SonicOS 7

Getting Started Guide

for NSsp 10700, 11700, 13700, and NSa Series

SONICWALL®

Contents

Introduction **4**

NSa Series Overview **5**

Deployment Options 5

Internet Edge Deployment 6

Medium and Distributed Enterprises 7

NSa Hardware Features 7

NSa System Requirements 9

NSsp 10700, 11700, and 13700 Overview **11**

Features 11

Connectivity, Port Density and Performance 12

Firmware Features 12

Hardware Features 13

+ 13

Rear Panel 16

System Specifications 17

Determining the WAN Type **18**

System Setup **20**

Default Settings 20

System Startup 21

Basic Configuration 23

Registration and Licensing 24

Creating a MySonicWall Account 24

Setup Options **26**

Zero Touch 26

Setting Up with NSM 26

Setting Up with SonicExpress 29

Setting Up with CLI 30

Running the Setup Wizard **31**

Testing and Troubleshooting Connectivity **33**

Testing Your Internet Connection 33

Troubleshooting your Internet Connection 33

Troubleshooting Your MGMT Connection 34
Troubleshooting Your LAN Connection 34
Using SafeMode 34

Migration Tool 35
About Migration 35
Using the Migration Tool 36

SonicWall Support 39
About This Document 40

1

Introduction

Today's distributed IT—where end points are on premises, in the cloud, in the data center, at a branch office or in a home office—is creating an unprecedented explosion of exposure across organizations. As the exposure points to multiply, business risks continue to escalate, and each one needs to be protected from today's sophisticated threats. SonicWall offers several firewall models to suit your business.

The NSa Series offers a mid-range solution. They are designed for businesses having 250 users and up. With cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, secure SD-WAN, real-time visualization, and WLAN management, the NSa Series provides flexible, fast and cost-effective security to keep the threats out.

To resolve similar challenges for enterprise-level customers, the SonicWall Network Security services platform (NSsp) is a high-end firewall series delivering advanced threat protection and fast speeds demanded by large enterprises, data centers and service providers. The NSsp 10700, 11700, and 13700 are the enterprise firewall to replace existing NSa 9650 firewalls.

This document describes how to get started on one of the firewalls from the NSa Series or on the NSsp 10700, 11700, and 13700. These systems run classic SonicOS 7. It also includes information on how to migrate the configuration settings from older firewalls to firewalls covered by this document.

ⓘ **NOTE:** This document does not include information pertaining to the NSsp 15700. For more information about that firewall, refer to SonicOS 7 NSsp 15700 Getting Started Guide.

Topics in this document include:

- NSa Series Overview
- NSsp 10700, 11700, and 13700 Overview
- Determining the WAN Type
- System Setup
- Setup Options
- Running the Setup Wizard
- Testing and Troubleshooting Connectivity
- Migration Tool

2

NSa Series Overview

The NSa Series offers a mid-range solution. They are designed for businesses having 250 users and up. With cloud-based and on-box capabilities like TLS/SSL decryption and inspection, application intelligence and control, secure SD-WAN, real-time visualization, and WLAN management, the NSa Series provides flexible, fast and cost-effective security to keep the threats out.

The updated NSa Series has been built from the ground up with the latest hardware components, all designed to deliver multi-gigabit threat prevention throughput — even for encrypted traffic. The firewalls support high port density, including multiple 40 GbE and 10 GbE ports, hardware redundancy with high availability, and dual power supplies, depending on the model.

This section describes how to get started on one of the firewalls from the NSa Series:

- Deployment Options
- NSa Hardware Features
- NSa System Requirements

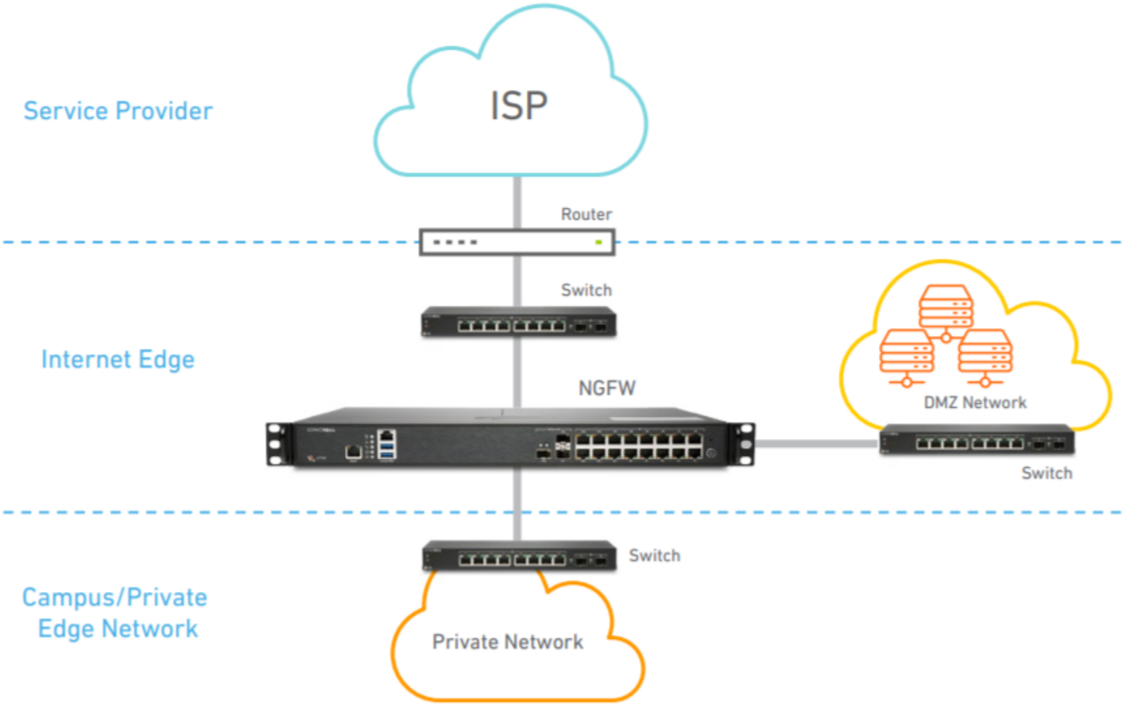
Deployment Options

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

- Internet Edge Deployment
- Medium and Distributed Enterprises

Internet Edge Deployment

In this standard deployment option, the NSa Series—a next generation firewall (NGFW)—protects private networks from malicious traffic coming from the Internet.

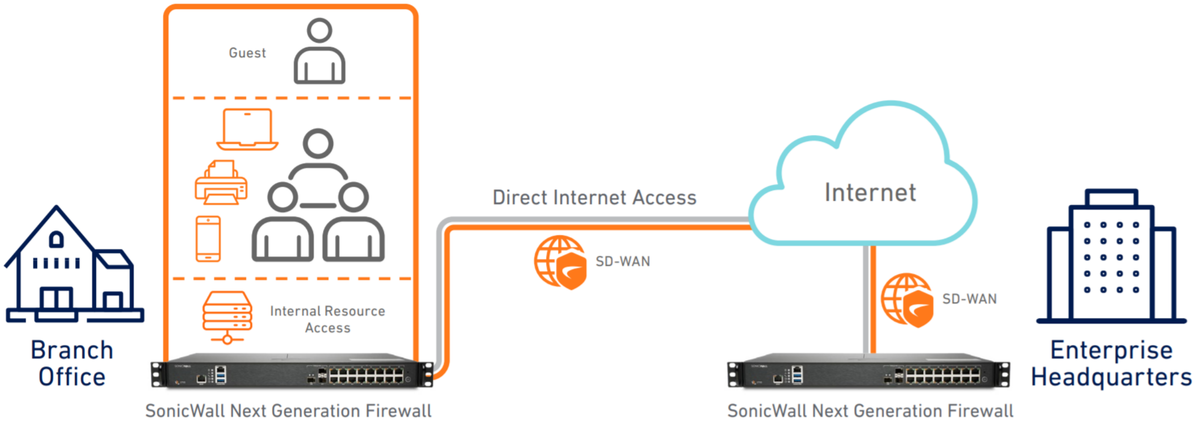


It allows you to:

- Deploy a proven NSa Series solution with highest performance and port density (including 40 GbE and 10 GbE connectivity) 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 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

Medium and Distributed Enterprises

The SonicWall NSa Series supports SD-WAN and can be centrally managed, making it an ideal fit for medium and distributed enterprises.



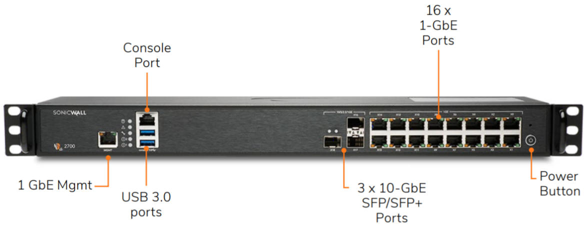
This deployment allows organizations to:

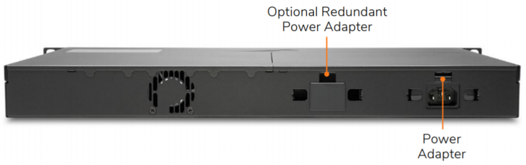
- Future-proof against an ever-changing threat landscape by investing in a firewall with multigigabit threat analysis performance
- Provide direct and secure Internet access to distributed branch offices instead of back-hauling through corporate headquarters
- Allow distributed branch offices to securely access internal resources in corporate headquarters or in a public cloud, significantly improving application latency
- Automatically block threats that use encrypted protocols such as TLS 1.3, securing networks from the most advanced attacks
- Reduce complexity and maximize efficiency using a central management system delivered through an intuitive single pane of glass user interface
- Leverage high port density that includes 40 GbE and 10 GbE connectivity to support a distributed enterprise and wide area networks

NSa Hardware Features

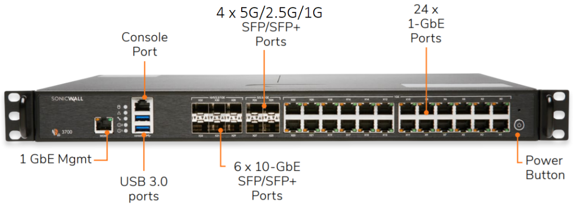
The following images show the front and back panel of each of the NSa Series firewalls. The ports and key features are also identified.

