FIREWALL TOOLBOX

Full Report

Appliance Details

Serial-Number:	0040103CD830
Firewall Name:	UDS-NSV270
Appliance Model:	SonicWall NSv 270
Uptime:	0 Days, 0 Hours, 22 Minutes, 15 Seconds
Firmware Version:	7.3.0-7012-R8150

Report Details

Date & Time Report created	15.09.2026 16:34:24
EXP File:	C:\Us...es_Backup_EXP_18C24198A992_Aug_16_26_52705209.exp
EXP Timestamp:	15.09.2026 16:33:48
TSR File:	C:\Us...es_Backup_TSR_18C24198A992_Aug_15_26_a35035a5.wri
TSR Timestamp:	15.09.2026 16:33:49

Additional Information

- IPv6 is disabled. IPv6-related reports are not included

- Auto-added rules are excluded from this report

Table of content

Recommendations - Best Practise Report

Explanation

Configuration Alignment with Best Practices

This report evaluates the current SonicWall firewall configuration against established best-practice recommendations. Its purpose is to identify settings that already align with operational and security standards, while also highlighting areas where improvements may be advisable. The assessment is intended to support a structured review of the device configuration with regard to security, maintainability, resilience, and overall service reliability.

A well-aligned firewall configuration helps reduce operational risk, simplifies administration, and improves transparency during support and audit activities. In addition to technical security controls, best-practice alignment also includes configuration consistency, clear device identification, and the avoidance of unnecessary or legacy settings. Each reviewed section in this report is therefore designed to provide both a status indication and a brief explanation of why the evaluated item is relevant from an operational or security perspective.

Particular attention is given to the software and firmware state of the firewall. The report checks whether the currently installed firmware is up to date and whether indications of an unsupported firmware downgrade have been detected. This is important because outdated firmware may expose the device to known issues, while unsupported downgrade scenarios can affect stability, compatibility, and vendor supportability. A compliant firmware state is therefore a key requirement for secure and reliable operation.

The report also reviews whether IPv6 is enabled and whether its use appears appropriate for the environment. If IPv6 is not required, it should generally be disabled in order to reduce unnecessary attack surface and administrative complexity. In the same way, the report evaluates whether High Availability is enabled. Where High Availability is not in use, its implementation is strongly recommended, as it improves resilience and reduces downtime in the event of hardware failure or planned maintenance.

Another important area is connectivity redundancy. The configuration is reviewed to determine whether multiple WAN connections are available. If only a single WAN uplink is in use, an additional WAN connection is highly recommended to improve redundancy and maintain Internet connectivity during provider outages. WAN-related optimization settings such as MTU are also considered. If the WAN MTU appears to be configured unusually low, this should be reviewed, as unnecessarily low MTU values can reduce transmission efficiency and negatively affect performance.

From a security perspective, the report includes checks related to user account protection, VPN hardening, and threat defense capabilities. It evaluates whether administrative accounts are protected by two-factor authentication, which is strongly recommended to reduce the risk of unauthorized access through weak, reused, or compromised credentials. The VPN configuration is also reviewed for the presence of outdated encryption algorithms, weak ciphers, or legacy settings that may reduce the security of encrypted communications. In addition, the report checks whether detection and prevention features are enabled, as these functions are essential for identifying suspicious activity and blocking potential threats at an early stage.

Administrative visibility and operational discipline are further addressed through checks such as internal audit logging and packet capture status. An enabled internal audit function is important because it provides traceability for configuration changes and administrative actions, which supports troubleshooting, security investigations, and compliance requirements. The report also identifies whether packet capture is still running. A continuously active packet capture may indicate unfinished troubleshooting and can create unnecessary overhead if left enabled without a valid operational reason.

Finally, the report considers the overall utilization state of the firewall. Reviewing overall utilization is important to determine whether the device is operating within an acceptable load range or approaching capacity limits. A consistently high utilization may indicate performance risks and should be evaluated further. In combination, the findings in this report provide a practical overview of the current configuration quality and help identify measures that can improve security posture, operational stability, and long-term maintainability.

Firewall Name has been changed

Renaming a SonicWall firewall from its serial number to a meaningful device name improves administration, troubleshooting, and reporting. A descriptive name makes it easier to identify the firewall's location, role, or customer assignment at a glance, especially in environments with multiple devices. This reduces confusion, speeds up support activities, and lowers the risk of configuration or operational errors.

Feature - Setting	Status	Recommendation
Firewall Name has been changed	Status	-

Firmware and Settings

This section shows whether the current firmware version is in use and whether an unsupported firmware downgrade has been detected. This allows the software status to be assessed quickly and any potential risks to operation, compatibility, and supportability to be identified.

Feature - Setting	Status	Recommendation
Firmware version is up to date	update available	Upgrade firmware

Unsupported Firmware downgrade

This is a check if an unsupported Firmware downgrade has occured

Feature - Setting	Status	Recommendation
Unsupported Firmware downgrade	not detected	-

IPv6 Status

If IPv6 is not required in the environment, it should be disabled to reduce unnecessary attack surface and administrative complexity.

Feature - Setting	Status	Recommendation
IPv6 Status	disabled	-

High Availability Status

If High Availability is not enabled, its use is highly recommended to improve resilience and reduce downtime in the event of hardware failure or maintenance. It helps ensure service continuity and increases overall availability of the security infrastructure.

Feature - Setting	Status	Recommendation
High Availability Status	present	-

Redundant WAN Lines

If only a single WAN connection is in use, an additional WAN line is highly recommended to improve redundancy and maintain Internet connectivity in the event of a provider outage. Multiple WAN connections also increase overall availability and can support failover or load balancing.

Feature - Setting	Status	Recommendation
Redundant WAN Lines	configured	-

VPN Configuration

This section highlights potential issues in the VPN Configuration, such as outdated encryption algorithms, weak ciphers, or legacy settings.Such findings may reduce the overall security of the VPN connection and can lead to compatibility, compliance, or supportability issues. A review and update of the VPN configuration is recommended to align it with current security standards and best practices.

Feature - Setting	Status	Recommendation
VPN unsafe algorithms used	yes	Reconfigure VPN Tunnels

Internal Firewall Audit

This section shows whether the internal audit function is enabled on the SonicWall firewall. An enabled audit function is important because it records configuration changes and administrative actions, improving traceability and accountability. This supports troubleshooting, security investigations, and compliance requirements.

Feature - Setting	Status	Recommendation
Internal Firewall Audit	enabled	-

Built-in administrator account used for administration

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

Feature - Setting	Status	Recommendation
Built-in administrator account used for administrationyes		use personalized accounts

Detection and Prevention Functions

This section shows whether Detection and Prevention features are enabled on the SonicWall firewall.

Feature - Setting	Status	Recommendation
Detection and Prevention Functions	enabled	-

Packet Capture running

This section shows whether Packet Capture is currently still running on the SonicWall firewall.
A continuously active packet capture should be reviewed, as it may indicate unfinished troubleshooting and can consume system resources or generate unnecessary capture data.
If it is no longer needed, it should be stopped to avoid unnecessary overhead and operational impact.

Feature - Setting	Status	Recommendation
Packet Capture running	no	-

Account Protection

This section shows whether user accounts on the SonicWall firewall are protected with two-factor authentication (2FA).

Feature - Setting	Status	Recommendation
Admin Account TOTP Secured	no	Enable Service or Feature
User Accounts protected with TOTP	no	Enable Service or Feature

Firewall Utilization

Monitoring overall utilization is important to identify elevated load conditions that may affect performance, stability, or the effectiveness of security services.

Feature - Setting	Status	Recommendation
Utilization last minute	0 %	OK
Utilization last hour	0 %	OK
Utilization last day	0 %	OK
Utilization last day	0 %	OK

Security services that are licensed but not in use

This report shows the number of Security Services that are licensed, but not in use

Feature - Setting	Status	Recommendation
Number of Services	1	Enable Service or Feature

Security Service not activated

Enabling a security service on a zone while the service itself is globally disabled results in no effective protection. Although the zone configuration indicates that the service is active, the underlying engine is not running, so no inspection or filtering is performed. This can create a false sense of security and lead to misconfigured firewall policies.

