

# Configuration Audit



## Appliance Details

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

## Report Details

Date & Time Report created: 06.10.2025 - 17:56:30  
  
EXP File: C:\U...\Repository\0040XXXXXXXX\exp\_api\_downloaded.exp  
EXP Timestamp: 06.10.2025 17:51  
  
TSR File: C:\U...\Repository\0040XXXXXXXX\tsr\_api\_downloaded.wri  
TSR Timestamp: 06.10.2025 17:51

## 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: 7.3.0-7012-R8150

Latest Firmware on MySonicWall: 7.3.0-7012

### Summary

The newest firmware for this model is already installed

## 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. As well, an aged configuration that has been used on multiple different devices or has been migrated frequently can cause problems.

| Firmware        | TimeStamp           | Action           | Comment |
|-----------------|---------------------|------------------|---------|
| 7.0.1-5145-2363 | 2024-01-24 01:33:01 | Settings import  |         |
| 7.1.1-7040-5387 | 2024-01-24 08:25:53 | Firmware applied |         |
| 7.1.1-7047-5557 | 2024-03-01 07:37:45 | Firmware applied |         |
| 7.1.1-7047-5557 | 2024-11-27 18:21:03 | Settings import  |         |
| 7.1.1-7058-6162 | 2024-12-03 20:01:06 | Firmware applied |         |
| 7.1.1-7058-6162 | 2025-02-05 21:58:08 | Settings import  |         |
| 7.1.1-7058-6162 | 2025-03-21 16:23:00 | Settings import  |         |
| 7.1.3-7015-6965 | 2025-03-31 21:24:27 | Firmware applied |         |
| 7.3.0-7012-8150 | 2025-09-08 18:29:24 | Firmware applied |         |

### Summary

No unallowed firmware downgrade found

## 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

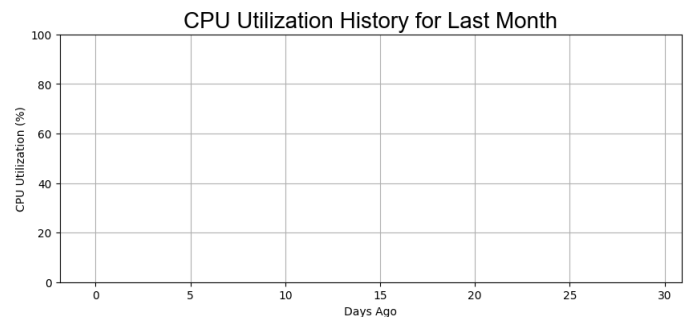
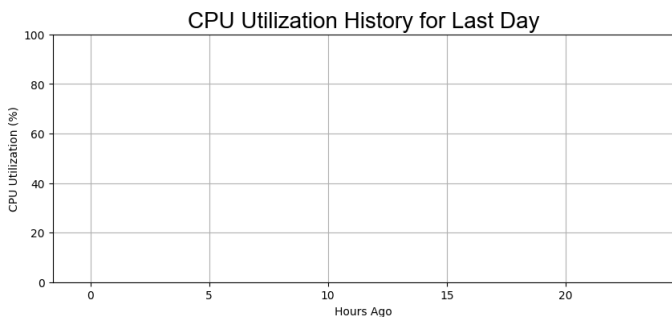
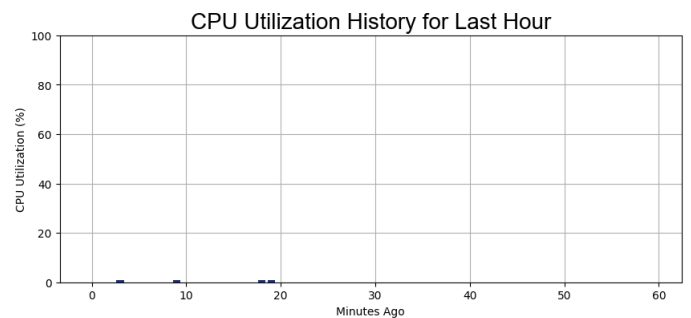
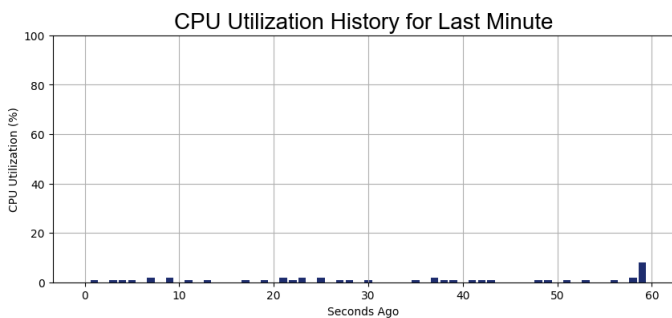
## Firewall Utilization

### 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 by netflow or SNMP based external systems. For Netflow reporting, SonicWall has a product called "Analytics" that works perfectly 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:   | 0 %      | 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:       | 0040XXXXXXXX Demo |
| HA secondary Serial-Number:     | 0040XXXXXXXX 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 | None      | None       |
| X5        | WAN  |             | None      | None       |

WAN Load Balancing is: not enabled

## Security Services License Check

### Explanation

*This report shows if services have an active license*

## Security Services License Check

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