SonicOS 7.1

Network Access Control

Administration Guide

SONICWALL®

Contents

1

Overview

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 the management interface, API (Application Program Interface), and the Command Line Interface (CLI) for firewall configuration.

Topics:

About SonicOS

SonicOS refers to the web management interface used for configuring, managing, and monitoring the features, policies, security services, connected devices, and threats to your environment. SonicOS runs on top of SonicCore, SonicWall's secure underlying operating system. SonicOS management interface facilitates the following:

- 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. The *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. The following table identifies which modes can be used on the different SonicWall firewalls:

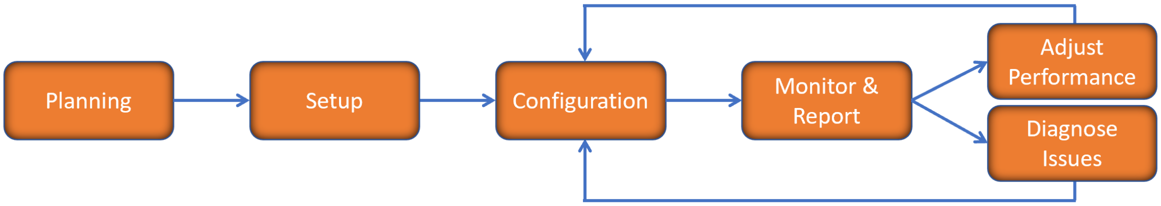
Firewall Type	Classic Mode	Policy Mode	Comments
TZ Series	yes	no	The entry level TZ Series, also known as desktop firewalls, deliver revamped features such as 5G readiness, better connectivity options, improved threat, SSL and decryption performance that address HTPPS bandwidth issues; built-in SD-WAN, 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 firwalls 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 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.

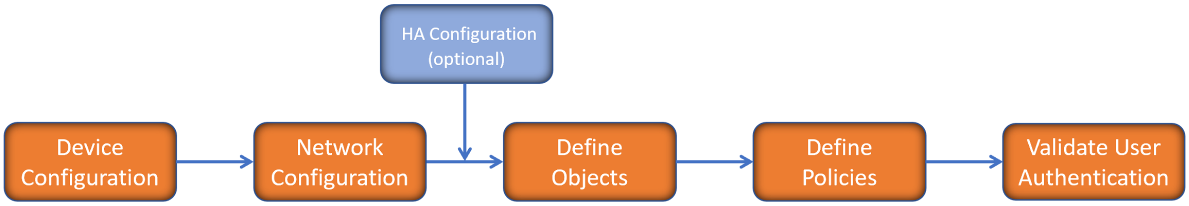


You begin your planning as you start making your purchasing decisions. Your sales partners can help you assess your environment and make recommendations based on the kinds of security services you need to protect your environment. You can learn more about SonicWall products by reviewing product information 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 features of the security solution so you can focus on one at a time. Some documents may be used for all solutions, but others may be used use 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 a 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.

