

Sonicwall NSa3800

SonicWall NSa3800 Next-Generation Firewall Instruction Manual

Model: NSa3800 (Part Number: 03-SSC-1843)

1. INTRODUCTION

The SonicWall NSa3800 Next-Generation Firewall is designed to provide advanced security and network performance for large enterprises and distributed networks. This appliance offers robust threat prevention, secure SD-WAN capabilities, and high throughput to protect your network infrastructure.

Key features include:

- High firewall throughput and threat prevention capabilities.
- Multiple Ethernet and SFP+ interfaces for flexible connectivity.
- Support for a large number of concurrent connections and VPN tunnels.
- Integration with SonicWall services like Capture ATP sandboxing, intrusion prevention, and TLS 1.3 inspection.



Figure 1: SonicWall NSa3800 Next-Generation Firewall, front view.

2. SETUP

This section outlines the steps for physically setting up your SonicWall NSa3800 appliance.

2.1 Unpacking and Inspection

Carefully unpack the NSa3800 appliance and its accessories. Inspect all components for any signs of damage. If any items are damaged or missing, contact SonicWall support immediately.

2.2 Front Panel Overview

Familiarize yourself with the front panel ports and indicators.

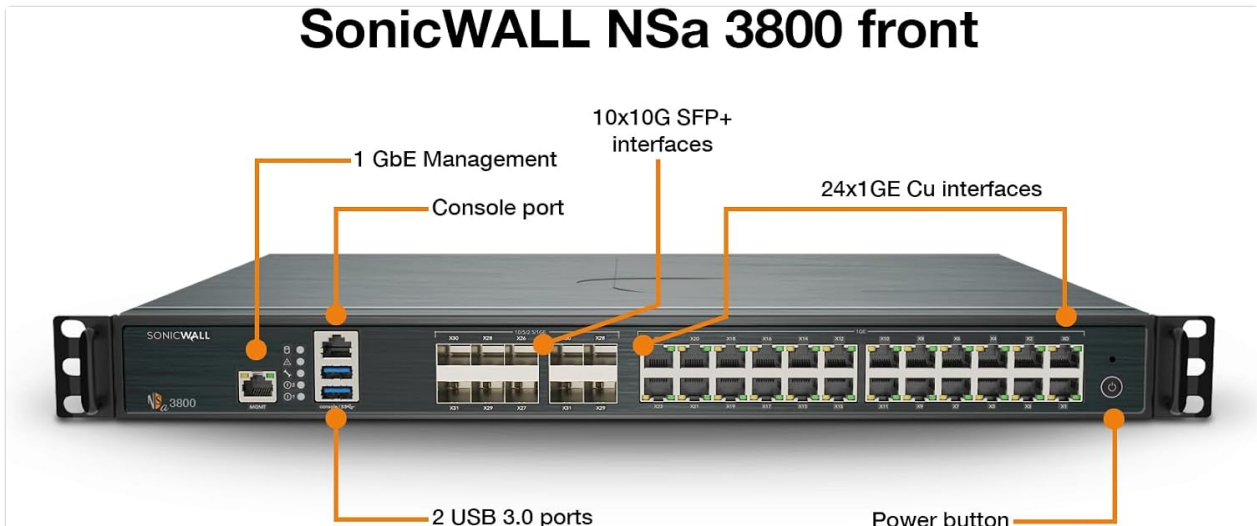


Figure 2: Front panel of the SonicWall NSa3800, showing 1 GbE Management port, Console port, 2 USB 3.0 ports, 10x10G SFP+ interfaces, 24x1GE Cu interfaces, and Power button.

2.3 Rear Panel Overview

Understand the rear panel connections, including power and optional redundant power.



Figure 3: Rear panel of the SonicWall NSa3800, indicating the Power Adapter input and an Optional Redundant Power Adapter slot.

2.4 Rack Mounting

The NSa3800 is designed for rack installation. Secure the appliance in a standard 19-inch rack using the provided rack-mount kit. Ensure adequate ventilation around the unit.



Figure 4: SonicWall NSA3800 appliance securely mounted in a server rack.

2.5 Initial Power-On and Connectivity

1. Connect the power cable to the appliance and a grounded power outlet.
2. Press the power button on the front panel.
3. Connect the 1 GbE Management port to your network for initial configuration.
4. For advanced configuration, connect a console cable to the Console port and use a terminal emulator.
5. The NSA3800 supports zero-touch deployment, simplifying initial setup and configuration.

3. OPERATING THE NSA3800

The SonicWall NSA3800 operates on SonicOS, providing a comprehensive suite of security and networking features. This section covers general operational aspects.

3.1 Core Functionality

The NSA3800 functions as a Next-Generation Firewall, offering:

- **Firewall Inspection:** Stateful packet inspection and deep packet inspection for network traffic.
- **Threat Prevention:** Intrusion Prevention System (IPS), anti-malware, and Capture ATP sandboxing.
- **Secure SD-WAN:** Optimizes network performance and security for distributed environments.
- **VPN:** Supports IPsec VPN and SSL VPN for secure remote access and site-to-site connectivity.
- **TLS 1.3 Inspection:** Decrypts and inspects encrypted traffic for hidden threats.

