FIREWALL TOOLBOX

Installation and Usersguide

Based on Version 3.1.0.0

Introduction

- What is Firewall Toolbox?
- Main capabilities
- Supported SonicWall platforms / SonicOS versions
- Intended audience
- How Firewall Toolbox works: TSR, EXP, API and MySonicWall

Installation and First Start

- System requirements
- Installation
- Licensing / Trial version
- Initial configuration
- Repository / storage location

Getting Started

- Basic workflow
- Adding/importing a firewall
- Manual TSR/EXP import
- Downloading configuration through the API
- Connecting to MySonicWall
- Automatic analysis after import
- Opening the Full Audit Report

Understanding the User Interface

- Main window
- Firewall selection
- The five main categories
- Settings
- Status and progress information

Security Audit

- Overview
- Individual reports
- What each report checks
- How to interpret findings
- Security Audit Summary

 Health

- System health reports
- Utilization
- Licensing / Security Services
- Health Summary

 Configuration Audit

- Configuration checks
- Firmware
- HA
- WAN Failover
- VPN configuration
- Configuration Audit Summary

 Documentation

- Firewall Rules
- NAT Policies
- Zones
- Interfaces
- Address Objects
- Users / Groups
- VPNs
- Other configuration documentation
- Complete Documentation Report

 Maintenance

- Unused Address Objects
- Disabled/unused Firewall Rules
- Disabled/unused NAT Policies
- TCP Timeout analysis
- Duplicate objects
- Naming checks
- Maintenance Summary

 Full Audit / All-in-One Report

- Automatic report generation

- Highlights / Recommendations
- Table of Contents
- Understanding report sections
- Creating reports manually
- Report languages

 Working with the SonicWall API

- Establishing an API connection
- Required permissions
- SSL certificate handling
- Backups and safety mechanisms
- Disabling Firewall Rules
- Deleting Firewall Rules
- NAT Policy operations
- Deleting unused Address Objects
- Resetting TCP Timeouts
- Restoring/reverting changes

 Settings and Customization

- Report language
- IPv6 reports
- Default objects
- Automatically added rules
- Repository settings
- Report appearance
- Date/time settings

 Troubleshooting

- TSR/EXP cannot be imported
- API connection fails
- Authentication problems
- MySonicWall connection
- Missing reports/data
- PDF/report generation problems

 Appendix

- Terminology
- File and directory structure
- Report overview
- API operations overview
- Version information / support
- Configuration steps for API Connection to Firewall
- Configuration steps for API Connection to MySonicWall

1. Introduction

1.1 About Firewall Toolbox

Firewall Toolbox is a software solution for analyzing, auditing, documenting, and maintaining SonicWall firewalls.

Managing a firewall involves much more than configuring rules and security services. Over time, configurations grow, requirements change, objects and policies are added, and settings that were originally required may no longer be necessary.

Regularly reviewing such an environment manually can be a time-consuming process.

Firewall Toolbox helps automate this process.

It imports configuration and diagnostic information from a SonicWall firewall, analyzes the collected data, and presents the results in structured reports.

The software can help administrators identify security risks, configuration issues, unused objects and policies, inconsistent settings, and other conditions that may otherwise be difficult to detect during a manual review.

In addition to analysis and auditing, Firewall Toolbox provides comprehensive reports that can be used to document the current firewall configuration.

For selected tasks, Firewall Toolbox can also communicate directly with the firewall through the **SonicWall API**. This allows administrators to perform certain maintenance and configuration operations directly from Firewall Toolbox.

The objective is to combine four important aspects of firewall administration in a single application:

Analyze – Audit – Document – Maintain

1.2 Who Is Firewall Toolbox For?

Firewall Toolbox is designed for anyone who regularly manages or reviews SonicWall firewalls.

Typical users include:

- Network and security administrators
- IT departments
- IT service providers
- System integrators
- Managed Service Providers (MSPs)
- SonicWall consultants
- Organizations that need to regularly audit or document their firewall environments

Firewall Toolbox can be particularly useful for IT service providers and consultants who manage multiple customer environments and need a consistent method for analyzing and documenting different SonicWall installations.

1.3 How Firewall Toolbox Works

Firewall Toolbox performs its analyses using information retrieved from the SonicWall firewall.

The two primary data sources are:

TSR – Tech Support Report

The TSR contains extensive diagnostic and operational information about the firewall, including system information, configuration details, status information, statistics, and other technical data.

EXP – Configuration Export

The EXP file contains the firewall configuration and provides Firewall Toolbox with additional information required for many of its analyses and documentation functions.

Both files can be selected and imported manually.

Alternatively, Firewall Toolbox can connect directly to the firewall through the **SonicWall API** and retrieve the required information automatically.

Using the API significantly simplifies the workflow, particularly when audits are performed regularly.

Optionally, Firewall Toolbox can also connect to **MySonicWall** to retrieve additional information that is not directly available from the firewall, such as information about available firmware versions.

Typical Workflow

A typical Firewall Toolbox audit consists of the following steps:

1. Retrieve or select the TSR and EXP files.
2. Import the firewall data into Firewall Toolbox.
3. Analyze and enrich the imported configuration data.
4. Automatically perform the available audit checks.
5. Generate the Full Audit Report.
6. Review findings and recommendations.
7. Generate additional reports where required.
8. Optionally use the API functions to perform selected maintenance or configuration tasks.

Most of these processes are automated. Once the firewall data has been imported, Firewall Toolbox can immediately begin analyzing the configuration and preparing the corresponding reports.

1.4 Main Areas of Firewall Toolbox

Firewall Toolbox Version 3 organizes its functions and reports into five main categories.

Security Audit

The Security Audit section examines configuration settings that may have an impact on the security of the firewall and the protected network.

It includes checks for firewall rules, security services, administrative access, VPN security, user permissions, logging, and other security-relevant settings.

Health

The Health section focuses on the operational state of the firewall.

Reports in this area provide information about system utilization, security service status, licensing, and other indicators that can help identify operational problems.

Configuration Audit

The Configuration Audit section examines important configuration and operational settings.

This includes areas such as firmware, High Availability, WAN failover, interfaces, VPN configuration, and other settings that influence the operation and reliability of the firewall.

Documentation

The Documentation section creates structured reports describing the current firewall configuration.

These reports can document firewall rules, NAT policies, address objects, interfaces, zones, users, groups, VPNs, and many other configuration elements.

They can be used for internal documentation, customer documentation, system handovers, troubleshooting, and future maintenance.

Maintenance

The Maintenance section helps administrators identify configuration elements that may require cleanup or modification.

Examples include unused address objects, disabled or unused policies, duplicate objects, naming inconsistencies, and modified TCP timeout settings.

Some maintenance tasks can also be performed directly from Firewall Toolbox using the SonicWall API.

1.5 Reports and Analysis

Firewall Toolbox provides both individual reports and combined reports.

Individual reports focus on a specific aspect of the firewall configuration, allowing administrators to investigate a particular area in detail.

Each of the five main categories also provides a **Summary Report**, combining the relevant analyses into a single document.

For a complete overview of the firewall, Firewall Toolbox can generate a **Full Audit Report**.

The Full Audit Report combines the different areas of analysis and documentation into one comprehensive document.

It begins with a **Highlights section** that summarizes important findings and recommendations. This allows critical or noteworthy results to be identified quickly before reviewing the detailed technical sections of the report.

1.6 Report Languages

The Firewall Toolbox user interface is provided in English.

Reports, however, can be generated in several languages:

- English
- German
- French
- Italian
- Spanish

The selected language applies not only to report headings and results, but also to explanatory information included with the reports.

These explanations describe the purpose of an analysis and provide additional context to help the reader understand and interpret the results.

This makes the reports suitable both for technical administrators and for recipients who may not work with SonicWall firewalls on a daily basis.

1.7 Using the SonicWall API

Firewall Toolbox can optionally establish an API connection to a SonicWall firewall.

The API is used for two primary purposes:

Retrieving information

Firewall Toolbox can automatically retrieve configuration and diagnostic information required for an audit.

Performing changes

Selected Firewall Toolbox functions allow configuration changes to be performed directly on the firewall.

Depending on the function, this can include operations such as:

- Disabling firewall rules
- Deleting firewall rules
- Disabling or deleting NAT policies
- Deleting unused address objects
- Resetting modified TCP timeout values

Firewall Toolbox provides selection and review steps before these operations are performed, allowing the administrator to determine exactly which objects or policies should be modified.

Before configuration changes are made, Firewall Toolbox also creates backups and records the corresponding operations to provide a recovery path if a change needs to be reversed.

Important: API-based configuration changes should only be performed by administrators who understand the purpose and potential impact of the selected operation.

The API functionality is covered in detail later in this guide.

1.8 About This User Guide

This guide describes the installation, configuration, and operation of Firewall Toolbox Version 3.

In addition to explaining how individual functions are used, the guide provides background information to help understand the purpose of the available analyses and reports.

Throughout the guide, additional information is highlighted using notes, tips, and warnings where appropriate.

Note
Provides additional information about a function or configuration.

Tip
Provides practical recommendations that can simplify a task or improve the workflow.

Important
Highlights information that should be considered before continuing.

Warning
Indicates an operation that may modify the firewall configuration or otherwise have a significant impact.

The following chapters begin with the installation and initial configuration of Firewall Toolbox before introducing the normal workflow and individual analysis, documentation, and maintenance functions.

2. Installation and First Start

This chapter describes how to install Firewall Toolbox, activate the software, and configure the basic settings required before performing the first firewall analysis.

2.1 System Requirements

Firewall Toolbox is a Windows desktop application.

Before installing the software, make sure that the computer meets the required system requirements and that sufficient permissions are available to install and run the application.

Firewall Toolbox requires access to local storage for application data, reports, configuration backups, and firewall repository files.

If the integrated API functionality is used, the computer must also be able to establish an HTTPS connection to the management interface of the SonicWall firewall.

For optional MySonicWall functionality, Internet access is required.

Note:
Communication with a SonicWall firewall through the API requires network connectivity between the computer running Firewall Toolbox and the firewall management interface. The SonicWall API must also be enabled on the firewall. For detailed instructions check the “Configuration steps for API Connection to Firewall” in Appendix

---

2.2 Installing Firewall Toolbox

Firewall Toolbox is provided with a Windows installation program.

Start the installer and follow the instructions displayed by the setup wizard.

Depending on the Windows security configuration, administrator privileges may be required during installation.

After the installation has been completed, Firewall Toolbox can be started from the Windows Start menu or from a shortcut created during installation.

Important:
When upgrading an existing Firewall Toolbox installation, make sure that important reports, firewall repositories, and configuration backups are stored in their designated data directories and are included in your normal backup procedures.

2.3 Starting Firewall Toolbox

When Firewall Toolbox is started, the main application window is displayed.

The available functions depend on the installed version, license status, and whether firewall configuration data has already been imported.

Before performing the first audit, it is recommended to review the application settings.

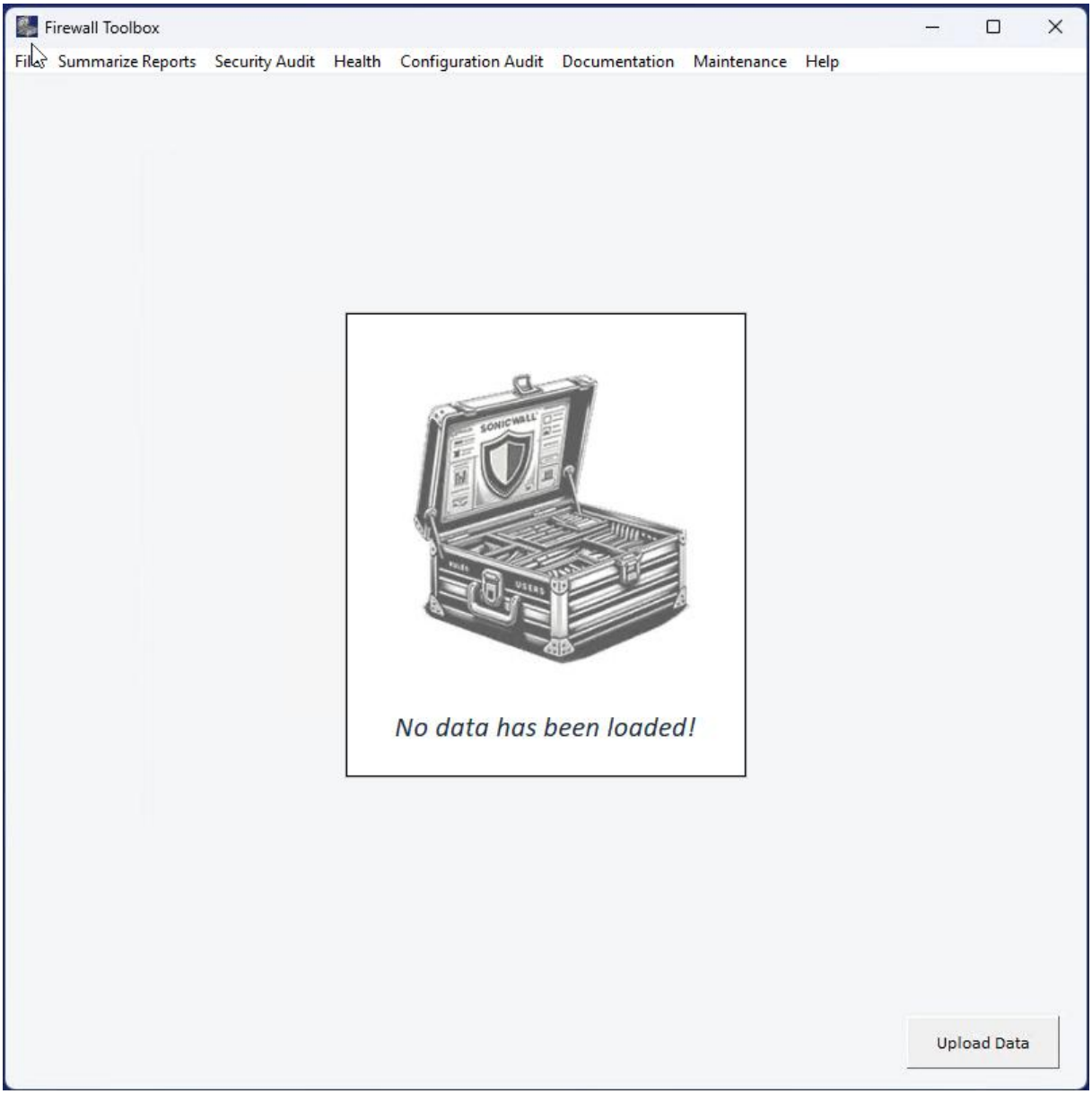


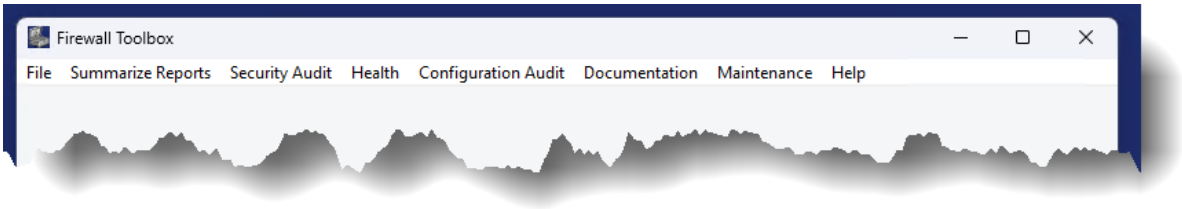
Figure 1: First start with empty database

The main window provides access to the different analysis and reporting categories as well as the configuration and management functions of Firewall Toolbox.

The user interface is divided into five main areas:

- Security Audit
- Health
- Configuration Audit
- Documentation
- Maintenance

These areas and their individual functions are described in detail later in this guide.

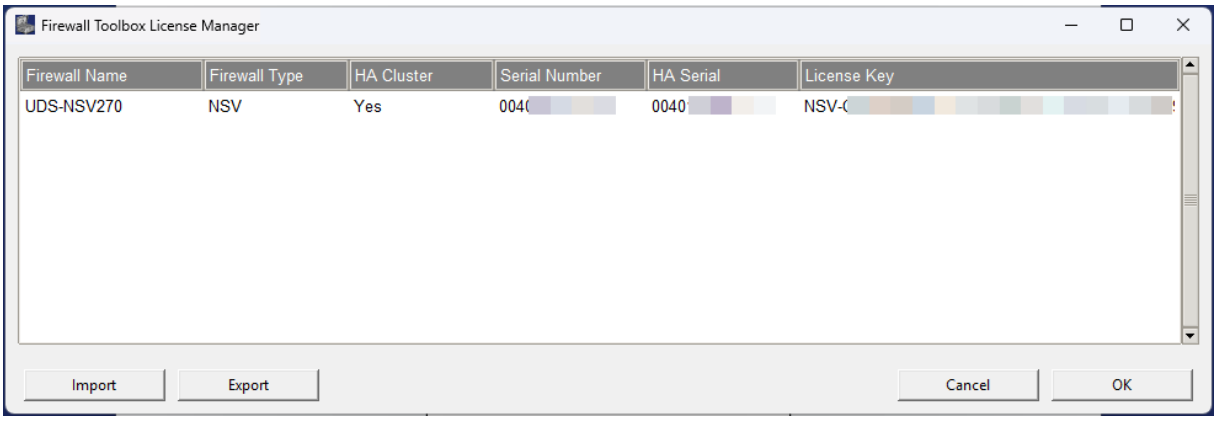


2.4 Licensing Firewall Toolbox

Firewall Toolbox requires a valid license for full functionality.

Depending on the license and software version, Firewall Toolbox can be operated as a licensed installation or as a trial version.

The current license information can be viewed through the **License Manager**.



The License Manager provides information about the current license status and the licensed Firewall Toolbox installation.

If a license has not yet been activated, the corresponding activation options are available from this dialog.

Note:
The trial version can be used to evaluate Firewall Toolbox before purchasing a license. Some reports or functions may not be available in the trial version or reports may be shortened to only show a few entries.

2.5 Firewall Repository

Firewall Toolbox uses a repository to store information and files associated with analyzed firewalls.

When configuration data is imported, Firewall Toolbox can create a dedicated directory for the firewall. This provides a central location for files associated with that particular system.

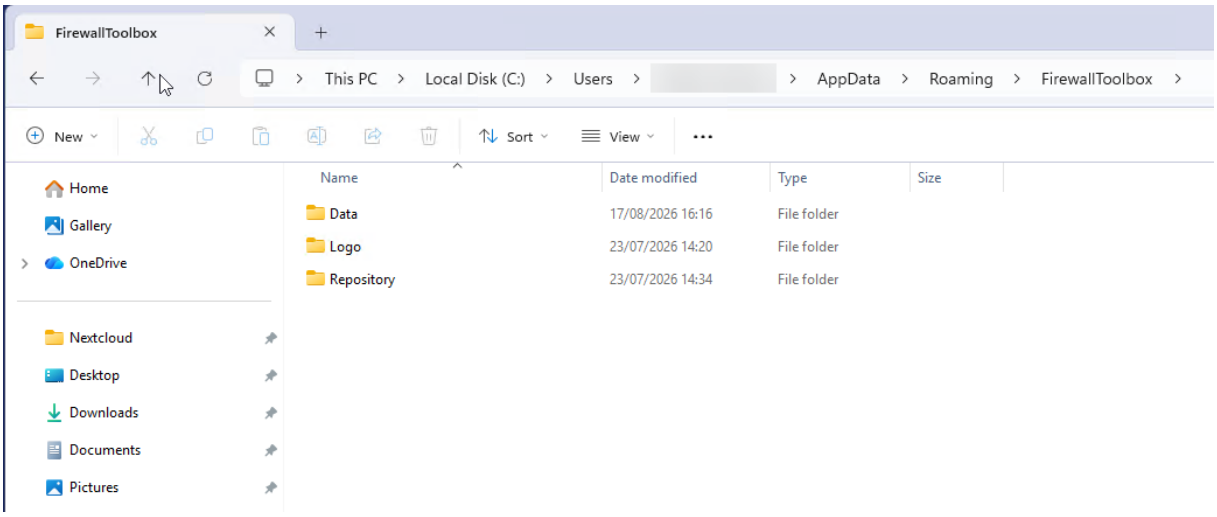
Depending on the operation being performed, the repository may contain items such as:

- TSR files

- EXP configuration files
- Configuration backups
- API operation information
- Generated or related firewall data

This structure is particularly useful when Firewall Toolbox is used to manage or audit multiple firewalls.

Instead of keeping configuration exports and diagnostic files in unrelated directories, the repository provides a consistent structure for each firewall.



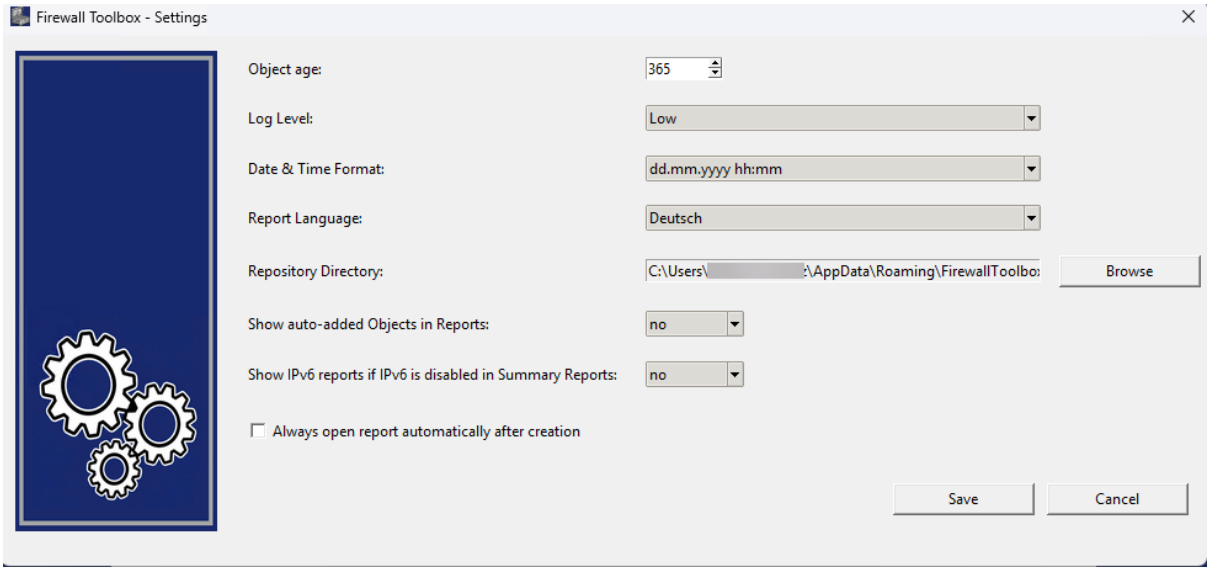
Tip:
Store the Firewall Toolbox repository in a location that is included in your regular backup strategy. Firewall configuration exports may be extremely useful when troubleshooting changes or reviewing the historical configuration of a system.

If multiple users are working with Firewall Toolbox, move the repository to a shared directory that is accessible to all users. The repository location can be changed in the Firewall Toolbox settings.

2.6 Basic Settings

Before importing the first firewall, review the Firewall Toolbox settings.

The available settings control both the application behavior and the contents of generated reports.



Settings include options for:

- Repository location
- Report language
- Date and time format
- IPv6 reports
- Display of default configuration elements
- Display of automatically added firewall rules or NAT policies
- Report appearance
- Logging
- MySonicWall integration

Not every setting needs to be changed before using Firewall Toolbox. In most environments, the default settings provide a suitable starting point.

Individual settings and their effects are described in more detail in the **Settings and Customization** chapter.

2.7 Selecting the Report Language

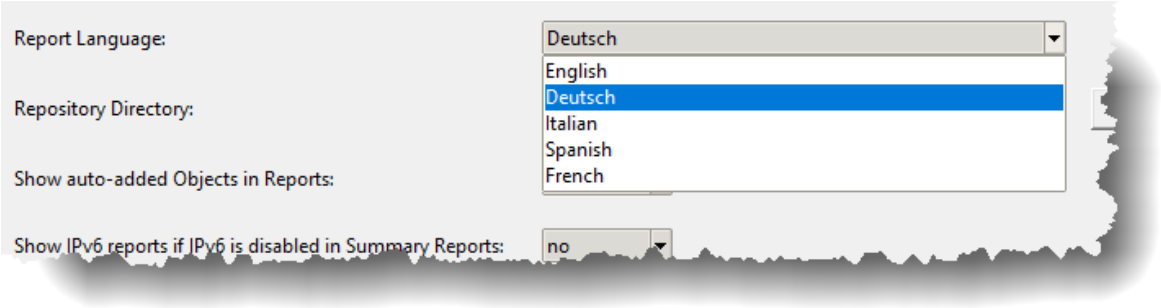
The Firewall Toolbox user interface is displayed in English, while generated reports can be created in different languages.

Depending on the installed version, the following report languages are available:

- English
- German
- French
- Italian

- Spanish

The selected language is used for report content as well as the explanatory text included with individual analyses.



Changing the report language does not modify the imported firewall configuration or the Firewall Toolbox user interface. It only affects subsequently generated reports.

Tip:
The report language can be selected according to the intended recipient. For example, an administrator may work with the English user interface while generating a German, French, Italian, or Spanish report for a customer.

2.8 Preparing a SonicWall for API Access

Using the SonicWall API is optional. Firewall Toolbox can also analyze configuration files that have been exported manually.

However, enabling API access provides a much more convenient workflow.

With an API connection, Firewall Toolbox can retrieve the required firewall information directly and can also perform supported maintenance operations.

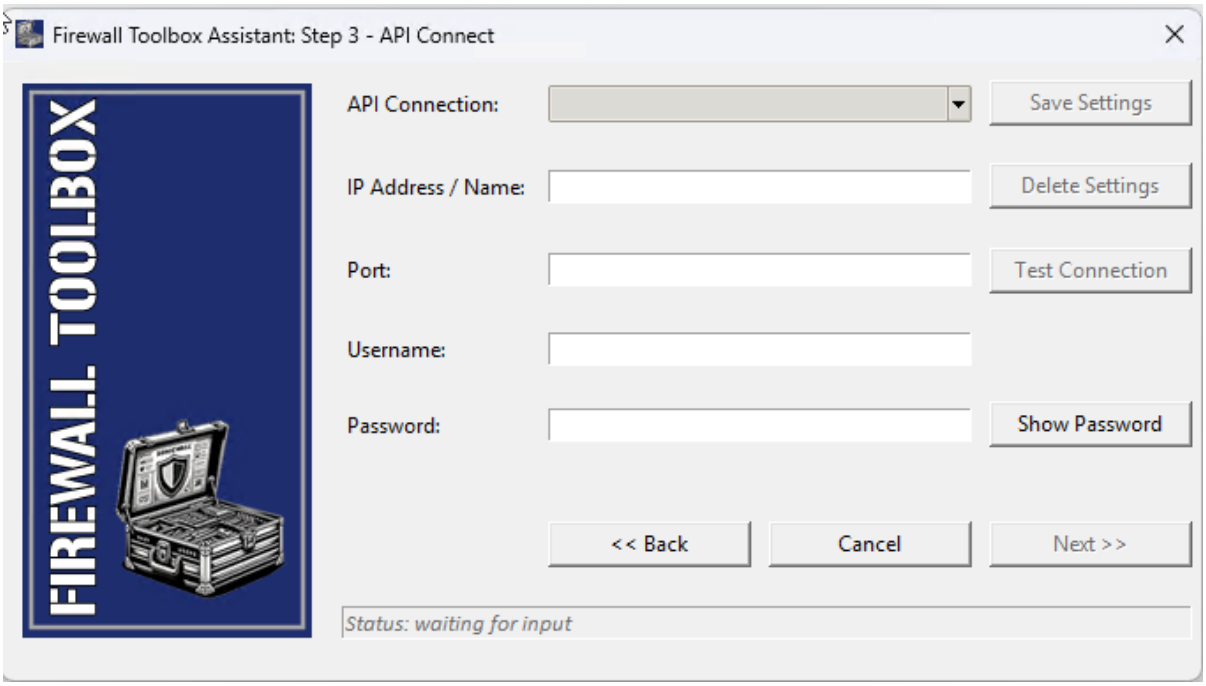
Before an API connection can be established, API access must be enabled on the SonicWall firewall.

The administrator account used for the connection must have sufficient permissions for the intended operations.

Firewall Toolbox requires the following information when establishing a connection:

- Firewall IP address or hostname
- Management HTTPS port
- Username
- Password

Starting Version 3.1, authentication with 2 Factor Auth is possible as well. The user needs to have access to the device generating the 2FA Code.



Depending on the environment and certificate configuration, additional SSL certificate handling may be required.

Security Note:
A dedicated administrative account for API access can be useful in environments where administrative activities need to be clearly separated or audited.

Important:
The permissions assigned to the API account determine which operations can be performed. Read-only analysis and configuration-changing operations may require different levels of administrative access. For Firewall Toolbox, a full admin user is required!

Note:
A detailed description about the configuration steps required on the Firewall can be found in Appendix.

2.9 Testing the API Connection

After entering the firewall connection information, Firewall Toolbox attempts to establish an HTTPS connection and authenticate against the SonicWall API.

A successful connection confirms that:

- The firewall can be reached from the computer
- The specified HTTPS management port is accessible
- API access is available
- The supplied credentials are accepted

If the connection cannot be established, verify the network connection, management port, API configuration, credentials, and SSL settings.

Detailed troubleshooting information is provided later in this guide.