Feature - Setting	Status	Recommendation
Security Service not activated	yes	Enable Service or Feature

WAN MTU Settings

A correctly configured WAN MTU is important to ensure efficient packet transmission and stable network communication. A low MTU value can cause problems in data transmission

Feature - Setting	Status	Recommendation
Low WAN MTU size detected	not detected	-

TCP Connection Timeout

Changing the global TCP timeout affects every TCP session processed by the firewall. It is generally recommended to leave the default value unchanged and adjust timeouts only for individual access rules when required.

Feature - Setting	Status	Recommendation
Default TCP Timeout has been changed	not detected	-

Firewall-Rules not used for a long time

Rules that are not currently in use provide no operational value. To keep the framework clear and efficient, these unused rules should be reassessed and, where appropriate, eliminated

Rule-Type	Number of Occurences
Firewall-Rules never used (IP v4)	0
Firewall-Rules not used for a long time (IP v4)	21

Firewall Rules Disabled

Rules that are not currently in use provide no operational value. To keep the framework clear and efficient, these unused rules should be reassessed and, where appropriate, eliminated

Rule-Type	Number of Occurences
Firewall Rules Disabled (IP v4)	0

Firewall Rules allow WAN to internal networks

Firewall rules allowing WAN-to-internal network access increase exposure and should be restricted to essential services only, with regular validation of business need

Rule-Type	Number of Occurences
Firewall Rules allow WAN to internal networks (IP v4)	0

ANY <> ANY Rules

Rules allowing any source to any destination on any port create excessive exposure and should be avoided unless there is a clearly justified and documented business need.

Rule-Type	Number of Occurences
ANY <> ANY Rules (IP v4)	0

Rules allowing Management Access

Rules allowing management access should be strictly limited to authorized sources and secured services only, as they present a high risk if exposed too broadly.

Rule-Type	Number of Occurences
Rules allowing Management Access (IP v4)	4

Unused NAT Policies

Unused NAT policies provide no active function and should be reviewed regularly to determine whether they are still needed or can be removed.

Rule-Type	Number of Occurences
Unused NAT Policies (IP v4)	0

Disabled NAT Policies

Unused NAT policies provide no active function and should be reviewed regularly to determine whether they are still needed or can be removed.

Rule-Type	Number of Occurences
Disabled NAT Policies (IP v4)	0

Additional Information

- Auto-added rules are excluded from this report

Security Report

Explanation

The Security Audit focuses on identifying potential security risks and policy weaknesses. It analyzes firewall rules for overly permissive configurations, detects unused or risky objects, and reviews user privileges and access rights. The goal is to highlight misconfigurations that could be exploited or that violate best practices, providing actionable insights to improve the overall security posture.

Audit Settings Report

Explanation

Internal Firewall Audit
Internal auditing on firewalls is an essential component of maintaining operational integrity, accountability, and security within a network environment. The firewall represents one of the most critical control points in an organization, and auditing provides visibility into configuration changes, access events, and administrative actions that directly influence network security posture.

Accountability and Traceability
Audit logs document who made changes, when they were made, and what was modified. This traceability ensures that responsibilities are clearly assigned and that any misconfiguration, deviation from standards, or unauthorized change can be quickly identified and corrected.

Detection of Unauthorized or Risky Modifications
Firewalls directly affect access control, data protection, and traffic flow. Internal auditing allows administrators to detect intentional or accidental configuration changes, helping to identify security incidents, policy violations, or potential misuse of administrative privileges.

Support for Compliance and Governance
Many regulatory frameworks require auditing of critical systems such as firewalls. Internal audit records support compliance with standards relevant to industries such as finance, healthcare, and government. They provide proof that policies are followed and that protective mechanisms are properly enforced.

Operational Insight and Continuous Improvement
Audit logs help security teams understand configuration history and operational trends. Reviewing these records on a regular basis allows organizations to refine access policies, identify recurring issues, and strengthen change management practices.

Incident Investigation and Forensics
When a security event occurs, internal audit data is often one of the most valuable sources of evidence. It enables investigators to reconstruct actions taken on the firewall, analyze root causes, and determine whether malicious activity or human error contributed to the incident.

Conclusion
Internal auditing is necessary for ensuring transparency, consistency, and accountability in firewall operations. It enhances security, supports regulatory requirements, enables faster troubleshooting, and provides a key foundation for resilient network management.

Audit Settings Report

Audit Details

Internal Auditing:	on
Audit Records Found in the TS Report:	2000
Most Recent Audit Entry Found in the TS Report:	15.09.2026 16:33:49
Oldest Audit Entry Found in the TS Report	27.07.2026 08:29:20

Users identified in the audit log

- UDSAdmin
- admin
- apiuser
- HA Sync

Additional Information

Use of Generic Administrator Account

The user account *"admin"* has been detected in the audit records. It is recommended to avoid using generic or shared administrator accounts for firewall management. Instead, each administratorshould log in using a personalized account.

Using individual user identities ensures that configuration changes can be tracked

Comment
The account *HA Sync* is an internal system user that is used exclusively for synchronizing configuration and operational data between appliances in a High Availability (HA) setup. This account is not intended for manual login or administrative use.

Report Rules DPI SSL Disabled

Explanation

Rules with Deep Packet Inspection Disabled
Deep Packet Inspection (DPI) allows the firewall to inspect traffic beyond basic connection information such as source, destination, and port. It is an important prerequisite for applying security services and detecting threats within network traffic.
This report identifies access rules for which Deep Packet Inspection is disabled. Traffic matching these rules may bypass DPI-based inspection and therefore may not benefit from all configured security services.
Disabling DPI can be appropriate for specific traffic, for example due to compatibility requirements, performance considerations, or because the traffic does not require additional inspection. However, DPI should normally only be disabled intentionally and for a documented reason.
Review the rules listed in this report and verify that disabling DPI is required. Where no specific reason exists, consider enabling DPI to ensure that traffic receives the intended level of security inspection.

Rules where Client DPI SSL Inspection is switched off

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

- Auto-added rules are excluded from this report

Number of records: 2

Client DPI SSL Decryption

Explanation

DPI-SSL Client Inspection is a key security feature that enables the firewall to inspect encrypted outbound HTTPS traffic. Without decryption, security services such as Gateway Anti-Virus, Intrusion Prevention, Capture ATP, Content Filtering, and Application Control have limited visibility into encrypted connections, potentially allowing threats to bypass inspection.
This report verifies whether DPI-SSL Client Inspection is licensed and enabled on the firewall. It also identifies the zones on which client inspection is active and highlights any access rules where DPI-SSL has been explicitly disabled. Rule-level exceptions should be carefully reviewed, as they may create blind spots where encrypted traffic is not inspected and security services cannot be fully applied.
Organizations should ensure that DPI-SSL Client Inspection is enabled where appropriate and that exceptions are limited to applications or services with documented compatibility requirements. Regular review of DPI-SSL configuration helps maintain visibility into encrypted traffic and reduces the risk of undetected threats.

Client DPI SSL Decryption

```
DPI SSL Licensed:          yes
```

```
SSL-Decryption for outgoing traffic is disabled (!)
```

Client DPI SSL Decryption

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

Rules where Client DPI SSL Inspection is switched off

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

- Auto-added rules are excluded from this report

Number of records: 3

Detection and Prevention Functions

Explanation

The options Randomize IP ID and Enable Stealth Mode provide additional protection against network reconnaissance and certain classes of attacks. Randomizing the IP Identification field makes it more difficult for attackers to perform operating system fingerprinting or infer traffic patterns, while Stealth Mode prevents the firewall from responding to unsolicited connection attempts, reducing its visibility on untrusted networks.

Detection and Prevention Functions

Stealth Mode

Stealth Mode activated	on

Randomize IP ID

Randomize IP ID activated	on

Rules allowing Any Destination and Any Port (IPv4)

Explanation

Why Firewall Rules that allow "Any" are risky
In the realm of network security, firewall rules play a critical role in controlling inbound and outbound traffic to and from a network. One common, yet highly discouraged, practice is the implementation of "any to any" rules. These rules permit unrestricted traffic flow from any source to any destination, essentially allowing all types of data packets to pass through the firewall without any filtering.

