Full Report

Appliance Details

Serial-Number:	0040XXXXXXXX (Demo)
Firewall Name:	UDS-NSV270
Appliance Model:	SonicWall NSv 270
Uptime:	9 Days, 16 Hours, 22 Minutes, 19 Seconds
Firmware Version:	7.1.1-7047-R5557

Report Details

Date & Time Report created:	19.10.2024 - 16:29:34
Repository Directory:	C:\Users\ms\AppData\Roaming\FirewallToolbox\Repository
EXP File:	C:\U...\Repository\0040XXXXXXXX\exp_api_downloaded.exp
EXP Timestamp:	19.10.2024 13:35
TSR File:	C:\U...\Repository\0040XXXXXXXX\tsr_api_downloaded.wri
TSR Timestamp:	19.10.2024 14:01

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 SSH:	on

Explanation

SSL-Decryption is disabled. If there are no other technologies in place that decrypt HTTPS traffic, the firewall is blind to most of the traffic and security services like Gateway AV, IPS etc. do not work for most of the traffic.

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		31 Jan 2025
Gateway Anti-malware/Intrusion Prevention/App Control	Licensed		16 Feb 2025
Capture Client Basic	Not Licensed		
Capture Client Advanced	Not Licensed		
Capture Client Premier	Not Licensed		
Content Filtering Service	Licensed		16 Feb 2025
SSL VPN	Licensed	2 Max: 100	
Global VPN Client	Licensed	50 Max: 1000	
Stateful High Availability	Licensed		
Capture Advanced Threat Protection	Licensed		16 Feb 2025
Syslog Analytics	Expired		03 Feb 2024
DNS Filtering	Licensed		31 Jan 2025
Essential Protection Service Suite	Licensed		16 Feb 2025
Advanced Protection Service Suite	Not Licensed		
24x7 Support	Licensed		16 Feb 2025
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.

Interface HTTP / HTTPS / SNMP / SSH Management

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	<unconfigured>	off	off	off	off	off
X7	<unconfigured>	off	off	off	off	off

IPSec (VPN)

IPSec: **enabled**

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

SSL-VPN

SSL VPN Web Management:	off
SSL VPN SSH Management:	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	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	Ping	Auto-added management rule
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	HTTPS Management	Auto-added management rule
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	HTTP Management	Auto-added management rule
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	Ping	Auto-added management rule
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	HTTPS Management	Auto-added management rule
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	HTTP Management	Auto-added management rule
YES	A	LAN	LAN	any	All LAN Management IP	SSH Management	Auto-added management rule
YES	A	LAN	LAN	any	All LAN Management IP	Ping	Auto-added management rule
YES	A	LAN	LAN	any	All LAN Management IP	HTTPS Management	Auto-added management rule
YES	A	LAN	LAN	any	All LAN Management IP	HTTP Management	Auto-added management rule
YES	A	SSLVPN	LAN	any	any	HTTPS Management	
YES	A	VPN	060466	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All LAN Management IP	Ping	Auto-added management rule
YES	A	VPN	LAN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	WAN	WAN	any	All WAN Management IP	SSH Management	Auto-added management rule
YES	A	WAN	WAN	any	All X5 Management IP	Ping	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	Ping	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	HTTPS Management	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	HTTP Management	Auto-added management rule
YES	A	WAN	WAN	WAN Interface IP	any	IKE	Auto-added outbound IKE rule
YES	A	WAN	WAN	any	WAN Interface IP	IKE	Auto-added inbound IKE rule

Management Rules (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	HTTPS Management	Auto-added management rule
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	HTTP Management	Auto-added management rule
YES	A	VPN	060466	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA

Users with Administrative Rights

Explanation

This report shows all users with admin rights.

Users with Full Admin rights

mschmitz

Webadmin

LocalAdmin

Uwe

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

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

VPN Crypt Check

Explanation

The Importance of Checking VPN Proposals, Authentication, and Encryption Methods

Enhanced Security: VPNs are crucial for securing data transmission over the internet. Regularly checking and updating VPN proposals, authentication, and encryption methods ensures the use of the latest and most secure protocols. As cyber threats evolve, outdated methods become vulnerable to attacks, so staying updated is key to protecting sensitive data.

Compliance with Standards and Regulations: Many industries are governed by strict regulatory standards which mandate high levels of data security, especially for sensitive information. Regular checks ensure compliance with these regulations, thereby avoiding legal penalties and maintaining customer trust.

Preventing Unauthorized Access: Strong authentication methods are vital in preventing unauthorized access to networks. As techniques used by attackers become more sophisticated, maintaining robust authentication protocols is essential to ensure that only authorized users can access the VPN.

Data Integrity and Confidentiality: Encryption methods used in VPNs ensure that data remains confidential and intact during transmission. Regular reviews of encryption standards help in safeguarding against new vulnerabilities, ensuring that data cannot be intercepted or tampered with by malicious actors.

Optimized Performance: VPN technologies are continuously improving, offering better speed and efficiency. Regular updates can enhance network performance, reduce latency, and provide a smoother user experience.

Future-proofing the Network: As technology evolves, so do the standards and best practices in network security. Regularly updating VPN settings helps in future-proofing the network against emerging threats and technological advancements.

In summary, regular checks and updates of VPN proposals, authentication methods, and encryption protocols are vital for maintaining robust security, compliance with regulatory standards, preventing unauthorized access, ensuring data integrity, optimizing performance, and preparing for future technological advancements.

Outlining Unsafe Cryptographic Elements in VPNs

When setting up a Virtual Private Network (VPN), it is crucial to use secure cryptographic elements to ensure the confidentiality, integrity, and authenticity of the data being transmitted. Here is an outline of various cryptographic ciphers, Diffie-Hellman (DH) groups, IKE versions, and hash functions that are considered unsafe for use in VPNs, along with the reasons why they are considered insecure.

1. Symmetric Ciphers
Symmetric ciphers are used to encrypt and decrypt data. Unsafe symmetric ciphers include:

DES (Data Encryption Standard)

Reason: DES uses a 56-bit key, which is no longer considered secure due to advances in computational power. It is vulnerable to brute-force attacks.

3DES (Triple DES)

Reason: While an improvement over DES, 3DES effectively has a 112-bit key strength, which is now considered borderline secure. Additionally, it suffers from vulnerabilities such as meet-in-the-middle attacks and has been deprecated by NIST.

2. Diffie-Hellman (DH) Groups
DH groups are used in the key exchange process to securely establish a shared secret. Unsafe DH groups include:

DH Group 1 (768-bit)

Reason: The 768-bit key length is too short to provide adequate security. It is susceptible to brute-force attacks and can be broken by modern computing power.

DH Group 2 (1024-bit)

Reason: The 1024-bit key length is also considered insecure due to the potential for being broken by advanced computational techniques, including those used by state-level actors.

DH Group 5 (1536-bit)

Reason: Though more secure than DH Group 2, 1536-bit DH is still considered weak by todays standards and vulnerable to sophisticated attacks.

3. IKE Versions
The Internet Key Exchange (IKE) protocol is used to set up a secure, authenticated communications channel. Unsafe IKE versions include:

IKEv1

Reason: IKEv1 is considered less secure than IKEv2 due to various vulnerabilities and lack of support for modern cryptographic algorithms. IKEv1 is also more complex and has more attack vectors compared to IKEv2.

4. Hash Functions

Hash functions are used for data integrity and authentication. Unsafe hash functions include:

MD5 (Message-Digest Algorithm 5)

Reason: MD5 is vulnerable to collision attacks, where different inputs produce the same hash output. This makes it possible for attackers to forge data and compromise integrity.

SHA-1 (Secure Hash Algorithm 1)

Reason: SHA-1 is also susceptible to collision attacks. Advances in cryptanalysis have made SHA-1 collisions feasible, and it is considered insecure for cryptographic use.

5. Key Management

Pre-Shared Keys (PSK)
Reason: PSKs can be vulnerable to dictionary attacks, especially if weak or easily guessable keys are used. Proper key

management and the use of stronger authentication methods, like certificates, are recommended.

6. Recommendations for Secure VPN Configuration

To ensure the security of your VPN, consider the following recommendations:

Symmetric Ciphers:

Use AES (Advanced Encryption Standard) with key sizes of at least 128 bits, preferably 256 bits (e.g., AES-128, AES-256).

Diffie-Hellman Groups:

Use DH groups with key sizes of at least 2048 bits. Preferably, use ECDH (Elliptic Curve Diffie-Hellman) with secure curves like P-256 or P-384.

IKE Versions:

Use IKEv2, which offers better security, efficiency, and support for modern cryptographic algorithms.

Hash Functions:

Use SHA-256 or better (e.g., SHA-384, SHA-512) for data integrity and authentication.

Key Management:

Use strong, randomly generated pre-shared keys if PSKs are necessary. Preferably, use certificate-based authentication for enhanced security.

Conclusion

Using outdated or insecure cryptographic elements in your VPN setup can expose you to significant security risks. It is essential to stay informed about the latest cryptographic standards and best practices to ensure the safety and integrity of your VPN communications. Regularly review and update your cryptographic configurations to align with current security recommendations.

VPN Crypt Check

Ena	Name	Phase1 Exchange Mode	Phase1 DH-Group	Phase 1 Encr	Phase1 Auth	Phase2 Protcl	Phase2 Encr	Phase2 Auth	Phase 2 PFS
no	Bad Tunnel	IKEv2	Group 2 (!)	3DES (!)	SHA-1 (!)	ESP	3DES (!)	off (!)	Group 2 (!)
yes	New York	Main (!)	Group 2 (!)	AES-128 (C)	SHA-1 (!)	ESP	AESCGM16-256	off (!)	Group 2 (!)
yes	Remote Site1	IKEv2	Group 2 (!)	AESCGM16-256 (C)	SHA-1 (!)	ESP	AESCGM16-256	off (!)	Group 2 (!)
no	SNWL Policy Mode	IKEv2	521-Bit R ECP Group	AESCGM16-256 (C)	SHA-1 (!)	ESP	AESCGM16-256	on	384-Bit R ECP Group
no	Test	IKEv2	Group 2 (!)	AES-128 (C)	SHA-1 (!)	AH (C)	AESCGM16-256	off (!)	Group 2 (!)
yes	To TZ570	IKEv2	521-Bit R ECP Group	AES-256	SHA-1 (!)	ESP	AESCGM16-256	on	
no	WAN GroupVPN	Aggressive (!)	Group 14	AES-256	SHA-512	ESP	AES-256	on	Group 14

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.