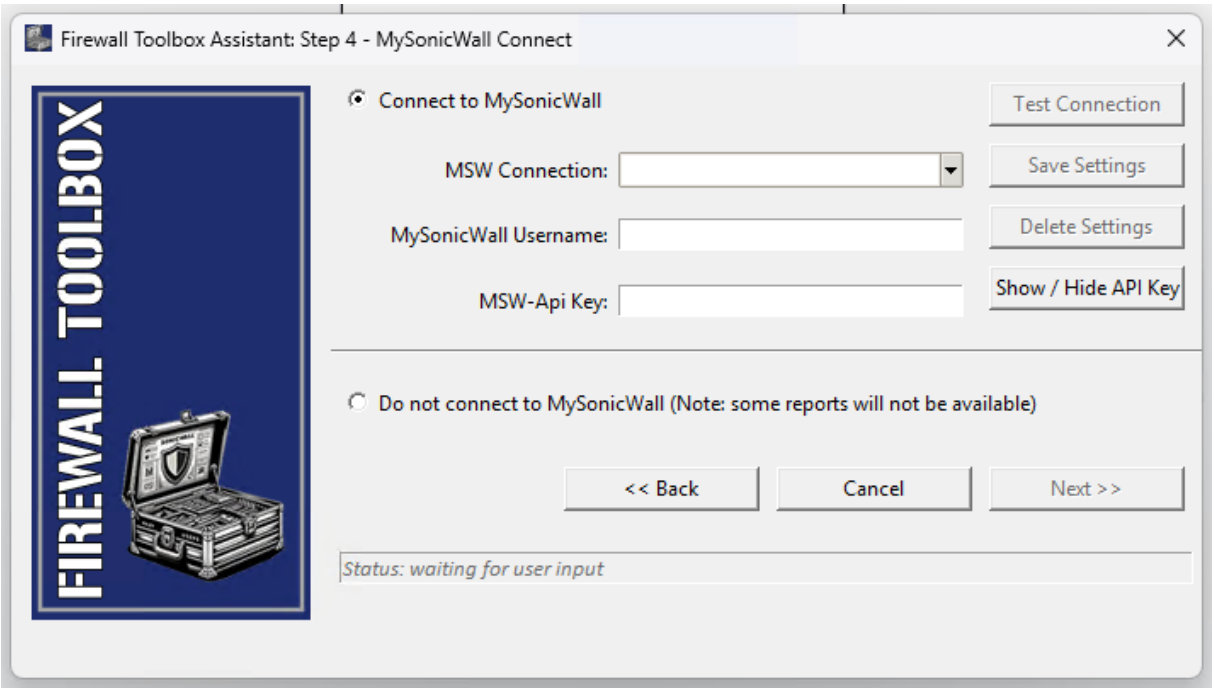
Tip:
If the Firewall Toolbox computer and the firewall are located in different networks, verify that the required management access is permitted before troubleshooting the application itself.

2.10 MySonicWall Integration

Firewall Toolbox can optionally use information from MySonicWall.

This integration provides additional information that may not be available directly from the firewall configuration.

For example, Firewall Toolbox can use MySonicWall information when checking whether newer firmware versions are available for a firewall.



MySonicWall integration is optional and is not required for the basic analysis of TSR and EXP files.

If MySonicWall integration is not configured, functions that depend on this information may be unavailable or may provide limited results.

Note:
A detailed description about the configuration steps required on the Firewall can be found in Appendix.

2.11 Ready for the First Audit

Once Firewall Toolbox has been installed and the basic settings have been reviewed, the application is ready to analyze the first firewall.

There are two primary ways to provide the required firewall data:

Manual Import

Existing TSR and EXP files are selected from the local computer and imported into Firewall Toolbox.

API Download

Firewall Toolbox connects directly to the SonicWall firewall and retrieves the required data automatically.

Regardless of how the files are obtained, the subsequent analysis process is largely the same.

During the import, Firewall Toolbox processes and analyzes the configuration data and prepares the information required by the individual reports.

With Version 3, the analysis process also automatically generates the **Full Audit Report**, allowing the first results to be reviewed immediately after the import has been completed.

The next chapter describes this process in detail and walks through the **first firewall audit** step by step.

3. Getting Started – Your First Firewall Audit

This chapter provides a practical introduction to Firewall Toolbox by walking through a complete firewall audit from start to finish.

The objective is to import the configuration of a SonicWall firewall, allow Firewall Toolbox to analyze the data, and open the automatically generated **Full Audit Report**.

There are two ways to obtain the required firewall data:

- Manually import existing TSR and EXP files
- Download the required files directly from the firewall using the SonicWall API

Both methods result in the same analysis process.

3.1 Required Firewall Data

Firewall Toolbox primarily uses two files from the SonicWall firewall:

TSR – Tech Support Report

The TSR contains detailed technical and operational information about the firewall. This includes system information, status information, statistics, configuration details, and other diagnostic data.

EXP – Configuration Export

The EXP file contains the firewall configuration and provides additional information required for analysis and documentation.

For the most complete analysis, both files should originate from the same firewall and should have been created at approximately the same time.

Important:
Using TSR and EXP files from different points in time may result in inconsistencies. For example, a firewall rule contained in the EXP file may no longer correspond to the operational information contained in an older TSR file.

Firewall Toolbox compares the creation dates of both files. If the time difference between the TSR and EXP files exceeds a defined threshold, a warning is displayed.

3.2 Starting the Data Import

The import function is used to load firewall information into Firewall Toolbox.

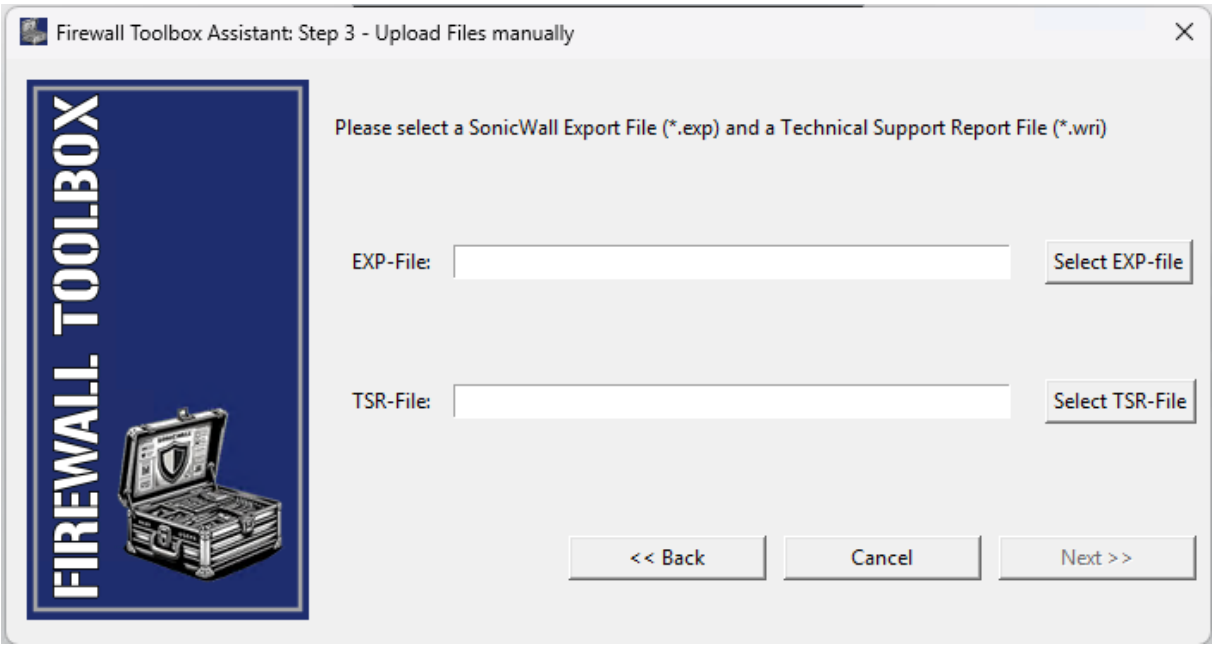
Depending on how the firewall data is available, select either the manual file import or the API-based download.

After the files have been selected or downloaded, Firewall Toolbox begins processing the configuration.

3.3 Manual Import of TSR and EXP Files

If the TSR and EXP files have already been obtained from the firewall, they can be imported manually.

Select the corresponding import function and specify the location of the two files.



Note:
If an exp file is selected and in the same directory an TSR File exists, it will be automatically selected.

Firewall Toolbox verifies and processes the selected files before importing the contained information.

This method is useful when:

- Direct network access to the firewall is not available
- API access is disabled
- Configuration files have been provided by a customer
- An archived firewall configuration needs to be analyzed
- An offline analysis is required

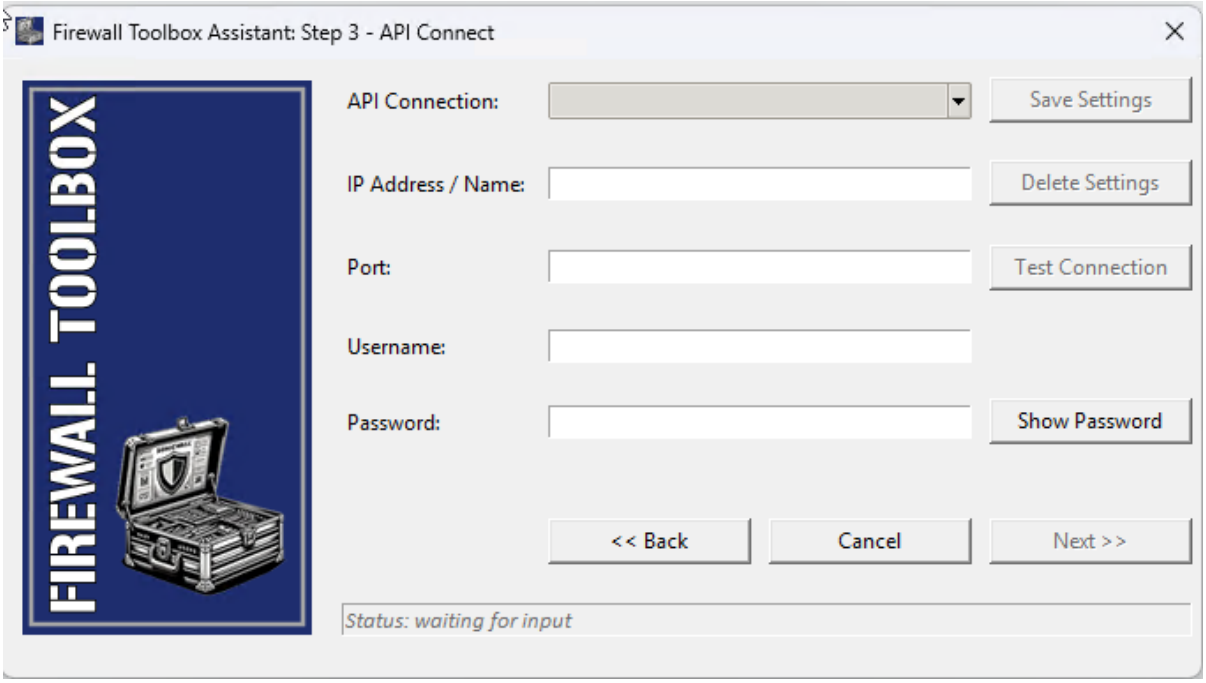
Once the files have been selected, start the import process.

3.4 Downloading the Data Through the SonicWall API

If API access has been configured, Firewall Toolbox can retrieve the required firewall data directly.

This avoids having to manually log in to the firewall, create the files, download them, and select them in Firewall Toolbox.

Enter or select the API connection information for the firewall and start the download.

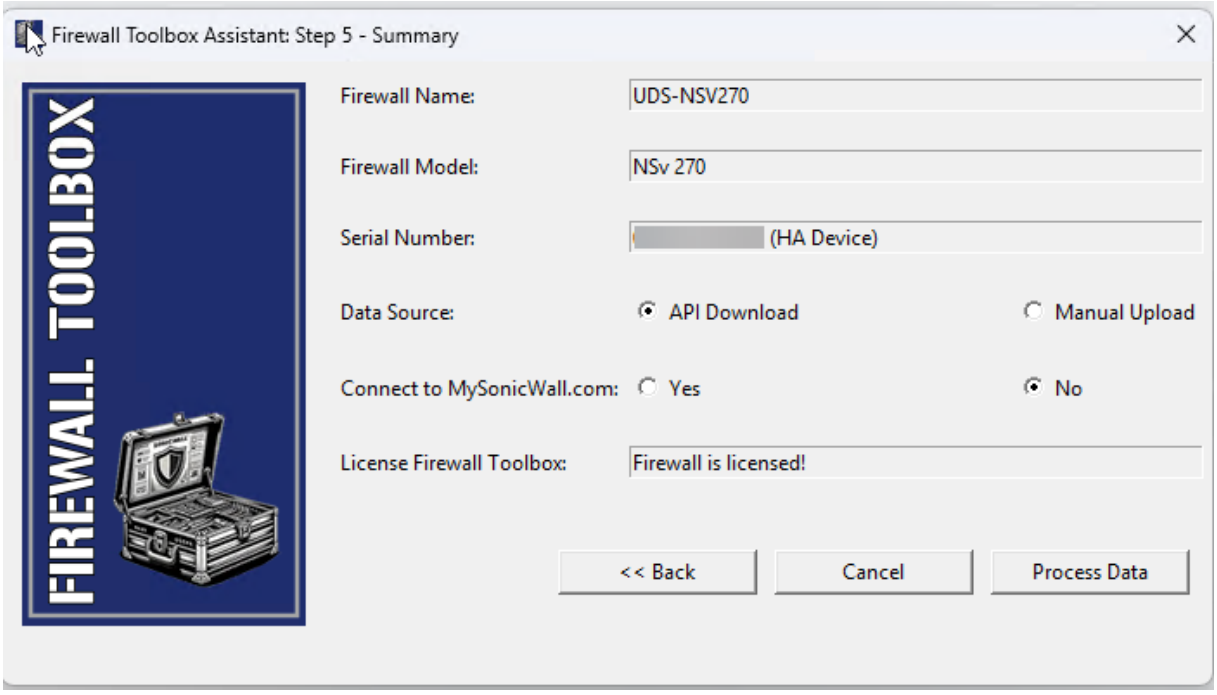


Firewall Toolbox connects to the firewall and retrieves the information required for the analysis.

The downloaded TSR and EXP files are also stored in the firewall repository, providing a copy of the configuration used for the audit.

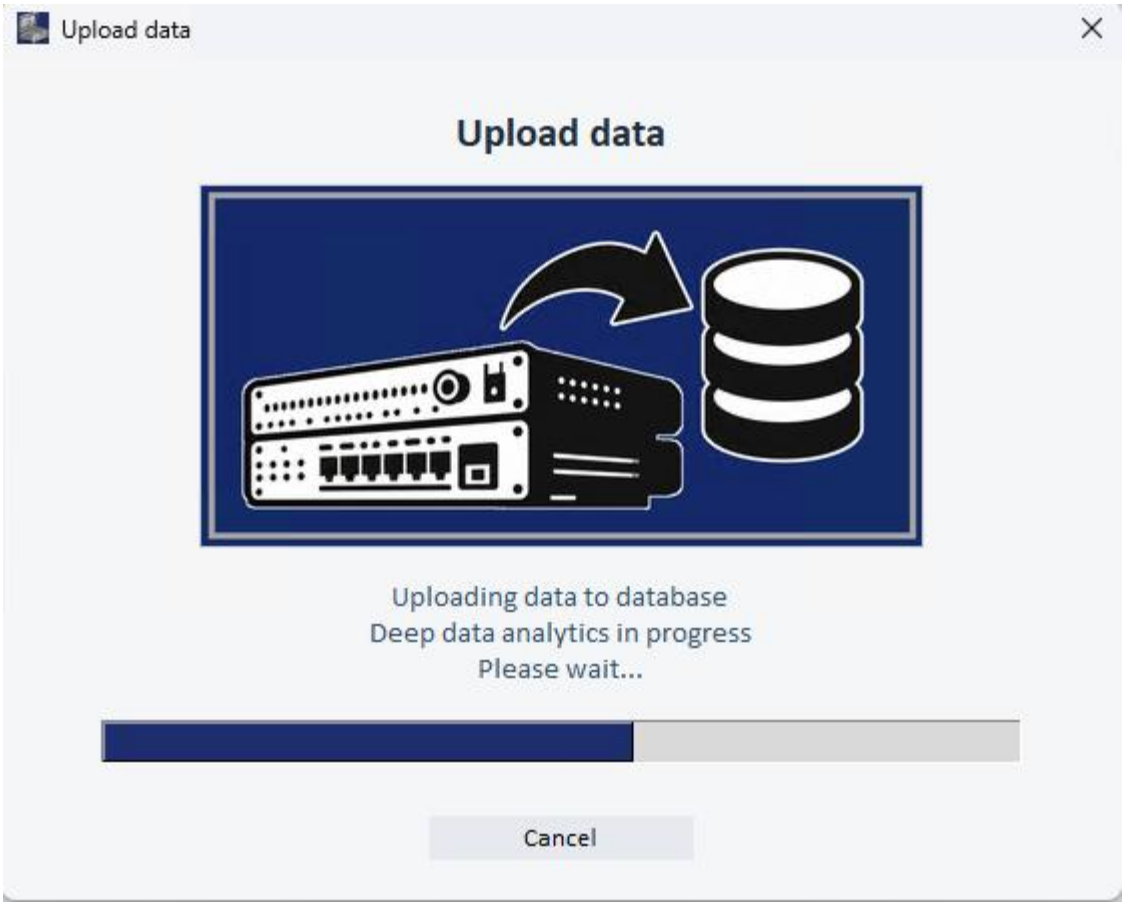
Tip:
API download is particularly useful when audits are performed regularly. It reduces the number of manual steps and ensures that the TSR and EXP files used for the analysis represent the firewall at approximately the same point in time.

3.5 Importing and Analyzing the Configuration



After the TSR and EXP files have been selected or downloaded, Firewall Toolbox starts importing the data.

During this process, the information contained in the files is processed and prepared for the different analysis and reporting functions.



Firewall Toolbox performs a number of processing and analysis tasks during the import.

Depending on the configuration, these can include:

- Processing firewall rules
- Processing NAT policies
- Processing address objects and groups
- Analyzing interfaces and zones
- Processing users and groups
- Analyzing VPN information
- Processing security service information
- Analyzing firmware information
- Identifying relationships between configuration objects
- Preparing data for the individual audit reports

The progress indicator shows the current state of the operation.

The amount of time required depends on the size and complexity of the firewall configuration and the available system resources.

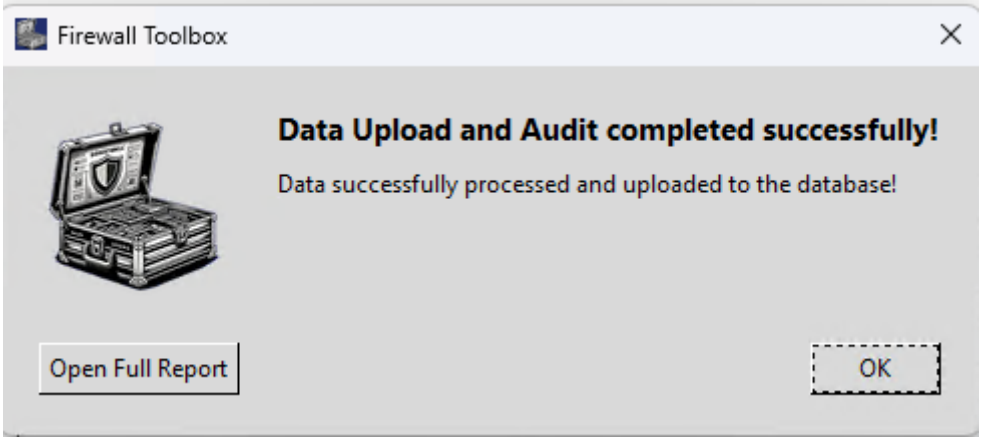
3.6 Automatic Full Audit

With Firewall Toolbox Version 3, the audit process starts automatically as part of the data import.

While the configuration data is being processed, Firewall Toolbox performs the analyses required for the **Full Audit Report**.

This means that there is no need to start a separate full audit after importing the firewall.

Once processing has been completed, the complete report is immediately available.



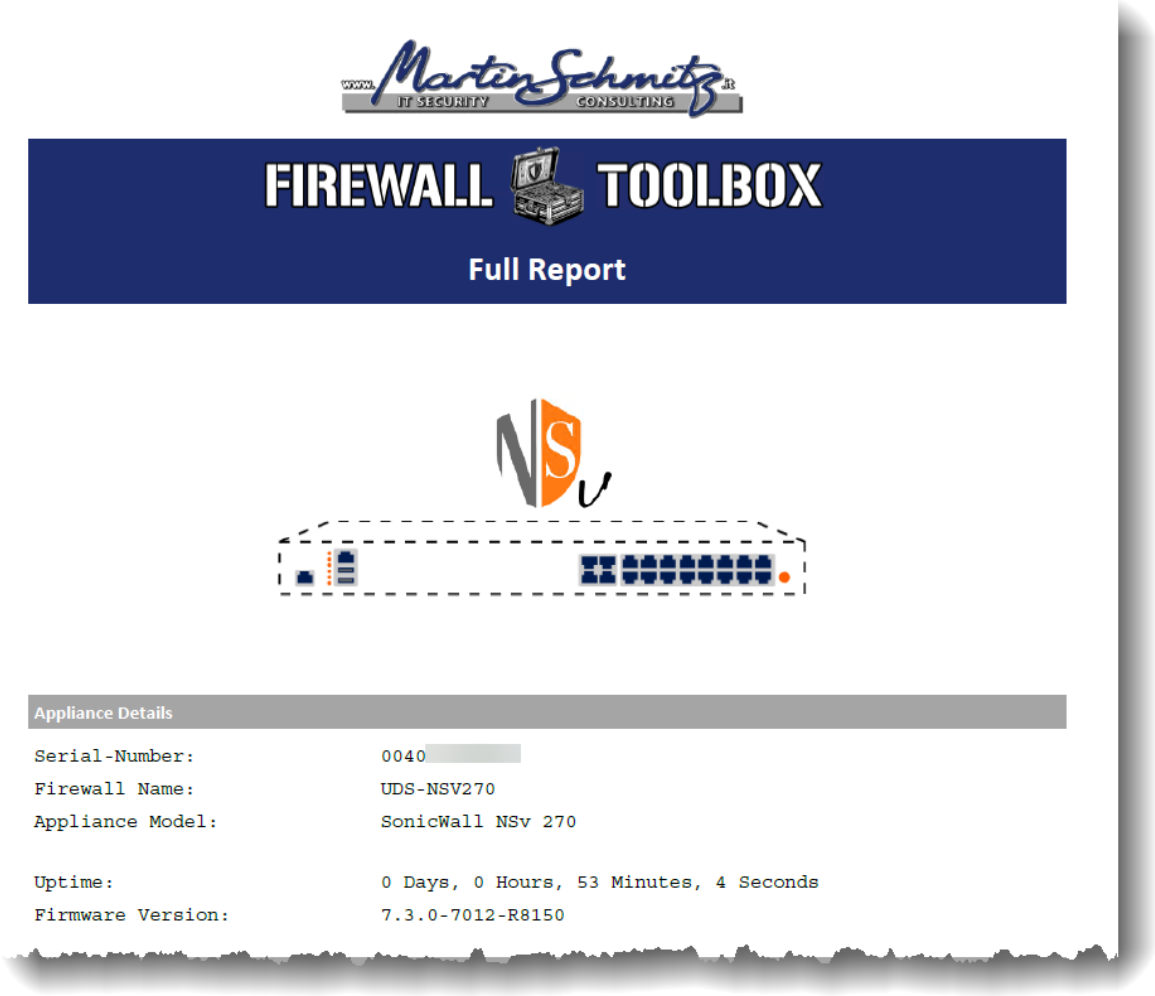
From the completion dialog, select **Open Full Report** to open the generated report.

This provides the quickest way to move from a firewall configuration to a complete analysis.

3.7 The Full Audit Report

The Full Audit Report combines the major analysis and documentation areas of Firewall Toolbox into a single document.

Rather than opening each individual report separately, the Full Audit Report provides a comprehensive overview of the firewall in one document.



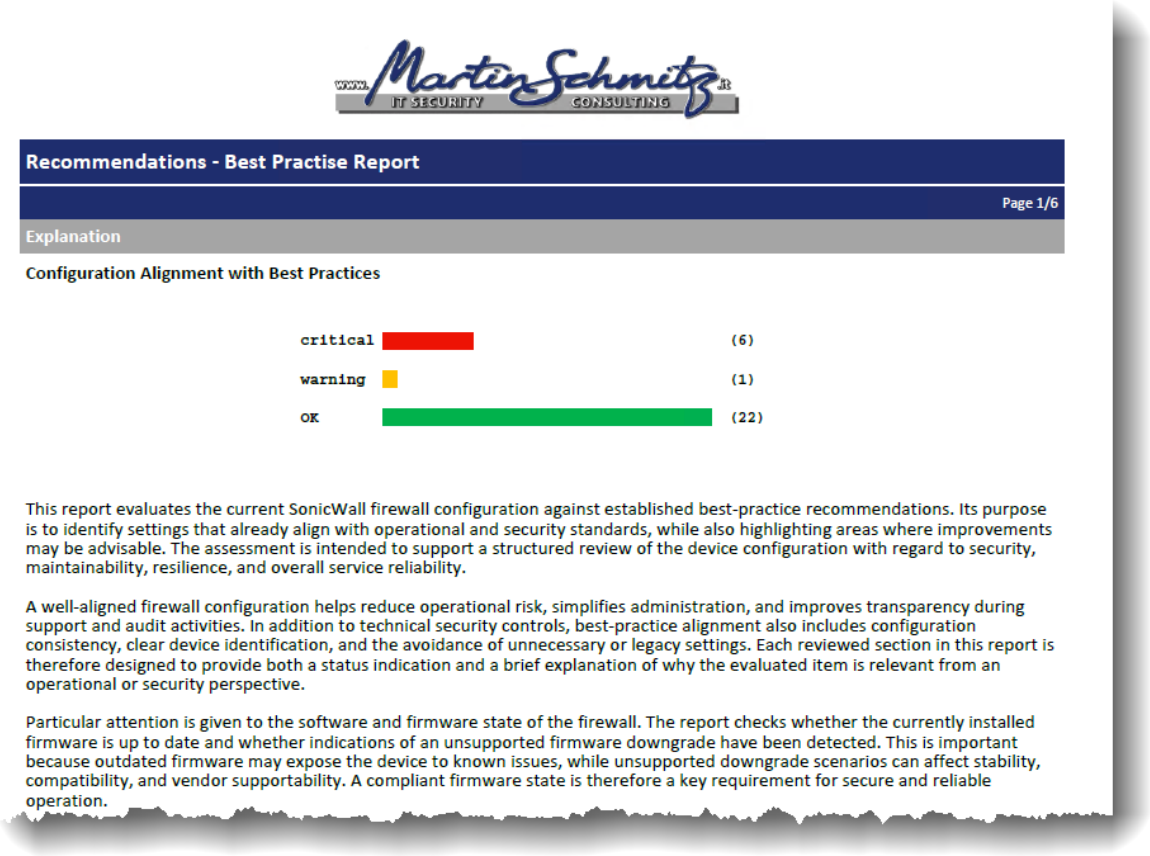
The report contains information from the main Firewall Toolbox categories:

- Security Audit
- Health
- Configuration Audit
- Documentation
- Maintenance

The individual sections contain both the results of the analyses and explanatory information that helps the reader understand the purpose and relevance of each check.

3.8 Highlights and Recommendations

One of the first sections of the Full Audit Report provides a consolidated overview of important findings identified during the analysis.



Recommendations - Best Practise Report

Page 1/6

Explanation

Configuration Alignment with Best Practices

critical		(6)
warning		(1)
OK		(22)

This report evaluates the current SonicWall firewall configuration against established best-practice recommendations. Its purpose is to identify settings that already align with operational and security standards, while also highlighting areas where improvements may be advisable. The assessment is intended to support a structured review of the device configuration with regard to security, maintainability, resilience, and overall service reliability.

A well-aligned firewall configuration helps reduce operational risk, simplifies administration, and improves transparency during support and audit activities. In addition to technical security controls, best-practice alignment also includes configuration consistency, clear device identification, and the avoidance of unnecessary or legacy settings. Each reviewed section in this report is therefore designed to provide both a status indication and a brief explanation of why the evaluated item is relevant from an operational or security perspective.

Particular attention is given to the software and firmware state of the firewall. The report checks whether the currently installed firmware is up to date and whether indications of an unsupported firmware downgrade have been detected. This is important because outdated firmware may expose the device to known issues, while unsupported downgrade scenarios can affect stability, compatibility, and vendor supportability. A compliant firmware state is therefore a key requirement for secure and reliable operation.

This section is designed to provide a quick overview without requiring the reader to immediately review the complete technical report.

Depending on the firewall configuration, it may highlight items such as:

- Security-related findings
- Configuration issues
- Maintenance recommendations
- Unusual or inconsistent settings
- Items that should be reviewed by an administrator

The detailed sections later in the report provide the additional information required to investigate each finding.

Tip:
Start with the Highlights and Recommendations section when reviewing a firewall for the first time. It provides a useful overview of the areas that deserve immediate attention.

Important:
A recommendation does not automatically mean that a configuration is incorrect. Firewall configurations are highly dependent on the environment and its requirements. Findings should therefore always be evaluated in the context of the individual network.

3.9 Using the Table of Contents

The Full Audit Report contains a table of contents to simplify navigation through the different sections.