Security Implications *The primary concern with "any to any" rules is the significant security risk they pose. Firewalls are designed to act as gatekeepers, scrutinizing incoming and outgoing traffic to protect the network from unauthorized access, cyber-attacks, and other malicious activities. By setting rules that indiscriminately allow all traffic, the firewall's essential function is bypassed, exposing the network to potential threats. This open gateway can be exploited by attackers to gain access to sensitive information, inject malware, or launch other detrimental exploits.*

Lack of Traffic Control *Apart from security vulnerabilities, "any to any" rules hinder the ability to monitor and control network traffic effectively. Effective network management relies on understanding and managing the flow of data. Unrestricted rules make it challenging to track, analyze, or prioritize traffic, leading to potential network performance issues, including bandwidth congestion and reduced efficiency.*

Compliance and Best Practices *In many industries, regulatory requirements dictate strict control and monitoring of data traffic. "Any to any" rules may violate compliance standards, leading to legal and reputational repercussions. Moreover, cybersecurity best practices advocate for a principle of least privilege, where only necessary traffic is permitted, further highlighting the inadvisability of such permissive rules.*

Recommendation *Instead of adopting "any to any" rules, it is recommended to implement specific, well-defined firewall rules based on the principle of least privilege. These rules should be tailored to only allow necessary and legitimate traffic required for business operations, ensuring both network security and optimal performance.*

Rules allowing Any Destination and Any Port (IPv4)

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	Example any<> any
YES	A	Allow FTP	any		any	any	FTP	any	

- Auto-added rules are excluded from this report

Number of records: 5

Firewall rules that allow management services from untrusted networks (IPv4)

Explanation

Firewall rules that allow management services from untrusted networks
Management services such as SSH (Secure Shell), HTTPS (Hypertext Transfer Protocol Secure), and similar administration interfaces are intended for privileged access. Allowing them directly from untrusted networks introduces multiple security concerns.

Why such rules are risky:
Exposure to Attacks
Allowing management services to be accessed over the Internet exposes them to attacks such as brute-force login attempts, exploitation of software vulnerabilities, or denial-of-service attacks targeting the service.

Elevation of Privilege
If an attacker successfully connects to a management service, they may gain administrator-level access. This could allow them to modify firewall configurations, create persistent access mechanisms, or interrupt network communication.

Sniffing and Eavesdropping
Unencrypted management protocols may allow attackers to intercept sensitive information. Even encrypted services can be at risk if keys are exposed, outdated encryption is used, or implementation flaws exist.

Lack of Monitoring
Management interfaces are often not monitored as thoroughly as user-facing systems, increasing the chance that unauthorized access remains undetected.

Complexity and Human Error
The more services exposed externally, the greater the risk of misconfiguration or operational mistakes, which can lead to accidental exposure of critical systems.

Recommended Best Practices
Management access should be limited strictly to trusted internal networks. If remote administration is required, it should be performed through secure access channels such as VPN connections with strong encryption. Multi-factor authentication should be implemented wherever possible, management services should be actively monitored for unauthorized access attempts, and devices must be kept updated with current patches to mitigate known vulnerabilities.

Firewall rules that allow management services from untrusted networks (IPv4)

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...

- Auto-added rules are excluded from this report

Number of records: 4

Management Access Options

Explanation

Management Access Options and Security Considerations

There are several methods available to access firewall management, each offering different usability benefits and security implications. Because firewall management interfaces provide administrative control over critical network infrastructure, improper exposure of these access methods can introduce significant risk.

Unauthorized access to firewall management may result in configuration manipulation, disclosure of sensitive security parameters, or even full compromise of the network environment. For this reason, it is essential to review regularly which management access mechanisms are enabled and ensure that only secure, justified, and properly protected methods remain accessible.

Restricting management access to trusted networks, enforcing strong authentication, and monitoring administrative activity are key practices in maintaining a secure and controlled configuration landscape.

Management Access Options

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

Management Access Options: 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

Management Access Options: IPSec (VPN)

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 - Overview En- And Disabled

Explanation

Active Security Services
This report shows which Security Services are currently enabled on the device. However, activation at the system level only indicates that the service functionality is available—it does not guarantee that traffic is actually being inspected.

To effectively analyze traffic, Security Services must also be explicitly assigned to zones or applied to specific firewall rules. Without this configuration step, the enabled technologies may remain inactive for relevant network flows, resulting in reduced protection coverage.

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

Additional Information

No Route-All VPN Tunnel Configured

There is no route-all VPN tunnel currently configured and active. This is a common scenario in environments where all traffic is forwarded to an upstream security device, which is responsible for traffic inspection, policy enforcement, and additional security processing.

In such setups, the firewall functions primarily as a routing or segmentation device, while deeper inspection is handled by a centralized security solution, such as a secure web gateway, cloud security service, or dedicated inspection platform.

Security Services - Assignment per Zone

Explanation

Security Services
This report shows which Security Services are enabled on each zone. While enabling a service globally makes its functionality available, actual protection is only applied if the service is actively assigned at the zone level.

Security Services bound to zones determine which network segments receive inspection for threats such as malware, intrusion attempts, or unwanted content. Zones without corresponding service assignments may remain insufficiently protected, even if the feature is enabled on the system.

This overview helps identify coverage gaps, verify that critical zones (such as LAN or VPN access areas) are properly protected, and ensure that inspection policies align with organizational security requirements.

Additional Information

Security services marked with (!) are enabled on the zone but disabled globally.

Security Services - Assignment per Zone

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

Users account protection

Explanation

User Account Protection Overview
This report lists all user accounts and indicates how they are protected, including whether two-factor authentication (2FA) is enabled. This helps verify the strength of authentication mechanisms and identify accounts that may require additional protection.

Users account protection

Username	TOTP Enabled
admin	**NO**
All LDAP Users	NO
apiuser	NO
Isabel	NO
LocalAdmin	YES
mschmitz	NO
Robert	NO
Sylvia	NO
Udo	NO
Uwe	NO
Webadmin	NO

User external authentication methods

Explanation

External Authentication Configuration Overview
This report lists which external authentication systems are configured, whether they are enabled, and highlights any potential security concerns related to their setup. External authentication can significantly strengthen user identity management when implemented correctly, but improper configuration may introduce security and operational risks.

LDAP (Lightweight Directory Access Protocol)
When LDAP is used, authentication requests are forwarded to an external directory such as Microsoft Active Directory. Using LDAP centralizes user identity and password management, reducing local account dependency. However, LDAP authentication should always be secured through TLS (LDAPS). Unencrypted LDAP communication exposes usernames, passwords, and group membership information to interception, increasing risk of credential theft.

RADIUS Authentication
RADIUS is commonly used for VPN access and central authentication services. It supports challenge-response methods, central logging, and standardized enforcement of authentication policies. Security risks arise when shared secrets are weak or reused across multiple systems. Additionally, if RADIUS servers become unavailable, access could be disrupted unless proper fallback mechanisms are configured.

TACACS+ Authentication
TACACS+ is typically used for administrative authentication, especially in enterprise environments. It separates authentication, authorization, and accounting functions (AAA), which ensures traceable administrator activity and granular privilege control. Although secure in design, TACACS+ requires proper configuration of encrypted channels and unique keys. Central TACACS+ outages can block administrative access unless redundancy is in place.

Properly configuring and securing external authentication systems helps improve accountability, reduce management complexity, and enhance overall access security. Regular review of availability, encryption settings, authentication policy mapping, and fallback behavior ensures reliable and secure authentication processes across the environment.

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(!)

Administrative User Overview

Explanation

Administrative User
This report lists all users who hold administrative privileges. Accounts with administrative rights have elevated access to configuration settings, policy changes, sensitive information, and system management functions.
Reviewing these users ensures that only authorized personnel retain privileged access and supports compliance, accountability, and secure access control practices.

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

Additional Information

Important Notice Regarding LDAP Group Assignments
If administrative rights are assigned to LDAP groups, all members of those groups automatically inherit administrator privileges. This means that any changes to LDAP membership - such as adding new users or synchronizing external directory structures - may unintentionally grant elevated access.

Regularly reviewing group assignments and membership is essential to ensure that only authorized personnel receive administrative privileges and that access control remains aligned with organizational security policies.

Best Practices for VPN Security

Explanation

VPN Security
Virtual Private Networks (VPNs) are essential for protecting data across untrusted networks. To remain effective, their cryptographic settings must be reviewed and updated regularly. Outdated methods weaken security, reduce compliance, and expose organizations to unnecessary risks.

Why regular checks matter:

- Security:
Cyber threats evolve quickly. Old encryption or authentication methods can be compromised with modern computing power.
- Compliance:
Many industries require strong encryption to meet regulatory requirements.
- Access control:
Strong authentication prevents unauthorized use of the VPN.
- Data protection:
Updated encryption ensures confidentiality and integrity of sensitive information.
- Performance & future readiness:
Newer standards increase not only security, but also efficiency and scalability.

