

FIREWALL TOOLBOX

Vollständiger Bericht



Appliance-Details

Seriennummer: 0040103CD830
Firewall-Name: UDS-NSV270
Appliance-Modell: SonicWall NSv 270

Betriebszeit (Uptime): 0 Days, 0 Hours, 22 Minutes, 15 Seconds
Firmware-Version: 7.3.0-7012-R8150

Berichtsdetails

Erstellt am: 15.09.2026 16:35:43

EXP-Datei: C:\Us...ox\Repository\0040103CD830\exp_api_downloaded.exp
EXP-Zeitstempel: 15.09.2026 16:33:48

TSR-Datei: C:\Us...ox\Repository\0040103CD830\tsr_api_downloaded.wri
TSR-Zeitstempel: 15.09.2026 16:33:49

Zusatzinformation

- IPv6 ist deaktiviert. IPv6-bezogene Berichte sind nicht enthalten.
- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Inhaltsverzeichnis

Empfehlungen - Best-Practice-Bericht	3
Sicherheitsreport	9
Bericht zu Audit-Einstellungen	10
Report Regeln bei denen DPI SSL nicht aktiv ist	12
Client DPI-SSL-Entschlüsselung	14
Regeln, die Any Destination und Any Port erlauben (IPv4)	20
Regeln, die Zugriff aus unsicheren Netzen erlauben (IPv4)	22
Optionen für Verwaltungszugriff	24
Security Services - Übersicht (aktiviert - deaktiviert)	28
Security Services - Zuweisung pro Zone	29
Benutzerkonten-Schutz	31
Externe Authentifizierungsmethoden für Benutzer	33
Übersicht Administrativer Benutzer	34
Konfigurationsempfehlungen für VPN-Sicherheit	35
Health-Report	38
Firewall-Auslastungsanalyse	39
Übersicht Konfigurations- und Firmware-Historie	43
Zuverlässigkeit - High Availability	44
Produkt-Lifecycle-Informationen	46
Security Services - Lizenzstatus-Übersicht	47
Zuverlässigkeit - WAN-Failover	49
Konfigurationsreport	51
TCP Connection Timeout	51
Firewall Dokumentationsreport	54
Alle Audit-Einträge	55
Alle Regeln (IPv4)	58
Management-Regeln (IPv4)	60
Interfaces (IPv4)	63
Übersicht Benutzer- und Gruppenmitgliedschaften	65
Zonen Report	69
Wartungsbericht	71
Vorschläge für Namenskonventionen	72
Doppelte Adress Objekte	74
Externe Protokollierung	76
Deaktivierte Firewall-Regeln	78
Firewall-Regeln lange ungenutzt (IPv4)	80
Deaktivierte NAT-(Network Address Translation)-Policies (IPv4)	82
Aktive NAT-Policies ohne Traffic-Hits (IPv4)	84

Empfehlungen – Best-Practice-Bericht

Seite 1/6

Erläuterung

Konfigurationsabgleich mit Best Practices

Kritisch		(8)
Warnung		(0)
OK		(21)

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.

Empfehlungen – Best-Practice-Bericht

Seite 2/6

Firewall Name wurde geändert

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

Unerlaubtes Firmware downgrade

Hier wird geprüft, ob ein von SonicWall nicht unterstützter Firmware downgrade stattgefunden hat.

Funktion - Einstellung	Status	Empfehlung
Unerlaubtes Firmware downgrade	nicht erkannt	-

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
High-Availability-Status	verfügbar	-

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	-

Empfehlungen – Best-Practice-Bericht

Seite 3/6

VPN Konfiguration

Dieser Abschnitt weist auf mögliche Probleme in der VPN-Konfiguration hin, wie veraltete Verschlüsselungsalgorithmen, schwache Chiffren oder Legacy-Einstellungen. Solche Feststellungen können die Gesamtsicherheit der VPN-Verbindung beeinträchtigen und zu Problemen bei Kompatibilität, Compliance oder Supportfähigkeit führen. Es wird empfohlen, die VPN-Konfiguration zu überprüfen und zu aktualisieren, um sie an aktuelle Sicherheitsstandards und Best Practices anzupassen.

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 Firewall Audit	aktiviert	-

Standard-Administratorkonto wurde verwendet

If internal Audit is active, this feature checks if the generic Admin user was detected in the audit log, It is recommended to use personalied accounts for administration

Funktion - Einstellung	Status	Empfehlung
Standard-Administratorkonto 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
Detection und Prevention Funktionen	aktiviert	-

Packet Capture aktiv

Dieser Abschnitt zeigt, ob Packet Capture auf der SonicWall-Firewall aktuell noch aktiv ist. Eine dauerhaft aktive Paketaufzeichnung sollte überprüft werden, da sie auf eine nicht abgeschlossene Fehlersuche hindeuten kann und Systemressourcen verbrauchen oder unnötige Erfassungsdaten erzeugen kann. Wird sie nicht mehr benötigt, sollte sie gestoppt werden, um unnötigen Overhead und Auswirkungen auf den Betrieb zu vermeiden.

Funktion - Einstellung	Status	Empfehlung
Packet Capture aktiv	nein	-

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	nein	Service oder Feature aktivieren
User Konten mit TOTP geschützt	nein	Service oder Feature aktivieren

Empfehlungen – Best-Practice-Bericht

Seite 4/6

Firewall Auslastung

Die Überwachung der Gesamtauslastung ist wichtig, um erhöhte Lastzustände zu erkennen, die die Leistung, Stabilität oder Wirksamkeit der Sicherheitsdienste beeinträchtigen 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 SicherheitsdiensteLizenzierte, aber nicht genutzte Sicherheitsdienste bieten keinen wirksamen Sc

Dieser Bericht zeigt die Anzahl der Security Services, die lizenziert, aber nicht in Verwendung sind

Funktion - Einstellung	Status	Empfehlung
Anzahl der Services	1	Service oder Feature aktivieren

Security Service nicht aktiv

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
Security Service nicht aktiv	ja	Service oder Feature aktivieren

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 erkannt	nicht gefunden	-

TCP Connection Timeout

Eine Änderung des globalen TCP-Timeouts wirkt sich auf alle TCP-Verbindungen aus, die von der Firewall verarbeitet werden. Es wird daher empfohlen, den Standardwert beizubehalten und abweichende Timeouts nur bei Bedarf für einzelne Zugriffsregeln zu konfigurieren.

Funktion - Einstellung	Status	Empfehlung
Default TCP Timeout wurde geändert	nicht gefunden	-

Empfehlungen – Best-Practice-Bericht

Seite 5/6

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)	21

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)	4

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

Empfehlungen – Best-Practice-Bericht

Seite 6/6

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

Zusatzinformation

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen



Sicherheitsreport

Erläuterung

Security Audit

konzentriert sich auf die Identifizierung potenzieller Sicherheitsrisiken und Schwachstellen in den Richtlinien. Dabei werden Firewall-Regeln auf zu weit gefasste Konfigurationen analysiert, ungenutzte oder riskante Objekte erkannt sowie Benutzerrechte und Zugriffsberechtigungen überprüft. Ziel ist es, Fehlkonfigurationen hervorzuheben, die ausgenutzt werden könnten oder gegen Best Practices verstoßen, und konkrete, umsetzbare Hinweise zur Verbesserung der gesamten Sicherheitslage zu liefern.

Bericht zu Audit-Einstellungen

Erläuterung

Internes Firewall Audit

Interne Auditierung auf Firewalls ist ein wesentlicher Bestandteil zur Sicherstellung operativer Integrität, Nachvollziehbarkeit und Sicherheit in einer Netzwerkumgebung. Die Firewall stellt einen der kritischsten Kontrollpunkte in einer Organisation dar, und Auditierung schafft Transparenz über Konfigurationsänderungen, Zugriffsereignisse und administrative Aktionen, die die Security-Posture direkt beeinflussen.

Verantwortlichkeit und Nachvollziehbarkeit

Audit-Logs dokumentieren, wer Änderungen vorgenommen hat, wann sie erfolgt sind und was verändert wurde. Diese Traceability stellt sicher, dass Zuständigkeiten klar zugeordnet sind und Fehlkonfigurationen, Abweichungen von Standards oder unautorisierte Änderungen schnell identifiziert und korrigiert werden können.

Erkennung unautorisierter oder riskanter Änderungen

Firewalls beeinflussen Zugriffskontrolle, Datenschutz und Traffic-Flows unmittelbar. Interne Auditierung ermöglicht es Administratoren, absichtliche oder versehentliche Konfigurationsänderungen zu erkennen und Sicherheitsvorfälle, Policy-Verstöße oder potenziellen Missbrauch administrativer Privilegien zu identifizieren.

Unterstützung für Compliance und Governance

Viele regulatorische Frameworks verlangen Auditierung kritischer Systeme wie Firewalls. Interne Audit-Einträge unterstützen die Einhaltung von Standards, die z. B. in Finanz-, Gesundheits- oder Behördenumgebungen relevant sind. Sie liefern Nachweise, dass Richtlinien befolgt werden und Schutzmechanismen korrekt durchgesetzt sind.

Operative Einblicke und kontinuierliche Verbesserung

Audit-Logs helfen Security-Teams, Konfigurationshistorie und operative Trends zu verstehen. Eine regelmäßige Review dieser Einträge ermöglicht es Organisationen, Zugriffspolicies zu verfeinern, wiederkehrende Probleme zu identifizieren und Change-Management-Praktiken zu stärken.

Incident-Untersuchung und Forensik

Bei einem Security Event sind interne Audit-Daten häufig eine der wertvollsten Evidenzquellen. Sie ermöglichen, Aktionen auf der Firewall zu rekonstruieren, Root Causes zu analysieren und zu bestimmen, ob bösartige Aktivität oder menschlicher Fehler zum Incident beigetragen haben.

Fazit

Interne Auditierung ist notwendig, um Transparenz, Konsistenz und Verantwortlichkeit im Firewall-Betrieb sicherzustellen. Sie erhöht die Sicherheit, unterstützt regulatorische Anforderungen, ermöglicht schnelleres Troubleshooting und liefert eine zentrale Grundlage für resilientes Netzwerkmanagement.

Bericht zu Audit-Einstellungen

Audit Details

Internes Audit:	on
Im TS-Report identifizierte Audit-Einträge:	2000
Neuester im TS-Report gefundener Audit-Eintrag:	15.09.2026 16:33:49
Ältester im TS-Report gefundener Audit-Eintrag:	27.07.2026 08:29:20

Im Audit-Log identifizierte Benutzer

- UDSAdmin
- admin
- apiuser
- HA Sync

Zusätzliche Informationen

Verwendung eines generischen Administrator-Kontos

Das Benutzerkonto „admin“ wurde in den Audit-Einträgen erkannt. Es wird empfohlen, generische oder gemeinsam genutzte Administrator-Konten für das Firewall-Management zu vermeiden. Stattdessen sollte jeder Administrator ein personalisiertes Konto verwenden.

Die Verwendung individueller Benutzeridentitäten stellt sicher, dass Konfigurationsänderungen nachvollziehbar zugeordnet werden können.

Kommentar

Das Konto HA Sync ist ein internes Systemkonto, das ausschließlich zur Synchronisierung von Konfigurations- und Betriebsdaten zwischen Appliances in einer High-Availability-(HA)-Konfiguration verwendet wird. Dieses Konto ist nicht für manuelle Anmeldung oder administrative Nutzung vorgesehen.

Report Regeln bei denen DPI SSL nicht aktiv ist

Erläuterung

Regeln mit deaktivierter Deep Packet Inspection

Deep Packet Inspection (DPI) ermöglicht es der Firewall, den Netzwerkverkehr über grundlegende Verbindungsinformationen wie Quelle, Ziel und Port hinaus zu analysieren. Sie ist eine wichtige Voraussetzung für die Anwendung von Sicherheitsdiensten und die Erkennung von Bedrohungen im Netzwerkverkehr.

Dieser Bericht identifiziert ****Zugriffsregeln, für die Deep Packet Inspection deaktiviert ist****. Datenverkehr, der diesen Regeln entspricht, kann die DPI-basierte Prüfung umgehen und daher möglicherweise nicht von allen konfigurierten Sicherheitsdiensten profitieren.

Das Deaktivieren von DPI kann für bestimmten Datenverkehr sinnvoll sein, beispielsweise aufgrund von Kompatibilitätsanforderungen, Performance-Aspekten oder weil der betreffende Datenverkehr keine zusätzliche Prüfung erfordert. DPI sollte jedoch grundsätzlich nur bewusst und aus einem dokumentierten Grund deaktiviert werden.

Überprüfen Sie die in diesem Bericht aufgeführten Regeln und stellen Sie sicher, dass die Deaktivierung von DPI erforderlich ist. Wenn kein spezifischer Grund vorliegt, sollte DPI aktiviert werden, damit der Datenverkehr der vorgesehenen Sicherheitsprüfung unterzogen wird.

Regeln, bei denen DPI-SSL Client ausgeschaltet wurde

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	DPI Disabled
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	True
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	True

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Anzahl der Datensätze: 2

Client DPI-SSL-Entschlüsselung

Erläuterung

DPI-SSL Client Inspection ist eine zentrale Sicherheitsfunktion, die es der Firewall ermöglicht, verschlüsselten ausgehenden HTTPS-Verkehr zu untersuchen. Ohne Entschlüsselung haben Sicherheitsdienste wie Gateway Anti-Virus, Intrusion Prevention, Capture ATP, Content Filtering und Application Control nur eingeschränkte Sichtbarkeit auf verschlüsselte Verbindungen, wodurch Bedrohungen die Prüfung möglicherweise umgehen können.

Dieser Bericht prüft, ob DPI-SSL Client Inspection lizenziert und auf der Firewall aktiviert ist. Er zeigt außerdem, auf welchen Zonen die Client Inspection aktiv ist, und hebt Zugriffsregeln hervor, bei denen DPI-SSL explizit deaktiviert wurde. Ausnahmen auf Regelebene sollten sorgfältig überprüft werden, da sie blinde Flecken erzeugen können, in denen verschlüsselter Verkehr nicht untersucht wird und Sicherheitsdienste nicht vollständig greifen können.