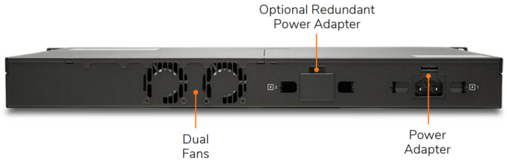
NSa 2700:



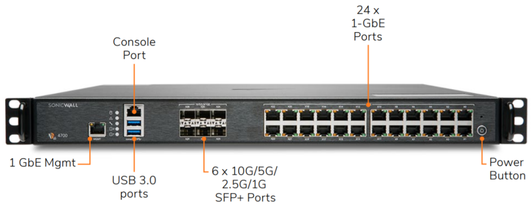


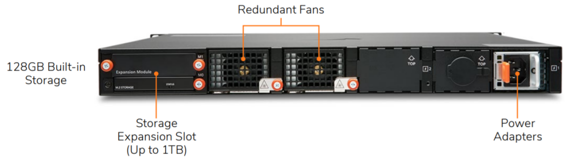
NSa 3700:



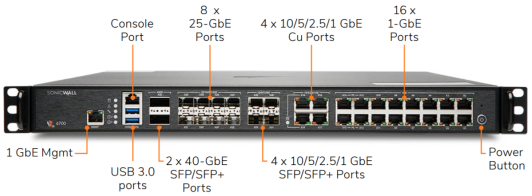


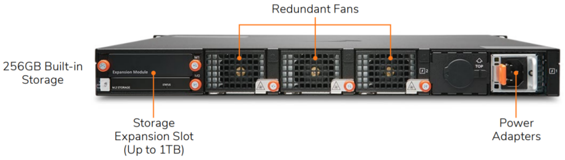
NSa 4700:





NSa 6700:


Console Port
8 x 25-GbE Ports
4 x 10/5/2.5/1 GbE Cu Ports
16 x 1-GbE Ports
1 GbE Mgmt
USB 3.0 ports
2 x 40-GbE SFP/SFP+ Ports
4 x 10/5/2.5/1 GbE SFP/SFP+ Ports
Power Button



NSa System Requirements

The NSa Series firewalls meet the following system requirements:

Model	NSa 2700	NSa 3700	NSa 4700	NSa 6700
Storage	64GB (M.2)	128GB (M.2)	128 GB	256GB (M.2)
System Memory	Storage expansion slot, up to 256GB	Storage expansion slot, up to 256GB	Storage expansion slot, up to 1TB	Storage expansion slot, up to 1TB
VLAN interfaces	256	256	512	512
Maximum access point supported	32	32	512	512
Interfaces	• 16 x 1GbE • 3 x 10G SFP+ • 2 USB 3.0 • 1 Console • 1 Mgmt port	• 24 x 1GbE, • 6 x 10G SFP+ • 4 x 5G/2.5G/1G SFP/SFP+ • 2 USB 3.0 • 1 Console • 1 Mgmt port	• 6 x 10G/5G/2.5G/1G SFP+ • 24 x 1GbE, • 2 USB 3.0 • 1 Console • 1 Mgmt port	• 2 x 40G QSFP28 • 8 x 25G/10G/5G/2.5G/1G SFP28 • 4 x 10G/5G/2.5G/1G SFP+ • 4 x 10G/5G/2.5G/1G Cu • 16 x 1GbE, • 2 USB 3.0 • 1 Console • 1 Mgmt port

Model	NSa 2700	NSa 3700	NSa 4700	NSa 6700
Fans	1	2	2 (removable)	2 (removable)
Power supply	60W	90W	1x350W	1x350W
Chassis Dimension (1U)	16.9 x 12.8 x. 1.8 in 43 x 32.5 x 4.5 cm	16.9 x 12.8 x. 1.8 in 43 x 32.5 x 4.5 cm	16.9 x 18.1 x. 1.8 in 43 x 46.5 x 4.5 cm	16.9 x 18.1 x. 1.8 in 43 x 46.5 x 4.5 cm

3

NSsp 10700, 11700, and 13700 Overview

The SonicWall Network Security services platform (NSsp) firewall series delivers the advanced threat protection, fast speeds and budget friendly price that large enterprises, data centers, and service providers require. Designed for large distributed enterprises, data centers, government agencies and service providers, the NSsp 10700, 11700, and 13700 pairs advanced technologies like Real-Time Deep Memory Inspection (RTDMI™) with high-speed performance.

The NSsp 10700, 11700, and 13700 are a high-end firewall delivering advanced threat protection and the fast speeds demanded by large enterprises, data centers and service providers. The NSsp 10700, 11700, and 13700 are the enterprise firewall to replace existing NSa 9650 firewalls.

Topics:

- Features
- System Specifications

Features

The SonicWall NSsp 10700, 11700, and 13700 are the next-generation firewall (NGFW) with multiple interfaces (100/40/25/10/5/2.5/1.0 GbE), capable of processing millions of connections. Its high-speed connectivity and large port density—coupled with superior IPS and TLS1.3 inspection support—make the NSsp 10700, 11700, and 13700 are an ideal threat protection platform for enterprise Internet edge and data center deployments. SonicWall NSsp 10700, 11700, and 13700 combine validated security effectiveness and best-in-class price performance in a high-end, single-rack-mountable NGFW appliance.

Topics:

- Connectivity, Port Density and Performance
- Firmware Features

Connectivity, Port Density and Performance

The NSsp 10700, 11700, and 13700 are an energy-efficient, reliable appliances in a compact form factor. It can process millions of encrypted and unencrypted connections to deliver the security required for large organizations. The high-port-density NSsp 10700, 11700, and 13700 include the following interfaces:

- 2 100GbE and 40GbE interfaces
- 8 25/10/5/2.5/1G interfaces
- 8 10/5/2.5/1GbE interfaces
- 16 1GbE interfaces

It also features a dedicated management port, 512GB of built-in storage, and redundant power supplies and fans. Performance specifications are targeted at:

- 45 Gbps of threat prevention throughput
- 57 Gbps of application inspection throughput
- 48 Gbps of IPS throughput
- 5 Gbps of TLS inspection throughput
- 14 million stateful connections
- 12 million DPI connections

Firmware Features

The SonicWall NSsp 10700, 11700, and 13700 runs on SonicOS 7.0.1, a new operating system built to deliver a modern user interface, intuitive workflows, and user-first design principles. SonicOS 7 provides multiple features that facilitate enterprise-level workflows, easy configuration, and simplified management—all of which allow enterprises to improve both their security and operational efficiency. SonicOS 7 features:

- Sandboxing using Reassembly-Free Deep Packet Inspection® (RFDPI) and Real-Time Deep Memory Inspection™ (RTDMI) technology
- Secure SD-WAN
- High Availability
- TLS 1.3 support
- DNS Security
- Gateway Anti-Virus, Intrusion Prevention, and Application Control
- Capture ATP Multi-Engine Sandboxing
- URL Filtering
- Error-free change management with Network Security Manager (NSM)
- New intuitive dashboards with single-pane-of-glass management

- New application framework
- Enhanced APIs
- Configuration audit
- Notification center providing actionable alerts
- Usage statistics for rules, objects and services

Hardware Features

Review the following for more details about the NSsp 10700, 11700, and 13700 hardware features.

Topics:

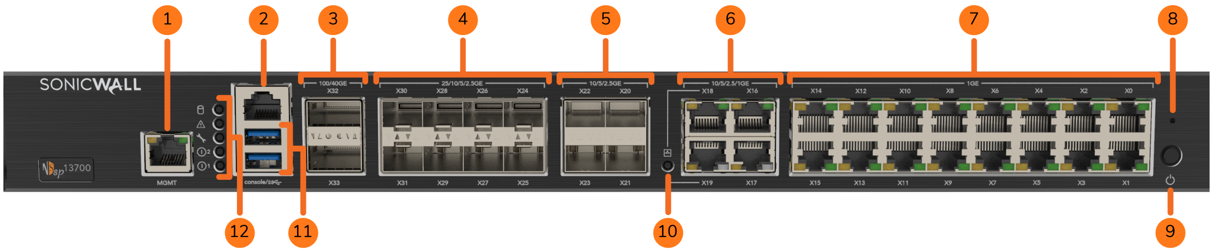
- +
- Rear Panel
- System Specifications

+

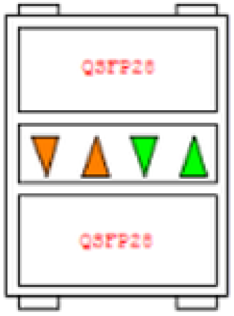
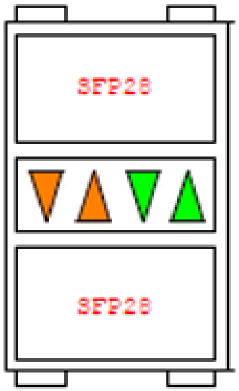
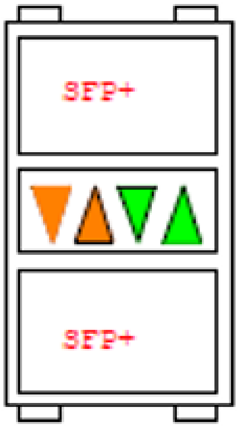
-Front Panel

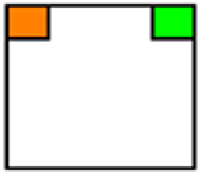
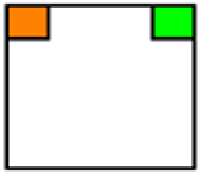
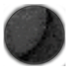
Refer to the following front panel and the associated table to understand the ports and LED lighting on the ports.