ANY <> ANY Rules (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	060466	150971-Test	any	any	any	
YES	A	060466	DMZ	any	any	any	
YES	A	060466	DMZ-sec	any	any	any	
YES	A	060466	DMZ-unsec	any	any	any	
YES	A	060466	LAN	any	any	any	
YES	A	060466	MULTICAST	any	any	any	
YES	A	060466	Test	any	any	any	
YES	A	060466	WAN	any	any	any	
YES	A	150971-Test	060466	any	any	any	
YES	A	150971-Test	DMZ	any	any	any	
YES	A	150971-Test	DMZ-sec	any	any	any	
YES	A	150971-Test	DMZ-unsec	any	any	any	
YES	A	150971-Test	LAN	any	any	any	
YES	A	150971-Test	MULTICAST	any	any	any	
YES	A	150971-Test	Test	any	any	any	
YES	A	150971-Test	WAN	any	any	any	
YES	A	DMZ	DMZ-sec	any	any	any	
YES	A	DMZ	DMZ-unsec	any	any	any	
YES	A	DMZ	MULTICAST	any	any	any	
YES	A	DMZ	WAN	any	any	any	
YES	A	DMZ-sec	DMZ	any	any	any	
YES	A	DMZ-sec	DMZ-unsec	any	any	any	
YES	A	DMZ-sec	MULTICAST	any	any	any	
YES	A	DMZ-sec	WAN	any	any	any	
YES	A	DMZ-unsec	DMZ	any	any	any	
YES	A	DMZ-unsec	DMZ-sec	any	any	any	
YES	A	DMZ-unsec	MULTICAST	any	any	any	
YES	A	DMZ-unsec	WAN	any	any	any	
YES	A	LAN	060466	any	any	any	
YES	A	LAN	150971-Test	any	any	any	
YES	A	LAN	DMZ	any	any	any	
YES	A	LAN	DMZ-sec	any	any	any	
YES	A	LAN	DMZ-unsec	any	any	any	
YES	A	LAN	MULTICAST	any	any	any	
YES	A	LAN	Test	any	any	any	
YES	A	LAN	WAN	any	any	any	
YES	A	Test	060466	any	any	any	
YES	A	Test	150971-Test	any	any	any	
YES	A	Test	DMZ	any	any	any	
YES	A	Test	DMZ-sec	any	any	any	
YES	A	Test	DMZ-unsec	any	any	any	
YES	A	Test	LAN	any	any	any	
YES	A	Test	MULTICAST	any	any	any	
YES	A	Test	WAN	any	any	any	

ANY <> ANY Rules (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	060466	150971-Test	any	any	any	
YES	A	060466	DMZ	any	any	any	
YES	A	060466	DMZ-sec	any	any	any	
YES	A	060466	DMZ-unsec	any	any	any	
YES	A	060466	LAN	any	any	any	
YES	A	060466	MULTICAST	any	any	any	
YES	A	060466	Test	any	any	any	
YES	A	060466	WAN	any	any	any	
YES	A	150971-Test	060466	any	any	any	
YES	A	150971-Test	DMZ	any	any	any	
YES	A	150971-Test	DMZ-sec	any	any	any	
YES	A	150971-Test	DMZ-unsec	any	any	any	
YES	A	150971-Test	LAN	any	any	any	
YES	A	150971-Test	MULTICAST	any	any	any	
YES	A	150971-Test	Test	any	any	any	
YES	A	150971-Test	WAN	any	any	any	
YES	A	DMZ	DMZ-sec	any	any	any	
YES	A	DMZ	DMZ-unsec	any	any	any	
YES	A	DMZ	MULTICAST	any	any	any	
YES	A	DMZ	WAN	any	any	any	
YES	A	DMZ-sec	DMZ	any	any	any	
YES	A	DMZ-sec	DMZ-unsec	any	any	any	
YES	A	DMZ-sec	MULTICAST	any	any	any	
YES	A	DMZ-sec	WAN	any	any	any	
YES	A	DMZ-unsec	DMZ	any	any	any	
YES	A	DMZ-unsec	DMZ-sec	any	any	any	
YES	A	DMZ-unsec	MULTICAST	any	any	any	
YES	A	DMZ-unsec	WAN	any	any	any	
YES	A	LAN	060466	any	any	any	
YES	A	LAN	150971-Test	any	any	any	
YES	A	LAN	DMZ	any	any	any	
YES	A	LAN	DMZ-sec	any	any	any	
YES	A	LAN	DMZ-unsec	any	any	any	
YES	A	LAN	MULTICAST	any	any	any	
YES	A	LAN	Test	any	any	any	
YES	A	LAN	WAN	any	any	any	
YES	A	Test	060466	any	any	any	
YES	A	Test	150971-Test	any	any	any	
YES	A	Test	DMZ	any	any	any	
YES	A	Test	DMZ-sec	any	any	any	
YES	A	Test	DMZ-unsec	any	any	any	
YES	A	Test	LAN	any	any	any	
YES	A	Test	MULTICAST	any	any	any	
YES	A	Test	WAN	any	any	any	

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.

Rules never used (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	060466	150971-Test	any	any	any	
YES	A	060466	DMZ	any	any	any	
YES	A	060466	DMZ-sec	any	any	any	
YES	A	060466	DMZ-unsec	any	any	any	
YES	A	060466	LAN	any	any	any	
YES	A	060466	MULTICAST	any	any	any	
YES	A	060466	Test	any	any	any	
NO	A	060466	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	060466	WAN	any	any	any	
YES	A	150971-Test	060466	any	any	any	
YES	A	150971-Test	DMZ	any	any	any	
YES	A	150971-Test	DMZ-sec	any	any	any	
YES	A	150971-Test	DMZ-unsec	any	any	any	
YES	A	150971-Test	LAN	any	any	any	
YES	A	150971-Test	MULTICAST	any	any	any	
YES	A	150971-Test	Test	any	any	any	
NO	A	150971-Test	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	150971-Test	WAN	any	any	any	
YES	B	DMZ	060466	any	any	any	
YES	B	DMZ	150971-Test	any	any	any	
YES	A	DMZ	DMZ	any	any	any	Auto-added Interface Trust rule
YES	A	DMZ	DMZ-sec	any	any	any	
YES	A	DMZ	DMZ-unsec	any	any	any	
YES	B	DMZ	LAN	any	any	any	
YES	A	DMZ	MULTICAST	any	any	any	
YES	B	DMZ	Test	any	any	any	
NO	A	DMZ	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	DMZ	WAN	any	any	any	
YES	B	DMZ-sec	060466	any	any	any	
YES	B	DMZ-sec	150971-Test	any	any	any	
YES	A	DMZ-sec	DMZ	any	any	any	
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	Ping	Auto-added management rule
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	HTTPS Management	Auto-added management rule
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	HTTP Management	Auto-added management rule
YES	A	DMZ-sec	DMZ-unsec	any	any	any	
YES	B	DMZ-sec	LAN	any	any	any	
YES	A	DMZ-sec	MULTICAST	any	any	any	
YES	B	DMZ-sec	Test	any	any	any	
NO	A	DMZ-sec	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	B	DMZ-unsec	060466	any	any	any	
YES	B	DMZ-unsec	150971-Test	any	any	any	
YES	A	DMZ-unsec	DMZ	any	any	any	
YES	A	DMZ-unsec	DMZ-sec	any	any	any	
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	Ping	Auto-added management rule
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	HTTPS Management	Auto-added management rule
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	HTTP Management	Auto-added management rule
YES	B	DMZ-unsec	LAN	any	any	any	
YES	A	DMZ-unsec	MULTICAST	any	any	any	

Rules never used (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	B	DMZ-unsec	Test	any	any	any	
NO	A	DMZ-unsec	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	DMZ-unsec	WAN	any	any	any	
YES	A	LAN	060466	any	any	any	
YES	A	LAN	150971-Test	any	any	any	
YES	A	LAN	DMZ	any	any	any	
YES	A	LAN	DMZ-unsec	any	any	any	
YES	A	LAN	MULTICAST	any	any	any	
YES	A	LAN	SSLVPN	LAN Primary Subnet	SSLVPN-NetExtender Range	any	Auto added for outbound SSL VPN Traffic
YES	A	LAN	Test	any	any	any	
NO	A	LAN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	LAN	VPN	LAN Subnets	LAN-UDS-Analytics-10.100.10.50	any	Auto added for outbound VPN - Bad Tunnel
YES	A	LAN	VPN	LAN Primary Subnet	TZ570 LAN	any	Auto added for outbound VPN - To TZ570
YES	A	LAN	VPN	LAN Primary Subnet	DEAG_Adress	any	Auto added for outbound VPN - Remote Site1
YES	A	LAN	VPN	LAN Primary Subnet	Server	any	Auto added for outbound VPN - New York
NO	A	SSLVPN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	Test	060466	any	any	any	
YES	A	Test	150971-Test	any	any	any	
YES	A	Test	DMZ	any	any	any	
YES	A	Test	DMZ-sec	any	any	any	
YES	A	Test	DMZ-unsec	any	any	any	
YES	A	Test	LAN	any	any	any	
YES	A	Test	MULTICAST	any	any	any	
NO	A	Test	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	Test	WAN	any	any	any	
YES	A	VPN	060466	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
NO	A	VPN	060466	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	150971-Test	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
NO	A	VPN	150971-Test	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	DMZ	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	DMZ	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	DMZ-sec	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	DMZ-sec	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	DMZ-unsec	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	DMZ-unsec	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	LAN	any	All LAN Management IP	Ping	Auto-added management rule

Rules never used (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	VPN	LAN	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	LAN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	LAN	any	LAN Primary Subnet	any	Auto added for inbound VPN - Test
NO	A	VPN	LAN	LAN-UDS-Analytics-10.100.10.50	LAN Subnets	any	Auto added for inbound VPN - Bad Tunnel
YES	A	VPN	LAN	TZ570 LAN	LAN Primary Subnet	any	Auto added for inbound VPN - To TZ570
YES	A	VPN	LAN	DEAG_Adress	LAN Primary Subnet	any	Auto added for inbound VPN - Remote Site1
YES	A	VPN	LAN	Server	LAN Primary Subnet	any	Auto added for inbound VPN - New York
YES	A	VPN	MULTICAST	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	MULTICAST	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	SSLVPN	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	SSLVPN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	Test	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
NO	A	VPN	Test	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	VPN	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	VPN	VPN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	WAN	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	WAN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	B	WAN	060466	any	any	any	
YES	B	WAN	150971-Test	any	any	any	
YES	B	WAN	DMZ	any	any	any	
YES	B	WAN	DMZ-sec	any	any	any	
YES	B	WAN	DMZ-unsec	any	any	any	
YES	A	WAN	LAN	WAN-TZ570-10.10.10.254	any	NetFlow / IPFIX	
YES	B	WAN	LAN	any	any	any	
YES	B	WAN	MULTICAST	any	any	any	
YES	B	WAN	Test	any	any	any	
YES	A	WAN	WAN	any	All WAN Management IP	SSH Management	Auto-added management rule
YES	A	WAN	WAN	any	All X5 Management IP	Ping	Auto-added management rule

