

Leistungsfähiges Audit Tool

Wie funktioniert Firewall Toolbox?

Die Software Firewall Toolbox benötigt zwei zentrale Dateien:

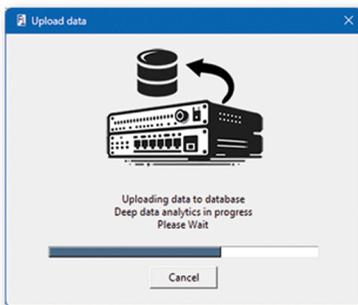
- den Firewall Technical Support Report (TSR) und den
- SonicWall System Export (.exp)

Diese Dateien können entweder manuell oder automatisch per API von der Firewall heruntergeladen werden.

Optional kann das Tool auch zusätzlich auf MySonicWall zugreifen, um weitere Informationen abzurufen.

Ein benutzerfreundlicher Assistent führt durch den Prozess der Dateneinreichung. Sobald die Informationen gesammelt wurden, werden sie verarbeitet und in strukturierter Form in eine SQL-Datenbank hochgeladen und analysiert.

Das Tool generiert daraufhin eine Vielzahl von Berichten, die dem Auditor einfachen Zugriff auf die wichtigsten Informationen zum aktuellen Zustand der Firewall ermöglichen.



Das Erscheinungsbild der Berichte kann angepasst werden, indem das Logo und die farbliche Gestaltung der Überschriften individuell festgelegt werden.

Aktuell sind zwei Module implementiert: Security Audit und Configuration Audit. Weitere Module sind in Planung.

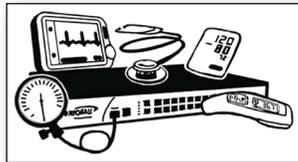
Begleitete Audits

Firewall-Audits mit Expertenunterstützung

Sollten Sie nicht über das umfassende Know-how im Bereich Firewalling verfügen, können Sie einen begleiteten Audit buchen – direkt bei Martin Schmitz IT Security Consulting oder bei einem IT-Sicherheitspartner, der die Firewall Toolbox verwendet.

Ein typischer Ablauf eines Audits gestaltet sich wie folgt:

- Die Konfiguration der Firewall wird exportiert und mit Firewall Toolbox verarbeitet, woraufhin ein detaillierter Bericht erstellt wird
- Der Kunde und der Reseller analysieren den Bericht gemeinsam und entwickeln einen Änderungsplan
- Nach der Umsetzung der Änderungen wird ein neuer Bericht erstellt und besprochen. Dieser Prozess wird so lange wiederholt, bis das Ergebnis zufriedenstellend ist



Die Software läuft auf Windows 10 / 11. Ausschliesslich SonicWall Firewalls mit den Firmware Versionen 6 & 7 sind unterstützt. SonicOS „unified Policy“ ist zur Zeit nicht supported.

Kontakt

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



Mehr Infos und gratis Testversion:
www.firewall-toolbox.com



FIREWALL TOOLBOX

Firewall Audit für SonicWall: schnell und effektiv

Firewall Toolbox

Nutzen Sie SonicWall Firewalls in Ihrem Unternehmen?

Können Sie die folgenden Fragen spontan und ohne zeitaufwändiges Suchen beantworten?

- Welche Benutzer haben welche Zugriffsrechte?
- Sind alle Security Services lizenziert und aktiv?
- Sind temporäre Regeln noch aktiv, die ursprünglich nur zu Testzwecken erstellt wurden?
- Ist das System gegen Ausfälle geschützt?
- Was passiert, wenn die Firewall oder die Internet-Verbindung ausfällt?

Die Software „Firewall Toolbox“ bietet Ihnen schnelle und präzise Antworten und vereinfacht zudem Firewall-Audits erheblich. So sparen Sie Zeit und verbessern die Effizienz Ihrer Sicherheitsprüfungen.

Audits: der Schlüssel zu mehr Sicherheit & Konformität

Audits adressieren diese Themen:

- Konformität mit Vorschriften (NIS-2, DSGVO / GDPR)
- Regelmäßige Anpassung an Bedrohungen
- Sicherheitslücken identifizieren
- Leistungsoptimierung
- Schutz vor internen Bedrohungen

Autor von Firewall Toolbox

Martin Schmitz beschäftigt sich seit mehr als 20 Jahren mit SonicWall Firewalls. Er war 12 Jahre als Systems Engineer bei SonicWall angestellt und ist seit 2017 freiberuflicher Security Consultant. Hier berät er Kunden zu SonicWall und ist zertifizierter SonicWall Firewall Trainer.



User Interface / Reports

Screenshots



Abb. links:
GUI Startseite

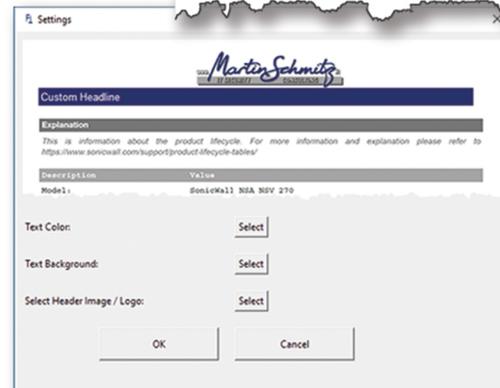
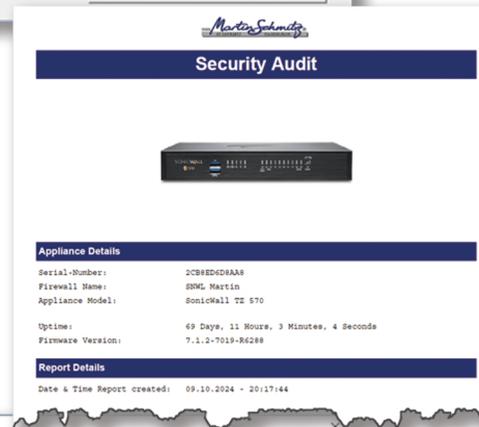


Abb. oben:
Beispielreport
(Ausschnitt)

Abb. oben: Anpassungsmöglichkeiten

Reports

Security Audit



Firewall Rules / NAT Regeln

- Firewall Regeln / NAT Policies die nie verwendet wurden
- Regeln die Zugriffe von WAN auf interne Netze erlauben
- deaktivierte Regeln
- Regeln über die eine definierte Zeit kein Verkehr gelaufen ist

VPN

- Crypt Check (schwache Ciphers etc.)

Benutzer

- Benutzer in Administrativen Gruppen
- Externe User Authentication
- VPN Zugriffsrechte

Audit

- Firewall Audit Einstellungen und Daten

Configuration Audit



Security Services

- Status & Ablauf
- Auf welchen Zonen aktiviert?

Hochverfügbarkeit

- High Availability Status / Einstellungen
- WAN Failover Status / Nutzung

Firmware

- History (Upgrades / hochgeladene Settings)
- Status / Updates available