Security Audit

Appliance Details

Serial-Number:	0040XXXXXXXX (Demo)
Firewall Name:	UDS-NSV270
Appliance Model:	SonicWall NSv 270
Uptime:	0 Days, 6 Hours, 44 Minutes, 47 Seconds
Firmware Version:	7.3.0-7012-R8150

Report Details

Date & Time Report created:	06.10.2025 - 18:11:35
EXP File:	C:\U...\Repository\0040XXXXXXXX\exp_api_downloaded.exp
EXP Timestamp:	06.10.2025 17:51
TSR File:	C:\U...\Repository\0040XXXXXXXX\tsr_api_downloaded.wri
TSR Timestamp:	06.10.2025 17:51

Security Services General Status

Explanation

This report shows which Security Services are enabled. This only indicates if the technology has been enabled, it does not mean the Services are effectively analyzing traffic, because they additionally need to be assigned per Zone or Rule.

Security Services General Status	
Gateway AntiVirus:	on
Intrusion Detection and Prevention:	on
Geo IP:	off
Anti-Spyware:	on
Botnet Filter:	off
Application Control:	on
Content Filter:	on
DPI SSL (Client):	off
DPI SSL (Server):	off
DPI SSH:	on

Explanation

DPI SSH: on

There is no route all VPN Tunnel configured and enabled. This is a common scenario where all the traffic is routed via an upstream Security Device that takes care of traffic inspection.

Security Services per Zone

Explanation

This report shows which Security Services are enabled on which Zone.

Security Services per Zone

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

Security Services License Check

Explanation

This report shows if services have an active license

Security Services License Check

Service Name	License Status	Count	Expiration
Model Upgrade	Not Licensed		
NSM Essential	Not Licensed		
NSM Advanced	Licensed		30 Jan 2026
Gateway Anti-malware/Intrusion Prevention/App Control	Licensed		16 Feb 2026
Capture Client Basic	Not Licensed		
Capture Client Advanced	Not Licensed		
Capture Client Premier	Not Licensed		
Content Filtering Service	Licensed		16 Feb 2026
SSL VPN	Licensed	2 Max: 100	
Global VPN Client	Licensed	50 Max: 1000	
Stateful High Availability	Licensed		
Capture Advanced Threat Protection	Licensed		16 Feb 2026
Syslog Analytics	Expired		03 Feb 2024
DNS Filtering	Licensed		30 Jan 2026
Essential Protection Service Suite	Licensed		16 Feb 2026
Advanced Protection Security Suite	Not Licensed		
Managed Protection Security Suite	Not Licensed		
24x7 Support	Licensed		16 Feb 2026
Standard Support	Not Licensed		

Firewall Management Access

Explanation

There are multiple ways to grant access to firewall management, each with its own set of advantages and potential vulnerabilities. Because management access can pose significant security risks, it is crucial to carefully review and control which methods are enabled. Unauthorized access to firewall management can lead to configuration changes, exposure of sensitive information, and potential network breaches. Therefore, ensuring that only secure and necessary management access methods are enabled is a key aspect of maintaining network security.

Central Management	
Central Management (NSM / GMS):	off

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

API	
API access:	enabled

Firewall Management Access

Interface HTTP / HTTPS / SNMP / SSH Management **Page: 1/1**

Interface	Zone	HTTP	HTTPS	PING	SSH	SNMP
X0	LAN	off	on	on	on	on
X1	WAN	off	on	on	on	off
X2	DMZ-unsec	off	on	on	off	off
X3	DMZ-sec	off	on	on	off	off
X4	<unconfigured>	off	off	off	off	off
X5	WAN	off	off	on	off	off
X6	LAN	off	on	on	off	off
X7	<unconfigured>	off	off	off	off	off

Firewall Management Access

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

Management Rules (IPv4)

Explanation

Firewall rules that permit management services such as SSH (Secure Shell), HTTPS (Hypertext Transfer Protocol Secure), and others to be accessed from untrusted networks pose significant security risks. These services are designed for administrators to configure and manage the device, and they often provide high levels of access and control over the system.

Here are the key reasons why such rules are risky:

Exposure to Attacks: Allowing management services to be accessed over the Internet exposes them to a wide range of attacks, such as brute force attacks to guess passwords, exploits targeting vulnerabilities in the management software, or DDoS attacks to overwhelm the service.