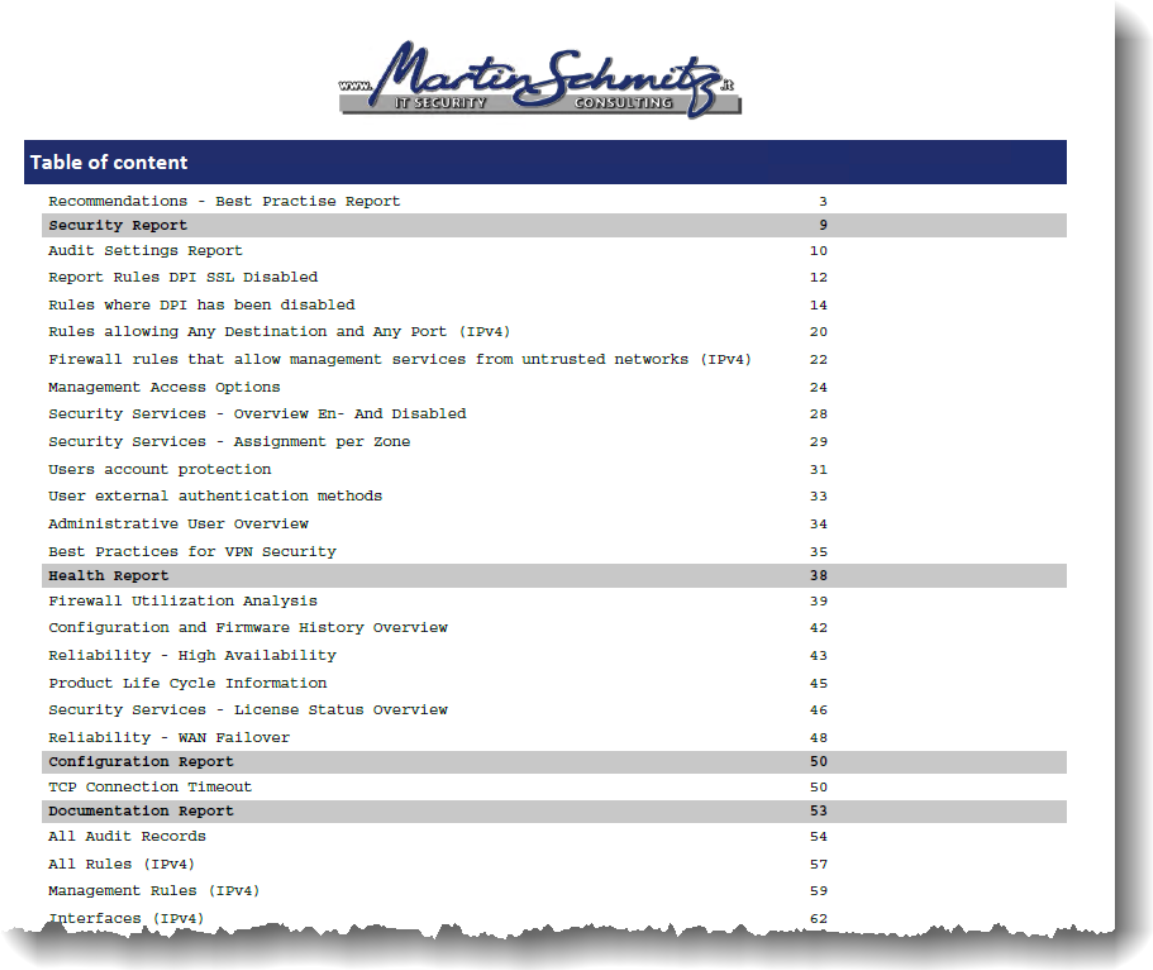


Table of content

Recommendations - Best Practise Report	3
Security Report	**9**
Audit Settings Report	10
Report Rules DPI SSL Disabled	12
Rules where DPI has been disabled	14
Rules allowing Any Destination and Any Port (IPv4)	20
Firewall rules that allow management services from untrusted networks (IPv4)	22
Management Access Options	24
Security Services - Overview En- And Disabled	28
Security Services - Assignment per Zone	29
Users account protection	31
User external authentication methods	33
Administrative User Overview	34
Best Practices for VPN Security	35
Health Report	**38**
Firewall Utilization Analysis	39
Configuration and Firmware History Overview	42
Reliability - High Availability	43
Product Life Cycle Information	45
Security Services - License Status Overview	46
Reliability - WAN Failover	48
Configuration Report	**50**
TCP Connection Timeout	50
Documentation Report	**53**
All Audit Records	54
All Rules (IPv4)	57
Management Rules (IPv4)	59
Interfaces (IPv4)	62

The report is organized according to the same logical categories used in the Firewall Toolbox user interface.

This makes it easy to move between the application and the corresponding sections of the report.

For example, if a finding relates to firewall rules, the detailed information can be located in the corresponding Security Audit or Documentation section.

3.10 Understanding Individual Reports

Most individual reports follow a similar structure.

A report generally consists of:

Report Title

Identifies the configuration area or condition being analyzed.

Explanation

Describes what the report checks and why the configuration may be relevant.

Results

Lists the configuration elements or findings detected by the analysis.

Depending on the report, additional information may be provided to help evaluate the result.

User external authentication methods

Explanation

External Authentication Configuration Overview
This report lists which external authentication systems are configured, whether they are enabled, and highlights any potential security concerns related to their setup. External authentication can significantly strengthen user identity management when implemented correctly, but improper configuration may introduce security and operational risks.

LDAP (Lightweight Directory Access Protocol)
When LDAP is used, authentication requests are forwarded to an external directory such as Microsoft Active Directory. Using LDAP centralizes user identity and password management, reducing local account dependency. However, LDAP authentication should always be secured through TLS (LDAPS). Unencrypted LDAP communication exposes usernames, passwords, and group membership information to interception, increasing risk of credential theft.

RADIUS Authentication
RADIUS is commonly used for VPN access and central authentication services. It supports challenge-response methods, central logging, and standardized enforcement of authentication policies. Security risks arise when shared secrets are weak or reused across multiple systems. Additionally, if RADIUS servers become unavailable, access could be disrupted unless proper fallback mechanisms are configured.

TACACS+ Authentication
TACACS+ is typically used for administrative authentication, especially in enterprise environments. It separates authentication, authorization, and accounting functions (AAA), which ensures traceable administrator activity and granular privilege control. Although secure in design, TACACS+ requires proper configuration of encrypted channels and unique keys. Central TACACS+ outages can block administrative access unless redundancy is in place.

Properly configuring and securing external authentication systems helps improve accountability, reduce management complexity, and enhance overall access security. Regular review of availability, encryption settings, authentication policy mapping, and fallback behavior ensures reliable and secure authentication processes across the environment.

LDAP

Server	Enabled	TLS	UserName
udsserver.uds.local	on	on	UDSReadDir

Radius

Server	Enabled	VPN
10.10.33.11	off	off(!)

Tacacs

Server	Enabled	VPN

This consistent structure makes it easier to understand reports even when the reader is not familiar with every SonicWall configuration option.

3.11 No Finding Does Not Always Mean No Risk

Firewall Toolbox performs automated analyses based on the available configuration and diagnostic information.

These analyses can identify many common configuration issues, security concerns, maintenance requirements, and deviations from recommended configurations.

However, an automated audit cannot determine every requirement of an individual network.

For example, Firewall Toolbox may identify a permissive firewall rule, but only the administrator can determine whether that rule is actually required for a specific business application.

Similarly, the absence of a finding does not guarantee that a firewall or network is completely secure.

Firewall Toolbox should therefore be used as a tool to support technical review and decision-making, rather than as a replacement for professional security assessment.

3.12 Running Individual Reports

After the initial audit, individual reports can be generated at any time without importing the firewall data again.

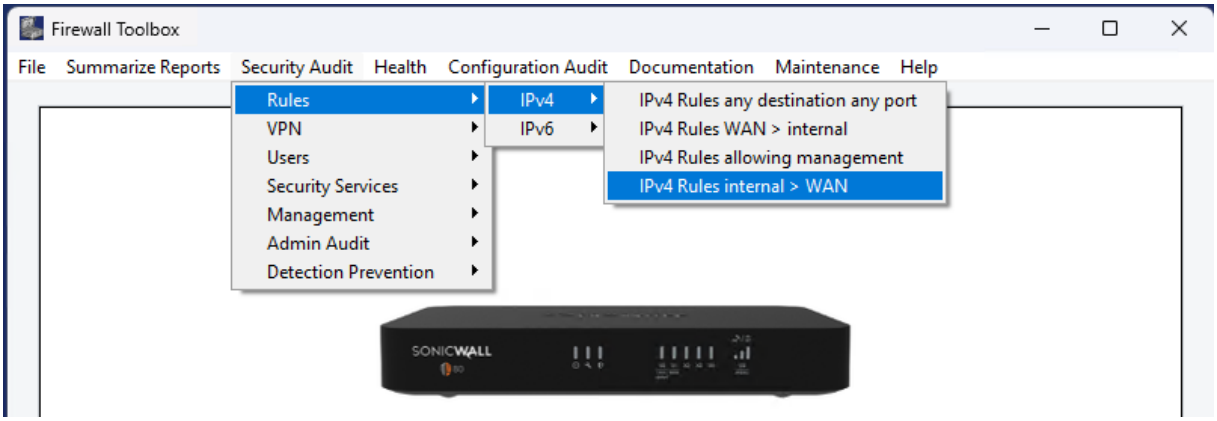
Navigate to the appropriate category and select the required report.

For example:

Security Audit → [Report]

or

Maintenance → [Report]



This is useful when investigating a specific configuration area or when only a particular section needs to be provided to a customer or colleague.

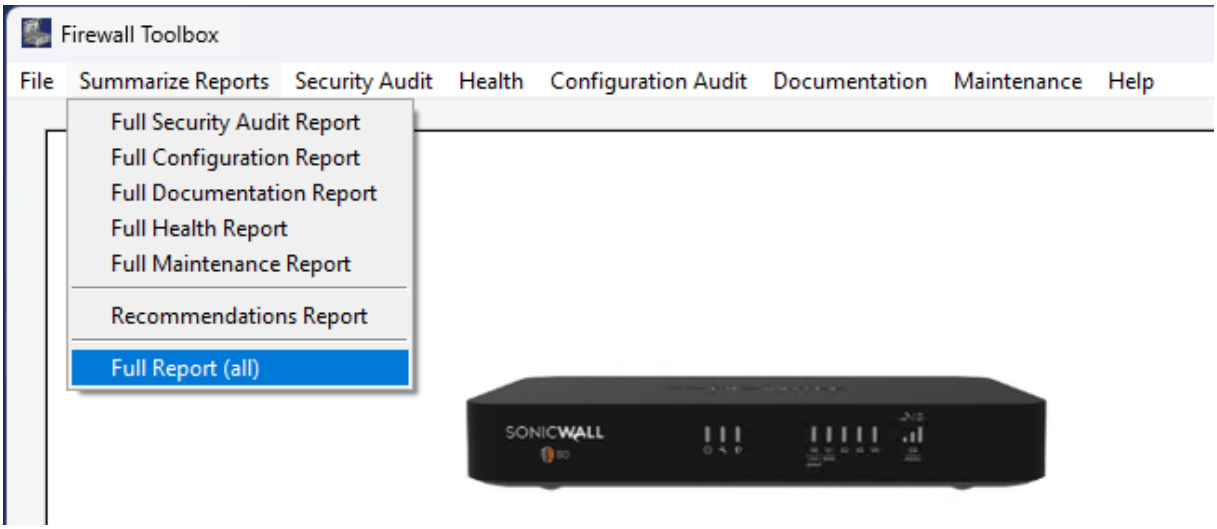
3.13 Category Summary Reports

In addition to individual reports and the Full Audit Report, each of the five main categories provides a combined summary report.

These reports include the relevant analyses for that specific category.

For example, the **Security Audit Summary** provides a consolidated security-focused report without including the complete documentation and maintenance sections.

Category reports are useful when the recipient is interested only in a specific aspect of the firewall.



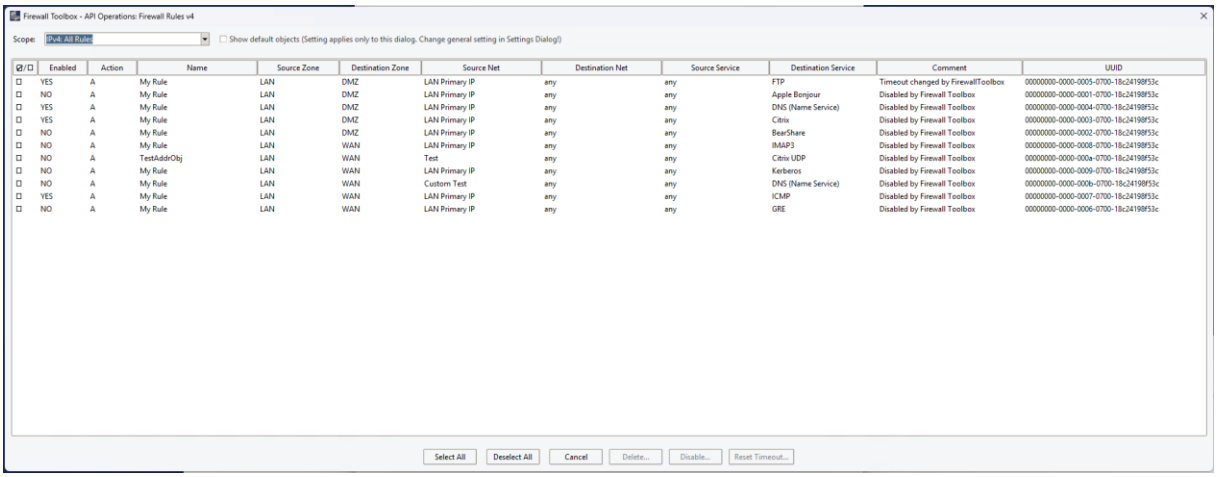
3.14 Making Changes Based on Audit Results

Some findings identified by Firewall Toolbox can be addressed directly through the integrated SonicWall API functions.

For example, Firewall Toolbox can assist with tasks such as:

- Disabling unused firewall rules
- Deleting unused firewall rules
- Disabling or deleting NAT policies
- Deleting unused address objects
- Resetting modified TCP timeout values

Where supported, Firewall Toolbox allows the administrator to review the affected objects and select which items should be modified.



Warning:
API operations modify the active firewall configuration. Always review the selected objects and the potential impact before executing an operation.

Firewall Toolbox creates configuration backups and records API operations before making supported configuration changes.

The complete API workflow and recovery mechanisms are described in the **Working with the SonicWall API** chapter.

3.15 The Recommended Audit Workflow

For most environments, the following workflow provides a practical approach:

1. Obtain the current TSR and EXP files, preferably through the API.
2. Import the files into Firewall Toolbox.
3. Wait for the automatic analysis to complete.
4. Open the Full Audit Report.
5. Review the Highlights and Recommendations first.
6. Investigate relevant findings in the detailed report sections.
7. Generate individual or category reports where additional analysis is required.
8. Decide which findings require configuration changes.
9. Use the API functions for supported changes where appropriate.
10. Verify the firewall configuration after making changes.

This approach separates **analysis** from **configuration changes**.

Firewall Toolbox first provides the information required to understand the current state of the firewall. The administrator can then decide which changes are appropriate for the individual environment.

3.16 Next Steps

After completing the first audit, the next step is to become familiar with the Firewall Toolbox user interface and the organization of its functions.

The following chapter introduces the **main application window, menus, firewall selection, report categories, and other navigation elements** used throughout Firewall Toolbox.

4. Understanding the User Interface

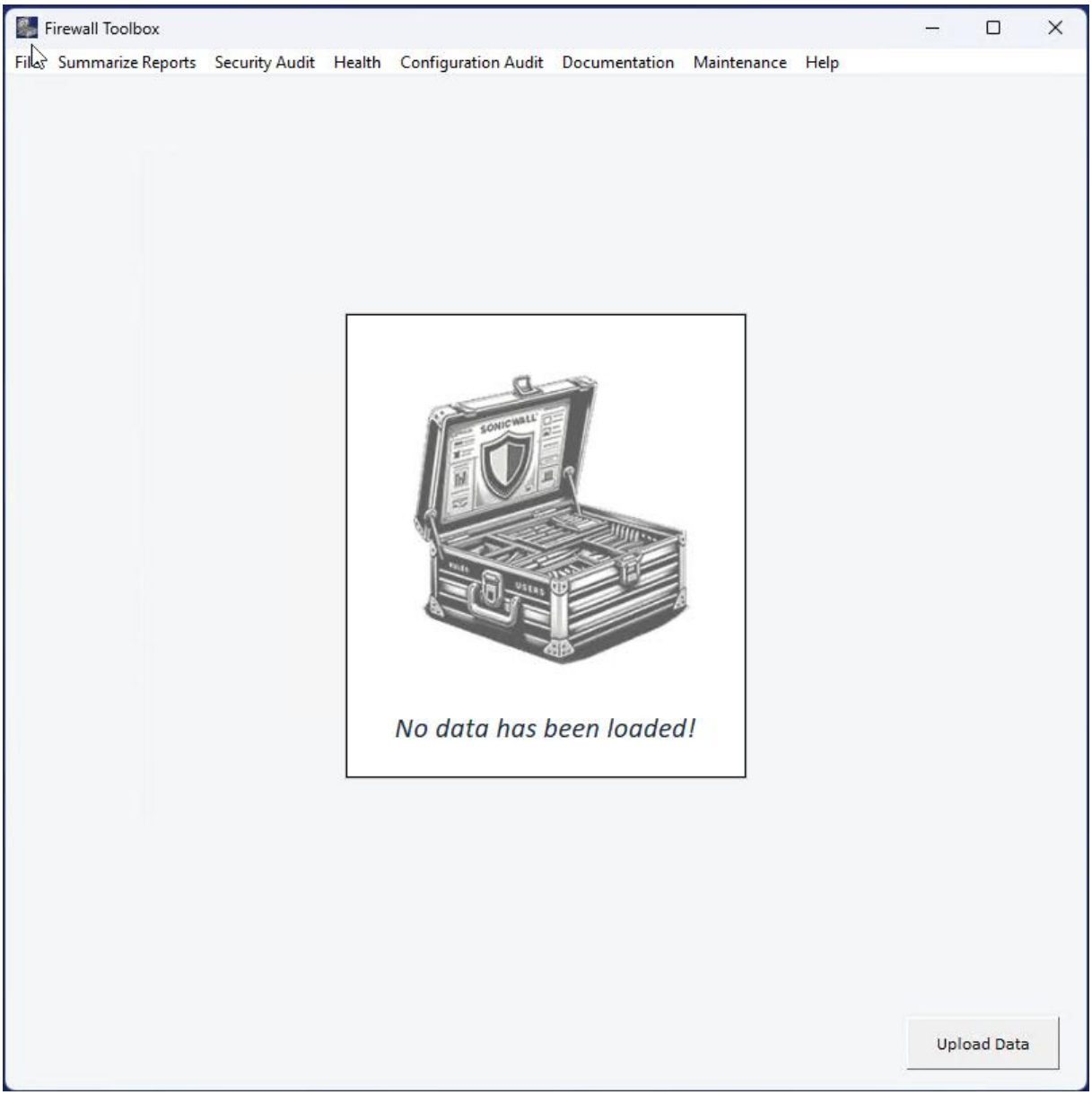
Firewall Toolbox Version 3 uses a structured user interface designed to provide quick access to analysis, reporting, documentation, and maintenance functions.

The main functions are organized into five categories that correspond directly to the structure used in the generated reports.

This chapter provides an overview of the main application window and explains how to navigate through Firewall Toolbox.

4.1 The Main Window

After starting Firewall Toolbox, the main application window provides access to all major functions.



The main window contains the controls required to:

- Import firewall data

- Select and manage the current firewall
- Access individual reports
- Generate combined reports
- Perform supported API operations
- Configure Firewall Toolbox
- Access licensing and application information

Once firewall data has been imported, the available reports and functions operate on the currently loaded firewall configuration.

4.2 The Five Main Categories

The reporting and analysis functions are organized into five main categories:

Security Audit

Contains reports that examine security-relevant configuration settings and identify potential security concerns.

Health

Provides information about the operational state of the firewall and its services.

Configuration Audit

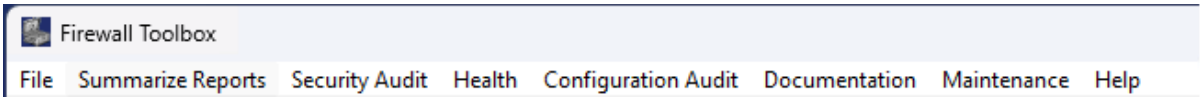
Examines important configuration settings and identifies conditions that may require review.

Documentation

Creates detailed technical documentation of the firewall configuration.

Maintenance

Provides reports and tools that help identify obsolete, unused, inconsistent, or otherwise unnecessary configuration elements.



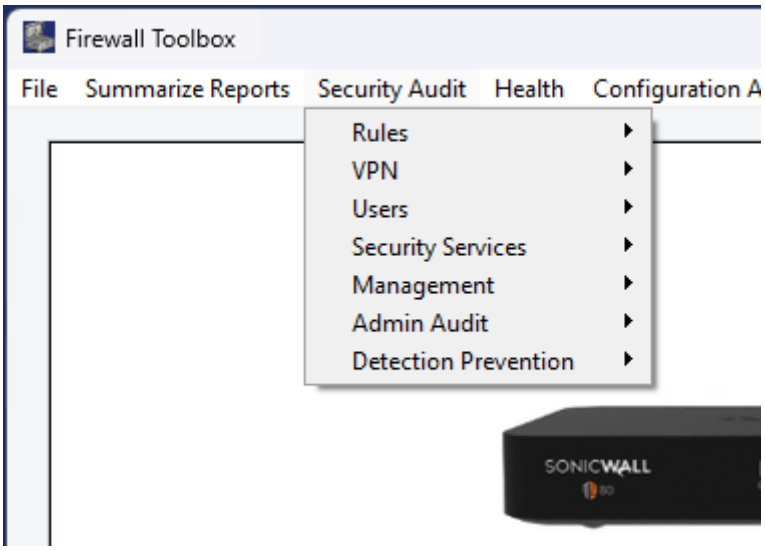
The same category structure is also used within the Full Audit Report. This makes it easier to locate a finding in Firewall Toolbox after discovering it in a generated report.

4.3 Security Audit

The **Security Audit** category contains analyses that focus primarily on the security of the firewall configuration.

Depending on the firewall model, SonicOS version, and available configuration data, this area may contain reports relating to:

- Firewall rules
- Security Services
- Administrative access
- External logging
- User and administrator permissions
- VPN security
- Access rights
- Security-related system settings



The objective of these reports is to identify configurations that may increase the attack surface or otherwise deserve additional review.

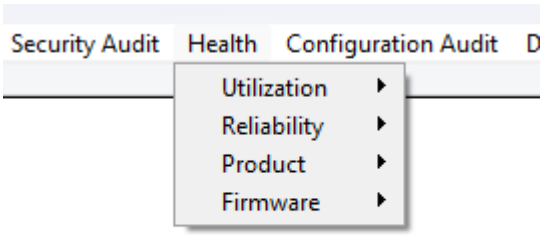
A finding does not necessarily indicate an incorrect configuration. The report identifies conditions that should be evaluated in the context of the individual environment.

The Security Audit functions are described in detail in the following chapter.

4.4 Health

The **Health** category focuses on the operational condition of the firewall.

Reports in this section can help identify problems relating to system resources, services, licensing, and other operational indicators.



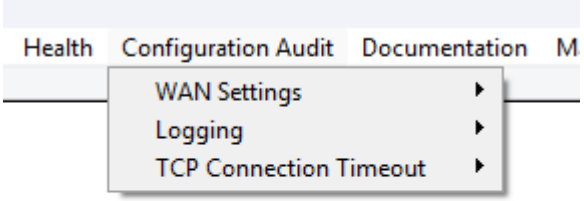
Depending on the available data, Health reports may include information such as:

- System utilization
- Security Service status
- Licensing information
- Operational statistics
- Other system health indicators

Health information can be particularly useful when analyzing performance problems or when performing a regular preventive review of a firewall.

4.5 Configuration Audit

The **Configuration Audit** category examines settings that influence the operation, reliability, and maintainability of the firewall.



Reports in this area may include checks relating to:

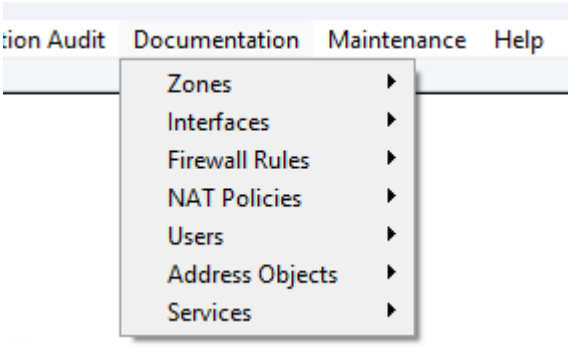
- Firmware
- High Availability
- WAN Failover
- Interfaces
- VPN configuration
- Other important system configuration settings

The Configuration Audit complements the Security Audit.

While the Security Audit primarily focuses on potential security concerns, the Configuration Audit examines whether important operational settings deserve attention.

4.6 Documentation

The **Documentation** category provides detailed reports describing the current firewall configuration.



Depending on the imported configuration, documentation can be generated for areas such as:

- Firewall rules
- NAT policies
- Address objects
- Address groups
- Interfaces
- Zones
- Users
- User groups
- VPN configurations
- Other firewall configuration elements

These reports can be used to create technical documentation without manually collecting information from numerous pages of the SonicWall management interface.

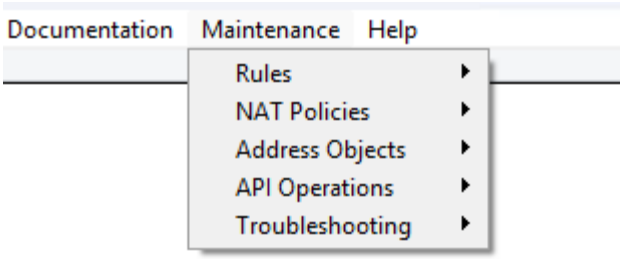
The resulting documentation can be useful for:

- Internal IT documentation
- Customer documentation
- System handovers
- Change planning
- Troubleshooting
- Security reviews

- Maintenance activities

4.7 Maintenance

The **Maintenance** category contains reports and functions intended to help keep firewall configurations clean and manageable.



Over time, firewall configurations often accumulate objects and policies that are no longer required.

Examples include old firewall rules, disabled NAT policies, unused address objects, duplicate objects, or settings that were changed for a temporary requirement and never restored.

Maintenance reports help identify these conditions.

Depending on the analysis, Firewall Toolbox can identify items such as:

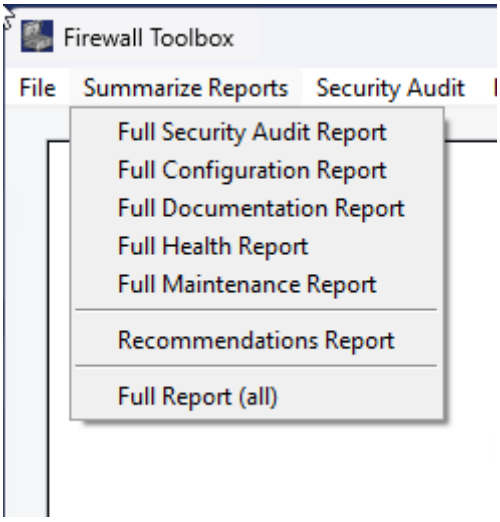
- Unused firewall rules
- Disabled firewall rules
- Unused or disabled NAT policies
- Unused address objects
- Duplicate address objects
- Address object naming inconsistencies
- Modified TCP timeout settings

For selected reports, corresponding API functions are available to perform maintenance operations directly on the firewall.

4.8 Summary Reports

Each of the five categories provides a combined report containing the relevant analyses for that area.

For example, instead of generating every Security Audit report individually, the corresponding combined report can be used to create a complete security-focused assessment.



This provides three levels of reporting:

Individual Report
Focuses on one specific analysis or configuration area.

Category Summary Report
Combines the analyses belonging to one of the five main categories.

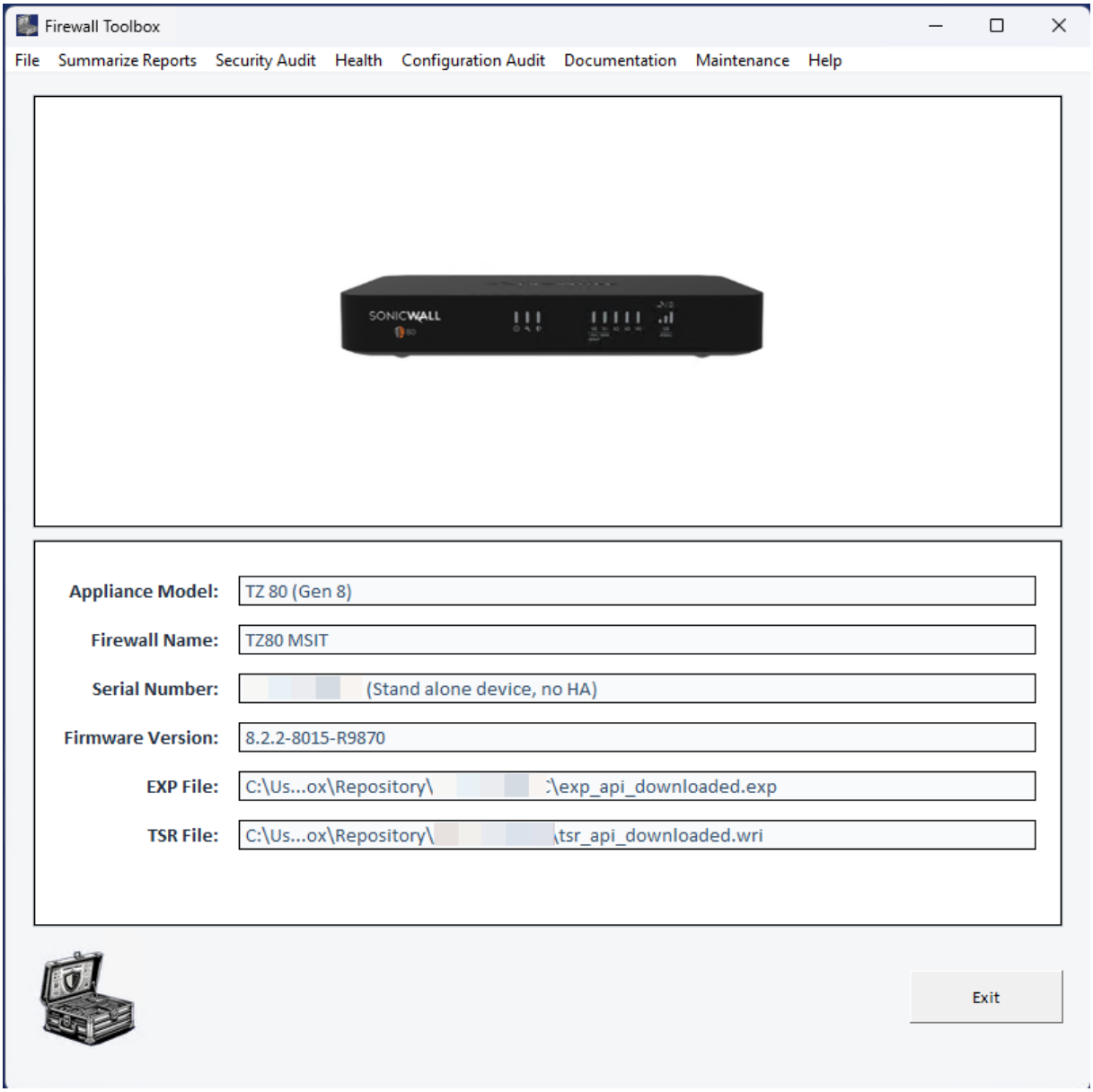
Full Audit Report
Combines the major analysis and documentation areas into one comprehensive report.

