SonicOS 7

NSv Getting Started Guide

for KVM

SONICWALL®

Contents

1

Introducing the NSv Series

This Getting Started Guide describes how to install SonicWall NSv and QMU environments and provides basic configuration information.

The SonicWall® NSv is SonicWall's virtualized next-generation firewall appliance that provides Deep Packet Inspection (DPI) security and segmentation in virtual environments. With some platform specific differences, SonicOS 7 running on the NSv offers the same feature functionality and security features of a physical appliance, with comparable performance. SonicOS Virtual is a fully featured 64-bit SonicOS 7 powered by SonicCore.

SonicWall® NSv series firewalls support both ***Classic*** mode and ***Policy*** mode. Selection of or changing between ***Classic*** and ***Policy*** modes is supported on NSv series from SonicOS 7.0.1 pnwards. For more information on supported or unsupported feature list refer to the Feature Support Information section and changing between ***Classic*** and ***Policy*** modes is supported on NSv series refer to the *About SonicOS 7 for the TZ, NSa, NSv, and NSsp Series Features Specific to NSv* guide in https://www.sonicwall.com/support/technical-documentation.

Topics:

- Feature Support Information
- Node Counts Per Platform
- Installation File / Supported Platforms
- Hardware Compatibility
- KVM/QEMU
- Hardware-Assisted Full Virtualization
- Paravirtualization
- Product Matrix and Requirements
- Backup and Recovery Information
- Importing Firewall Configurations
- High Availability Configurations
- Upgrading to a Higher Capacity NSv Model
- Creating a MySonicWall Account

Feature Support Information

The Feature Support List table shows key SonicOS features and whether or not they are supported or unsupported in deployments of the NSv. The SonicWall NSv has nearly all the features and functionality of a SonicWall NSa hardware virtual machine running SonicOS 7 firmware.

For more information about supported features, refer to the SonicOS 7 NSv administration guide. This and other documents for the SonicWall NSv are available by selecting **NSv** as the **Product** at: https://www.sonicwall.com/support/technical-documentation.

The Feature Support List of NSv table shows the key SonicOS 7 features.

FEATURE SUPPORT LIST

Functional Category	Feature Area	Feature
Unified Security Policy	**Unified Policy combining Layer 4 to Layer 3 Rules**	Source/Destination IP/Port/Service
		Application based Control
		CFS/Web Filtering
		Botnet
		Geo-IP/country
		Single Pass Security
		Services enforcement
		Decryption Policy
		DoS Policy
		EndPoint Security Policy
		Rule Diagram
	Profile Based Objects	
		Endpoint Security
		Bandwidth Management
		QoS Marking
		Content Filter
		Intrusion Prevention
		DHCP Option
		AWS VPN
	Action Profiles	
		Security Profile
		DoS Profile
	Signature Objects	

Functional Category	Feature Area	Feature
		AntiVirus Signature Object
		AntiSpyware Signature Object
	Rule Management	
		Cloning
		Shadow rule analysis
		In-cell editing
		Group editing
		Export of Rules
		LiveCounters
	Managing Views	
		Used/unused rules
		Active/inactive rules
		Sections
		Customizable Grid/Layout
		Custom Grouping
TLS 1.3	**Supporting TLS 1.3 with enhanced security**	
SDWAN	**SDWAN Scalability**	
	SDWAN Usability Wizard	
API	**API Driven Management**	
	Full API Support	
Dashboard	**Enhanced Home Page**	
		Actionable Dashboard
		Enhanced Device View
		Top Traffic and User summary
		Insights to threats
		Policy/Object Overview
		Profiles and Signatures Overview
		Zero-Day Attack Origin Analysis
	Notification Center	
Debugging	**Enhanced Packet Monitoring**	