Rules never used (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	060466	150971-Test	any	any	any	
YES	A	060466	DMZ	any	any	any	
YES	A	060466	DMZ-sec	any	any	any	
YES	A	060466	DMZ-unsec	any	any	any	
YES	A	060466	LAN	any	any	any	
YES	A	060466	MULTICAST	any	any	any	
YES	A	060466	Test	any	any	any	
YES	A	060466	WAN	any	any	any	
YES	A	150971-Test	060466	any	any	any	
YES	A	150971-Test	DMZ	any	any	any	
YES	A	150971-Test	DMZ-sec	any	any	any	
YES	A	150971-Test	DMZ-unsec	any	any	any	
YES	A	150971-Test	LAN	any	any	any	
YES	A	150971-Test	MULTICAST	any	any	any	
YES	A	150971-Test	Test	any	any	any	
YES	A	150971-Test	WAN	any	any	any	
YES	B	DMZ	060466	any	any	any	
YES	B	DMZ	150971-Test	any	any	any	
YES	A	DMZ	DMZ	any	any	any	Auto-added Interface Trust rule for IPv6
YES	A	DMZ	DMZ-sec	any	any	any	
YES	A	DMZ	DMZ-unsec	any	any	any	
YES	B	DMZ	LAN	any	any	any	
YES	A	DMZ	MULTICAST	any	any	any	
YES	B	DMZ	Test	any	any	any	
YES	A	DMZ	WAN	any	any	any	
YES	B	DMZ-sec	060466	any	any	any	
YES	B	DMZ-sec	150971-Test	any	any	any	
YES	A	DMZ-sec	DMZ	any	any	any	
YES	A	DMZ-sec	DMZ-unsec	any	any	any	
YES	B	DMZ-sec	LAN	any	any	any	
YES	A	DMZ-sec	MULTICAST	any	any	any	
YES	B	DMZ-sec	Test	any	any	any	
YES	A	DMZ-sec	WAN	any	any	any	
YES	B	DMZ-unsec	060466	any	any	any	
YES	B	DMZ-unsec	150971-Test	any	any	any	
YES	A	DMZ-unsec	DMZ	any	any	any	
YES	A	DMZ-unsec	DMZ-sec	any	any	any	
YES	B	DMZ-unsec	LAN	any	any	any	
YES	A	DMZ-unsec	MULTICAST	any	any	any	
YES	B	DMZ-unsec	Test	any	any	any	
YES	A	DMZ-unsec	WAN	any	any	any	
YES	A	LAN	060466	any	any	any	
YES	A	LAN	150971-Test	any	any	any	
YES	A	LAN	DMZ	any	any	any	
YES	A	LAN	DMZ-sec	any	any	any	
YES	A	LAN	DMZ-unsec	any	any	any	
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	Ping6	Auto-added management rule
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	HTTPS Management	Auto-added management rule

Rules never used (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	HTTP Management	Auto-added management rule
YES	A	LAN	LAN	any	any	any	Auto-added Interface Trust rule for IPv6
YES	A	LAN	MULTICAST	any	any	any	
YES	A	LAN	Test	any	any	any	
YES	A	Test	060466	any	any	any	
YES	A	Test	150971-Test	any	any	any	
YES	A	Test	DMZ	any	any	any	
YES	A	Test	DMZ-sec	any	any	any	
YES	A	Test	DMZ-unsec	any	any	any	
YES	A	Test	LAN	any	any	any	
YES	A	Test	MULTICAST	any	any	any	
YES	A	Test	WAN	any	any	any	
YES	A	VPN	060466	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	LAN Management IPv6 Addresses	Ping6	Auto-added management rule
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA

Rules never used (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	B	WAN	060466	any	any	any	
YES	B	WAN	150971-Test	any	any	any	
YES	B	WAN	DMZ	any	any	any	
YES	B	WAN	DMZ-sec	any	any	any	
YES	B	WAN	DMZ-unsec	any	any	any	
YES	B	WAN	LAN	any	any	any	
YES	B	WAN	Test	any	any	any	
YES	A	WAN	WAN	any	WAN Interface IPv6 Addresses	SSLVPN	Auto added for inbound SSL VPN Traffic

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.

Rules WAN to internal networks (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	WAN	LAN	WAN-TZ570-10.10.10.254	any	NetFlow / IPFIX	
YES	A	WAN	WAN	any	All WAN Management IP	SSH Management	Auto-added management rule
YES	A	WAN	WAN	any	All X5 Management IP	Ping	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	Ping	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	HTTPS Management	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	HTTP Management	Auto-added management rule
YES	A	WAN	WAN	any	WAN Interface IP	SSLVPN	Auto added for inbound SSL VPN Traffic
YES	A	WAN	WAN	WAN Interface IP	any	IKE	Auto-added outbound IKE rule
YES	A	WAN	WAN	any	WAN Interface IP	IKE	Auto-added inbound IKE rule

Rules WAN to internal networks (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	WAN	WAN	any	WAN Interface IPv6 Addresses	SSLVPN	Auto added for inbound SSL VPN Traffic

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	A	SrcZone	DstZone	Src	Dst	Svc	Comment
NO	A	060466	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	150971-Test	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	DMZ	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	DMZ-sec	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	DMZ-unsec	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	LAN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	LAN	VPN	LAN Primary Subnet	any	any	Auto added for outbound VPN - Test
NO	A	LAN	VPN	LAN Subnets	LAN-UDS-Analytics-10.100.10.50	any	Auto added for outbound VPN - Bad Tunnel
NO	A	SSLVPN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	Test	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	VPN	060466	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	150971-Test	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	DMZ	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	DMZ-sec	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	DMZ-unsec	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	LAN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	LAN	any	LAN Primary Subnet	any	Auto added for inbound VPN - Test
NO	A	VPN	LAN	LAN-UDS-Analytics-10.100.10.50	LAN Subnets	any	Auto added for inbound VPN - Bad Tunnel
NO	A	VPN	MULTICAST	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	SSLVPN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	Test	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	VPN	VPN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	WAN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN

Disabled Firewall Rules (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	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 99 days.

Firewall Rules not used for a long time (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Last time hit
YES	A	LAN	LAN	any	All LAN Management IP	SNMP	10.11.2023 21:13
YES	A	LAN	LAN	any	All LAN Management IP	HTTPS Management	31.05.2024 15:24
YES	A	LAN	LAN	any	All LAN Management IP	HTTP Management	05.10.2023 08:43
YES	A	LAN	LAN	SonicWALL SSO Agents	LAN Interface IP	SonicWALL SSO Agents	12.06.2024 18:17
YES	A	LAN	DMZ	any	any	any	never
NO	A	LAN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
NO	A	LAN	VPN	LAN Subnets	LAN-UDS-Analytics-10.100.10.50	any	never
YES	A	LAN	VPN	LAN Primary Subnet	TZ570 LAN	any	never
YES	A	LAN	VPN	LAN Primary Subnet	DEAG_Adress	any	never
YES	A	LAN	VPN	LAN Primary Subnet	Server	any	never
YES	A	LAN	SSLVPN	LAN Primary Subnet	SSLVPN-NetExtender Range	any	never
YES	A	LAN	MULTICAST	any	any	any	never
YES	A	LAN	DMZ-unsec	any	any	any	never
YES	A	LAN	DMZ-sec	any	any	any	27.02.2024 10:53
YES	A	LAN	Test	any	any	any	never
YES	A	LAN	150971-Test	any	any	any	never
YES	A	LAN	060466	any	any	any	never
YES	A	WAN	LAN	WAN-TZ570-10.10.10.254	any	NetFlow / IPFIX	never
YES	B	WAN	LAN	any	any	any	never
YES	A	WAN	WAN	any	All WAN Management IP	SSH Management	never
YES	A	WAN	WAN	any	All X5 Management IP	Ping	never
YES	A	WAN	WAN	any	All WAN Management IP	Ping	05.10.2023 08:22
YES	A	WAN	WAN	any	All WAN Management IP	HTTP Management	02.11.2023 20:39
YES	B	WAN	DMZ	any	any	any	never
YES	B	WAN	MULTICAST	any	any	any	never
YES	B	WAN	DMZ-unsec	any	any	any	never
YES	B	WAN	DMZ-sec	any	any	any	never
YES	B	WAN	Test	any	any	any	never
YES	B	WAN	150971-Test	any	any	any	never
YES	B	WAN	060466	any	any	any	never
YES	B	DMZ	LAN	any	any	any	never
YES	A	DMZ	WAN	any	any	any	never
YES	A	DMZ	DMZ	any	any	any	never
NO	A	DMZ	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
YES	A	DMZ	MULTICAST	any	any	any	never
YES	A	DMZ	DMZ-unsec	any	any	any	never
YES	A	DMZ	DMZ-sec	any	any	any	never
YES	B	DMZ	Test	any	any	any	never
YES	B	DMZ	150971-Test	any	any	any	never
YES	B	DMZ	060466	any	any	any	never
YES	A	VPN	LAN	any	All LAN Management IP	Ping	never
YES	A	VPN	LAN	any	All Interface IP	SNMP	never
YES	A	VPN	LAN	any	All Interface IP	SSH Management	never
YES	A	VPN	LAN	any	All Interface IP	HTTPS Management	never
NO	A	VPN	LAN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
NO	A	VPN	LAN	any	LAN Primary Subnet	any	never
NO	A	VPN	LAN	LAN-UDS-Analytics-10.100.10.50	LAN Subnets	any	never
YES	A	VPN	LAN	TZ570 LAN	LAN Primary Subnet	any	never

Firewall Rules not used for a long time (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Last time hit
YES	A	VPN	LAN	DEAG_Adress	LAN Primary Subnet	any	never
YES	A	VPN	LAN	Server	LAN Primary Subnet	any	never
YES	A	VPN	WAN	any	All Interface IP	SNMP	never
YES	A	VPN	WAN	any	All Interface IP	SSH Management	never
YES	A	VPN	WAN	any	All Interface IP	HTTPS Management	never
NO	A	VPN	WAN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	DMZ	any	All Interface IP	SNMP	never
YES	A	VPN	DMZ	any	All Interface IP	SSH Management	never
YES	A	VPN	DMZ	any	All Interface IP	HTTPS Management	never
NO	A	VPN	DMZ	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	VPN	any	All Interface IP	SNMP	never
YES	A	VPN	VPN	any	All Interface IP	SSH Management	never
YES	A	VPN	VPN	any	All Interface IP	HTTPS Management	never
NO	A	VPN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
NO	A	VPN	VPN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	SSLVPN	any	All Interface IP	SNMP	never
YES	A	VPN	SSLVPN	any	All Interface IP	SSH Management	never
YES	A	VPN	SSLVPN	any	All Interface IP	HTTPS Management	never
NO	A	VPN	SSLVPN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	MULTICAST	any	All Interface IP	SNMP	never
YES	A	VPN	MULTICAST	any	All Interface IP	SSH Management	never
YES	A	VPN	MULTICAST	any	All Interface IP	HTTPS Management	never
NO	A	VPN	MULTICAST	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	DMZ-unsec	any	All Interface IP	SNMP	never
YES	A	VPN	DMZ-unsec	any	All Interface IP	SSH Management	never
YES	A	VPN	DMZ-unsec	any	All Interface IP	HTTPS Management	never
NO	A	VPN	DMZ-unsec	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	DMZ-sec	any	All Interface IP	SNMP	never
YES	A	VPN	DMZ-sec	any	All Interface IP	SSH Management	never
YES	A	VPN	DMZ-sec	any	All Interface IP	HTTPS Management	never
NO	A	VPN	DMZ-sec	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	Test	any	All Interface IP	SNMP	never
YES	A	VPN	Test	any	All Interface IP	SSH Management	never
YES	A	VPN	Test	any	All Interface IP	HTTPS Management	never
YES	A	VPN	Test	any	All Interface IP	HTTP Management	never
NO	A	VPN	Test	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	150971-Test	any	All Interface IP	SNMP	never
YES	A	VPN	150971-Test	any	All Interface IP	SSH Management	never
YES	A	VPN	150971-Test	any	All Interface IP	HTTPS Management	never
YES	A	VPN	150971-Test	any	All Interface IP	HTTP Management	never
NO	A	VPN	150971-Test	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
YES	A	VPN	060466	any	All Interface IP	SNMP	never
YES	A	VPN	060466	any	All Interface IP	SSH Management	never
YES	A	VPN	060466	any	All Interface IP	HTTPS Management	never
YES	A	VPN	060466	any	All Interface IP	HTTP Management	never
NO	A	VPN	060466	Vpn DHCP Clients	WAN RemoteAccess Networks	any	never
NO	A	SSLVPN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
YES	B	DMZ-unsec	LAN	any	any	any	never

