

# FIREWALL TOOLBOX

## Vollständiger Sicherheits- und Audit-Bericht



### Appliance-Details

Seriennummer: 0040XXXXXXXX (Demo)  
Firewall-Name: UDS-NSV270  
Appliance-Modell: SonicWall NSv 270  
Betriebszeit (Uptime): 0 Days, 0 Hours, 3 Minutes, 12 Seconds  
Firmware-Version: 7.3.0-7012-R8150

### Berichtsdetails

Erstellt am: 10.02.2026 - 15:44:35  
EXP File: C:\U...\Repository\0040XXXXXXXX\exp\_api\_downloaded.exp  
EXP-Zeitstempel: 10.02.2026 15:38  
TSR-Datei: C:\U...\Repository\0040XXXXXXXX\tsr\_api\_downloaded.wri  
TSR-Zeitstempel: 10.02.2026 15:38

### Zusatzinformation

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

## 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
Gateway Anti-malware/Intrusion Prevention/App Control	Licensed		14.02.2027 00:00
Capture Client Basic	Not Licensed		
Capture Client Advanced	Not Licensed		
Capture Client Premier	Not Licensed		
Content Filtering Service	Licensed		14.02.2027 00:00
SSL VPN	Licensed	2 Max: 100	
Global VPN Client	Licensed	50 Max: 1000	
Stateful High Availability	Licensed		
Comprehensive Anti-Spam Service	None		
Capture Advanced Threat Protection	Licensed		14.02.2027 00:00
Syslog Analytics	Expired		03.02.2024 00:00
Basic Reporting (7 days)	Not Licensed		
Advanced Reporting & Analytics	None		
DNS Filtering	Licensed		14.02.2027 00:00
Threat Protection Service Suite	None		
Essential Protection Service Suite	Disabled		05.02.2026 00:00
Advanced Protection Security Suite	Licensed		14.02.2027 00:00
Managed Protection Security Suite	Not Licensed		
24x7 Support	Licensed		14.02.2027 00:00
Standard Support	Not Licensed		
Hardware Warranty	None		
Remote Implementation Service	None		
Gateway Anti Virus	None		
Intrusion Prevention	None		
AppControl	None		
GeoIP Filtering	None		
SSL Control	Licensed		
Anti Spyware	None		
BotNet Block	None		
DPI SSL Client	Licensed		
DPI SSL Server	Licensed		
DPI SSH	Licensed		
Global VPN Client Enterprise	None		
Advanced Reporting & Analytics (7 days)	Licensed		14.02.2027 00:00
SonicOS Expanded	None		
NSM Essential	None		
NSM Advanced	None		
Model Upgrade	Not Licensed		
Capture Client MDR	None		

## 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
Content Filtering Service	On
DPI SSH	On
DPI SSL Client	Off
DPI SSL Server	Off
SSL Control	On
Gateway Anti-malware/Intrusion Prevention/App Control	-
- Anti Spyware	On
- AppControl	On
- BotNet Block	On
- Gateway Anti Virus	On
- GeoIP Filtering	On
- Intrusion Prevention	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.

#### SSL/TLS-Entschlüsselung ist deaktiviert

Heutzutage ist der Großteil des Netzwerkverkehrs mit SSL/TLS verschlüsselt. Diese Verschlüsselung schützt zwar die Vertraulichkeit der Daten, verhindert jedoch gleichzeitig, dass klassische Sicherheitsmechanismen den Datenverkehr auf Bedrohungen überprüfen können. Ohne Entschlüsselung können Schadsoftware, Command-and-Control-Kommunikation sowie Datenabfluss unbemerkt über verschlüsselte Verbindungen erfolgen. Die Entschlüsselung von SSL/TLS-Verkehr auf der Firewall – oder auf dem Client, falls eine Entschlüsselung auf der Firewall nicht möglich ist – ermöglicht es Sicherheitssystemen, den Datenverkehr in Echtzeit zu analysieren, versteckte Bedrohungen zu erkennen, Sicherheitsrichtlinien durchzusetzen und Angriffe zu verhindern, die andernfalls unsichtbar bleiben würden. Dadurch wird die Erkennungsrate deutlich erhöht und das Risiko von Sicherheitsvorfällen reduziert, während die Verschlüsselung nach der Prüfung erneut angewendet wird.