Elevation of Privilege: If an attacker successfully gains access to a management service, they may achieve a level of privilege similar to that of an administrator. This could lead to a full system compromise where an attacker can alter firewall rules, create backdoors, or disrupt network traffic.

Sniffing and Eavesdropping: Unencrypted management protocols can allow attackers to intercept traffic and gain sensitive information. Even encrypted services can be at risk if there are flaws in the encryption implementation or if keys are mishandled.

Lack of Monitoring: Management interfaces are not always monitored as rigorously as other systems, potentially allowing malicious activity to go unnoticed.

Complexity and Human Error: The more complex the rules and the more services that are exposed, the higher the chance of misconfiguration or human error, which can introduce vulnerabilities.

To mitigate these risks, management access should be restricted to trusted networks only. When remote management is necessary, it should be done through secure methods such as VPNs (Virtual Private Networks) with strong encryption, and multi-factor authentication should be used to enhance security. Additionally, management interfaces should be monitored for unauthorized access attempts, and software should be kept up-to-date with patches to protect against known vulnerabilities.

Management Rules (IPv4)

Explanation

These are the Service Objects and Groups that are considered as Management Services.

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	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
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 Maintenance...

Management Rules (IPv6)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
--- No records found ---									

Users with Administrative Rights

Explanation

This report shows all users with admin rights.

Users with Full Admin Rights

mschmitz

Webadmin

LocalAdmin

Uwe

apiuser

UDS-SNWL-Admins@uds.local

Users with Limited Admin Rights

- no entries -

Users with Read-Only Admin Rights

Udo

Users with Guest Admin Rights

Robert

Silvia

Summary

Note that if admin-rights are assigned to LDAP Groups, all members of the LDAP Groups inherit those admin rights!

Users and Group Membership

Explanation

This report details all users and their respective group memberships, highlighting the effective VPN access rights granted to them through these group affiliations.

Users in Groups

All LDAP Users

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

Silvia

- 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 VPN access rights to: - WAN Primary IP
- Grants VPN access rights to: - LAN Primary Subnet
- Grants VPN 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 VPN access rights to: - WAN Primary IP
- Grants VPN access rights to: - LAN Primary Subnet
- Grants VPN access rights to: - WAN-GoogleDNS-8.8.8.8

Users VPN Access Rights assigned

Explanation

This report shows the access rights to network objects assigned to users

Users VPN Access Rights assigned

User: Isabel

- 060466 Subnets
- 150971-Test Interface IP
- DEAG_Test

User: LocalAdmin

- LAN Subnets

User: Webadmin

- LAN Primary Subnet

User: mschmitz

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

Users account protection

Explanation

This report lists all users and if TOTP (time-based one-time-password) is enabled for that user

User-Name	TOTP Enabled
admin	**NO**
mschmitz	NO
All LDAP Users	NO
Webadmin	NO
LocalAdmin	YES
Robert	NO
Isabel	NO
Silvia	NO
Udo	NO
Uwe	NO
apiuser	NO

VPN Policy Crypto Settings Audit

Explanation

Best Practices for 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 broken with modern computing power.
Compliance: Many industries require strong encryption to meet regulatory standards.
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 not only improve 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 broken and no longer secure.
Key Management: Weak or static pre-shared keys (PSKs) are easily guessed or brute-forced.

Recommended Secure Choices

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 over PSKs; if PSKs are used, generate 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, maintain compliance, and prepare your network for future challenges. Regularly review and update your VPN configuration to stay secure.

VPN Policy Crypto Settings Audit

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
no	Bad Tunnel	IKEv2	192-Bit R ECP Group	3DES (!)	MD5 (!)	ESP	AES-192 (C)	SHA384 (C)	on	Group 1 (C)
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 (!)
no	SNWL Policy Mode	IKEv2	521-Bit R ECP Group	AESCGM16-256 (C)	SHA-1 (!)	ESP	None (!)	MD5 (C)	on	384-Bit R ECP Group
no	Test	IKEv2	Group 2 (!)	AES-128 (C)	SHA-1 (!)	AH (C)	AESCGM16-256	SHA-256 (C)	off (!)	Group 2 (!)
yes	To TZ570	IKEv2	Group 1 (!)	AES-256	SHA-1 (!)	ESP	AES-256	n/a	on	n/a
no	WAN GroupVPN	Aggressive (!)	Group 14	AES-256	SHA-512	ESP	AES-256	AES-XCBC (C)	on	Group 14

VPN 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

ANY-ANY Rules (IPv4)

Explanation

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.