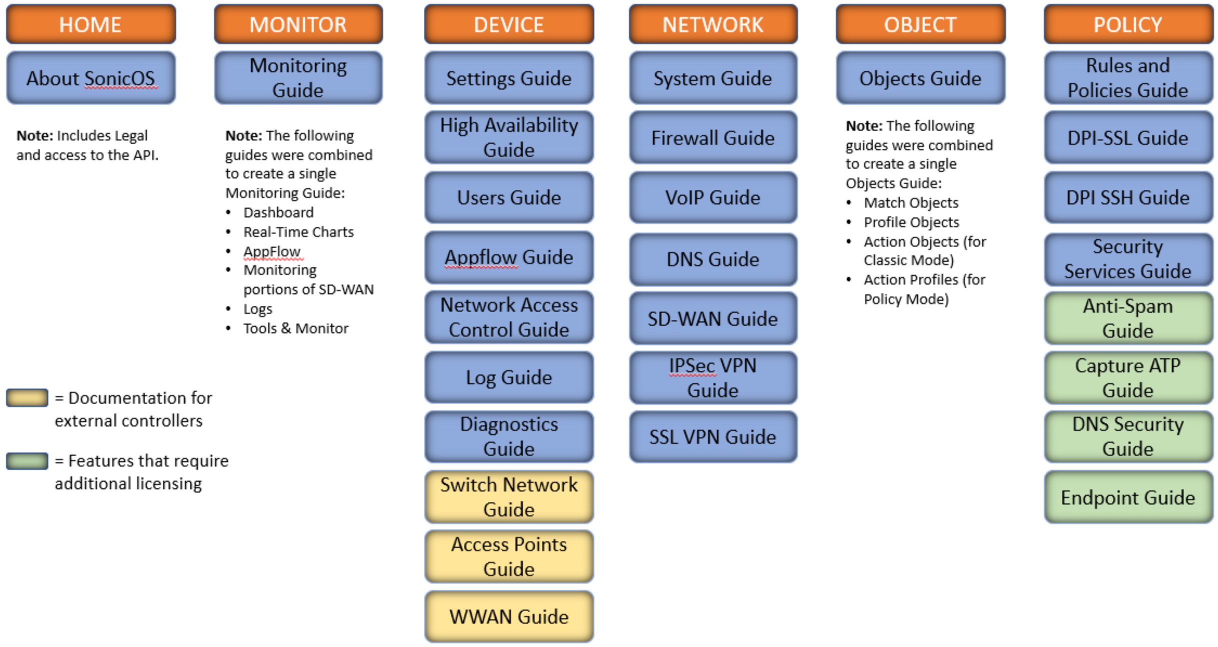


There is some flexibility in the order in which you do things, but this is the general workflow you would follow when configuring your firewall. Start by defining the settings on the firewall. Next you set up the system and other devices that your firewall is connected to, and you can choose to implement 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 environment. 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 actually a collection of administration 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 Monitoring Guide* and the *SonicOS 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 to SonicWall management interface.



Note: Includes Legal and access to the API.

Note: The following guides were combined to create a single Monitoring Guide:

- Dashboard
- Real-Time Charts
- AppFlow
- Monitoring portions of SD-WAN
- Logs
- Tools & Monitor

Note: The following guides were combined to create a single Objects Guide:

- Match Objects
- Profile Objects
- Action Objects (for Classic Mode)
- Action Profiles (for Policy Mode)

🟨 = Documentation for external controllers

🟩 = Features that require additional licensing

The SonicOS Administration Guides, along with related documentation, such as the getting started guides, are available on the .

Guide Conventions

These text conventions are used in this guide:

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

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

ⓘ | **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.**

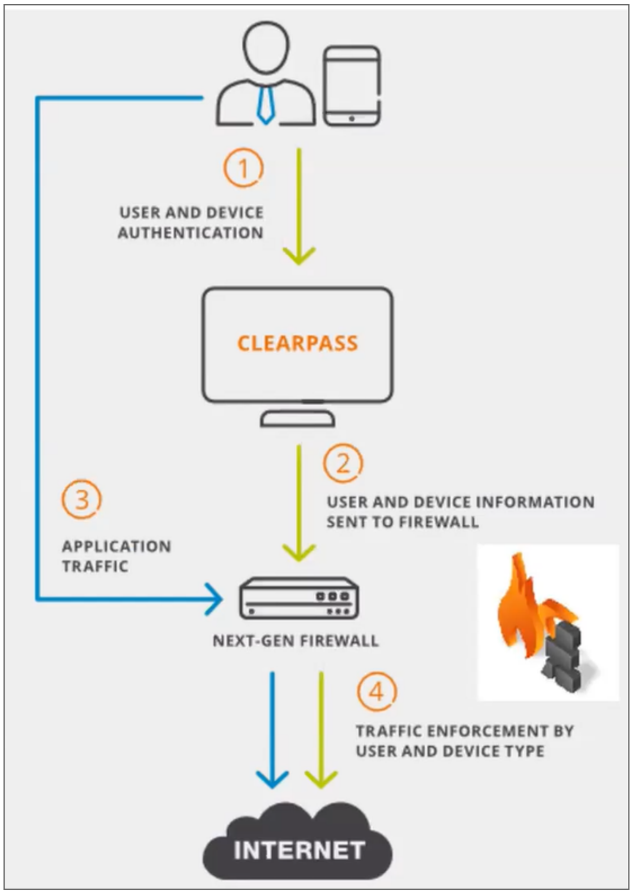
⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

Convention	Description
Bold text	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.
Function | Menu group > Menu item	Indicates a multiple step menu choice on the user interface. For example, **NETWORK | System > Interfaces** means to select the **NETWORK** functions at the top of the window, then click on **System** in the left navigation menu to open the menu group (if needed) and select **Interfaces** to display the page.
`Code`	Indicates sample computer programming code. If bold, it represents text to be typed in the command line interface.
<Variable>	Represents a variable name. The variable name and angle brackets need to be replaced with an actual value. For example in the segment **serialnumber=**<*your serial number*>, replace the variable and brackets with the serial number from your device, such as serialnumber=2CB8ED000004.
Italics	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.

Aruba ClearPass NAC Support

SonicOS provides Restful threat APIs to NAC vendors (Aruba ClearPass) using which they can pass security context to SonicOS firewall. Using the security context SonicOS builds policies for mitigation actions. SonicOS fetches dynamic user roles and other information from NAC vendor (Aruba ClearPass) to build information model and perform the traffic filtering.