Firewall Rules not used for a long time (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Last time hit
YES	A	DMZ-unsec	WAN	any	any	any	never
YES	A	DMZ-unsec	DMZ	any	any	any	never
NO	A	DMZ-unsec	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
YES	A	DMZ-unsec	MULTICAST	any	any	any	never
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	Ping	never
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	HTTPS Management	never
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	HTTP Management	never
YES	A	DMZ-unsec	DMZ-sec	any	any	any	never
YES	B	DMZ-unsec	Test	any	any	any	never
YES	B	DMZ-unsec	150971-Test	any	any	any	never
YES	B	DMZ-unsec	060466	any	any	any	never
YES	B	DMZ-sec	LAN	any	any	any	never
YES	A	DMZ-sec	WAN	any	any	any	27.02.2024 21:16
YES	A	DMZ-sec	DMZ	any	any	any	never
NO	A	DMZ-sec	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
YES	A	DMZ-sec	MULTICAST	any	any	any	never
YES	A	DMZ-sec	DMZ-unsec	any	any	any	never
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	Ping	never
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	HTTPS Management	never
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	HTTP Management	never
YES	B	DMZ-sec	Test	any	any	any	never
YES	B	DMZ-sec	150971-Test	any	any	any	never
YES	B	DMZ-sec	060466	any	any	any	never
YES	A	Test	LAN	any	any	any	never
YES	A	Test	WAN	any	any	any	never
YES	A	Test	DMZ	any	any	any	never
NO	A	Test	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
YES	A	Test	MULTICAST	any	any	any	never
YES	A	Test	DMZ-unsec	any	any	any	never
YES	A	Test	DMZ-sec	any	any	any	never
YES	A	Test	150971-Test	any	any	any	never
YES	A	Test	060466	any	any	any	never
YES	A	150971-Test	LAN	any	any	any	never
YES	A	150971-Test	WAN	any	any	any	never
YES	A	150971-Test	DMZ	any	any	any	never
NO	A	150971-Test	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
YES	A	150971-Test	MULTICAST	any	any	any	never
YES	A	150971-Test	DMZ-unsec	any	any	any	never
YES	A	150971-Test	DMZ-sec	any	any	any	never
YES	A	150971-Test	Test	any	any	any	never
YES	A	150971-Test	060466	any	any	any	never
YES	A	060466	LAN	any	any	any	never
YES	A	060466	WAN	any	any	any	never
YES	A	060466	DMZ	any	any	any	never
NO	A	060466	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	never
YES	A	060466	MULTICAST	any	any	any	never
YES	A	060466	DMZ-unsec	any	any	any	never
YES	A	060466	DMZ-sec	any	any	any	never

Firewall Rules not used for a long time (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Last time hit
YES	A	060466	Test	any	any	any	never
YES	A	060466	150971-Test	any	any	any	never

Firewall Rules not used for a long time (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Last time hit
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	Ping6	never
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	HTTPS Management	never
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	HTTP Management	never
YES	A	LAN	LAN	any	any	any	never
YES	A	LAN	DMZ	any	any	any	never
YES	A	LAN	MULTICAST	any	any	any	never
YES	A	LAN	DMZ-unsec	any	any	any	never
YES	A	LAN	DMZ-sec	any	any	any	never
YES	A	LAN	Test	any	any	any	never
YES	A	LAN	150971-Test	any	any	any	never
YES	A	LAN	060466	any	any	any	never
YES	B	WAN	LAN	any	any	any	never
YES	A	WAN	WAN	any	WAN Interface IPv6 Addresses	SSLVPN	never
YES	B	WAN	DMZ	any	any	any	never
YES	B	WAN	MULTICAST	any	any	any	05.10.2023 08:43
YES	B	WAN	DMZ-unsec	any	any	any	never
YES	B	WAN	DMZ-sec	any	any	any	never
YES	B	WAN	Test	any	any	any	never
YES	B	WAN	150971-Test	any	any	any	never
YES	B	WAN	060466	any	any	any	never
YES	B	DMZ	LAN	any	any	any	never
YES	A	DMZ	WAN	any	any	any	never
YES	A	DMZ	DMZ	any	any	any	never
YES	A	DMZ	MULTICAST	any	any	any	never
YES	A	DMZ	DMZ-unsec	any	any	any	never
YES	A	DMZ	DMZ-sec	any	any	any	never
YES	B	DMZ	Test	any	any	any	never
YES	B	DMZ	150971-Test	any	any	any	never
YES	B	DMZ	060466	any	any	any	never
YES	A	VPN	LAN	any	LAN Management IPv6 Addresses	Ping6	never
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	HTTPS Management	never

Firewall Rules not used for a long time (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Last time hit
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	Test	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	Test	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	Test	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	Test	any	All Interface IPv6 Addresses	HTTP Management	never
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	HTTP Management	never
YES	A	VPN	060466	any	All Interface IPv6 Addresses	SNMP	never
YES	A	VPN	060466	any	All Interface IPv6 Addresses	SSH Management	never
YES	A	VPN	060466	any	All Interface IPv6 Addresses	HTTPS Management	never
YES	A	VPN	060466	any	All Interface IPv6 Addresses	HTTP Management	never
YES	B	DMZ-unsec	LAN	any	any	any	never
YES	A	DMZ-unsec	WAN	any	any	any	never
YES	A	DMZ-unsec	DMZ	any	any	any	never
YES	A	DMZ-unsec	MULTICAST	any	any	any	never
YES	A	DMZ-unsec	DMZ-sec	any	any	any	never
YES	B	DMZ-unsec	Test	any	any	any	never
YES	B	DMZ-unsec	150971-Test	any	any	any	never
YES	B	DMZ-unsec	060466	any	any	any	never
YES	B	DMZ-sec	LAN	any	any	any	never
YES	A	DMZ-sec	WAN	any	any	any	never
YES	A	DMZ-sec	DMZ	any	any	any	never
YES	A	DMZ-sec	MULTICAST	any	any	any	never
YES	A	DMZ-sec	DMZ-unsec	any	any	any	never
YES	B	DMZ-sec	Test	any	any	any	never
YES	B	DMZ-sec	150971-Test	any	any	any	never
YES	B	DMZ-sec	060466	any	any	any	never
YES	A	Test	LAN	any	any	any	never
YES	A	Test	WAN	any	any	any	never
YES	A	Test	DMZ	any	any	any	never
YES	A	Test	MULTICAST	any	any	any	never
YES	A	Test	DMZ-unsec	any	any	any	never
YES	A	Test	DMZ-sec	any	any	any	never
YES	A	Test	150971-Test	any	any	any	never
YES	A	Test	060466	any	any	any	never
YES	A	150971-Test	LAN	any	any	any	never
YES	A	150971-Test	WAN	any	any	any	never
YES	A	150971-Test	DMZ	any	any	any	never
YES	A	150971-Test	MULTICAST	any	any	any	never
YES	A	150971-Test	DMZ-unsec	any	any	any	never
YES	A	150971-Test	DMZ-sec	any	any	any	never

Firewall Rules not used for a long time (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Last time hit
YES	A	150971-Test	Test	any	any	any	never
YES	A	150971-Test	060466	any	any	any	never
YES	A	060466	LAN	any	any	any	never
YES	A	060466	WAN	any	any	any	never
YES	A	060466	DMZ	any	any	any	never
YES	A	060466	MULTICAST	any	any	any	never
YES	A	060466	DMZ-unsec	any	any	any	never
YES	A	060466	DMZ-sec	any	any	any	never
YES	A	060466	Test	any	any	any	never
YES	A	060466	150971-Test	any	any	any	never

All Rules (IPv4)

Explanation

The following table lists all rules that are found on the system.

All Rules (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	060466	150971-Test	any	any	any	
YES	A	060466	DMZ	any	any	any	
YES	A	060466	DMZ-sec	any	any	any	
YES	A	060466	DMZ-unsec	any	any	any	
YES	A	060466	LAN	any	any	any	
YES	A	060466	MULTICAST	any	any	any	
YES	A	060466	Test	any	any	any	
NO	A	060466	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	060466	WAN	any	any	any	
YES	A	150971-Test	060466	any	any	any	
YES	A	150971-Test	DMZ	any	any	any	
YES	A	150971-Test	DMZ-sec	any	any	any	
YES	A	150971-Test	DMZ-unsec	any	any	any	
YES	A	150971-Test	LAN	any	any	any	
YES	A	150971-Test	MULTICAST	any	any	any	
YES	A	150971-Test	Test	any	any	any	
NO	A	150971-Test	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	150971-Test	WAN	any	any	any	
YES	B	DMZ	060466	any	any	any	
YES	B	DMZ	150971-Test	any	any	any	
YES	A	DMZ	DMZ	any	any	any	Auto-added Interface Trust rule
YES	A	DMZ	DMZ-sec	any	any	any	
YES	A	DMZ	DMZ-unsec	any	any	any	
YES	B	DMZ	LAN	any	any	any	
YES	A	DMZ	MULTICAST	any	any	any	
YES	B	DMZ	Test	any	any	any	
NO	A	DMZ	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	DMZ	WAN	any	any	any	
YES	B	DMZ-sec	060466	any	any	any	
YES	B	DMZ-sec	150971-Test	any	any	any	
YES	A	DMZ-sec	DMZ	any	any	any	
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	Ping	Auto-added management rule
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	HTTPS Management	Auto-added management rule
YES	A	DMZ-sec	DMZ-sec	any	All X3 Management IP	HTTP Management	Auto-added management rule
YES	A	DMZ-sec	DMZ-unsec	any	any	any	
YES	B	DMZ-sec	LAN	any	any	any	
YES	A	DMZ-sec	MULTICAST	any	any	any	
YES	B	DMZ-sec	Test	any	any	any	
NO	A	DMZ-sec	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	DMZ-sec	WAN	any	any	any	
YES	B	DMZ-unsec	060466	any	any	any	
YES	B	DMZ-unsec	150971-Test	any	any	any	
YES	A	DMZ-unsec	DMZ	any	any	any	
YES	A	DMZ-unsec	DMZ-sec	any	any	any	
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	Ping	Auto-added management rule
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	HTTPS Management	Auto-added management rule
YES	A	DMZ-unsec	DMZ-unsec	any	All X2 Management IP	HTTP Management	Auto-added management rule
YES	B	DMZ-unsec	LAN	any	any	any	

