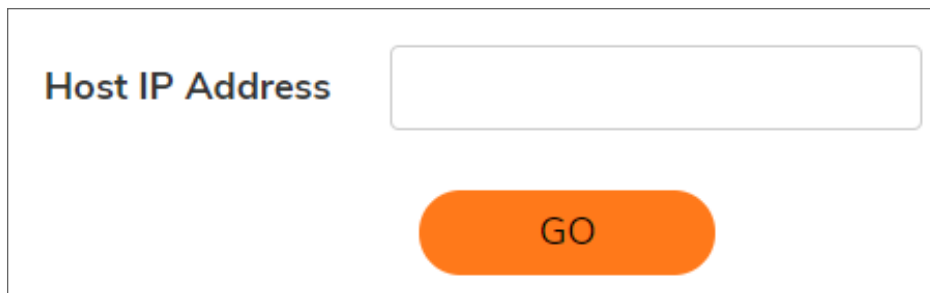
① **NOTE:** This feature is only available when the Essential Protection Service Suite or Comprehensive Anti-Spam Service is licensed on the firewall.

***To look up the MX record of an emailer or domain:***

1. Navigate to **Device > Diagnostics > MX and Banner**.
2. Enter the domain name or IP address in the **Lookup name or IP** field.
3. Click **GO**. The results are displayed.

## GRID Check

This feature helps to check the GRID Network IP Reputation - the reputation a particular IP address has, with members of the SonicWall GRID Network. When this feature is enabled, email is not accepted from IP addresses with a bad reputation. When SonicWall receives a connection from a known bad IP address, it responds with a **554 no smtpd here** error and the SMTP session is rejected.



The screenshot shows a web interface for performing a GRID check. It features a label 'Host IP Address' on the left, followed by a rectangular text input field. Below the input field is a prominent orange rounded button with the text 'GO' in white capital letters.

**NOTE:** This feature is only available when the Essential Protection Service Suite or Comprehensive Anti-Spam Service is licensed on the firewall.

***To perform a grid-check:***

1. Navigate to **Device > Diagnostics > Grid Check**.
2. Specify the Host IP Address.
3. Click **Go**.

# URL Rating Request

Content Filtering Service feature classifies websites under 64 categories based on the content. You can find information about a website by looking up the URL in the CFS URL Rating Request feature.



The screenshot shows a user interface for looking up a URL. It consists of a rectangular box containing the text "Lookup Rating for URL" on the left, a white text input field in the center, and an orange rounded button with the text "GO" on the right.


***To look up a URL:***

1. Navigate to **Device > Diagnostics > URL Rating Request**.
2. Enter the URL in the **Lookup Rating for URL** field.
3. Click **Go**.

## PMTU Discovery

PMTU Discovery is a diagnostic tool that uses a standardized technique for determining the maximum transmission unit (MTU) size on the network path between two Internet Protocol (IP) hosts, usually with the goal of avoiding IP fragmentation. PMTU Discovery works with both IPv4 and IPv6 protocols.

**Path MTU Discovery to this host or IP address**

**Interface**  

**GO**

### *To troubleshoot with PMTU Discovery::*

1. Navigate to **Device > Diagnostics > PMTU Discovery**.
2. Type the IP address or domain name of the destination host in the **Path MTU Discovery to this host or IP address** field.
3. In the Interface drop-down menu, select which WAN-specific interface you want to test the trace route from. Selecting **ANY**, the default, allows the firewall to choose among all interfaces—including those not listed in the drop-down menu.
4. Click **GO**.  
Depending on the route, this may take a few minutes. A pop-up table displays with each hop to the destination host. By following the route, you can diagnose where the connection fails between the firewall and the destination.

# Switch Diagnostics

The **Switch Diagnostics** page displays the port status and port counters of a SonicWall Switch connected to the firewall.

The screenshot shows the 'SWITCH DIAGNOSTICS' page with an 'Interface' dropdown menu set to 'X0'. The page is divided into two sections: 'PORT STATUS' and 'PORT COUNTERS'.

PORT STATUS		PORT COUNTERS	
Interface	X0	RxFrames	902276
Link Status	UP	RxBytes	308107326
Speed	10000	TxFrames	2965
Duplex	FD	TxBytes	889017
		Collisions	0
		RxErrors	7
		RxUnicastFrames	1463
		TxUnicastFrames	1581
		RxNotUnicastFrames	900813
		TxNotUnicastFrames	1384
		RxMulticastFrames	899014
		TxMulticastFrames	1264
		RxBroadcastFrames	1799
		RxBroadcastFrames	1799
		TxBroadcastFrames	120

### To access Switch Diagnostics:

1. Navigate to **Device > Diagnostics > Switch Diagnostics**.
2. Select the interface that is connected to the Switch from the **Interface** drop-down menu.



# SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to <https://www.sonicwall.com/support>.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at <https://community.sonicwall.com/technology-and-support>.
- View video tutorials
- Access <https://mysonicwall.com>
- Learn about SonicWall Professional Services at <https://sonicwall.com/pes>.
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit <https://www.sonicwall.com/support/contact-support>.

# About This Document

SonicOS Diagnostics for Classic Mode Administration Guide

Updated - December 2023

Software Version - 7.1

232-005866-00 Rev A

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products.

EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit <https://www.sonicwall.com/legal>.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: <https://www.sonicwall.com/legal/end-user-product-agreements/>.

## Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request  
Attn: Jennifer Anderson  
1033 McCarthy Blvd  
Milpitas, CA 95035