Note: Auto-added rules are excluded from this report

ANY-ANY Rules (IPv4)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
YES	A	Rule10	DMZ-sec	Test	any	any	Echo	any	
YES	A	Rule6	DMZ-sec	Test	any	any	IDENT	any	
YES	A	Rule7	DMZ-sec	Test	any	any	IPcomp	any	
YES	A	Rule8	DMZ-sec	Test	any	any	Inverse Neighbor Discovery...	any	
YES	A	Rule9	DMZ-sec	Test	any	any	Lotus Notes	any	
YES	A	Rule10	DMZ-sec	Test	any	any	MMS UDP	any	
YES	A	Rule11	DMZ-sec	Test	any	any	Megaco Binary H.248 UDP	any	
YES	A	Rule12	DMZ-sec	Test	any	any	Mobile Prefix Advertisemen...	any	
YES	A	Allow syslog	DMZ-unsec	DMZ-sec	any	any	HTTPS Management	any	
YES	A	Allow syslog	DMZ-unsec	Test	any	any	Syslog	any	
YES	A	Test a/a	any		any	any	Citrix UDP	any	

Note: Auto-added rules are excluded from this report

ANY-ANY Rules (IPv6)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
--- No records found ---									

Rules never used (IPv4)

Explanation

Managing Unused Firewall Rules:

Firewall rules that have never been used can introduce unnecessary complexity and potential risks to a network. These rules, whether created during initial configurations or added over time for anticipated scenarios, can remain dormant, cluttering the firewall policy without ever facilitating traffic. Here's why addressing them is important:

Unnecessary Complexity: Unused rules add clutter to the firewall policy, making it more difficult to manage and troubleshoot. This complexity can slow down auditing and rule modification efforts, increasing the chance of human error during rule management.

Performance Impact: Even though unused rules may not process traffic, they still need to be evaluated by the firewall when checking for matches in the rule set. In environments with extensive rule sets, this can lead to slight performance degradation, particularly as the number of rules grows.

Security Risks: Dormant rules can become vulnerabilities. In some cases, unused rules may unintentionally provide openings for unauthorized traffic if they were misconfigured or forgotten about. Hackers might exploit these hidden rules, especially if they have broader permissions than necessary.

Audit and Compliance Concerns: Firewalls need to comply with security policies and regulations. Unused rules can create ambiguities and make it difficult to prove that all rules are necessary and serve a defined purpose, which could raise issues during audits.

Best Practices for Handling Unused Rules:
Regular Audits: Periodically review all firewall rules to identify which ones are not being used. Automated tools or firewall monitoring logs can help detect unused rules based on traffic patterns.

Rule Expiration Policy: Implement a policy where rules expire after a certain period if they are not used. This encourages administrators to actively review and remove old, unused rules.

Tagging and Documentation: Properly tag and document each rule with its purpose, creator, and date of implementation. This helps identify and justify the existence of each rule during audits and reviews.

Graceful Removal: When a rule is identified as unused, remove it carefully. Before deleting, consider disabling it first and monitoring the network to ensure that no critical services are affected.

Cleaning up unused firewall rules enhances the security, performance, and manageability of the network, ensuring that the firewall remains optimized and responsive to both current and future security needs.