This allows the report scope to be selected according to its intended purpose and audience.

4.9 The Currently Loaded Firewall

Most analysis and reporting functions operate on the firewall data that is currently loaded in Firewall Toolbox.

Information identifying the current firewall is displayed within the application.



Before generating reports or performing API operations, verify that the correct firewall configuration is loaded.

This is particularly important when working with multiple customer environments.

Important:
Always verify the selected firewall before performing an API operation. Reports only analyze the imported data, while API operations can modify the configuration of an active firewall.

4.10 Status and Progress Information

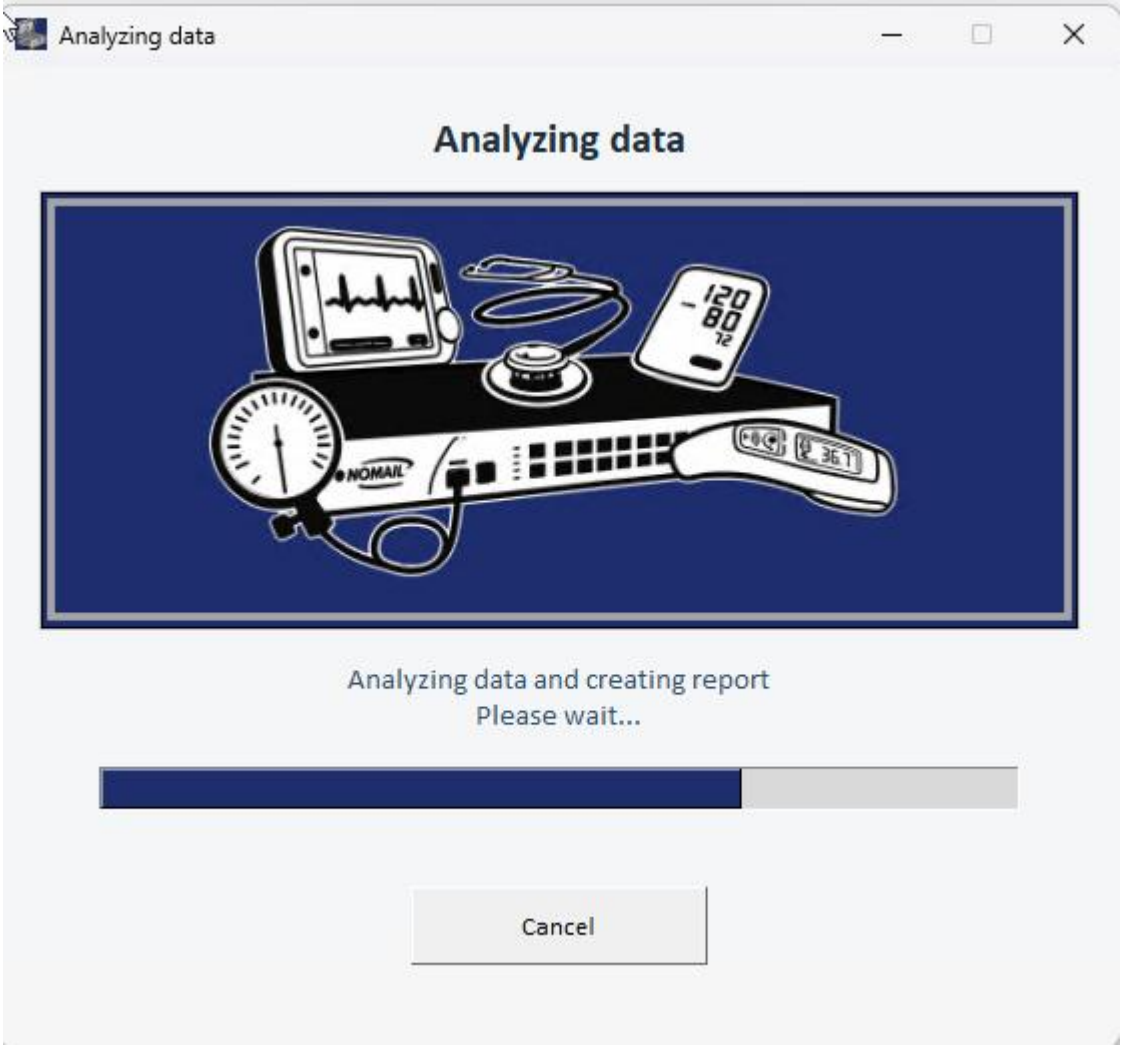
Some Firewall Toolbox operations require multiple processing steps.

Examples include:

- Importing TSR and EXP files
- Processing large configurations

- Performing a Full Audit
- Generating comprehensive reports
- Retrieving firewall information through the API
- Performing API operations

During these operations, Firewall Toolbox displays status and progress information.



The displayed information provides an indication of the current processing stage and helps determine whether an operation is still running.

For large firewall configurations, some analysis or report generation tasks may take longer to complete.

4.11 Report Windows and PDF Output

Firewall Toolbox generates its reports as PDF documents.

After report generation has completed, the resulting PDF can be opened using the default PDF viewer configured in Windows.

Reports are designed to provide both technical results and explanatory information.

Depending on the report type, a document may contain:

- Report headings
- Explanatory text
- Configuration tables
- Findings
- Recommendations
- Category sections
- Table of contents
- Page numbering

FIREWALL TOOLBOX

TCP Connection Timeout

Appliance Details	
Serial-Number:	[redacted]
Firewall Name:	TZ80 MSIT
Appliance Model:	SonicWall TZ 80
Uptime:	0 Days, 5 Hours, 7 Minutes, 52 Seconds
Firmware Version:	8.2.2-8015-R9870

Report Details	
Date & Time Report created	20.08.2026 14:36:35
EXP File:	C:\Us...ox\Repository\[redacted]\exp_api_downloaded.exp
EXP Timestamp:	20.08.2026 14:19:01
TSR File:	C:\Us...ox\Repository\[redacted]\tsr_api_downloaded.wri
TSR Timestamp:	20.08.2026 14:19:03

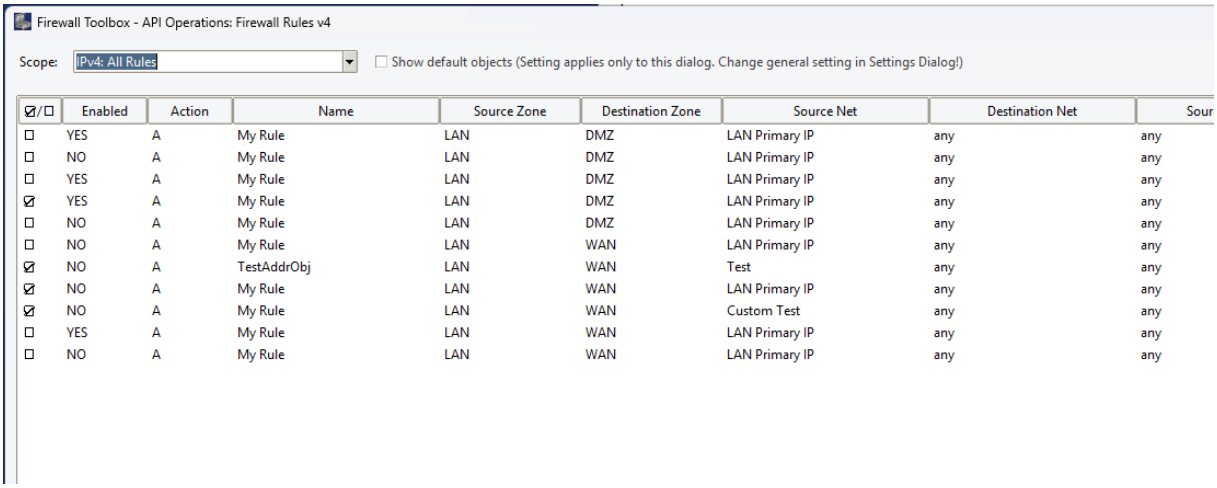
The report layout is consistent across the different categories, making it easier to navigate between individual reports and the Full Audit Report.

4.12 Context-Sensitive API Functions

Some reports identify configuration elements for which Firewall Toolbox provides a corresponding API operation.

For example, a report may identify unused objects or policies and provide the basis for selecting those items for modification.

The API operation window displays the relevant configuration elements and allows the administrator to select which items should be processed.



☑/☐	Enabled	Action	Name	Source Zone	Destination Zone	Source Net	Destination Net	Sour
☐	YES	A	My Rule	LAN	DMZ	LAN Primary IP	any	any
☐	NO	A	My Rule	LAN	DMZ	LAN Primary IP	any	any
☐	YES	A	My Rule	LAN	DMZ	LAN Primary IP	any	any
☑	YES	A	My Rule	LAN	DMZ	LAN Primary IP	any	any
☐	NO	A	My Rule	LAN	DMZ	LAN Primary IP	any	any
☐	NO	A	My Rule	LAN	WAN	LAN Primary IP	any	any
☑	NO	A	TestAddrObj	LAN	WAN	Test	any	any
☑	NO	A	My Rule	LAN	WAN	LAN Primary IP	any	any
☑	NO	A	My Rule	LAN	WAN	Custom Test	any	any
☐	YES	A	My Rule	LAN	WAN	LAN Primary IP	any	any
☐	NO	A	My Rule	LAN	WAN	LAN Primary IP	any	any

Depending on the report and object type, available actions may include:

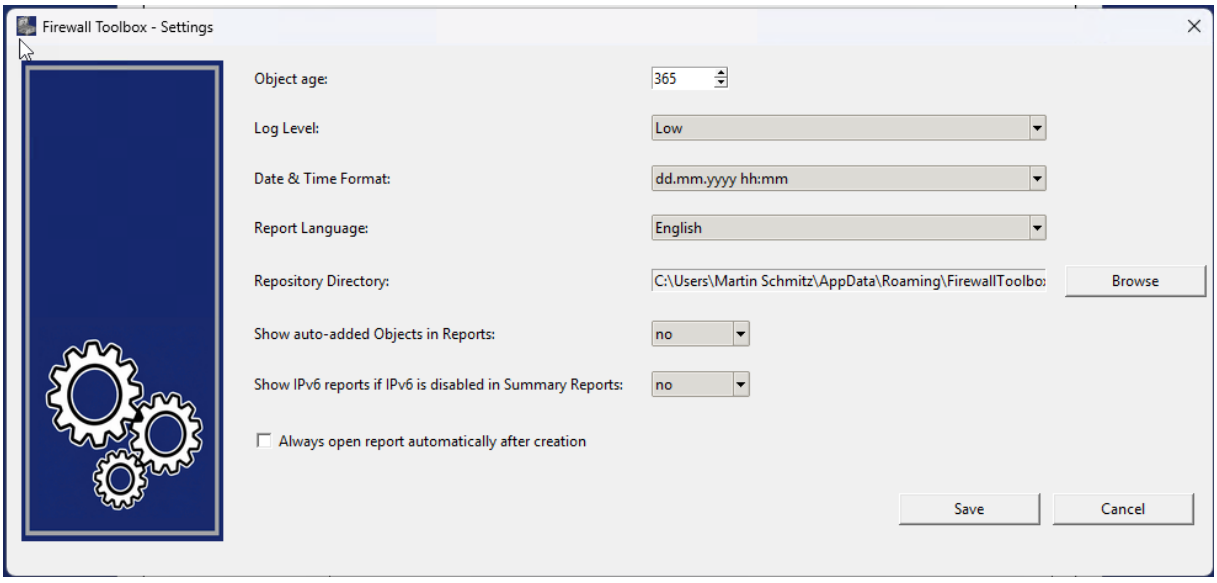
- Disable
- Delete
- Reset to a default value

This approach allows the analysis to be used directly as the basis for a maintenance operation.

Warning:
Unlike reports, API operations affect the active firewall configuration. Review the selected records carefully before executing the requested action.

4.13 Application Settings

The Firewall Toolbox settings provide options that control application behavior, report generation, and the information displayed by the software.



Settings can include options relating to:

- Report language

- IPv6 reporting
- Repository location
- Default configuration objects
- Automatically generated rules and policies
- Date and time formatting
- Report appearance
- Logging
- MySonicWall integration

Some settings directly influence which information appears in generated reports.

For this reason, report settings should be reviewed when Firewall Toolbox is first installed and whenever reporting requirements change.

A detailed description of the available settings is provided later in this guide.

4.14 Working with IPv4 and IPv6

Where applicable, Firewall Toolbox provides separate analyses for IPv4 and IPv6 configuration elements.

This is particularly relevant for areas such as firewall rules.

The availability of IPv6 reports depends on both the firewall configuration and the corresponding Firewall Toolbox settings.

If IPv6 is not used in the analyzed environment, IPv6-specific reports can be excluded to keep the report structure focused on relevant information.

4.15 Navigating Between Analysis and Maintenance

One of the key concepts of Firewall Toolbox is the relationship between **analysis, documentation, and action**.

A typical workflow might look like this:

1. A report identifies an unusual or unnecessary configuration.
2. The administrator reviews the detailed information.
3. The configuration is evaluated against the requirements of the environment.
4. If a change is required, the corresponding API function can be opened.
5. The affected objects or policies are selected.
6. Firewall Toolbox performs the requested operation.
7. The configuration can subsequently be analyzed again to verify the result.

This creates a workflow in which findings can move from **identification** to **documentation** and, where appropriate, to **correction**.

4.16 Before Continuing

At this point, you should be familiar with the basic structure of Firewall Toolbox and know where the different types of reports and functions are located.

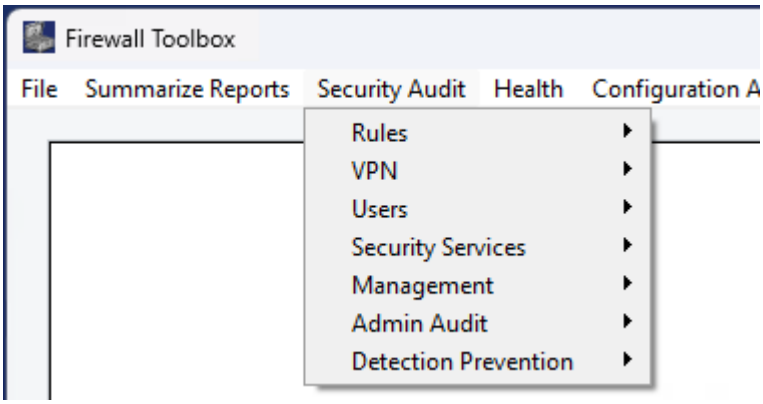
The following chapters examine each of the five main categories in detail.

We will begin with **Security Audit**, which contains the reports and analyses focusing on security-relevant aspects of the SonicWall configuration.

5. Security Audit

The **Security Audit** section contains reports designed to identify security-relevant settings, potentially risky configurations, and conditions that should be reviewed by an administrator.

Rather than simply documenting the current configuration, these reports evaluate selected settings and highlight configurations that may have an impact on the security of the firewall or the protected network.



5.1 Purpose of the Security Audit

A SonicWall firewall contains many configuration areas that influence security.

Firewall rules are an obvious example, but the overall security of a firewall also depends on areas such as:

- Security Services
- Management access
- Administrative permissions
- Logging
- User access rights
- VPN configuration
- Zone settings
- General security settings

Reviewing all these areas manually can require navigating through many different sections of the SonicWall management interface.

Firewall Toolbox collects the relevant information and presents it in structured reports.

Important:
A finding does not automatically indicate a security vulnerability or an incorrect configuration. Some configurations may be required for operational reasons. Findings should always be evaluated in the context of the individual environment.

5.2 Security Audit Summary

The **Security Audit Summary** combines the individual security analyses into a single report.

[Screenshot: Security Audit Summary]

This report is useful when a security-focused assessment is required without generating the complete Full Audit Report.

It provides a structured overview of the security-relevant configuration and allows administrators to quickly identify areas that deserve further investigation.

For a complete assessment, the individual findings should be reviewed together with their corresponding explanations and configuration details.

5.3 Firewall Rule Analysis

Firewall rules are one of the most important elements of network security.

They determine which traffic is permitted or denied between networks and security zones.

Over time, rule sets often become increasingly complex. Temporary rules may remain enabled, obsolete rules may no longer be required, and permissive rules may provide more access than originally intended.

Firewall Toolbox provides several reports to help analyze the firewall rule base.

Depending on the configuration, separate reports are available for IPv4 and IPv6 rules.

5.4 ANY-to-ANY Firewall Rules

Rules permitting traffic from **ANY** source to **ANY** destination deserve particular attention.

Such rules can potentially allow a very broad range of network communication.

Firewall Toolbox identifies these rules and presents them in a dedicated report.

[Screenshot: IPv4 ANY-to-ANY Firewall Rules report]

The report provides the information required to determine why the rule exists and whether its scope is still appropriate.

When reviewing an ANY-to-ANY rule, consider:

- Source and destination zones
- Allowed services
- Rule action
- Whether the rule is enabled
- Business requirement
- Security Services applied to the traffic
- Whether the scope could be restricted

Important:
An ANY-to-ANY rule is not automatically insecure. For example, its effect may already be restricted by source and destination zones or permitted services. The complete rule must always be evaluated.

5.5 Rules Providing Access from WAN to Internal Networks

Rules allowing traffic from the WAN toward internal networks are particularly security-relevant because they may expose internal systems or services to external networks.

Firewall Toolbox provides reports that identify these rules and make them easier to review.

[Screenshot: WAN to Internal Networks report]

When reviewing these rules, particular attention should be paid to:

- Destination systems
- Allowed services
- Source restrictions
- Whether the rule is still required
- Associated NAT policies
- Security Services
- Logging
- Last usage information

Internet-facing services should generally be restricted as much as the application requirements allow.

5.6 Rules Using ANY as a Source or Destination

Firewall Toolbox can also identify other broadly defined rules where **ANY** is used for relevant source or destination parameters.

These reports help locate policies whose scope may be wider than necessary.

[Screenshot: Example ANY/WAN rule analysis]

A broad rule may have been intentionally created, but it is good practice to periodically verify whether the original requirement still exists.

In many environments, older rules can be made more specific after the actual communication requirements are better understood.

5.7 Disabled Firewall Rules

Disabled firewall rules do not currently process traffic, but they remain part of the configuration.

[Screenshot: Disabled Firewall Rules report]

There are valid reasons for retaining disabled rules temporarily. For example, a rule may have been disabled during troubleshooting or while a service is being migrated.

However, a large number of permanently disabled rules can make a configuration unnecessarily difficult to understand and maintain.

The report helps identify these rules so that administrators can determine whether they should:

- Remain disabled
- Be re-enabled
- Be documented
- Be permanently removed

Where supported, Firewall Toolbox can also provide API functions for managing the identified rules.

5.8 Firewall Rules That Have Never Been Used

Firewall Toolbox can identify rules for which no usage has been recorded.

[Screenshot: Firewall Rules Never Used report]

A rule that has never been used may indicate:

- An obsolete requirement
- An incorrectly configured rule
- A service that was never implemented
- A redundant policy
- A rule that is shadowed or otherwise ineffective

However, usage information should be interpreted carefully.

Some rules exist specifically for rare events, emergency procedures, seasonal applications, or infrequent administrative tasks.

Important:
Never delete a firewall rule solely because it has no recorded hits. Verify the purpose of the rule and consider the available logging and uptime information before making a decision.

5.9 Firewall Rules Not Used for a Long Time

In addition to rules that have never been used, Firewall Toolbox can identify rules that have not been used for an extended period.

[Screenshot: Firewall Rules Not Used for a Long Time report]

These rules are useful candidates for review during firewall maintenance.

Before removing such a rule, consider whether it supports:

- Infrequently used applications

- Backup systems
- Disaster recovery procedures
- Administrative access
- Seasonal processes
- External service providers
- Emergency connections

Where uncertainty exists, disabling a rule before permanently deleting it can provide a safer cleanup strategy.

5.10 Security Services

SonicWall Security Services provide important protection against threats passing through the firewall.

Firewall Toolbox analyzes information about the configured and licensed Security Services and provides reports that help determine whether the expected protection is available.

[Screenshot: Security Services report]

Depending on the firewall and available licenses, this may include services such as:

- Gateway Anti-Virus
- Intrusion Prevention
- Anti-Spyware
- Application Control
- Content Filtering
- Other licensed security functionality

The reports can help identify services that are unavailable, disabled, expired, or otherwise require attention.

5.11 Security Services by Zone

Having a Security Service licensed does not necessarily mean that it is applied everywhere it is required.

For this reason, Firewall Toolbox also evaluates the use of Security Services in relation to firewall zones.

[Screenshot: Security Services by Zone report]

This allows administrators to determine whether the required protection mechanisms are enabled for the relevant network areas.

For example, an active IPS license provides limited benefit for traffic that passes through a zone where IPS inspection has not been enabled.

Tip:
When reviewing Security Services, evaluate both the license status and where each service is actually enabled.

5.12 Management Access

Administrative access to the firewall is a particularly sensitive part of the configuration.

Firewall Toolbox provides reports that help identify which management protocols and services are available through the different interfaces or zones.

[Screenshot: Management Access report]

Depending on the environment, management access may include protocols such as:

- HTTPS
- SSH
- SNMP
- Other administrative services

Management access should generally be limited to trusted networks and only enabled where required.

Special attention should be given to management services that are accessible from external or untrusted networks.

5.13 External Logging

Centralized logging can be an important component of security monitoring, troubleshooting, auditing, and incident investigation.

Firewall Toolbox checks the relevant configuration and provides information about external logging.

[Screenshot: External Logging report]

External logging can help preserve security-relevant information even when local firewall logs are no longer available.

Depending on organizational requirements, external logging may also be required for compliance or audit purposes.

5.14 Administrative Users and Groups

Firewall administration should be restricted to users who actually require administrative privileges.

Firewall Toolbox provides reports that help identify users belonging to administrative groups.

[Screenshot: Users in Administrative Groups report]

These reports make it easier to review administrative access and identify accounts that may no longer require elevated permissions.

When reviewing administrative users, consider:

- Whether the account is still required
- Whether the user still requires administrative privileges
- Whether individual administrator accounts are used
- Whether old or unused accounts remain configured
- Whether permissions follow the principle of least privilege

---

5.15 Users and Group Memberships

User group membership can have a significant effect on network access.

Firewall Toolbox provides reports showing which groups users belong to.

[Screenshot: Users and Group Memberships report]

This can be particularly useful when access rights are assigned indirectly through group membership.

The report helps administrators understand the relationship between users, groups, and the permissions that may result from those memberships.

5.16 Access Rights Assigned to Users

SonicWall configurations can contain network access rights associated with individual users or groups.

Firewall Toolbox analyzes these relationships and provides reports showing the corresponding assignments.

[Screenshot: Access Rights Assigned to Users report]

This information can help identify:

- Unexpected access permissions
- Historical assignments
- Access to networks that may no longer be required
- User-specific exceptions

These reports can also be useful when reviewing permissions for users who have changed roles within an organization.

5.17 User Account Protection

Firewall Toolbox includes analyses relating to user account protection and authentication settings.

[Screenshot: User Account Protection report]

The objective is to identify settings that influence how accounts are protected against unauthorized access or repeated authentication attempts.

The exact recommendations depend on the security requirements of the organization and the authentication methods in use.

5.18 VPN Security

VPN connections often remain configured for many years, while cryptographic recommendations continue to evolve.

Firewall Toolbox can analyze relevant VPN policy settings and help identify configurations that use older or potentially inappropriate cryptographic parameters.

[Screenshot: VPN Policy Crypto Check report]

Depending on the VPN configuration, the analysis can evaluate parameters such as:

- Phase 1 encryption
- Phase 1 authentication
- Diffie-Hellman groups
- Phase 2 encryption
- Phase 2 authentication
- Perfect Forward Secrecy

The objective is not simply to identify older algorithms, but to make the configured parameters visible so that they can be evaluated against current security requirements and compatibility constraints.

Important:
Changing VPN cryptographic parameters requires corresponding changes on the remote VPN endpoint. Do not modify these settings without coordinating both sides of the VPN connection.

5.19 VPN Tunnels That Have Never Been Used

Firewall Toolbox can identify VPN policies for which no usage has been detected.

[Screenshot: VPN Tunnels Never Used report]

Unused VPN configurations may be remnants of:

- Former branch offices
- Previous business partners
- Decommissioned systems
- Migration projects
- Test environments

Such configurations should be reviewed to determine whether they are still required.

Removing obsolete VPN configurations can reduce complexity and make the active security configuration easier to understand.

5.20 Additional Security Settings

Firewall Toolbox also evaluates additional SonicWall security-related settings that may not belong to a single firewall rule or Security Service.

Examples can include settings related to packet handling and system behavior.

[Screenshot: Detection / Prevention settings report]

These reports help identify less obvious configuration options that might otherwise be overlooked during a routine manual review.

5.21 Interpreting Security Findings

Security Audit findings should be considered as **indicators for review**, not automatic instructions to change the firewall.

For each finding, consider three questions:

Why is this configuration present?

Determine the original technical or business requirement.

Is the requirement still valid?

Configurations frequently remain in place after the application, user, customer, or service that required them has changed.

Can the configuration be made more restrictive?

If the requirement still exists, determine whether the same functionality can be provided with a more specific configuration.

This approach is particularly useful when reviewing firewall rules and access permissions.

5.22 Recommended Security Audit Workflow

A practical security review can follow this sequence:

1. Generate the Security Audit Summary or Full Audit Report.
2. Review the highlighted security findings.
3. Examine externally accessible services and WAN rules.
4. Review broad firewall rules such as ANY-to-ANY policies.
5. Verify Security Services and their zone assignments.
6. Review management access.
7. Review administrative users and permissions.
8. Examine user access rights.

9. Review VPN cryptographic settings and obsolete tunnels.
10. Investigate unused and long-unused firewall rules.
11. Document findings that require further investigation.
12. Perform configuration changes only after their impact has been evaluated.

After changes have been completed, importing a new TSR and EXP and repeating the audit provides a convenient way to verify the updated configuration.

5.23 Next Steps

The Security Audit focuses primarily on the security implications of the firewall configuration.

The next chapter covers **Health**, which examines the operational condition of the firewall, including utilization, services, licensing, and other indicators that can help identify operational issues before they become critical.

6. Health

The **Health** section of Firewall Toolbox focuses on the operational condition of the SonicWall firewall.

While the Security Audit evaluates security-related configuration settings, the Health reports help determine whether the firewall itself and its associated services are operating as expected.

These reports can be useful during regular maintenance, troubleshooting, capacity planning, and general system reviews.

[Screenshot: Health menu]

6.1 Purpose of the Health Analysis

A firewall can be correctly configured from a security perspective while still experiencing operational problems.

High resource utilization, unavailable services, expired licenses, or unusual system conditions may affect performance or reduce the level of protection provided by the firewall.

Firewall Toolbox collects relevant operational information from the available firewall data and presents it in structured reports.

The objective is to provide a quick overview of the current condition of the firewall and highlight areas that may require further investigation.

Important:
Health information represents the state and statistics available in the imported firewall data. A single audit therefore provides a snapshot of the system. Long-term performance assessment may require additional historical monitoring data.

6.2 Health Summary

The **Health Summary** combines the available health-related analyses into a single report.

[Screenshot: Health Summary report]

This provides a convenient starting point when reviewing the operational condition of a firewall.

Rather than opening each Health report individually, the summary allows the administrator to review the relevant information in one document and then investigate individual areas where necessary.

6.3 System Utilization

Resource utilization is an important indicator of firewall health.

Firewall Toolbox evaluates available utilization information to help identify periods or conditions where system resources may be heavily used.

[Screenshot: System Utilization report]

Depending on the information available from the firewall, utilization reports can provide different views of the collected data, including:

- Minute
- Hour
- Day
- Month
- Summary information

These different time ranges make it possible to distinguish short utilization peaks from longer-term trends.

6.4 Understanding Utilization Values

High utilization does not automatically indicate a problem.

A firewall is designed to use its available resources, and short periods of high utilization can occur during normal operation.

More important factors include:

- How long the utilization remains high
- Whether high utilization occurs regularly
- Whether users experience performance problems at the same time
- Whether the utilization pattern has changed
- Whether traffic volume or enabled security functionality has increased

A consistently heavily utilized firewall may indicate that the appliance is approaching the limits of its current workload.

Tip:
Evaluate utilization together with changes in the environment. New users, additional VPN connections, increased Internet bandwidth, additional Security Services, or new applications can significantly change the workload of a firewall.

6.5 Short-Term Utilization

Short-term utilization data provides a detailed view of recent firewall activity.

[Screenshot: Minute/Hour Utilization report]

This information can be useful when investigating a recently reported performance issue.

For example, if users experienced slow network performance at a particular time, the short-term utilization data may help determine whether the firewall was under unusually high load during that period.

Short peaks should generally be distinguished from sustained high utilization.

6.6 Long-Term Utilization

Longer-term views help identify trends that may not be obvious from a short snapshot.

[Screenshot: Day/Month Utilization report]

For example, an appliance may operate normally most of the time but regularly reach high utilization during business hours.

Long-term information can therefore be useful for:

- Capacity planning
- Identifying recurring load patterns
- Evaluating appliance sizing
- Comparing current utilization with previous audits
- Planning future upgrades

6.7 Utilization Summary

The utilization summary provides a condensed overview of the available performance information.

[Screenshot: Utilization Summary]

This report is particularly useful when the objective is to quickly determine whether resource utilization deserves further investigation.

If unusual values are identified, the more detailed utilization reports can then be used for additional analysis.

6.8 Security Service Status

Security Services are an important part of the protection provided by a SonicWall firewall.

Firewall Toolbox evaluates available Security Service information and provides an overview of their status.

[Screenshot: Security Services Status report]

Depending on the firewall and licensing configuration, this information may include services such as:

- Gateway Anti-Virus
- Intrusion Prevention
- Anti-Spyware
- Application Control
- Content Filtering
- Other SonicWall security subscriptions

A service may be configured correctly but still be unable to provide the expected protection if its license has expired.

For this reason, both configuration and licensing information should be reviewed.

6.9 Security Service Licensing

Firewall Toolbox can display available licensing information for the Security Services.

[Screenshot: Security Services Licensing report]

Depending on the available firewall data, the report can include information such as:

- Service name
- License status
- Expiration information
- Other available subscription details

This makes it easier to identify licenses that have expired or may require renewal.