Organisationen sollten sicherstellen, dass DPI-SSL Client Inspection dort aktiviert ist, wo es sinnvoll ist, und dass Ausnahmen auf Anwendungen oder Dienste mit dokumentiertem Kompatibilitätsbedarf beschränkt bleiben. Eine regelmäßige Überprüfung der DPI-SSL-Konfiguration trägt dazu bei, die Sichtbarkeit auf verschlüsselten Verkehr aufrechtzuerhalten und das Risiko unentdeckter Bedrohungen zu verringern.

Client DPI-SSL-Entschlüsselung

DPI SSL Licensed: yes

SSL-Entschlüsselung für ausgehenden Verkehr ist nicht aktiv (!)

Client DPI-SSL-Entschlüsselung

Seite 1/1

Zone	DPI SSL Client
LAN	On
WAN	Off
DMZ	Off
VPN	Off
SSLVPN	Off
MULTICAST	Off
DMZ-unsec	Off
DMZ-sec	Off
Test	On
150971-Test	Off
060466	Off

Regeln, bei denen DPI-SSL Client ausgeschaltet wurde

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	DPI-SSL Client Disabled
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	True
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	True
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	True

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Anzahl der Datensätze: 3

Detection und Prevention Funktionen

Erläuterung

Die Optionen Randomize IP ID und Enable Stealth Mode bieten zusätzlichen Schutz vor Netzwerk-Reconnaissance und bestimmten Angriffsarten. Durch die Randomisierung des IP-Identification-Felds wird es für Angreifer schwieriger, ein Betriebssystem-Fingerprinting durchzuführen oder Verkehrsmuster abzuleiten, während der Stealth Mode verhindert, dass die Firewall auf unaufgeforderte Verbindungsversuche reagiert, wodurch ihre Sichtbarkeit in nicht vertrauenswürdigen Netzwerken reduziert wird.

Detection und Prevention Funktionen

Stealth Mode

Stealth Mode aktiviert on

Randomize IP ID

Randomize IP ID aktiviert on

Regeln, die Any Destination und Any Port erlauben (IPv4)

Erläuterung

Warum Firewall-Regeln mit „Any“ riskant sind

Im Bereich der Netzwerksicherheit spielen Firewall-Regeln eine zentrale Rolle bei der Kontrolle von ein- und ausgehendem Traffic. Eine häufige, jedoch stark abzuratende Praxis ist die Implementierung von „any to any“-Regeln. Diese Regeln erlauben unbeschränkten Traffic von jeder Quelle zu jedem Ziel und lassen damit praktisch alle Datenpakete ohne Filterung passieren.

Sicherheitsimplikationen

Das Hauptproblem bei „any to any“-Regeln ist das erhebliche Sicherheitsrisiko. Firewalls sind als Gatekeeper konzipiert und prüfen ein- und ausgehenden Datenverkehr, um das Netzwerk vor unautorisiertem Zugriff, Cyberangriffen und anderen böartigen Aktivitäten zu schützen. Werden Regeln gesetzt, die sämtlichen Traffic indiscriminately zulassen, wird die Kernfunktion der Firewall umgangen und das Netzwerk potenziellen Bedrohungen ausgesetzt. Dieses offene „Gateway“ kann von Angreifern genutzt werden, um auf sensible Informationen zuzugreifen, Malware einzuschleusen oder andere schädliche Exploits auszuführen.

Mangelnde Traffic-Kontrolle

Neben Sicherheitslücken erschweren „any to any“-Regeln auch eine wirksame Überwachung und Steuerung des Netzwerkverkehrs. Effektives Netzwerkmanagement setzt Verständnis und Steuerung von Datenflüssen voraus. Unbeschränkte Regeln machen es schwierig, Traffic zu verfolgen, zu analysieren oder zu priorisieren, was zu Performanceproblemen führen kann, einschließlich Bandbreitenengpässen und geringerer Effizienz.

Compliance und Best Practices

In vielen Branchen verlangen regulatorische Vorgaben eine strikte Kontrolle und Überwachung von Datenverkehr. „Any to any“-Regeln können Compliance-Standards verletzen und rechtliche sowie reputative Folgen nach sich ziehen. Darüber hinaus fordern Best Practices in der Cybersecurity das Least-Privilege-Prinzip, nach dem nur notwendiger Traffic erlaubt wird – was die Problematik permissiver Regeln zusätzlich unterstreicht.

Empfehlung

Anstatt „any to any“-Regeln zu verwenden, wird empfohlen, spezifische und klar definierte Firewall-Regeln nach dem Least-Privilege-Prinzip umzusetzen. Diese Regeln sollten so gestaltet sein, dass sie nur den für den Geschäftsbetrieb notwendigen und legitimen Traffic zulassen und damit sowohl Netzwerksicherheit als auch optimale Performance sicherstellen.

Regeln, die Any Destination und Any Port erlauben (IPv4)

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any
YES	A	Allow Citrix	any		any	any	Citrix UDP	any
YES	A	Allow FTP	any		any	any	FTP	any

Example any<> any

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Anzahl der Datensätze: 5

Regeln, die Zugriff aus unsicheren Netzen erlauben (IPv4)

Erläuterung

Firewall-Regeln mit Zugriff vom WAN auf interne Netze – Risiken und Bewertung

Firewall-Regeln, die eingehenden Datenverkehr aus unsicheren Netzen wie dem Internet (WAN) in interne Netze (LAN, DMZ oder andere interne Zonen) erlauben, stellen ein erhebliches Sicherheitsrisiko dar. Solche Regeln sollten nur in klar definierten Ausnahmefällen existieren und besonders sorgfältig geprüft werden.

Erhöhte Angriffsfläche

Das WAN gilt grundsätzlich als nicht vertrauenswürdig. Jede Regel, die Verbindungen aus dem Internet in interne Netze zulässt, erweitert die Angriffsfläche des Systems. Angreifer können diese Regeln gezielt nutzen, um Schwachstellen in Diensten, Betriebssystemen oder Anwendungen auszunutzen.

Gefahr durch ungepatchte oder falsch konfigurierte Dienste

Intern bereitgestellte Dienste sind häufig nicht für direkten Internetzugriff ausgelegt. Werden solche Systeme über Firewall-Regeln aus dem WAN erreichbar gemacht, können ungepatchte Sicherheitslücken, schwache Authentifizierungsmechanismen oder Fehlkonfigurationen zu erfolgreichen Angriffen führen.

Umgehung interner Sicherheitszonen

WAN-zu-LAN-Regeln unterlaufen häufig das Zonen- und Segmentierungskonzept eines Netzwerks. Ein erfolgreicher Zugriff aus dem WAN kann es Angreifern ermöglichen, sich lateral im internen Netz zu bewegen und weitere Systeme zu kompromittieren.

Risiko durch zu breite Regeln

Besonders kritisch sind Firewall-Regeln mit sehr breiten Quelladressen, unbeschränkten Zielsystemen oder offenen Port- und Service-Bereichen. Solche Konfigurationen widersprechen dem Least-Privilege-Prinzip und erhöhen die Wahrscheinlichkeit von Missbrauch erheblich.

Compliance- und Audit-Risiken

Viele Sicherheitsstandards und Regularien wie ISO 27001, BSI-Grundschutz oder PCI DSS verlangen eine strikte Kontrolle externer Zugriffe. Unzureichend dokumentierte oder nicht notwendige WAN-Zugriffe können zu Audit-Feststellungen und Compliance-Verstößen führen.

Best Practices und Empfehlungen

WAN-Zugriffe sollten nur dann erlaubt werden, wenn sie technisch und fachlich zwingend erforderlich sind. Statt direkter Zugriffe sollten sichere Mechanismen wie VPN-Verbindungen, Reverse Proxies oder Application Gateways eingesetzt werden. Zusätzlich sind strikte Einschränkungen von Quelle, Ziel und Dienst sowie eine regelmäßige Überprüfung und Dokumentation aller entsprechenden Regeln erforderlich.

Fazit

Firewall-Regeln, die Verkehr aus unsicheren Netzen in interne Netze zulassen, gehören zu den kritischsten Konfigurationselementen einer Firewall. Sie sollten auf ein absolutes Minimum reduziert, technisch abgesichert und regelmäßig überprüft werden, um das Risiko von Sicherheitsvorfällen nachhaltig zu senken.

Regeln, die Zugriff aus unsicheren Netzen erlauben (IPv4)

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc
YES	A	Test 24	WAN	060466	any	any	any	OSPF
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)
YES	A	Test 23	WAN	060466	any	any	any	MSN
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH

Temp, Rule to allow M...

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Anzahl der Datensätze: 4

Optionen für Verwaltungszugriff

Erläuterung

Managementzugriffsoptionen und sicherheitsrelevante Aspekte

Es stehen mehrere Methoden für den Managementzugriff auf Firewalls zur Verfügung, die jeweils unterschiedliche Usability-Vorteile und Sicherheitsimplikationen besitzen. Da Managementschnittstellen administrative Kontrolle über kritische Netzwerkinfrastruktur ermöglichen, kann eine unsachgemäße Exponierung dieser Zugangsarten erhebliche Risiken verursachen. Unautorisierter Zugriff auf das Firewall-Management kann zu Konfigurationsmanipulation, Offenlegung sensibler Sicherheitsparameter oder sogar zur vollständigen Kompromittierung der Netzwerkumgebung führen. Daher ist es essenziell, regelmäßig zu überprüfen, welche Managementzugriffsmechanismen aktiviert sind, und sicherzustellen, dass nur sichere, begründete und angemessen geschützte Methoden erreichbar bleiben.

Die Beschränkung des Managementzugriffs auf vertrauenswürdige Netzwerke, die Durchsetzung starker Authentifizierung sowie das Monitoring administrativer Aktivitäten sind zentrale Best Practices zur Aufrechterhaltung einer sicheren und kontrollierten Konfigurationslandschaft.

Optionen für Verwaltungszugriff

Central Management

Central Management (NSM / GMS):	off
NSM ZeroTouch:	enabled

SSL - VPN

SSL VPN Web Management:	on
SSL VPN SSH Management:	off

API

API access:	enabled
-------------	---------

Optionen für Verwaltungszugriff: Interface-Verwaltung

Seite 1/1

Interface	Zone	HTTP	HTTPS	PING	SSH	SNMP	API
X0	LAN	off	on	on	on	on	on
X1	WAN	off	on	on	on	off	on
X2	DMZ-unsec	off	on	on	off	off	on
X3	DMZ-sec	off	on	on	off	off	on
X4	HA Data & Control	off	off	off	off	off	off
X5	WAN	off	off	on	off	off	off
X6	LAN	off	on	on	off	off	on
X7	DMZ-sec	off	off	off	off	off	off
X6:V100	LAN	off	off	off	off	off	off

Optionen für Verwaltungszugriff: IPSec (VPN)

Seite 1/1

Tunnel-Name	Enabled	HTTP	HTTPS	SSH	SNMP
WAN GroupVPN	False	off	off	off	off
SNWL Policy Mode	False	off	on	on	on
Test	False	off	off	off	off
Bad Tunnel	False	off	off	off	off
To TZ570	True	off	off	off	off
Remote Site1	True	off	off	off	off
New York	True	off	off	off	off

Security Services – Übersicht (aktiviert - deaktiviert)

Erläuterung

Aktive Security Services

Dieser Bericht zeigt, welche Security Services auf dem Gerät aktuell aktiviert sind. Eine Aktivierung auf Systemebene bedeutet jedoch nur, dass die Service-Funktionalität verfügbar ist – sie garantiert nicht, dass der Verkehr tatsächlich inspiziert wird.

Für eine wirksame Netzwerkverkehrsanalyse müssen die Security Dienste zusätzlich explizit Zonen zugewiesen oder auf spezifische Firewall-Regeln angewendet werden. Ohne diesen Konfigurationsschritt können die aktivierten Technologien für relevante Netzwerkflüsse inaktiv bleiben, wodurch dann kein Schutz mehr gewährleistet ist.

Security-Service-Status

Deep Packet Inspection for SSL (DPI-SSL)	Off
Gateway AV	On
Anti-Spyware	On
Intrusion Prevention	On
App Control	On
Content Filtering Service	On
GeoIP Filtering	On

Zusatzinformation

Kein Route-All VPN-Tunnel konfiguriert

Derzeit ist kein Route-All VPN-Tunnel konfiguriert und aktiv. Dies ist ein häufiges Szenario in Umgebungen, in denen der gesamte Traffic an ein vorgeschaltetes Security-Device weitergeleitet wird, das für Traffic-Inspection, Policy-Enforcement und zusätzliche Sicherheitsverarbeitung verantwortlich ist. In solchen Setups fungiert die Firewall primär als Routing- oder Segmentierungsgerät, während tiefere Inspektionen durch eine zentrale Sicherheitslösung erfolgen, z. B. Secure Web Gateway, Cloud-Security-Service oder eine dedizierte Inspection-Plattform.

Security Services – Zuweisung pro Zone

Erläuterung

Security Services

Dieser Bericht zeigt, welche Security Services auf jeder Zone aktiviert sind. Während eine globale Aktivierung die Funktionalität bereitstellt, wird tatsächlicher Schutz nur angewendet, wenn der Service aktiv auf Zonenebene zugewiesen ist. Security Services, die an Zonen gebunden sind, bestimmen, welche Netzwerksegmente auf Bedrohungen wie Malware, Intrusion-Versuche oder unerwünschte Inhalte geprüft werden. Zonen ohne entsprechende Service-Zuweisung können unzureichend geschützt bleiben – selbst wenn die Funktion im System aktiviert ist. Diese Übersicht hilft, Coverage-Gaps zu identifizieren, zu verifizieren, dass kritische Zonen (z. B. LAN oder VPN-Zugriffsbereiche) angemessen geschützt sind, und sicherzustellen, dass Inspection-Policies mit organisatorischen Sicherheitsanforderungen übereinstimmen.

Zusatzinformation

Sicherheitsdienste, die mit (!) gekennzeichnet sind, sind in der Zone aktiviert, jedoch global deaktiviert.