Note: Auto-added rules are excluded from this report

Rules never used (IPv4)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	
YES	A	Rule7	DMZ-sec	Test	any	KlausMeier	DHCP Server	any	
YES	A	Rule10	DMZ-sec	Test	any	any	Echo	any	
YES	A	Rule6	DMZ-sec	Test	any	any	IDENT	any	
YES	A	Rule7	DMZ-sec	Test	any	any	IPcomp	any	
YES	A	Rule8	DMZ-sec	Test	any	any	Inverse Neighbor Discovery...	any	
YES	A	Rule9	DMZ-sec	Test	any	any	Lotus Notes	any	
YES	A	Rule10	DMZ-sec	Test	any	any	MMS UDP	any	
YES	A	Rule11	DMZ-sec	Test	any	any	Megaco Binary H.248 UDP	any	
YES	A	Rule12	DMZ-sec	Test	any	any	Mobile Prefix Advertisemen...	any	
YES	A	Rule9	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	DNS (Name Service)	any	
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	
YES	A	Rule6	DMZ-sec	Test	KlausMeier	Test13	Citrix	any	
YES	A	Allow syslog	DMZ-unsec	DMZ-sec	any	any	HTTPS Management	any	
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	
YES	A	Allow syslog	DMZ-unsec	Test	any	any	Syslog	any	
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	Temp, Rule to allow Maintenance...
YES	A	Test a/a	any		any	any	Citrix UDP	any	

Note: Auto-added rules are excluded from this report

Rules never used (IPv6)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
--- No records found ---									

Rules WAN to internal networks (IPv4)

Explanation

Allowing inbound traffic from the internet to local networks through firewall rules poses significant security risks. Here are some potential problems that can arise from such configurations:

Increased Exposure to External Threats: By allowing internet traffic into the local network, organizations open themselves up to a variety of attacks. Hackers can exploit vulnerabilities in publicly exposed services, leading to unauthorized access, data breaches, or even complete system takeovers. The more services and ports exposed, the larger the attack surface.

Risk of Malware and Ransomware Infections: Malicious actors can introduce malware, including ransomware, into internal systems by exploiting open ports and services. Once inside the network, the malware can spread rapidly, encrypt files, and demand a ransom for their release, or disrupt critical services.

Lack of Segmentation: Poorly defined firewall rules might not segment the network properly. This means that once attackers gain access through an exposed service, they might move laterally within the network, accessing sensitive data or further compromising other systems.

Misconfigurations and Human Error: Incorrectly configured rules can inadvertently allow more traffic than intended. For example, an open rule might allow not just the specific service that needs access, but also other protocols and services that dont need to be exposed, thereby increasing risk.

Denial of Service (DoS) Attacks: Open inbound rules could allow attackers to flood network resources with excessive traffic, overwhelming them and causing legitimate services to be unavailable. This can lead to significant downtime and affect business operations.

Vulnerability to Zero-Day Attacks: Firewall rules that allow traffic into the network could also make it easier for zero-day vulnerabilities (unknown and unpatched flaws in software) to be exploited. Attackers often scan exposed services looking for such flaws to exploit.

Insufficient Logging and Monitoring: In many cases, firewall rules that allow inbound traffic dont have proper logging and monitoring set up. This makes it difficult to detect suspicious activity or respond quickly to incidents.

Mitigation Strategies
Least Privilege Principle: Only allow traffic that is absolutely necessary, and block all other inbound traffic by default.
Use of VPNs: Restrict access to local networks via Virtual Private Networks (VPNs) instead of exposing services directly to the internet.
Regular Audits: Continuously audit and review firewall rules to ensure they are up to date and only permit legitimate traffic.
Intrusion Detection Systems (IDS): Implement IDS or Intrusion Prevention Systems (IPS) to detect and block suspicious traffic that gets through firewall rules.
Carefully managing firewall rules is essential to maintaining network security. Properly configured firewalls reduce exposure to potential cyberattacks and protect critical internal assets from internet-based threats.

Note: Auto-added rules are excluded from this report

Rules WAN to internal networks (IPv4)

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

Note: Auto-added rules are excluded from this report

Rules WAN to internal networks (IPv6)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
--- No records found ---									

Disabled Firewall Rules (IPv4)

Explanation

Disabled firewall rules, although temporarily inactive, still hold importance within the network security framework. While these rules may not actively filter or monitor network traffic, they serve as valuable components of the firewall configuration for several reasons.

Firstly, disabled firewall rules act as a backup or contingency plan for network administrators. In certain situations, such as during troubleshooting, maintenance activities, or planned changes, administrators may need to temporarily disable specific rules to accommodate legitimate network traffic or avoid unintended disruptions. Having these rules readily available allows administrators to quickly re-enable them when necessary, restoring the intended security posture without the need for extensive reconfiguration.