Important:
An expired Security Service license can affect the protection provided by the firewall. License-related findings should therefore be reviewed together with the corresponding service configuration.

6.10 License Expiration

Where expiration information is available, Firewall Toolbox can help identify Security Services approaching or exceeding their expiration date.

[Screenshot: Security Service Expiration report]

Reviewing this information during regular audits can help avoid situations where a security subscription expires unnoticed.

For organizations managing multiple firewalls, this can be particularly useful because license information is included as part of the normal audit process rather than requiring a separate manual check for each appliance.

6.11 Evaluating Health Findings

Health findings should be evaluated in relation to the normal operating conditions of the firewall.

For example:

A short utilization peak may be normal.

A sustained high utilization level may deserve investigation.

An expired service may be intentional if that functionality is no longer required.

An unexpected expired service may indicate that the firewall is no longer providing the intended protection.

The purpose of the Health section is therefore to make relevant operational information visible and easier to review.

6.12 Comparing Health Information Over Time

Regular audits can provide additional value because they allow administrators to compare the condition of a firewall over time.

For example, repeated audits may reveal:

- Increasing system utilization
- Changes in workload
- Approaching license expiration
- Changes in Security Service availability
- New operational conditions

The firewall repository can help retain the configuration and diagnostic files used for previous analyses.

Tip:
Performing audits at regular intervals provides more information than a single assessment. Changes in utilization and system status can often be more meaningful than an isolated value.

6.13 Health Analysis and Troubleshooting

Firewall Toolbox is not intended to replace real-time monitoring or specialized network monitoring systems.

Instead, the Health reports provide additional information as part of the overall firewall audit.

When troubleshooting a performance issue, the Firewall Toolbox results can be combined with other information such as:

- SonicWall real-time monitoring
- Firewall logs
- SNMP monitoring
- Network monitoring systems
- Interface statistics
- Application monitoring
- User reports

This helps determine whether the firewall itself may be contributing to the observed problem.

6.14 Recommended Health Review Workflow

A regular firewall health review can follow this sequence:

1. Generate the Health Summary or Full Audit Report.
2. Review the utilization summary.
3. Investigate unusual utilization values.
4. Compare short-term and long-term utilization.
5. Review Security Service status.
6. Check Security Service licensing and expiration dates.
7. Investigate unexpected or unavailable services.
8. Compare the results with previous audits where available.
9. Document findings that require monitoring or further investigation.

This provides a structured approach to evaluating the operational condition of the firewall.

6.15 Next Steps

The Health section provides information about the operational state of the firewall.

The next chapter covers the **Configuration Audit**.

This area examines important configuration elements such as firmware, High Availability, WAN Failover, and other operational settings to help identify configurations that may affect the reliability or maintainability of the firewall.

7. Configuration Audit

The **Configuration Audit** section examines important SonicWall settings that affect the operation, reliability, and maintainability of the firewall.

While the Security Audit focuses primarily on security-related findings and the Health section examines the operational condition of the appliance, the Configuration Audit evaluates how important firewall functions are configured.

[Screenshot: Configuration Audit menu]

7.1 Purpose of the Configuration Audit

Firewall configurations evolve over time.

Firmware is upgraded, Internet connections are replaced, High Availability is introduced, VPNs are added, and settings are modified to accommodate changing technical requirements.

As a result, some configuration settings may remain in place long after the original requirement has disappeared.

The Configuration Audit helps make these settings visible and provides structured information for reviewing them.

Depending on the firewall configuration and available data, the analysis can cover areas such as:

- Firewall lifecycle
- Firmware
- Firmware history
- High Availability
- WAN Failover
- Interfaces
- VPN configuration
- Other operational settings

Important:
Configuration Audit findings should be evaluated against the requirements of the individual environment. A configuration that differs from a common recommendation may still be correct and intentional.

7.2 Configuration Audit Summary

The **Configuration Audit Summary** combines the available configuration-related analyses into a single report.

[Screenshot: Configuration Audit Summary]

This report provides a convenient overview of important configuration settings and highlights areas that may require additional review.

If a finding requires further investigation, the corresponding individual report can be generated separately.

7.3 Firewall Lifecycle

Firewall appliances have a defined product lifecycle.

As hardware platforms become older, support status, firmware availability, and replacement planning become increasingly important.

Firewall Toolbox provides lifecycle information where the required data is available.

[Screenshot: Firewall Lifecycle report]

Lifecycle information can help determine whether an appliance:

- Is actively supported
- Is approaching a lifecycle milestone
- Should be considered for replacement planning
- May have limited access to future firmware or support

This information can be particularly useful when reviewing customer environments containing appliances that have been operating for many years.

Tip:
Lifecycle information should be considered during budget and infrastructure planning rather than only when an appliance reaches the end of its supported lifetime.

7.4 Firmware Version

Keeping firewall firmware at an appropriate version is an important part of firewall maintenance.

Firmware updates can contain:

- Security fixes
- Stability improvements
- Bug fixes
- Performance improvements
- Compatibility changes
- New functionality

Firewall Toolbox identifies the firmware version running on the analyzed firewall and provides this information as part of the Configuration Audit.

[Screenshot: Firmware report]

The installed version can then be evaluated against the organization's update policy and SonicWall recommendations.

7.5 Checking for Available Firmware

If MySonicWall integration is configured, Firewall Toolbox can use additional information to determine whether other firmware versions are available for the firewall.

[Screenshot: Firmware Up-to-Date report]

This can simplify regular audits because the administrator does not need to manually check the available downloads for every appliance.

Important:
The availability of a newer firmware version does not automatically mean that it should immediately be installed. Compatibility, release notes, known issues, maintenance windows, and organizational update policies should be reviewed before performing an upgrade.

7.6 Firmware History

Firewall Toolbox can process available firmware history information and include it in the audit.

[Screenshot: Firmware History report]

Firmware history can provide useful context when troubleshooting or reviewing an appliance.

For example, it can help determine:

- When firmware changes occurred
- Which versions were previously installed
- Whether a reported issue may be related to an upgrade
- How frequently the firewall has been updated

This information can also be useful when taking over responsibility for an existing firewall where the previous maintenance history is not fully documented.

7.7 High Availability

SonicWall High Availability allows two compatible appliances to operate as an HA pair to improve service availability.

Firewall Toolbox analyzes available HA configuration information and indicates whether the firewall is operating as part of an HA environment.

[Screenshot: High Availability report]

Depending on the available data, the report can provide information about the HA configuration and the role of the analyzed appliance.

High Availability should be reviewed as part of a configuration audit because an HA configuration provides value only when both appliances and the synchronization mechanisms are operating as intended.

7.8 Auditing Firewalls in an HA Cluster

When analyzing an HA environment, it is important to understand which appliance provided the imported data.

Certain operational information may be specific to the individual HA member.

Firewall Toolbox therefore identifies when the analyzed firewall is part of an HA cluster and provides corresponding information in the report.

Important:
Not all operational information is necessarily synchronized between HA members. For example, certain audit or logging information may be specific to the appliance from which the TSR was obtained.

For a complete investigation of an HA-related problem, information from both appliances may be required.

7.9 HA Configuration and Failover Considerations

A correctly configured HA environment depends on more than simply enabling High Availability.

When reviewing an HA installation, administrators should also consider factors such as:

- HA status
- Synchronization
- Interface configuration
- Monitoring
- Network connectivity
- Firmware compatibility
- Session synchronization
- Failover behavior

Firewall Toolbox provides configuration information that can assist with this review.

However, an actual HA failover test remains the most reliable method of verifying the complete failover process.

Tip:
Where operational requirements permit, HA functionality should be tested periodically rather than assuming that a configured HA pair will automatically fail over correctly when required.

7.10 WAN Failover

Many SonicWall installations use more than one Internet connection to improve availability.

WAN Failover allows the firewall to switch between connections when the preferred connection becomes unavailable.

Firewall Toolbox analyzes the available WAN Failover configuration and presents the relevant information in a structured report.

[Screenshot: WAN Failover report]

This can help determine whether redundancy is configured and how the available WAN connections participate in the failover configuration.

7.11 Reviewing WAN Failover

A WAN Failover configuration should be evaluated together with the requirements of the environment.

Important questions can include:

- Which interface is the preferred WAN connection?
- Which interfaces provide backup connectivity?
- How is a failed connection detected?
- Is preemption required?
- Are probe targets appropriate?
- Are all required routes and policies compatible with failover?
- Do VPN connections behave correctly after failover?

A configuration can appear correct while still failing to provide the expected redundancy if the complete failover path has never been tested.

Tip:
Like High Availability, WAN Failover should ideally be tested periodically under controlled conditions.

7.12 Interface Configuration

Interfaces form the connection between the SonicWall firewall and the surrounding network infrastructure.

Firewall Toolbox processes interface information and associates interfaces with their corresponding zones.

[Screenshot: Interface / Zone information]

This information provides important context for many other reports.

For example, understanding which interfaces belong to the WAN, LAN, DMZ, or other zones helps interpret firewall rules, management access, and network topology.

Interface documentation can also be useful during:

- Troubleshooting
- Hardware replacement
- Firewall migration
- Network redesign
- System handover

7.13 Zones and Interfaces

SonicWall uses zones to group interfaces with similar security requirements.

Firewall Toolbox analyzes the relationship between interfaces and zones and uses this information throughout its reports.

[Screenshot: Zone and Interface overview]

Examples of common zones include:

- LAN
- WAN
- DMZ
- WLAN
- VPN
- Custom security zones

The actual zone structure depends on the individual firewall configuration.

Understanding these relationships is particularly important when reviewing firewall rules because the same address or service configuration can have very different security implications depending on the source and destination zones.

7.14 VPN Configuration

VPN configurations are an important part of many SonicWall environments.

Firewall Toolbox processes available VPN information for both security and configuration analysis.

While security-related parameters such as cryptographic algorithms are primarily covered by the Security Audit, the Configuration Audit can provide additional information about the configured VPN environment.

[Screenshot: VPN Configuration report]

VPN documentation and analysis can help identify:

- Existing VPN policies

- Historical configurations
- Unused connections
- Configuration inconsistencies
- Settings that should be reviewed

7.15 Configuration Changes Over Time

One of the challenges when maintaining a firewall is understanding why a particular setting exists.

A configuration may have been modified years earlier to solve a temporary problem, support an application, or accommodate a previous network design.

The original reason may no longer be documented.

Regular Configuration Audits can help identify such settings before they become difficult to understand.

This is especially relevant for firewalls that have been migrated or upgraded several times while retaining much of their original configuration.

7.16 Configuration Audit and Documentation

The Configuration Audit and Documentation sections serve different purposes.

The **Configuration Audit** asks questions such as:

Does this setting require attention?

The **Documentation** section answers questions such as:

How is this firewall currently configured?

Both views are useful.

For example, the Configuration Audit may identify an unusual WAN Failover configuration, while the Documentation section provides the detailed interface, zone, policy, and object information required to understand the complete environment.

7.17 Interpreting Configuration Findings

When Firewall Toolbox identifies a configuration that deserves review, the administrator should determine:

What is configured?

Understand the current setting.

Why was it configured this way?

Determine whether there is a documented technical or business reason.

Is the reason still valid?

Older configurations frequently contain settings related to systems or requirements that no longer exist.

What would be affected by a change?

Before modifying a configuration, identify dependent systems, policies, VPNs, routes, or applications.

This approach reduces the risk of removing a configuration that still serves an important purpose.

7.18 Recommended Configuration Audit Workflow

A regular Configuration Audit can follow this sequence:

1. Generate the Configuration Audit Summary or Full Audit Report.
2. Review lifecycle information.
3. Check the installed firmware version.
4. Review available firmware information where MySonicWall integration is enabled.
5. Examine the firmware history.
6. Review High Availability configuration where applicable.
7. Review WAN Failover configuration.
8. Verify interface and zone relationships.
9. Review relevant VPN configuration.
10. Investigate unusual or undocumented settings.
11. Document required changes.
12. Plan configuration changes and maintenance windows where necessary.

After significant configuration changes, a new audit can be performed to document and verify the updated state.

7.19 Next Steps

The Configuration Audit provides information about how important operational features of the firewall are configured.

The next chapter covers **Documentation**.

This is one of the major areas expanded in Firewall Toolbox Version 3 and provides detailed technical documentation of the SonicWall configuration, including firewall rules, NAT policies, zones, interfaces, address objects, users, VPNs, and other configuration elements.

8. Documentation

The **Documentation** section of Firewall Toolbox creates structured technical documentation of the SonicWall firewall configuration.

While the Security Audit, Health, and Configuration Audit sections primarily analyze the firewall and identify conditions that may require attention, the Documentation section focuses on a different question:

How is this firewall currently configured?

Firewall Toolbox extracts the relevant information from the imported firewall data and converts it into structured PDF reports that can be stored, reviewed, or provided to customers and colleagues.

[Screenshot: Documentation menu]

8.1 Purpose of the Documentation Section

Creating complete firewall documentation manually can be a time-consuming task.

A SonicWall configuration can contain hundreds or even thousands of individual elements distributed across many areas of the management interface.

These may include:

- Firewall rules
- NAT policies
- Address objects
- Address groups
- Interfaces
- Zones
- Users and groups
- Access rights
- VPN policies
- Security settings
- System configuration

Firewall Toolbox automatically processes this information and presents it in a consistent format.

This significantly reduces the effort required to create and maintain technical firewall documentation.

8.2 Documentation Summary

The **Documentation Summary** combines the available documentation reports into a single document.

[Screenshot: Documentation Summary report]

This is useful when comprehensive technical documentation is required without including the audit and maintenance analyses contained in the Full Audit Report.

Individual documentation reports can also be generated separately when only a specific configuration area is required.

8.3 Firewall Rule Documentation

Firewall rules are among the most important configuration elements to document.

Firewall Toolbox creates structured reports containing the configured firewall rules and their relevant properties.

[Screenshot: Firewall Rules documentation]

Depending on the available configuration information, the documentation can include details such as:

- Rule name
- Enabled or disabled state
- Action
- Source zone
- Destination zone
- Source network or object
- Destination network or object
- Source service
- Destination service
- Comments
- Usage information

Separate documentation can be provided for IPv4 and IPv6 rules where applicable.

8.4 Why Firewall Rule Documentation Matters

Firewall rule sets often become difficult to understand as they grow.

A rule may have been created for a specific application years earlier, while the people currently responsible for the firewall may have little information about its original purpose.

Good rule documentation helps answer questions such as:

- What traffic is permitted?
- Between which network zones?
- Which systems are involved?
- Which services are allowed?

- Why does the rule exist?
- Is the rule currently enabled?
- Is there a useful administrative comment?

Firewall Toolbox makes the technical configuration visible, but meaningful rule names and comments remain important.

Tip:
Use descriptive rule names and comments directly on the firewall. Automatically generated documentation becomes significantly more useful when the configuration itself contains meaningful descriptions.

8.5 IPv4 and IPv6 Firewall Rules

Where IPv6 is enabled and the corresponding reporting option is active, Firewall Toolbox can document IPv6 firewall rules separately from IPv4 rules.

[Screenshot: IPv6 Firewall Rules documentation]

Keeping IPv4 and IPv6 rules clearly documented is important because the security policies for the two protocols may differ.

An environment with a carefully restricted IPv4 rule base should not assume that the IPv6 configuration provides the same restrictions automatically.

8.6 NAT Policy Documentation

Network Address Translation policies are another important part of a SonicWall configuration.

Firewall Toolbox creates reports describing the configured NAT policies.

[Screenshot: NAT Policies documentation]

Depending on the available data, the report can include information such as:

- Policy name
- Enabled or disabled state
- Original source
- Translated source
- Original destination
- Translated destination
- Original service
- Translated service
- Policy comments

NAT documentation is particularly valuable when troubleshooting externally published services or complex network configurations.

8.7 Understanding NAT Relationships

A NAT policy often needs to be considered together with other configuration elements.

For example, publishing an internal server to the Internet may involve:

- An address object for the public IP address
- An address object for the internal server
- A service object
- A NAT policy
- A corresponding firewall rule

Looking at only one of these elements may not provide the complete picture.

Firewall Toolbox documentation helps make the individual components visible so that their relationships can be reviewed more easily.

8.8 Address Objects

Address objects are used throughout SonicWall configurations to represent hosts, networks, address ranges, and other network resources.

Firewall Toolbox can document the configured address objects and their relevant properties.

[Screenshot: Address Objects documentation]

Depending on the object type, the information may include:

- Object name
- Zone
- Object type
- IP address
- Network
- Address range
- Other object-specific values

Address object documentation can be particularly useful when analyzing older or complex configurations.

8.9 Address Groups

Address groups combine multiple address objects or other groups into logical collections.

Firewall Toolbox processes these relationships and can provide documentation showing how address objects are grouped.

[Screenshot: Address Groups documentation]

This helps answer questions such as:

- Which objects belong to a particular group?
- Are groups nested inside other groups?
- Which network resources are represented by a group?
- Does a group still contain valid and required objects?

Understanding group membership is important because a single group can be referenced by multiple firewall rules, NAT policies, VPN configurations, or user access rights.

8.10 Zones

Zones are a fundamental part of the SonicWall security architecture.

Firewall Toolbox provides documentation of the configured zones and their relevant settings.

[Screenshot: Zones documentation]

Typical zones may include:

- LAN
- WAN
- DMZ
- WLAN
- VPN
- Custom zones

Zone documentation helps provide an overview of the logical security structure of the firewall.

It is also useful when reviewing firewall rules because rules are generally defined between source and destination zones.

8.11 Interfaces

Firewall Toolbox documents the available firewall interfaces and their relationship to the configured zones.

[Screenshot: Interfaces documentation]

Depending on the available information, interface documentation can help identify:

- Interface names
- Zone assignments

- Interface roles
- Network assignments
- WAN interfaces
- Internal interfaces

This information is useful for understanding the physical and logical network topology connected to the firewall.

8.12 Interfaces and Network Topology

Interface documentation can provide the foundation for creating or maintaining a network diagram.

For example, an administrator can use the information to determine which firewall interfaces connect to:

- Internet connections
- Internal LANs
- DMZ networks
- Wireless networks
- Server networks
- Management networks
- Additional security zones

Tip:
Firewall Toolbox documentation can provide much of the technical information required for a network diagram, but the report itself does not replace a graphical topology diagram.

8.13 Users

User accounts configured on the firewall can also be included in the documentation.

[Screenshot: User documentation]

This provides an overview of locally configured users and the information available for those accounts.

User documentation can be useful during:

- Security reviews
- Account cleanup
- System handovers
- Permission reviews
- Troubleshooting

Accounts that are no longer required should be reviewed and removed according to the organization's account management procedures.

8.14 User Groups

Firewall Toolbox can document user groups and their relationships.

[Screenshot: User Groups documentation]

Group membership is particularly important because permissions are often assigned to groups rather than directly to individual users.

A user may therefore receive access to network resources indirectly through membership in one or more groups.

The documentation helps make these relationships easier to understand.

8.15 User Access Rights

SonicWall configurations can assign access rights to users or groups.

Firewall Toolbox analyzes these assignments and provides corresponding documentation.

[Screenshot: User Access Rights documentation]

This can help determine which users or groups have access to particular network resources.

Such documentation is useful for both security reviews and general access management.

8.16 VPN Documentation

VPN configurations are often business-critical and should be included in technical firewall documentation.

Firewall Toolbox processes available VPN information and provides structured reports describing the configured VPN environment.

[Screenshot: VPN documentation]

Depending on the configuration, the documentation may include information relating to:

- Site-to-site VPN policies
- Remote networks
- VPN policy parameters
- Authentication and encryption settings
- Other available VPN information

This documentation can be useful when troubleshooting VPN connections, replacing a firewall, or transferring responsibility for an environment to another administrator.

8.17 Documenting High Availability

Where the analyzed firewall is part of a High Availability cluster, this information should also form part of the technical documentation.

[Screenshot: HA documentation]

Knowing that an appliance is part of an HA pair is important when planning:

- Firmware upgrades
- Hardware maintenance
- Network changes
- Firewall replacement
- Troubleshooting
- Disaster recovery procedures

Firewall Toolbox identifies the HA context where the required information is available.

8.18 Documentation for System Handovers

One of the most useful applications of the Documentation section is the handover of an existing firewall environment.

When responsibility for a firewall moves to another administrator, IT department, or service provider, the new team needs to understand the existing configuration.

Firewall Toolbox can significantly reduce the effort required to collect this information.

A documentation package can provide an overview of:

- Network structure
- Firewall rules
- NAT policies
- Objects and groups
- Interfaces and zones
- Users and permissions
- VPNs
- Other relevant firewall settings

Tip:
Generate a new documentation report immediately before a system handover so that the documentation reflects the current configuration.

8.19 Documentation for Customers

IT service providers can use Firewall Toolbox reports as part of their customer documentation.

Instead of manually creating configuration lists, reports can be generated directly from the firewall data.

This can be useful for:

- Initial customer assessments
- Project completion documentation
- Firewall migrations
- Regular maintenance reports
- Customer handovers
- Compliance documentation
- Internal customer IT records

The report language can be selected according to the recipient.

8.20 Documentation Before Configuration Changes

Creating documentation before significant configuration changes provides a useful reference to the previous state of the firewall.

For example, before:

- Replacing a firewall
- Migrating to a new appliance
- Redesigning firewall rules
- Modifying network zones
- Reworking VPN configurations
- Performing a major cleanup

a complete documentation report can provide an additional record of the existing environment.

This does not replace a configuration backup, but complements it by providing the configuration in a human-readable format.

8.21 Documentation and Configuration Backups

Documentation and backups serve different purposes.

A **configuration backup** is primarily intended to restore a firewall configuration.

A **documentation report** is intended to make the configuration understandable to people.

Both are important.

A configuration backup may contain everything required to restore an appliance, but it is not necessarily suitable for quickly answering questions about firewall rules, network objects, interfaces, or user permissions.

Similarly, a PDF report provides useful technical documentation but cannot replace an EXP configuration backup.

Important:
Maintain both configuration backups and human-readable documentation for important firewall environments.

8.22 Keeping Documentation Current

Firewall documentation becomes less useful as the actual firewall configuration changes.

For this reason, documentation should be regenerated after significant configuration changes or as part of a regular maintenance schedule.

Because Firewall Toolbox creates the documentation automatically from the current firewall data, updating the documentation requires considerably less effort than maintaining the same information manually.

A practical workflow is:

1. Retrieve a current TSR and EXP.
2. Import the files into Firewall Toolbox.
3. Generate the required documentation.
4. Store the report with the corresponding audit date.
5. Repeat the process after significant changes or during the next scheduled review.

8.23 Sensitive Information in Documentation

Firewall documentation can contain security-sensitive information.

Depending on the selected reports, the documentation may reveal details about:

- Internal IP addressing
- Network structure
- Firewall rules
- Published services
- Administrative configuration
- VPN connections
- User accounts
- Access permissions

Generated reports should therefore be handled as confidential technical documentation.

Important:
Store and distribute Firewall Toolbox reports according to your organization's security requirements. Avoid sending complete firewall documentation to recipients who do not require access to the contained information.

8.24 Recommended Documentation Workflow

A practical documentation workflow can follow these steps:

1. Retrieve current TSR and EXP files from the firewall.
2. Import the data into Firewall Toolbox.
3. Verify that the correct firewall has been loaded.
4. Select the required report language.
5. Generate the Documentation Summary or the required individual reports.
6. Review the generated documentation for completeness.
7. Add external information where necessary, such as network diagrams, provider details, or operational procedures.
8. Store the final documentation in an appropriate protected location.
9. Regenerate the documentation after significant configuration changes.

This approach provides a repeatable method for maintaining current technical firewall documentation.

8.25 Next Steps

Documentation explains **what is configured**.

The next chapter, **Maintenance**, focuses on determining **what may no longer be required or what should be reviewed and cleaned up**.

This includes functions for identifying unused and disabled firewall rules, unused NAT policies, unused address objects, duplicate objects, naming inconsistencies, and modified TCP timeout settings.

For several of these areas, Firewall Toolbox can go one step further: after identifying the relevant configuration elements, the integrated SonicWall API functions can be used to perform selected maintenance operations directly on the firewall.

9. Maintenance

The **Maintenance** section of Firewall Toolbox helps identify configuration elements that may no longer be required, have become inconsistent over time, or deserve periodic review.

Firewall configurations rarely remain static. New rules, NAT policies, address objects, VPNs, and exceptions are continuously added as requirements change.

While adding a new configuration is usually straightforward, removing obsolete configuration elements is often neglected.

The result can be a firewall configuration containing rules and objects that nobody is entirely sure about anymore.

[Screenshot: Maintenance menu]

Firewall Toolbox helps identify these elements and, for selected functions, provides API-based tools to clean up the configuration directly.

9.1 Purpose of Regular Firewall Maintenance

A firewall configuration that has been operating for many years can contain a significant amount of historical configuration.

Typical examples include:

- Rules for applications that no longer exist
- Rules that have been disabled for years
- NAT policies for decommissioned servers
- Address objects that are no longer referenced
- Duplicate address objects
- Temporary configuration exceptions
- Inconsistent object names
- Modified timeout settings
- Configuration elements created during troubleshooting

These items may not cause an immediate technical problem, but they increase complexity.

A complex configuration is more difficult to:

- Understand
- Audit
- Troubleshoot
- Document
- Modify safely
- Transfer to another administrator

Regular maintenance therefore improves both manageability and security.

9.2 Maintenance Summary

The **Maintenance Summary** combines the available maintenance analyses into a single report.

[Screenshot: Maintenance Summary report]

This provides a convenient overview of configuration elements that may be candidates for cleanup or further investigation.

The report can be used as the starting point for a regular firewall maintenance process.

Important:
An item appearing in a Maintenance report is not automatically safe to delete. Firewall Toolbox identifies potential candidates for review. The administrator must determine whether the configuration element is still required.

9.3 Disabled Firewall Rules

Firewall Toolbox identifies firewall rules that are currently disabled.

[Screenshot: Disabled Firewall Rules report]

Disabled rules are not actively processing traffic, but they remain part of the firewall configuration.

There are many valid reasons for temporarily disabling a rule. For example:

- Troubleshooting
- Application migration
- Temporary service shutdown
- Testing
- Planned future use

However, rules that have remained disabled for a long period may no longer be required.

The report provides a convenient way to review these rules and determine whether they should remain in the configuration.

9.4 Unused Firewall Rules

Firewall Toolbox uses available usage information to identify firewall rules that appear to be unused.

Depending on the report, this can include:

- Rules that have never been used
- Rules that have not been used for an extended period

[Screenshot: Unused Firewall Rules report]

These rules are useful candidates for maintenance review.

However, usage information alone should never be the only reason for deleting a rule.

Some rules may intentionally be used only in exceptional situations.

Examples include:

- Disaster recovery
- Emergency administration
- Backup systems
- Seasonal applications
- External support access
- Rarely used business processes

Important:
Always determine the purpose of a rule before removing it.

9.5 Disabling Before Deleting

When the purpose of an apparently unused firewall rule is uncertain, disabling the rule first can provide a safer alternative to immediate deletion.

Firewall Toolbox supports this workflow through its API functionality.

Instead of permanently removing a selected rule, the administrator can disable it.

The rule remains in the configuration but no longer processes traffic.

This provides an opportunity to determine whether disabling the rule causes any operational problems before permanently deleting it.

[Screenshot: API function – Disable Firewall Rules]

This functionality was introduced specifically to support a more controlled cleanup process.

Tip:
For older configurations, consider a staged cleanup process: **identify → review → disable → observe → delete**.

9.6 Firewall Rules Disabled by Firewall Toolbox

When Firewall Toolbox disables a firewall rule through the API, the operation can be identified in the configuration.

This makes it possible to distinguish rules that were intentionally disabled as part of a Firewall Toolbox maintenance operation.

[Screenshot: Rules Disabled by Firewall Toolbox report]

These rules can subsequently be reviewed after an appropriate observation period.

If no problems have occurred and the rule is confirmed to be unnecessary, it can then be permanently removed.

This provides a safer workflow than immediately deleting a rule whose purpose is uncertain.

9.7 Disabled NAT Policies

Like firewall rules, NAT policies may remain in the configuration even when they are disabled.

Firewall Toolbox identifies disabled NAT policies and lists them in the corresponding report.

[Screenshot: Disabled NAT Policies report]

A disabled NAT policy may represent:

- A decommissioned service
- A previous server
- An old Internet connection
- A temporary configuration
- A migration
- A troubleshooting configuration

The report allows these policies to be reviewed as part of regular maintenance.

9.8 Unused NAT Policies

Where sufficient usage information is available, Firewall Toolbox can also identify NAT policies that appear to be unused.

[Screenshot: Unused NAT Policies report]

As with firewall rules, an unused NAT policy should be investigated before it is removed.

The corresponding firewall rules and address objects should also be considered because these configuration elements are often related.

9.9 API Operations for Firewall Rules and NAT Policies

For supported maintenance reports, Firewall Toolbox can use the SonicWall API to modify the identified policies.

Depending on the selected function, available operations can include:

- Disable selected policies
- Delete selected policies

The API operation window displays the identified records and allows the administrator to select the individual items to be processed.

[Screenshot: API policy selection window]

This means that a report containing many findings does not require all items to be modified.

The administrator remains in control of which policies are selected.

Warning:
Deleting a firewall rule or NAT policy modifies the active firewall configuration and may immediately affect network connectivity. Review each selected policy carefully before executing the operation.

9.10 Unused Address Objects

Address objects are used throughout a SonicWall configuration.

They can be referenced by:

- Firewall rules
- NAT policies
- Address groups
- VPN configurations
- Routing policies
- DNS-related configuration
- User access rights
- Other configuration elements

Over time, address objects may remain in the configuration even after the associated system or policy has been removed.

Firewall Toolbox analyzes these relationships to identify address objects that appear to be unused.

[Screenshot: Unused Address Objects report]

9.11 How Unused Address Objects Are Determined

Simply checking whether an address object appears directly in a firewall rule is not sufficient.

An object may be used indirectly through an address group or another configuration element.

Firewall Toolbox therefore analyzes multiple configuration areas when determining whether an address object is in use.

This reduces the risk of incorrectly identifying an object as unused simply because it does not appear directly in a firewall rule.

Important:
Complex configurations can contain dependencies that are not immediately obvious. The list of unused address objects should therefore still be reviewed before performing a deletion.

9.12 Deleting Unused Address Objects Through the API

Firewall Toolbox provides an API function for removing selected unused address objects.