Insecure elements to avoid:
- Symmetric ciphers:
DES and 3DES are obsolete and vulnerable.
- Diffie-Hellman (DH) groups:
Groups 1 (768-bit), 2 (1024-bit), and 5 (1536-bit) are too weak.
- IKE versions:
IKEv1 is outdated; IKEv2 is recommended.
- Hash functions:
MD5 and SHA-1 are considered compromised and no longer secure.
- Key management:
Weak or static pre-shared keys (PSKs) are easy to guess or brute-force.

Recommended secure options

- Encryption:
- AES-128 or AES-256.
- Key exchange:
- DH groups ≥ 2048-bit or Elliptic Curve Diffie-Hellman (P-256/P-384).
- Protocol:
- IKEv2 for modern VPN setups.
- Integrity:
- SHA-256 or stronger.
- Authentication:
Prefer certificates; if PSKs are used, use strong, random keys.

Conclusion
VPNs are only as strong as their cryptographic foundations. By avoiding weak algorithms and adopting modern standards, you protect sensitive data, meet compliance requirements, and prepare your network for future challenges. Review and update your VPN configuration regularly to remain secure.

Explanation

(!) = unsafe © = caution

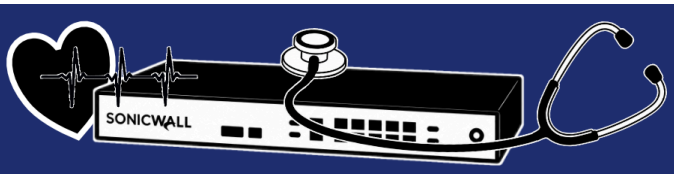
Best Practices for VPN Security

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 (!)	AESCGM16-256 (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 Policy Crypto Settings – Used Unsafe Algorithms

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

Explanation

The Maintenance Report helps identify configuration items that should be reviewed regularly to keep the firewall clean, efficient, and easy to manage. Over time, firewall configurations naturally grow as new rules, objects, VPNs, and services are added. Without periodic maintenance, obsolete or unused entries can accumulate, increasing administrative overhead and making troubleshooting more difficult.
This report highlights configuration elements that may require attention, such as disabled or unused firewall rules, inactive NAT policies, unused address and service objects, expired security services, and other configuration items that are no longer actively used. It also identifies settings that may benefit from optimization or cleanup.
The purpose of this report is not to recommend automatic removal of every listed item. Instead, it provides administrators with a structured overview of configuration components that should be verified before any changes are made. Some objects or rules may still be required for future projects, temporary environments, disaster recovery procedures, or infrequently used services.
Regular maintenance provides several important benefits:
- Reduces configuration complexity and improves readability.
- Makes troubleshooting and auditing significantly easier.
- Helps identify obsolete or forgotten configuration elements.
- Reduces the risk of accidental configuration errors.
- Improves long-term manageability of the firewall.
- Supports a well-documented and professionally maintained security environment.
A well-maintained firewall is easier to administer, easier to audit, and provides a stronger foundation for future configuration changes and security improvements.

Firewall Utilization Analysis

Explanation

Firewall Utilization Analysis
These graphs illustrate the firewall's utilization level during the period preceding data export. High utilization can lead to performance degradation, including delayed traffic processing or dropped packets. To gain meaningful insights, the Technical Support Report used as data source should ideally be generated during a period of high system load.

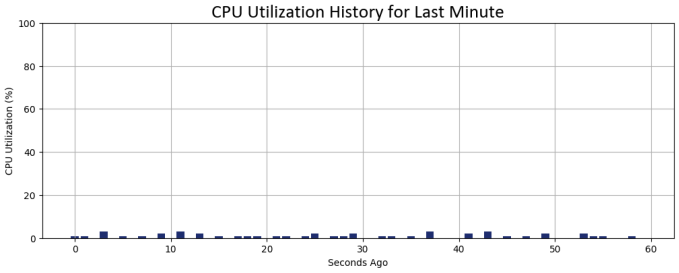
Recommended Data Sources
More accurate utilization statistics are typically obtained from NetFlow- or SNMP-based external monitoring systems. For NetFlow-based reporting, SonicWall provides a dedicated solution named *Analytics*, which integrates seamlessly with SonicWall firewalls.

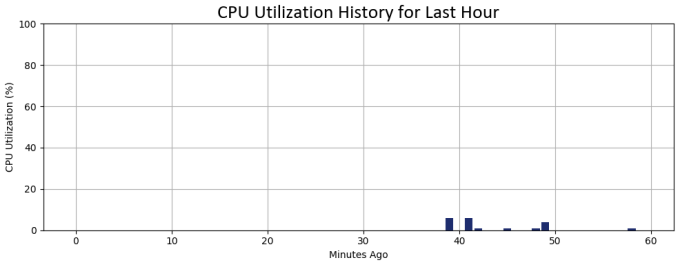
Important Considerations for HA Environments
If utilization values are missing for the selected timeframe, verify whether the firewall operates in a High Availability (HA) cluster. When the standby unit becomes active during the reporting period, utilization data may not be captured in the expected device, resulting in incomplete or missing chart information.

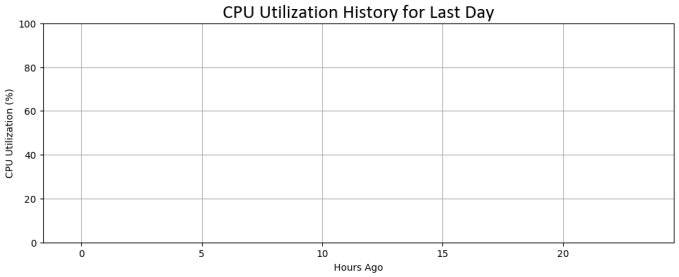
Firewall Utilization Analysis

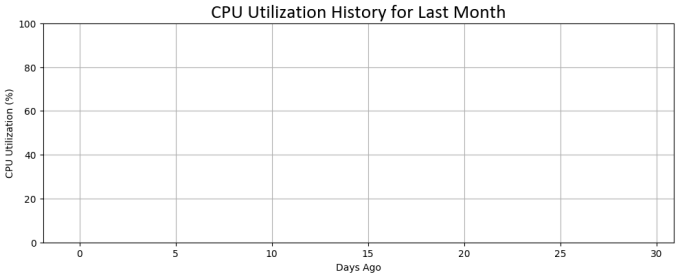
Timeframe	Average	Status
Minute:	0 %	OK
Hour:	0 %	OK
Day:	0 %	OK
Month:	0 %	OK

Performance Utilization Graphs









Firmware Version Check

Explanation

Firmware Version Comparison
This section compares the currently installed firmware version with the latest available release on MySonicWall. This helps identify whether the device is up-to-date, requires a recommended upgrade, or is running an outdated software build that may lack enhancements, bug fixes, or security improvements.

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

Additional Information

Firmware 7.3.3-7015 is available on MySonicWall.com, consider upgrading to that version

Configuration and Firmware History Overview

Explanation

Configuration and Firmware History Overview
The following table provides an overview of past configuration states and firmware versions implemented on the device. It highlights how often settings were migrated and whether unsupported firmware downgrades occurred.

Unsupported Downgrades
A firmware downgrade is considered unsupported if no configuration from the downgraded firmware version was imported afterward. In such cases, system compatibility cannot be guaranteed, and operational issues may arise.

Impact of Aged or Frequently Migrated Configurations
Configuration sets that have been migrated repeatedly or used across multiple devices may gradually accumulate inconsistencies or outdated parameters. This can lead to unexpected behavior, degraded performance, or configuration processing errors during future migrations or upgrades.

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	

Additional Information

No unsupported firmware downgrade found

Configuration and Firmware History Overview

Explanation

Configuration Conversion Overview
This report indicates whether configuration settings were converted using SonicWall's Conversion Tool. This helps identify migrated configurations and provides insight into whether settings originated from previous platforms or earlier deployments.

Details

```
Settings were converted in the past: No
```

Reliability - High Availability

Explanation

Importance of High Availability on Firewall Systems

1. Continuous Security Enforcement
High Availability (HA) ensures uninterrupted operation of firewall systems, maintaining continuous security controls even during hardware issues, updates, or planned maintenance. This prevents gaps in threat detection, access validation, and policy enforcement.