Secondly, disabled firewall rules serve as documentation of past configurations and security policies. By preserving these rules in a disabled state, network administrators maintain a historical record of previous security measures and decision-making processes. This documentation can be invaluable for auditing purposes, compliance assessments, or forensic investigations, providing insights into the evolution of the networks security posture over time.

Additionally, disabled firewall rules offer flexibility and agility in adapting to changing security requirements. As network environments evolve and new threats emerge, administrators may need to adjust firewall policies to address emerging risks or compliance mandates. By keeping unused rules disabled rather than permanently deleting them, administrators retain the option to reactivate or modify these rules in response to evolving security needs, ensuring the firewall remains adaptable and responsive to emerging threats.

In conclusion, while disabled firewall rules may not actively enforce security policies, they play a significant role in network security management by providing backup options, documenting past configurations, and facilitating agility in response to changing security requirements. Network administrators should carefully manage and periodically review disabled rules to ensure they align with current security objectives and operational needs.

Disabled Firewall Rules (IPv4)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
--- No records found ---									

Disabled Firewall Rules (IPv6)

Ena	Act	Name	SRC Zone	DST Zone	SRC Address	DST Address	SRC Service	DST Service	Comment
--- No records found ---									

Firewall Rules not used for a long time (IPv4)

Explanation

Disabled firewall rules, although temporarily inactive, still hold importance within the network security framework. While these rules may not actively filter or monitor network traffic, they serve as valuable components of the firewall configuration for several reasons.

Firstly, disabled firewall rules act as a backup or contingency plan for network administrators. In certain situations, such as during troubleshooting, maintenance activities, or planned changes, administrators may need to temporarily disable specific rules to accommodate legitimate network traffic or avoid unintended disruptions. Having these rules readily available allows administrators to quickly re-enable them when necessary, restoring the intended security posture without the need for extensive reconfiguration.

Secondly, disabled firewall rules serve as documentation of past configurations and security policies. By preserving these rules in a disabled state, network administrators maintain a historical record of previous security measures and decision-making processes. This documentation can be invaluable for auditing purposes, compliance assessments, or forensic investigations, providing insights into the evolution of the networks security posture over time.

Additionally, disabled firewall rules offer flexibility and agility in adapting to changing security requirements. As network environments evolve and new threats emerge, administrators may need to adjust firewall policies to address emerging risks or compliance mandates. By keeping unused rules disabled rather than permanently deleting them, administrators retain the option to reactivate or modify these rules in response to evolving security needs, ensuring the firewall remains adaptable and responsive to emerging threats.

In conclusion, while disabled firewall rules may not actively enforce security policies, they play a significant role in network security management by providing backup options, documenting past configurations, and facilitating agility in response to changing security requirements. Network administrators should carefully manage and periodically review disabled rules to ensure they align with current security objectives and operational needs.

Scope

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

Note: Auto-added rules are excluded from this report

Firewall Rules not used for a long time (IPv4)

Ena	A	SrcZone	DstZone	Src Zone	Dst Zone	Svc	Dst Addr	Src Service	Last time hit
YES	A	Heating Maintenance	WAN	LAN	any	LAN Subnets	any	SSH	never
YES	A	Allow syslog	DMZ-unsec	DMZ-unsec	any	any	SSH Management	any	never
YES	A	Allow syslog	DMZ-unsec	DMZ-sec	any	any	HTTPS Management	any	never
YES	A	Allow syslog	DMZ-unsec	Test	any	any	Syslog	any	never
YES	A	Rule6	DMZ-sec	Test	any	Test13	Citrix TCP	any	never
YES	A	Rule7	DMZ-sec	Test	any	KlausMeier	DHCP Server	any	never
YES	A	Rule10	DMZ-sec	Test	any	any	Echo	any	never
YES	A	Rule6	DMZ-sec	Test	any	any	IDENT	any	never
YES	A	Rule7	DMZ-sec	Test	any	any	IPcomp	any	never
YES	A	Rule8	DMZ-sec	Test	any	any	Inverse Neighbor Disc...	any	never
YES	A	Rule9	DMZ-sec	Test	any	any	Lotus Notes	any	never
YES	A	Rule10	DMZ-sec	Test	any	any	MMS UDP	any	never
YES	A	Rule11	DMZ-sec	Test	any	any	Megaco Binary H.248 UDP	any	never
YES	A	Rule12	DMZ-sec	Test	any	any	Mobile Prefix Adverti...	any	never
YES	A	Rule9	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	DNS (Name Service)	any	never
YES	A	Rule10	DMZ-sec	Test	WAN-GoogleDNS-8.8.8.8	any	Direct Connect	any	never
YES	A	Rule6	DMZ-sec	Test	KlausMeier	Test13	Citrix	any	never
YES	A	Test a/a	any		any	any	Citrix UDP	any	never