Functional Category	Feature Area	Feature
	UI based System Logs Download	
	SSH Terminal on UI	
	System Diagnostic Utility Tools	
	Policy Lookup	
Capture Threat Assessment (CTA 2.0)	Executive Template	
	Customizable Logo/Name/Company	
	Industry and Global Average Statistics	
	Risky File Analysis	
	Risky Application Summary	
	Malware Analysis	
	Glimpse of Threats	
Monitoring	Risky Application Summary	
	Enhanced AppFlow Monitoring	
Management	CSC Simple Reporting	
	ZeroTouch Registration and Provisioning	
General	SonicCoreX and SonicOS Containerization	
	Data Encryption using AES-256	
	Enhanced Online Help	

Node Counts Per Platform

The supported node count varies by NSv platform. This is the maximum number of nodes/users that can connect to the NSv at any one time, and is displayed on the **System Status** page. The Maximum Node Counts Per Platform table shows this information.

MAXIMUM NODE COUNTS PER PLATFORM

Platform	Maximum Node Count
NSv70	unlimited
NSv 270	unlimited
NSv 470	unlimited
NSv 870	unlimited

Installation File / Supported Platforms

Release Version	Supported Linux / Kernel / KVM / VMM Versions
SonicOS 7 for Linux KVM/QEMU	Ubuntu 18.04 • Kernel: 4.4.0-31-generic • KVM version: 2.5.0 • Virtual machine manager: 1.5.1
	CentOS-7 • Kernel: 3.10.0-693.e17.x86_64 • KVM version: 1.5.3 • Virtual machine manager: 1.5.1

ⓘ | **IMPORTANT:** Determine which environment you are working with before ordering the NSv image.

After you have received a purchase confirmation email, go to Obtaining the NSv Image for download instructions.

Hardware Compatibility

SonicWall NSv is supported on x86-64 platforms supporting KVM/QEMU with sufficient resources. The following section, Product Matrix and Requirements, outlines core, interface, memory, and storage requirements for different NSv models.

KVM/QEMU

KVM, or Kernel-based virtual machine is a software module that allows Linux to operate as a hypervisor. QEMU, or Quick Emulator, allows guest operating systems to run on the KVM hypervisor and supports virtualization where applications executing in the user space can achieve near-native speeds through full virtualization or paravirtualization.

Hardware-Assisted Full Virtualization

KVM features hardware-assisted full virtualization when the underlying x86 processor hardware supports Intel VT-x or AMD-V virtualization extensions. This allows a guest operating system (SonicOS) to setup a virtual context and execute instructions directly on the processor's hardware.

For an overview of virtualization techniques, see: https://www.unixarena.com/2017/12/para-virtualization-full-virtualization-hardware-assisted-virtualization.html/

Paravirtualization

In hardware-assisted full virtualization, guest operating systems issue calls directly to the hardware. In paravirtualization, guest operating systems communicate with the hypervisor (KVM/QEMU) with an API (Virtio). This API defines paravirtual devices including Ethernet cards, disk I/O subsytems, and VGA interfaces with SPICE drivers.

For an overview of VirtIO, see: https://www.cs.cmu.edu/~412/lectures/Virtio_2015-10-14.pdf

Product Matrix and Requirements

The following table shows the hardware resource requirements for the SonicWall NSv virtual machines.

Product Models	NSv 70	NSv 270	NSv 470	NSv 870
Maximum Cores[1]	2	2	4	8
Minimum Total Cores	2	2	4	8
Minimum Management Cores	1	1	1	1
Data Plane Cores (fixed)	1	1	3	7
Network Interfaces	8	8	8	8
Supported IP/Nodes	Unlimited	Unlimited	Unlimited	Unlimited
Minimum Memory Required [2]	4G	6G	8G	10G
Minimum Hard Disk/Storage	50G	50G	50G	50G

On NSv deployments with Jumbo Frame support enabled, the Minimum Memory requirements are higher. This increases TCP performance. See the Memory Requirements on NSv with Jumbo Frames Enabled vs Disabled table that follows.

MEMORY REQUIREMENTS ON NSV WITH JUMBO FRAMES ENABLED VS DISABLED

NSv Model	Minimum Memory – Jumbo Frames Enabled	Minimum Memory – Jumbo Frames Disabled
NSv 70	6G	4G
NSv 270	6G	4G
NSv 470	10G	8G
NSv 870	14G	10G

[1] If the actual number of cores allocated exceeds the number of cores defined in the previous table, extra cores are used as CPs.