[Screenshot: API function – Delete Unused Address Objects]

The identified objects are displayed in a selection window.

The administrator can then choose:

- A single object
- Multiple objects
- All displayed objects

Only the selected objects are submitted for deletion.

This can significantly reduce the effort required to clean up large configurations containing many historical address objects.

9.13 Duplicate Address Objects

Firewall configurations sometimes contain multiple address objects representing the same host, network, or IP address.

For example:

Server01
192.168.10.20

and

WebServer
192.168.10.20

may both refer to the same system.

Firewall Toolbox can identify potential duplicate address objects and list them in a dedicated report.

[Screenshot: Duplicate Address Objects report]

Duplicate objects are not necessarily incorrect.

There may be valid reasons for using different logical object names for the same address.

However, unnecessary duplicates can make the configuration more difficult to understand and maintain.

9.14 Reviewing Duplicate Objects

Before removing a duplicate object, determine where each object is used.

One object may be referenced by firewall rules while another is used by a NAT policy, VPN, group, or other configuration.

A cleanup may therefore require replacing references before the duplicate object itself can be deleted.

The Duplicate Address Objects report should primarily be used to identify candidates for consolidation.

9.15 Address Object Naming

Consistent naming conventions make firewall configurations considerably easier to understand.

Firewall Toolbox can analyze address object names and help identify naming inconsistencies.

[Screenshot: Address Object Naming report]

A well-designed naming convention can provide information such as:

- Object type
- Location
- Network
- Function
- Customer
- System role

For example, an administrator looking at an object name should ideally be able to understand its purpose without first opening the object configuration.

Naming conventions are particularly valuable in environments containing hundreds or thousands of objects.

9.16 TCP Connection Timeout Analysis

Firewall Toolbox includes a dedicated analysis of **TCP Connection Timeout** settings.

A SonicWall firewall maintains information about active TCP connections in its connection table.

The TCP timeout determines how long an inactive connection remains in the table before the firewall removes it.

A global TCP timeout provides the default behavior, but individual firewall rules can also use different timeout values.

[Screenshot: TCP Timeout report]

9.17 Why Modified TCP Timeouts Matter

There are valid reasons for increasing the TCP timeout for particular applications or long-lived connections.

However, problems can arise when timeout values are set unnecessarily high or remain configured long after the original requirement has disappeared.

The longer inactive connections remain in the connection table, the longer the firewall must maintain those sessions.

On heavily utilized systems, unnecessarily high timeout values may therefore have an operational impact.

Modified values are also easy to overlook during a normal firewall review because they are configured within individual rules.

9.18 Identifying Modified TCP Timeouts

Firewall Toolbox analyzes the global TCP timeout as well as the configured firewall rules.

Rules that use an individual TCP timeout can be identified and displayed in a dedicated report.

The report makes it easy to determine:

- Which rules differ from the default
- Which TCP timeout is configured
- Which policies should be reviewed

[Screenshot: Firewall Rules with Modified TCP Timeout report]

This is particularly useful for firewall configurations that have evolved over many years.

A timeout may have been modified for a temporary requirement and then forgotten.

9.19 Resetting TCP Timeouts Through the API

Firewall Toolbox can also reset selected TCP timeout settings through the SonicWall API.

[Screenshot: Reset TCP Timeout API window]

The API window displays the firewall rules whose TCP timeout differs from the standard value.

The administrator can select:

- An individual rule
- Multiple rules
- All displayed rules

The selected policies can then be reset to the standard TCP timeout value.

This combines three important maintenance steps in a single workflow:

Identify – Document – Correct

Important:
Before resetting a TCP timeout, verify whether the modified value was intentionally configured for a particular application.

9.20 Backups Before API Changes

Firewall Toolbox implements backup mechanisms before supported API configuration changes are performed.

Before modifying the firewall, the current configuration information is stored, including the corresponding TSR and EXP files.

Firewall Toolbox also records the API operations associated with the change.

[Screenshot: API backup / operation information]

This provides important information that can be used if a configuration change needs to be reviewed or reversed.

Important:
A backup provides an important recovery mechanism, but it does not eliminate the need to carefully review configuration changes before executing them.

9.21 Maintaining Older Firewall Configurations

The Maintenance section is particularly useful for configurations that have evolved over many years.

Such configurations often contain multiple generations of:

- Network designs
- Servers
- Applications
- VPN connections
- Internet connections
- Administrators
- Naming conventions
- Security policies

Attempting to clean up everything at once can introduce unnecessary risk.

A staged approach is usually more appropriate.

For example:

1. Identify potentially unused elements.
2. Review their purpose and dependencies.
3. Document the current configuration.
4. Disable policies where appropriate.
5. Observe the environment.

6. Remove confirmed obsolete configuration.
7. Perform another audit.

This allows the configuration to be simplified gradually while reducing the risk of disrupting required services.

9.22 Re-Auditing After Maintenance

After completing significant maintenance operations, it is recommended to perform another audit.

Retrieve a new TSR and EXP from the firewall and import them into Firewall Toolbox.

The new audit can then confirm that:

- Deleted objects are no longer present
- Disabled or deleted policies have been removed from the relevant findings
- TCP timeout values have been corrected
- The configuration remains consistent
- No unexpected issues are visible

The resulting Full Audit Report also provides updated documentation of the firewall after the maintenance work.

9.23 Recommended Maintenance Workflow

A regular maintenance process can follow this sequence:

1. Retrieve the current TSR and EXP.
2. Perform a Full Audit.
3. Review the Maintenance Summary.
4. Review disabled firewall rules and NAT policies.
5. Investigate rules and policies that appear to be unused.
6. Review unused address objects.
7. Examine duplicate address objects.
8. Review naming inconsistencies.
9. Check modified TCP timeout settings.
10. Determine which configuration elements are genuinely obsolete.
11. Create or verify current backups.
12. Disable uncertain policies before deleting them where appropriate.
13. Use the API functions for supported maintenance operations.

14. Verify connectivity and critical services after changes.
15. Retrieve a new TSR and EXP.
16. Perform another audit to verify and document the resulting configuration.

Regular maintenance helps keep the firewall configuration understandable and reduces the amount of obsolete configuration that accumulates over time.

9.24 Next Steps

The previous chapters have examined the five primary areas of Firewall Toolbox:

Security Audit – Health – Configuration Audit – Documentation – Maintenance

The next chapter brings these areas together.

Full Audit and the All-in-One Report explains how Firewall Toolbox combines the different analyses into a comprehensive report, how the Highlights and Recommendations section works, how the report is structured, and how the different report languages can be used.

10. Full Audit and the All-in-One Report

The **Full Audit Report**, also referred to as the **All-in-One Report**, provides the most comprehensive view of a SonicWall firewall available in Firewall Toolbox.

Instead of generating and reviewing numerous reports individually, the Full Audit Report combines the major analyses and documentation into one structured PDF document.

With Firewall Toolbox Version 3, the Full Audit Report is also automatically generated when new firewall data is imported.

[Screenshot: Full Audit Report – Cover Page]

10.1 Purpose of the Full Audit Report

Different people may require different levels of information about a firewall.

An administrator may need detailed information about individual rules, objects, interfaces, or VPNs.

A technical manager may primarily be interested in significant security or configuration findings.

A customer may require both a high-level overview and detailed technical documentation.

The Full Audit Report is designed to address these different requirements within a single document.

It combines:

- Important findings and recommendations
- Security analyses
- Health information
- Configuration analyses
- Technical documentation
- Maintenance information

This allows the report to serve both as an audit document and as technical documentation of the firewall.

10.2 Automatic Report Generation

One of the major workflow improvements introduced with Version 3 is the automatic generation of the Full Audit Report.

Previously, importing firewall data and generating reports were separate steps.

In Version 3, the required analyses are performed as part of the data import process.

[Screenshot: Data import and audit progress]

Once the TSR and EXP files have been processed, the Full Audit Report is already available.

The completion dialog provides direct access to the generated report.

[Screenshot: Data Upload and Audit completed successfully]

This means that a complete firewall assessment is available immediately after the configuration data has been imported.

10.3 The All-in-One Concept

The Full Audit Report follows an **All-in-One** concept.

Rather than requiring separate documents for security, health, configuration, documentation, and maintenance, the relevant information is combined into one report.

This provides several advantages:

- One document contains the complete assessment
- Findings can be viewed together with detailed configuration information
- The document can be archived as a snapshot of the firewall
- Customers or colleagues can receive one consistent report
- The same report can support both review and documentation activities

Individual and category reports remain available when a smaller or more focused document is required.

10.4 Report Structure

The Full Audit Report follows the same basic structure as the Firewall Toolbox user interface.

The major sections correspond to the five main categories:

- Security Audit
- Health
- Configuration Audit
- Documentation
- Maintenance

[Screenshot: Full Audit Report – Category structure]

This consistent structure makes it easier to move between the application and the generated report.

A user who identifies an interesting result in the PDF can locate the corresponding area in Firewall Toolbox using the same category structure.

10.5 Highlights and Recommendations

At the beginning of the Full Audit Report, Firewall Toolbox provides a **Highlights and Recommendations** section.

[Screenshot: Highlights and Recommendations]

This section summarizes important findings identified during the analysis.

The objective is to make significant results immediately visible without requiring the reader to review the complete technical report first.

Depending on the analyzed configuration, this section can contain findings relating to:

- Security
- Configuration
- Health
- Maintenance
- Other noteworthy conditions

This makes the beginning of the report particularly useful for an initial review.

10.6 From Overview to Technical Detail

The Full Audit Report is designed to support two different levels of review.

The first level is the **overview**.

The Highlights and Recommendations section provides a compact summary of important findings.

The second level is the **technical detail**.

The remaining sections contain the individual analyses, explanations, configuration information, and documentation required to investigate the findings in detail.

A reader can therefore begin with the summary and only investigate the areas that require additional attention.

10.7 Understanding Recommendations

Recommendations generated by Firewall Toolbox are based on conditions identified in the imported firewall configuration.

They should be treated as indications that a configuration deserves review.

A recommendation does not necessarily mean that the current configuration is incorrect.

For example, a firewall rule that appears unusually permissive may have a valid business requirement.

Similarly, an old or unused configuration element may intentionally remain available for emergency purposes.

Important:
Always evaluate recommendations in the context of the individual network, application requirements, and organizational security policies before making configuration changes.

Firewall Toolbox provides the technical information required for the review, while the final decision remains with the administrator.

10.8 Report Explanations

Firewall Toolbox reports contain explanatory text in addition to the actual analysis results.

[Screenshot: Report explanation followed by results]

These explanations describe:

- What is being analyzed
- Why the setting is relevant
- What the result may indicate
- What should be considered when evaluating the finding

This makes the report useful not only to experienced SonicWall administrators but also to readers who may be less familiar with a particular firewall function.

10.9 Table of Contents

Because a Full Audit Report can contain many pages, a structured table of contents is included.

[Screenshot: Full Audit Report – Table of Contents]

The table of contents lists the major categories and individual report sections together with their corresponding page numbers.

This makes it possible to quickly locate a specific analysis without manually searching through the document.

The table of contents is generated automatically based on the reports included in the Full Audit.

10.10 Category Sections

Each major report category begins with its own section.

[Screenshot: Security Audit category page]

These category pages visually separate the different areas of the Full Audit Report and make the document easier to navigate.

The category sections correspond directly to the Firewall Toolbox menu structure:

Security Audit
Security-related configuration and findings.

Health
Operational and service-related information.

Configuration Audit
Important operational configuration settings.

Documentation
Detailed technical firewall configuration.

Maintenance
Configuration elements that may require cleanup or review.

10.11 Individual Reports Within the Full Audit

Within each category, the corresponding individual reports are generated in sequence.

A typical report contains a title, an explanation, and the actual results.

Depending on the type of analysis, the result may be presented as:

- A table
- A configuration overview
- A list of findings
- Status information
- Recommendations
- Detailed technical information

[Screenshot: Example report within Full Audit]

The exact reports included depend on the firewall configuration, Firewall Toolbox settings, and available functionality.

10.12 IPv4 and IPv6 Content

Where applicable, Firewall Toolbox can include both IPv4 and IPv6 reports.

Whether IPv6 reports are included depends on:

- Whether IPv6 is enabled on the analyzed firewall
- The Firewall Toolbox IPv6 reporting setting
- Whether an IPv6 version of the corresponding analysis is available

If IPv6 is not used, IPv6-specific content can be omitted to keep the Full Audit Report focused and more compact.

10.13 Report Language

The Full Audit Report can be generated in any of the supported report languages:

- English

- German
- French
- Italian
- Spanish

[Screenshot: Report language selection]

The selected language applies to the report content as well as the explanatory information provided with the analyses.

The Firewall Toolbox user interface itself remains in English.

This allows an administrator to work with a consistent English interface while producing documentation in the language required by a customer or organization.

10.14 Generating Reports for Different Recipients

Different recipients may require different versions of the same firewall information.

For example:

Technical administrator

May require the complete Full Audit Report including detailed configuration information.

IT manager

May primarily be interested in the Highlights and Recommendations and the most important audit findings.

Customer

May require a Full Audit Report in the local language.

Support engineer

May require only a specific technical report.

For this reason, Firewall Toolbox provides the Full Audit Report, category reports, and individual reports.

The appropriate report can be selected according to the purpose.

10.15 Full Audit Versus Category Reports

The Full Audit Report is the most comprehensive option, but it is not always necessary.

A category report may be more appropriate when the scope is limited.

For example:

- Use **Security Audit** for a security-focused review.
- Use **Health** for an operational review.

- Use **Configuration Audit** for configuration assessment.
- Use **Documentation** when technical documentation is required.
- Use **Maintenance** when planning configuration cleanup.

Use the **Full Audit Report** when a complete assessment and documentation package is required.

10.16 Full Audit as a Configuration Snapshot

A Full Audit Report can also serve as a human-readable snapshot of the firewall at a particular point in time.

When stored together with the corresponding TSR and EXP files, it provides three useful elements:

TSR
Technical and diagnostic information.

EXP
Restorable firewall configuration.

Full Audit Report
Human-readable analysis and documentation.

Together, these provide a useful record of the firewall state at the time of the audit.

Tip:
Consider retaining the Full Audit Report together with its corresponding TSR and EXP files, particularly before major configuration changes or firewall migrations.

10.17 Comparing Audits Over Time

Regular Full Audits provide a way to review how a firewall configuration evolves.

For example, audits from different dates can help identify:

- New firewall rules
- Removed policies
- Configuration changes
- Changes in utilization
- Firmware updates
- New or removed VPNs
- License changes
- Maintenance improvements

Firewall Toolbox does not require the administrator to manually recreate documentation after every change. A new audit can generate an updated report from the current firewall data.

10.18 Using the Full Audit for Regular Reviews

The Full Audit Report is particularly useful as part of a scheduled firewall review process.

For example, an organization may decide to perform a complete firewall audit:

- Monthly
- Quarterly
- Every six months
- Annually
- Before major infrastructure changes
- After significant configuration changes

The appropriate interval depends on the environment, change frequency, security requirements, and organizational policies.

Regular audits can help identify configuration drift and obsolete settings before they accumulate over many years.

10.19 Using Findings as the Basis for Maintenance

The Full Audit Report is not intended to be the end of the process.

Findings can be used as the basis for further investigation and maintenance.

A typical workflow is:

1. Generate the Full Audit Report.
2. Review Highlights and Recommendations.
3. Investigate the relevant detailed sections.
4. Determine whether a configuration change is required.
5. Identify the affected configuration elements.
6. Use a corresponding API function where available.
7. Verify the result.
8. Perform another audit if significant changes were made.

This creates a continuous process of:

Analyze → Understand → Decide → Change → Verify → Document

10.20 Reports as Confidential Information

A Full Audit Report can contain extensive information about the firewall and the protected network.

Depending on the configuration, this may include:

- Internal IP addresses
- Network topology
- Firewall rules
- Published services
- VPN information
- Users and permissions
- Administrative configuration
- Security findings

The Full Audit Report should therefore be treated as confidential technical information.

Important:
Store and distribute Full Audit Reports only through appropriately protected systems and only provide them to recipients who require access to the contained information.

10.21 Recommended Full Audit Workflow

For a complete firewall assessment, the following workflow is recommended:

1. Retrieve current TSR and EXP files.
2. Import the files into Firewall Toolbox.
3. Allow the automatic Full Audit to complete.
4. Open the generated Full Audit Report.
5. Review Highlights and Recommendations.
6. Use the table of contents to navigate to relevant findings.
7. Review the corresponding detailed reports.
8. Determine which findings require action.
9. Generate additional individual reports where required.
10. Perform supported configuration changes through the API where appropriate.
11. Verify the firewall after any changes.
12. Retrieve new TSR and EXP files after significant maintenance.
13. Generate a new Full Audit Report to document the resulting configuration.
14. Store the report and corresponding configuration files according to the organization's documentation and security requirements.

10.22 Next Steps

The Full Audit Report brings together the analysis, documentation, and maintenance capabilities of Firewall Toolbox.

The next chapter covers one of the other major capabilities of the software in detail: **Working with the SonicWall API**.

This chapter explains how Firewall Toolbox connects to a firewall, how API operations are performed, how objects and policies are selected for modification, what backup and recovery mechanisms are used, and how Firewall Toolbox helps make configuration changes controlled and traceable.

11. Working with the SonicWall API

The integrated **SonicWall API functionality** extends Firewall Toolbox beyond analysis and reporting.

While reports identify configuration issues and maintenance candidates, the API functions allow selected changes to be performed directly on the firewall.

This creates a workflow in which Firewall Toolbox can:

Identify → Analyze → Select → Modify → Verify

[Screenshot: Firewall Toolbox API functions]

The API is also used to automatically retrieve the TSR and EXP files required for an audit.

11.1 Purpose of the API Integration

Without API access, Firewall Toolbox can still analyze manually exported TSR and EXP files and generate the corresponding reports.

API integration provides two additional capabilities:

Automated data retrieval

Firewall Toolbox can connect to the SonicWall and retrieve the required firewall data automatically.

Configuration changes

Selected maintenance operations can be performed directly from Firewall Toolbox.

Depending on the function, these operations include:

- Disabling firewall rules
- Deleting firewall rules
- Disabling NAT policies
- Deleting NAT policies
- Deleting unused address objects
- Resetting modified TCP timeout values

This eliminates many repetitive manual configuration steps.

11.2 Requirements for API Access

Before Firewall Toolbox can communicate with a SonicWall through the API, API access must be available on the firewall.

The computer running Firewall Toolbox must also be able to reach the firewall management interface.

The connection requires:

- Firewall IP address or hostname
- HTTPS management port

- Administrative username
- Password

[Screenshot: API Connection dialog]

The administrative account must have sufficient permissions for the requested operation.

Important:
API access provides the ability to modify the active firewall configuration. Access credentials should therefore be protected in the same way as other administrative firewall credentials.

11.3 Enabling the SonicWall API

The SonicWall API must be enabled in SonicOS before Firewall Toolbox can use it.

The exact location of the setting may differ depending on the SonicOS version.

After enabling API access, verify that the management interface is reachable from the computer running Firewall Toolbox.

[Screenshot: SonicOS – Enable API setting]

Security Note:
API access should only be permitted from trusted management networks. Avoid unnecessarily exposing firewall management services to untrusted networks.

11.4 Establishing an API Connection

When an API operation is started, Firewall Toolbox establishes a secure HTTPS connection to the firewall.

The connection information identifies the firewall and provides the credentials required for authentication.

[Screenshot: Enter API connection information]

After successful authentication, Firewall Toolbox can perform the requested operation according to the permissions of the account.

If the connection cannot be established, verify:

- IP address or hostname
- HTTPS management port
- Network connectivity
- API status on the firewall
- Username and password
- Administrative permissions
- SSL certificate settings

11.5 SSL Certificate Handling

SonicWall management interfaces frequently use certificates that may not be trusted by the Windows computer running Firewall Toolbox.

This can occur, for example, when:

- The firewall uses a self-signed certificate
- The certificate was issued by an internal CA
- The certificate name does not match the address used for the connection

Firewall Toolbox provides an option for environments where SSL certificate validation needs to be handled accordingly.

[Screenshot: Ignore SSL Certificate Error option]

Security Note:
Certificate validation provides protection against connecting to an unexpected system. Ignoring certificate errors should therefore only be used when the identity of the firewall and the management network are trusted.

11.6 Retrieving Firewall Data Through the API

One of the most convenient uses of the API is retrieving the files required for an audit.

Instead of manually logging in to the SonicWall, creating a TSR, exporting the configuration, downloading both files, and then selecting them in Firewall Toolbox, the application can automate the process.

[Screenshot: API download function]

Firewall Toolbox retrieves the required information and stores the resulting files in the firewall repository.

The data can then immediately be imported and analyzed.

With Version 3, this process also leads directly to the automatic generation of the Full Audit Report.

11.7 From Report to API Operation

Several Firewall Toolbox reports are directly associated with API maintenance functions.

For example, a report may identify:

- Unused firewall rules
- Disabled firewall rules
- Unused NAT policies
- Disabled NAT policies

- Unused address objects
- Modified TCP timeout settings

The corresponding API function uses the results of the analysis to present the relevant configuration elements.

[Screenshot: Report and corresponding API operation]

This means that the administrator does not need to manually locate every identified object again in the SonicWall management interface.

11.8 Selecting Objects and Policies

Before an API modification is performed, Firewall Toolbox displays the affected objects or policies in a selection window.

[Screenshot: API selection window]

Depending on the function, information can include:

- Policy or object name
- Source and destination
- Zone information
- Current status
- UUID
- Other relevant configuration information

The administrator can select exactly which records should be processed.

Depending on the operation, it is possible to select:

- A single record
- Multiple records
- All displayed records

This provides control over the scope of the operation.

11.9 Reviewing the Selection

Before executing an API operation, review the selected records carefully.

This is particularly important for deletion operations.

A report may identify a configuration element as unused based on the available firewall information, but the administrator should still consider its purpose and possible dependencies.

Important:
Firewall Toolbox assists with identifying and processing configuration elements. It does not replace the administrator's assessment of whether a particular object or policy is still required.

For uncertain firewall rules or NAT policies, disabling them first may be preferable to immediate deletion.

11.10 Disabling Firewall Rules

Firewall Toolbox can disable selected firewall rules through the SonicWall API.

[Screenshot: Disable Firewall Rules API function]

This is particularly useful when cleaning up older rule sets.

Instead of immediately deleting a rule that appears to be obsolete, it can first be disabled.

The administrator can then observe the environment and determine whether the rule is still required.

This supports the maintenance workflow:

Identify → Disable → Observe → Delete

11.11 Identifying Rules Disabled by Firewall Toolbox

When a rule is disabled through Firewall Toolbox, the operation is documented so that the rule can subsequently be identified.

[Screenshot: Firewall rules disabled by Firewall Toolbox]

This helps distinguish rules disabled as part of a controlled maintenance operation from rules that may have been disabled manually for another reason.

After an appropriate observation period, these rules can be reviewed again.

If no operational requirement remains, they can then be considered for permanent deletion.

11.12 Deleting Firewall Rules

Firewall Toolbox can permanently delete selected firewall rules through the API.

[Screenshot: Delete Firewall Rules API function]

Deletion should only be performed after the purpose and dependencies of the rule have been evaluated.

Warning:
Deleting a firewall rule can immediately affect network connectivity. A deleted rule may interrupt application traffic, administrative access, VPN communication, or other services.

For rules whose purpose is uncertain, consider disabling them first.

11.13 Disabling NAT Policies

NAT policies can also be disabled through Firewall Toolbox.

[Screenshot: Disable NAT Policies API function]

This provides the same staged cleanup approach available for firewall rules.

A NAT policy can be disabled while remaining in the configuration, allowing the administrator to determine whether it is still required before permanently removing it.

11.14 Deleting NAT Policies

Selected NAT policies can be permanently deleted through the API.

[Screenshot: Delete NAT Policies API function]

Before deleting a NAT policy, consider the corresponding:

- Firewall rules
- Address objects
- Published services
- VPN configurations
- Routing requirements
- External DNS configuration

A NAT policy may be used only by a specific service that is not continuously active.

Warning:
Deleting a NAT policy can immediately make a published or translated service unavailable.

11.15 Deleting Unused Address Objects

Firewall Toolbox analyzes multiple configuration areas to determine whether address objects appear to be unused.

Objects identified by this analysis can be presented in the API deletion window.

[Screenshot: Delete Unused Address Objects]

The administrator can select individual, multiple, or all displayed objects for deletion.

This can significantly simplify the cleanup of configurations containing large numbers of historical objects.

Important:
Review the selected objects before deletion, particularly in complex configurations containing nested groups or unusual dependencies.

11.16 Resetting TCP Timeout Values

Firewall Toolbox identifies firewall rules whose TCP timeout differs from the standard value.

The corresponding API function displays only the affected rules.

[Screenshot: Reset TCP Timeout API function]

The administrator can select the rules whose timeout should be reset.

This can be performed for:

- One rule
- Multiple rules
- All displayed rules

The selected TCP timeout values are then returned to the standard setting.

Important:
A modified TCP timeout may have been configured intentionally for a particular application. Verify the requirement before resetting the value.

11.17 Backup Before Configuration Changes

Before supported API configuration changes are made, Firewall Toolbox creates a backup of the firewall configuration.

This includes the relevant firewall configuration and diagnostic information, including:

- EXP configuration
- TSR information

[Screenshot: API backup directory]

The backup provides a reference to the state of the firewall before the operation was performed.

Important:
The backup should be retained until the configuration change has been verified and the affected services have been confirmed to operate correctly.

11.18 Recording API Commands

In addition to the configuration backup, Firewall Toolbox records the API operations performed during the modification process.

[Screenshot: API command backup/log]

This provides a trace of the changes made by Firewall Toolbox and can assist with:

- Troubleshooting
- Change documentation
- Reviewing previous operations
- Reversing changes where supported

This is particularly valuable when multiple objects or policies are modified in a single operation.

11.19 Applying Configuration Changes

SonicOS API configuration changes are performed within the firewall's configuration process and committed to the appliance.

Firewall Toolbox handles the required API communication as part of the selected operation.

During this process, status information is displayed so that the administrator can follow the progress of the operation.

[Screenshot: API operation progress window]

Depending on the selected task, Firewall Toolbox processes each selected configuration element and reports the progress of the operation.

Do not close Firewall Toolbox or interrupt network connectivity while a configuration operation is in progress.

11.20 Verifying Changes

After an API operation has completed, verify that the firewall is operating as expected.

The appropriate verification depends on the change.

For example:

Firewall rule changes

Verify the applications and network communication affected by the rule.

NAT policy changes

Verify access to the corresponding translated or published services.

Address object cleanup

Verify that the firewall configuration remains consistent.

TCP timeout changes

Verify applications that previously required modified timeout values.

For significant changes, Firewall Toolbox can retrieve a new TSR and EXP and perform another audit.

11.21 Re-Auditing the Firewall

A new audit provides a convenient method of verifying the resulting configuration.

The workflow is:

1. Complete the API maintenance operation.
2. Verify critical network functionality.
3. Retrieve a new TSR and EXP.
4. Import the new firewall data.
5. Allow the Full Audit to run.

6. Review the updated reports.

This confirms that the configuration analyzed by Firewall Toolbox reflects the current firewall state.

11.22 Recovery and Reversing Changes

Firewall Toolbox creates backups and records API operations to provide a recovery path when supported changes need to be reversed.

The exact recovery method depends on the type of operation.

For example, a disabled rule can normally be enabled again, while recovering a deleted configuration element may require recreating the original configuration or restoring information from the backup.

Important:
Do not assume that every API operation can be reversed with a single click. Retain the generated backup information and verify the recovery procedure appropriate for the change being performed.

For major changes, standard organizational backup and change-management procedures should also be followed.

11.23 API Logging and Troubleshooting

Firewall Toolbox records information about API communication and operations in its log files.

These logs can help diagnose issues such as:

- Authentication failures
- Connection problems
- API errors
- Unsupported operations
- Failed configuration changes

[Screenshot: Firewall Toolbox API log]

If an API operation fails, review the displayed status information and the corresponding log before attempting the operation again.

Repeatedly executing a failed configuration operation without understanding the cause should be avoided.

11.24 API Security Considerations

API access should be treated as administrative access to the firewall.

Recommended practices include:

- Allow API access only from trusted management networks
- Use appropriate administrative credentials

- Protect stored credentials
- Restrict management access at the firewall
- Review API logs
- Verify the target firewall before making changes
- Use individual administrator accounts where appropriate
- Follow organizational change-management procedures

Warning:
Firewall Toolbox API functions can modify production firewall configurations. Always verify the target firewall and selected configuration elements before starting an operation.

11.25 Using API Functions in HA Environments

Additional care should be taken when performing configuration changes in a High Availability environment.

Before making changes, verify:

- Which firewall or management address Firewall Toolbox is connected to
- The current HA status
- That configuration synchronization is functioning correctly
- That both HA members are operating normally

After making changes, verify that the expected configuration has synchronized correctly within the HA pair.

For significant modifications, an updated audit can be used to document the resulting configuration.

11.26 Recommended API Workflow

For configuration changes performed through Firewall Toolbox, the following workflow is recommended:

1. Perform a current firewall audit.
2. Review the corresponding report.
3. Determine which configuration elements require modification.
4. Verify that the correct firewall is selected.
5. Establish the API connection.
6. Review the records displayed by the API function.
7. Select only the required records.
8. Verify that the backup has been created.

9. Execute the API operation.
10. Monitor the displayed progress.
11. Verify critical network functionality.
12. Review the API log if necessary.
13. Retrieve a new TSR and EXP after significant changes.
14. Perform another audit.
15. Retain the updated documentation and configuration backup.

This provides a controlled process from identifying a configuration issue to verifying the completed change.

11.27 Next Steps

The API integration connects Firewall Toolbox analysis directly with firewall maintenance.

The next chapter covers **Settings and Customization**.

It explains the application settings that control report languages, IPv6 reporting, default objects, automatically generated rules and policies, repository locations, date and time formats, logging, report appearance, and other Firewall Toolbox behavior.

12. Settings and Customization

Firewall Toolbox provides a number of settings that control application behavior, report generation, data storage, and the information included in analyses.

Most environments can begin with the default settings. However, reviewing the available options allows Firewall Toolbox to be adapted to individual reporting and administrative requirements.

[Screenshot: Firewall Toolbox Settings window]

12.1 Opening the Settings

The application settings can be accessed from the Firewall Toolbox user interface.

