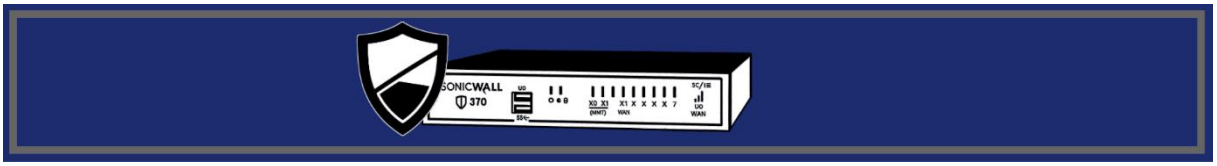


The 10 Most Important Points When Reviewing a SonicWall Firewall

A firewall is only as secure as its configuration. During security assessments and health checks, the same configuration mistakes repeatedly appear — often remaining unnoticed for years. The following ten areas should therefore be reviewed regularly to ensure the security, stability, and transparency of a SonicWall environment.

1. Review Firewall Rules

Firewall rules determine which traffic is allowed or blocked. Over time, temporary exceptions, test rules, and outdated configurations often accumulate.

Pay particular attention to:

- Rules from WAN to internal networks
- “Any → Any” permissions
- Overly broad service definitions
- Disabled but not removed rules
- Duplicate or overlapping rules

Excessively permissive or unnecessary rules significantly increase the attack surface.

2. Review Administrator Accounts and Access Rights

Administrative access should only be granted to authorized personnel.

Check for:

- Unused administrator accounts
- Shared user accounts
- Weak passwords
- Excessive privileges
- Management access from insecure networks

Every administrator account should be assigned to a specific individual and protected by strong authentication.

3. Verify Security Service Licensing and Activation

Many companies invest in security licenses but do not fully utilize the available protection mechanisms.

Check the status of:

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

A valid license alone does not provide protection — the services must also be enabled and assigned to the appropriate security zones.

4. Review VPN Security Settings

VPN connections are often operated unchanged for many years and may no longer meet current security standards.

Pay attention to:

- The IKE version in use
- Encryption algorithms
- Authentication methods
- Diffie-Hellman groups
- Perfect Forward Secrecy (PFS)
- Unused VPN tunnels

Modern cryptographic methods improve security and support compliance requirements.

5. Check Firmware Version and Security Updates

Outdated firmware may contain known vulnerabilities and can affect system stability.

Review:

- Installed firmware version
- Available updates
- Known security advisories
- Firmware history
- Hardware end-of-life status

Regular firmware updates are among the most important measures in secure firewall administration.

6. Identify Unused Objects

Many environments contain hundreds or even thousands of address and service objects, some of which are no longer used.

Look for:

- Unused address objects
- Unused service objects
- Empty groups
- Duplicate entries
- Remnants from previous migrations

Cleaning up unused objects improves clarity and reduces administrative overhead.

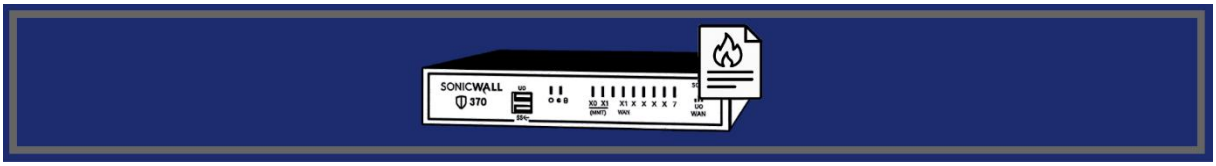
7. Review NAT Policies

NAT rules are often created but rarely removed.

Check for:

- Unused NAT policies
- Disabled NAT entries
- Duplicate translations
- Overly broad port forwarding
- Outdated configurations

Every active NAT rule should be properly documented and technically justified.



8. Validate Logging and Monitoring

Without meaningful logs, security incidents often remain undetected.

Ensure that:

- Logging is enabled
- Syslog servers are reachable
- Security events are being logged
- Audit data is retained long enough
- Alerting functions operate correctly

A firewall can only be effectively monitored if relevant events are captured and analyzed.

9. Test High Availability and WAN Failover

Many organizations rely on redundancy mechanisms without regularly testing their functionality.

Review:

- High Availability configuration status
- Synchronization between devices
- WAN failover settings
- Reachability checks (probes)
- Load balancing configurations
- Documented failover events

Only tested redundancy mechanisms provide the desired resiliency during outages.

10. Review Management Services and External Accessibility

Administrative services should never be unnecessarily accessible from the Internet.

Pay particular attention to:

- HTTPS management
- SSH access
- SNMP access
- API access
- SSL-VPN portals
- Authentication services

Management access should generally be restricted to trusted networks or VPN connections.

Conclusion

In many organizations, the SonicWall firewall represents the central security component of the network. Regular reviews help identify security risks early, avoid misconfigurations, and ensure the long-term stability of the environment.

A structured analysis not only uncovers technical vulnerabilities but also creates transparency regarding security services, access rights, VPN configurations, and the overall quality of the firewall configuration.

If these ten points are reviewed regularly, infrastructure security can be significantly improved while reducing administrative effort.

Firewall Toolbox

Sounds like a lot of work? The software “Firewall Toolbox” creates a comprehensive report about your SonicWall firewall within just a few minutes. More information at:

No time or resources available?

Book a guided firewall audit — either directly with Martin Schmitz or through a reseller using Firewall Toolbox.

Contact: Martin Schmitz / martin@martinschmitz.it