All Rules (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	DMZ-unsec	MULTICAST	any	any	any	
YES	B	DMZ-unsec	Test	any	any	any	
NO	A	DMZ-unsec	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	DMZ-unsec	WAN	any	any	any	
YES	A	LAN	060466	any	any	any	
YES	A	LAN	150971-Test	any	any	any	
YES	A	LAN	DMZ	any	any	any	
YES	A	LAN	DMZ-sec	any	any	any	
YES	A	LAN	DMZ-unsec	any	any	any	
YES	A	LAN	LAN	any	All LAN Management IP	SNMP	Auto-added management rule
YES	A	LAN	LAN	any	All LAN Management IP	SSH Management	Auto-added management rule
YES	A	LAN	LAN	any	All LAN Management IP	Ping	Auto-added management rule
YES	A	LAN	LAN	any	All LAN Management IP	HTTPS Management	Auto-added management rule
YES	A	LAN	LAN	any	All LAN Management IP	HTTP Management	Auto-added management rule
YES	A	LAN	LAN	SonicWALL SSO Agents	LAN Interface IP	SonicWALL SSO Agents	Auto-added for SSO agent authentication
YES	A	LAN	LAN	any	any	any	Auto-added Interface Trust rule
YES	A	LAN	MULTICAST	any	any	any	
YES	A	LAN	SSLVPN	LAN Primary Subnet	SSLVPN-NetExtender Range	any	Auto added for outbound SSL VPN Traffic
YES	A	LAN	Test	any	any	any	
NO	A	LAN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	LAN	VPN	LAN Primary Subnet	any	any	Auto added for outbound VPN - Test
NO	A	LAN	VPN	LAN Subnets	LAN-UDS-Analytics-10.100.10.50	any	Auto added for outbound VPN - Bad Tunnel
YES	A	LAN	VPN	LAN Primary Subnet	TZ570 LAN	any	Auto added for outbound VPN - To TZ570
YES	A	LAN	VPN	LAN Primary Subnet	DEAG_Adress	any	Auto added for outbound VPN - Remote Site1
YES	A	LAN	VPN	LAN Primary Subnet	Server	any	Auto added for outbound VPN - New York
YES	A	LAN	WAN	any	any	any	
YES	A	SSLVPN	LAN	any	any	HTTPS Management	
YES	A	SSLVPN	LAN	SSLVPN-NetExtender Range	LAN Primary Subnet	any	Auto added for inbound SSL VPN Traffic
NO	A	SSLVPN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	Test	060466	any	any	any	
YES	A	Test	150971-Test	any	any	any	
YES	A	Test	DMZ	any	any	any	
YES	A	Test	DMZ-sec	any	any	any	
YES	A	Test	DMZ-unsec	any	any	any	
YES	A	Test	LAN	any	any	any	
YES	A	Test	MULTICAST	any	any	any	
NO	A	Test	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
YES	A	Test	WAN	any	any	any	
YES	A	VPN	060466	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
NO	A	VPN	060466	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	150971-Test	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
NO	A	VPN	150971-Test	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN

All Rules (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	VPN	DMZ	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	DMZ	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	DMZ-sec	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	DMZ-sec	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	DMZ-unsec	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	DMZ-unsec	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	LAN	any	All LAN Management IP	Ping	Auto-added management rule
YES	A	VPN	LAN	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	LAN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
NO	A	VPN	LAN	any	LAN Primary Subnet	any	Auto added for inbound VPN - Test
NO	A	VPN	LAN	LAN-UDS-Analytics-10.100.10.50	LAN Subnets	any	Auto added for inbound VPN - Bad Tunnel
YES	A	VPN	LAN	TZ570 LAN	LAN Primary Subnet	any	Auto added for inbound VPN - To TZ570
YES	A	VPN	LAN	DEAG_Adress	LAN Primary Subnet	any	Auto added for inbound VPN - Remote Site1
YES	A	VPN	LAN	Server	LAN Primary Subnet	any	Auto added for inbound VPN - New York
YES	A	VPN	MULTICAST	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	MULTICAST	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	SSLVPN	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	SSLVPN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	Test	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IP	HTTP Management	Auto added for VPN enabled management via this SA
NO	A	VPN	Test	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	VPN	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	VPN	WAN RemoteAccess Networks	Vpn DHCP Clients	any	Auto added for outbound VPN - WAN GroupVPN
NO	A	VPN	VPN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	A	VPN	WAN	any	All Interface IP	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IP	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IP	HTTPS Management	Auto added for VPN enabled management via this SA
NO	A	VPN	WAN	Vpn DHCP Clients	WAN RemoteAccess Networks	any	Auto added for inbound VPN - WAN GroupVPN
YES	B	WAN	060466	any	any	any	
YES	B	WAN	150971-Test	any	any	any	
YES	B	WAN	DMZ	any	any	any	
YES	B	WAN	DMZ-sec	any	any	any	

All Rules (IPv4)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	B	WAN	DMZ-unsec	any	any	any	
YES	A	WAN	LAN	WAN-TZ570-10.10.10.254	any	NetFlow / IPFIX	
YES	B	WAN	LAN	any	any	any	
YES	B	WAN	MULTICAST	any	any	any	
YES	B	WAN	Test	any	any	any	
YES	A	WAN	WAN	any	All WAN Management IP	SSH Management	Auto-added management rule
YES	A	WAN	WAN	any	All X5 Management IP	Ping	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	Ping	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	HTTPS Management	Auto-added management rule
YES	A	WAN	WAN	any	All WAN Management IP	HTTP Management	Auto-added management rule
YES	A	WAN	WAN	any	WAN Interface IP	SSLVPN	Auto added for inbound SSL VPN Traffic
YES	A	WAN	WAN	WAN Interface IP	any	IKE	Auto-added outbound IKE rule
YES	A	WAN	WAN	any	WAN Interface IP	IKE	Auto-added inbound IKE rule

All Rules (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	060466	150971-Test	any	any	any	
YES	A	060466	DMZ	any	any	any	
YES	A	060466	DMZ-sec	any	any	any	
YES	A	060466	DMZ-unsec	any	any	any	
YES	A	060466	LAN	any	any	any	
YES	A	060466	MULTICAST	any	any	any	
YES	A	060466	Test	any	any	any	
YES	A	060466	WAN	any	any	any	
YES	A	150971-Test	060466	any	any	any	
YES	A	150971-Test	DMZ	any	any	any	
YES	A	150971-Test	DMZ-sec	any	any	any	
YES	A	150971-Test	DMZ-unsec	any	any	any	
YES	A	150971-Test	LAN	any	any	any	
YES	A	150971-Test	MULTICAST	any	any	any	
YES	A	150971-Test	Test	any	any	any	
YES	A	150971-Test	WAN	any	any	any	
YES	B	DMZ	060466	any	any	any	
YES	B	DMZ	150971-Test	any	any	any	
YES	A	DMZ	DMZ	any	any	any	Auto-added Interface Trust rule for IPv6
YES	A	DMZ	DMZ-sec	any	any	any	
YES	A	DMZ	DMZ-unsec	any	any	any	
YES	B	DMZ	LAN	any	any	any	
YES	A	DMZ	MULTICAST	any	any	any	
YES	B	DMZ	Test	any	any	any	
YES	A	DMZ	WAN	any	any	any	
YES	B	DMZ-sec	060466	any	any	any	
YES	B	DMZ-sec	150971-Test	any	any	any	
YES	A	DMZ-sec	DMZ	any	any	any	
YES	A	DMZ-sec	DMZ-unsec	any	any	any	
YES	B	DMZ-sec	LAN	any	any	any	
YES	A	DMZ-sec	MULTICAST	any	any	any	
YES	B	DMZ-sec	Test	any	any	any	
YES	A	DMZ-sec	WAN	any	any	any	
YES	B	DMZ-unsec	060466	any	any	any	
YES	B	DMZ-unsec	150971-Test	any	any	any	
YES	A	DMZ-unsec	DMZ	any	any	any	
YES	A	DMZ-unsec	DMZ-sec	any	any	any	
YES	B	DMZ-unsec	LAN	any	any	any	
YES	A	DMZ-unsec	MULTICAST	any	any	any	
YES	B	DMZ-unsec	Test	any	any	any	
YES	A	DMZ-unsec	WAN	any	any	any	
YES	A	LAN	060466	any	any	any	
YES	A	LAN	150971-Test	any	any	any	
YES	A	LAN	DMZ	any	any	any	
YES	A	LAN	DMZ-sec	any	any	any	
YES	A	LAN	DMZ-unsec	any	any	any	
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	Ping6	Auto-added management rule
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	HTTPS Management	Auto-added management rule

All Rules (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	LAN	LAN	any	LAN Management IPv6 Addresses	HTTP Management	Auto-added management rule
YES	A	LAN	LAN	any	any	any	Auto-added Interface Trust rule for IPv6
YES	A	LAN	MULTICAST	any	any	any	
YES	A	LAN	Test	any	any	any	
YES	A	LAN	WAN	any	any	any	
YES	A	Test	060466	any	any	any	
YES	A	Test	150971-Test	any	any	any	
YES	A	Test	DMZ	any	any	any	
YES	A	Test	DMZ-sec	any	any	any	
YES	A	Test	DMZ-unsec	any	any	any	
YES	A	Test	LAN	any	any	any	
YES	A	Test	MULTICAST	any	any	any	
YES	A	Test	WAN	any	any	any	
YES	A	VPN	060466	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	060466	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	150971-Test	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-sec	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	DMZ-unsec	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	LAN Management IPv6 Addresses	Ping6	Auto-added management rule
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	LAN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	MULTICAST	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	SSLVPN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	Test	any	All Interface IPv6 Addresses	HTTP Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	VPN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	SNMP	Auto added for VPN enabled management via this SA

All Rules (IPv6)

Ena	A	SrcZone	DstZone	Src	Dst	Svc	Comment
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	SSH Management	Auto added for VPN enabled management via this SA
YES	A	VPN	WAN	any	All Interface IPv6 Addresses	HTTPS Management	Auto added for VPN enabled management via this SA
YES	B	WAN	060466	any	any	any	
YES	B	WAN	150971-Test	any	any	any	
YES	B	WAN	DMZ	any	any	any	
YES	B	WAN	DMZ-sec	any	any	any	
YES	B	WAN	DMZ-unsec	any	any	any	
YES	B	WAN	LAN	any	any	any	
YES	B	WAN	MULTICAST	any	any	any	
YES	B	WAN	Test	any	any	any	
YES	A	WAN	WAN	any	WAN Interface IPv6 Addresses	SSLVPN	Auto added for inbound SSL VPN Traffic

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.

Nat Policies disabled (IPv4)

Ena	Name	OrigDst	OrigSrv	TransSRC	TransDst	TransSvc	Comment
NO	Default NAT Policy	any	Idle HF	HF Backup X0 IP	original	original	
NO	Default NAT Policy	any	Idle HF	HF Primary X0 IP	original	original	
NO	Netflow	WAN Interface IP	NetFlow / IPFIX	any	LAN-UDS-Analytics-10.100.10.50	original	

Nat Policies disabled (IPv6)

Ena	Name	OrigDst	OrigSrv	TransSRC	TransDst	TransSvc	Comment
--- 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.

