SonicWall Configuration Audit Report

Generated: 2026-02-03T07:55:32.363664

Firewall Information

Model	NSa 2800
Firmware	8.1.0-8017-R8779
Ha Enabled	No
Factory Default	off

Executive Summary

Severity	Count
CRITICAL	0
HIGH	3
MEDIUM	3
LOW	1
INFO	3

Detailed Findings

Administrative Access

[HIGH] **Multi-Factor Authentication Not Enforced**

Description: One-Time Password (TOTP) is not required for administrator login.

Current Value: MFA Disabled

Recommended: Enable TOTP for all administrators

Reference: CIS Controls - Use Multi-Factor Authentication

Remediation: Navigate to Device > Settings > Administration and enable 'Require OTP for login'.

[MEDIUM] **Admin Login Timeout Too Long**

Description: Admin session timeout is set too high, increasing risk of session hijacking.

Current Value: 999 minutes

Recommended: 5-15 minutes

Reference: SonicWall Best Practices Guide - Administrative Access

Remediation: Navigate to Device > Settings > Administration and set 'Administrator inactivity timeout' to 15 minutes or less.

[LOW] **Login Banner Not Configured**

Description: A login warning banner is not configured.

Current Value: No banner configured

Recommended: Configure authorized use warning banner

Reference: NIST 800-53 AC-8 - System Use Notification

Remediation: Configure login banner via Device > Settings > Administration.

[INFO] **Admin Session Preemption Not Configured**

Description: Administrator session preemption behavior is not configured.

Current Value: Default (no preemption)

Recommended: Configure based on requirements

Reference: SonicWall Administration Guide

Remediation: Consider configuring admin session preemption policy.

NAT Policies

[INFO] **NAT Policies Review Recommended**

Description: NAT policies are configured. Review to ensure only necessary services are exposed.

Current Value: 2514 NAT-related settings found

Recommended: Review all inbound NAT policies

Reference: Network Security Best Practices

Remediation: Audit NAT policies to minimize attack surface.

Security Services

[HIGH] **DPI-SSL Client Inspection Disabled**

Description: DPI-SSL Client inspection is disabled. Encrypted traffic will not be inspected.

Current Value: DPI-SSL Client: Disabled

Recommended: Enable DPI-SSL for encrypted traffic inspection

Reference: SonicWall DPI-SSL Deployment Guide

Remediation: Enable DPI-SSL Client inspection under Firewall Settings > DPI-SSL.

[MEDIUM] **DPI-SSL Server Inspection Disabled**

Description: DPI-SSL Server inspection is disabled.

Current Value: DPI-SSL Server: Disabled

Recommended: Enable DPI-SSL Server for inbound inspection

Reference: SonicWall DPI-SSL Deployment Guide

Remediation: Enable DPI-SSL Server inspection if hosting internal services.

Logging & Monitoring

[MEDIUM] **Analytics Integration Not Configured**

Description: SonicWall Analytics/NSM integration is not configured.

Current Value: Analytics: Not configured

Recommended: Configure NSM or Analytics integration

Reference: SonicWall Network Security Manager Guide

Remediation: Consider enabling NSM or Analytics for centralized management.

[INFO] **Syslog Server Configured**

Description: Syslog server is configured to send logs to external server.

Current Value: Syslog: nsm-uswest-syslog.sonicwall.com

Recommended: Verify logs are being received

Reference: NIST 800-53 AU-4 - Audit Storage Capacity

Remediation: Verify syslog server is receiving logs and retention is adequate.

SSL/TLS Security

[HIGH] **Weak TLS Ciphers Enabled**

Description: Found 18 weak or obsolete cipher suites enabled.

Current Value: Weak ciphers enabled: 18

Recommended: Disable weak ciphers (NULL, EXPORT, RC4, DES)

Reference: NIST TLS Implementation Guidelines

Remediation: Review and disable weak cipher suites in TLS settings.