Note: Auto-added rules are excluded from this report

Firewall Rules not used for a long time (IPv6)

Ena	A	SrcZone	DstZone	Src Zone	Dst Zone	Svc	Dst Addr	Src Service	Last time hit

--- No records found ---

Nat Policies disabled (IPv4)

Explanation

Disabled NAT (Network Address Translation) policies on firewalls can pose significant operational and security issues within a network. Here is a detailed explanation of the potential impacts:

1. Loss of Network Segmentation
NAT policies play a crucial role in translating private IP addresses to public ones, allowing internal devices to communicate with the outside world while maintaining network segmentation. When NAT policies are disabled:

Direct Exposure of Internal IPs: Without NAT, internal IP addresses may be exposed to external networks, which could lead to attacks targeting devices that were intended to remain isolated.
Lack of Isolation: NAT helps in isolating traffic between different network zones (e.g., internal, DMZ, and external networks). Disabling it can blur the boundaries between these zones, weakening overall security.
2. Increased Security Risks
Direct Attacks on Internal Systems: NAT policies typically mask internal IP addresses, providing an extra layer of security. Disabled NAT policies can allow attackers to directly target internal devices with malicious traffic.
Bypassing of Security Controls: Many security controls rely on NAT policies to enforce restrictions on incoming or outgoing traffic. Disabling NAT might lead to bypassing these controls, making it easier for unauthorized traffic to enter the network.
3. Communication Breakdowns
Internal Systems Losing Connectivity: NAT enables devices within the network to share a single public IP for internet access. If NAT policies are disabled, internal systems may lose their ability to communicate with external networks or services because of IP conflicts or routing issues.
Complex Troubleshooting: Without NAT, misconfigurations might arise where some devices can access external resources while others cannot. This can lead to increased troubleshooting complexity and downtime.
4. Interference with Multi-Network Communication
Issues in VPNs and Remote Access: Many remote access systems, like VPNs, rely on NAT policies to map traffic between different networks. Disabling NAT could break these configurations, disrupting communication for remote users.
IP Conflicts: Disabling NAT can result in overlapping IP address spaces when multiple internal networks attempt to communicate, leading to network traffic confusion or blockages.
5. Challenges with Policy Enforcement
Access Control and Monitoring: NAT policies help enforce access control policies by mapping internal traffic to specific external addresses or ranges. Without it, administrators may struggle to enforce consistent access control or monitor traffic effectively.
Reduced Auditability: NAT allows for logging of network traffic in a structured and manageable way. Disabling it can make it harder to track and log traffic, reducing visibility and the ability to respond to incidents.
6. Public IP Address Exhaustion
High Demand for Public IPs: NAT allows multiple devices in a network to share a limited number of public IP addresses. Disabling NAT may require assigning public IPs to every device that needs internet access, quickly exhausting the available public IP pool, especially with IPv4 addressing.
Conclusion
Disabled NAT policies can lead to numerous security vulnerabilities, operational issues, and communication breakdowns within a network. It is essential to carefully consider the use of NAT as a security and traffic management tool and ensure that its policies are configured properly to maintain secure and efficient network operations.