NSsp 10700, 11700, and13700 Front Panel



1	**MGMT**	**MGMT Port - RJ45**: The MGMT port is a dedicated 1GE interface for appliance management and SafeMode access. • Solid green = link at 1G or lower • Blinking green = activity
2	**console**	**Console Port - RJ45**: Serial Console for CLI access

3		**X32 - X33**	**Port form factor**: QSFP28 indicating MAX supporting speed of 100G. **Supported speeds**: 10G*/40G/100G *with QSFP to SFP+ adapter **100/40GE QSFP28 Ports and LEDs**: • Solid amber = link at 100G or 40G • Blinking amber = activity • Solid green = link at 1G or lower • Blinking green = activity • Off = no link **NOTE:** Breakout cables are not supported on these ports
4		**X24 - X31**	**Port form factor**: SFP/SFP+/SFP28 **Supported speeds**: 10M/100M/1G/10G/25G **25/10/5/2.5GE SFP28 Ports and LEDs**: • Solid amber = link at 25G, 10G, 5G, or 2.5G • Blinking amber = activity at 25G, 10G, 5G, or 2.5G • Solid green = link at 1G or lower • Blinking green = activity • Off = no link
5		**X20 - X23**	**Port form factor**: SFP+ **Supported speeds**: 10M/100M/1G/10G **10/5/2.5GE SFP+ Ports and LEDs**: • Solid amber = link at 10G, 5G, or 2.5G • Blinking amber = activity • Solid green = link at 1G or lower • Blinking green = activity • Off = no link

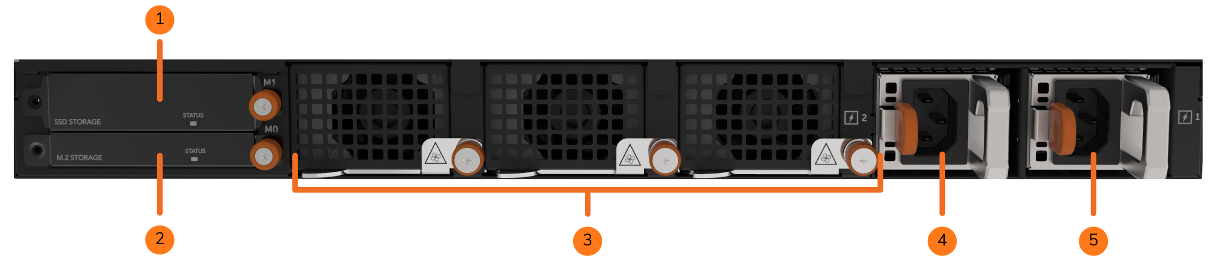
6		**X16 - X19**	**10/5/2.5/1GE Copper RJ45 Ports and LEDs**: • X18 and X19 are LAN Bypass ports • Solid green = link at speeds 1G or lower • Blinking green = activity at 1G or lower • Amber = unused • Off = no link
7		**X0 - X15**	**1GE Copper RJ45 Ports and LEDs**: • Solid green = link at speeds 1G or lower • Blinking green = activity at 1G or lower • Amber = unused • Off = no link
8			**SafeMode Button**: A recessed button used to enter SafeMode: • If NSsp is up, press button with a narrow, straight object. • If NSsp is down, press while connecting NSsp to power and hold until Test LED blinks yellow three times.
9			**Power Button**: • Short press powers ON if button was used to power system off. • Short press powers OFF with graceful shutdown. Test and Alarm LEDs turn red. Standby power to some circuitry stays on. • Long press (5+ sec) = forced shutdown. Standby power to some circuitry stays on.
10			**LAN Bypass LED**: When NSsp is without power and LED is off, LAN Bypass state is difficult to distinguish. It can be either: • Bypass disabled (default), traffic cannot pass • Bypass enabled, power is lost, traffic can pass Yellow = bypass active and traffic is passing while NSsp is powered but not available, such as during reboot. Green = bypass enabled and traffic can pass if firewall goes down.

11	SS	**USB SS 3.0 Ports**: For configuration, recovery, re-imaging the NSsp, and USB WWAN device support.
12	⛁	**Storage LED**: Status on internal and external storage. • Blinking green = activity • Yellow = storage warning • Off = no activity
13	⚠	**Alarm LED**: • Red = high Level alarm (such as fan failure) or power down requested • Yellow = lower level alarm
13	🔧	**Test LED**: • Red = power down requested • Yellow = initializing • Blinking yellow = SafeMode/FIPS test in progress • Off = normal
15	⏻	**Power LED: 1 = Primary, 2 = Redundant** • Blue = powered on • Yellow = defective redundant power supply

Rear Panel

Refer to the following rear panel illustration and the associated table to understand the slots and parts.

NSsp 10700, 11700, and 13700 Rear Panel



1	M1 slot for SSD: Extended storage drive

2	M0 slot for M.2 module: Boot drive
3	System fans (3)
4	Redundant power input
5	Primary power input

System Specifications

The NSsp 10700, 11700, and 13700 are built with an Intel-based CPU. It ships with a storage module and 350W redundant power supplies. It has compact footprint, requiring only one slot in the chassis. The hardware specifications for the NSsp 10700, 11700, and 13700 are listed below:

Model	**NSsp 10700, 11700, and 13700**
CPU model	Xeon D-2187NT
# Cores per CPU	16C (32T)
CPU frequency (Base/Max. Turbo)	2.0/3.0 GHz
Hardware security support	Intel QAT: 100 Gbps
System Memory, DDR4 2400 ECC, RDIMM	64 GB
Interfaces	• 2 x 100G/40G • 8 x 25G/10G/5/2.5G/1G SFP28 • 4 x 10G/5G/2.5G/1G SFP+ • 4 x 10G/5G/2.5G/1G Cu • 16 x GbE Cu • 1 GbE MGMT • 1 Console (RJ45) • 2 USB 3.0
Expansion (M1)	1TB SSD
Expansion (M0)	M.2 512 GB
Fan	3 (removable)
Power supply	2x 350W (removable)
Chassis Dimension (1U)	43cm x 46cm x 4.5cm

4

Determining the WAN Type

Before configuring your SonicWall appliance, you need to determine the type of WAN connection for your setup . SonicWall supports the following types:

- **Static**—Configures the appliance for a network that uses static IP addresses.
- **DHCP**—Configures the appliance to request IP settings from a DHCP server on the Internet.
- **PPPoE**—Point-to-Point Protocol over Ethernet (PPPoE) is typically used with a DSL modem. If your ISP requires desktop software with a username and password, select NAT with PPPoE mode.
- **PPTP**—Point-to-Point Tunneling Protocol (PPTP) is used to connect to a remote server. PPTP typically supports older Microsoft Windows implementations that require tunneling connectivity.
- **L2TP**—Layer 2 Tunneling Protocol (L2TP) is used to transmit Layer 2 data over IP or other Layer 3 routed networks. Internet Service Providers (ISPs) often use it to enable virtual private networks (VPNs) for customers over the Internet. It does not encrypt network traffic itself.

  ⓘ **NOTE:** If L2TP is not available in the Setup Wizard, you can configure it later in the SonicOS management interface.
- **Wire Mode (2-Port Wire)**—Inserts the appliance into the network using two paired interfaces. Available Wire Mode types include Bypass, Inspect, and Secure. Bypass mode allows for quick and non-disruptive insertion into the data path. Inspect mode extends Bypass mode with traffic inspection for classification and flow reporting. Secure mode provides full SonicWall ReAssembly-Free Deep Packet Inspection™ (RF-DPI) and control of network traffic.

  Secure Mode also affords the same level of visibility and enforcement as conventional NAT or L2 Bridged Mode deployments, but without any L3/L4 transformations, and with no alterations of ARP or routing behavior. If Wire Mode is not available in the Setup Wizard, you can configure it later in the SonicOS management interface.

  ⓘ **NOTE:** When operating in Wire Mode, the MGMT interface is used for local management. To enable remote management, dynamic security services, and application intelligence updates, a WAN interface (separate from the Wire Mode interfaces) must be configured for Internet connectivity.
- Tap Mode (1-Port Tap)—Using a single interface, the firewall connects to and receives mirrored packets from an adjacent switch SPAN port. Similar to Inspect mode in Wire Mode, but with a single port and not in the physical path of traffic.

  If Tap Mode is not available in the Setup Wizard, you can configure it later in the SonicOS management interface.

For more information about WAN types including Wire Mode, Tap Mode, L2TP, and others, refer to the SonicOS 7 Network Firewall Administration Guide at the Technical Documentation portal.

5

System Setup

While the firewalls described in this document have some differences in hardware, the implementation and setup follow much the same process. These sections described the basic setup information required. Additional setup options, those that leverage other applications or solutions, are described in Setup Options. For more details on specific features, refer to the SonicOS technical document set.

