

Powerful Analysis Tool

How does Firewall Toolbox work?

Firewall Toolbox requires two key files:

- the Firewall Technical Support Report (TSR) and
- the SonicWall System Export (.exp)

These files can either be uploaded manually or downloaded automatically from the firewall via the API.

Optionally, the tool can also connect to MySonicWall to retrieve additional information.

A user-friendly wizard guides you through the data import process. Once the required information has been collected, it is processed, loaded into a structured database, and analyzed.

Firewall Toolbox then generates a wide range of reports, providing the auditor with quick and easy access to the most important information about the firewall's current status.

Analyze – and Take Action!

Firewall Toolbox not only provides comprehensive analyses and identifies areas for optimization, but also directly supports you in implementing improvements. Powerful API functions allow selected configuration changes to be applied directly to the firewall – quickly, conveniently, and without time-consuming manual adjustments.

This means that an identified weakness can be turned into a concrete improvement in just a few steps.

Security is a key priority throughout the process: Backups are created automatically before changes are made, ensuring that the original configuration remains available at all times. If required, not only complete configurations but also individual objects or firewall rules can be restored selectively.

In this way, Firewall Toolbox combines analysis, optimization, and implementation in a seamless and controlled process.

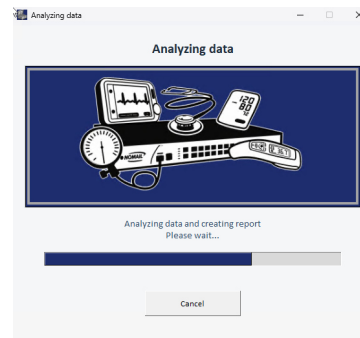
Guided Audits

Firewall Audits with Expert Support

If you do not have extensive expertise in firewalling, you can book an assisted audit – either directly with Martin Schmitz IT Security Consulting or through an IT security partner using Firewall Toolbox.

A typical audit process is as follows:

- The firewall configuration is exported and processed using Firewall Toolbox, which generates a detailed report.
- The customer and reseller review the report together and develop a plan for the required changes.
- Once the changes have been implemented, a new report is generated and reviewed. This process is repeated until the desired result is achieved.



Contact

Martin Schmitz
IT Security Consulting
Auf dem Kamp 6
41352 Korschenbroich
02182 / 5731 400
martin@martinschmitz.it



V 3.0.0.8 / Sept 2026

Get more Information and a free Trial-Version here:
www.firewall-toolbox.com



FIREWALL TOOLBOX

Audit, Reporting and Management for SonicWall Firewalls

Firewall Toolbox

Do You Use SonicWall Firewalls?

Can you answer the following questions immediately and without time-consuming research?

Which users have which access rights?

Are all Security Services licensed and active?

Are all firewall rules up to date?

Are there still temporary rules active that were originally created for testing purposes?

Is the system adequately protected against failures – for example, in the event of a firewall or Internet connection failure?

Firewall Toolbox provides fast and precise answers to these and many other questions. It analyzes your firewall configuration, helps you identify security risks and misconfigurations, and significantly simplifies regular firewall audits.

This saves you time, improves the quality of your security assessments, and provides a structured overview of the current state of your firewall.

Audits: More Security & Compliance

Audits address the following areas:

- Regulatory compliance (NIS2, GDPR)
- Continuous adaptation to evolving threats
- Identification of security vulnerabilities
- Performance optimization
- Protection against internal threats
- Traceability and accountability
- Disaster recovery

Author of Firewall Toolbox

Martin Schmitz has been working with SonicWall firewalls for more than 25 years. He spent 12 years as a Systems Engineer at SonicWall and has been working as an independent Security Consultant since 2017. In this role, he advises customers on SonicWall solutions, among other areas, and is a certified SonicWall Firewall Trainer.



User Interface / Reports

Screenshots

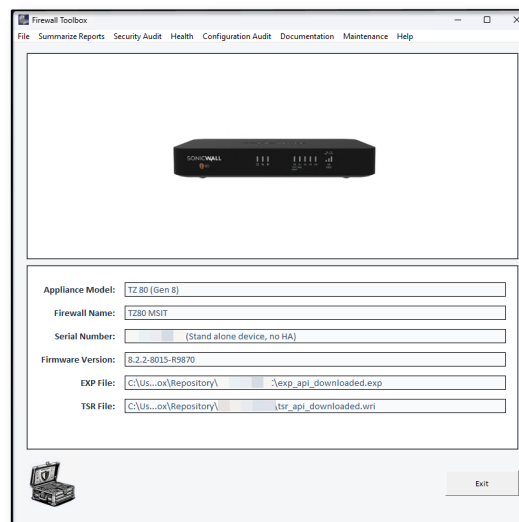


Figure left:
Main GUI

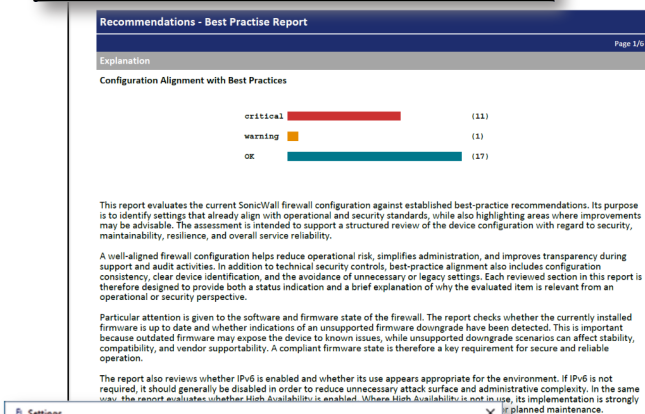


Figure above:
Sample Report
(Excerpt)

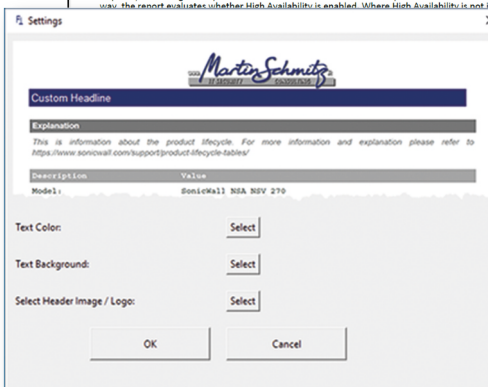


Figure above: Report Customization Options – Colors / Logo

Reports

Security Audit



- Firewall Rules / NAT Rules / Usage
- Rules Allowing Access from WAN to Internal Networks
- Rules Allowing Management Access
- Disabled Rules
- Rules with No Traffic for a Defined Period
- VPN Check (Weak or Insecure Settings)
- Users in Administrative Groups
- External User Authentication
- User Access Rights
- Firewall Audit Settings and Data
- Detection and Prevention Features
- Security Services Status

Configuration Audit



- WAN MTU Settings
- TCP Connection Timeout

System Health



- System Utilization
- High Availability
- High Availability Status / Settings
- WAN Failover Status / Usage
- Firmware

Documentation



- Zones
- Interfaces
- Firewall Rules
- Nat Rules
- User
- Addressobjects
- Serviceobjects