Note: Auto-added rules are excluded from this report

Nat Policies disabled (IPv4)

Ena	Name	Original Source	Translasted Source	Original Destination	Translated Destination	Original Service	Translated Service
None	Default NAT Policy	Default NAT Policy	Default NAT Policy	Default NAT Policy	Default NAT Policy	Default NAT Policy	Default NAT Policy

Note: Auto-added rules are excluded from this report

Nat Policies disabled (IPv6)

Ena	Name	Original Source	Translasted Source	Original Destination	Translated Destination	Original Service	Translated Service
--- No records found ---							

Nat Policies never used (IPv4)

Explanation

The Report shows NAT Policies that are enabled and have no hits (meaning have never been used).
Disabled NAT (Network Address Translation) policies on firewalls can pose significant operational and security issues within a network. Heres a detailed explanation of the potential impacts:

1. Loss of Network Segmentation
NAT policies play a crucial role in translating private IP addresses to public ones, allowing internal devices to communicate with the outside world while maintaining network segmentation. When NAT policies are disabled:

Direct Exposure of Internal IPs: Without NAT, internal IP addresses may be exposed to external networks, which could lead to attacks targeting devices that were intended to remain isolated.
Lack of Isolation: NAT helps in isolating traffic between different network zones (e.g., internal, DMZ, and external networks). Disabling it can blur the boundaries between these zones, weakening overall security.
2. Increased Security Risks
Direct Attacks on Internal Systems: NAT policies typically mask internal IP addresses, providing an extra layer of security. Disabled NAT policies can allow attackers to directly target internal devices with malicious traffic.
Bypassing of Security Controls: Many security controls rely on NAT policies to enforce restrictions on incoming or outgoing traffic. Disabling NAT might lead to bypassing these controls, making it easier for unauthorized traffic to enter the network.
3. Communication Breakdowns
Internal Systems Losing Connectivity: NAT enables devices within the network to share a single public IP for internet access. If NAT policies are disabled, internal systems may lose their ability to communicate with external networks or services because of IP conflicts or routing issues.
Complex Troubleshooting: Without NAT, misconfigurations might arise where some devices can access external resources while others cannot. This can lead to increased troubleshooting complexity and downtime.
4. Interference with Multi-Network Communication
Issues in VPNs and Remote Access: Many remote access systems, like VPNs, rely on NAT policies to map traffic between different networks. Disabling NAT could break these configurations, disrupting communication for remote users.
IP Conflicts: Disabling NAT can result in overlapping IP address spaces when multiple internal networks attempt to communicate, leading to network traffic confusion or blockages.
5. Challenges with Policy Enforcement
Access Control and Monitoring: NAT policies help enforce access control policies by mapping internal traffic to specific external addresses or ranges. Without it, administrators may struggle to enforce consistent access control or monitor traffic effectively.
Reduced Auditability: NAT allows for logging of network traffic in a structured and manageable way. Disabling it can make it harder to track and log traffic, reducing visibility and the ability to respond to incidents.
6. Public IP Address Exhaustion
High Demand for Public IPs: NAT allows multiple devices in a network to share a limited number of public IP addresses. Disabling NAT may require assigning public IPs to every device that needs internet access, quickly exhausting the available public IP pool, especially with IPv4 addressing.
Conclusion
Disabled NAT policies can lead to numerous security vulnerabilities, operational issues, and communication breakdowns within a network. It is essential to carefully consider the use of NAT as a security and traffic management tool and ensure that its policies are configured properly to maintain secure and efficient network operations.

Note: Auto-added rules are excluded from this report

Nat Policies never used (IPv4)

Ena	Name	Original Source	Translasted Source	Original Destination	Translated Destination	Original Service	Translated Service
None	Default NAT Policy	Default NAT Policy	Default NAT Policy	Default NAT Policy	Default NAT Policy	Default NAT Policy	Default NAT Policy

Note: Auto-added rules are excluded from this report

Nat Policies never used (IPv6)

Ena	Name	Original Source	Translasted Source	Original Destination	Translated Destination	Original Service	Translated Service
--- No records found ---							

Audit Settings Report

Explanation

This is the audit report, it lists all Audit Events that are found in the Technical Support Report (TSR). It shows which changes have been made on the firewall by which user.
Attention: SonicWall does not synchronize Audit Data if High Availablility is used!

Audit Details

Auditing:	on
Audit Records found in TS-Report:	2000
Newest Audit entry found in TS-Report:	30.09.2025 10:52
Oldest Audit entry found in TS-Report:	08.09.2025 19:13

Users appearing in Audit Log

- admin
- apiuser
- HA Sync

Summary

User 'admin' is present in SNWL_Audit. The recommendation is only to use personalized user accounts for firewall-management so there is an option to retrace who made changes!

Comment: HA Sync is an internal user for synchronizing HA-Settings