FIREWALL TOOLBOX

Empfehlungen – Best-Practice-Bericht

Appliance-Details

Seriennummer:	0040XXXXXXXX (Demo)
Firewall-Name:	UDS-NSV270
Appliance-Modell:	SonicWall NSv 270
Betriebszeit (Uptime):	0 Days, 0 Hours, 8 Minutes, 0 Seconds
Firmware-Version:	7.3.0-7012-R8150

Berichtsdetails

Erstellt am:	15.04.2026 09:22:04
EXP File:	C:\U...\Repository\0040XXXXXXXX\exp_api_downloaded.exp
EXP-Zeitstempel:	15.04.2026 08:42:20
TSR-Datei:	C:\U...\Repository\0040XXXXXXXX\tsr_api_downloaded.wri
TSR-Zeitstempel:	15.04.2026 08:42:21

Empfehlungen – Best-Practice-Bericht

Konfigurationsabgleich mit Best Practices

Dieser Bericht bewertet die aktuelle Konfiguration der SonicWall-Firewall anhand etablierter Best-Practice-Empfehlungen. Ziel ist es, Einstellungen zu identifizieren, die bereits den betrieblichen und sicherheitstechnischen Standards entsprechen, und gleichzeitig Bereiche hervorzuheben, in denen Verbesserungen sinnvoll sein können. Die Analyse soll eine strukturierte Überprüfung der Gerätekonfiguration im Hinblick auf Sicherheit, Wartbarkeit, Ausfallsicherheit und allgemeine Betriebsstabilität unterstützen.

Eine an Best Practices ausgerichtete Firewall-Konfiguration trägt dazu bei, betriebliche Risiken zu reduzieren, die Administration zu vereinfachen und die Nachvollziehbarkeit bei Support- und Audit-Aktivitäten zu verbessern. Neben technischen Sicherheitsmechanismen umfasst dies auch eine konsistente Konfiguration, eine eindeutige Gerätebezeichnung sowie die Vermeidung unnötiger oder veralteter Einstellungen. Jeder geprüfte Abschnitt dieses Berichts dient daher nicht nur der Statusanzeige, sondern erläutert auch kurz die betriebliche oder sicherheitstechnische Relevanz des jeweiligen Prüfpunkts.

Besondere Aufmerksamkeit gilt dem Software- und Firmware-Stand der Firewall. Der Bericht prüft, ob die aktuell installierte Firmware dem vorgesehenen Stand entspricht und ob Hinweise auf ein nicht unterstütztes Firmware-Downgrade vorliegen. Dies ist wichtig, da veraltete Firmware bekannte Probleme oder Sicherheitsrisiken mit sich bringen kann, während nicht unterstützte Downgrade-Szenarien Stabilität, Kompatibilität und Herstellersupport beeinträchtigen können. Ein konformer Firmware-Stand ist daher eine wesentliche Voraussetzung für einen sicheren und zuverlässigen Betrieb.

Darüber hinaus wird geprüft, ob IPv6 aktiviert ist und ob dessen Nutzung für die jeweilige Umgebung sinnvoll erscheint. Wird IPv6 nicht benötigt, sollte es in der Regel deaktiviert werden, um unnötige Angriffsfläche und zusätzlichen Administrationsaufwand zu vermeiden. Ebenso bewertet der Bericht, ob High Availability aktiviert ist. Ist High Availability nicht im Einsatz, wird deren Implementierung dringend empfohlen, da sie die Ausfallsicherheit erhöht und Ausfallzeiten bei Hardwarefehlern oder geplanten Wartungsarbeiten reduziert.

Ein weiterer wichtiger Bereich ist die Redundanz der Internetanbindung. Die Konfiguration wird daraufhin überprüft, ob mehrere WAN-Verbindungen vorhanden sind. Wenn nur eine einzelne WAN-Anbindung genutzt wird, wird eine zusätzliche WAN-Leitung dringend empfohlen, um die Redundanz zu erhöhen und die Internetverbindung bei einem Providerausfall aufrechtzuerhalten. Auch WAN-bezogene Optimierungseinstellungen wie die MTU werden berücksichtigt. Falls die WAN-MTU ungewöhnlich niedrig konfiguriert ist, sollte dies geprüft werden, da unnötig niedrige MTU-Werte die Übertragungseffizienz verringern und die Netzwerkleistung beeinträchtigen können.