The Settings window groups the available options and displays the currently configured values.

[Screenshot: Settings menu / Settings window]

Some changes take effect immediately, while others affect the next report, import, or analysis.

Tip:
Review the settings after the initial installation and again whenever reporting or operational requirements change.

12.2 Report Language

The Firewall Toolbox user interface is provided in English, but reports can be generated in several languages.

The available report languages are:

- English
- German
- French
- Italian
- Spanish

[Screenshot: Report Language setting]

The selected language affects subsequently generated reports.

This includes not only headings and report results, but also the explanatory text that describes the purpose and interpretation of individual analyses.

This makes it possible to operate Firewall Toolbox using the English interface while generating reports in the preferred language of a customer or organization.

12.3 Changing the Report Language

To create a report in another language, select the required language before generating the report.

Changing the report language does not modify:

- The Firewall Toolbox user interface
- Imported firewall data
- The SonicWall configuration
- Previously generated reports

Only reports generated after the language selection are affected.

Tip:
The same firewall data can be used to generate reports in different languages without importing the TSR and EXP files again.

12.4 IPv6 Reporting

Firewall Toolbox provides IPv6 versions of selected reports where applicable.

The **Show IPv6 Reports** setting determines whether IPv6-specific analyses should be included.

[Screenshot: Show IPv6 Reports setting]

IPv6 reports are only relevant if IPv6 is used by the analyzed firewall.

Disabling IPv6 reporting in environments that use only IPv4 can reduce the number of report sections and keep generated reports more focused.

Important:
Before disabling IPv6 reports, verify that IPv6 is genuinely not used in the environment. IPv6 may be active even in networks that primarily operate with IPv4.

12.5 Default Configuration Elements

SonicWall configurations contain a number of predefined or default objects and configuration elements.

Depending on the purpose of a report, displaying all default elements may add a large amount of information that is not relevant to the review.

Firewall Toolbox therefore provides an option to control whether default elements are displayed.

[Screenshot: Show Default Elements setting]

Including default elements can be useful when complete technical documentation is required.

Excluding them can make audit and maintenance reports easier to read by focusing on configuration elements created or modified for the individual environment.

12.6 Automatically Added Rules and Policies

SonicOS can automatically create certain configuration elements as a result of other features or settings.

Firewall Toolbox provides options controlling whether automatically added firewall rules or NAT policies should be included in relevant reports.

[Screenshot: Show Automatically Added Rules/NAT Policies setting]

This can be useful because automatically generated policies may otherwise make large rule sets considerably more difficult to review.

When complete configuration documentation is required, including these policies may be appropriate.

For audit or maintenance purposes, hiding them may make it easier to focus on administrator-created configuration.

12.7 Repository Location

Firewall Toolbox uses a repository to organize files associated with analyzed firewalls.

The repository location can be configured in the application settings.

[Screenshot: Repository Directory setting]

For each firewall, Firewall Toolbox can maintain a dedicated directory containing associated data.

Depending on the operations performed, this can include:

- TSR files
- EXP files
- API backups
- Other firewall-related files

The repository provides a consistent structure for retaining firewall information across multiple audits.

12.8 Choosing a Repository Location

The repository should be stored in a location that is:

- Reliable
- Accessible to the Firewall Toolbox user
- Included in the organization's backup strategy
- Protected against unauthorized access

Firewall data can contain sensitive information about the protected network.

For this reason, the repository should not be placed in an unrestricted shared directory.

Important:
Treat the Firewall Toolbox repository as security-sensitive data. TSR and EXP files can contain detailed information about the firewall and network configuration.

12.9 Repository Structure

Firewall Toolbox creates and uses directories associated with the analyzed firewall.

[Screenshot: Example Firewall Toolbox repository structure]

This makes it easier to keep configuration information from multiple firewalls separated.

For example, data retrieved from one customer firewall can be stored independently from data belonging to another environment.

The repository is also useful when historical configuration information needs to be retained.

12.10 Date and Time Format

Firewall Toolbox provides configurable date and time formatting.

[Screenshot: Date and Time Format setting]

This affects how date and time information is presented in applicable parts of the application and reports.

Selecting an appropriate format can be particularly useful when reports are generated for users in different countries.

For example, date formats commonly differ between European and North American environments.

Consistent date formatting also makes historical audit reports easier to compare.

12.11 Report Appearance

Firewall Toolbox provides settings that influence the appearance of generated reports.

Depending on the software version, available options can include report header or other presentation settings.

[Screenshot: Report Appearance settings]

These options allow reports to be adapted to the desired visual presentation while retaining the standard Firewall Toolbox report structure.

When reports are regularly provided to customers, consistent visual settings can help create a standardized documentation package.

12.12 Logging

Firewall Toolbox records information about application operations in log files.

Logging is particularly useful for:

- Troubleshooting
- API operations

- Import problems
- Report generation problems
- Application diagnostics

The logging level can be configured according to the amount of detail required.

[Screenshot: Logging Level setting]

A higher logging level may provide more diagnostic information but can also result in larger log files.

Tip:
If a problem needs to be investigated, increasing the logging level before reproducing the issue can provide additional diagnostic information.

12.13 MySonicWall Integration

Firewall Toolbox can optionally connect to MySonicWall to obtain additional information.

[Screenshot: MySonicWall setting]

This functionality can be enabled or disabled according to the requirements of the environment.

When enabled and correctly configured, MySonicWall information can be used by functions such as firmware availability checks.

MySonicWall integration is not required for basic TSR and EXP analysis.

12.14 API Connection Settings

Firewall Toolbox requires connection information when communicating with a SonicWall firewall through the API.

Depending on the function, the connection information includes:

- IP address or hostname
- HTTPS port
- Username
- Password
- SSL certificate handling

[Screenshot: API Connection settings]

Where connection information is retained by Firewall Toolbox, access to the computer and application should be appropriately protected.

Security Note:
Firewall administrative credentials provide privileged access to security infrastructure and should be handled accordingly.

12.15 SSL Certificate Validation

The API connection settings can include an option for handling SSL certificate validation errors.

This may be required in environments using self-signed certificates or certificates issued by an internal certification authority that is not trusted by the local computer.

[Screenshot: Ignore SSL Errors setting]

Ignoring SSL validation errors can simplify connectivity but reduces the protection provided by certificate verification.

Where possible, using a properly trusted management certificate is preferable.

12.16 Settings That Affect Reports

Some settings directly affect the content of generated reports.

Examples include:

- Report language
- IPv6 reporting
- Display of default elements
- Display of automatically generated rules or policies

When comparing reports created at different times, consider whether the same reporting settings were used.

A difference between two reports may result from a changed configuration, but it may also result from a changed Firewall Toolbox setting.

Tip:
For recurring customer audits, use a consistent set of report settings to make reports easier to compare over time.

12.17 Settings and the Trial Version

The availability of certain reports or functions may depend on the installed Firewall Toolbox license.

The trial version is intended to provide an opportunity to evaluate the application, but not every function available in the licensed version may be enabled.

If a report or option is unavailable, verify the current license status before troubleshooting the firewall configuration.

[Screenshot: Trial version / License status]

12.18 Recommended Initial Settings

Before performing the first production audit, review at least the following settings:

1. **Repository location**
   Verify where firewall configuration and backup information will be stored.
2. **Report language**
   Select the language appropriate for the report recipient.
3. **IPv6 reporting**
   Determine whether IPv6 reports should be included.
4. **Default elements**
   Decide whether predefined configuration elements should be shown.
5. **Automatically generated policies**
   Determine whether these should appear in the reports.
6. **Date and time format**
   Select the appropriate regional format.
7. **Logging**
   Verify that the logging level is appropriate.
8. **MySonicWall**
   Enable the integration if the corresponding functionality is required.
9. **API connection**
   Configure and test API access if automated downloads or configuration changes will be used.

12.19 Settings for Customer Reports

When Firewall Toolbox is used by an IT service provider or consultant, reporting requirements may differ between customers.

Before generating the final report, consider:

- Preferred language
- Whether IPv6 information is relevant
- Required level of technical detail
- Whether default objects should be included
- Whether automatically generated policies should be shown
- Date and time format

The underlying firewall data does not need to be imported again simply to create another report format.

This allows the same analysis to be presented differently according to the intended recipient.

12.20 Maintaining Consistent Audit Settings

For recurring audits, consistency is valuable.

If reports are intended to be compared over time, use the same reporting settings whenever possible.

For example, changing whether default objects are displayed can substantially alter the size and content of a report even though the firewall itself has not changed.

A standardized audit configuration therefore makes historical comparisons easier.

For organizations managing multiple firewalls, establishing a standard Firewall Toolbox configuration can also help ensure that all environments are assessed in a consistent way.

12.21 Restoring or Changing Settings

Settings can be modified whenever requirements change.

After changing a reporting option, generate the relevant report again to see the effect of the new configuration.

Changes to Firewall Toolbox settings do not modify the SonicWall firewall itself unless a specific API configuration operation is explicitly performed.

This distinction is important:

Firewall Toolbox settings control how the application behaves.

API operations can modify the active SonicWall configuration.

12.22 Next Steps

With the application configured appropriately, Firewall Toolbox should require relatively little day-to-day configuration.

The next chapter covers **Troubleshooting**.

It provides a structured approach to diagnosing common problems involving TSR and EXP imports, API connections, authentication, SSL certificates, MySonicWall integration, missing report information, PDF generation, and other Firewall Toolbox operations.

13. Troubleshooting

This chapter provides guidance for diagnosing common problems that may occur when using Firewall Toolbox.

Problems can generally be divided into several areas:

- TSR and EXP file import
- SonicWall API connectivity
- Authentication
- SSL certificates
- MySonicWall integration
- Missing or unexpected report information
- Report generation
- API configuration operations
- Application logging

When troubleshooting a problem, first determine whether it relates to the firewall, network connectivity, imported data, or Firewall Toolbox itself.

13.1 General Troubleshooting Approach

When a function does not operate as expected, use the following basic approach:

1. Verify that the correct firewall is being analyzed.
2. Verify that current TSR and EXP files are being used.
3. Check the Firewall Toolbox status or error message.
4. Verify network connectivity if the API or MySonicWall is involved.
5. Review the Firewall Toolbox log.
6. Repeat the operation if appropriate.
7. Increase the logging level if additional diagnostic information is required.

Tip:
When reporting a problem to support, provide the exact error message and relevant Firewall Toolbox log information. This is considerably more useful than a general description such as “the import does not work.”

13.2 TSR or EXP File Cannot Be Imported

If Firewall Toolbox cannot import a TSR or EXP file, first verify that the selected file is a valid SonicWall file of the expected type.

Possible causes include:

- Incorrect file selected
- Incomplete download
- Damaged file
- Unsupported format
- Unexpected file contents
- Insufficient file permissions
- File locked by another application

Try creating or downloading a new TSR and EXP from the firewall and importing those files.

[Screenshot: File import error]

If the problem continues, review the Firewall Toolbox log for additional information.

13.3 TSR and EXP Do Not Match

For the most reliable analysis, the TSR and EXP should originate from the same firewall and approximately the same point in time.

If files from different dates or different appliances are used, the information may not correspond.

This can result in unexpected report contents or apparent inconsistencies.

For example:

- A rule may exist in one file but not the other.
- An address object may have been modified between exports.
- Usage statistics may not correspond to the imported configuration.
- Firmware information may differ.
- VPN or interface configuration may have changed.

Recommendation:
When possible, retrieve both files immediately before performing the audit. Using the integrated API download function is the easiest way to ensure that the files are collected together.

13.4 API Connection Cannot Be Established

If Firewall Toolbox cannot connect to the SonicWall API, verify the connection parameters first.

Check:

- Firewall IP address or hostname
- HTTPS management port
- Network connectivity
- API availability on the firewall

- Management access
- Username
- Password
- SSL certificate handling

[Screenshot: API connection failed]

A successful connection requires the Firewall Toolbox computer to be able to reach the firewall management interface.

If the firewall cannot be reached from a browser or through the network, Firewall Toolbox will also be unable to establish the API connection.

13.5 Verify Network Connectivity

Before troubleshooting API-specific issues, verify basic network connectivity.

Confirm that:

- The firewall address is reachable.
- The configured HTTPS management port is accessible.
- No intermediate firewall blocks the connection.
- Management access is permitted from the source network.
- The correct management address is being used.

If the SonicWall management interface cannot be opened from the same computer, resolve the connectivity problem before troubleshooting Firewall Toolbox.

13.6 API Is Not Enabled

The SonicWall API must be enabled before Firewall Toolbox can use it.

If normal HTTPS management works but the API connection fails, verify the API configuration in SonicOS.

[Screenshot: SonicOS API configuration]

The exact location of the API setting depends on the SonicOS version.

After enabling API access, retry the connection from Firewall Toolbox.

13.7 Authentication Failure

An authentication error usually indicates a problem with the supplied credentials or account permissions.

Verify:

- Username
- Password
- Account status
- Administrative privileges
- Authentication requirements configured on the firewall

If possible, verify the same account directly against the SonicWall management interface.

Important:
Do not repeatedly attempt authentication with an incorrect password. Depending on the configured security settings, repeated failures may cause the account to be temporarily locked.

13.8 Insufficient Permissions

An API connection may be established successfully while a particular operation still fails.

In this case, verify whether the administrative account has sufficient privileges for the requested action.

Reading information and modifying the firewall configuration may require different permissions.

For example, an account that can retrieve information may not necessarily be permitted to:

- Delete firewall rules
- Disable policies
- Delete address objects
- Modify TCP timeout values

Review the permissions assigned to the API account.

13.9 SSL Certificate Errors

SSL certificate errors can occur when the firewall management interface uses:

- A self-signed certificate
- A certificate from an untrusted internal CA
- An expired certificate
- A certificate issued for a different hostname
- A certificate that does not match the IP address used for the connection

Firewall Toolbox provides an option to handle environments where certificate validation cannot be completed normally.

[Screenshot: SSL certificate option]

Security Note:
Ignoring SSL certificate validation removes an important identity check. Use this option only when the firewall and management network are trusted.

Where possible, configure the firewall with a valid certificate trusted by the computer running Firewall Toolbox.

13.10 API Connection Works but Download Fails

If authentication succeeds but downloading the firewall data fails, review the status information and Firewall Toolbox log.

Possible causes include:

- Insufficient permissions
- API response errors
- Firewall processing problems
- Network interruption
- Timeout
- Unsupported firmware behavior

Try the operation again after verifying that the firewall is operating normally.

If the problem is reproducible, retain the corresponding log information for troubleshooting.

13.11 API Operation Fails

An API configuration operation may fail even when the API connection itself is working.

Possible causes include:

- Object or policy no longer exists
- Configuration changed since the audit
- Insufficient permissions
- Invalid API request for the current SonicOS version
- Firewall rejected the configuration
- Network interruption
- Commit failure

[Screenshot: API operation error]

Review the Firewall Toolbox API log to determine which operation failed.

Important:
Do not repeatedly execute a failed modification without first determining the cause.

13.12 Configuration Changed Since the Audit

Firewall Toolbox API maintenance functions are based on the configuration information that was imported and analyzed.

If another administrator modifies the firewall after the audit, the active configuration may no longer exactly match the data currently loaded in Firewall Toolbox.

This is particularly important when working in environments with multiple administrators.

Before performing significant API operations, consider retrieving a new TSR and EXP if the firewall may have changed since the last import.

Tip:
For maintenance work, perform the audit and resulting API operations within the same maintenance session whenever possible.

13.13 An Expected Report Is Missing

If an expected report is not available or does not appear in a combined report, several factors may be responsible.

Check:

- Firewall Toolbox license or trial status
- IPv6 settings
- Firewall configuration
- Availability of the required source data
- Report settings
- Whether the feature applies to the analyzed firewall

Some reports are only relevant when a particular firewall feature is configured.

For example, an HA-specific analysis may not be applicable to a standalone firewall.

13.14 IPv6 Reports Are Missing

If IPv6 reports are expected but do not appear, verify:

- IPv6 is enabled or present on the firewall.
- **Show IPv6 Reports** is enabled in Firewall Toolbox.
- The selected analysis provides an IPv6 version.
- The installed license provides access to the corresponding functionality.

[Screenshot: Show IPv6 Reports setting]

If IPv6 is not used, the absence of IPv6 reports is expected.

13.15 Report Contains Unexpected Default Objects

If reports contain a large number of predefined SonicWall objects that are not relevant to the intended analysis, review the **Show Default Elements** setting.

Disabling the display of default elements can make some reports considerably easier to read.

Conversely, enable the option when complete configuration documentation is required.

13.16 Automatically Added Rules Are Missing

SonicOS may automatically create firewall rules or NAT policies for certain features.

If these elements are expected but do not appear in a report, review the corresponding Firewall Toolbox setting controlling automatically generated configuration elements.

[Screenshot: Automatically Added Rules setting]

For complete technical documentation, these elements may need to be included.

For audit purposes, excluding them can reduce unnecessary report content.

13.17 Report Information Appears Outdated

Firewall Toolbox analyzes the imported TSR and EXP data.

It does not automatically know about configuration changes performed on the firewall after those files were obtained.

If report information appears outdated:

1. Retrieve a new TSR and EXP.
2. Import the files.
3. Allow the automatic audit to complete.
4. Generate the report again.

The newly generated report should then represent the updated firewall configuration.

13.18 Report Language Is Incorrect

If a report is generated in the wrong language, verify the selected report language in Firewall Toolbox settings.

Changing the report language affects newly generated reports.

Previously generated PDF files are not modified.

After selecting the correct language, generate the report again.

13.19 PDF Report Does Not Open

Firewall Toolbox generates PDF documents and normally opens them using the PDF application associated with Windows.

If the report is generated but does not open automatically:

- Verify that a PDF viewer is installed.
- Verify the Windows default application for PDF files.
- Locate the generated report manually.
- Check whether another application has locked the file.

If no PDF is generated, review the Firewall Toolbox log for report-generation errors.

13.20 Report Generation Takes Longer Than Expected

Large firewall configurations can contain thousands of objects, rules, policies, and relationships.

A Full Audit requires considerably more processing than an individual report.

Report generation time can therefore depend on:

- Firewall configuration size
- Number of rules and objects
- Number of reports included
- IPv4 and IPv6 content
- Computer performance
- Repository/storage performance

The Firewall Toolbox progress display indicates whether processing is still active.

Avoid closing the application while report generation is in progress.

13.21 MySonicWall Information Is Unavailable

If MySonicWall-dependent information is unavailable, verify:

- MySonicWall integration is enabled.
- The required connection information is configured.
- Internet connectivity is available.
- Authentication succeeds.
- The firewall is associated with the appropriate MySonicWall account.

Functions that do not require MySonicWall can continue to operate normally.

For example, TSR and EXP analysis does not depend on a MySonicWall connection.

13.22 Firmware Check Does Not Show Expected Version

Firmware availability information may depend on MySonicWall data and the specific firewall model.

If the expected firmware information is not displayed:

- Verify MySonicWall connectivity.
- Verify the identified firewall model.
- Verify that the appliance is correctly associated with the MySonicWall account.
- Check the available firmware directly in MySonicWall if necessary.

Remember that an available firmware version is not automatically the correct version for immediate deployment.

Always review the corresponding SonicWall release information before upgrading a production firewall.

13.23 Unused Address Object Appears to Be in Use

Determining whether an address object is unused can be complex because objects can be referenced indirectly.

Firewall Toolbox analyzes multiple relationships, including groups and other configuration areas.

If an object listed as unused appears to be required:

1. Verify where you believe the object is used.
2. Check whether the reference exists in the imported configuration.
3. Verify that current TSR and EXP files were used.
4. Review nested groups and indirect relationships.
5. Do not delete the object until its dependency has been understood.

If Firewall Toolbox consistently identifies an actively referenced object as unused, retain the relevant configuration and log information for further investigation.

13.24 A Firewall Rule Shows No Usage but Is Required

A rule with no recorded hits is not necessarily obsolete.

Possible explanations include:

- The service is rarely used.
- The rule is intended for emergencies.
- Usage statistics were reset.
- The firewall was recently restarted.

- The rule supports a seasonal process.
- The rule is intended for disaster recovery.
- The available data does not cover a sufficiently long period.

Firewall Toolbox therefore treats usage information as a maintenance indicator rather than proof that a rule can safely be deleted.

13.25 TCP Timeout Is Reported as Modified

Firewall Toolbox reports firewall rules whose TCP timeout differs from the expected standard value.

This does not automatically indicate an error.

Some applications require longer-lived inactive TCP sessions.

Before resetting the timeout:

- Identify the application using the rule.
- Determine why the value was changed.
- Verify whether the requirement still exists.
- Consider the effect of returning to the standard timeout.

If the modified value is no longer required, the corresponding API function can be used to reset it.

13.26 Problems After an API Change

If a service stops working after an API configuration change:

1. Identify the operation that was performed.
2. Review the Firewall Toolbox API log.
3. Check the backup created before the operation.
4. Verify the affected firewall rule, NAT policy, object, or setting.
5. Restore or recreate the previous configuration where required.
6. Test the affected service again.

[Screenshot: API backup and command log]

For this reason, backups and API operation records should be retained until the change has been verified.

13.27 Firewall Toolbox Log Files

The Firewall Toolbox log is one of the most important sources of information when troubleshooting application problems.

Depending on the configured logging level, it can contain information about:

- Application operations
- Data import
- Report processing
- API communication
- Authentication
- Errors
- Configuration operations

[Screenshot: Firewall Toolbox log location / log file]

When investigating a reproducible problem, increase the logging level if necessary and repeat the operation.

This can provide additional diagnostic information.

13.28 Information to Collect for Support

If a problem cannot be resolved, collecting the relevant information before requesting support can significantly reduce troubleshooting time.

Useful information includes:

- Firewall Toolbox version
- SonicWall model
- SonicOS version
- Description of the operation
- Exact error message
- Relevant Firewall Toolbox log information
- Whether the issue is reproducible
- Whether manual or API-based import was used
- Whether the problem affects one firewall or multiple firewalls

Where configuration files or reports are required for troubleshooting, remember that they may contain sensitive network information.

Important:
Do not send passwords, API credentials, or other authentication secrets as part of a support request.

13.29 Troubleshooting Checklist

When something does not work as expected, check the following:

- Is the correct firewall loaded?

- Are the TSR and EXP current?
- Do the TSR and EXP belong to the same firewall?
- Is the required feature enabled on the firewall?
- Is the Firewall Toolbox setting correct?
- Is the function available with the current license?
- Is network connectivity available?
- Is the correct API management port being used?
- Are the credentials correct?
- Does the account have sufficient permissions?
- Is an SSL certificate problem preventing communication?
- Does the Firewall Toolbox log provide additional information?

Working through these questions resolves many common problems without requiring additional troubleshooting.

13.30 Next Steps

The main operational chapters of this guide are now complete.

The final chapter is the **Appendix and Reference** section.

It provides a compact reference for terminology, report categories, API operations, important files, recommended audit workflows, and other information that is useful to have available without searching through the complete manual.

14. Appendix and Reference

This appendix provides a compact reference to terminology, files, report categories, API operations, and recommended workflows used throughout Firewall Toolbox.

It is intended as a quick reference for users who are already familiar with the basic operation of the software.

14.1 Terminology

API

Application Programming Interface

The SonicWall API allows Firewall Toolbox to communicate directly with a SonicWall firewall.

Firewall Toolbox uses the API to retrieve firewall information and, for supported functions, perform configuration changes.

EXP

SonicWall Configuration Export

The EXP file contains the firewall configuration and can be used to restore or transfer configuration information.

Firewall Toolbox uses information from the EXP file for analysis and documentation.

TSR

Tech Support Report

The TSR contains extensive technical, diagnostic, configuration, status, and statistical information about a SonicWall firewall.

It is one of the primary data sources used by Firewall Toolbox.

MySonicWall

SonicWall's online platform for managing registered appliances, licensing, firmware, and other product-related information.

Firewall Toolbox can optionally use MySonicWall information for selected analyses.

SonicOS

The operating system used by SonicWall firewalls.

Available functionality and configuration options may differ between SonicOS versions.

Firewall Rule / Access Rule

A policy controlling whether network traffic is allowed or denied between sources, destinations, services, and security zones.

NAT Policy

A policy that performs Network Address Translation between original and translated addresses or services.

Address Object

A reusable configuration object representing a host, network, address range, or other network resource.

Address Group

A logical collection of address objects and, depending on the configuration, other address groups.

Zone

A logical security area to which firewall interfaces are assigned.

Common examples include LAN, WAN, DMZ, WLAN, and VPN.

HA

High Availability

A configuration in which two compatible SonicWall appliances operate as an HA pair to improve service availability.

TCP Connection Timeout

The period for which an inactive TCP connection is retained in the firewall's connection table before it is removed.

SonicWall provides a global timeout as well as the ability to configure different timeout values for individual firewall rules.

14.2 Firewall Toolbox Main Categories

Firewall Toolbox Version 3 organizes reports and functions into five main categories.

Security Audit

Focuses on security-relevant configuration and potential security concerns.

Typical areas include:

- Firewall rules
- Security Services
- Management access
- Logging
- Administrative users
- User permissions
- VPN security
- Other security settings

Health

Focuses on the operational state of the firewall.

Typical areas include:

- System utilization
- Security Service status
- Licensing
- License expiration
- Operational indicators

Configuration Audit

Focuses on important operational configuration.

Typical areas include:

- Lifecycle
- Firmware
- Firmware history
- High Availability
- WAN Failover
- Interfaces
- VPN configuration

Documentation

Provides detailed technical documentation of the firewall.

Typical areas include:

- Firewall rules
- NAT policies
- Address objects
- Address groups
- Zones
- Interfaces
- Users
- Groups
- Access rights
- VPN configuration

Maintenance

Helps identify configuration elements that may require cleanup or review.

Typical areas include:

- Disabled firewall rules
- Unused firewall rules
- Disabled NAT policies
- Unused NAT policies
- Unused address objects
- Duplicate address objects
- Address object naming
- Modified TCP timeout values

14.3 Report Types

Firewall Toolbox provides three primary levels of reporting.

Individual Report

Contains information about one specific analysis or configuration area.

Use an individual report when a focused technical assessment is required.

Category Report

Combines the relevant reports from one of the five main categories.

Examples include:

- Security Audit Summary
- Health Summary
- Configuration Audit Summary
- Documentation Summary
- Maintenance Summary

Full Audit Report

The most comprehensive report.

It combines the major analyses and documentation from all five categories and begins with the Highlights and Recommendations section.

Use the Full Audit Report when a complete assessment and technical documentation package is required.

14.4 Supported Report Languages

Firewall Toolbox reports can be generated in:

- English
- German
- French
- Italian
- Spanish

The Firewall Toolbox user interface remains in English.

Changing the report language does not require the firewall data to be imported again.

14.5 Primary Firewall Data Sources

Firewall Toolbox primarily uses the following data sources:

Data Source	Purpose
TSR	Technical, diagnostic, operational, and configuration information
EXP	Firewall configuration
SonicWall API	Automated retrieval and supported configuration operations
MySonicWall	Optional additional product and firmware information

For the most complete audit, current TSR and EXP files should be available.

14.6 Manual Import Versus API Download

Manual Import

Use manual import when:

- Direct firewall connectivity is unavailable
- API access is disabled
- Files were provided by a customer
- An archived configuration needs to be analyzed
- Offline analysis is required

API Download

Use API download when:

- The firewall is directly reachable
- API access is enabled
- Current data is required

- Audits are performed regularly
- A more automated workflow is preferred

API download also helps ensure that the TSR and EXP are collected at approximately the same point in time.

14.7 API Operations Reference

Firewall Toolbox provides API functions for selected maintenance tasks.

Depending on the installed version and firewall configuration, operations can include:

Configuration Element	Operation
Firewall Rule	Disable
Firewall Rule	Delete
NAT Policy	Disable
NAT Policy	Delete
Address Object	Delete unused object
Firewall Rule	Reset TCP timeout

API operations modify the active firewall configuration.

Warning:
Always verify the target firewall and selected configuration elements before executing an API operation.

14.8 Recommended Rule Cleanup Process

For firewall rules whose purpose is uncertain, use a staged approach:

Identify → Review → Disable → Observe → Delete

This provides an opportunity to determine whether a rule is still required before permanently removing it.

The same general approach can also be useful for NAT policies.

14.9 API Backup Process

Before supported configuration changes are performed through the API, Firewall Toolbox creates backup information.

This includes:

- Current EXP configuration

- Current TSR
- Information about the API operations performed

The backup provides a reference to the firewall state before the change.

Important:
Retain the backup until the change has been verified and all affected services have been tested.

14.10 API Safety Checklist

Before executing an API operation, verify:

- The correct firewall is selected.
- The firewall data is current.
- The API connection points to the intended firewall.
- The selected records have been reviewed.
- The purpose of each selected object or policy is understood.
- Dependencies have been considered.
- A backup is available.
- A recovery procedure is understood.
- Critical services can be tested after the change.

In HA environments, also verify the current HA status and configuration synchronization.

14.11 Firewall Repository

The Firewall Toolbox repository provides a structured location for files associated with analyzed firewalls.

Depending on the operation, the repository can contain:

- TSR files
- EXP files
- Configuration backups
- API operation information
- Other firewall-related data

The repository should be stored in a protected location and included in an appropriate backup strategy.

14.12 Sensitive Information

Firewall Toolbox processes information about security infrastructure.

TSR files, EXP files, generated reports, logs, and repository data may contain sensitive information such as:

- Internal IP addresses
- Network topology
- Firewall rules
- NAT configuration
- Published services
- VPN information
- User information
- Administrative configuration
- Security findings

Access to these files should therefore be restricted to authorized personnel.

14.13 Recommended First Audit Workflow

For a new firewall or a first assessment:

1. Review Firewall Toolbox settings.
2. Configure the repository location.
3. Select the required report language.
4. Configure API access if available.
5. Retrieve the current TSR and EXP.
6. Import the firewall data.
7. Allow the automatic Full Audit to complete.
8. Open the Full Audit Report.
9. Review Highlights and Recommendations.
10. Investigate the relevant detailed findings.
11. Generate additional individual reports if required.
12. Document any required actions.

14.14 Recommended Regular Audit Workflow

For recurring firewall reviews:

1. Retrieve current TSR and EXP files.
2. Perform the Full Audit.

3. Review new or significant findings.
4. Check Security Audit results.
5. Review Health information.
6. Review configuration changes.
7. Check Maintenance findings.
8. Compare with previous audits where appropriate.
9. Perform required maintenance.
10. Re-audit after significant changes.
11. Store the updated report and configuration files.