Topics:

- Default Settings
- System Setup
- Basic Configuration
- Registration and Licensing

Default Settings

The following table lists the default values, or identifies where you can find them, for certain key settings.

Port or Setting	IP Address / Login / Password
Serial number	On the nameplate or in the initial firmware
Authentication code	Available in the user interface on the Dashboard with the system information.
Registration code	From MySonicWall
Maintenance key	From MySonicWall

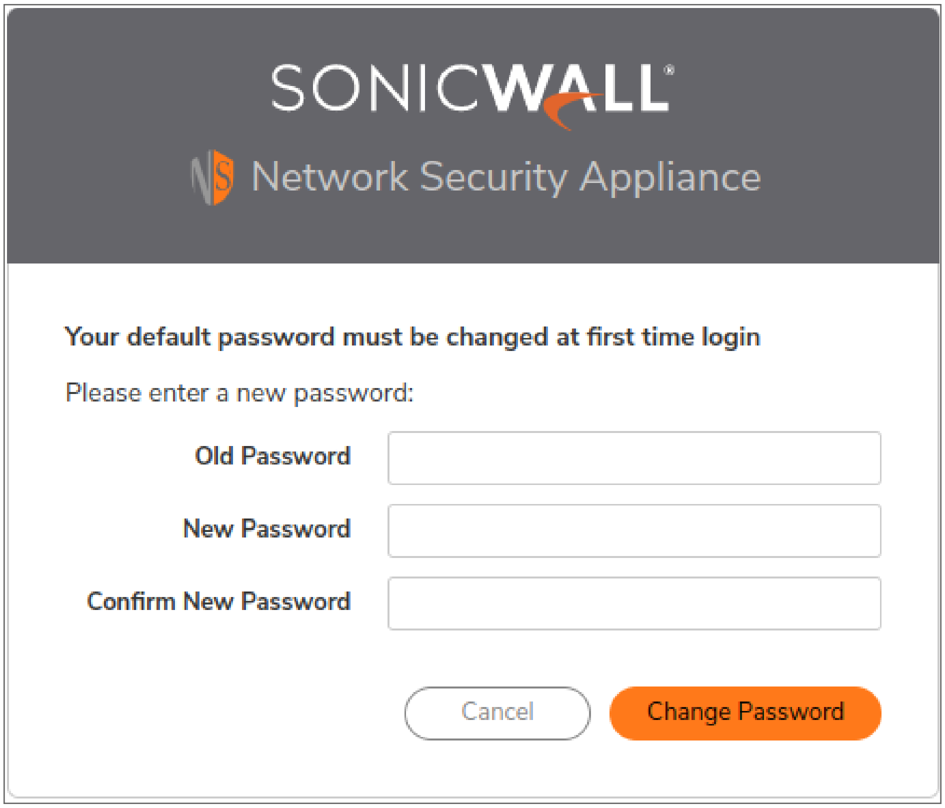
Port or Setting	IP Address / Login / Password
Console	• Serial port baud rate = 11520 • Data: 8 • Parity = none • Stop = 1 • Flow control = none • Login = *admin* / *password* by default
X0	`192.168.168.168`
X1	Not set by default
Management	`192.168.1.254`
SafeMode	SafeMode is accessed through the MGMT port which is by default `https://192.168.1.254`. If SonicOS is unavailable, the default login credential is *admin* / *password*, otherwise, the administrator's credentials should work. ⓘ | **NOTE:** Ensure to use the new password if you have updated the default password. For detailed information about accessing SafeMode, refer to the SonicOS 7 Upgrade Guide.
MySonicWall	Register on https://mysonicwall.com to set up an account

System Startup

Once the firewall is connected to a power source, SonicOS comes up within a few minutes. You can configure the firewall from either the X0 or MGMT interface. The X0 interface can be configured as a static, transparent, or Layer-2, Bridged-Mode interface. The MGMT port is a dedicated 1 Gigabit Ethernet interface for appliance management and SafeMode access.

To configure HTTPS management via X0:

1. Connect your management computer to the **X0** interface. DHCP addressing is available by default on **X0**.
2. In your browser, enter the default IP address `https://192.168.168.168` and log in using the default credentials:
   Username: *admin*
   Password: *password*
3. Your default password must be changed at first time while logging in after upgrade. Create a password that meets the security requirements. A password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, S0nicW@ll.



Your default password must be changed at first time login

Please enter a new password:

Old Password

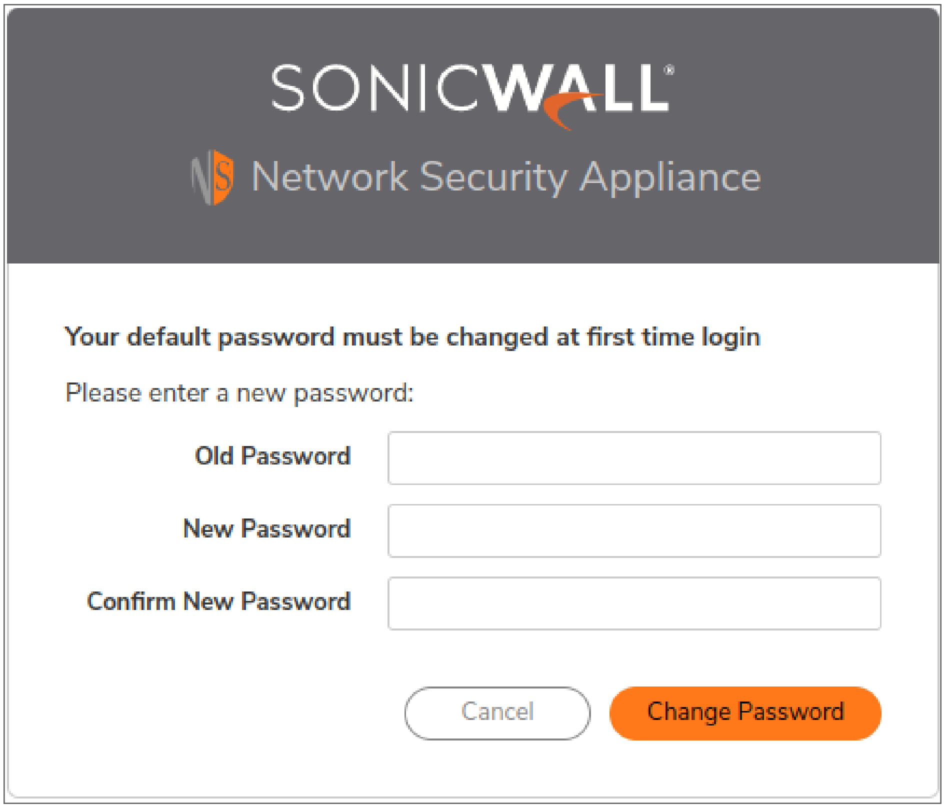
New Password

Confirm New Password

4. Perform the following steps to change password:
   a. In **Old Password** text box, enter your default password.
   b. In **New Password** text box, enter your new password.
   c. In **Confirm Password** text box, re-enter your new password.
5. Click **Change Password**.
6. Refer to Basic Configuration for the remaining steps for a basic configuration.

To configure HTTPS management through the MGMT port:

1. Connect your management computer to the **MGMT** interface.
2. Configure your computer with a static IP address on the `192.168.1.0/24` subnet, such as `192.168.1.20`.
3. In your browser, enter the default IP address `https://192.168.1.254` and log in using the default credentials:
   Username: *admin*
   Password: *password*
4. After Enter your default user name and password. Your default password must be changed at first time while logging in after upgrade. Create a password that meets the security requirements. A password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, S0nicW@ll.



Your default password must be changed at first time login

Please enter a new password:

Old Password

New Password

Confirm New Password

5. Perform the following steps to change password:
   a. In **Old Password** text box, enter your default password.
   b. In **New Password** text box, enter your new password.
   c. In **Confirm Password** text box, re-enter your new password.
6. Click **Change Password**.
7. Refer to Basic Configuration for the remaining steps for a basic configuration.

If the services are enabled while using the MGMT port, you can also access SafeMode, SSH or ping via the MGMT port. From SafeMode, you can upgrade firmware, boot backup images and more.

You can also configure your firewall using the SonicOS command line interface (CLI). For more information on using CLI, refer to Setting Up with CLI.

Basic Configuration

Use the following steps to complete a basic system configuration.

1. Navigate to **POLICY | Rules and Policies** to create security rules for handling traffic. There are node fault rules, so no traffic can be passed until rules are created.

ⓘ | **IMPORTANT:** Without policy rules, SonicOS only allows management traffic on X0 or the MGMT port. No other traffic is allowed until policy rules are created by the administrator.

2. Navigate to **NETWORK | System > Interfaces** to configure the X1 WAN interface.

   - **Static** – Configures the appliance for a network that uses static IP addresses.
   - **DHCP** – Configures the appliance to request IP settings from a DHCP server in the network.

   WAN connectivity is needed for product registration and licensing. Be sure to configure DNS for the WAN interface.

3. Configure the administrator username and password.

   ⓘ | **NOTE:** Ensure to use the new password if you have updated the default password.

4. Connect the X0 interface to your LAN network and connect X1 to the Internet, as described in the *Quick Start Guide* that came with your firewall. You can also find the *Quick Start Guide* on the Technical Documentation portal. Search for your firewall model.

5. Register SonicOS as described in Registration and Licensing .

Registration and Licensing

To register your firewall, you can click **Register** in the web management interface, and then enter your MySonicWall credentials. If you don't have a MySonicWall account, refer to Creating a MySonicWall Account for instructions.