[2] Memory requirements are higher with Jumbo Frames enabled. See the Memory Requirements on NSv with Jumbo Frames Enabled vs Disabled table.

Backup and Recovery Information

In certain situations, it might be necessary to contact SonicWall for help as directed in SonicWall Support, or visit SonicWall, use SafeMode, or deregister the NSv virtual machine:

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Contact SonicWall Technical Support for assistance.
- If the disk is not recoverable, then the NSv virtual machine needs to be deregistered with MySonicWall. Contact technical support for more information.
- If SonicOS does not boot up, you can go into SafeMode and download the log files, upload a new SonicOS image, or take other actions. For more information about SafeMode, see Using SafeMode on the NSv.
- If SonicOS fails three times during the boot process, it boots into SafeMode. Verify that the minimum required memory is available and allocated based on the NSv model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall Technical Support for assistance.

Moving configuration settings from SonicWall physical appliances to the NSv is not supported. However, configuration settings can be moved from one NSv to another. Contact SonicWall Technical Support for assistance.

Importing Firewall Configurations

Configuration settings import is not supported from SonicWall physical appliances to the NSv.

High Availability Configurations

The KVM/QEMU on Linux implementations allows configuration of virtual machines in high availability pairs.

NSv virtual machines deployed on NSv can be configured as high availability Active/Standby pairs to eliminate a single point of failure and provide higher reliability. Two identical NSv instances are configured so that when the primary fails, the secondary takes over to maintain communications between the Internet and the protected network. These redundant NSv instances could share the same license when registered on MySonicWall as associated products. For details, refer to the technical publications portal.

Additional licensing allows configuration of an Active/Standby pair to handle a Stateful fail-over in which the Standby NSv takes over without having to initialize network connections and VPNs. However, dynamic ARP entries and common virtual MACs are not currently supported. For more details, refer to the technical publications portal.

Upgrading from SonicOS 6.5

SonicOS 7 NSv supports only fresh deployments. You can register NSv as SonicOS (Classic mode) or SonicOSX (Policy mode). If running SonicOS, you can import settings from a 6.5.4.4 NSv. If the NSv is registered as SonicOSX, you cannot import settings and must manually navigate policies, application rules, and content filtering rules for SonicOS 7 NSv installations. Note that there are console, API, and SonicOS web approaches to completing these configurations.

ⓘ **NOTE:** Upgrading to SonicOS 7 from SonicOS 6.5.4 requires a Secure Upgrade Path key that must be purchased separately. You can choose from any of the following:

- SONICWALL NSV 70 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 270 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 470 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 870 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 70 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 270 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 470 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 870 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)

To upgrade an existing SonicOS 6.5.4.v NSv deployment to SonicOS 7.0.1 or higher:

1. Purchase a Secure Upgrade license key.
2. Log into MySonicWall and register the Secure Upgrade serial number. Enter a descriptive "friendly" name in the available field, shown here as "SecureUpgrade1."
3. Click **Choose management options**.
4. In the **Secure Upgrade** popup window, select **Register Only** at the top.
5. Select the Trade-In Unit from the list of registered NSv instances. This is the SonicOS 6.5.4.v NSv instance to be upgraded to SonicOS 7.
6. Click **Done** after selecting the Trade-In Unit. The Secure Upgrade serial number is then registered to your MySonicWall account.
7. The action item Secure Upgrade Transfer is added to the To do list at the bottom of the page.

   You can perform the service transfer ***after*** you have deployed the SonicOS 7 NSv instance and moved the configuration settings ("prefs") from the SonicOS 6.5.4.v NSv to the new SonicOS 7 NSv.

   The service transfer moves all active services from the SonicOS 6.5.4.v NSv to the new SonicOS 7 NSv and then deregisters the SonicOS 6.5.4.v NSv.

   ⓘ **NOTE:** If you do not perform the service transfer within 60 days, the transfer is performed automatically.
8. Deploy a new SonicOS 7 NSv instance with the desired model and platform.