Security Services – Zuweisung pro Zone

Seite 1/1

Zone	ClientAV	GatewayAV	IPS	AntiSpyware	DPI SSL Client	DPI SSL Server	SSLControl
LAN	Off	On	On	On	On (!)	Off	Off
WAN	Off	On	On	On	Off	On (!)	Off
DMZ	Off	Off	Off	Off	Off	Off	Off
VPN	Off	Off	Off	Off	Off	Off	Off
SSLVPN	Off	Off	Off	Off	Off	Off	Off
MULTICAST	Off	Off	Off	Off	Off	Off	Off
DMZ-unsec	Off	Off	Off	Off	Off	Off	Off
DMZ-sec	Off	Off	Off	Off	Off	Off	Off
Test	Off	On	On	On	On (!)	Off	Off
150971-Test	Off	Off	Off	Off	Off	Off	Off
060466	Off	On	On	On	Off	Off	Off

Benutzerkonten-Schutz

Erläuterung

Übersicht Benutzerkontoschutz

Dieser Bericht listet alle Benutzerkonten auf und zeigt, wie sie geschützt sind, einschließlich der Frage, ob Zwei-Faktor-Authentifizierung (2FA) aktiviert ist. Dies hilft, die Stärke der Authentifizierungsmechanismen zu verifizieren und Konten zu identifizieren, die zusätzlichen Schutz benötigen.

Benutzerkonten-Schutz

Seite 1 / 1

Benutzername	Einmalpasswort (TOTP) aktiviert
admin	NO
All LDAP Users	NO
apiuser	NO
Isabel	NO
LocalAdmin	YES
mschmitz	NO
Robert	NO
Sylvia	NO
Udo	NO
Uwe	NO
Webadmin	NO

Externe Authentifizierungsmethoden für Benutzer

Erläuterung

Übersicht externe Authentifizierungskonfiguration

Dieser Bericht zeigt, welche externen Authentifizierungssysteme konfiguriert sind, ob sie aktiviert sind, und weist auf potenzielle Sicherheitsbedenken in Bezug auf deren Setup hin. Externe Authentifizierung kann das Identity Management erheblich stärken, wenn sie korrekt implementiert ist; eine fehlerhafte Konfiguration kann jedoch Sicherheits- und Betriebsrisiken verursachen.

LDAP (Lightweight Directory Access Protocol)

Wenn LDAP verwendet wird, werden Authentifizierungsanfragen an ein externes Verzeichnis wie Microsoft Active Directory weitergeleitet.

LDAP zentralisiert Benutzeridentitäten und Passwortmanagement und reduziert die Abhängigkeit von lokalen Konten.

LDAP-Authentifizierung sollte jedoch stets über TLS (LDAPS) abgesichert werden.

Unverschlüsselte LDAP-Kommunikation setzt Benutzernamen, Passwörter und Gruppenmitgliedschaften dem Risiko des Abfangens aus und erhöht die Gefahr von Credential-Diebstahl.

RADIUS-Authentifizierung

RADIUS wird häufig für VPN-Zugriff und zentrale Authentifizierungsdienste eingesetzt.

Es unterstützt Challenge-Response-Methoden, zentrales Logging und standardisierte Durchsetzung von Authentifizierungsrichtlinien.

Sicherheitsrisiken entstehen, wenn Shared Secrets schwach sind oder über mehrere Systeme hinweg wiederverwendet werden.

Zudem kann der Zugriff beeinträchtigt werden, wenn RADIUS-Server nicht verfügbar sind, sofern keine geeigneten Fallback-Mechanismen konfiguriert wurden.

TACACS+-Authentifizierung

TACACS+ wird typischerweise für administrative Authentifizierung eingesetzt, insbesondere in Enterprise-Umgebungen.

Es trennt Authentication, Authorization und Accounting (AAA) und ermöglicht nachvollziehbare Administratoraktivitäten sowie granulare Privilegiensteuerung.

Obwohl das Design sicher ist, erfordert TACACS+ eine korrekte Konfiguration verschlüsselter Kanäle und eindeutige Schlüssel.

Zentrale TACACS+-Ausfälle können den administrativen Zugriff blockieren, sofern keine Redundanz vorhanden ist.

Eine korrekte Konfiguration und Absicherung externer Authentifizierungssysteme verbessert Nachvollziehbarkeit, reduziert Management-Komplexität und erhöht die Zugriffssicherheit. Regelmäßige Reviews von Verfügbarkeit,

Verschlüsselungseinstellungen, Zuordnung von Authentifizierungsrichtlinien und Fallback-Verhalten stellen zuverlässige und sichere Authentifizierungsprozesse sicher.

LDAP

Server	Enabled	TLS	UserName
udsserver.uds.local	on	on	UDSReadDir

Radius

Server	Enabled	VPN
10.10.33.11	off	off(!)

Tacacs

Server	Enabled	VPN
1.2.3.4	off	off(!)

Übersicht Administrativer Benutzer

Erläuterung

Administrative User

Dieser Bericht listet alle Benutzer auf, die über administrative Berechtigungen verfügen. Konten mit administrativen Rechten haben erweiterten Zugriff auf Konfigurationseinstellungen, Richtlinienänderungen, sensible Informationen sowie Systemverwaltungsfunktionen.

Die Überprüfung dieser Benutzer stellt sicher, dass nur autorisiertes Personal privilegierten Zugriff behält, und unterstützt Compliance, Nachvollziehbarkeit sowie sichere Zugriffskontrollpraktiken.

Users with Full Admin Rights

UDSAdmin

mschmitz

Webadmin

LocalAdmin

Uwe

apiuser

UDS-SNWL-Admins@uds.local

Users with Limited Admin Rights

- no entries -

Users with Read-Only Admin Rights

Udo

Users with Guest Admin Rights

Robert

Sylvia

Zusätzliche Informationen

Hinweis zu LDAP-Gruppenzuweisungen

Wenn administrative Rechte LDAP-Gruppen zugewiesen werden, erben alle Mitglieder dieser Gruppen automatisch Administratorprivilegien. Das bedeutet, dass Änderungen an LDAP-Mitgliedschaften – z. B. das Hinzufügen neuer Benutzer oder das Synchronisieren externer Verzeichnisstrukturen – unbeabsichtigt erhöhten Zugriff gewähren können.

Eine regelmäßige Überprüfung der Gruppenzuweisungen und Mitgliedschaften ist essenziell, um sicherzustellen, dass nur autorisierte Personen Administratorrechte erhalten und die Zugriffskontrolle mit den organisatorischen Sicherheitsrichtlinien übereinstimmt.

Konfigurationsempfehlungen für VPN-Sicherheit

Erläuterung

VPN Sicherheit

Virtuelle Private Netzwerke (VPNs) sind essenziell, um Daten über nicht vertrauenswürdige Netzwerke zu schützen. Damit sie wirksam bleiben, müssen ihre kryptografischen Einstellungen regelmäßig überprüft und aktualisiert werden. Veraltete Verfahren schwächen die Sicherheit, reduzieren die Compliance und setzen Organisationen unnötigen Risiken aus.

Warum regelmäßige Prüfungen wichtig sind:

- Sicherheit:

Cyberbedrohungen entwickeln sich schnell weiter. Alte Verschlüsselungs- oder Authentifizierungsverfahren können mit moderner Rechenleistung kompromittiert werden.

- Compliance:

Viele Branchen verlangen starke Verschlüsselung, um regulatorische Vorgaben zu erfüllen.

- Zugriffskontrolle:

Starke Authentifizierung verhindert die unautorisierte Nutzung des VPN.

- Datenschutz:

Aktualisierte Verschlüsselung stellt Vertraulichkeit und Integrität sensibler Informationen sicher.

- Performance & Zukunftssicherheit:

Neuere Standards erhöhen nicht nur die Sicherheit, sondern auch Effizienz und Skalierbarkeit.

Unsichere Elemente, die zu vermeiden sind:

- Symmetrische Verfahren:

DES und 3DES sind veraltet und verwundbar.

- Diffie-Hellman-(DH)-Gruppen:

Gruppen 1 (768 Bit), 2 (1024 Bit) und 5 (1536 Bit) sind zu schwach.

- IKE-Versionen:

IKEv1 ist veraltet; IKEv2 wird empfohlen.

- Hash-Funktionen:

MD5 und SHA-1 gelten als kompromittiert und nicht mehr sicher.

- Key Management:

Schwache oder statische Pre-Shared Keys (PSKs) lassen sich leicht erraten oder per Brute Force ermitteln.

Empfohlene sichere Optionen

- Verschlüsselung:

- AES-128 oder AES-256.

- Schlüsselaustausch:

- DH-Gruppen $\geq$ 2048 Bit oder Elliptic Curve Diffie-Hellman (P-256/P-384).

- Protokoll:

- IKEv2 für moderne VPN-Setups.

- Integrität:

- SHA-256 oder stärker.

- Authentifizierung:

Zertifikate bevorzugen; bei PSKs starke, zufällige Schlüssel verwenden.

Fazit

VPNs sind nur so stark wie ihre kryptografischen Grundlagen. Durch das Vermeiden schwacher Algorithmen und die Nutzung moderner Standards schützen Sie sensible Daten, erfüllen Compliance-Anforderungen und bereiten Ihr Netzwerk auf zukünftige Herausforderungen vor. Prüfen und aktualisieren Sie Ihre VPN-Konfiguration regelmäßig, um dauerhaft sicher zu bleiben.

Erläuterung

(!) = unsicher

(C) = akzeptabel, aber kann verbessert werden

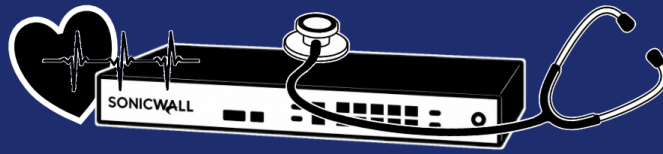
Konfigurationsempfehlungen für VPN-Sicherheit

Ena	Name	Phase1 Exchange Mode	Phase1 DH-Group	Phase 1 Encr	Phase1 Auth	Phase2 Protcl	Phase2 Encr	Phase2 Auth	Phase 2 PFS	Phase 2 DH-Group
yes	New York	Main (!)	224-Bit R ECP Group	AES-128 (C)	MD5 (!)	ESP	DES (!)	AES-XCBC (C)	off (!)	Group 2 (!)
yes	Remote Site1	IKEv2	Group 2 (!)	AESGCM16-256 (C)	SHA-1 (!)	ESP	AESGMAC-128	n/a	off (!)	Group 2 (!)
yes	To TZ570	IKEv2	Group 1 (!)	AES-256	SHA-1 (!)	ESP	AES-256	n/a	on	n/a

VPN – Verwendete unsichere kryptografische Algorithmen

Unsafe		
Category	Type	Comment
DH Group	192-Bit R ECP Group	Too small ECC group
Encryption	DES	Broken unsafe
IKE	Aggressive	Leads to info leaks insecure
Integrity	MD5	Broken collisions possible
Integrity	SHA-1	Deprecated collision attacks
Misc	None	No encryption integrity

Not recommended		
Category	Type	Comment
DH Group	224-Bit R ECP Group	Borderline ECC group aging out
Encryption	3DES	Legacy slow 112-bit effective strength
Encryption	AES-XCBC	Niche less common not widely supported
IKE	Main	Standard for IKEv1 secure but older
Protocol	AH	Rarely used integrity only no encryption



Health-Report

Erläuterung

Der Wartungsbericht unterstützt Administratoren dabei, Konfigurationselemente zu identifizieren, die regelmäßig überprüft werden sollten, um die Firewall-Konfiguration übersichtlich, effizient und wartbar zu halten. Im Laufe der Zeit wachsen Firewall-Konfigurationen durch neue Regeln, Objekte, VPN-Verbindungen und Sicherheitsdienste kontinuierlich an. Ohne regelmäßige Wartung sammeln sich häufig veraltete oder nicht mehr benötigte Einträge an, was die Administration erschwert und die Fehlersuche unnötig komplex macht.

Dieser Bericht hebt Konfigurationselemente hervor, die überprüft werden sollten, wie beispielsweise deaktivierte oder ungenutzte Firewall-Regeln, inaktive NAT-Richtlinien, nicht verwendete Adress- und Service-Objekte, abgelaufene Security Services sowie weitere Konfigurationseinträge, die möglicherweise nicht mehr benötigt werden. Darüber hinaus werden Einstellungen aufgeführt, die von einer Optimierung oder Bereinigung profitieren können.

Der Zweck dieses Berichts besteht nicht darin, alle aufgeführten Elemente automatisch zur Löschung zu empfehlen. Vielmehr bietet er Administratoren eine strukturierte Übersicht über Konfigurationseinträge, die vor einer möglichen Änderung geprüft werden sollten. Manche Objekte oder Regeln werden möglicherweise nur selten verwendet oder sind für zukünftige Projekte, Testumgebungen, Notfallkonzepte oder besondere Anwendungsfälle weiterhin erforderlich.

Eine regelmäßige Wartung der Firewall bietet zahlreiche Vorteile:

- Reduziert die Komplexität der Konfiguration und verbessert die Übersichtlichkeit.
- Erleichtert die Fehlersuche sowie Audits und Sicherheitsüberprüfungen.
- Hilft dabei, veraltete oder vergessene Konfigurationseinträge zu identifizieren.
- Verringert das Risiko von Konfigurationsfehlern.
- Verbessert die langfristige Wartbarkeit und Administrierbarkeit der Firewall.
- Unterstützt eine saubere, dokumentierte und professionell gepflegte Sicherheitsumgebung.

Eine regelmäßig gewartete Firewall ist einfacher zu administrieren, leichter zu auditieren und bildet eine zuverlässige Grundlage für zukünftige Konfigurationsänderungen sowie eine dauerhaft sichere Netzwerkumgebung.

Firewall-Auslastungsanalyse

Erläuterung

Firewall-Auslastungsanalyse

Diese Diagramme veranschaulichen den Auslastungsgrad der Firewall im Zeitraum vor dem Datenexport. Eine hohe Auslastung kann zu Leistungseinbußen führen, einschließlich verzögerter Traffic-Verarbeitung oder verworfener Pakete. Um aussagekräftige Erkenntnisse zu erhalten, sollte der als Datenquelle verwendete Technical Support Report idealerweise während einer Phase hoher Systemauslastung erstellt werden.

Empfohlene Datenquellen

Genauere Auslastungsstatistiken werden in der Regel über externe Monitoring-Systeme auf Basis von NetFlow oder SNMP gewonnen. Für NetFlow-basiertes Reporting stellt SonicWall eine dedizierte Lösung namens Analytics bereit, die sich nahtlos in SonicWall-Firewalls integriert.