## 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.*

### Erläuterung

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

## 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. Unautorisierte 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

### SSL-VPN

SSL VPN Web Management: on

SSL VPN SSH Management: off

### API

API access: enabled

## Optionen für Verwaltungszugriff: Interface Management

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

## 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)

(Page 1/1)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
YES	A	Allow management via S...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow Maintenanc...

## 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

admin

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

Silvia

### 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.

## 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

(Page 1/2)

### 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

### Silvia

- 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
- Gewährt Zugriffsrechte auf: WAN-GoogleDNS-8.8.8.8

## Zusätzliche Informationen

### Warum der Einsatz eines externen Benutzerverzeichnisses sinnvoll ist, wenn eine Firewall mehr als 10 lokale Benutzer hat

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 – Multifaktor-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.

## Benutzerzugriff auf Netzwerkobjekte

### Erläuterung

#### **Benutzerzugriff auf Netzwerkobjekte**

*Dieser Bericht zeigt die Zugriffsrechte, die Benutzern für spezifische Netzwerkobjekte zugewiesen sind. Er stellt dar, welche Ressourcen einzelne Benutzer erreichen dürfen, und hilft zu prüfen, ob diese Berechtigungen mit dem beabsichtigten Zugriffslevel übereinstimmen.*

*Diese Informationen sind hilfreich, um überprivilegierte Konten zu identifizieren, Zugriffspolicies zu validieren und sicherzustellen, dass Netzwerkressourcen gemäß organisatorischen Sicherheitsanforderungen geschützt sind.*

## Benutzerzugriff auf Netzwerkobjekte

Seite 1

### Benutzer / Zugriffsrechte

User: Isabel

- 060466 Subnets
- 150971-Test Interface IP
- DEAG\_Test

User: LocalAdmin

- LAN Subnets

User: Webadmin

- LAN Primary Subnet

User: mschmitz

- DMZ Subnets
- DMZ-unsec IPv6 Subnets
- DMZ-unsec Interface IP
- LAN Primary Subnet
- WAN-TZ570-10.10.10.254

## 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

Benutzername	Einmalpasswort (TOTP) aktiviert
<b>admin</b>	<b>NO</b>
mschmitz	NO
All LDAP Users	NO
Webadmin	NO
LocalAdmin	YES
Robert	NO
Isabel	NO
Silvia	NO
Udo	NO
Uwe	NO
apiuser	NO

## 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

(Page 1/1)

Ena	Name	Phase1 Exchange Mode	Phase1 DH-Group	Phase 1 Encr	Phase1 Auth	Phase2 Protocl	Phase2 Encr	Phase2 Auth	Phase 2 PFS	Phase 2 DH-Group
no	Bad Tunnel	IKEv2	192-Bit R ECP Group	3DES (!)	MD5 (!)	ESP	AES-192 (C)	SHA384 (C)	on	Group 1 (!)
yes	New York	Main (!)	224-Bit R ECP Group	AES-128 (C)	MD5 (!)	ESP	DES (!)	AES-XCBC (C)	off (!)	Group 2 (!)
yes	Remote Sitel	IKEv2	Group 2 (!)	AESCGM16-256 (C)	SHA-1 (!)	ESP	AESGMAC-128	n/a	off (!)	Group 2 (!)
no	SNWL Policy Mode	IKEv2	521-Bit R ECP Group	AESCGM16-256 (C)	SHA-1 (!)	ESP	None (!)	MD5 (C)	on	384-Bit R ECP Group
no	Test	IKEv2	Group 2 (!)	AES-128 (C)	SHA-1 (!)	AH (C)	AESCGM16-256	SHA-256 (C)	off (!)	Group 2 (!)
yes	To TZ570	IKEv2	Group 1 (!)	AES-256	SHA-1 (!)	ESP	AES-256	n/a	on	n/a
no	WAN GroupVPN	Aggressive (!)	Group 14	AES-256	SHA-512	ESP	AES-256	AES-XCBC (C)	on	Group 14