9. Register the SonicOS 7 NSv using the **Secure Upgrade** serial number. When prompted to select either Classic mode or Policy mode, select Classic mode. Classic mode supports configuration settings imported from a SonicOS 6.5.4.v NSv.

   Registration initiates a 60-day countdown at the end of which the SonicOS 6.5.4.v NSv is deregistered, completing the Secure Upgrade Transfer.

10. Log into the SonicOS 6.5.4.v NSv and export the configuration settings to a file on your management computer.

11. Using the migration tool (https://migratetool.global.sonicwall.com/), migrate the SonicOS 6 NSv preferences to SonicOS 7 NSv model.

12. Log into SonicOS 7 NSv and import the configuration settings file.

    The upgrade is now complete and the SonicOS 7 NSv is ready for use.

Upgrading to a Higher Capacity NSv Model

It is possible to move up to a higher capacity NSv model, but not down to a lower capacity model. Refer to the knowledgebase article: https://www.sonicwall.com/support/knowledge-base/how-do-i-upgrade-from-one-nsv-model-to-another/190503165228828/

For additional details, go to https://www.sonicwall.com/support/technical-documentation/ and search for **SonicOS 7 updates and upgrades**.

For details on the number of process and memory to allocate to the virtual machine to upgrade, refer to Product Matrix and Requirements.

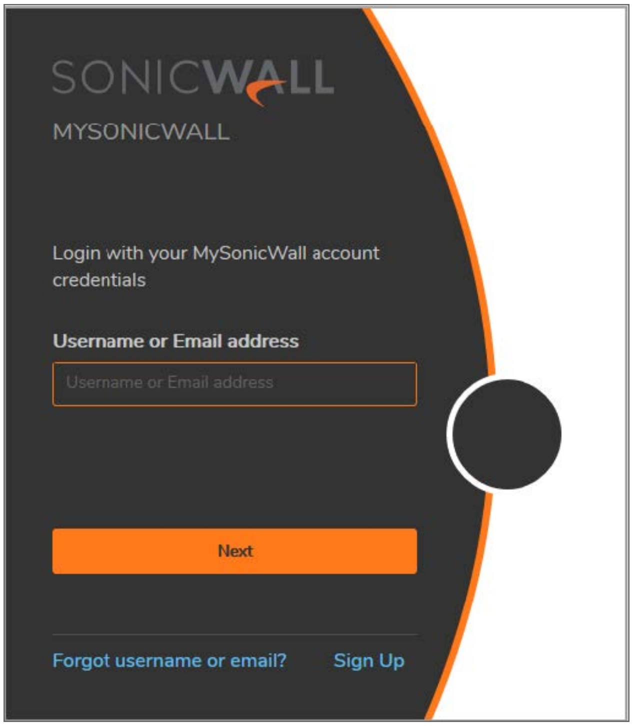
Creating a MySonicWall Account

A MySonicWall account is required to obtain the OVA file for initial installation of the NSv virtual machine, for product registration to enable full functionality of SonicOS features, and for access to licensed security services. For a High Availability configuration, MySonicWall provides a way to associate a secondary NSv that can share security service licenses with your primary virtual machine.

MySonicWall registration information is not sold or shared with any other company.

To create a MySonicWall account:

1. In your web browser, navigate to https://www.mysonicwall.com.
2. In the login screen, click the **Sign Up** link.



Login with your MySonicWall account credentials

Username or Email address
Username or Email address
Next
Forgot username or email?
Sign Up

3. Complete the account information, including email and password.
4. Enable two-factor authentication if desired.
5. If you enabled two-factor authentication, select one of the following authentication methods:
    - **Email (one-time passcode)** where an email with a one-time passcode is sent each time you log into your MySonicWall account.
    - **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code. After the code is scanned, you need only click a button.
6. Click **Continue** to go to the **COMPANY** page.
7. Complete the company information and click **Continue**.
8. On the **YOUR INFO** page, select whether you want to receive security renewal emails.
9. Identify whether you are interested in beta testing of new products.
10. Click **Continue** to go to the **EXTRAS** page.
11. Select whether you want to add additional contacts to be notified for contract renewals.
12. If you opted for additional contacts, input the information and click **Add Contact**.
13. Click **Finish**.
14. 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 link.