The frequency of audits should be selected according to the security requirements and rate of configuration change in the environment.

14.15 Recommended Maintenance Workflow

For configuration cleanup:

1. Perform a current audit.
2. Review the Maintenance Summary.
3. Identify unused or disabled policies.
4. Review unused address objects.
5. Examine duplicate objects.
6. Review naming inconsistencies.
7. Check modified TCP timeout values.
8. Determine dependencies.
9. Disable uncertain policies first where appropriate.
10. Observe the environment.
11. Delete confirmed obsolete configuration.
12. Verify critical services.
13. Retrieve new firewall data.
14. Perform another audit.

This staged approach reduces the risk associated with cleaning up older configurations.

14.16 Recommended Documentation Workflow

For creating technical firewall documentation:

1. Retrieve a current TSR and EXP.
2. Import the firewall data.
3. Select the appropriate report language.
4. Generate the Documentation Summary or Full Audit Report.
5. Review the documentation.
6. Add external documentation where required.
7. Store the report in a protected documentation system.
8. Regenerate the documentation after significant configuration changes.

External documentation may include information that cannot be derived directly from the firewall, such as:

- Network diagrams
- Provider information
- Contact details
- Change procedures
- Disaster recovery procedures
- Application ownership

14.17 Before Major Firewall Changes

Before performing a major firewall change, consider creating a current Firewall Toolbox audit.

Examples include:

- Firmware upgrade
- Firewall migration
- Hardware replacement
- Major rule cleanup
- Network redesign
- VPN migration
- WAN provider change
- HA maintenance

A useful pre-change package consists of:

Current TSR + Current EXP + Full Audit Report

This provides both machine-readable configuration information and human-readable technical documentation of the firewall before the change.

14.18 After Major Firewall Changes

After completing significant changes:

1. Verify network connectivity.
2. Test critical applications.
3. Verify VPN connectivity.
4. Verify Internet-facing services.
5. Check HA status where applicable.
6. Retrieve a new TSR and EXP.
7. Perform another Full Audit.
8. Review unexpected findings.
9. Store the updated documentation.

This creates a documented **before-and-after state** of the firewall.

14.19 Report Interpretation

Firewall Toolbox findings are intended to support technical decision-making.

A finding can indicate that a configuration:

- Deserves review
- Differs from an expected value
- May no longer be required
- May represent a security concern
- May require maintenance
- Should be documented

A finding does not automatically mean that a configuration is incorrect.

The administrator should always consider:

- Business requirements
- Application requirements
- Network architecture
- Security policies
- Operational dependencies
- Compatibility requirements

Firewall Toolbox provides the analysis and technical information required to make that assessment.

14.20 Firewall Toolbox Version Information

When requesting support or documenting an audit, record the Firewall Toolbox version used to perform the analysis.

[Screenshot: About Firewall Toolbox / Version Information]

The version number can be important because reports, analyses, API functionality, and supported configuration elements may change between Firewall Toolbox releases.

When troubleshooting, it is also useful to record:

- Firewall model
- SonicOS version
- Firewall Toolbox version
- Date of the audit

14.21 Support Information

If assistance is required, collect the relevant information before contacting support.

Useful information includes:

- Firewall Toolbox version
- SonicWall model
- SonicOS version
- Description of the problem
- Exact error message
- Relevant Firewall Toolbox log information
- Steps required to reproduce the issue

Do not include passwords or other authentication credentials.

Where TSR, EXP, or report files are required for troubleshooting, remember that these files can contain confidential information about the firewall and network environment.

14.22 Quick Reference – What Should I Use?

Requirement	Recommended Function
Complete firewall assessment	Full Audit Report
Security-focused review	Security Audit
Operational review	Health

Requirement	Recommended Function
Review important configuration	Configuration Audit
Create technical documentation	Documentation
Clean up old configuration	Maintenance
Review a single issue	Individual Report
Obtain current firewall data	API Download
Remove unused objects	Maintenance + API
Review old firewall rules	Maintenance
Safely phase out questionable rules	Disable via API
Check unusual TCP timeouts	TCP Timeout Report
Reset TCP timeouts	TCP Timeout API function
Check firmware	Configuration Audit
Document configuration before a change	Full Audit + TSR + EXP

14.23 Final Notes

Firewall configurations become more complex over time.

Regular analysis, documentation, and maintenance help ensure that the configuration remains understandable and that obsolete settings do not accumulate unnoticed.

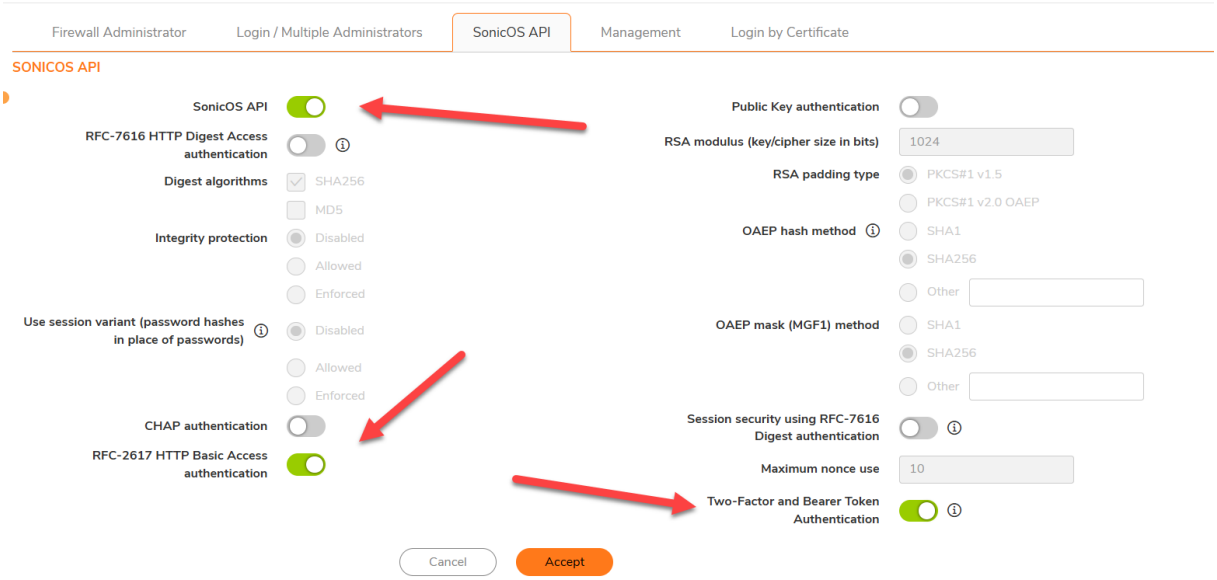
Firewall Toolbox brings these tasks together in a single workflow:

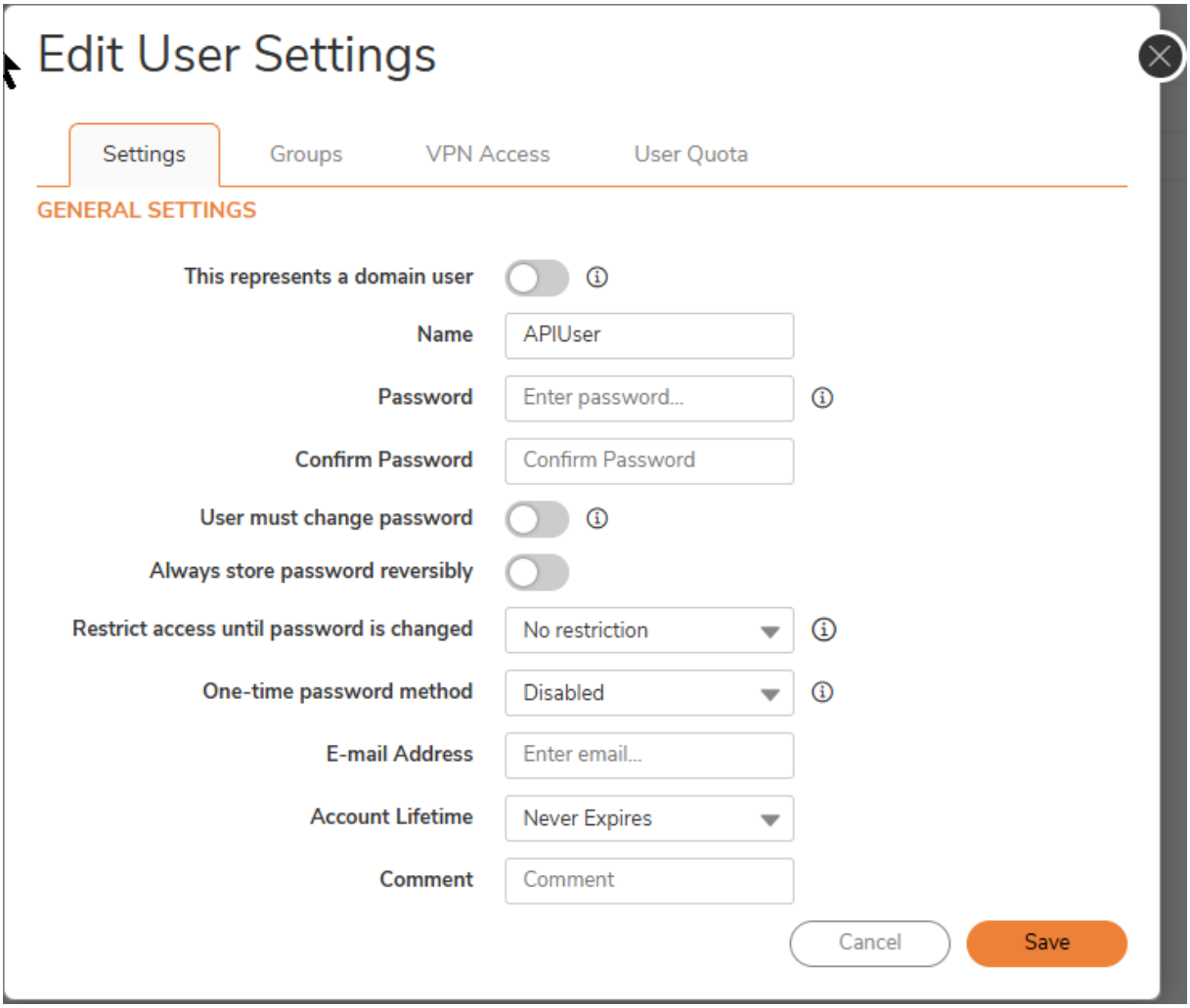
Analyze – Audit – Document – Maintain

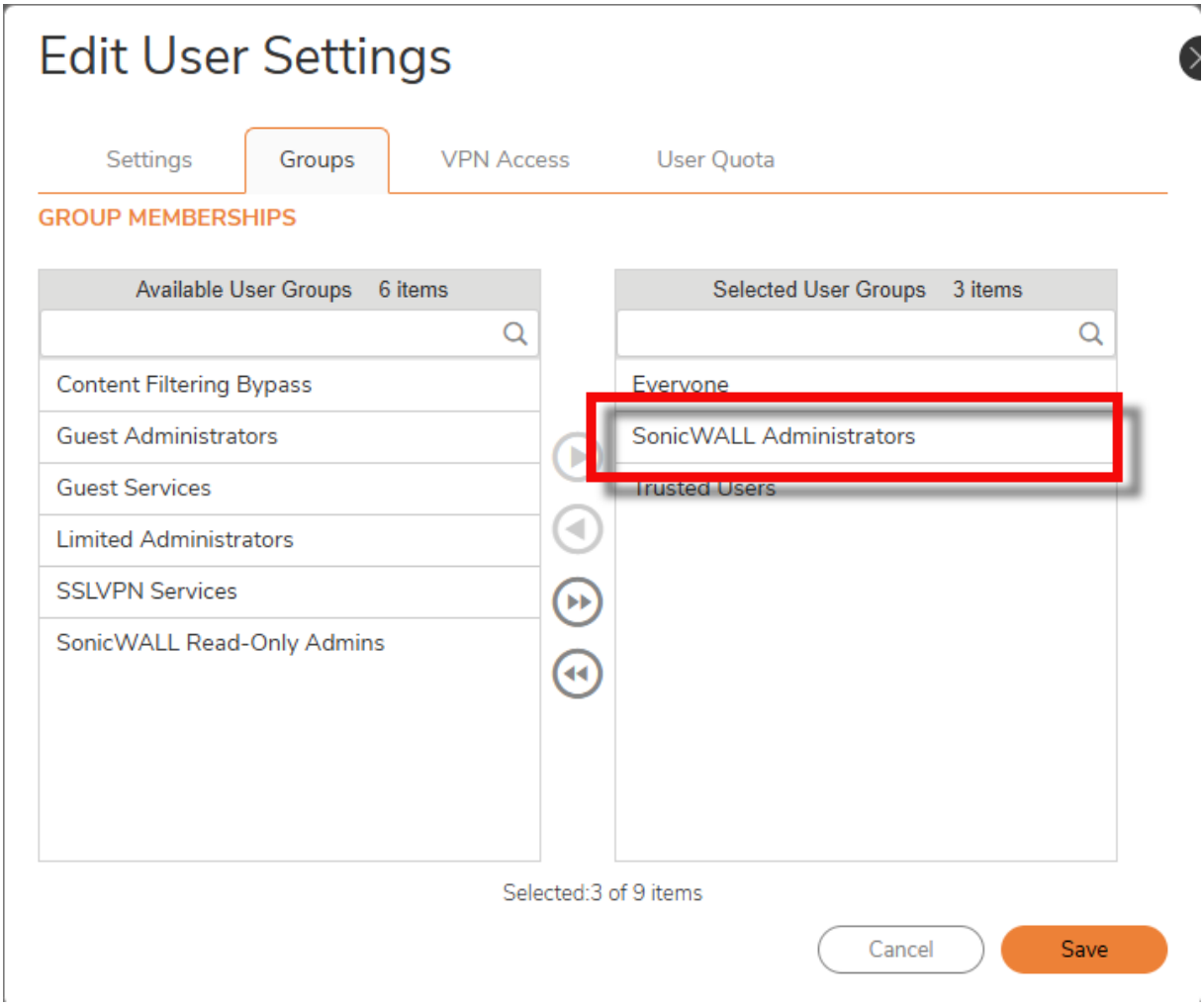
By combining automated analysis with structured reporting and selected SonicWall API functions, Firewall Toolbox helps administrators understand the current configuration, identify areas requiring attention, document the environment, and perform supported maintenance tasks efficiently.

The result is not only a cleaner firewall configuration, but also a configuration that is easier to understand, review, support, and maintain over its entire lifecycle.

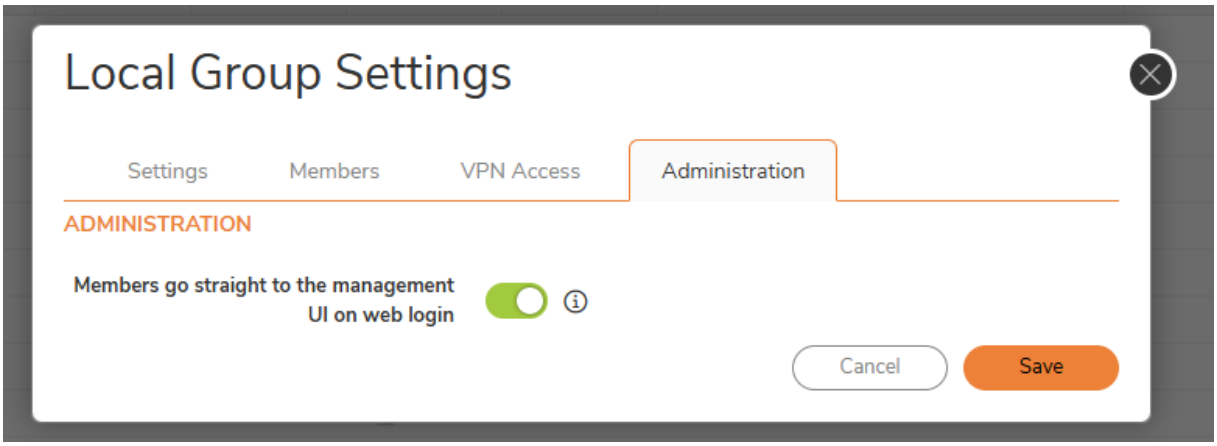
15.1 Enabling API on the SonicWall Firewall

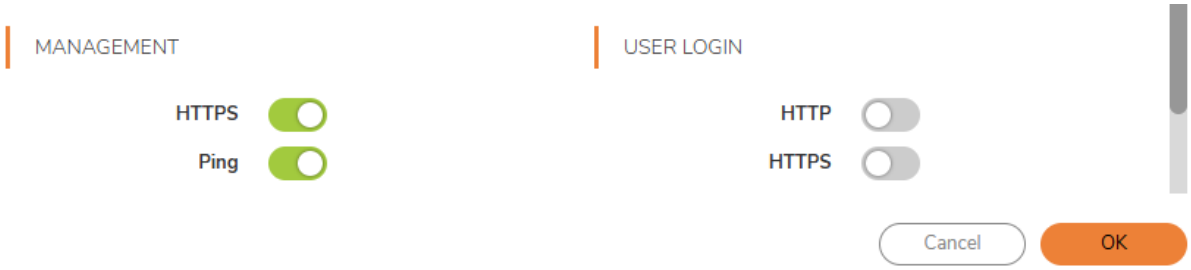






If you should use an individual user for API Access (highly recommended) please make sure that the user directly gets to the GUI and no PopUp is shown before:



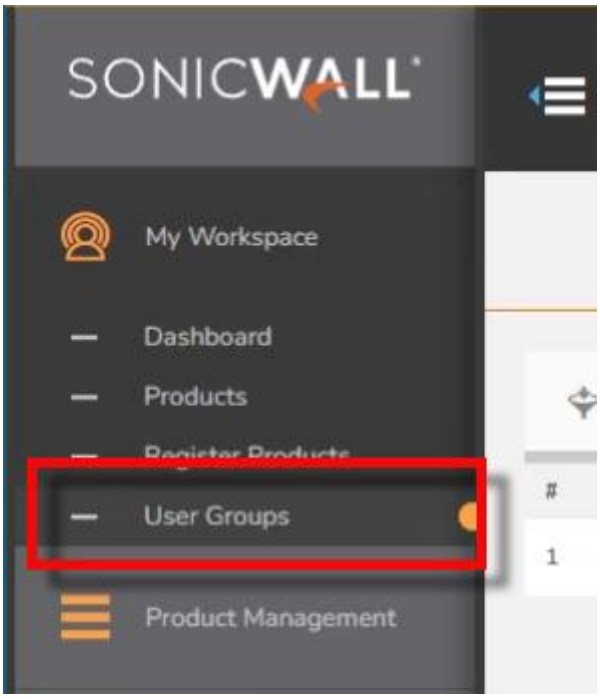

MANAGEMENT
HTTPS
Ping
USER LOGIN
HTTP
HTTPS
Cancel
OK

15.2 API to MySonicWall

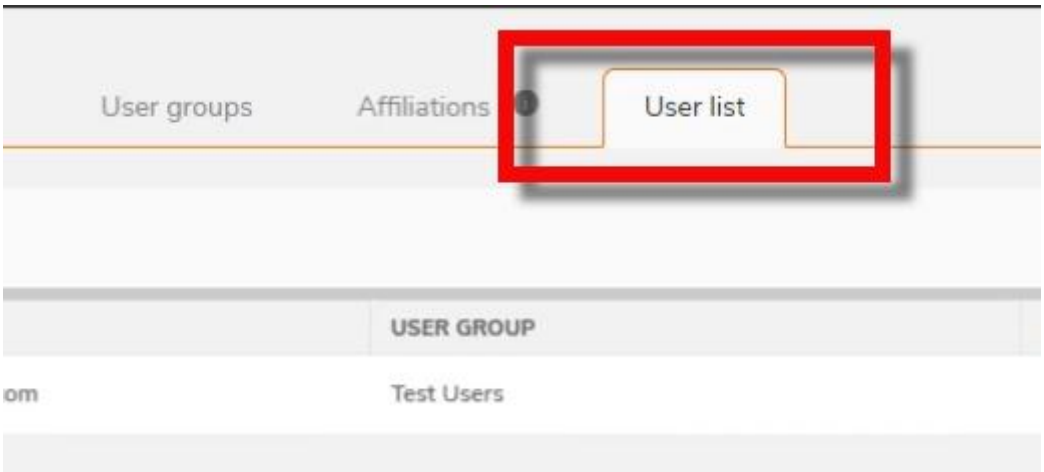
If access to MySonicWall via API is desired, please follow these steps:

Log in to My SonicWall.com

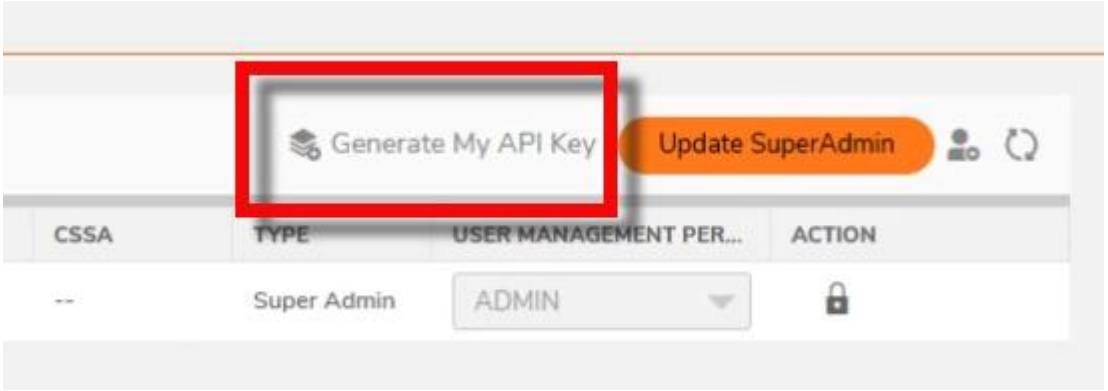
Go to “My Workspace” / “User Groups”



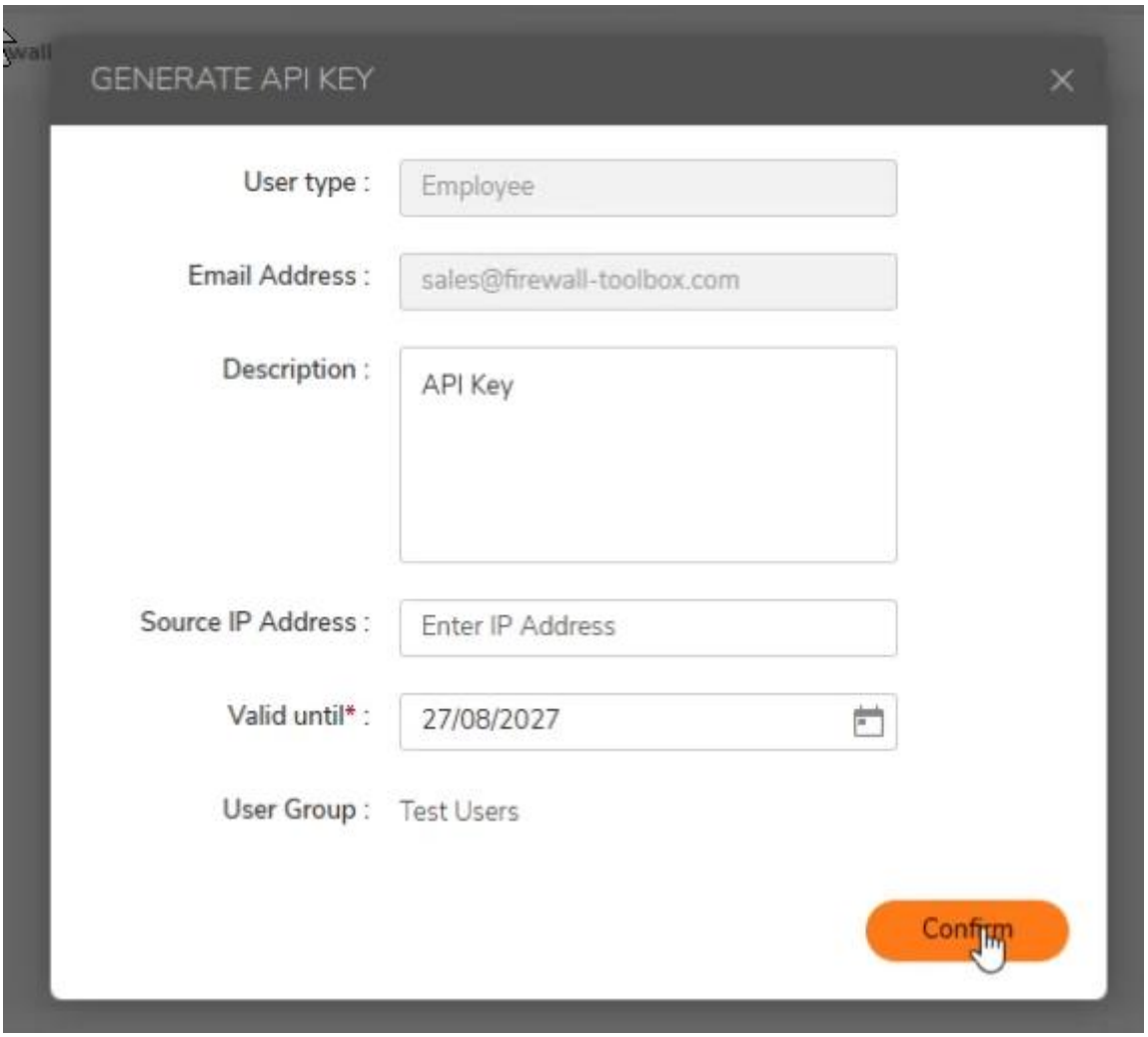
Go to the User List Tab



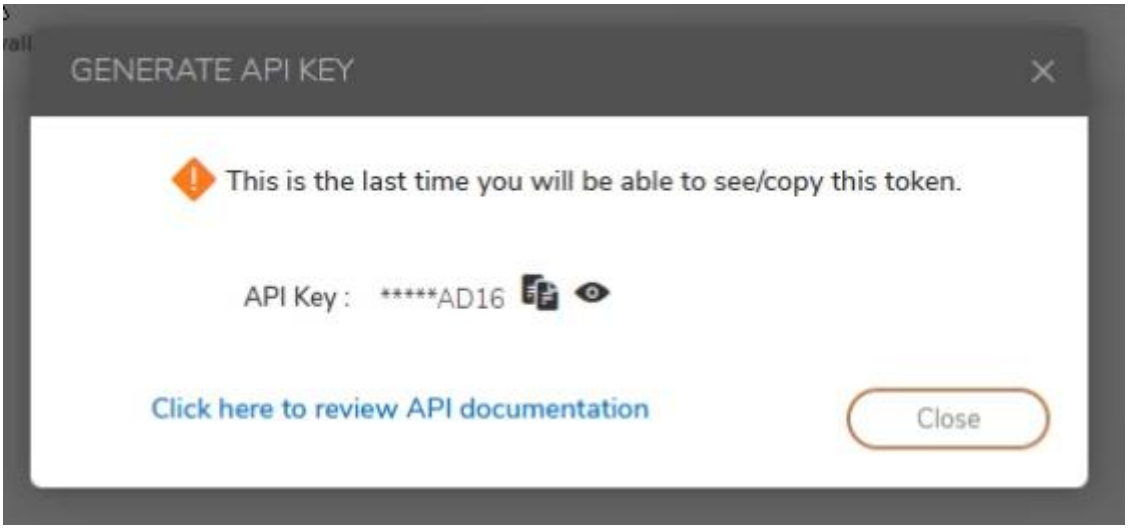
In the upper right corner of the screen there is a button “Generate My API Key”



Enter the details and how long you want this key to be active. You can also limit API Access to an IP-Address:



Copy the Key and save it



In Firewall Toolbox, in the MySonicWall API Screen, enter the Mailaddress of the MySonicWall Account and the API Key.

Keep in mind that the device you are analyzing in Firewall Toolbox needs to be in the same account.

16 Troubleshooting

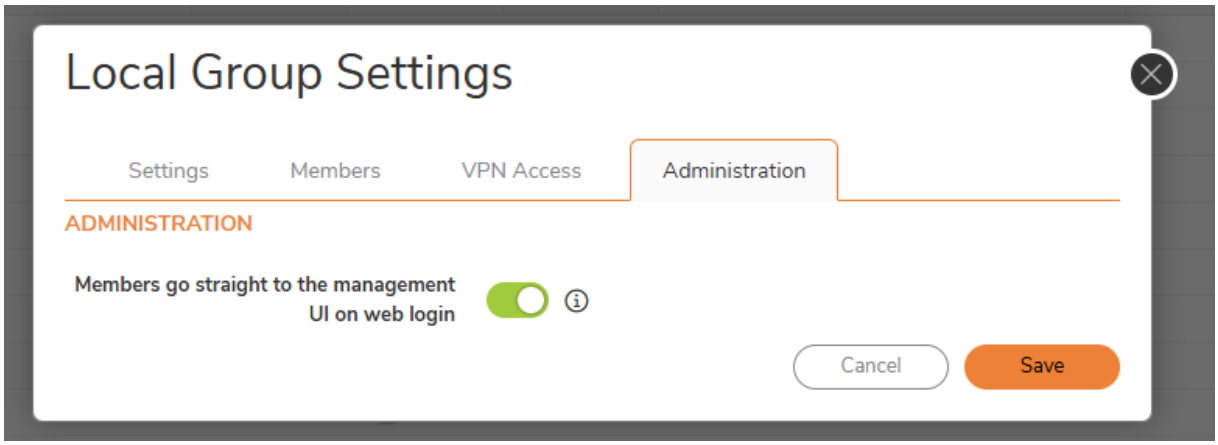
16.1 API Connection to Firewall does not work

Check IP / Port / Username / Password

Try to log in with that user on Firewall GUI.

Do you have full admin rights? If not, add the user to the Full SonicWall Administrators Group”

Do you get directly to the GUI or do you see the session window? If you see a session window, check this setting and enable “Members go straight to the management UI on web login”:



If still not successful Restart Firewall Toolbox and try again

Try to access the firewall with an API Tool (Postman / ARC Rest Client).

Contact support: support@firewall-toolbox.com