You can also log in to MySonicWall from a browser at https://mysonicwall.com and register your firewall there. When registration is complete, synchronize your licenses from within SonicOS.

Registration in MySonicWall requires your serial number and authentication code, which you can find on the appliance label or on the Device screen of the **HOME | Dashboard > System** page.

You can purchase additional Security Service licenses by clicking **Licenses** in the row for your firewall on the **My Products** page in MySonicWall.

After product registration, be sure to download the latest firmware and upgrade your firewall.

Creating a MySonicWall Account

You need to have a valid MySonicWall account to use SonicOS. A MySonicWall account is critical to receiving the full benefits from SonicWall security services, firmware updates, and technical support. MySonicWall is used to license your site and to activate or purchase licenses for other security services specific to your security solution.

To create a new MySonicWall account:

1. Navigate to https://mysonicwall.com.
2. In the login screen, click **Sign Up**.
3. Enter the email address you want associated with your MySonicWall account.

4. Create a password that meets the security requirements.
5. From the drop-down menu select how you want to use two-factor authentication.
6. Finish CAPTCHA and click on **Continue** to go the Company page.
7. Fill your company information and click **Continue**.
8. On the **YOUR INFO** page, complete the details and select your preferences.
9. Click **Continue** to go to the **EXTRAS** page.
10. Select whether you want to add additional contacts to be notified for contract renewals.
11. To set up additional contacts:
    a. Input the **First name**.
    b. Input the **Last name**.
    c. Add the **Email address** for that person
    d. Click **Add Contact**.
12. Select whether you want to add tax information.
13. If providing tax information:
    a. In the **Reseller for** field, select the state from the drop-down menu.
    b. Add your **Federal Tax ID**.
    c. Add the **Expiry (expiration) Date**.
    d. Enter the **Certificate ID**.
    e. Click on **ADD TAX ENTRY**.
14. Select whether you want to add your distributor information.
15. To set up the distributor information:
    a. Input the **Distributor Name**.
    b. Input the **Customer Number**.
    c. Click **Add Distributor**.
16. Click **Finish**.
17. Check your email for a verification code and enter it in the **Verification Code*** field. If you did not receive a code, contact Customer Support by clicking on the support link.

6

Setup Options

Aside from the basic setup process, you can choose to use other features or applications in your environments to enable your firewall setup. These include:

- Zero Touch
- Setting Up with NSM
- Setting Up with SonicExpress
- Setting Up with CLI

Zero Touch

Your SonicWall appliance is automatically enabled for the Zero-Touch feature. Zero-Touch makes it easy to register your unit and add it to Capture Security Center for management and reporting in three simple steps.

1. Be sure your firewall is registered on MySonicWall.
2. Enable Zero Touch.
3. Connect the firewall to power and turn it on.

For the details about using Zero Touch, refer to the *Zero-Touch Deployment Guide* on the Technical Documentation portal.

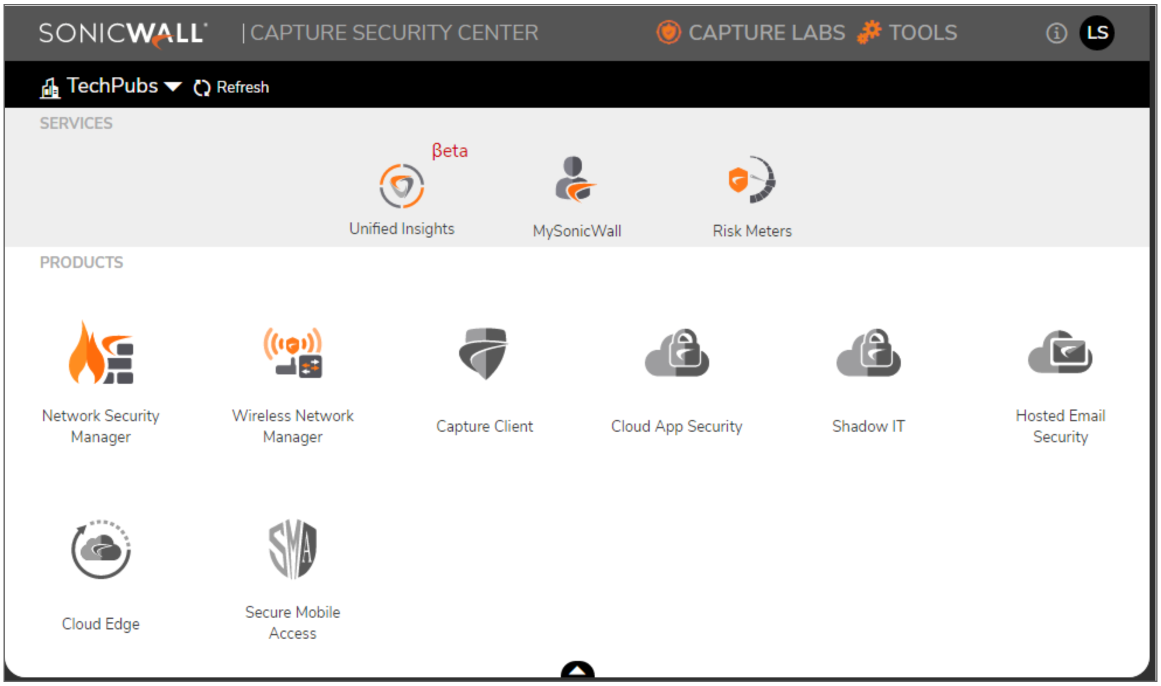
Setting Up with NSM

Network Security Manager (NSM) is centralized firewall manager. It allows central, error-free manage ofall firewall operations by adhering to auditable workflows. You can also use it to easily add and configure new firewalls, especially when combined with the Zero Touch feature. For details about Network Security Manager, refer to the NSM document set.

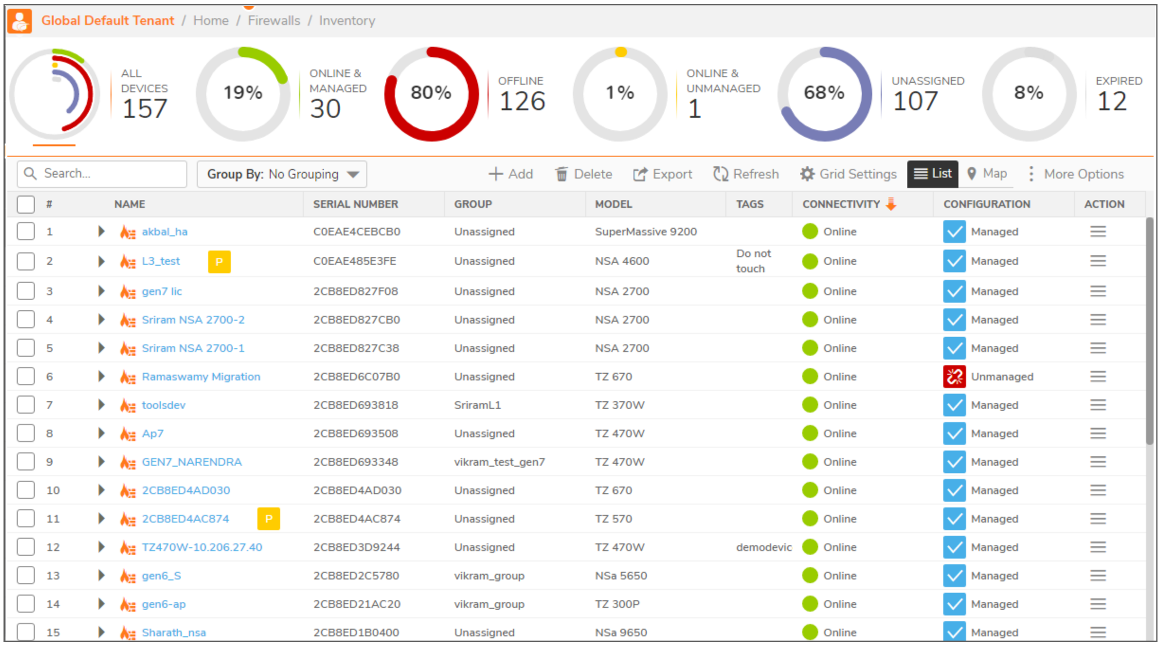
ⓘ | **NOTE:** This option requires either the Essential or Advanced NSM license.

To manage and configure your firewall:

1. Log into the Capture Security Center at cloud.sonicwall.com using your MySonicWall credentials.
2. Select the MySonicWall tile to register your firewall.
3. Enable **Zero Touch** and **NSM Essential/NSM Advanced** license on your firewall in MySonicWall.
4. Select the appropriate Data Center (for first time users only).
5. Modify the **Managed By** option from **On Box** to **Cloud**, and then enable **Zero Touch**.
6. Return to the CSC portal, and select the **Network Security Manager** tile to manage your firewall from the cloud.