SonicOS can support multiple NAC servers from different vendors simultaneously.


1
USER AND DEVICE AUTHENTICATION
CLEARPASS
2
USER AND DEVICE INFORMATION SENT TO FIREWALL
3
APPLICATION TRAFFIC
NEXT-GEN FIREWALL
4
TRAFFIC ENFORCEMENT BY USER AND DEVICE TYPE
INTERNET

Topics:

- Configure SonicWall Policy by API - Default Groups
- Enable ClearPass Integration

Configure SonicWall Policy by API - Default Groups

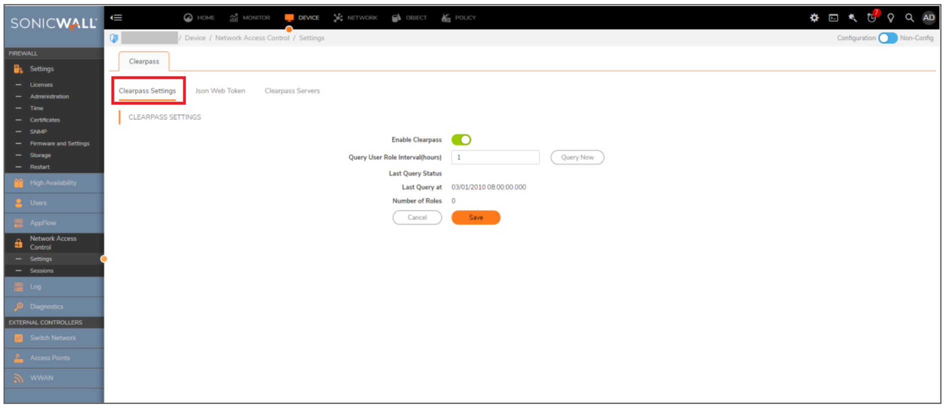
SonicOS creates a default container deny group which includes Transient, Quarantine, Infected and Unknown. All the default groups are editable and can be automatically updated with membership in SonicOS.

Enable ClearPass Integration

To be able to accept Threat APIs from ClearPass servers, you need to first enable the ClearPass in SonicOS.

To enable ClearPass:

1. Login to SonicOS using username and password.
2. Under **Device** page, navigate to **Network Access Control** > **Settings**.
3. Click on the ClearPass Settings tab.



Enable Clearpass ●

Query User Role Interval(hours) 1

Last Query Status

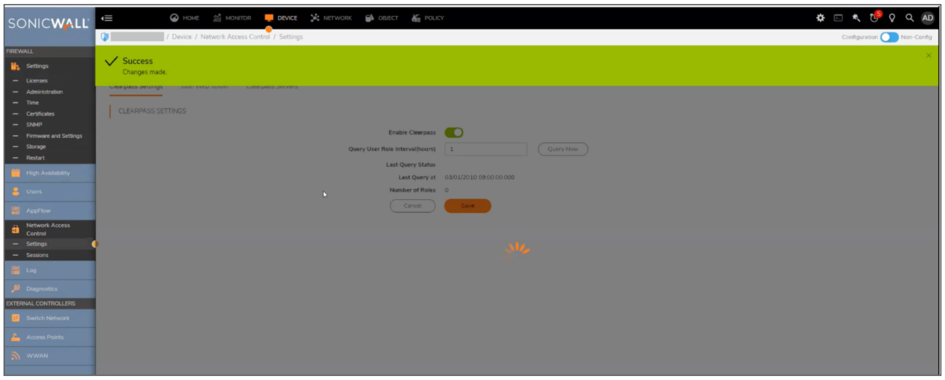
Last Query at 03/01/2010 08:00:00.000

Number of Roles 0

4. Enable the toggle button for **Enable ClearPass** option.
5. Set the **Query User Role Interval(hours)**.

   ⓘ **NOTE:** The information exchange between SonicOS and NAC is bi-directional, so query timer needs to be set.

6. Click **Save**.



[redacted] / Device / Network Access Control / Settings

Success
Changes made.