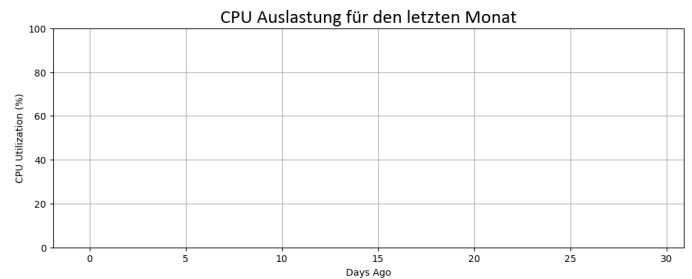
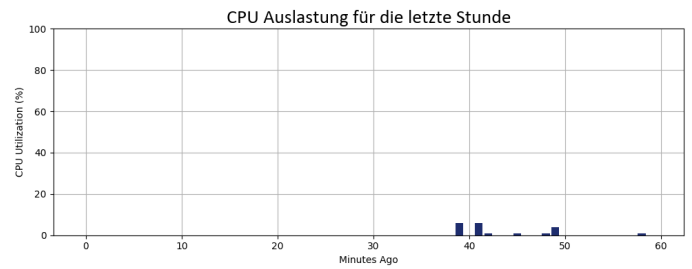
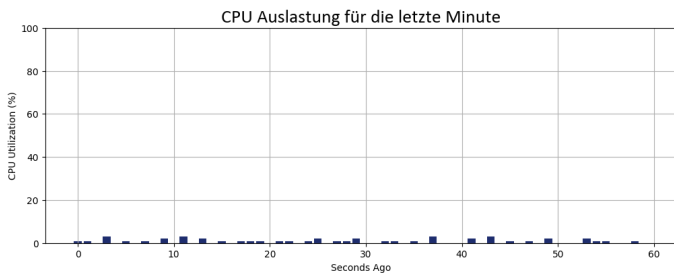
Wichtige Hinweise für HA-Umgebungen

Sollten für den ausgewählten Zeitraum keine Auslastungswerte verfügbar sein, ist zu prüfen, ob die Firewall in einem High-Availability-(HA)-Cluster betrieben wird. Wird die Standby-Einheit während des Berichtszeitraums aktiv, können Auslastungsdaten unter Umständen nicht auf dem erwarteten Gerät erfasst werden, was zu unvollständigen oder fehlenden Diagrammdaten führt.

Firewall-Auslastungsanalyse

Zeitraum	Durchschnitt	Status
Minute:	0 %	OK
Stunde:	0 %	OK
Tag:	0 %	OK
Monat:	0 %	OK

Performance-Auslastungsdiagramme



Firmware Version Check

Erläuterung

Firmware-Versionenvergleich

Dieser Abschnitt vergleicht die aktuell installierte Firmware-Version mit der neuesten verfügbaren Version auf MySonicWall. Dies hilft festzustellen, ob das Gerät aktuell ist, ein empfohlenes Upgrade benötigt oder eine veraltete Softwareversion ausführt, der Verbesserungen, Bugfixes oder Sicherheitsupdates fehlen könnten.

Firmware Version Check:

Firmware Installed on Firewall: 7.3.0-7012-R8150

Latest Firmware on MySonicWall: 7.3.3-7015

Firmware Release Date: 26.06.2026

Release Note URL:

https://software.sonicwall.com/Firmware/Documentation/232-006386-00_RevJ_SonicOS_7.3_ReleaseNotes.pdf

Zusätzliche Informationen

Firmware 7.3.3-7015 ist auf MySonicWall.com verfügbar. Es ist empfohlen, auf diese Version upzugraden

Übersicht Konfigurations- und Firmware-Historie

Erläuterung

Übersicht Konfigurations- und Firmware-Historie

Die folgende Tabelle bietet eine Übersicht über frühere Konfigurationsstände und Firmware-Versionen auf dem Gerät. Sie zeigt, wie häufig Einstellungen migriert wurden und ob nicht unterstützte Firmware-Downgrades erfolgt sind.

Nicht unterstützte Downgrades

Ein Firmware-Downgrade gilt als nicht unterstützt, wenn anschließend keine Konfiguration aus der heruntergestuften Firmware-Version importiert wurde. In solchen Fällen kann Systemkompatibilität nicht garantiert werden, und es können Betriebsprobleme auftreten.

Auswirkungen veralteter oder häufig migrierter Konfigurationen

Konfigurationsstände, die wiederholt migriert oder über mehrere Geräte hinweg genutzt wurden, können schrittweise Inkonsistenzen oder veraltete Parameter ansammeln. Dies kann zu unerwartetem Verhalten, reduzierter Performance oder Fehlern bei der Konfigurationsverarbeitung bei zukünftigen Migrationen oder Upgrades führen.

Firmware	TimeStamp	Action	Comment
7.0.1-5145-2363	24.01.2024 01:33:01	Settings import	
7.1.1-7040-5387	24.01.2024 08:25:53	Firmware applied	
7.1.1-7047-5557	01.03.2024 07:37:45	Firmware applied	
7.1.1-7047-5557	27.11.2024 18:21:03	Settings import	
7.1.1-7058-6162	03.12.2024 20:01:06	Firmware applied	
7.1.1-7058-6162	05.02.2025 21:58:08	Settings import	
7.1.1-7058-6162	21.03.2025 16:23:00	Settings import	
7.1.3-7015-6965	31.03.2025 21:24:27	Firmware applied	
7.3.0-7012-8150	08.09.2025 18:29:24	Firmware applied	
7.3.0-7012-8150	10.03.2026 14:38:34	Settings import	
7.3.0-7012-8150	10.03.2026 16:27:54	Settings import	
7.3.0-7012-8150	11.03.2026 02:01:27	Settings import	
7.3.0-7012-8150	11.03.2026 09:10:26	Settings import	
7.3.0-7012-8150	11.03.2026 11:03:15	Settings import	
7.3.0-7012-8150	21.05.2026 21:28:13	Settings import	

Zusätzliche Informationen

Kein nicht unterstütztes Firmware-Downgrade festgestellt

Übersicht Konfigurations- und Firmware-Historie

Erläuterung

Übersicht Konvertierung der Konfiguration

Dieser Bericht zeigt an, ob Konfigurationseinstellungen mit SonicWalls Conversion Tool konvertiert wurden. Dies hilft, migrierte Konfigurationen zu identifizieren und liefert Hinweise, ob Einstellungen aus früheren Plattformen oder älteren Deployments stammen.

Details

Settings wurden konvertiert: nein

Zuverlässigkeit – High Availability

Erläuterung

Bedeutung von High Availability auf Firewall-Systemen

1. Kontinuierliche Sicherheitsdurchsetzung

High Availability (HA) stellt den unterbrechungsfreien Betrieb von Firewall-Systemen sicher und hält Sicherheitskontrollen auch bei Hardwareproblemen, Updates oder geplanter Wartung aktiv. Dadurch entstehen keine Lücken in Threat Detection, Zugriffskontrolle und Policy-Enforcement.

2. Reduzierte Ausfallzeiten

In einer HA-Konfiguration übernimmt eine sekundäre Firewall automatisch, wenn die primäre Einheit ausfällt. Dieses nahtlose Failover minimiert Downtime und stellt den Zugriff auf kritische Anwendungen und Dienste sicher.

3. Verbesserte Systemzuverlässigkeit

Redundante Firewalls erhöhen die Resilienz gegen Hardwareausfälle, Konfigurationskorruption oder unerwartete Ausfälle erheblich. Die Zuverlässigkeit der Netzwerksicherheitsinfrastruktur steigt signifikant.

4. Unterstützung der Business Continuity

Organisationen, die auf Echtzeit-Konnektivität, Cloud-Zugriff und Online-Services angewiesen sind, können längere Ausfälle nicht tolerieren. HA schützt den Betrieb, indem Security-Enforcement während Ereignissen und Fehlerfällen aktiv bleibt.

5. Performance-Vorteile durch Lastverteilung

Einige HA-Umgebungen unterstützen Lastverteilung und erhöhen den Durchsatz durch Balance von Sessions oder Traffic-Pfaden über mehrere Appliances. Dadurch werden Processing-Bottlenecks reduziert und die Gesamtperformance verbessert.

6. Disaster-Recovery-Fähigkeit

HA ist ein wichtiger Bestandteil der Disaster-Recovery-Planung. Fällt ein Primärgerät aus, hält die sekundäre Einheit Policies, Routing, VPN-Tunnel und Security Services aktiv und reduziert so operative Auswirkungen.

7. Unterstützung von Regulatory Requirements und Compliance

Viele Branchen verlangen garantierte Verfügbarkeit von Sicherheitskontrollen und nachvollziehbare Failover-Mechanismen. HA unterstützt Compliance-Initiativen, Audit-Readiness und Service-Level-Verpflichtungen.

8. Verbesserte Nutzer- und Kundenerfahrung

Mit unterbrechungsfreiem Netzwerkzugang erleben Benutzer weniger Service-Unterbrechungen und eine schnellere Wiederherstellung nach Fehlern. Dies erhöht die Zufriedenheit und stabilisiert die Servicebereitstellung.

Zusammenfassung

High Availability auf Firewall-Systemen ist eine zentrale Grundlage für Business Resilience. Es stellt kontinuierlichen Schutz sicher, minimiert Downtime, unterstützt Disaster Recovery, verbessert Performance und ermöglicht Compliance. Durch reduzierte Serviceunterbrechungen und sichere Konnektivität steigert HA die operative und sicherheitsrelevante Wirksamkeit deutlich.

Zuverlässigkeit – High Availability

High Availability Settings

High Availability:	Enabled
HA Primary Serial-Number:	0040103CD830
HA Secondary Serial-Number:	0040103F5B1C
HA Stateful Sync:	Enabled
HA Preempt Mode:	Disabled
HA Control Interface:	X4
HA Data Interface:	X4
HA Role:	Primary
HA Firmware mismatch with peer:	No
HA Active Time:	0 Days 00:21:47

High Availability Status

HA Firewall Status:	Active
HA Peer State:	Peer not found / not active
HA Peer in sync:	No

Produkt-Lifecycle-Informationen

Erläuterung

Informationen zum Produkt-Lifecycle

Dieser Abschnitt bietet Einblick in den aktuellen Produkt-Lifecycle-Status. Er hilft zu bestimmen, ob ein Gerät vollständig unterstützt wird, sich dem Support-Ende nähert oder bereits außerhalb der offiziellen Wartungsperiode liegt. Für detaillierte Lifecycle-Beschreibungen, wichtige Meilensteine und aktuelle Support-Zeitpläne nutzen Sie bitte die offizielle SonicWall-Produkt-Lifecycle-Dokumentation, die über SonicWall-Supportressourcen verfügbar ist.

Description	Value
Model:	SonicWall NSA NSV 270
Last Order Date:	15.04.2022
ARM Begin:	16.04.2022
LRM Begin:	16.04.2024
1 Year LOD:	15.04.2025
End of Support:	16.04.2026

Zusätzliche Informationen

Bitte gleichen Sie diese Informationen bitte mit der offiziellen SonicWall Webseite ab.

Security Services – Lizenzstatus-Übersicht

Erläuterung

Security Services Lizenzen

Dieser Bericht zeigt, welche Services aktuell über eine aktive Lizenz verfügen. Lizenzierte Services sind voll funktionsfähig und können den vorgesehenen Schutz bzw. Funktionsumfang bereitstellen. Services ohne gültige Lizenz können in ihrer Funktion eingeschränkt oder vollständig inaktiv sein.

Diese Ansicht hilft zu verifizieren, ob erforderliche sicherheits- und abonnementsbasierte Funktionen betriebsbereit bleiben, und unterstützt die Planung von Verlängerungen zur Vermeidung von Serviceunterbrechungen.

Security Services – Lizenzstatus-Übersicht

Service Bezeichnung	Lizenzstatus	Anzahl	Ablaufdatum
Node Upgrade	None		Unlimited
Active/Active Clustering Service	None		Unlimited
NSM Essential (Retired)	Not Licensed		Unlimited
NSM Advanced (Retired)	Disabled		05.02.2026
Capture Client Basic	Not Licensed		Unlimited
Content Filtering Client	None		Unlimited
Capture Client Advanced	Not Licensed		Unlimited
Capture Client Premier	Not Licensed		Unlimited
Deep Packet Inspection for SSL (DPI-SSL)	Licensed		Unlimited
Deep Packet Inspection for SSH (DPI-SSH)	None		Unlimited
Virtual Assist	None		Unlimited
SSL VPN	Licensed	2 Max: 100	Unlimited
Global VPN Client	Licensed	50 Max: 1000	Unlimited
Global VPN Client Enterprise	None		Unlimited
WAN Acceleration Client	None		Unlimited
WAN Acceleration Software	None		Unlimited
Botnet Block	None		Unlimited
Stateful High Availability	Licensed		Unlimited
Comprehensive Anti-Spam Service	None		Unlimited
External IDS Support	None		Unlimited
CSC Analytics (includes Reporting)	None		Unlimited
CSC Management	None		Unlimited
CSC Management Lite	None		Unlimited
CSC Management and Reporting	None		Unlimited
CSC Management and 7-day Reporting	None		Unlimited
Syslog Analytics	Expired		03.02.2024
Comprehensive/Advanced Gateway Security Suite	None		Unlimited
Gateway AV	None		Unlimited
Anti-Spyware	None		Unlimited
Intrusion Prevention	None		Unlimited
App Control	None		Unlimited
App Visualization	None		Unlimited
Content Filtering: Premium Edition	None		Unlimited
Analyzer	None		Unlimited
Capture Advanced Threat Protection	Licensed		14.02.2027
Standard Support	Not Licensed		Unlimited
24x7 Support	Licensed		14.02.2027
SonicOS Expanded	None		Unlimited
Software and Firmware Updates	None		Unlimited
Hardware Warranty	None		Unlimited
Remote Implementation Service	None		Unlimited
Gateway Anti-malware/Intrusion Prevention/App Control	Licensed		14.02.2027
Content Filtering Service	Licensed		14.02.2027
Secure Connect Lite	None		Unlimited
Secure Connect	None		Unlimited
Advanced Reporting & Analytics (7 days)	Licensed		14.02.2027
DNS Filtering	Licensed		14.02.2027

Security Services – Lizenzstatus-Übersicht

Service Bezeichnung	Lizenzstatus	Anzahl	Ablaufdatum
Advanced Protection Security Suite	Licensed		14.02.2027
Managed Protection Security Suite	Not Licensed		Unlimited
Web and Chat Only Support	None		Unlimited
Basic Reporting (7 days)	Not Licensed		Unlimited
Essential Protection Service Suite	Disabled		05.02.2026
Advanced Reporting & Analytics	None		Unlimited
Threat Protection Service Suite	None		Unlimited
Model Upgrade	Not Licensed		Unlimited
GeoIP Filtering	None		Unlimited

Zuverlässigkeit – WAN-Failover

Erläuterung

Bedeutung von WAN-Failover auf Firewall-Systemen

1. Ununterbrochene Internet-Konnektivität

WAN-Failover stellt eine kontinuierliche Internetverbindung sicher, indem automatisch auf eine Backup-Verbindung umgeschaltet wird, wenn der primäre WAN-Link ausfällt. Dies ist entscheidend für den Betrieb von Geschäftsprozessen, die von Internet-Konnektivität abhängig sind.