7. In NSM, navigate to **HOME | Firewalls > Inventory** to configure and manage your firewalls.



□	#		NAME		SERIAL NUMBER	GROUP	MODEL	TAGS	CONNECTIVITY	CONFIGURATION	ACTION
□	1	▶	akbal_ha		C0EAE4CEBCB0	Unassigned	SuperMassive 9200		● Online	✓ Managed	≡
□	2	▶	L3_test	P	C0EAE485E3FE	Unassigned	NSA 4600	Do not touch	● Online	✓ Managed	≡
□	3	▶	gen7 lic		2CB8ED827F08	Unassigned	NSA 2700		● Online	✓ Managed	≡
□	4	▶	Sriram NSA 2700-2		2CB8ED827CB0	Unassigned	NSA 2700		● Online	✓ Managed	≡
□	5	▶	Sriram NSA 2700-1		2CB8ED827C38	Unassigned	NSA 2700		● Online	✓ Managed	≡
□	6	▶	Ramaswamy Migration		2CB8ED6C07B0	Unassigned	TZ 670		● Online	☒ Unmanaged	≡
□	7	▶	toolsdev		2CB8ED693818	SriramL1	TZ 370W		● Online	✓ Managed	≡
□	8	▶	Ap7		2CB8ED693508	Unassigned	TZ 470W		● Online	✓ Managed	≡
□	9	▶	GEN7_NARENDRA		2CB8ED693348	vikram_test_gen7	TZ 470W		● Online	✓ Managed	≡
□	10	▶	2CB8ED4AD030		2CB8ED4AD030	Unassigned	TZ 670		● Online	✓ Managed	≡
□	11	▶	2CB8ED4AC874	P	2CB8ED4AC874	Unassigned	TZ 570		● Online	✓ Managed	≡
□	12	▶	TZ470W-10.206.27.40		2CB8ED3D9244	Unassigned	TZ 470W	demodevic	● Online	✓ Managed	≡
□	13	▶	gen6_S		2CB8ED2C5780	vikram_group	NSa 5650		● Online	✓ Managed	≡
□	14	▶	gen6-ap		2CB8ED21AC20	vikram_group	TZ 300P		● Online	✓ Managed	≡
□	15	▶	Sharath_nsa		2CB8ED1B0400	Unassigned	NSa 9650		● Online	✓ Managed	≡

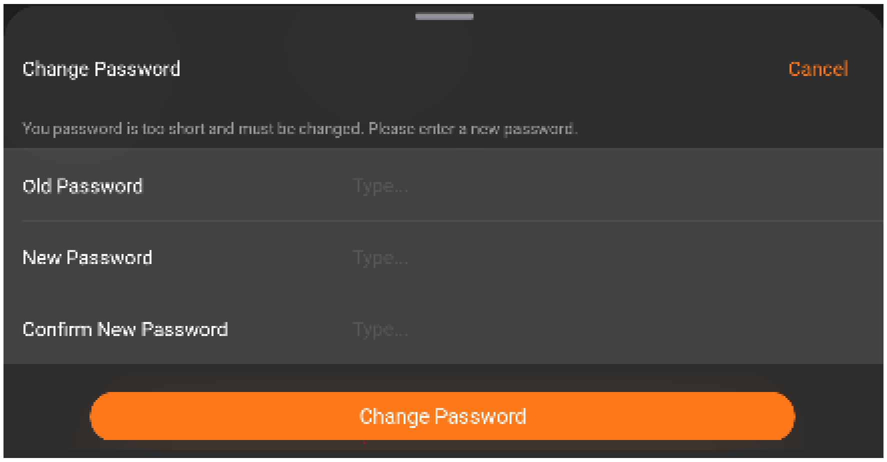
Setting Up with SonicExpress

SonicExpress is a mobile application that can be used from your phone simply on-board firewalls. It's designed for Apple and Android platforms. The application is available from the Apple App Store or the Google Play Store.

ⓘ **NOTE:** After the initial setup, be sure to download the latest firmware from MySonicWall to upgrade your firewall.

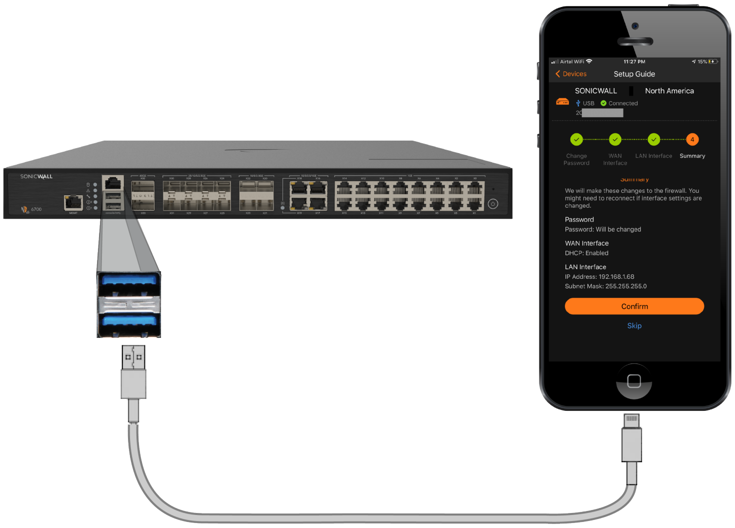
To setup firewalls using the SonicExpress App:

1. Download and launch the SonicExpress app on your iOS or Android device.
2. Tap **Login** and log in with your MySonicWall credentials.
3. Your default password must be changed at first time while logging in after upgrade. Create a password that meets the security requirements. A password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, S0nicW@ll.



You password is too short and must be changed. Please enter a new password.

4. Perform the following steps to change password:
   a. In **Old Password** field, enter your default password.
   b. In **New Password** field, enter your new password.
   c. In **Confirm Password** field, re-enter your new password.
5. Click **Change Password**
6. Select the Tenant for the firewall. Tenants can contain multiple SonicWall appliances.
7. Connect your iOS/Android device to the firewall with the smart phone USB cable. This cable is not supplied with the firewall.



We will make these changes to the firewall. You might need to reconnect if interface settings are changed.

Password

Password: Will be changed

WAN Interface

DHCP: Enabled

LAN Interface

IP Address: 192.168.1.68

Subnet Mask: 255.255.255.0

ⓘ | **NOTE:** Use the USB cable from your mobile device.

8. Use the **Setup Guide** within the application to register the firewall, synchronize service licenses, change the password, and configure essential interface settings.

   ⓘ | **NOTE:** Ensure to use the new password if you have updated the default password.

Setting Up with CLI

You can use the command line interface to set up your firewalls, and access is provided in two different ways. You can:

- Use a serial connection via the MGMT port (speed = 115200)

  You do not need to assign an IP address to the firewall to use the CLI on a serial connection to the Console port.

- Use an SSH management session via ethernet

  You can use an SSH client to access the CLI by connecting to the appliance with an Ethernet cable. This option is useful for customers who do not have access to an RJ45 to DB-9 serial cable for the Console port on the firewall. To use SSH management, you must assign an IP address to X0 (LAN) or X1 (WAN), or use the default LAN IP address of `192.168.168.168`.

ⓘ | **NOTE:** To use the CLI on a serial connection or in an SSH management session, you need to use a terminal emulation application (such as Tera Term) or an SSH Client application (such as PuTTY). You can find a suitable, free, terminal emulator to download from the Internet.

For details on how to use the command line interface for setting up for your firewall, refer to the *SonicOS 7 Command Line Interface Reference Guide* at the Technical Documentation portal.

7

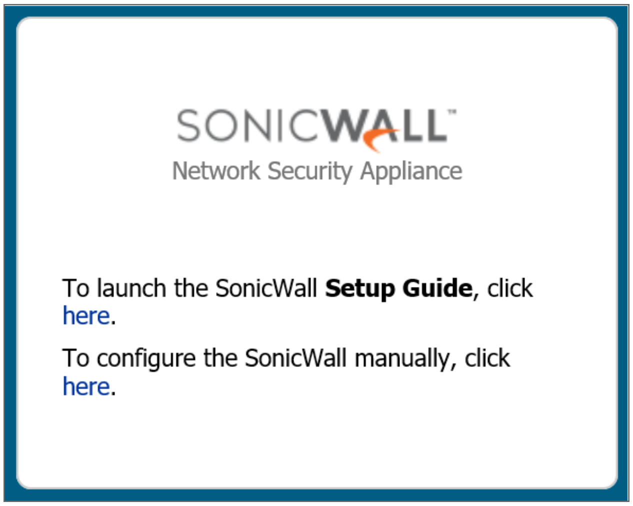
Running the Setup Wizard

After you have setup the firewall and can access the user interface, you can use the Setup Wizard to finalize the key settings.

1. Navigate to https://192.168.168.168 in your browser.

   ⓘ | **TIP:** You computer should be using DHCP IP addressing.

2. Click the link to launch the SonicWall Setup Guide.

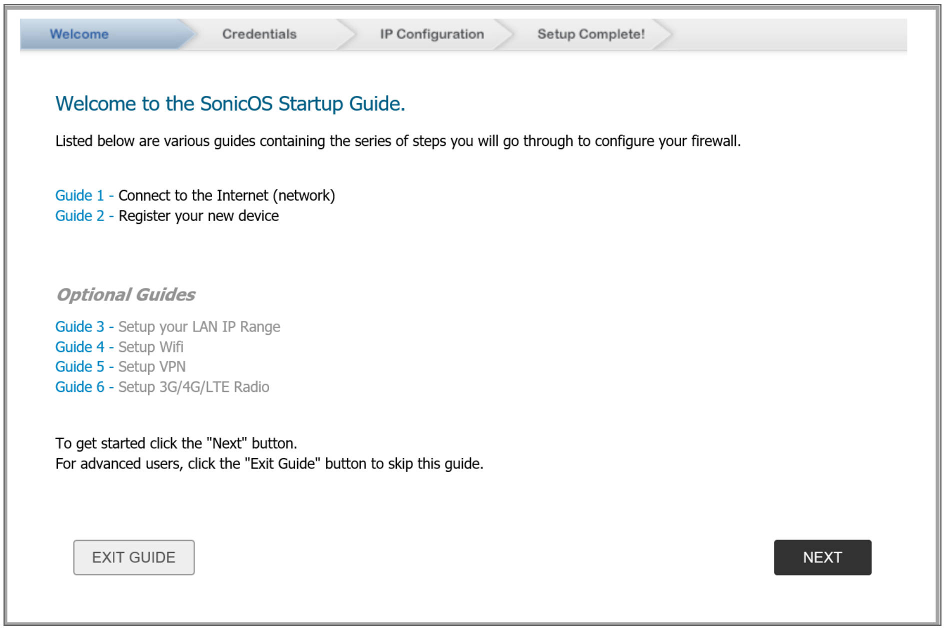


SONICWALL
Network Security Appliance

To launch the SonicWall **Setup Guide**, click here.