2. Reduced Downtime
In an HA configuration, a secondary firewall automatically takes over if the primary unit becomes unavailable. This seamless failover minimizes downtime, ensuring uninterrupted access to critical applications and services.

3. Improved System Reliability
Having multiple firewalls operating in a redundant pair increases resilience against hardware failures, configuration corruption, or unexpected outages. Reliability of network security infrastructure is significantly improved.

4. Business Continuity Support
Organizations that depend on real-time connectivity, cloud access, and online services cannot tolerate prolonged network outages. HA safeguards business operations by keeping security enforcement active throughout operational events and failure scenarios.

5. Performance Benefits with Load Distribution
Some HA environments support load distribution, improving throughput by balancing sessions or traffic paths across multiple appliances. This avoids processing bottlenecks and increases overall network performance.

6. Disaster Recovery Capability
HA plays a crucial role in disaster recovery planning. When a primary device fails, the secondary unit maintains active policies, routing, VPN tunnels, and security services, reducing operational impact during recovery activities.

7. Regulatory and Compliance Alignment
Many industries require guaranteed availability of security controls and traceable failover mechanisms. Implementing HA supports compliance initiatives, audit readiness, and service-level commitments.

8. Improved User and Customer Experience
With uninterrupted network access, users experience fewer service disruptions and faster restoration after failures. This directly contributes to higher satisfaction levels and more stable service delivery.

Summary
High Availability on firewall systems is a critical foundation for business resilience. It ensures continuous protection, minimizes operational downtime, supports disaster recovery, improves performance, and enables compliance. By reducing service interruptions and maintaining secure connectivity, HA significantly enhances both operational and security effectiveness.

Reliability - 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

Product Life Cycle Information

Explanation

Product Lifecycle Information
This section provides insight into the current product lifecycle status. It helps determine whether a device is fully supported, approaching end of support, or already beyond its official maintenance period.

For detailed lifecycle descriptions, important milestones, and current support schedules, please refer to the official SonicWall product lifecycle documentation available through SonicWall Support resources.

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

Additional Information

Please re-check these information from the official SonicWALL Website!

Security Services - License Status Overview

Explanation

Security Services Licenses
This report shows which services currently have an active license. Licensed services are fully functional and able to provide their intended protection or feature set. Services without a valid license may be limited in functionality or completely inactive.

This view helps verify whether required security and subscription-based features remain operational, and it assists in planning renewals to avoid service interruptions.

Security Services - License Status Overview

Service Name	License Status	Count	Expiration
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 - License Status Overview

Service Name	License Status	Count	Expiration
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

Reliability - WAN Failover

Explanation

Importance of WAN Failover on Firewall Systems

1. Uninterrupted Internet Connectivity
WAN failover ensures continuous internet access by automatically switching to a backup connection if the primary WAN link fails. This is crucial for maintaining business operations that rely on internet connectivity.

2. Enhanced Reliability and Availability
By providing a secondary connection, WAN failover enhances the reliability and availability of network services. This reduces downtime and increases overall productivity.

3. Business Continuity
Network outages can lead to financial losses, reduced customer satisfaction, and operational delays. WAN failover supports business continuity by minimizing disruptions and maintaining access to critical applications and services.

4. Load Balancing and Improved Performance
Some firewall platforms support both failover and load balancing. This allows traffic to be distributed across multiple WAN links, optimizing bandwidth and improving performance for end users.

5. Disaster Recovery Support
During unexpected outages or infrastructure failures, failover ensures that recovery processes remain accessible and uninterrupted, preserving service availability and data integrity.

6. Maintained Security Posture
Failover-capable firewalls ensure that all traffic—during normal operation and during failover events—continues to pass through security inspections. This prevents bypassing protection measures during outages.

7. Cost Efficiency
Although implementation of secondary WAN lines has associated costs, preventing service interruptions helps avoid financial losses, productivity decreases, and customer dissatisfaction, resulting in long-term savings.

Summary
WAN failover is a crucial capability in firewall systems. It maintains continuous internet access, supports disaster recovery, improves reliability, strengthens security consistency, and protects business continuity. By reducing downtime and improving performance, WAN failover helps organizations maintain service quality and operational efficiency.

Reliability - 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

Configuration Report

Explanation

The Configuration Audit reviews the technical setup and operational readiness of the firewall environment. It evaluates system features such as High Availability (HA), WAN Failover, and the status of security services. Additionally, it checks whether key components are correctly configured and aligned with recommended deployment standards.

TCP Connection Timeout

Explanation

The TCP connection timeout determines how long the firewall keeps an inactive TCP session in its connection table before it is removed. The global default value of 15 minutes is a reasonable setting for most environments and provides a good balance between supporting legitimate network traffic and conserving firewall resources
Changing the global TCP timeout affects every TCP connection that passes through the firewall. Increasing this value unnecessarily can lead to stale sessions remaining in memory for extended periods, consuming connection table entries and potentially reducing the overall capacity of the appliance. In large or busy environments, this may have a noticeable impact on firewall performance and resource utilization.
Some applications, however, require longer idle periods to maintain persistent connections. Examples may include certain database applications, legacy client/server software, or specialized industrial control systems. In these cases, it is considered best practice to leave the global timeout at its default value and instead configure a custom TCP timeout only on the specific access rules that require it.
Applying extended timeouts at the rule level provides several advantages:
Minimizes the impact on the overall firewall.
Limits increased resource consumption to the affected applications.
Reduces the number of stale sessions in the connection table.
Makes special application requirements visible and easier to document.
Simplifies future audits and troubleshooting.
This report displays the current global TCP timeout setting and lists all access rules that use a custom TCP timeout value. Rules with non-default settings should be reviewed periodically to ensure that the exception is still required and appropriately documented.
As a general recommendation, the global TCP timeout should remain at the default value whenever possible, while application-specific requirements should be addressed by using per-rule timeout overrides.

General TCP Setting

```
Global TCP Connection Timeout: 69
```

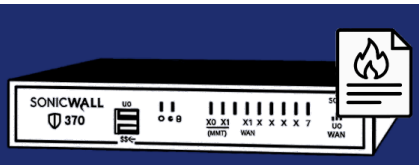
Additional Information

The default TCP Connection Timeout has been modified. It is recommended to keep the general setting at 15 minutes. If a certain service requires different values, change the TCP timeout on a specific rule

Rules, where the default TCP Timeout has been changed

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

Number of records: 3



Documentation Report

Explanation

The Documentation Report provides a structured overview of the firewall environment and its key configuration elements. It collects and presents relevant system information, including network settings, interface assignments, zone configurations, and applied policies.
The report is intended to serve as a comprehensive reference for administrators, supporting both operational tasks and knowledge transfer. It ensures that important configuration details are clearly documented and easily accessible, reducing dependency on manual inspection of the system.
Additionally, the documentation helps to maintain transparency and consistency across the environment, facilitating troubleshooting, audits, and future changes.

All Audit Records

Explanation

Internal Firewall Audit
Internal auditing on firewalls is an essential component of maintaining operational integrity, accountability, and security within a network environment. The firewall represents one of the most critical control points in an organization, and auditing provides visibility into configuration changes, access events, and administrative actions that directly influence network security posture.

Accountability and Traceability
Audit logs document who made changes, when they were made, and what was modified. This traceability ensures that responsibilities are clearly assigned and that any misconfiguration, deviation from standards, or unauthorized change can be quickly identified and corrected.

Detection of Unauthorized or Risky Modifications
Firewalls directly affect access control, data protection, and traffic flow. Internal auditing allows administrators to detect intentional or accidental configuration changes, helping to identify security incidents, policy violations, or potential misuse of administrative privileges.

Support for Compliance and Governance
Many regulatory frameworks require auditing of critical systems such as firewalls. Internal audit records support compliance with standards relevant to industries such as finance, healthcare, and government. They provide proof that policies are followed and that protective mechanisms are properly enforced.

Operational Insight and Continuous Improvement
Audit logs help security teams understand configuration history and operational trends. Reviewing these records on a regular basis allows organizations to refine access policies, identify recurring issues, and strengthen change management practices.

Incident Investigation and Forensics
When a security event occurs, internal audit data is often one of the most valuable sources of evidence. It enables investigators to reconstruct actions taken on the firewall, analyze root causes, and determine whether malicious activity or human error contributed to the incident.