Nat Policies never used (IPv4)

Ena	Name	OrigDst	OrigSrv	TransSRC	TransDst	TransSvc	Comment
0	Default NAT Policy	any	IKE	any	original	original	
0	Default NAT Policy	WAN Primary IP	SSH Management	any	original	original	
0	Default NAT Policy	X5 IP	Ping	any	original	original	
0	Default NAT Policy	X3 IP	Ping	any	original	original	
0	Default NAT Policy	X3 IP	HTTPS Management	any	original	original	
0	Default NAT Policy	X3 IP	HTTP Management	any	original	original	
0	Default NAT Policy	X2 IP	Ping	any	original	original	
0	Default NAT Policy	X2 IP	HTTPS Management	any	original	original	
0	Default NAT Policy	X2 IP	HTTP Management	any	original	original	
0	Default NAT Policy	any	any	X5 IP	original	original	
0	Default NAT Policy	any	any	X5 IP	original	original	
0	Default NAT Policy	any	any	X5 IP	original	original	
0	Default NAT Policy	any	any	X5 IP	original	original	
0	Default NAT Policy	any	any	WAN Primary IP	original	original	

Nat Policies never used (IPv6)

Ena	Name	OrigDst	OrigSrv	TransSRC	TransDst	TransSvc	Comment
0	Default NAT Policy	LAN Management IPv6 Addresses	Ping6	any	original	original	
0	Default NAT Policy	LAN Management IPv6 Addresses	HTTPS Management	any	original	original	
0	Default NAT Policy	LAN Management IPv6 Addresses	HTTP Management	any	original	original	
0	Default NAT Policy	WAN Interface IPv6 Addresses	SSLVPN	any	original	original	

All Nat Policies (IPv4)

Explanation

This report shows all NAT Policies

All Nat Policies (IPv4)

Ena	Name	OrigDst	OrigSrv	TransSRC	TransDst	TransSvc	Comment
NO	Default NAT Policy	any	Idle HF	HF Backup X0 IP	original	original	
NO	Default NAT Policy	any	Idle HF	HF Primary X0 IP	original	original	
YES	Default NAT Policy	any	IKE	any	original	original	
YES	Default NAT Policy	WAN Interface IP	IKE	any	original	original	
YES	Default NAT Policy	WAN Primary IP	SSH Management	any	original	original	
YES	Default NAT Policy	X5 IP	Ping	any	original	original	
YES	Default NAT Policy	LAN Primary IP	SNMP	any	original	original	
YES	Default NAT Policy	LAN Primary IP	SSH Management	any	original	original	
YES	Default NAT Policy	X3 IP	Ping	any	original	original	
YES	Default NAT Policy	X3 IP	HTTPS Management	any	original	original	
YES	Default NAT Policy	X3 IP	HTTP Management	any	original	original	
YES	Default NAT Policy	X2 IP	Ping	any	original	original	
YES	Default NAT Policy	X2 IP	HTTPS Management	any	original	original	
YES	Default NAT Policy	X2 IP	HTTP Management	any	original	original	
YES	Default NAT Policy	LAN Interface IP	SonicWALL SSO Agents	any	original	original	
YES	Default NAT Policy	WAN Primary IP	Ping	any	original	original	
YES	Default NAT Policy	LAN Primary IP	Ping	any	original	original	
YES	Default NAT Policy	LAN Primary IP	HTTPS Management	any	original	original	
YES	Default NAT Policy	LAN Primary IP	HTTP Management	any	original	original	
YES	Default NAT Policy	WAN Primary IP	HTTPS Management	any	original	original	
YES	Default NAT Policy	WAN Primary IP	HTTP Management	any	original	original	
YES	Default NAT Policy	any	any	WAN Primary IP	original	original	
YES	Default NAT Policy	any	any	X5 IP	original	original	
YES	Default NAT Policy	WAN Interface IP	SSLVPN	any	original	original	
NO	Netflow	WAN Interface IP	NetFlow / IPFIX	any	LAN-UDS-Analytics-10.100.10.50	original	
YES	Default NAT Policy	any	any	X5 IP	original	original	
YES	Default NAT Policy	any	any	X5 IP	original	original	
YES	Default NAT Policy	any	any	X5 IP	original	original	
YES	Default NAT Policy	any	any	WAN Primary IP	original	original	
YES	Default NAT Policy	any	any	WAN Primary IP	original	original	
YES	Default NAT Policy	any	any	WAN Primary IP	original	original	

All Nat Policies (IPv6)

Ena	Name	OrigDst	OrigSrv	TransSRC	TransDst	TransSvc	Comment
YES	Default NAT Policy	LAN Management IPv6 Addresses	Ping6	any	original	original	
YES	Default NAT Policy	LAN Management IPv6 Addresses	HTTPS Management	any	original	original	
YES	Default NAT Policy	LAN Management IPv6 Addresses	HTTP Management	any	original	original	
YES	Default NAT Policy	WAN Interface IPv6 Addresses	SSLVPN	any	original	original	

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.

Audit Details

Auditing:	on
Audit Records found in TS-Report:	156
Newest Audit entry found in TS-Report:	18.09.2024 11:07
Oldest Audit entry found in TS-Report:	15.10.2024 18:58

Users appearing in Audit Log

- admin
- mschmitz
- Robert

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!

All Audit Records

Explanation

This report shows all audit records from the technical support report

Firewall Internal Admin Audit Records


```
Timestamp:   14:19:51 Oct 18 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (18718)

Timestamp:   23:50:15 Oct 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (61304)

Timestamp:   15:24:47 Oct 16 2024
Description: Encryption Key
Old:         *****
New:         ******
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)

Timestamp:   15:24:47 Oct 16 2024
Description: Phase 2 Authentication
Old:         SHA1
New:         None
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)

Timestamp:   15:24:47 Oct 16 2024
Description: Phase 1 (IKE) Exchange
Old:         IKEv2 Mode
New:         Main Mode
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)

Timestamp:   15:24:47 Oct 16 2024
Description: Destination Networks
Old:
New:         Server
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)

Timestamp:   15:24:47 Oct 16 2024
Description: Local Networks
Old:
New:         X0 Subnet
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)

Timestamp:   15:24:47 Oct 16 2024
Description: Authentication Method
Old:
New:         IKE using Preshared Secret
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)
```

Firewall Internal Admin Audit Records


```
Timestamp:   15:24:47 Oct 16 2024
Description: Type of VPN Policy
Old:
New:         Site to Site
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)

Timestamp:   15:24:47 Oct 16 2024
Description: IPsec Gateway Address
Old:
New:         154.34.22.120
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)

Timestamp:   15:24:47 Oct 16 2024
Description: Added 'IPsec Name
Old:
New:         New York
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46906)

Timestamp:   15:23:50 Oct 16 2024
Description: Address Object Network
Old:         10.10.10.223
New:         10.99.10.223
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46741)

Timestamp:   15:23:05 Oct 16 2024
Description: Encryption Key
Old:         *****
New:         ******
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)

Timestamp:   15:23:05 Oct 16 2024
Description: Phase 2 Authentication
Old:         SHA1
New:         None
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)

Timestamp:   15:23:05 Oct 16 2024
Description: Phase 1 (IKE) Exchange
Old:         IKEv2 Mode
New:         Main Mode
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)

Timestamp:   15:23:05 Oct 16 2024
Description: Destination Networks
Old:
New:         Server
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)
```

Firewall Internal Admin Audit Records


```
Timestamp:   15:23:05 Oct 16 2024
Description: Local Networks
Old:
New:         X0 Subnet
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)

Timestamp:   15:23:05 Oct 16 2024
Description: Authentication Method
Old:
New:         IKE using Preshared Secret
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)

Timestamp:   15:23:05 Oct 16 2024
Description: Type of VPN Policy
Old:
New:         Site to Site
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)

Timestamp:   15:23:05 Oct 16 2024
Description: IPsec Gateway Address
Old:
New:         154.34.22.120
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)

Timestamp:   15:23:05 Oct 16 2024
Description: Added 'IPsec Name
Old:
New:         New York
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46585)

Timestamp:   15:22:47 Oct 16 2024
Description: Encryption Key
Old:         *****
New:         ******
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)

Timestamp:   15:22:47 Oct 16 2024
Description: Phase 2 Authentication
Old:         SHA1
New:         None
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)

Timestamp:   15:22:47 Oct 16 2024
Description: Phase 1 (IKE) Exchange
Old:         IKEv2 Mode
New:         Main Mode
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)
```

Firewall Internal Admin Audit Records


```
Timestamp:   15:22:47 Oct 16 2024
Description: Destination Networks
Old:
New:         Server
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)

Timestamp:   15:22:47 Oct 16 2024
Description: Local Networks
Old:
New:         X0 Subnet
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)

Timestamp:   15:22:47 Oct 16 2024
Description: Authentication Method
Old:
New:         IKE using Preshared Secret
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)

Timestamp:   15:22:47 Oct 16 2024
Description: Type of VPN Policy
Old:
New:         Site to Site
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)

Timestamp:   15:22:47 Oct 16 2024
Description: IPsec Gateway Address
Old:
New:         154.34.22.120
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)

Timestamp:   15:22:47 Oct 16 2024
Description: Added 'IPsec Name
Old:
New:         New York
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46525)

Timestamp:   15:22:24 Oct 16 2024
Description: Encryption Key
Old:         *****
New:         ******
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)

Timestamp:   15:22:24 Oct 16 2024
Description: Phase 2 Authentication
Old:         SHA1
New:         None
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)
```

Firewall Internal Admin Audit Records


```
Timestamp:   15:22:24 Oct 16 2024
Description: Phase 1 (IKE) Exchange
Old:         IKEv2 Mode
New:         Main Mode
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)

Timestamp:   15:22:24 Oct 16 2024
Description: Destination Networks
Old:
New:         Server
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)

Timestamp:   15:22:24 Oct 16 2024
Description: Local Networks
Old:
New:         X0 Subnet
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)

Timestamp:   15:22:24 Oct 16 2024
Description: Authentication Method
Old:
New:         IKE using Preshared Secret
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)

Timestamp:   15:22:24 Oct 16 2024
Description: Type of VPN Policy
Old:
New:         Site to Site
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)

Timestamp:   15:22:24 Oct 16 2024
Description: IPsec Gateway Address
Old:
New:         154.34.22.120
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)

Timestamp:   15:22:24 Oct 16 2024
Description: Added 'IPsec Name
Old:
New:         New York
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46457)

Timestamp:   15:22:18 Oct 16 2024
Description: Address Object Subnet Mask
Old:
New:         255.255.255.255
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46435)
```

Firewall Internal Admin Audit Records


```
Timestamp:   15:22:18 Oct 16 2024
Description: Address Object Network
Old:
New:         10.10.10.223
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46435)

Timestamp:   15:22:18 Oct 16 2024
Description: Address Object Zone
Old:
New:         LAN
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46435)

Timestamp:   15:22:18 Oct 16 2024
Description: Address Object Type
Old:
New:         IPv4 HOST
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46435)

Timestamp:   15:22:18 Oct 16 2024
Description: Address Object
Old:
New:         Server
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46435)

Timestamp:   15:21:26 Oct 16 2024
Description: Encryption Key
Old:         *****
New:         ******
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:21:26 Oct 16 2024
Description: Phase 2 Authentication
Old:         SHA1
New:         None
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:21:26 Oct 16 2024
Description: Phase 1 Encryption
Old:         AES-128
New:         3DES
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:21:26 Oct 16 2024
Description: Phase 1 (IKE) Exchange
Old:         IKEv2 Mode
New:         Main Mode
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)
```