To configure the SonicWall manually, click here.

3. When the **SonicOS Setup Guide** opens, click **NEXT** and follow the prompts in the **Setup Guide**.



Welcome to the SonicOS Startup Guide.

Listed below are various guides containing the series of steps you will go through to configure your firewall.

Guide 1 - Connect to the Internet (network)
Guide 2 - Register your new device

Optional Guides

Guide 3 - Setup your LAN IP Range
Guide 4 - Setup Wifi
Guide 5 - Setup VPN
Guide 6 - Setup 3G/4G/LTE Radio

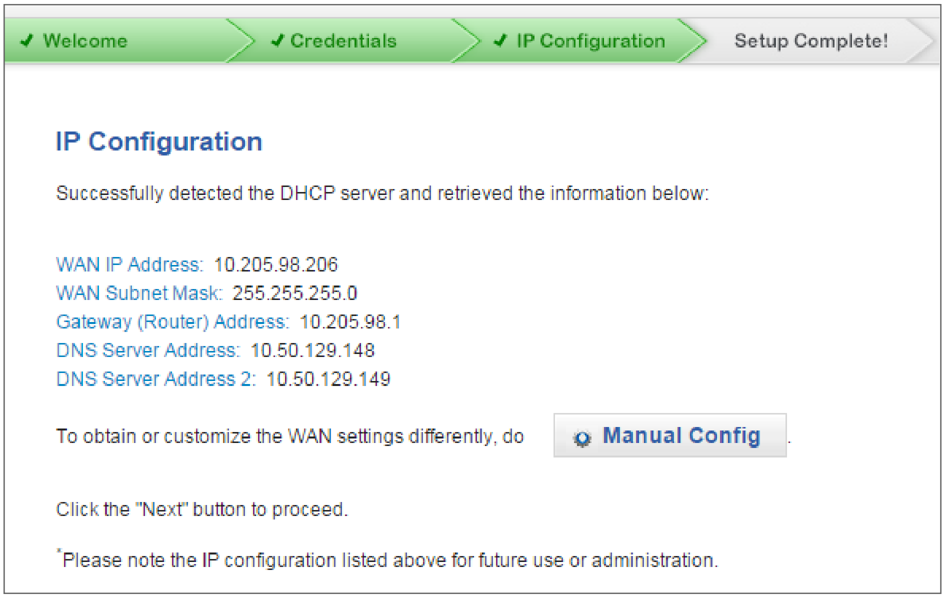
To get started click the "Next" button.
For advanced users, click the "Exit Guide" button to skip this guide.

4. On the **Credentials** screen, enter a new administrator password and click **NEXT**.

   The default administrator credentials are **Username**: *admin* **Password**: *password*.

   ⓘ | **NOTE:** Ensure to use the new password if you have updated the default password.

5. Validate the DHCP IP servers displayed on the **IP Configuration** screen and click **NEXT**.



IP Configuration

Successfully detected the DHCP server and retrieved the information below:

WAN IP Address: 10.205.98.206
WAN Subnet Mask: 255.255.255.0
Gateway (Router) Address: 10.205.98.1
DNS Server Address: 10.50.129.148
DNS Server Address 2: 10.50.129.149

To obtain or customize the WAN settings differently, do Manual Config .

Click the "Next" button to proceed.

*Please note the IP configuration listed above for future use or administration.

6. On the **Setup Complete** screen, review the settings and click **DONE.** The SonicOS login screen displays.

8

Testing and Troubleshooting Connectivity

If you have issues connecting to your firewall after setting it up, you can use the following tips to help diagnose the issue.

Testing Your Internet Connection

To test your Internet connection:

1. Reset your computer to use DHCP IP addressing and connect it to your LAN subnet or to the appliance X0 interface.
2. Point your browser to the X0 IP address configured during initial setup (default: `192.168.168.168`).
3. Log into SonicOS using the configured credentials (default: admin/password).
   ⓘ | **NOTE:** Ensure to use the new password if you have updated the default password.
4. In a command prompt window, type: `ping sonicwall.com`. You should receive a reply.
5. Open another browser tab or window and point it to https://www.sonicwall.com or another valid web site. If the site displays, you have correctly configured your appliance.

Troubleshooting your Internet Connection

To troubleshoot your Internet connection, try each of these suggestions:

- Verify that the Local Area Connection settings on your management computer are set to use either DHCP or a static IP on the LAN subnet. Restart it or renew the DHCP address.
- Verify that the WAN interface being used for Internet connectivity is not configured in Wire Mode or Tap Mode.
- Restart your Internet router or modem to communicate with the DHCP client in SonicOS on the appliance.
- Check all cable connections and IP addresses.

Troubleshooting Your MGMT Connection

If your MGMT connection doesn't seem to be working correctly, review the following suggestions:

- Did you correctly enter the firewall management IP address beginning with “http://” or “https://” in your web browser?
- Did you try restarting your management station while it is connected to the appliance?
- Are the Local Area Connection settings on your computer set to a static IP address on the `192.168.1.0/24` subnet?
- Is the Ethernet cable connected to your computer and to the MGMT port on your appliance, and are the connector clips properly seated in the ports?

Troubleshooting Your LAN Connection

If your LAN connection doesn't seem to be working correctly, review the following suggestions:

- Did you correctly enter the IP address for the SonicWall X0 interface into your web browser, beginning with “http://” or “https://”?
- Did you try restarting your management station while it is connected to the appliance?
- Are the Local Area Connection settings on your computer set to one of the following:
  - Obtain an IP address automatically using DHCP
  - A static IP address on the default LAN subnet (`192.168.168.0/24`)
  - A static IP address on the configured LAN subnet, if you changed it during initial setup
- Is the Ethernet cable connected to your computer and to the X0 (LAN) port on your appliance, and are the connector clips properly seated in the ports?

Using SafeMode

SafeMode is a limited web management interface that provides a way to upload firmware from your computer and reboot the appliance. The SafeMode feature allows you to recover quickly from uncertain configuration states with a simplified management interface that includes the same settings available on the **System > Settings** screen.

There is an E-CLI command `safemode` that restarts the firewall in SafeMode.

For more information about SafeMode, refer to SonicOS 7 Upgrade Guide.

9

Migration Tool

In the past, when directly importing a preference file from a different platform to a newly acquired firewall, certain configurations experienced some issues. SonicWall created the SonicWall Migration Tool to help users convert settings so they can be easily imported into a target Gen7 firewall.

Topics:

- About Migration
- Using the Migration Tool

About Migration

The SonicWall Migration Tool was developed to help users easily migrate from an old firewall to the SonicWall Gen 7 firewalls. It helps ease conversion issues related to:

- Transitioning to a target firewall with fewer interfaces
- SFP (small form pluggable) module configurations
- Internal wireless interfaces
- WWAN configuration on USB ports
- Gen 6 Global BWM (bandwidth management)
- Internal switch limitations (for example, portshield not being allowed on certain ports in the new firewall)

The Migration Tool allows you to convert the settings from existing SonicWall Gen 6 and Gen 6.5 firewall. You can also use it to convert other brands to SonicWall firewalls. The Migration Tools supports these platforms:

Platform	Versions
Cisco PIX/ASA	PIX 4.x, PIX 5.x, PIX 6.x, PIX 7.x, PIX 8.x
Check Point	Smart Center, Provider-1 (excluding VPN-1 Edge, Safe@Office, SMP) with OS NG FP1 (4.0)
Juniper	NetScreen Series, SRX Series, SSG Series
Palo Alto	PA-200, PA-500, PA-2000, PA-3000, PA-4000, PA-5000 Series

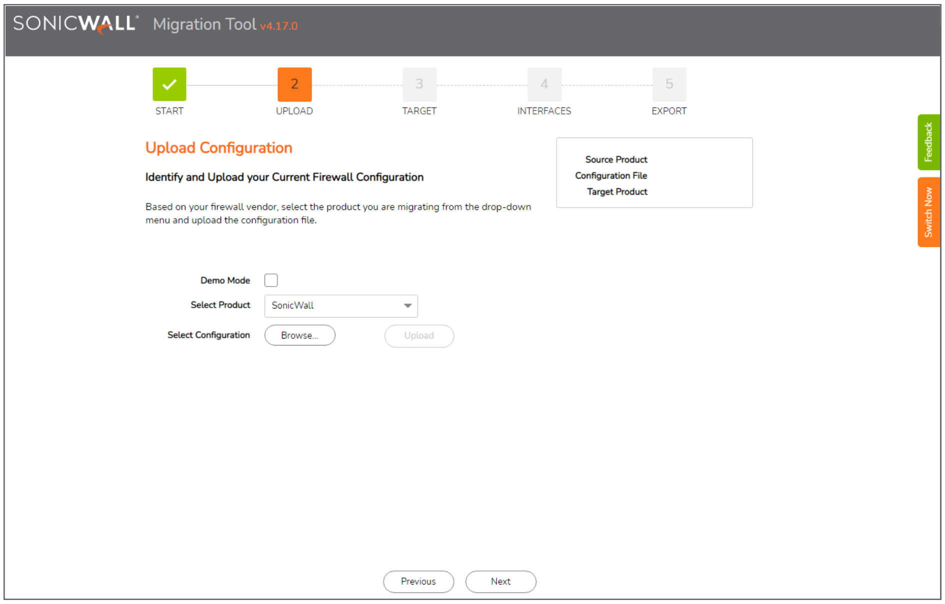
Platform	Versions
Fortinet	FortiGate Firewall Platform
Watchguard	FireBox, XTM Series
Sophos	SG, XG Series
SonicWall	TZ, NSa, SuperMassive, NSsp, NSv

ⓘ | **NOTE:** The Migration Tool currently does not support conversion of the Gen 5 configuration files.