Aus Sicherheitssicht umfasst der Bericht außerdem Prüfungen zu Benutzerschutz, VPN-Härtung und Bedrohungsabwehr. Es wird bewertet, ob administrative Benutzerkonten durch Zwei-Faktor-Authentifizierung geschützt sind, was dringend empfohlen wird, um das Risiko unbefugter Zugriffe durch schwache, wiederverwendete oder kompromittierte Zugangsdaten zu reduzieren. Zusätzlich wird die VPN-Konfiguration auf veraltete Verschlüsselungsalgorithmen, schwache Chiffren oder Legacy-Einstellungen geprüft, die die Sicherheit verschlüsselter Verbindungen beeinträchtigen können. Darüber hinaus wird kontrolliert, ob Detection- und Prevention-Funktionen aktiviert sind, da diese wesentlich dazu beitragen, verdächtige Aktivitäten frühzeitig zu erkennen und potenzielle Bedrohungen zu blockieren.

Auch die administrative Nachvollziehbarkeit und betriebliche Disziplin werden durch Prüfungen wie internes Audit-Logging und den Status von Packet Capture berücksichtigt. Eine aktivierte interne Audit-Funktion ist wichtig, da sie Konfigurationsänderungen und administrative Aktionen nachvollziehbar protokolliert und damit Fehlersuche, Sicherheitsanalysen und Compliance-Anforderungen unterstützt. Zudem zeigt der Bericht, ob Packet Capture noch aktiv ist. Eine dauerhaft laufende Paketaufzeichnung kann auf eine nicht abgeschlossene Fehlersuche hinweisen und unnötige Last verursachen, wenn sie ohne betrieblichen Grund aktiv bleibt.

Abschließend betrachtet der Bericht den allgemeinen Auslastungszustand der Firewall. Die Überprüfung der Gesamtauslastung ist wichtig, um zu erkennen, ob das Gerät innerhalb eines unkritischen Lastbereichs arbeitet oder sich seinen Kapazitätsgrenzen nähert. Eine dauerhaft hohe Auslastung kann auf Leistungsrisiken hinweisen und sollte weiter untersucht werden. Insgesamt liefern die Ergebnisse dieses Berichts einen praxisnahen Überblick über die Qualität der aktuellen Konfiguration und helfen dabei, Maßnahmen zur Verbesserung der Sicherheitslage, Betriebsstabilität und langfristigen Wartbarkeit zu identifizieren.

Firewall Name

Die Umbenennung einer SonicWall-Firewall von der Seriennummer in einen aussagekräftigen Gerätenamen verbessert Administration, Fehlersuche und Reporting. Ein beschreibender Name erleichtert die sofortige Zuordnung von Standort, Funktion oder Kundenzugehörigkeit, insbesondere in Umgebungen mit mehreren Geräten. Dadurch werden Verwechslungen reduziert, Support-Prozesse beschleunigt und das Risiko von Konfigurations- oder Bedienfehlern verringert.

Funktion - Einstellung	Status	Empfehlung
Firewall Name wurde geändert	Status	-

Firmware und Settings

Dieser Abschnitt zeigt, ob die aktuelle Firmware-Version verwendet wird und ob ein nicht unterstütztes Firmware-Downgrade erkannt wurde. So lässt sich der Softwarestand schnell bewerten und mögliche Risiken für Betrieb, Kompatibilität und Support erkennen.

Funktion - Einstellung	Status	Empfehlung
Firmware Version ist aktuell	Update verfügbar	Neue Firmware installieren
Firmware Version ist aktuell	Update verfügbar	Neue Firmware installieren

IPv6 Status

Wenn IPv6 in der Umgebung nicht benötigt wird, sollte es deaktiviert werden, um unnötige Angriffsfläche und administrativen Aufwand zu reduzieren.