Firewall Internal Admin Audit Records


```
Timestamp:   15:21:26 Oct 16 2024
Description: Destination Networks
Old:
New:         DEAG_Test
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:21:26 Oct 16 2024
Description: Local Networks
Old:
New:         X0 Subnet
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:21:26 Oct 16 2024
Description: Authentication Method
Old:
New:         IKE using Preshared Secret
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:21:26 Oct 16 2024
Description: Type of VPN Policy
Old:
New:         Site to Site
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:21:26 Oct 16 2024
Description: IPsec Gateway Address
Old:
New:         154.34.22.120
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:21:26 Oct 16 2024
Description: Added 'IPsec Name
Old:
New:         New York
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (46307)

Timestamp:   15:19:12 Oct 16 2024
Description: Local Group To User Object Dependency
Old:
New:         LAN Access66
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (45979)

Timestamp:   15:19:12 Oct 16 2024
Description: Local User To Group Object Dependency
Old:
New:         Uwe
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (45979)
```

Firewall Internal Admin Audit Records


```
Timestamp:   15:12:29 Oct 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (45536)

Timestamp:   22:23:49 Oct 15 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (63339)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_9775
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_3589
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_1045
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_550
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_8563
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_2603
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)
```

Firewall Internal Admin Audit Records


```
Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_8711
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_2820
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_4386
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:18 Oct 15 2024
Description: Deleted 'User Object
Old:         GW_432
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63264)

Timestamp:   22:23:12 Oct 15 2024
Description: Deleted 'Name of the Guest Profile
Old:         GaesteWeinkeller
New:
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (63209)

Timestamp:   21:40:12 Oct 15 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (61011)

Timestamp:   21:17:56 Oct 15 2024
Description: Generate Guest Accounts
Old:
New:
Status:      Succeeded
User:        Robert
Session:     API
Source:      10.10.10.10 (59166)

Timestamp:   21:17:35 Oct 15 2024
Description: Comments for the guest profile
Old:
New:
Status:      Succeeded
User:        Robert
Session:     API
Source:      10.10.10.10 (59105)
```

Firewall Internal Admin Audit Records


```
Timestamp:   21:17:35 Oct 15 2024
Description: Prefix for the randomly generated user name
Old:
New:         GW_
Status:      Succeeded
User:        Robert
Session:     API
Source:      10.10.10.10 (59105)

Timestamp:   21:17:35 Oct 15 2024
Description: Name of the Guest Profile
Old:
New:         GaesteWeinkeller
Status:      Succeeded
User:        Robert
Session:     API
Source:      10.10.10.10 (59105)

Timestamp:   21:00:13 Oct 15 2024
Description: Local Group To User Object Dependency
Old:
New:         SSLVPN Services
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (56724)

Timestamp:   21:00:13 Oct 15 2024
Description: Local User To Group Object Dependency
Old:
New:         Uwe
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (56724)

Timestamp:   20:53:01 Oct 15 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (56220)

Timestamp:   19:28:05 Oct 15 2024
Description: Enable Keep Alive
Old:         disabled
New:         enabled
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: Encryption Key
Old:         *****
New:         ******
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: Phase 2 Authentication
Old:         SHA1
New:         None
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)
```

Firewall Internal Admin Audit Records


```
Timestamp:   19:28:05 Oct 15 2024
Description: Phase 2 Encryption
Old:         AES-128
New:         AESGCM16-256
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: Phase 1 Encryption
Old:         AES-128
New:         AESGCM16-256
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: Destination Networks
Old:
New:         DEAG_Adress
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: Local Networks
Old:
New:         X0 Subnet
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: Authentication Method
Old:
New:         IKE using Preshared Secret
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: Type of VPN Policy
Old:
New:         Site to Site
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: IPsec Gateway Address
Old:
New:         10.20.30.40
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)

Timestamp:   19:28:05 Oct 15 2024
Description: Added 'IPsec Name
Old:
New:         Remote Site1
Status:      Succeeded
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51510)
```

Firewall Internal Admin Audit Records


```
Timestamp:   19:27:53 Oct 15 2024
Description: Enable Keep Alive
Old:         disabled
New:         enabled
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: Encryption Key
Old:         *****
New:         ******
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: Phase 2 Authentication
Old:         SHA1
New:         None
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: Phase 2 Encryption
Old:         AES-128
New:         AESGCM16-256
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: Phase 1 Encryption
Old:         AES-128
New:         AESGCM16-256
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: Destination Networks
Old:
New:         WAN-TZ570-10.10.10.254
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: Local Networks
Old:
New:         X0 Subnet
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: Authentication Method
Old:
New:         IKE using Preshared Secret
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)
```

Firewall Internal Admin Audit Records


```
Timestamp:   19:27:53 Oct 15 2024
Description: Type of VPN Policy
Old:
New:         Site to Site
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: IPsec Gateway Address
Old:
New:         10.20.30.40
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   19:27:53 Oct 15 2024
Description: Added 'IPsec Name
Old:
New:         Remote Site1
Status:      Failed
User:        mschmitz
Session:     API
Source:      10.10.10.10 (51450)

Timestamp:   18:58:40 Oct 15 2024
Description: Local Group To User Object Dependency
Old:
New:         Content Filtering Bypass
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47406)

Timestamp:   18:58:40 Oct 15 2024
Description: Local User To Group Object Dependency
Old:
New:         Isabel
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47406)

Timestamp:   18:58:40 Oct 15 2024
Description: Address Object in Group
Old:
New:         DEAG_Test
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47406)

Timestamp:   18:58:40 Oct 15 2024
Description: Address Object in Group
Old:
New:         150971-Test Interface IP
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47406)

Timestamp:   18:58:40 Oct 15 2024
Description: Address Object in Group
Old:
New:         060466 Subnets
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47406)
```

Firewall Internal Admin Audit Records


```
Timestamp:   18:58:40 Oct 15 2024
Description: Address Object Type
Old:
New:         GROUP
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47406)

Timestamp:   18:58:40 Oct 15 2024
Description: Address Object
Old:
New:         Isabel491c591950dc663a4094c097
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47406)

Timestamp:   18:57:29 Oct 15 2024
Description: User Object
Old:         Lololo
New:         Isabel
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47230)

Timestamp:   18:57:09 Oct 15 2024
Description: Local Group To User Object Dependency
Old:
New:         Guest Administrators
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47169)

Timestamp:   18:57:09 Oct 15 2024
Description: Local User To Group Object Dependency
Old:
New:         Robert
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47169)

Timestamp:   18:57:09 Oct 15 2024
Description: Deleted 'Local User To Group Object Dependency
Old:         Robert
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47169)

Timestamp:   18:57:09 Oct 15 2024
Description: User Object
Old:         Test
New:         Robert
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47169)

Timestamp:   18:56:28 Oct 15 2024
Description: User Object
Old:         webadmin
New:         Webadmin
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47062)
```

Firewall Internal Admin Audit Records


```
Timestamp:   18:56:18 Oct 15 2024
Description: User Object
Old:         udo
New:         Udo
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (47021)

Timestamp:   15:41:44 Oct 14 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (20634)

Timestamp:   13:00:25 Oct 14 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (12163)

Timestamp:   11:07:59 Sep 18 2024
Description: Enable packet capture
Old:         enabled
New:         disabled
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (55057)

Timestamp:   23:06:00 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (26597)

Timestamp:   23:05:24 Sep 16 2024
Description: SSLVPN Download URL (http://)
Old:         https://software.sonicwall.com
New:         software.sonicwall.com
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (26521)

Timestamp:   23:05:24 Sep 16 2024
Description: Enable SSH Management over SSL VPN
Old:         enabled
New:         disabled
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (26521)

Timestamp:   23:05:24 Sep 16 2024
Description: Enable web management over SSL VPN
Old:         enabled
New:         disabled
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (26521)
```

Firewall Internal Admin Audit Records


```
Timestamp:   22:59:11 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (26096)

Timestamp:   22:58:21 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (26059)

Timestamp:   22:52:24 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (25885)

Timestamp:   22:32:10 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (25234)

Timestamp:   22:21:27 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (24879)

Timestamp:   22:17:42 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (24675)

Timestamp:   22:05:55 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (21967)

Timestamp:   22:04:56 Sep 16 2024
Description: SSLVPN Download URL (http://)
Old:         https://software.sonicwall.com
New:         software.sonicwall.com
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (21840)
```

Firewall Internal Admin Audit Records


```
Timestamp:   22:04:56 Sep 16 2024
Description: Enable SSH Management over SSL VPN
Old:         disabled
New:         enabled
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (21840)

Timestamp:   22:04:56 Sep 16 2024
Description: Enable web management over SSL VPN
Old:         disabled
New:         enabled
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (21840)

Timestamp:   21:59:20 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (21493)

Timestamp:   21:57:28 Sep 16 2024
Description: SSLVPN Download URL (http://)
Old:         https://software.sonicwall.com
New:         software.sonicwall.com
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (21281)

Timestamp:   21:57:28 Sep 16 2024
Description: Enable SSH Management over SSL VPN
Old:         enabled
New:         disabled
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (21281)

Timestamp:   21:57:28 Sep 16 2024
Description: Enable web management over SSL VPN
Old:         enabled
New:         disabled
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (21281)

Timestamp:   16:21:42 Sep 16 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (10997)

Timestamp:   19:51:57 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (37909)
```

Firewall Internal Admin Audit Records


```
Timestamp:   19:39:35 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (37394)

Timestamp:   19:32:46 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (37142)

Timestamp:   19:22:19 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36826)

Timestamp:   19:21:02 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36782)

Timestamp:   19:19:56 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36743)

Timestamp:   19:18:14 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36691)

Timestamp:   19:17:55 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36679)

Timestamp:   19:16:59 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36645)
```

Firewall Internal Admin Audit Records


```
Timestamp:   19:16:15 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36606)

Timestamp:   19:13:14 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36514)

Timestamp:   19:12:06 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (36485)

Timestamp:   15:31:32 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (29957)

Timestamp:   15:29:22 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (29869)

Timestamp:   14:56:37 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (28726)

Timestamp:   14:41:56 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (28304)

Timestamp:   13:51:30 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (26658)
```

Firewall Internal Admin Audit Records


```
Timestamp:   12:56:31 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (25065)

Timestamp:   12:54:13 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (24994)

Timestamp:   12:52:01 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (24926)

Timestamp:   20:15:22 Sep 12 2024
Description: Export Configuration
Old:
New:
Status:      Succeeded
User:        admin
Session:     API
Source:      10.10.10.10 (23695)
```

Product Life Cycle Information

Explanation

This is information about the product lifecycle. For more information and explanation please refer to https://www.sonicwall.com/support/product-lifecycle-tables/

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

Summary

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

Firmware Version Check

Explanation

Here we compare the installed firmware with the latest available on MySonicWall.