Conclusion
Internal auditing is necessary for ensuring transparency, consistency, and accountability in firewall operations. It enhances security, supports regulatory requirements, enables faster troubleshooting, and provides a key foundation for resilient network management.

Additional Information

Important Note
The firewall analyzed in this report is part of a High Availability (HA) cluster. Audit logs are not synchronized between HA appliances. Therefore, configuration changes made on the secondary appliance while it was the active unit during a failover may not appear in the audit trail of the primary appliance. As a result, this report may not reflect all configuration changes made within the cluster. Future versions of Firewall Toolbox may address this limitation.

Additional Information

This report shows only the 10 most recent entries. Run the individual report to view all results.

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:        UDSAdmin
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:        UDSAdmin
Session:     GMS
Source:      127.0.0.1 (50325)
```

All Rules (IPv4)

Explanation

This report provides a complete inventory of all configured IPv4 access rules on the firewall, excluding the built-in default access rules. For each rule, the report lists the enabled status, action (Allow/Deny), rule name, source and destination zones, source and destination network objects, service objects, administrator comments, and the unique rule UUID.
Maintaining an up-to-date inventory of firewall rules is an essential part of firewall administration and security auditing. It allows administrators to review the implemented security policy, verify that rules follow the principle of least privilege, identify obsolete or redundant rules, and ensure that rule documentation is complete and meaningful. Regular review of the rule base helps reduce configuration complexity, improves troubleshooting, and minimizes the risk of unintended access caused by outdated or overly permissive firewall rules.

All Rules (IPv4)

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	

- Auto-added rules are excluded from this report

Number of records: 21

Management Rules (IPv4)

Explanation

Firewall Rules Allowing Management Access on SonicWall Firewalls (SSH / HTTPS)

SonicWall firewalls provide management services such as SSH and HTTPS to allow administrators to configure, monitor, and maintain the device. These services grant privileged access to the firewall and its security controls. Firewall rules that allow management access must therefore be handled with extreme care, as improper exposure can introduce serious security and operational risks.

Security Risks
Allowing management access through firewall rules increases the attack surface of the SonicWall appliance. Management interfaces are a common target for attackers because successful access provides direct administrative control. Exposed SSH or HTTPS services may be subject to brute-force login attempts, credential-stuffing attacks, or exploitation of vulnerabilities in the SonicWall management plane or underlying firmware.

If an attacker gains administrative access, they may modify firewall rules, disable security services, alter VPN configurations, or create persistent backdoors. Such actions can result in traffic interception, loss of network integrity, or complete compromise of the protected environment.

Exposure to Network-Based Attacks
When SonicWall management services are reachable from untrusted networks (such as the WAN or broadly defined zones), they become visible to automated scans, reconnaissance activity, and denial-of-service attacks. Even when encrypted protocols like HTTPS or SSH are used, risks remain if firmware is outdated, weak cryptographic settings are enabled, or access is not sufficiently restricted.

Additionally, misconfigured management access rules may unintentionally expose administrative ports on multiple interfaces or zones, increasing the likelihood of accidental or unauthorized access.

Operational and Compliance Impact
Management access rules that are too permissive complicate monitoring and incident detection on SonicWall firewalls. Unauthorized access attempts may be difficult to distinguish from legitimate administrative activity, especially if logging and alerting are not tightly configured. From a compliance perspective, unrestricted or undocumented management access often violates internal security policies and regulatory requirements that mandate strict control over privileged access and administrative interfaces.

Recommended Best Practices for SonicWall Firewalls
Management access on SonicWall devices should be restricted to trusted internal networks or dedicated management zones. Direct management access from WAN interfaces should be avoided whenever possible. If remote administration is required, it should be performed via secure VPN connections with strong authentication and encryption.

Additional recommended controls include limiting access by source IP address, enabling multi-factor authentication for administrative users, keeping SonicWall firmware up to date, and regularly reviewing management access rules and audit logs. These measures help ensure that administrative access remains controlled, auditable, and aligned with SonicWall security best practices.

Management Rules (IPv4)

Explanation

Management Service Objects and Groups
The items listed below represent the Service Objects and Groups that are classified as management services. These typically include protocols and ports used for administrative access, device configuration, and monitoring functions.

Identifying these services helps determine where management access is allowed and ensures that administrative interfaces are applied only to trusted and controlled areas of the network.

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 Rules (IPv4)

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...

Number of records: 4

Interfaces (IPv4)

Explanation

Interface Configuration Overview
This report displays all configured interfaces along with their assigned settings. It provides visibility into interface roles, addressing information, and operational parameters, helping assess connectivity, segmentation, and overall network structure.

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

Number of records: 9

User and Group Membership Overview

Explanation

Users and Group Memberships
This report provides a detailed list of all users along with their associated group memberships. Based on these affiliations, it highlights the effective VPN access rights that users inherit through assigned groups.
This helps identify who has access to VPN resources, verify proper entitlement, and detect potential over-privileged accounts resulting from group-based permissions.

User and Group Membership Overview

All LDAP Users
-is Member of Group: Trusted Users
-is Member of Group: SSLVPN Services
-is Member of Group: LAN Access66
- Grants access rights to: WAN Primary IP
- Grants access rights to: LAN Primary Subnet
- Grants access rights to: WAN-GoogleDNS-8.8.8.8

Isabel
-is Member of Group: Trusted Users
-is Member of Group: Content Filtering Bypass
-is Member of Group: Limited Administrators

LocalAdmin
-is Member of Group: Trusted Users
-is Member of Group: SonicWALL Administrators

Robert
-is Member of Group: Trusted Users
-is Member of Group: Guest Administrators

Sylvia
-is Member of Group: Trusted Users
-is Member of Group: Guest Administrators

UDS-SNWL-Admins@uds.local
-is Member of Group: SonicWALL Administrators

Udo
-is Member of Group: Trusted Users
-is Member of Group: SonicWALL Read-Only Admins

Uwe
-is Member of Group: Trusted Users
-is Member of Group: SonicWALL Administrators
-is Member of Group: SSLVPN Services
-is Member of Group: LAN Access66
- Grants access rights to: WAN Primary IP
- Grants access rights to: LAN Primary Subnet
- Grants access rights to: WAN-GoogleDNS-8.8.8.8

Webadmin
-is Member of Group: Trusted Users
-is Member of Group: SonicWALL Administrators
-is Member of Group: SSLVPN Services

apiuser
-is Member of Group: Trusted Users
-is Member of Group: SonicWALL Administrators

mschmitz
-is Member of Group: Trusted Users
-is Member of Group: SonicWALL Administrators
-is Member of Group: SSLVPN Services
-is Member of Group: LAN Access66
- Grants access rights to: WAN Primary IP
- Grants access rights to: LAN Primary Subnet

mschmitz (continued)

- Grants access rights to: WAN-GoogleDNS-8.8.8.8

External User Directories

Additional Information

When the number of local user accounts on a firewall exceeds a small threshold (typically around 10 users), managing identities directly on the firewall becomes inefficient, error-prone, and difficult to scale. In such environments, integrating an external user directory such as LDAP, RADIUS, or TACACS+ is strongly recommended.

1. Centralized User Management
External user directories provide a single source of truth for user identities.
- User accounts are created, modified, and deleted in one central system.
- Changes such as password updates or account deactivation apply immediately to all connected systems.
- Administrative effort is significantly reduced compared to maintaining users individually on each firewall.

This becomes increasingly important as user counts grow and staff changes occur more frequently.

2. Improved Security and Reduced Risk
Managing a growing number of local firewall users increases the risk of security gaps over time.
- Orphaned accounts may remain active after employees leave the organization.
- Password policies may be inconsistent or not enforced uniformly.
- Manual user administration increases the likelihood of configuration errors.

External authentication systems enforce consistent security policies, including password complexity, password rotation, account lockout rules, and—where supported—multi-factor authentication.

3. Better Scalability and Long-Term Maintainability
Firewalls are designed primarily for traffic inspection and policy enforcement, not for identity lifecycle management.
- Managing a small number of local users may be acceptable.
- Beyond approximately 10 users, administrative overhead grows disproportionately.
- External directories scale to dozens, hundreds, or thousands of users without increasing complexity on the firewall.