2. Erhöhte Zuverlässigkeit und Verfügbarkeit

Durch eine sekundäre Verbindung verbessert WAN-Failover die Zuverlässigkeit und Verfügbarkeit von Netzwerkdiensten. Dies reduziert Ausfallzeiten und steigert die Produktivität.

3. Business Continuity

Netzwerkausfälle können zu finanziellen Verlusten, geringerer Kundenzufriedenheit und operativen Verzögerungen führen. WAN-Failover unterstützt die Geschäftsfortführung, indem Unterbrechungen minimiert und der Zugriff auf kritische Anwendungen und Dienste aufrechterhalten wird.

4. Load Balancing und verbesserte Performance

Einige Firewall-Plattformen unterstützen sowohl Failover als auch Load Balancing. Dadurch kann Traffic über mehrere WAN-Links verteilt werden, was Bandbreite optimiert und die Performance für Endbenutzer verbessert.

5. Unterstützung für Disaster Recovery

Bei unerwarteten Ausfällen oder Infrastrukturproblemen stellt Failover sicher, dass Recovery-Prozesse zugänglich bleiben und nicht unterbrochen werden, wodurch Service-Verfügbarkeit und Datenintegrität erhalten bleiben.

6. Konsistente Sicherheitsdurchsetzung

Failover-fähige Firewalls stellen sicher, dass sämtlicher Traffic – im Normalbetrieb und während Failover-Ereignissen – weiterhin die Sicherheitsinspektionen durchläuft. Dadurch werden Schutzmechanismen nicht durch Ausfälle umgangen.

7. Kosteneffizienz

Auch wenn sekundäre WAN-Leitungen Kosten verursachen, hilft das Vermeiden von Service-Unterbrechungen, finanzielle Verluste, Produktivitätsrückgänge und Einbußen bei der Kundenzufriedenheit zu verhindern, was langfristig zu Einsparungen führt.

Zusammenfassung

WAN-Failover ist eine zentrale Fähigkeit von Firewall-Systemen. Es stellt kontinuierliche Internet-Konnektivität sicher, unterstützt Disaster Recovery, verbessert Zuverlässigkeit, stärkt die Konsistenz der Sicherheitskontrollen und schützt die Business Continuity. Durch reduzierte Ausfallzeiten und verbesserte Performance hilft WAN-Failover Organisationen, Servicequalität und operative Effizienz aufrechtzuerhalten.

Zuverlässigkeit – WAN-Failover

WAN Interface Summary

Number of WAN Interfaces configured & enabled: 2

Interface	Type	Comment	PacketsIn	PacketsOut
X1	WAN	Default WAN	9268	9071
X5	WAN		1215	328

WAN Load Balancing is: enabled

Interface	Probing	Type	Prim Dest	Protocol	Alt Dest	Protocol
X1	Logical	At least one target should reply	204.212.170.23	TCP	8.8.8.8	ICMP
X5	Physical	None	None	None	None	None



Konfigurationsreport

Erläuterung

Konfiguration Report
überprüft die technische Konfiguration und die Betriebsbereitschaft der Firewall-Umgebung. Dabei werden Systemfunktionen wie High Availability (HA), WAN-Failover sowie der Status der Sicherheitsdienste bewertet. Zusätzlich wird geprüft, ob zentrale Komponenten korrekt konfiguriert sind und den empfohlenen Einsatz- und Implementierungsstandards entsprechen.

TCP Connection Timeout

Erläuterung

Der TCP Connection Timeout bestimmt, wie lange die Firewall eine inaktive TCP-Sitzung in ihrer Verbindungstabelle hält, bevor sie entfernt wird. Der globale Standardwert von 15 Minuten ist für die meisten Umgebungen eine sinnvolle Einstellung und bietet eine gute Balance zwischen der Unterstützung von legitimem Netzwerkverkehr und der Schonung von Firewall-Ressourcen.

Eine Änderung des globalen TCP-Timeouts wirkt sich auf jede TCP-Verbindung aus, die die Firewall passiert. Wird dieser Wert unnötig erhöht, können veraltete Sitzungen über längere Zeit im Speicher verbleiben, Einträge in der Verbindungstabelle belegen und möglicherweise die Gesamtkapazität des Geräts verringern. In großen oder stark ausgelasteten Umgebungen kann dies spürbare Auswirkungen auf die Firewall-Leistung und die Ressourcennutzung haben.

Manche Anwendungen benötigen jedoch längere Leerlaufzeiten, um dauerhafte Verbindungen aufrechtzuerhalten. Beispiele hierfür sind bestimmte Datenbankanwendungen, ältere Client-/Server-Software oder spezialisierte industrielle Steuerungssysteme. In solchen Fällen empfiehlt es sich, den globalen Timeout auf dem Standardwert zu belassen und stattdessen einen benutzerdefinierten TCP-Timeout nur für die betreffenden Zugriffsregeln zu konfigurieren.

Die Anwendung erweiterter Timeouts auf Regelebene bietet mehrere Vorteile:

- Minimiert die Auswirkungen auf die gesamte Firewall.
- Begrenzt den erhöhten Ressourcenverbrauch auf die betroffenen Anwendungen.
- Reduziert die Anzahl veralteter Sitzungen in der Verbindungstabelle.
- Macht besondere Anwendungsanforderungen sichtbar und leichter dokumentierbar.
- Vereinfacht künftige Audits und die Fehlersuche.

Dieser Bericht zeigt die aktuelle globale TCP-Timeout-Einstellung und listet alle Zugriffsregeln auf, die einen benutzerdefinierten TCP-Timeout-Wert verwenden. Regeln mit von der Standardeinstellung abweichenden Werten sollten regelmäßig überprüft werden, um sicherzustellen, dass die Ausnahme weiterhin erforderlich und angemessen dokumentiert ist.

Als allgemeine Empfehlung sollte der globale TCP-Timeout möglichst auf dem Standardwert belassen werden, während anwendungsspezifische Anforderungen durch regelbasierte Timeout-Überschreibungen abgedeckt werden sollten.

General TCP Setting

Globaler TCP Connection Timeout: 69

Zusatzinformation

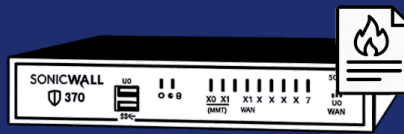
Der Standard-TCP Connection Timeout wurde geändert. Es wird empfohlen, die allgemeine Einstellung bei 15 Minuten zu belassen. Falls ein bestimmter Dienst abweichende Werte benötigt, ändern Sie den TCP-Timeout für die betreffende Regel

Regeln, bei denen der Standard-TCP-Timeout geändert wurde

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	TCP Timeout
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	66
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	10
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	30

Anzahl der Datensätze: 3



Firewall Dokumentationsreport

Erläuterung

Dokumentation Report

bietet einen strukturierten Überblick über die Firewall-Umgebung und deren zentrale Konfigurationselemente. Er sammelt und stellt relevante Systeminformationen dar, einschließlich Netzwerkeinstellungen, Interface-Zuordnungen, Zonenkonfigurationen und angewendeten Richtlinien.

Der Bericht dient als umfassende Referenz für Administratoren und unterstützt sowohl den operativen Betrieb als auch den Wissenstransfer. Er stellt sicher, dass wichtige Konfigurationsdetails klar dokumentiert und jederzeit leicht zugänglich sind, wodurch die Abhängigkeit von manuellen Systemprüfungen reduziert wird.

Darüber hinaus trägt die Dokumentation zur Transparenz und Konsistenz der Umgebung bei und erleichtert Fehleranalysen, Audits sowie zukünftige Änderungen.

Alle Audit-Einträge

Erläuterung

Internes Firewall Audit

Interne Auditierung auf Firewalls ist ein wesentlicher Bestandteil zur Sicherstellung operativer Integrität, Nachvollziehbarkeit und Sicherheit in einer Netzwerkumgebung. Die Firewall stellt einen der kritischsten Kontrollpunkte in einer Organisation dar, und Auditierung schafft Transparenz über Konfigurationsänderungen, Zugriffsereignisse und administrative Aktionen, die die Security-Posture direkt beeinflussen.

Verantwortlichkeit und Nachvollziehbarkeit

Audit-Logs dokumentieren, wer Änderungen vorgenommen hat, wann sie erfolgt sind und was verändert wurde. Diese Traceability stellt sicher, dass Zuständigkeiten klar zugeordnet sind und Fehlkonfigurationen, Abweichungen von Standards oder unautorisierte Änderungen schnell identifiziert und korrigiert werden können.

Erkennung unautorisierter oder riskanter Änderungen

Firewalls beeinflussen Zugriffskontrolle, Datenschutz und Traffic-Flows unmittelbar. Interne Auditierung ermöglicht es Administratoren, absichtliche oder versehentliche Konfigurationsänderungen zu erkennen und Sicherheitsvorfälle, Policy-Verstöße oder potenziellen Missbrauch administrativer Privilegien zu identifizieren.

Unterstützung für Compliance und Governance

Viele regulatorische Frameworks verlangen Auditierung kritischer Systeme wie Firewalls. Interne Audit-Einträge unterstützen die Einhaltung von Standards, die z. B. in Finanz-, Gesundheits- oder Behördenumgebungen relevant sind. Sie liefern Nachweise, dass Richtlinien befolgt werden und Schutzmechanismen korrekt durchgesetzt sind.

Operative Einblicke und kontinuierliche Verbesserung

Audit-Logs helfen Security-Teams, Konfigurationshistorie und operative Trends zu verstehen. Eine regelmäßige Review dieser Einträge ermöglicht es Organisationen, Zugriffspolicies zu verfeinern, wiederkehrende Probleme zu identifizieren und Change-Management-Praktiken zu stärken.

Incident-Untersuchung und Forensik

Bei einem Security Event sind interne Audit-Daten häufig eine der wertvollsten Evidenzquellen. Sie ermöglichen, Aktionen auf der Firewall zu rekonstruieren, Root Causes zu analysieren und zu bestimmen, ob bösartige Aktivität oder menschlicher Fehler zum Incident beigetragen haben.

Fazit

Interne Auditierung ist notwendig, um Transparenz, Konsistenz und Verantwortlichkeit im Firewall-Betrieb sicherzustellen. Sie erhöht die Sicherheit, unterstützt regulatorische Anforderungen, ermöglicht schnelleres Troubleshooting und liefert eine zentrale Grundlage für resilientes Netzwerkmanagement.

Zusatzinformation

Übersicht Audit-Events

Dieser Abschnitt listet alle Audit-Events auf, die aus dem Technical Support Report (TSR) extrahiert wurden. Er bietet Transparenz über Konfigurationsänderungen auf der Firewall und identifiziert die Benutzer, die diese Aktionen durchgeführt haben.

Wichtiger Hinweis

Audit-Logs werden in High-Availability-(HA)-Umgebungen nicht zwischen Appliances synchronisiert. Änderungen, die während Failover-Phasen auf der sekundären (aktiven) Einheit durchgeführt werden, erscheinen daher möglicherweise nicht im Audit-Trail der primären Appliance. Zukünftige Versionen von FirewallToolbox könnten dieses Thema adressieren.

Dieser Bericht hilft, administrative Aktivitäten zu validieren, unterstützt Nachvollziehbarkeit und hilft bei der Identifikation unerwünschter oder unautorisierter Konfigurationsänderungen.

Zusatzinformation

Dieser Bericht zeigt nur die 10 neuesten Einträge. Führen Sie den Einzelbericht aus, um alle Ergebnisse anzuzeigen.

Firewall Internal Admin Audit Records

ID: 3749 Timestamp: 15.09.2026 16:33:49
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19526)

ID: 3749 Timestamp: 15.09.2026 16:33:49
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19526)

ID: 3748 Timestamp: 15.09.2026 16:33:49
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19525)

ID: 3748 Timestamp: 15.09.2026 16:33:49
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (19525)

ID: 3747 Timestamp: 15.09.2026 16:31:36
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46610)

ID: 3747 Timestamp: 15.09.2026 16:31:36
Description: Export Tech Support Report
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46610)

ID: 3746 Timestamp: 15.09.2026 16:31:36
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46608)

ID: 3746 Timestamp: 15.09.2026 16:31:36
Description: Export Configuration
Old:
New:
Status:
User: UDSAdmin
Session: API
Source: 10.10.10.10 (46608)

Firewall Internal Admin Audit Records

ID: 3745 Timestamp: 15.09.2026 16:18:33
Description: End Configuration Mode
Old:
New:
Status:
User: UDAdmin
Session: GMS
Source: 127.0.0.1 (50325)

ID: 3745 Timestamp: 15.09.2026 16:18:33
Description: End Configuration Mode
Old:
New:
Status:
User: UDAdmin
Session: GMS
Source: 127.0.0.1 (50325)

Alle Regeln (IPv4)

Erläuterung

Dieser Bericht enthält eine vollständige Übersicht aller konfigurierten IPv4-Zugriffsregeln der Firewall, mit Ausnahme der standardmäßig integrierten Systemregeln. Für jede Regel werden der Aktivierungsstatus, die Aktion (Erlauben/Verweigern), der Regelname, Quell- und Zielzonen, Quell- und Zielobjekte, verwendete Dienste, Administrator-Kommentare sowie die eindeutige Regel-UUID aufgeführt.

Eine regelmäßige Überprüfung der Firewall-Regeln ist ein wesentlicher Bestandteil eines sicheren Firewall-Betriebs. Sie ermöglicht es, die implementierte Sicherheitsrichtlinie nachzuvollziehen, die Einhaltung des Least-Privilege-Prinzips zu überprüfen sowie veraltete, redundante oder unnötig weit gefasste Regeln zu identifizieren. Darüber hinaus erleichtert eine vollständige Regelübersicht die Dokumentation, vereinfacht die Fehlersuche und unterstützt Administratoren dabei, die Firewall-Konfiguration übersichtlich, wartbar und sicher zu halten.