Firmware Version Check:

```
Firmware Installed on Firewall:  7.1.1-7047-R5557
Latest Firmware on MySonicWall:
Firmware Release Date:
Release Note URL:
```

Summary

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

Firmware and Settings History

Explanation

The following table shows the history of the settings and firmware. Here it is shown how often the settings were migrated und if unsupported firmware downgrades were performed. A downgrade is unsupported, if no settings of the lower version were imported after the downgrade.

Firmware	TimeStamp	Action
7.1.1-7047-5557	01.03.2024 07:37	Firmware applied
7.0.1-5145-2363	24.01.2024 01:33	Settings import
7.1.1-7040-5387	24.01.2024 08:25	Firmware applied

Summary

Information regarding the firmware & settings history of this firewall

Caution: Possible unallowed Firmware downgrade found.
Please check manually!
(This information might not be correct as sometimes version numbers do not follow a unique schema)
A firmware downgrade without importing settings created with this downgrade version (or older) is not supported by SonicWall Technical Support!

Converted Settings with Conversion Tool

Explanation

This report shows if settings were converted via SonicWalls Conversion Tool

Details

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

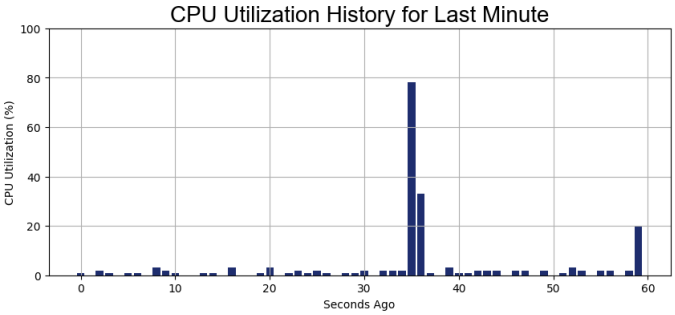
Firewall Utilization

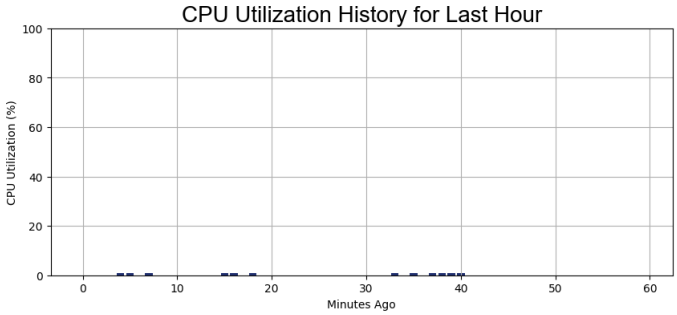
Explanation

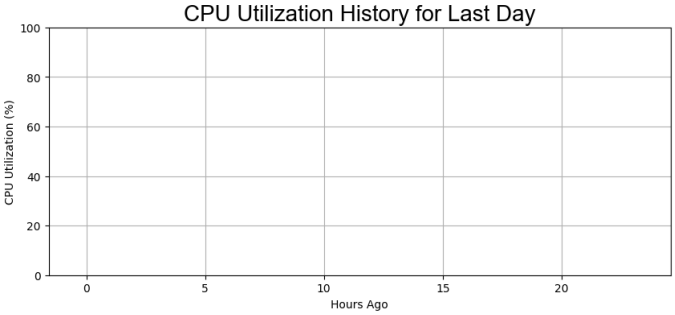
These graphs show the utilization of the firewall in the time before the data was exported. A high utilization can lead to problems as packets are not transmitted or delays are produced. The Technical Support Report that is used to pull the data should be created in a high-load moment. More reliable results are produced ba netflow or SNMP bases external systems. For Netflow reporting, SonicWall has a product called "Analytics" that work perfect with SNWL Firewalls. If there is no data for the reported timeframe, check if the firewall is operating in HA (High Availability mode). If during the reported timeframe the backup firewall was active, this report cannot show utilization data.

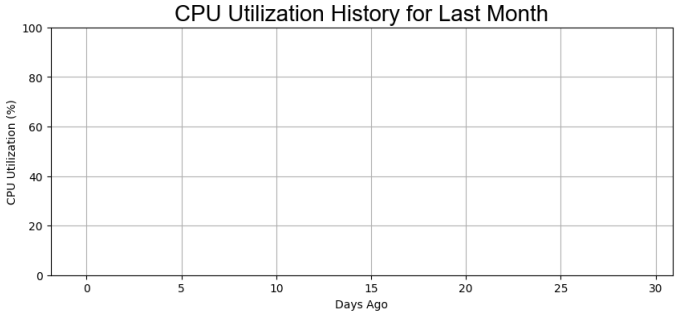
Timeframe	Avg Util	Status
Minute:	3 %	uncritical
Hour:	0 %	uncritical
Day:	0 %	uncritical
Month:	0 %	uncritical

Performance Utilization Graphs









Reliability - High Availability

Explanation

Importance of High Availability on Firewall Systems

1. Continuous Security: High availability (HA) ensures that firewall systems remain operational without interruption. This is critical for maintaining continuous protection against cyber threats, even during hardware failures or maintenance activities.

2. Minimized Downtime: HA configurations minimize network downtime by providing redundancy. If a primary firewall fails, a secondary firewall immediately takes over, ensuring that network services remain available and operational.

3. Improved Reliability: By having multiple firewalls in an HA setup, the network becomes more resilient to failures. This reliability is essential for maintaining business operations and avoiding costly disruptions.

4. Business Continuity: For businesses, especially those that rely heavily on online services and real-time data, any downtime can lead to significant financial losses. HA supports business continuity by ensuring that critical applications and services remain accessible.

5. Load Balancing: Some HA configurations also support load balancing, which can distribute traffic evenly across multiple firewalls. This improves overall network performance and prevents any single device from becoming a bottleneck.

6. Disaster Recovery: HA is a key component of disaster recovery plans. In case of a primary firewall failure, the secondary firewall ensures that security policies and protections continue to function, protecting the network during recovery efforts.

7. Compliance Requirements: Many industries have regulatory requirements for uptime and security. Implementing HA helps businesses comply with these standards by ensuring high availability and robust protection.

8. Customer Satisfaction: High availability contributes to better customer experiences by ensuring that services are always available, leading to higher customer satisfaction and retention.

Summary
High availability on firewall systems is essential for maintaining continuous security, minimizing downtime, and ensuring business continuity. It improves reliability, supports disaster recovery, meets compliance requirements, and enhances customer satisfaction by providing uninterrupted access to network services.

Reliability - High Availability

High Availability Status	
High Availability:	enabled
HA primary Serial-Number:	0040XXXXXXX Demo
HA secondary Serial-Number:	0040XXXXXXX Demo
Stateful Sync:	enabled
Preempt Mode:	disabled
HA-Role:	Primary
HA Peer in sync:	no
HA Firmware mismatch with peer:	no
HA-Firewall Status:	ACTIVE

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: For businesses, any network downtime can lead to significant financial losses and reduced customer satisfaction. WAN failover supports business continuity by minimizing disruptions and maintaining access to critical applications and services.

4. Load Balancing and Improved Performance: Some firewall systems with WAN failover capabilities also support load balancing. This optimizes bandwidth usage and improves network performance by distributing traffic across multiple WAN links.

5. Disaster Recovery: In the event of a failure in the primary WAN connection, having a failover mechanism ensures that disaster recovery processes can proceed without interruption, safeguarding data integrity and business operations.

6. Security: Firewalls with WAN failover capabilities help maintain security measures by ensuring that all traffic, even during a failover event, passes through the firewall, keeping the network protected from external threats.

7. Cost Savings: While there is an upfront cost for implementing WAN failover, the long-term benefits of avoiding downtime, maintaining productivity, and ensuring customer satisfaction can result in significant cost savings.

Summary

WAN failover on firewall systems is a critical feature for maintaining internet connectivity, ensuring business continuity, enhancing reliability, and improving overall network performance and security. It helps prevent downtime, supports disaster recovery, and can lead to significant cost savings for businesses.

Reliability WAN Failover

WAN Interface Summary

Number of WAN Interfaces configured & enabled: 2

Interface	Type	Comment	PacketsIn	PacketsOut
X1	WAN	Default WAN	5754753	2968353
X5	WAN		None	None

WAN Load Balancing is: not enabled

Summary

It seems that additional WAN lines are not used by the system because Wan Load Balancing is disabled and no routes for additional WAN Interfaces were found. This should be checked.

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		31 Jan 2025
Gateway Anti-malware/Intrusion Prevention/App Control	Licensed		16 Feb 2025
Capture Client Basic	Not Licensed		
Capture Client Advanced	Not Licensed		
Capture Client Premier	Not Licensed		
Content Filtering Service	Licensed		16 Feb 2025
SSL VPN	Licensed	2 Max: 100	
Global VPN Client	Licensed	50 Max: 1000	
Stateful High Availability	Licensed		
Capture Advanced Threat Protection	Licensed		16 Feb 2025
Syslog Analytics	Expired		03 Feb 2024
DNS Filtering	Licensed		31 Jan 2025
Essential Protection Service Suite	Licensed		16 Feb 2025
Advanced Protection Service Suite	Not Licensed		
24x7 Support	Licensed		16 Feb 2025
Standard Support	Not Licensed		

Security Audit Summary

Explanation

This report provides a high-level summary of the key findings from the security audit and includes actionable recommendations for addressing potential vulnerabilities. For more in-depth information and specific details, please refer to the full audit report

Feature	Status	Recommendation
Firmware and Settings		
Firmware Version:	update available	upgrade firmware
- Unallowed Firmware downgrade	possible	please verify
High Availability		
High Availability	enabled	-
- enable Stateful Sync:	enabled	-
- preempt mode	disabled	-
WAN Lines		
Multiple WAN Lines	configured	-
WAN Load-Balancing is enabled	no	enable WAN Load Balancing
VPN		
Weak ciphers found	no	-
Firewall internal audit		
Internal Audit	on	-
Detection Prevention		
Stealth Mode	on	-
Randomize IP IDs	on	-
Packet Capture		
Packet Capture	on	Disable if not needed
Users Account Protection		
WAN MTU Settings		
X1 Default WAN 1500	ok	-
X5 1500	ok	-

Statistic	Count
Rules	
- IPv4: Total Number of Rules:	227
- IPv6: Total Number of Rules:	89
- IPv4: Rules never used:	0
- IPv4: Rules never used:	0
- IPv4: Any <> Any Rules:	33
- IPv6: Any <> Any Rules:	44
- IPv4: Management Rules:	44
- IPv6: Management Rules:	27
- IPv4: Rules WAN > intern:	0
- IPv6: Rules WAN > intern:	0
- IPv4: Rules not used for a long time:	0
- IPv6: Rules not used for a long time:	89
- IPv4: Disabled Firewall Rules:	50
- IPv6: Disabled Firewall Rules:	0
NAT Policies	
- IPv4: Nat Policies never used	0
- IPv6: Nat Policies never used	0
- IPv4: Nat Policies disabled	0
- IPv6: Nat Policies disabled	0