The firewall becomes a consumer of identity services rather than the owner of user data.

4. Role-Based Access Control (RBAC)
External user directories allow access rights to be assigned using groups instead of individual user accounts.
- Users are assigned to directory groups such as VPN users or firewall administrators.
- Firewall rules reference these groups instead of specific users.
- Access changes can be implemented without modifying firewall configuration.

This separation of identity management and authorization improves clarity, consistency, and operational efficiency.

5. Easier Auditing and Compliance
Security standards and internal policies often require clear traceability of user access.
External authentication systems provide centralized authentication logs, traceable login events, and clear accountability per user.

This significantly simplifies audits and supports compliance with frameworks such as ISO 27001, NIST, or internal governance requirements.

6. Seamless Integration with Existing Infrastructure
Most organizations already operate centralized identity systems.
- LDAP or Active Directory for user identities
- RADIUS for VPN and network access
- TACACS+ for administrative access control

Integrating the firewall into these systems avoids duplicate user databases and aligns firewall access with established IT processes.

7. Reduced Operational Errors
Manual user management on firewalls frequently leads to operational issues.
- Forgotten account removals
- Inconsistent permissions
- Configuration drift over time

Delegating authentication to an external system results in cleaner firewall configurations and reduces the risk of human error.

Conclusion
While local firewall users may be sufficient for very small environments, they do not scale effectively.
Once the number of users exceeds approximately 10, using an external user directory provides clear benefits in terms of security,

scalability, administrative efficiency, and auditability.

For medium and large environments, integrating LDAP, RADIUS, or TACACS+ is considered best practice and a fundamental requirement for sustainable and secure firewall operations.

Zones Report

Explanation

This Report shows Details about Zones

Zones Report

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

Number of records: 11

Maintenance Report

Explanation

The Maintenance Report helps identify configuration items that should be reviewed regularly to keep the firewall clean, efficient, and easy to manage. Over time, firewall configurations naturally grow as new rules, objects, VPNs, and services are added. Without periodic maintenance, obsolete or unused entries can accumulate, increasing administrative overhead and making troubleshooting more difficult.
This report highlights configuration elements that may require attention, such as disabled or unused firewall rules, inactive NAT policies, unused address and service objects, expired security services, and other configuration items that are no longer actively used. It also identifies settings that may benefit from optimization or cleanup.
The purpose of this report is not to recommend automatic removal of every listed item. Instead, it provides administrators with a structured overview of configuration components that should be verified before any changes are made. Some objects or rules may still be required for future projects, temporary environments, disaster recovery procedures, or infrequently used services.
Regular maintenance provides several important benefits:
- Reduces configuration complexity and improves readability.
- Makes troubleshooting and auditing significantly easier.
- Helps identify obsolete or forgotten configuration elements.
- Reduces the risk of accidental configuration errors.
- Improves long-term manageability of the firewall.
- Supports a well-documented and professionally maintained security environment.
A well-maintained firewall is easier to administer, easier to audit, and provides a stronger foundation for future configuration changes and security improvements.

Address Object Naming Conventions

Explanation

Importance of Common Naming Conventions for Address Objects
Effective management of firewall address objects is essential for maintaining a secure and well-organized network environment. One key factor contributing to this effectiveness is the use of consistent and meaningful naming conventions.

Clarity and Faster Administration
When address objects follow uniform naming standards, administrators can immediately recognize their purpose, location, or related service without reviewing detailed configuration data. This reduces time spent troubleshooting, updating rules, or making policy changes, and minimizes the chance of modifying the wrong object.

Consistency and Accuracy in Configuration
Standardized naming formats establish uniformity across all configurations. This prevents duplication, avoids confusion, and reduces misconfigurations that could lead to unwanted access permissions or blocked communication flows. Predictable names allow administrators to interpret firewall policies more efficiently and accurately.

Better Collaboration and Knowledge Transfer
Consistent naming conventions allow teams to work with shared understanding. Administrators who are not familiar with a configuration can still immediately interpret object usage and dependencies. This improves collaboration, simplifies onboarding of new personnel, and ensures continuity over time, even when responsibilities change.

Conclusion
Common naming conventions strengthen the maintainability, accuracy, and transparency of firewall configurations. By improving clarity, reducing configuration complexity, and fostering collaboration, they contribute significantly to secure and sustainable network administration.

Address Object Naming Conventions

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

Duplicate Address Objects

Explanation

Duplicate Address Object Analysis
Duplicate address objects—where different names refer to the same IP address or network—can introduce multiple operational and security challenges on firewalls.
1. Increased Complexity and Misconfiguration Risk
When multiple objects reference the same destination, administrators may not know which one to use. This complicates policy creation, increases the likelihood of using the wrong object, and slows down audits, troubleshooting, and change processes.
2. Conflicting or Overlapping Policies
Different objects representing the same IP may be used inconsistently across rules. One rule may allow traffic while another blocks it, resulting in unpredictable behavior and difficult policy analysis.
3. Inconsistent Security Enforcement
When different teams or administrators create separate objects for the same resource, policy enforcement becomes fragmented. This may lead to unintentional access or partial policy coverage, weakening overall security posture.
4. Increased Maintenance Effort
Any change affecting a duplicated object must be updated in all policy references. Missing a location can lead to outdated rules, gaps in access restrictions, or configuration drift.
Recommended Best Practices
– *Consolidate Address Objects:* Identify duplicate entries and replace them with a single object representing each IP, subnet, or resource.
– *Use Clear Naming Conventions:* Names should reflect purpose or resource identity, improving consistency and readability.
– *Perform Regular Audits:* Periodic cleanup reduces redundancy and improves policy quality.
– *Document Usage and Ownership:* Proper documentation helps during maintenance and prevents re-creation of unnecessary objects.

Cleaning up duplicate address objects improves rule clarity, simplifies policy administration, reduces operational mistakes, and contributes to a stronger and more predictable security configuration.

Duplicate Address Objects

IP	Name
- no records found -	

External Logging

Explanation

External logging/telemetry on a firewall (e.g., Syslog, IPFIX/NetFlow, SNMP traps) is important because the firewall is one of the few devices that can reliably observe who talked to whom, when, how, and what was blocked or allowed. Without exporting those signals, you're essentially operating blind: you may still be protected by policy, but you lose the ability to detect, investigate, and prove what happened.
From a security perspective, external logs are the foundation for incident detection and response. Attacks rarely announce themselves with a single obvious alarm. They show up as patterns—repeated login failures, VPN anomalies, policy hits, unexpected outbound connections, lateral movement, or traffic to suspicious destinations. A SIEM or log platform can correlate these patterns across sources (firewall + endpoints + identity + servers). The firewall's events often provide the first high-quality indicator that something is wrong, and flow telemetry (NetFlow/IPFIX) provides the "network narrative" needed to understand scope and impact.
External collection is also critical for forensics and accountability. Firewalls have limited local log retention and can lose data during reboots, updates, or storage rotation. Central logging preserves evidence over longer periods, supports legal/regulatory requirements, and enables reliable reporting. In practice, many investigations start days or weeks after the initial compromise. If logs were only kept locally, the key timeframe may already be gone.
Operationally, telemetry improves stability and troubleshooting. SNMP monitoring and traps provide early warning on CPU/memory pressure, interface errors, tunnel instability, or resource saturation—issues that can look like "random outages" unless you have time-series data. Flow records help validate bandwidth usage, identify top talkers, detect misconfigurations (e.g., asymmetric routing), and confirm whether a change in policy actually had the intended effect.
Finally, external logging/telemetry supports continuous improvement. It lets you measure policy effectiveness, tune rules that are too permissive or too noisy, and identify shadow IT or risky services. In short: exporting firewall logs and telemetry turns the firewall from a box that "blocks traffic" into a control you can verify, audit, and operationalize—which is the difference between having security controls and having security assurance.