Alle Regeln (IPv4)

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc
YES	A	My Rule	DMZ-sec	DMZ-unsec	any	any	any	FTP Data
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS
YES	A	Test 20	DMZ-sec	DMZ-unsec	any	any	any	Kazaa / FastTrack
YES	A	Test 21	DMZ-sec	DMZ-unsec	any	any	any	Lotus Notes
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE
YES	A	Test 18	DMZ-sec	DMZ-unsec	any	any	any	ICMP
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any
YES	A	Test 22	DMZ-unsec	DMZ-sec	any	any	any	MSN
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management
YES	A	Test 24	WAN	060466	any	any	any	OSPF
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)
YES	A	Test 23	WAN	060466	any	any	any	MSN
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH Temp, Rule to allow M...
YES	A	Allow Citrix	any		any	any	Citrix UDP	any Example any<> any
YES	A	Allow FTP	any		any	any	FTP	any

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Anzahl der Datensätze: 21

Management-Regeln (IPv4)

Erläuterung

Firewall-Regeln mit Managementzugriff auf SonicWall-Firewalls

SonicWall-Firewalls stellen Management-Services wie z.B. SSH und HTTPS bereit, um Administratoren die Konfiguration, Überwachung und Wartung des Geräts zu ermöglichen. Diese Services gewähren privilegierten Zugriff auf die Firewall und ihre sicherheitsrelevanten Funktionen. Firewall-Regeln, die Managementzugriff erlauben, müssen daher mit besonderer Sorgfalt behandelt werden, da eine unsachgemäße Exponierung erhebliche Sicherheits- und Betriebsrisiken verursachen kann.

Sicherheitsrisiken

Das Zulassen von Managementzugriff über Firewall-Regeln vergrößert die Angriffsfläche der SonicWall-Appliance. Management-Schnittstellen sind ein häufiges Ziel von Angreifern, da erfolgreicher Zugriff unmittelbare administrative Kontrolle ermöglicht. Exponierte SSH- oder HTTPS-Dienste können Brute-Force-Anmeldeversuchen, Credential-Stuffing-Angriffen oder der Ausnutzung von Schwachstellen in der SonicWall-Management-Ebene oder der zugrunde liegenden Firmware ausgesetzt sein.

Gelangt ein Angreifer in den Besitz administrativer Rechte, kann er Firewall-Regeln verändern, Security Services deaktivieren, VPN-Konfigurationen manipulieren oder persistente Hintertüren einrichten. Dies kann zu Traffic-Manipulation, Verlust der Netzwerk-Integrität oder zur vollständigen Kompromittierung der geschützten Umgebung führen.

Exponierung gegenüber netzwerkbasierten Angriffen

Sind SonicWall-Management-Services aus nicht vertrauenswürdigen Netzwerken (z. B. WAN oder breit definierte Zonen) erreichbar, werden sie für automatisierte Scans, Reconnaissance-Aktivitäten und Denial-of-Service-Angriffe sichtbar. Auch bei Verwendung verschlüsselter Protokolle wie HTTPS oder SSH bestehen Risiken, wenn die Firmware nicht aktuell ist, schwache kryptografische Einstellungen verwendet werden oder der Zugriff nicht ausreichend eingeschränkt ist.

Darüber hinaus können fehlerhaft konfigurierte Management-Regeln dazu führen, dass administrative Ports unbeabsichtigt auf mehreren Interfaces oder Zonen freigegeben werden, was das Risiko unbeabsichtigten oder unautorisierten Zugriffs weiter erhöht.

Operative und Compliance-Auswirkungen

Zu weit gefasste Management-Zugriffsregeln erschweren das Monitoring und die Erkennung von Sicherheitsvorfällen auf SonicWall-Firewalls. Unautorisierte Zugriffsversuche lassen sich unter Umständen nur schwer von legitimer administrativer Nutzung unterscheiden, insbesondere wenn Logging und Alarmierung nicht konsequent konfiguriert sind. Aus Compliance-Sicht verstoßen unzureichend eingeschränkte oder nicht dokumentierte Managementzugriffe häufig gegen interne Sicherheitsrichtlinien sowie regulatorische Vorgaben, die eine strikte Kontrolle privilegierter Zugriffe verlangen.

Empfohlene Best Practices für SonicWall-Firewalls

Managementzugriff auf SonicWall-Geräte sollte strikt auf vertrauenswürdige interne Netzwerke oder dedizierte Management-Zonen beschränkt werden. Direkter Managementzugriff über WAN-Interfaces sollte nach Möglichkeit vermieden werden. Ist Remote-Administration erforderlich, sollte diese ausschließlich über sichere VPN-Verbindungen mit starker Authentifizierung und Verschlüsselung erfolgen.

Weitere empfohlene Maßnahmen sind die Einschränkung des Zugriffs auf definierte Quell-IP-Adressen, die Aktivierung von Multi-Faktor-Authentifizierung für administrative Benutzer, das regelmäßige Einspielen von Firmware-Updates sowie die kontinuierliche Überprüfung von Management-Zugriffsregeln und Audit-Logs. Diese Maßnahmen stellen sicher, dass administrativer Zugriff kontrolliert, nachvollziehbar und im Einklang mit SonicWall-Best-Practices erfolgt.

Management-Regeln (IPv4)

Erläuterung

Management-Service-Objekte und -Gruppen

Die unten aufgeführten Einträge stellen Service Objects und Gruppen dar, die als Management-Services klassifiziert sind. Dazu zählen typischerweise Protokolle und Ports für administrativen Zugriff, Gerätekonfiguration und Monitoring-Funktionen. Die Identifikation dieser Services hilft zu bestimmen, wo Managementzugriff erlaubt ist, und stellt sicher, dass administrative Schnittstellen nur in vertrauenswürdigen und kontrollierten Netzwerkbereichen zugänglich sind.

Service Objects

Citrix TCP

Citrix TCP (Session Reliability)

Citrix UDP

GMS HTTPS

HTTP

HTTP Management

HTTPS

HTTPS Management

IKE (Key Exchange)

IKE (Traversal)

Kerberos TCP

Ping

SSH

SSH Management

Syslog

Service-Groups

Citrix

Idle HF

Management Services

IKE

Kerberos

Interface Management Services

Management-Regeln (IPv4)

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH

Temp, Rule to allow M...

Anzahl der Datensätze: 4

Interfaces (IPv4)

Erläuterung

Übersicht Interface-Konfiguration

Dieser Bericht zeigt alle konfigurierten Interfaces einschließlich ihrer zugewiesenen Einstellungen. Er bietet Transparenz über Interface-Rollen, Adressierungsinformationen und Betriebsparameter und unterstützt die Bewertung von Konnektivität, Segmentierung und Netzwerkstruktur.

Interfaces (IPv4)

Name	Zone	Comment	Assignment	IP	Subnet Mask	Gateway
X0	LAN	Default LAN	Static LAN	10.100.10.254	255.255.255.0	0.0.0.0
X1	WAN	Default WAN	Static	10.10.15.1	255.255.255.0	10.10.15.254
X2	DMZ-unsec		Static LAN	10.100.30.254	255.255.255.0	0.0.0.0
X3	DMZ-sec		Static LAN	10.100.40.254	255.255.255.0	0.0.0.0
X4	HA Data & Control		n/a	n/a	n/a	n/a
X5	WAN		Static	10.10.16.1	255.255.255.0	172.16.1.254
X6	LAN		Static LAN	192.168.1.254	255.255.255.0	0.0.0.0
X6:V100	LAN		Static LAN	192.168.2.254	255.255.255.0	0.0.0.0
X7	DMZ-sec		Static LAN	192.169.1.1	255.255.255.0	0.0.0.0

Anzahl der Datensätze: 9

Übersicht Benutzer- und Gruppenmitgliedschaften

Erläuterung

Benutzer und Gruppenmitgliedschaften

Dieser Bericht enthält eine detaillierte Liste aller Benutzer einschließlich ihrer zugeordneten Gruppenmitgliedschaften. Auf Basis dieser Zugehörigkeiten werden die effektiven Zugriffsrechte hervorgehoben, die Benutzer über zugewiesene Gruppen erben.

Dies hilft zu identifizieren, wer Zugriff auf VPN-Ressourcen hat, korrekte Berechtigungen zu verifizieren und potenziell überprivilegierte Konten aufgrund gruppenbasierter Berechtigungen zu erkennen.

Übersicht Benutzer- und Gruppenmitgliedschaften

All LDAP Users

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:SSLVPN Services
- ist Mitglied der Gruppe:LAN Access66
- Gewährt Zugriffsrechte auf: WAN Primary IP
- Gewährt Zugriffsrechte auf: LAN Primary Subnet
- Gewährt Zugriffsrechte auf: WAN-GoogleDNS-8.8.8.8

Isabel

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:Content Filtering Bypass
- ist Mitglied der Gruppe:Limited Administrators

LocalAdmin

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:SonicWALL Administrators

Robert

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:Guest Administrators

Sylvia

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:Guest Administrators

UDS-SNWL-Admins@uds.local

- ist Mitglied der Gruppe:SonicWALL Administrators

Udo

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:SonicWALL Read-Only Admins

Uwe

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:SonicWALL Administrators
- ist Mitglied der Gruppe:SSLVPN Services
- ist Mitglied der Gruppe:LAN Access66
- Gewährt Zugriffsrechte auf: WAN Primary IP
- Gewährt Zugriffsrechte auf: LAN Primary Subnet
- Gewährt Zugriffsrechte auf: WAN-GoogleDNS-8.8.8.8

Webadmin

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:SonicWALL Administrators
- ist Mitglied der Gruppe:SSLVPN Services

apiuser

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:SonicWALL Administrators

mschmitz

- ist Mitglied der Gruppe:Trusted Users
- ist Mitglied der Gruppe:SonicWALL Administrators
- ist Mitglied der Gruppe:SSLVPN Services
- ist Mitglied der Gruppe:LAN Access66
- Gewährt Zugriffsrechte auf: WAN Primary IP
- Gewährt Zugriffsrechte auf: LAN Primary Subnet

Übersicht Benutzer- und Gruppenmitgliedschaften

mschmitz (fortgesetzt)

- Gewährt Zugriffsrechte auf: WAN-GoogleDNS-8.8.8.8

Wxterne Userdatenbanken

Zusätzliche Informationen

Wenn die Anzahl lokaler Benutzerkonten auf einer Firewall eine geringe Schwelle (in der Regel etwa 10 Benutzer) überschreitet, wird die direkte Verwaltung von Identitäten auf der Firewall ineffizient, fehleranfällig und schlecht skalierbar. In solchen Umgebungen wird die Anbindung an ein externes Benutzerverzeichnis wie LDAP, RADIUS oder TACACS+ dringend empfohlen.

1. Zentrale Benutzerverwaltung

Externe Benutzerverzeichnisse bieten eine zentrale und verbindliche Quelle für Benutzeridentitäten.

- Benutzerkonten werden in einem zentralen System angelegt, geändert und gelöscht.
 - Änderungen wie Passwortanpassungen oder Kontodeaktivierungen gelten sofort für alle angebotenen Systeme.
 - Der administrative Aufwand wird im Vergleich zur Einzelverwaltung von Benutzern auf jeder Firewall erheblich reduziert.
- Dies gewinnt insbesondere mit wachsender Benutzeranzahl und häufigeren Personalwechseln an Bedeutung.

2. Erhöhte Sicherheit und reduziertes Risiko

Die Verwaltung einer steigenden Anzahl lokaler Firewall-Benutzer erhöht im Laufe der Zeit das Sicherheitsrisiko.

- Verwaiste Benutzerkonten können nach dem Ausscheiden von Mitarbeitern weiterhin aktiv bleiben.
 - Passwortvorgaben sind möglicherweise uneinheitlich oder nicht konsequent durchgesetzt.
 - Manuelle Benutzerverwaltung erhöht die Wahrscheinlichkeit von Konfigurationsfehlern.
- Externe Authentifizierungssysteme erzwingen einheitliche Sicherheitsrichtlinien, einschließlich Passwortkomplexität, Passwortwechsel, Sperrmechanismen und – sofern unterstützt – Mehrfaktor-Authentifizierung.

3. Bessere Skalierbarkeit und langfristige Wartbarkeit

Firewalls sind primär für die Paketprüfung und Richtliniendurchsetzung ausgelegt, nicht für das Management des Benutzerlebenszyklus.

- Die Verwaltung einer kleinen Anzahl lokaler Benutzer ist unter Umständen noch vertretbar.
- Ab etwa 10 Benutzern steigt der administrative Aufwand überproportional.
- Externe Verzeichnisse skalieren problemlos auf Dutzende, Hunderte oder Tausende Benutzer, ohne die Komplexität der Firewall zu erhöhen.

Die Firewall fungiert damit lediglich als Verbraucher von Identitätsdiensten und nicht als primärer Speicherort für Benutzerdaten.

4. Rollenbasierte Zugriffskontrolle (RBAC)

Externe Benutzerverzeichnisse ermöglichen die Vergabe von Zugriffsrechten über Gruppen statt über einzelne Benutzerkonten.

- Benutzer werden Gruppen wie VPN-Benutzer oder Firewall-Administratoren zugeordnet.
- Firewall-Regeln referenzieren diese Gruppen anstelle einzelner Benutzer.
- Zugriffsänderungen können umgesetzt werden, ohne die Firewall-Konfiguration anzupassen.

Diese Trennung von Identitätsverwaltung und Autorisierung erhöht die Übersichtlichkeit, Konsistenz und Betriebssicherheit.

5. Vereinfachte Auditierung und Compliance

Sicherheitsstandards und interne Richtlinien verlangen eine klare Nachvollziehbarkeit von Benutzerzugriffen.

Externe Authentifizierungssysteme bieten zentrale Anmeldeprotokolle, nachvollziehbare Login-Ereignisse und eine eindeutige Zuordnung von Aktionen zu einzelnen Benutzern. Dies erleichtert Audits erheblich und unterstützt die Einhaltung von Vorgaben wie ISO 27001, NIST oder internen Governance-Richtlinien.

6. Nahtlose Integration in bestehende IT-Infrastrukturen

Die meisten Organisationen betreiben bereits zentrale Identitäts- und Zugriffssysteme.