3.2 Performance Metrics

The NSA3800 is engineered for high performance in demanding network environments.



SonicWall NSa 3800

- 8 Gbps** IPSec VPN throughput
- 512** Access points supported
- 3,000** Site-to-site VPN tunnels
- 50 (1,000)** IPSec VPN clients (max)

Figure 5: Performance metrics for the SonicWall NSa3800, including IPS Throughput, Anti-Malware Inspection Throughput, Threat Protection Throughput, Firewall Inspection Throughput, TLS/SSL inspection and encryption throughput, and IPSec VPN Throughput.

3.3 Deployment Scenarios

The NSa3800 can be deployed in various network architectures, including Internet Edge and Campus/Private Edge Network configurations.

Deployments

The Gen 8 NSa Series has two main deployment options for medium and distributed enterprises:

Internet Edge Deployment

In this standard deployment option, the Gen 8 NSa Series NGFW protects private networks from malicious traffic coming from the internet, allowing you to:

- Deploy a proven NGFW solution with highest performance in its class
- Gain visibility and inspect encrypted traffic, including TLS 1.3, to block evasive threats coming from the Internet — all without compromising performance
- Protect your enterprise with integrated security, including malware analysis, cloud app security, URL filtering and reputation services
- Save space and money with an integrated NGFW solution that includes advanced security and networking capabilities
- Reduce complexity and maximize efficiency using a central management system delivered through an intuitive single-pane-of-glass user interface

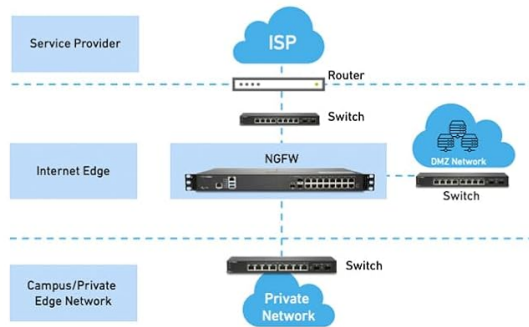


Figure 6: Deployment options for the NSa Series, showing how the NGFW integrates into Internet Edge and Campus/Private Edge Network setups.

4. MAINTENANCE

Regular maintenance ensures optimal performance and security of your NSa3800 appliance.

- **Firmware Updates:** Regularly check for and apply the latest SonicOS firmware updates to ensure you have the most current security features and bug fixes.
- **Configuration Backups:** Periodically back up your appliance configuration. This allows for quick recovery in case of unforeseen issues.
- **System Monitoring:** Monitor system logs and performance metrics through the SonicOS interface to identify and address potential issues proactively.
- **Physical Inspection:** Ensure the appliance has adequate airflow and that all cables are securely connected. Keep the environment clean and free of dust.

5. TROUBLESHOOTING

This section provides basic troubleshooting steps for common issues.

- **No Power:** Verify the power cable is securely connected to both the appliance and the power outlet. Check the power button status.
- **Network Connectivity Issues:** Ensure Ethernet cables are properly connected to the correct ports. Check network configurations in SonicOS. Verify upstream network devices (modems, switches) are functioning.
- **Slow Performance:** Review system logs for high resource utilization. Check for active threats or misconfigured security policies that might be impacting performance.
- **Accessing Management Interface:** Confirm your computer's IP address is in the same subnet as the management interface. Clear browser cache or try a different browser.
- **Consult Documentation:** For detailed troubleshooting, refer to the comprehensive SonicWall NSa3800 administration guide available on the official SonicWall support portal.

6. SPECIFICATIONS

Detailed technical specifications for the SonicWall NSa3800 Next-Generation Firewall.

Feature	Specification
Brand	Sonicwall
Model Name	NSa3800
Model Number	03-SSC-1843
Connectivity Technology	Ethernet
Operating System	SonicOS
Number of Ports	32
Data Transfer Rate	20 Gigabits Per Second
LAN Port Bandwidth	10 Gbps
Wireless Communication Standard	802.11 ac
Frequency Band Class	Dual-Band

Feature	Specification
Recommended Uses	Business
Special Feature	QoS
UPC	758479318439
GTIN	758479318439

7. WARRANTY AND SUPPORT

For warranty information, please refer to the official SonicWall warranty policy available on their website or contact your authorized SonicWall reseller. SonicWall provides comprehensive technical support for its products.

7.1 Technical Support

If you encounter issues that cannot be resolved using this manual or the online documentation, please contact SonicWall Technical Support. Have your product serial number and a detailed description of the issue ready. You can find support resources, including knowledge bases, forums, and contact information, on the official SonicWall support portal: www.sonicwall.com/support