## 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

## 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 bösartigen 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.*

### Erläuterung

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

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

(Page 1/1)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
YES	A	Test a/a	any		any	any	Citrix UDP	any	

## Ungenutzte Firewall-Regeln (IPv4)

### Erläuterung

#### **Warum ungenutzte Firewall-Regeln nicht im System verbleiben sollten**

*Firewall-Regelwerke entwickeln sich im Laufe der Zeit weiter, um Anwendungen, Dienste, Infrastrukturänderungen und Benutzeranforderungen zu unterstützen. Wenn Regeln jedoch bestehen bleiben, obwohl sie nicht mehr genutzt werden, verursachen sie Risiken, ohne einen operativen Nutzen zu liefern.*

#### **Sicherheitsrisiken**

*Ungenutzte Regeln vergrößern die Angriffsfläche der Firewall. Auch wenn sie derzeit nicht verwendet werden, können sie weiterhin Zugriffspfade erlauben, die Administratoren nicht (mehr) bewusst sind. Werden sie unbeabsichtigt oder durch Fehlkonfiguration reaktiviert, könnten sie unautorisierten Datenverkehr zulassen. Zudem suchen Angreifer häufig nach inaktiven oder vergessenen Einträgen, da diese seltener überwacht oder korrekt durchgesetzt werden.*

#### **Operative Ineffizienz**

*Große Regelwerke verlangsamen administrative Tätigkeiten, erhöhen den Aufwand für Troubleshooting und reduzieren die Wartbarkeit. Wenn sich Regeln im Laufe der Zeit ansammeln, wird es für Security-Teams schwieriger, relevante Einträge schnell zu identifizieren oder das Verkehrsverhalten zu analysieren. Dies führt häufig zu längeren Incident-Response-Zeiten und höheren Betriebskosten.*

#### **Reduzierte Performance**

*Auch wenn moderne Firewalls große Regelwerke effizient verarbeiten können, verbrauchen unnötige Regeln weiterhin Speicher und können die Performance der Regelverarbeitung negativ beeinflussen – insbesondere in Umgebungen mit umfangreichen Policy-Definitionen. Eine schlanke und korrekte Regelbasis sorgt für schnellere Auswertung und reduziert System-Overhead.*

#### **Herausforderungen bei Compliance und Audits**

*Ungenutzte Regeln werden in Sicherheitsprüfungen häufig beanstandet. Sie können gegen interne Sicherheitsrichtlinien oder externe Compliance-Frameworks verstoßen, die Begründung, Review-Historie, Verantwortlichkeit und Zweck jeder aktiven Regel verlangen. Ohne klare Dokumentation führen ungenutzte Regeln häufig zu Findings und Remediation-Anforderungen.*

#### **Best Practice**

*Firewall-Konfigurationen sollten regelmäßig überprüft werden. Regeln ohne aufgezeichnete Aktivität über definierte Zeiträume sollten bewertet werden. Ist eine Regel nicht mehr erforderlich, verbessert ihre Entfernung die Klarheit, reduziert Risiken und stellt sicher, dass die Firewall-Policy die tatsächlichen operativen und sicherheitsrelevanten Anforderungen der Organisation widerspiegelt.*

### Erläuterung

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

## Ungenutzte Firewall-Regeln (IPv4)

(Page 1/1)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	
YES	A	Rule7	DMZ-sec	Test	any	KlausMeier	DHCP Server	any	
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	
YES	A	Rule6	DMZ-sec	Test	KlausMeier	Test13	Citrix	any	
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow Maintenanc...
YES	A	Test a/a	any		any	any	Citrix UDP	any	

## 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.*

### Erläuterung

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

## Regeln, die Zugriff aus unsicheren Netzen erlauben (IPv4)

(Page 1/1)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow Maintenanc...