- LDAP oder Active Directory für Benutzeridentitäten
- RADIUS für VPN- und Netzwerkzugriffe
- TACACS+ für administrative Zugriffe

Durch die Integration der Firewall in diese Systeme werden doppelte Benutzerverwaltungen vermieden und Firewall-Zugriffe an bestehende IT-Prozesse angepasst.

7. Reduzierung operativer Fehler

Die manuelle Benutzerverwaltung auf Firewalls führt häufig zu betrieblichen Problemen.

- Vergessene Benutzerlöschungen
- Uneinheitliche Berechtigungen
- Konfigurationsdrift über die Zeit

Die Auslagerung der Authentifizierung an ein externes System führt zu schlankeren Firewall-Konfigurationen und reduziert das Risiko menschlicher Fehler deutlich.

Fazit

Lokale Benutzerkonten auf Firewalls sind für sehr kleine Umgebungen unter Umständen ausreichend, skalieren jedoch nicht nachhaltig. Sobald die Anzahl der Benutzer etwa 10 überschreitet, bietet der Einsatz eines externen Benutzerverzeichnisses klare Vorteile in Bezug auf Sicherheit, Skalierbarkeit, administrativen Aufwand und Auditierbarkeit.

Zonen Report

Erläuterung

Dieser Bericht zeigt Details zu Zonen

Zonen Report

Seite 1/1

Zone	Type	Member Interfaces	Trust	Active Security Services	SSLVPN	SSO
060466	1	None	Blocked	GAV, IPS, ASPY	No	No
150971-Test	1	None	Blocked	None	No	No
DMZ	2	None	Allowed	None	No	Yes
DMZ-sec	2	X3, X7	Blocked	None	No	Yes
DMZ-unsec	2	X2	Blocked	None	No	No
LAN	1	X0, X6, X6:V100	Allowed	GAV, IPS, ASPY, DPI-SSL-C	No	Yes
MULTICAST	6	None	Blocked	None	No	No
SSLVPN	8	None	Blocked	None	Yes	No
Test	1	None	Blocked	GAV, IPS, ASPY, DPI-SSL-C	No	Yes
VPN	5	None	Blocked	None	No	No
WAN	0	X1, X5	Blocked	GAV, IPS, ASPY, DPI-SSL-S, GVPN	Yes	No

Anzahl der Datensätze: 11



Wartungsbericht

Erläuterung

Der Wartungsbericht unterstützt Administratoren dabei, Konfigurationselemente zu identifizieren, die regelmäßig überprüft werden sollten, um die Firewall-Konfiguration übersichtlich, effizient und wartbar zu halten. Im Laufe der Zeit wachsen Firewall-Konfigurationen durch neue Regeln, Objekte, VPN-Verbindungen und Sicherheitsdienste kontinuierlich an. Ohne regelmäßige Wartung sammeln sich häufig veraltete oder nicht mehr benötigte Einträge an, was die Administration erschwert und die Fehlersuche unnötig komplex macht.

Dieser Bericht hebt Konfigurationselemente hervor, die überprüft werden sollten, wie beispielsweise deaktivierte oder ungenutzte Firewall-Regeln, inaktive NAT-Richtlinien, nicht verwendete Adress- und Service-Objekte, abgelaufene Security Services sowie weitere Konfigurationseinträge, die möglicherweise nicht mehr benötigt werden. Darüber hinaus werden Einstellungen aufgeführt, die von einer Optimierung oder Bereinigung profitieren können.

Der Zweck dieses Berichts besteht nicht darin, alle aufgeführten Elemente automatisch zur Löschung zu empfehlen. Vielmehr bietet er Administratoren eine strukturierte Übersicht über Konfigurationseinträge, die vor einer möglichen Änderung geprüft werden sollten. Manche Objekte oder Regeln werden möglicherweise nur selten verwendet oder sind für zukünftige Projekte, Testumgebungen, Notfallkonzepte oder besondere Anwendungsfälle weiterhin erforderlich.

Eine regelmäßige Wartung der Firewall bietet zahlreiche Vorteile:

- Reduziert die Komplexität der Konfiguration und verbessert die Übersichtlichkeit.
- Erleichtert die Fehlersuche sowie Audits und Sicherheitsüberprüfungen.
- Hilft dabei, veraltete oder vergessene Konfigurationseinträge zu identifizieren.
- Verringert das Risiko von Konfigurationsfehlern.
- Verbessert die langfristige Wartbarkeit und Administrierbarkeit der Firewall.
- Unterstützt eine saubere, dokumentierte und professionell gepflegte Sicherheitsumgebung.

Eine regelmäßig gewartete Firewall ist einfacher zu administrieren, leichter zu auditieren und bildet eine zuverlässige Grundlage für zukünftige Konfigurationsänderungen sowie eine dauerhaft sichere Netzwerkumgebung.

Vorschläge für Namenskonventionen

Erläuterung

Bedeutung einheitlicher Namenskonventionen für Address-Objects

Ein effektives Management von Firewall-Address-Objects ist entscheidend für eine sichere und gut organisierte Netzwerkumgebung. Ein wesentlicher Faktor hierfür ist die Verwendung konsistenter und aussagekräftiger Namenskonventionen.

Klarheit und schnellere Administration

Wenn Address-Objects einheitlichen Namensstandards folgen, erkennen Administratoren sofort Zweck, Standort oder zugehörigen Service, ohne detaillierte Konfigurationsdaten prüfen zu müssen. Dies reduziert den Aufwand bei Troubleshooting, Regelanpassungen und Policy-Änderungen und minimiert das Risiko, das falsche Object zu verändern.

Konsistenz und Genauigkeit in der Konfiguration

Standardisierte Namensformate schaffen Einheitlichkeit über die gesamte Konfiguration. Dies verhindert Duplikate, reduziert Verwechslungen und minimiert Fehlkonfigurationen, die zu unerwünschten Zugriffsberechtigungen oder blockierten Kommunikationsflüssen führen können. Vorhersehbare Namen erleichtern das effiziente und korrekte Interpretieren von Firewall-Policies.

Bessere Zusammenarbeit und Wissenstransfer

Konsistente Namenskonventionen ermöglichen eine gemeinsame Verständigungsbasis im Team. Auch Administratoren, die mit einer Konfiguration nicht vertraut sind, können Object-Nutzung und Abhängigkeiten schnell interpretieren. Das verbessert die Zusammenarbeit, erleichtert Onboarding und stellt Kontinuität sicher – auch bei wechselnden Zuständigkeiten.

Fazit

Einheitliche Namenskonventionen erhöhen Wartbarkeit, Genauigkeit und Transparenz von Firewall-Konfigurationen. Durch verbesserte Klarheit, reduzierte Komplexität und bessere Zusammenarbeit tragen sie wesentlich zu einer sicheren und nachhaltigen Netzwerkadministration bei.

Vorschläge für Namenskonventionen

Address Object Name old	Address Object Name new
SSLVPN-NetExtender Range	AO-SSLVPN-NetExtender Range-192.168.168.100
WAN-GoogleDNS-8.8.8.8	AO-WAN-GoogleDNS-8.8.8.8
WAN-TZ570-10.10.10.254	AO-WAN-TZ570-10.10.10.254
LAN-UDS-Analytics-10.100.10.50	AO-LAN-UDSAnalytics-10.100.10.50
WAN-GoogleDNS-8.8.8.8-2	AO-WAN-GoogleDNS2-8.8.8.8
TZ570 LAN	AO-VPN-TZ570 LAN-10.10.10.0
Server	AO-LAN-Server-10.99.10.223
MartinSchmitz	AO-LAN-MartinSchmitz-1.1.1.1
KlausMeier	AO-LAN-KlausMeier-1.1.2.2
FTP Server Private	AO-LAN-FTP Server Private-172.20.20.101
FTP Server Public1	AO-WAN-FTP Server Public1-10.10.20.2
Test	AO-LAN-Test-10.100.10.99
Test1	AO-LAN-Test1-10.100.10.99
Test4	AO-LAN-Test4-10.100.10.99
x0 und x6 subnet	AO--x0 und x6 subnet-0.0.0.0
Test12	AO-LAN-Test12-10.100.10.99
Test_111	AO-LAN-Test_111-10.100.10.111
Test_112	AO-LAN-Test_112-10.100.10.112
Test_113	AO-LAN-Test_113-10.100.10.113
Test_114	AO-LAN-Test_114-10.100.10.114
Test_115	AO-LAN-Test_115-10.100.10.115
Test_116	AO-LAN-Test_116-10.100.10.116
Test_117	AO-LAN-Test_117-10.100.10.117
Test_118	AO-LAN-Test_118-10.100.10.118
Test13	AO-LAN-Test13-10.100.10.13
Syslog Synology	AO-WAN-Syslog Synology-10.10.40.50
Test Group	AO--Test Group-0.0.0.0

Doppelte Adress Objekte

Erläuterung

Analyse doppelter Address-Objekte

Doppelte Adress-Objekte bei denen unterschiedliche Namen auf dieselbe IP-Adresse oder dasselbe Netzwerk verweisen – können mehrere operative und sicherheitsrelevante Herausforderungen verursachen.

1. Erhöhte Komplexität und Risiko von Fehlkonfigurationen

Wenn mehrere Objects auf dasselbe Ziel verweisen, ist oft unklar, welches verwendet werden soll. Das erschwert die Policy-Erstellung, erhöht die Wahrscheinlichkeit, das falsche Object zu nutzen, und verlangsamt Audits, Troubleshooting und Change-Prozesse.

2. Konfliktierende oder überlappende Policies

Unterschiedliche Objects für dieselbe IP können inkonsistent in Regeln verwendet werden. Eine Regel kann Traffic erlauben, während eine andere blockiert, was zu unvorhersehbarem Verhalten und schwieriger Policy-Analyse führt.

3. Uneinheitliche Sicherheitsdurchsetzung

Wenn unterschiedliche Teams oder Administratoren separate Objects für dieselbe Ressource anlegen, wird die Policy-Durchsetzung fragmentiert. Dies kann zu unbeabsichtigtem Zugriff oder unvollständiger Policy-Abdeckung führen und die Security-Posture schwächen.

4. Erhöhter Wartungsaufwand

Änderungen, die ein dupliziertes Object betreffen, müssen in allen Policy-Referenzen aktualisiert werden. Wird eine Stelle übersehen, entstehen veraltete Regeln, Lücken in Zugriffsbeschränkungen oder Configuration Drift.

Empfohlene Best Practices

– Address-Objekte konsolidieren:

Duplikate identifizieren und durch ein einzelnes Object je IP/Subnetz/Ressource ersetzen.

– Klare Namenskonventionen verwenden:

Namen sollten Zweck oder Ressourcenidentität widerspiegeln, um Konsistenz und Lesbarkeit zu verbessern.

– Regelmäßige Audits durchführen: Periodische Bereinigung reduziert Redundanz und verbessert die Policy-Qualität.

– Nutzung und Verantwortlichkeit dokumentieren: *Dokumentation unterstützt Wartung und verhindert das erneute Anlegen unnötiger Objects.*

Die Bereinigung doppelter Address-Objects verbessert die Klarheit von Regeln, vereinfacht die Policy-Administration, reduziert operative Fehler und trägt zu einer stärkeren und besser vorhersehbaren Sicherheitskonfiguration bei.

Duplicate Address Objects

IP	Name
- Keine Daten gefunden -	

Externe Protokollierung

Erläuterung

Externe Protokollierung und Telemetrie auf einer Firewall (z. B. Syslog, IPFIX/NetFlow, SNMP-Traps) sind wichtig, weil die Firewall zu den wenigen Komponenten gehört, die zuverlässig beobachten können, wer mit wem, wann, wie und mit welchem Ergebnis kommuniziert hat – also was erlaubt und was blockiert wurde. Ohne das Ausleiten dieser Informationen arbeitet man im Grunde im Blindflug: Die Policies können zwar schützen, aber es fehlt die Fähigkeit, Vorfälle zu erkennen, sauber zu untersuchen und belastbar nachzuweisen, was passiert ist.

Aus Sicht der IT-Sicherheit ist externe Logsammlung die Basis für Erkennung und Incident Response. Angriffe zeigen sich selten durch einen einzelnen, eindeutigen Alarm. Häufig sind es Muster: wiederholte Fehlanmeldungen, auffällige VPN-Anmeldungen, ungewöhnliche Policy-Treffer, unerwartete ausgehende Verbindungen oder Traffic zu verdächtigen Zielen. Ein SIEM oder eine Log-Plattform kann solche Signale über mehrere Quellen hinweg korrelieren (Firewall + Endpunkte + Identität + Server). Gerade Firewall-Events liefern oft die ersten hochwertigen Hinweise, und Flow-Telemetrie (NetFlow/IPFIX) liefert die „Netzwerk-Geschichte“, um Umfang und Auswirkungen eines Vorfalls zu verstehen.

Externe Sammlung ist außerdem entscheidend für Forensik und Nachvollziehbarkeit. Firewalls speichern Logs lokal nur begrenzt und können Daten bei Reboots, Updates oder durch Log-Rotation verlieren. Zentrale Systeme halten Nachweise länger vor, erfüllen Compliance-Anforderungen und ermöglichen verlässliche Reports. In der Praxis beginnen viele Untersuchungen erst Tage oder Wochen nach dem eigentlichen Ereignis. Wenn Logs nur lokal verfügbar waren, ist der relevante Zeitraum dann oft bereits überschrieben.

Auch operativ bringt Telemetrie klare Vorteile: Sie verbessert Stabilität und Troubleshooting. SNMP-Monitoring und Traps liefern Frühwarnungen bei CPU-/RAM-Spitzen, Interface-Fehlern, instabilen Tunneln oder Ressourcenengpässen – Probleme, die sonst wie „zufällige Ausfälle“ wirken, solange keine Zeitreihen vorliegen. Flow-Daten helfen, Bandbreitenverbrauch zu belegen, „Top Talker“ zu identifizieren, Fehlkonfigurationen zu erkennen (z. B. asymmetrisches Routing) und zu prüfen, ob eine Policy-Änderung wirklich den gewünschten Effekt hatte.