Funktion - Einstellung	Status	Empfehlung
IPv6 Status	deaktiviert	-

High Availability Status

Wenn High Availability nicht aktiviert ist, wird der Einsatz dringend empfohlen, um die Ausfallsicherheit zu erhöhen und Ausfallzeiten bei Hardwarefehlern oder Wartungsarbeiten zu reduzieren. Dadurch wird die Servicekontinuität verbessert und die Gesamtverfügbarkeit der Sicherheitsinfrastruktur erhöht.

Funktion - Einstellung	Status	Empfehlung
HA-Gerät / VM	verfügbar	-
- Stateful Sync:	enabled	-
- preempt mode	disabled	-

Redundante WAN Leitungen

Wenn nur eine einzelne WAN-Verbindung genutzt wird, wird eine zusätzliche WAN-Leitung dringend empfohlen, um die Redundanz zu erhöhen und die Internetanbindung bei einem Providerausfall aufrechtzuerhalten. Mehrere WAN-Verbindungen verbessern zudem die Gesamtverfügbarkeit und können Failover oder Lastverteilung unterstützen.

Funktion - Einstellung	Status	Empfehlung
Redundante WAN Leitungen	konfiguriert	-

VPN Konfiguration

Dieser Abschnitt weist auf mögliche Probleme in der VPN-Konfiguration hin, wie veraltete Verschlüsselungsalgorithmen, schwache Chiffren oder Legacy-Einstellungen.

Funktion - Einstellung	Status	Empfehlung
VPN unsichere Algorithmen verwendet	ja	Änderung der VPN Konfiguration

Internes Firewall Audit

Dieser Abschnitt zeigt, ob die interne Audit-Funktion auf der SonicWall-Firewall aktiviert ist. Eine aktivierte Audit-Funktion ist wichtig, da sie Konfigurationsänderungen und administrative Aktionen nachvollziehbar protokolliert. Dies unterstützt die Fehlersuche, Sicherheitsanalysen und die Erfüllung von Compliance-Anforderungen.

Funktion - Einstellung	Status	Empfehlung
Internes Audit	aktiviert	-
Admin User wurde verwendet	ja	personalisierte Accounts verwenden

Detection und Prevention Funktionen

Dieser Abschnitt zeigt, ob Detection- und Prevention-Funktionen auf der SonicWall-Firewall aktiviert sind.

Funktion - Einstellung	Status	Empfehlung
Stealth Mode	aktiviert	-
Randomize IP ID	aktiviert	-

Packet Capture aktiv

Dieser Abschnitt zeigt, ob Packet Capture auf der SonicWall-Firewall aktuell noch aktiv ist.

Funktion - Einstellung	Status	Empfehlung
Paketaufzeichnung	deaktiviert	-

Benutzerkontenschutz

Dieser Abschnitt zeigt, ob Benutzerkonten auf der SonicWall-Firewall durch Zwei-Faktor-Authentifizierung (2FA) geschützt sind.

Funktion - Einstellung	Status	Empfehlung
Admin Konto 2FA geschützt	ja	Service oder Feature aktivieren
User Konten mit TOTP geschützt	nein	-

Firewall Auslastung

Dieser Abschnitt zeigt die Gesamtauslastung der SonicWall-Firewall. Die Überwachung der Gesamtauslastung ist wichtig, um erhöhte Lastzustände zu erkennen, die sich auf Performance, Stabilität oder die Wirksamkeit von Sicherheitsdiensten auswirken können.

Funktion - Einstellung	Status	Empfehlung
Auslastung letzte Minute	0 %	OK
Auslastung letzte Stunde	0 %	OK
Auslastung letzter Tag	0 %	OK
Auslastung letzter Tag	0 %	OK

Lizenzierte, aber nicht genutzte Sicherheitsdienste

Lizenzierte, aber nicht genutzte Sicherheitsdienste bieten keinen wirksamen Schutz und sollten überprüft werden, um festzustellen, ob sie aktiviert, optimiert oder eingestellt werden sollten.