## 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 Netzwerkkumgebungen 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

(Page 1/1)

Ena	Act Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
-	Keine Daten	gefunden	-					

## 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.

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

## Firewall-Regeln lange ungenutzt (IPv4)

(Page 1/1)

Ena	A	SrcZone	DstZone	Src Zone	Dst Zone	Svc	Dst Addr	Src Service	Last time hit
- Keine Daten gefunden -									

## Firewall Regeln die Zugriffe ins WAN erlauben (IPv4)

### Erläuterung

Explanation Firewall Rules Internal > WAN

### Erläuterung

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

## Firewall Regeln die Zugriffe ins WAN erlauben (IPv4)

(Page 1/1)

Ena	Act Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
-	Keine Daten	gefunden	-					

## Alle Regeln (IPv4)

### Erläuterung

Die folgende Tabelle listet alle Regeln auf, die im System gefunden wurden.

### Erläuterung

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

## Alle Regeln (IPv4)

(Page 1/1)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	
YES	A	Rule7	DMZ-sec	Test	any	KlausMeier	DHCP Server	any	
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	
YES	A	Rule6	DMZ-sec	Test	KlausMeier	Test13	Citrix	any	
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	
YES	A	Allow management via S...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow Maintenanc...
YES	A	Test a/a	any		any	any	Citrix UDP	any	

## 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.

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

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

(Page 1/1)

Ena	Name	Original Source	Translasted Source	Original Destination	Translated Destination	Original Service	Translated Service
-	Keine Daten	gefunden	-				

## 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.

Hinweis: Automatisch hinzugefügte Regeln sind in diesem Bericht ausgeschlossen

## Aktive NAT-Policies ohne Traffic-Hits (IPv4)

(Page 1/1)

Ena Name	Original Source	Translasted Source	Original Destination	Translated Destination	Original Service	Translated Service
NoneDefault NAT Policy	Any	Any	Any	Any	Any	

## 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, Zugriffseignisse 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:	30.09.2025 09:52
Ältester im TS-Report gefundener Audit-Eintrag:	10.02.2026 14:36

### Im Audit-Log identifizierte Benutzer

- admin1
- 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.*

## Product Life Cycle Information

### 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.

## Firmware Version Check

### Erläuterung

Firewall-Auslastungsanalyse

### Firmware Version Check:

Firmware Installed on Firewall: 7.3.0-7012-R8150

Latest Firmware on MySonicWall: 7.3.1-7013

Firmware Release Date: Nov 18, 2025

Release Note URL:

[https://software.sonicwall.com/Firmware/Documentation/232-006386-00\\_RevB\\_SonicOS\\_7.3.1\\_ReleaseNotes.pdf](https://software.sonicwall.com/Firmware/Documentation/232-006386-00_RevB_SonicOS_7.3.1_ReleaseNotes.pdf)

### Zusätzliche Informationen

Firmware 7.3.1-7013 is available on MySonicWall.com, consider upgrading to that version

## 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	None	Settings import	
7.1.1-7047-5557	None	Settings import	
7.1.1-7058-6162	None	Settings import	
7.1.1-7058-6162	None	Settings import	
7.1.1-7040-5387	2024-01-24 08:25:53	Firmware applied	
7.1.1-7047-5557	2024-03-01 07:37:45	Firmware applied	
7.1.1-7058-6162	2024-12-03 20:01:06	Firmware applied	
7.1.3-7015-6965	2025-03-31 21:24:27	Firmware applied	
7.3.0-7012-8150	2025-09-08 18:29:24	Firmware applied	