Schließlich unterstützt externe Protokollierung/Telemetrie die kontinuierliche Verbesserung: Man kann die Wirksamkeit von Regeln messen, zu großzügige oder zu „laute“ Policies gezielt nachschärfen und Schatten-IT bzw. riskante Dienste sichtbar machen. Kurz gesagt: Das Ausleiten von Logs und Telemetrie macht aus der Firewall nicht nur ein Gerät, das „Traffic blockt“, sondern einen Sicherheitsbaustein, den man verifizieren, auditieren und nachhaltig betreiben kann – und genau das ist der Unterschied zwischen Sicherheitsmaßnahmen und echter Sicherheitswirksamkeit.

Externe Protokollierung

Central Management

Central Management (NSM / GMS):	off
NSM ZeroTouch:	enabled

Syslog

Syslog Server Name:	n/a
Syslog Standby Server Name:	n/a
Syslog Server Port:	n/a

Netflow

Netflow Internal:	n/a
Netflow External:	n/a
Netflow External Address:	n/a

Log to FTP Server

Log to FTP Server:	
FTP Server IP Address:	n/a

Deaktivierte Firewall-Regeln

Erläuterung

Bedeutung deaktivierter Firewall-Regeln

Deaktivierte Firewall-Regeln setzen zwar keine aktiven Sicherheitskontrollen durch, sind jedoch weiterhin Teil der Konfiguration und können im Rahmen der Sicherheitsstrategie relevant sein.

Operatives Backup und schnelle Reaktivierung

Deaktivierte Regeln dienen häufig als vordefinierte Konfigurationsalternativen. Administratoren deaktivieren Regeln z. B. temporär während Wartung, Troubleshooting oder geplanten Änderungen und aktivieren sie später wieder, ohne die Policy neu entwerfen zu müssen. Dies ermöglicht eine schnelle Wiederherstellung beabsichtigter Sicherheitskontrollen.

Dokumentation für Konfiguration und Audits

Inaktive Regeln liefern Einblick in historische Regelwerke und frühere Sicherheitsentscheidungen. Ihre Sichtbarkeit unterstützt Audits, Compliance-Prüfungen und forensische Analysen, indem Konfigurationsabsicht und Änderungshistorie nachvollziehbar bleiben.

Flexibilität für zukünftige Anforderungen

Mit veränderten Netzwerkumgebungen können zuvor deaktivierte Regeln wieder relevant werden. Das Beibehalten ermöglicht schnelle Reaktivierung oder Anpassung, ohne komplexe Policies oder Objects neu erstellen zu müssen.

Fazit

Auch wenn deaktivierte Firewall-Regeln keinen Traffic filtern, bleiben sie wertvolle Referenzpunkte für operative Wiederherstellung, Dokumentation früherer Konfigurationen und schnelle Anpassung an zukünftige Anforderungen. Sie sollten regelmäßig überprüft werden, um sicherzustellen, dass sie weiterhin gültig, beabsichtigt und mit aktuellen Sicherheitszielen abgestimmt sind.

Deaktivierte Firewall-Regeln

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc
-----	---	------	---------	---------	--------	--------	--------	--------

- Keine Daten gefunden -

Anzahl der Datensätze: 0

Firewall-Regeln lange ungenutzt (IPv4)

Erläuterung

Firewall-Regeln, die über einen längeren Zeitraum nicht verwendet wurden

Firewall-Regeln, die über einen langen Zeitraum nicht verwendet wurden, deuten häufig auf veraltete Zugriffspfade, stillgelegte Services oder Legacy-Konfigurationen hin, die nicht mehr relevant sind. Das Beibehalten ungenutzter Regeln erhöht den administrativen Aufwand und kann zu unnötiger Sicherheits-Exposure führen.

Inaktive Regeln können versehentlich reaktiviert oder verändert werden und dadurch unbeabsichtigte Zugriffe erlauben oder die Policy-Durchsetzung schwächen. Das Entfernen oder Deaktivieren solcher Regeln hilft, eine saubere Rulebase zu erhalten, verbessert die Manageability und reduziert die gesamte Angriffsfläche der Umgebung.

Eine regelmäßige Überprüfung ungenutzter Regeln stellt sicher, dass nur notwendige und aktiv genutzte Zugriffspfade bestehen bleiben und unterstützt damit sowohl operative Effizienz als auch Security Best Practices.

Der folgende Bericht zeigt Regeln, die seit mehr als 365 Tagen nicht verwendet wurden.

Firewall-Regeln lange ungenutzt (IPv4)

Seite 1/1

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	Last time hit
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	Firewall-Regeln lange...
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Firewall-Regeln lange...
YES	A	Test 24	WAN	060466	any	any	any	OSPF	Firewall-Regeln lange...
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)	Firewall-Regeln lange...
YES	A	Test 23	WAN	060466	any	any	any	MSN	Firewall-Regeln lange...
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any	Firewall-Regeln lange...
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	Firewall-Regeln lange...
YES	A	Test 22	DMZ-unsec	DMZ-sec	any	any	any	MSN	Firewall-Regeln lange...
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	Firewall-Regeln lange...
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any	Firewall-Regeln lange...
YES	A	My Rule	DMZ-sec	DMZ-unsec	any	any	any	FTP Data	Firewall-Regeln lange...
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS	Firewall-Regeln lange...
YES	A	Test 20	DMZ-sec	DMZ-unsec	any	any	any	Kazaa / FastTrack	Firewall-Regeln lange...
YES	A	Test 21	DMZ-sec	DMZ-unsec	any	any	any	Lotus Notes	Firewall-Regeln lange...
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE	Firewall-Regeln lange...
YES	A	Test 18	DMZ-sec	DMZ-unsec	any	any	any	ICMP	Firewall-Regeln lange...
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	Firewall-Regeln lange...
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	Firewall-Regeln lange...
YES	A	Allow Citrix	any		any	any	Citrix UDP	any	Firewall-Regeln lange...
YES	A	Allow FTP	any		any	any	FTP	any	Firewall-Regeln lange...
YES	A	Allow management via ... SSLVPN		LAN	SSLVPN-NetExtender	Range any	any	HTTPS Management	2025-03-31 11:40:59

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Anzahl der Datensätze: 21

Deaktivierte NAT-(Network Address Translation)-Policies (IPv4)

Erläuterung

Deaktivierte NAT-Policies und deren Auswirkungen

Deaktivierte NAT-(Network Address Translation)-Policies können erhebliche operative und sicherheitsrelevante Auswirkungen in einem Netzwerk haben. Nachfolgend eine Übersicht der wichtigsten Risiken und technischen Implikationen im Zusammenhang mit inaktiven oder entfernten NAT-Regeln.

1. Verlust von Netzsegmentierung

NAT-Policies unterstützen die logische Trennung zwischen internen und externen Netzwerken, indem interne IP-Adressen vor dem Verlassen des Netzwerks umgesetzt werden.

Potenzielle Risiken:

– Exponierung interner IPs:

Ohne NAT können interne Adressierungsschemata extern sichtbar werden und zuvor isolierte Geräte erreichbar machen.

– **Reduzierte Trennung zwischen Zonen:** NAT unterstützt die Isolation zwischen LAN-, DMZ- und WAN-Segmenten. Deaktiviertes NAT kann Sicherheitsgrenzen unbeabsichtigt verwischen.

2. Erhöhte Sicherheitsrisiken

NAT bietet indirekt eine zusätzliche Schutzwirkung, indem es unaufgeforderte eingehende Verbindungen zu internen Hosts erschwert.

Mögliche Konsequenzen:

- Angreifer können interne Geräte direkt adressieren.
- Firewall-basierte Einschränkungen können umgangen werden.
- Interne Ressourcen lassen sich leichter enumerieren oder scannen.

3. Kommunikationsstörungen

Viele Kommunikationsflüsse setzen voraus, dass NAT für Translation und Routing aktiv ist.

Wenn NAT deaktiviert ist:

- Geräte verlieren ggf. Zugriff auf externe Services.
- Benutzer erleben inkonsistente Konnektivität.
- Troubleshooting wird komplexer durch Routing-Fehler oder nicht erreichbare Dienste.

4. Probleme in Multi-Network- und VPN-Szenarien

VPNs, Routing und Remote-Access-Technologien sind häufig auf NAT angewiesen, um interne und externe Adressräume abzugleichen.

Zentrale Risiken:

- Remote-Access-Sessions können fehlschlagen.
- Adressraum-Überlappungen können auftreten.
- Externe Systeme können Rückantwort-Traffic nicht korrekt routen.

5. Herausforderungen bei Policy-Enforcement und Monitoring

Zugriffssteuerungslogik nutzt NAT häufig, um Flows zu verfolgen und zu klassifizieren.

Konsequenzen deaktivierten NATs:

- Reduzierte Möglichkeit zur Überwachung/Korrelation von Traffic.
- Schwierige Zuordnung von Aktivitäten zu Geräten/Benutzern.
- Lücken in der Logging-Genauigkeit.

6. Höherer Verbrauch öffentlicher IP-Adressen

NAT ermöglicht vielen internen Geräten, eine einzelne oder kleine Pools öffentlicher IP-Adressen zu teilen.

Ohne NAT:

- Jedes System kann eine eigene routbare IP benötigen.
- IPv4-Knappheit wird zu einem operativen Problem.

Fazit

Deaktivierte NAT-Policies können zu unerwarteten Routing-Fehlern, geschwächten Schutzgrenzen und erhöhter Sicherheits-Exposure führen. In den meisten Umgebungen dient NAT nicht nur der Adressumsetzung, sondern auch der Durchsetzung von Isolation, Logging-Transparenz und vorhersehbarem Routing-Verhalten. Für stabilen und sicheren Betrieb sollten NAT-Policies sorgfältig überprüft, gepflegt und nur in intentionalen, gut kontrollierten Design-Szenarien deaktiviert werden.

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Deaktivierte NAT-(Network Address Translation)-Policies (IPv4)

Seite 1/1

Ena	Name	Original Source	Translated Source	Original Destination	Translated Destination	Original Service	Translated Service
NO	Test disabled NAT	DMZ-sec Subnets	Original	Any	Server	Citrix UDP	Original
NO	My Rule	DMZ-unsec Subnets	Original	All WAN IP	DEAG_Test	Any	Original
NO	Deact 3	FTP Server Private	FTP Server Public1	Any	Original	Any	Original

Aktive NAT-Policies ohne Traffic-Hits (IPv4)

Erläuterung

NAT-Policies ohne Traffic-Hits

Dieser Bericht hebt NAT-(Network Address Translation)-Policies hervor, die derzeit aktiviert sind, aber im überwachten Zeitraum nicht genutzt wurden. Eine NAT-Policy ohne aufgezeichnete Hits deutet typischerweise darauf hin, dass die Regel nicht mehr zu aktiven Traffic-Flows passt oder sich auf Services, Netzwerke oder Geräte bezieht, die nicht mehr genutzt werden.

Mögliche Ursachen für ungenutzte NAT-Policies

- Der zugehörige Service ist nicht mehr aktiv
- Geräte- oder Netzwerkreferenzen haben sich geändert
- Routing wurde umgestellt und macht die NAT-Translation obsolet
- Eine temporäre oder migrationsbezogene Regel wurde nicht entfernt

Warum ungenutzte NAT-Policies relevant sind

1. Erhöhte Policy-Komplexität

Ungenutzte NAT-Einträge machen die Konfiguration schwerer verständlich und wartbar. Administratoren investieren zusätzliche Zeit in die Bewertung nicht mehr relevanter Regeln, was Troubleshooting und Change Management verlangsamt.

2. Risiko unbeabsichtigter Aktivierung

Eine inaktive NAT-Policy kann aktiv werden, wenn sich Netzwerkbedingungen oder Routing ändern. Dadurch können interne Geräte unbeabsichtigt exponiert, Adressmappings verändert oder beabsichtigte Zugriffskontrollen umgangen werden.

3. Potenzielle Sicherheits-Exposure

Auch ungenutzte NAT-Regeln definieren grundsätzlich einen möglichen Translation-Pfad. Wird er unbeabsichtigt aktiv, kann dies:

- interne Adressierung offenlegen
- unerwünschte eingehende/ausgehende Verbindungen ermöglichen
- erwartete Filter-/Inspection-Punkte umgehen

4. Reduzierte operative Effizienz

Große NAT-Regelwerke erhöhen den administrativen Aufwand und reduzieren Konfigurationsklarheit. Das Entfernen obsoleter Einträge führt zu einem saubereren, besser vorhersehbaren Policy-Set und senkt operative Risiken.

Empfohlene Wartungspraktiken

- Regelmäßig prüfen, ob NAT-Regeln weiterhin erforderlich sind
- Verantwortlichkeit und Zweck dokumentieren
- Ungenutzte Mappings entfernen oder temporär deaktivieren und Auswirkungen validieren
- NAT-Policies nach Redesigns, Migrationen oder Decommissioning-Aktivitäten überprüfen

Fazit

Aktivierte NAT-Policies ohne Traffic-Aktivität weisen häufig auf veraltete oder unnötige Konfigurationsobjekte hin. Die Bereinigung reduziert Komplexität, verhindert unbeabsichtigte Exposure-Pfade und verbessert Wartbarkeit und Security-Posture. Regelmäßige Reviews stellen sicher, dass die Firewall-Policy das erforderliche und tatsächlich aktive Netzwerkverhalten abbildet.

- Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

Aktive NAT-Policies ohne Traffic-Hits (IPv4)

Seite 1/1

Ena	Name	Original Source	Translated Source	Original Destination	Translated Destination	Original Service	Translated Service
NO	Test disabled NAT	DMZ-sec Subnets	Original	Any	Server	Citrix UDP	Original
YES	Test 1	DMZ-sec Subnets	Original	Any	CSE_Access_Tier_AIP_1	Citrix TCP	Original
NO	My Rule	DMZ-unsec Subnets	Original	All WAN IP	DEAG_Test	Any	Original
NO	Deact 3	FTP Server Private	FTP Server Public1	Any	Original	Any	Original
YES	Default NAT Policy	Any	Any	Any	Any	Any	Original

WAN MTU Einstellung

Erläuterung

Dieser Abschnitt prüft, ob die WAN-MTU-Einstellung auf der SonicWall-Firewall ungewöhnlich niedrig konfiguriert ist. Ein zu niedrig eingestellter MTU-Wert kann die Übertragungseffizienz verringern und sich negativ auf die Netzwerkleistung auswirken.

Wird eine solche Einstellung festgestellt, sollte sie überprüft werden, um sicherzustellen, dass sie technisch erforderlich ist und nicht auf einer unnötigen Konfigurationseinschränkung beruht.

X1	WAN	1500	ok	-
X5	WAN	1500	ok	-