Using the Migration Tool

To migrate firewall configuration file:

1. Navigate to migratetool.global.sonicwall.com.
2. Validate that your old firewall is part of the supported set listed and click **Next** to start the wizard.



Upload Configuration

Identify and Upload your Current Firewall Configuration

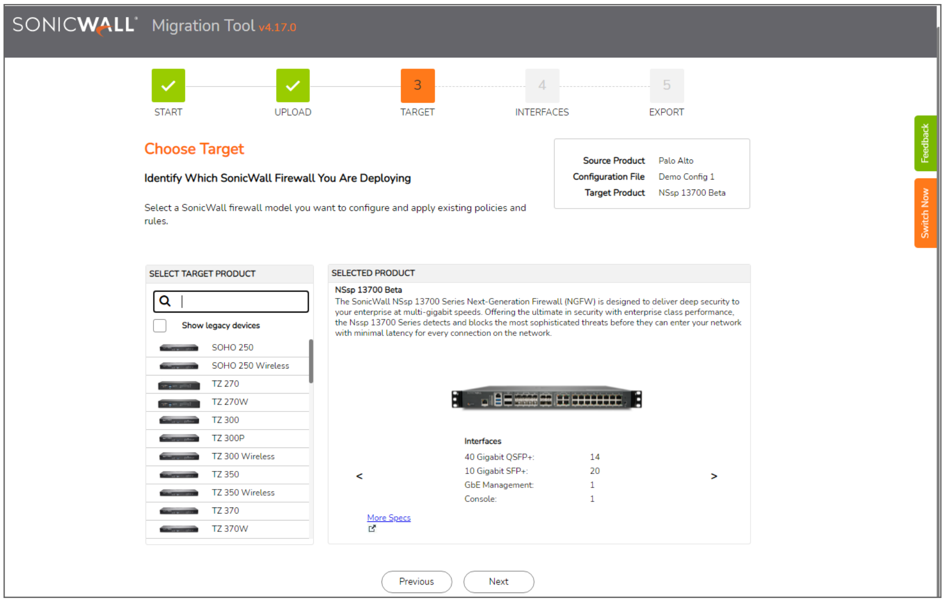
Based on your firewall vendor, select the product you are migrating from the drop-down menu and upload the configuration file.

Demo Mode □

Select Product: SonicWall

Select Configuration

3. In the **Select Product** drop-down list, select the vendor name of the firewall you are migrating from.
4. Click on **Browse** to select the configuration from for your old firewall.
5. Click **Next**.



Choose Target

Identify Which SonicWall Firewall You Are Deploying

Select a SonicWall firewall model you want to configure and apply existing policies and rules.

Source Product	Palo Alto
Configuration File	Demo Config 1
Target Product	NSsp 13700 Beta

SELECT TARGET PRODUCT

□ Show legacy devices

- SOHO 250
- SOHO 250 Wireless
- TZ 270
- TZ 270W
- TZ 300
- TZ 300P
- TZ 300 Wireless
- TZ 350
- TZ 350 Wireless
- TZ 370
- TZ 370W

SELECTED PRODUCT

NSsp 13700 Beta

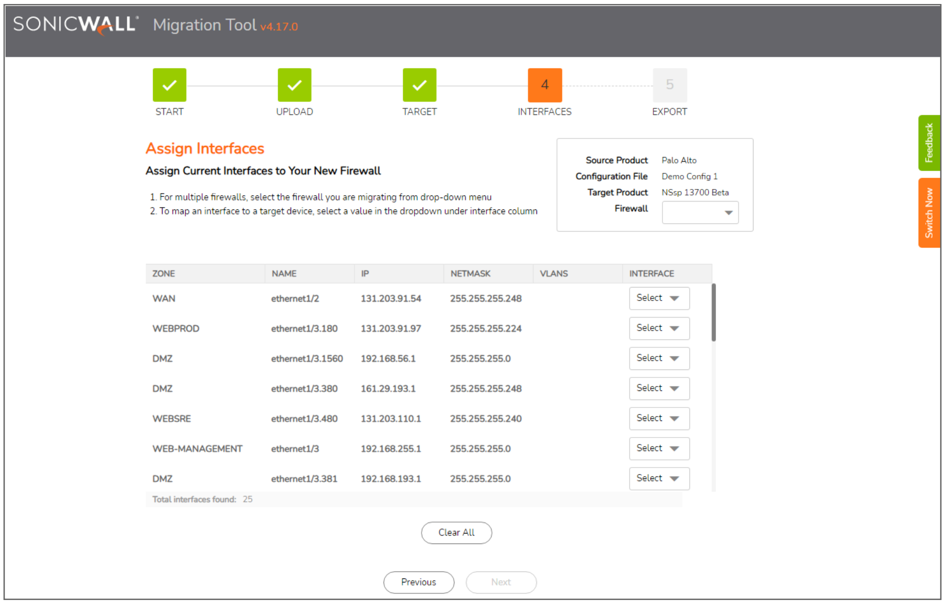
The SonicWall NSsp 13700 Series Next-Generation Firewall (NGFW) is designed to deliver deep security to your enterprise at multi-gigabit speeds. Offering the ultimate in security with enterprise class performance, the Nssp 13700 Series detects and blocks the most sophisticated threats before they can enter your network with minimal latency for every connection on the network.

Interfaces	
40 Gigabit QSFP+:	14
10 Gigabit SFP+:	20
GbE Management:	1
Console:	1

6. Select the firewall model you want to configure from the **SELECT TARGET PRODUCT** list.

   The selected product displays in **SELECTED PRODUCT** pane. You can read more about that product by using the forward and back arrows to navigate the specifications. Click on the link for **More Specs** to see the product page for that firewall.

7. Click **Next**.



Assign Interfaces

Assign Current Interfaces to Your New Firewall

1. For multiple firewalls, select the firewall you are migrating from drop-down menu
2. To map an interface to a target device, select a value in the dropdown under interface column

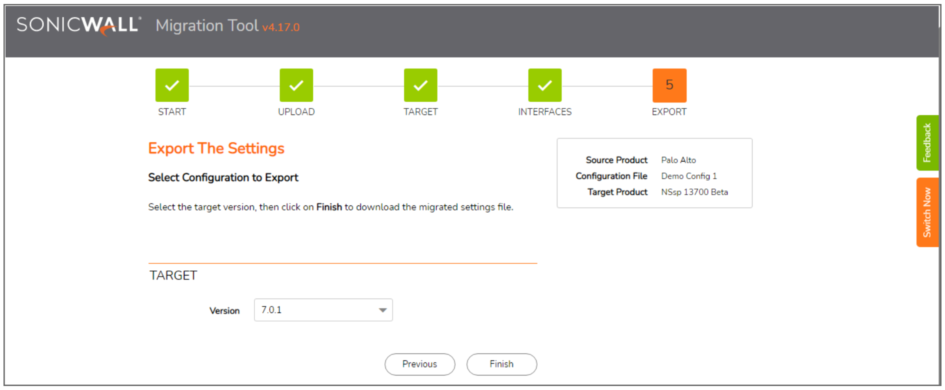
Source Product	Palo Alto
Configuration File	Demo Config 1
Target Product	NSsp 13700 Beta
Firewall	

ZONE	NAME	IP	NETMASK	VLANS	INTERFACE
WAN	ethernet1/2	131.203.91.54	255.255.255.248		Select
WEBPROD	ethernet1/3.180	131.203.91.97	255.255.255.224		Select
DMZ	ethernet1/3.1560	192.168.56.1	255.255.255.0		Select
DMZ	ethernet1/3.380	161.29.193.1	255.255.255.248		Select
WEBSRE	ethernet1/3.480	131.203.110.1	255.255.255.240		Select
WEB-MANAGEMENT	ethernet1/3	192.168.255.1	255.255.255.0		Select
DMZ	ethernet1/3.381	192.168.193.1	255.255.255.0		Select

Total interfaces found: 25

8. Assign the current interfaces to your new firewall on the interface map.

9. Click **Next**.



Export The Settings

Select Configuration to Export

Select the target version, then click on **Finish** to download the migrated settings file.

Source Product	Palo Alto
Configuration File	Demo Config 1
Target Product	NSsp 13700 Beta

TARGET

Version: 7.0.1

10. Select the target version from the drop-down list.
11. Click Finish. The old file is converted based on the parameters you gave. When done the new file is downloaded so you save it to your local system.

    > **TIP:** You should reset the firewall to factory defaults before importing the configuration file (not required if the device is fresh out of the box).

12. If not already done, register the firewall and upgrade the firmware.
13. Upload the newly created file settings.
14. Check the DNS settings (configure them manually, if needed).
15. Reboot the firewall.

10

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

SonicOS Getting Started Guide for the NSsp 10700, 11700, 13700, and NSa Series Series
Updated - June 2023
Software Version - 7
232-005738-00 Rev C

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035