### Zusätzliche Informationen

Kein nicht unterstütztes Firmware-Downgrade festgestellt

## Mit Conversion Tool konvertierte Einstellungen

### 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

## 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.*

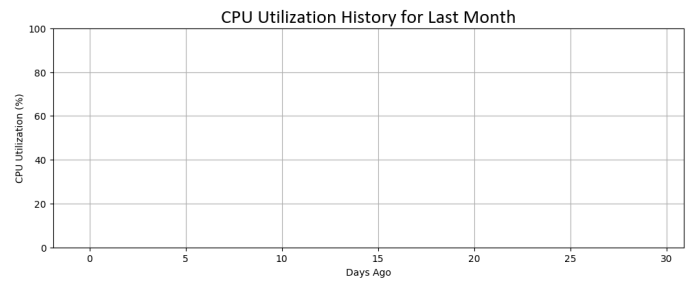
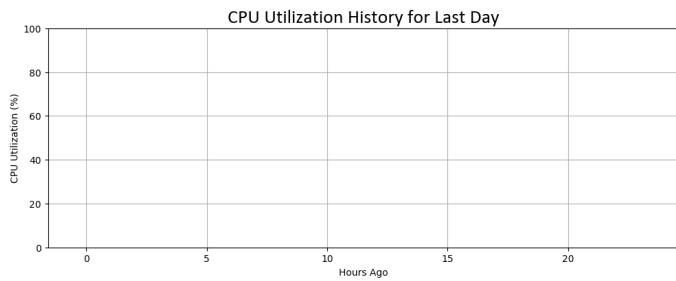
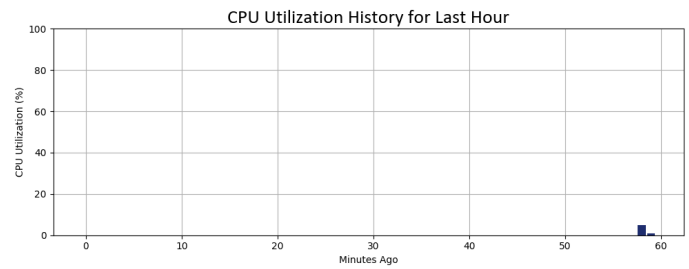
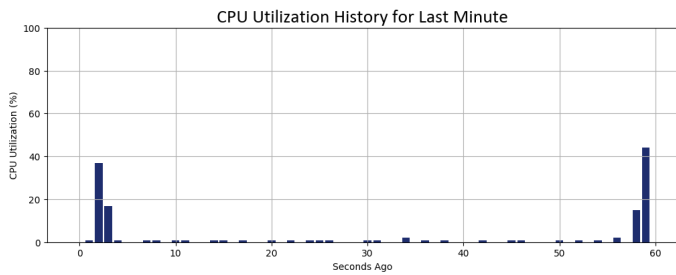
#### **Wichtige Hinweise für HA-Umgebungen**

*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

Timeframe	Avg Util	Status
Minute:	2 %	unkritisch
Hour:	0 %	unkritisch
Day:	0 %	unkritisch
Month:	0 %	unkritisch

## Performance-Auslastungsdiagramme



## 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:	0040XXXXXXXX Demo
HA Secondary Serial-Number:	0040XXXXXXXX Demo
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 00:02:45

### High Availability Status

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

## 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 Geschäftsführung, 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	7607	6077
X5	WAN		552	43

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

## Empfehlungen – Best-Practice-Bericht

### Erläuterung

#### Konfigurationsabgleich mit Best Practices

Dieser Bericht bewertet die aktuelle Konfiguration im Vergleich zu SonicWall-Best-Practice-Empfehlungen. Er hebt Bereiche hervor, die den empfohlenen Richtlinien entsprechen, sowie Einstellungen, die Anpassungen erfordern könnten, um Sicherheit, Performance oder operative Zuverlässigkeit zu verbessern.

Feature	Status	Recommendation
<b>Firewall Name</b>		
- Firewall Name has been changed:	yes	-
<b>Firmware and Settings</b>		
- Firmware Version current:	up to date	-
- Unallowed Firmware downgrade	not detected	-
<b>IPv6</b>		
IPv6	disabled	-
<b>High Availability</b>		
High Availability	enabled	-
- Stateful Sync:	enabled	-
- preempt mode	disabled	-
<b>WAN Lines</b>		
Multiple WAN Lines	configured	-
<b>VPN</b>		
Weak ciphers found	yes	reconfigure VPN Tunnels
<b>Firewall internal audit</b>		
Internal Audit	on	-
<b>Detection Prevention</b>		
Stealth Mode	on	-
Randomize IP IDs	on	-
<b>Packet Capture</b>		
Packet Capture	on	Disable if not needed
<b>Users Account Protection</b>		
Admin TOTP secured	no	Enable TOTP for Admin
Users with no TOTP	yes	Enable TOTP for these users
<b>WAN MTU Settings</b>		
X1 1500	ok	-

x5 1500

ok

-