External Logging

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

Disabled Firewall Rules

Explanation

Importance of Disabled Firewall Rules
Disabled firewall rules, although not actively enforcing security controls, still hold relevance within the firewall configuration and overall security strategy.
Operational Backup and Quick Re-Enablement
Disabled rules often serve as predefined configuration alternatives. Administrators may temporarily disable a rule during maintenance, troubleshooting, or planned changes and later re-enable it without redesigning or recreating the policy. This ensures fast restoration of intended security controls.
Configuration and Audit Documentation
Inactive rules provide insight into historical rule sets and previous security decisions. Keeping them visible supports audits, compliance verification, and forensic analysis by preserving configuration intent and change history.
Flexibility for Future Requirements
As network environments change, previously disabled rules may become relevant again. Retaining them allows quick reactivation or modification without recreating complex access policies or address objects from scratch.
Conclusion
While disabled firewall rules do not actively filter traffic, they are still useful reference points for operational recovery, documentation of previous configurations, and rapid adaptation to future security requirements. They should be reviewed periodically to ensure they remain valid, intentional, and aligned with current security objectives.

Disabled Firewall Rules

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc

- no records found -

Number of records: 0

Firewall Rules not used for a long time (IPv4)

Explanation

Firewall Rules Not Used for an Extended Period
Firewall rules that have not been used for a long period of time often indicate outdated access paths, decommissioned services, or legacy configurations that are no longer relevant. Keeping unused rules in place increases administrative overhead and may create unnecessary security exposure.

Inactive rules can be mistakenly reactivated or modified, potentially granting unintended access or weakening policy enforcement. Removing or disabling these rules helps maintain a clean rule base, improves manageability, and reduces the overall attack surface of the environment.

Regular review of unused rules ensures that only necessary and actively used access paths remain, supporting both operational efficiency and security best practices.

The following report shows rules not used for more than 365 days.

Firewall Rules not used for a long time (IPv4)

Ena	A	Name	SrcZone	DstZone	SrcNet	DstNet	SrcSvc	DstSvc	Last time hit
YES	A	Allow WAN1	LAN	WAN	KlausMeier	any	any	any	Firewall Rules not us...
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Firewall Rules not us...
YES	A	Test 24	WAN	060466	any	any	any	OSPF	Firewall Rules not us...
YES	A	Test 25	WAN	060466	any	any	any	POP3 (Retrieve E-Mail)	Firewall Rules not us...
YES	A	Test 23	WAN	060466	any	any	any	MSN	Firewall Rules not us...
YES	A	Allow WAN1	DMZ-unsec	WAN	any	any	Citrix UDP	any	Firewall Rules not us...
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	Firewall Rules not us...
YES	A	Test 22	DMZ-unsec	DMZ-sec	any	any	any	MSN	Firewall Rules not us...
YES	A	Complicated Rule	DMZ-unsec	Test	any	any	Citrix UDP	any	Firewall Rules not us...
YES	A	Allow WAN1	DMZ-sec	WAN	any	any	Enhanced TV	any	Firewall Rules not us...
YES	A	My Rule	DMZ-sec	DMZ-unsec	any	any	any	FTP Data	Firewall Rules not us...
YES	A	Test 17	DMZ-sec	DMZ-unsec	any	any	any	HTTPS	Firewall Rules not us...
YES	A	Test 20	DMZ-sec	DMZ-unsec	any	any	any	Kazaa / FastTrack	Firewall Rules not us...
YES	A	Test 21	DMZ-sec	DMZ-unsec	any	any	any	Lotus Notes	Firewall Rules not us...
YES	A	Test 19	DMZ-sec	DMZ-unsec	any	any	any	IKE	Firewall Rules not us...
YES	A	Test 18	DMZ-sec	DMZ-unsec	any	any	any	ICMP	Firewall Rules not us...
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	Firewall Rules not us...
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	Firewall Rules not us...
YES	A	Allow Citrix	any		any	any	Citrix UDP	any	Firewall Rules not us...
YES	A	Allow FTP	any		any	any	FTP	any	Firewall Rules not us...
YES	A	Allow management via ...	SSLVPN	LAN	SSLVPN-NetExtender Range	any	any	HTTPS Management	2025-03-31 11:40:59

- Auto-added rules are excluded from this report

Number of records: 21

Disabled NAT (Network Address Translation) policies (IPv4)

Explanation

Disabled NAT Policies and Their Impact
Disabled NAT (Network Address Translation) policies on firewalls can introduce significant operational and security-related issues within a network. Below is an overview of the main risks and technical implications associated with inactive or removed NAT rules.

1. Loss of Network Segmentation
NAT policies support logical separation between internal and external networks by translating internal IP addresses before traffic leaves the network.
Potential risks:
– *Exposure of Internal IPs:* Without NAT, internal addressing schemes may be visible externally, making previously isolated devices reachable.
– *Reduced Isolation Between Zones:* NAT supports isolation between LAN, DMZ, and WAN segments. Disabled NAT can unintentionally blur security boundaries.

2. Increased Security Risks
NAT indirectly provides a layer of security by preventing unsolicited inbound connections toward internal hosts.
Possible consequences:
– Attackers can directly target internal devices
– Firewall-based restrictions may be bypassed
– Internal resources become easier to enumerate or scan

3. Communication Breakdowns
Many network communication flows assume that NAT is active for translation and routing.
When NAT is disabled:
– Devices may lose access to external services
– Users may experience inconsistent connectivity
– Troubleshooting becomes more complex due to routing failures or unreachable services

4. Issues with Multi-Network and VPN Connectivity
VPNs, routing, and remote access technologies often depend on NAT to align internal and external address spaces.
Key risks:
– Remote access sessions may fail
– Network overlap may occur when IP spaces conflict
– External systems cannot route return traffic correctly

5. Challenges in Policy Enforcement and Monitoring
Access-control logic frequently leverages NAT to track and categorize flows.
Consequences of disabled NAT include:
– Reduced ability to monitor or correlate traffic
– Difficulty in attributing activity to specific devices/users
– Gaps in logging accuracy

6. Higher Consumption of Public IP Space
NAT allows many internal devices to share one or a small pool of public IP addresses.
Without NAT:
– Each system may require its own routable IP
– IPv4 exhaustion becomes a real operational concern

Conclusion
Disabled NAT policies can cause unexpected routing failures, weakened protection boundaries, and increased security exposure. In most environments, NAT serves not only for address translation but also as a method for enforcing isolation, logging visibility, and predictable routing behavior. For stable and secure operations, NAT policies should be reviewed carefully, properly maintained, and disabled only in intentional and well-controlled design scenarios.

- Auto-added rules are excluded from this report

Disabled NAT (Network Address Translation) policies (IPv4)

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

NAT Policies that are enabled and have no hits (IPv4)

Explanation

NAT Policies with No Traffic Hits
This report highlights NAT (Network Address Translation) policies that are currently enabled but have not been used within the monitored timeframe. A NAT policy without any recorded hits typically indicates that the rule no longer corresponds to active traffic flows or is associated with services, networks, or devices that are no longer in use.

Possible Causes for Unused NAT Policies
– The corresponding service is no longer active
– A device or network reference has changed
– Routing was redesigned, making this NAT translation obsolete
– A temporary or migration-related rule was never removed

Why Unused NAT Policies Matter
1. Increased Policy Complexity
Unused NAT entries make the configuration harder to understand and maintain. Administrators may spend additional time evaluating rules that are no longer relevant, slowing down troubleshooting and change management.

2. Risk of Accidental Activation
A dormant NAT policy may become active if network conditions change or routing shifts. This could inadvertently expose internal devices, alter address mappings, or bypass intended access policies.

3. Potential Security Exposure
Even if unused, a NAT rule still defines a possible translation path. If activated unintentionally, it may:
– reveal internal addressing
– enable unwanted inbound or outbound connections
– bypass expected filtering or inspection points

4. Reduced Operational Efficiency
Large NAT rule sets increase administrative workload and reduce configuration clarity. Removing obsolete entries results in a cleaner, more predictable policy set and lowers operational risk.

Recommended Maintenance Practices
– Periodically verify whether NAT rules are still needed
– Document rule ownership and intended purpose
– Remove unused mappings or disable them temporarily for validation
– Review NAT policies after network redesigns, migrations, or decommissioning activities

Conclusion
Enabled NAT policies without traffic activity often indicate outdated or unnecessary configuration objects. Cleaning up unused rules reduces complexity, prevents unintended exposure paths, and improves maintainability and security posture. Regular review ensures that the firewall policy accurately reflects required and active network behavior.

- Auto-added rules are excluded from this report

NAT Policies that are enabled and have no hits (IPv4)

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 Settings

Explanation

This section checks whether the WAN MTU setting on the SonicWall firewall is configured unusually low.
An MTU value that is set too low can reduce transmission efficiency and may negatively affect network performance.
If such a setting is detected, it should be reviewed to confirm that it is technically required and not the result of an unnecessary configuration limitation.

X1	WAN	1500	ok	-
X5	WAN	1500	ok	-