CLEARPASS SETTINGS

Enable Clearpass

Query User Role Interval(hours) 1

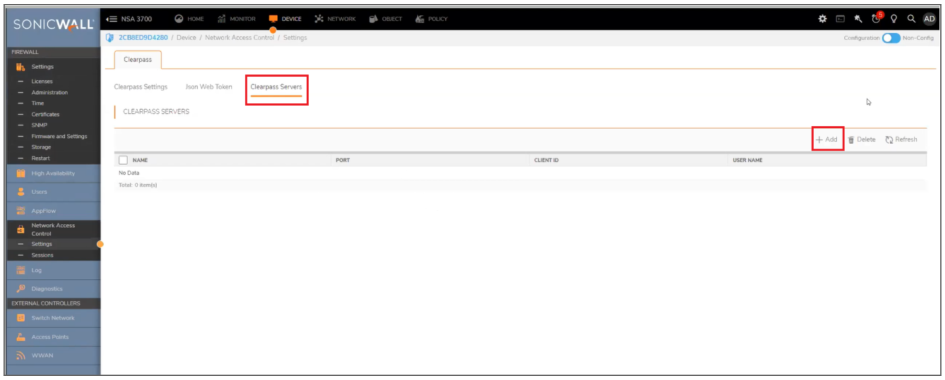
Last Query Status

Last Query at 03/01/2010 08:00:00.000

Number of Roles 0

To add ClearPass Server:

1. Click on **ClearPass Servers** tab. Click on **Add**.



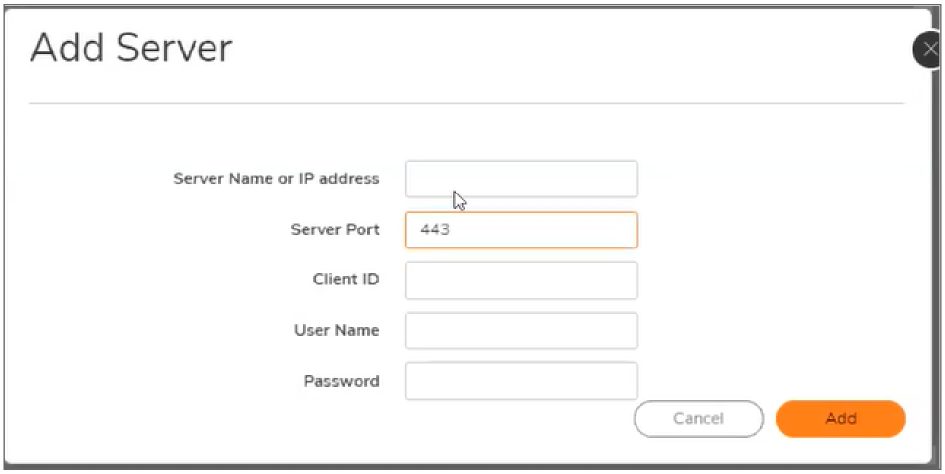
2CB8ED9D4280 / Device / Network Access Control / Settings

CLEARPASS SERVERS

NAME	PORT	CLIENT ID	USER NAME
No Data			

Total: 0 item(s)

2. Enter the details of the NAC server. Click on **Add.**



Add Server

Server Name or IP address

Server Port 443

Client ID

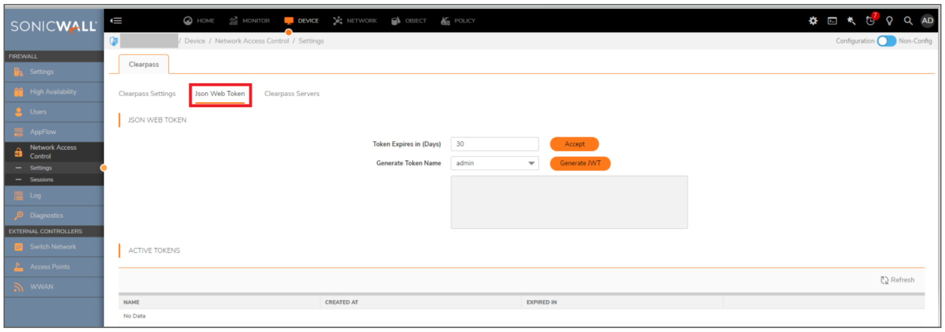
User Name

Password

ⓘ **NOTE:** To secure the communication between NAC and Firewall, a dynamic JSON Web Token (JWT) needs to be created. Whenever a NAC device tries to connect to SonicOS firewall, JSON Web Token (JWT) has to be generated first. The NAC device can then include the generated JSON Web Token (JWT) in their UI, to be able to establish a connection.

To generate JSON Web Token:

1. Click on **JSON Web Token** tab.



Token Expires in (Days): 30

Generate Token Name: admin

NAME	CREATED AT	EXPIRED IN
No Data		

2. Enter the **Token Expires in (Days)** and click **Accept**.

3. Select the username from the drop-down list under **Generate Token Name**.

4. Click on **Generate JWT**.

3

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 Network Access Control Administration Guide
Updated - December 2023
Software Version - 7.1
232-005864-00 Rev A

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