Funktion - Einstellung	Status	Empfehlung
Anzahl der Services	2	Service oder Feature aktivieren

Ein oder mehrere Security Services sind aktiv auf der Zone, aber generell ausgeschaltet

Das Aktivieren eines Sicherheitsdienstes auf einer Zone, während der Dienst selbst global deaktiviert ist, führt zu keiner wirksamen Schutzwirkung. Obwohl die Zonenkonfiguration anzeigt, dass der Dienst aktiv ist, läuft die zugrunde liegende Engine nicht, sodass keine Inspektion oder Filterung erfolgt. Dies kann ein falsches Sicherheitsgefühl erzeugen und zu fehlerhaft konfigurierten Firewall-Richtlinien führen.

Funktion - Einstellung	Status	Empfehlung
Ein oder mehrere Security Services sind aktiv auf der Zone, aber generell ausgeschaltet	True	

WAN MTU Einstellung

Eine korrekt konfigurierte WAN-MTU ist wichtig, um eine effiziente Paketübertragung und eine stabile Netzwerkkommunikation sicherzustellen. Ist der MTU-Wert zu niedrig eingestellt, kann dies den Durchsatz verringern, den Overhead erhöhen und die Performance von Anwendungen oder VPN-Verbindungen negativ beeinflussen.

Funktion - Einstellung	Status	Empfehlung
Niedriger WAN MTU Wert	nicht gefunden	-

Firewall Regeln, die lange nicht verwendet wurden

Regeln, die derzeit nicht verwendet werden, bieten keinen betrieblichen Mehrwert. Um das Regelwerk klar und effizient zu halten, sollten diese ungenutzten Regeln neu bewertet und, wo angemessen, entfernt werden.

Regel-Typ	Anzahl
Firewall-Regeln, die nie verwendet wurden (IP v4)	0
Firewall Regeln, die eine lange Zeit nicht verwendet wurden (IP v4)	0

Deaktivierte Firewall Rules

Regeln, die derzeit nicht verwendet werden, bieten keinen betrieblichen Mehrwert. Um das Regelwerk klar und effizient zu halten, sollten diese ungenutzten Regeln neu bewertet und, wo angemessen, entfernt werden.

Regel-Typ	Anzahl
Deaktivierte Firewall Regeln (IP v4)	0

Firewall Regeln, die Zugriffe aus unsicheren Netzen zulassen

Diese Regeln erhöhen die Angriffsfläche und sollten auf unbedingt erforderliche Dienste beschränkt werden, bei regelmäßiger Überprüfung der geschäftlichen Notwendigkeit.

Regel-Typ	Anzahl
Firewall-Regeln, die Zugriffe aus dem WAN erlauben (IP v4)	0

ANY <> ANY Regeln

Regeln, die beliebigen Verkehr von jeder Quelle zu jedem Ziel über jeden Port erlauben, schaffen eine übermäßige Exponierung und sollten vermieden werden, sofern keine klar begründete und dokumentierte geschäftliche Notwendigkeit besteht.

Regel-Typ	Anzahl
ANY <> ANY Regeln (IP v4)	0

Regeln, die Management Zugriffe erlauben

Regeln, die Management-Zugriff erlauben, sollten strikt auf autorisierte Quellen und abgesicherte Dienste beschränkt werden, da sie bei zu weitreichender Freigabe ein hohes Risiko darstellen.

Regel-Typ	Anzahl
Regeln, die Management Zugriffe erlauben (IP v4)	0

Ungenutzte NAT Policies

Ungenutzte NAT-Richtlinien haben keine aktive Funktion und sollten regelmäßig überprüft werden, um festzustellen, ob sie weiterhin benötigt oder entfernt werden können.

Regel-Typ	Anzahl
Ungenutzte NAT Policies (IP v4)	0

Deaktivierte NAT Policies

Ungenutzte NAT-Richtlinien haben keine aktive Funktion und sollten regelmäßig überprüft werden, um festzustellen, ob sie weiterhin benötigt oder entfernt werden können.

Regel-Typ	Anzahl
Deaktivierte NAT Policies (IP v4)	0

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen