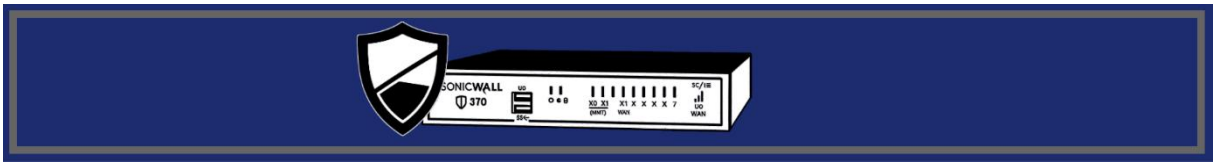


Die 10 wichtigsten Punkte bei der Überprüfung einer SonicWall Firewall

Eine Firewall ist nur so sicher wie ihre Konfiguration. Bei Sicherheitsanalysen und Health Checks treten immer wieder die gleichen Konfigurationsfehler auf – oftmals bleiben diese über Jahre unbemerkt. Die folgenden zehn Bereiche sollten daher regelmäßig überprüft werden, um die Sicherheit, Stabilität und Nachvollziehbarkeit einer SonicWall-Umgebung sicherzustellen.

1. Firewall Regeln überprüfen

Firewall-Regeln bestimmen, welcher Datenverkehr zugelassen oder blockiert wird. Im Laufe der Zeit sammeln sich häufig temporäre Freigaben, Testregeln und veraltete Konfigurationen an.

Prüfen Sie insbesondere auf:

- Regeln von WAN zu internen Netzwerken
- „Any → Any“-Freigaben
- Zu weit gefasste Service-Definitionen
- Deaktivierte, aber nicht entfernte Regeln
- Doppelte oder sich überschneidende Regeln

Übermäßig großzügige oder unnötige Regeln erhöhen die Angriffsfläche erheblich.

2. Administrator-Konten und Zugriffsrechte kontrollieren

Administrativer Zugriff sollte ausschließlich autorisierten Personen vorbehalten sein.

Überprüfen Sie:

- Nicht mehr genutzte Administrator-Konten
- Gemeinsame Benutzerkonten
- Schwache Passwörter
- Übermäßige Berechtigungen
- Management-Zugriffe aus unsicheren Netzwerken

Jedes Administrator-Konto sollte einer konkreten Person zugeordnet und durch starke Authentifizierung geschützt sein.

3. Sicherheitsdienste auf Lizenzierung und Aktivierung prüfen

Viele Unternehmen investieren in Sicherheitslizenzen, nutzen die bereitgestellten Schutzmechanismen jedoch nicht vollständig.

Kontrollieren Sie den Status von:

- DPI SSL (Aufbrechen von HTTPS Verkehr)
- Gateway Anti-Virus (GAV)
- Intrusion Prevention Service (IPS)
- Anti-Spyware
- Capture ATP
- Content Filtering Service (CFS)
- Botnet Filtering
- Geo-IP Filtering

Eine gültige Lizenz allein bietet keinen Schutz – die Dienste müssen auch aktiviert und den entsprechenden Sicherheitszonen zugewiesen sein.

4. VPN-Sicherheitseinstellungen überprüfen

VPN-Verbindungen werden häufig über viele Jahre unverändert betrieben und entsprechen nicht immer aktuellen Sicherheitsstandards.

Achten Sie auf:

- Verwendete IKE-Version
- Verschlüsselungsalgorithmen
- Authentifizierungsverfahren
- Diffie-Hellman-Gruppen
- Perfect Forward Secrecy (PFS)
- Nicht mehr genutzte VPN-Tunnel

Aktuelle kryptografische Verfahren erhöhen die Sicherheit und unterstützen die Einhaltung von Compliance-Anforderungen.

5. Firmware-Version und Sicherheitsupdates kontrollieren

Veraltete Firmware kann bekannte Schwachstellen enthalten und die Stabilität des Systems beeinträchtigen.

Prüfen Sie:

- Installierte Firmware-Version
- Verfügbare Updates
- Bekannte Sicherheitswarnungen
- Firmware-Historie
- End-of-Life-Status der Hardware

Regelmäßige Firmware-Updates gehören zu den wichtigsten Maßnahmen einer sicheren Firewall-Administration.

6. Ungenutzte Objekte identifizieren

In vielen Umgebungen existieren hunderte oder sogar tausende Adress- und Serviceobjekte, von denen ein Teil nicht mehr verwendet wird.

Suchen Sie nach:

- Ungenutzten Adressobjekten
- Ungenutzten Serviceobjekten
- Leeren Gruppen
- Doppelten Einträgen
- Überresten früherer Migrationen

Das Bereinigen nicht verwendeter Objekte verbessert die Übersichtlichkeit und reduziert den Verwaltungsaufwand.

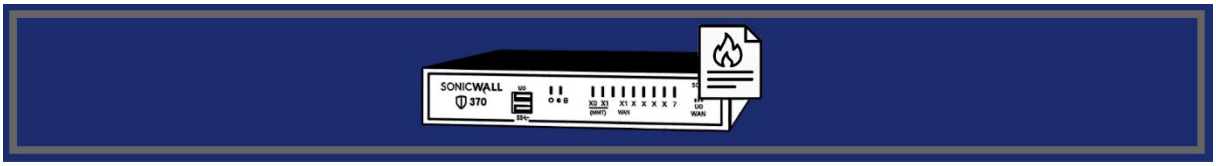
7. NAT-Richtlinien überprüfen

NAT-Regeln werden häufig erstellt, jedoch selten wieder entfernt.

Kontrollieren Sie:

- Ungenutzte NAT-Richtlinien
- Deaktivierte NAT-Einträge
- Doppelte Übersetzungen
- Zu weit gefasste Portfreigaben
- Veraltete Konfigurationen

Jede aktive NAT-Regel sollte nachvollziehbar dokumentiert und fachlich begründet sein.



8. Protokollierung und Monitoring validieren

Ohne aussagekräftige Protokolle bleiben Sicherheitsvorfälle häufig unentdeckt.

Stellen Sie sicher, dass:

- Logging aktiviert ist
- Syslog-Server erreichbar sind
- Sicherheitsereignisse protokolliert werden
- Audit-Daten ausreichend lange gespeichert werden
- Alarmierungsfunktionen korrekt arbeiten

Eine Firewall kann nur dann wirksam überwacht werden, wenn relevante Ereignisse auch erfasst und ausgewertet werden.

9. Hochverfügbarkeit und WAN-Failover testen

Viele Unternehmen verlassen sich auf Redundanzmechanismen, ohne deren Funktion regelmäßig zu überprüfen.

Kontrollieren Sie:

- Status der High-Availability-Konfiguration
- Synchronisation zwischen den Geräten
- WAN-Failover-Einstellungen
- Erreichbarkeitsprüfungen (Probes)
- Load-Balancing-Konfigurationen
- Dokumentierte Failover-Ereignisse

Nur getestete Redundanzmechanismen bieten im Ernstfall die gewünschte Ausfallsicherheit.

10. Management-Dienste und externe Erreichbarkeit prüfen

Administrationsdienste sollten niemals unnötig aus dem Internet erreichbar sein.

Überprüfen Sie insbesondere:

- HTTPS-Management
- SSH-Zugriffe
- SNMP-Zugriff
- API-Zugänge
- SSL-VPN-Portale
- Authentifizierungsdienste

Management-Zugriffe sollten grundsätzlich auf vertrauenswürdige Netzwerke oder VPN-Verbindungen beschränkt werden.

Fazit

Die SonicWall Firewall bildet in vielen Unternehmen die zentrale Sicherheitskomponente des Netzwerks. Regelmäßige Überprüfungen helfen dabei, Sicherheitsrisiken frühzeitig zu erkennen, Fehlkonfigurationen zu vermeiden und die langfristige Stabilität der Umgebung sicherzustellen.

Eine strukturierte Analyse deckt nicht nur technische Schwachstellen auf, sondern schafft auch Transparenz über Sicherheitsdienste, Zugriffsrechte, VPN-Konfigurationen und die allgemeine Qualität der Firewall-Konfiguration.

Werden diese zehn Punkte regelmäßig überprüft, lässt sich die Sicherheit der Infrastruktur nachhaltig verbessern und der administrative Aufwand deutlich reduzieren.

Klingt nach viel Arbeit? Die Software „Firewall Toolbox“ erstellt Ihnen in wenigen Minuten einen umfangreichen Report über ihre SonicWall Firewall. Mehr Infos unter www.firewall-toolbox.com.

Keine Zeit / keine Ressourcen?

Buchen Sie einen begleiteten Firewall Audit! Bei mir oder einem Reseller, der Firewall Toolbox einsetzt

Kontakt: Martin Schmitz / martin@martinschmitz.it