15. Click **Done**. You are returned to the login window so you can login into MySonicWall with your new account.

2

Installing SonicOS on the NSv Series

Topics:

- Preparing the Linux Server System
- Obtaining the NSv Image
- Installing the NSv Series on Ubuntu-KVM/QEMU
- Installing the NSv Series on CentOS-KVM/QEMU

Preparing the Linux Server System

Before installing a SonicWall NSv Series virtual machine on a Linux server, prepare the server:

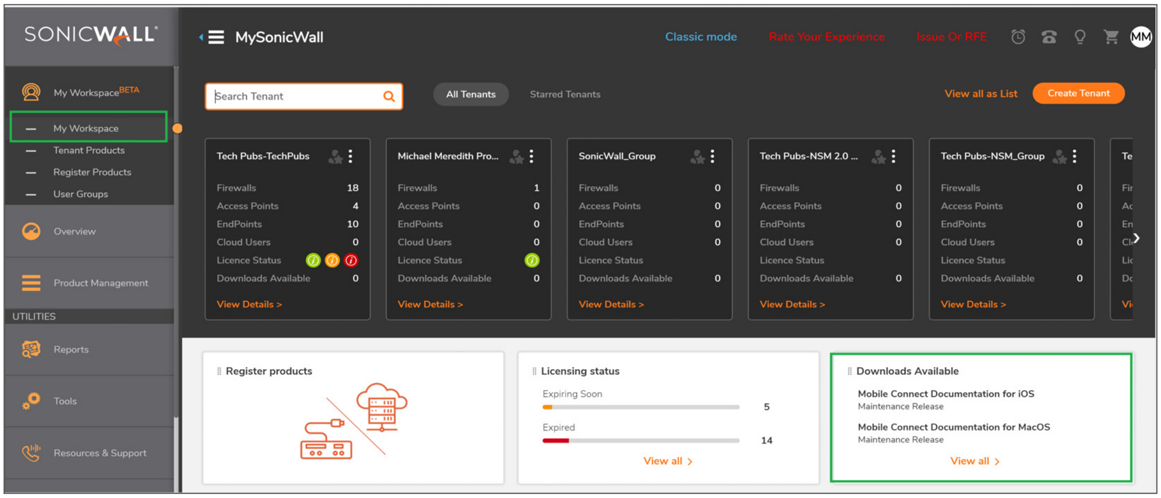
- Install Ubuntu or CentOS on the server. For version details refer to Installation File / Supported Platforms.
- Install KVM and QEMU on server.
- Connect the Linux Server system to an external switch.

Obtaining the NSv Image

After purchasing NSv, you will receive an email with a serial number and Authentication Code. Log into mysonicwall.com (refer to Creating a MySonicWall Account) and go to the Download Center:

To download image:

1. Login to MySonicWall.com and then navigate to **My WorkSpace > Downloads Available**.



	Tech Pubs-TechPubs	Michael Meredith Pro...	SonicWall_Group	Tech Pubs-NSM 2.0 ...	Tech Pubs-NSM_Group
Firewalls	18	1	0	0	0
Access Points	4	0	0	0	0
EndPoints	10	0	0	0	0
Cloud Users	0	0	0	0	0
Licence Status	● ● ●	●			
Downloads Available	0	0	0	0	0

Licensing status

Expiring Soon	5
Expired	14

Downloads Available

Mobile Connect Documentation for iOS
Maintenance Release

Mobile Connect Documentation for MacOS
Maintenance Release

2. Click **List All** and the list of available downloads comes up.
3. Identify the NSv product and click on the title; when the details appear, click the download symbol to download:
4. Keep the serial number and Authentication code from the purchase confirmation email to complete product registration after the virtual machine in installed. Refer to Registering the NSv Appliance from SonicOS.

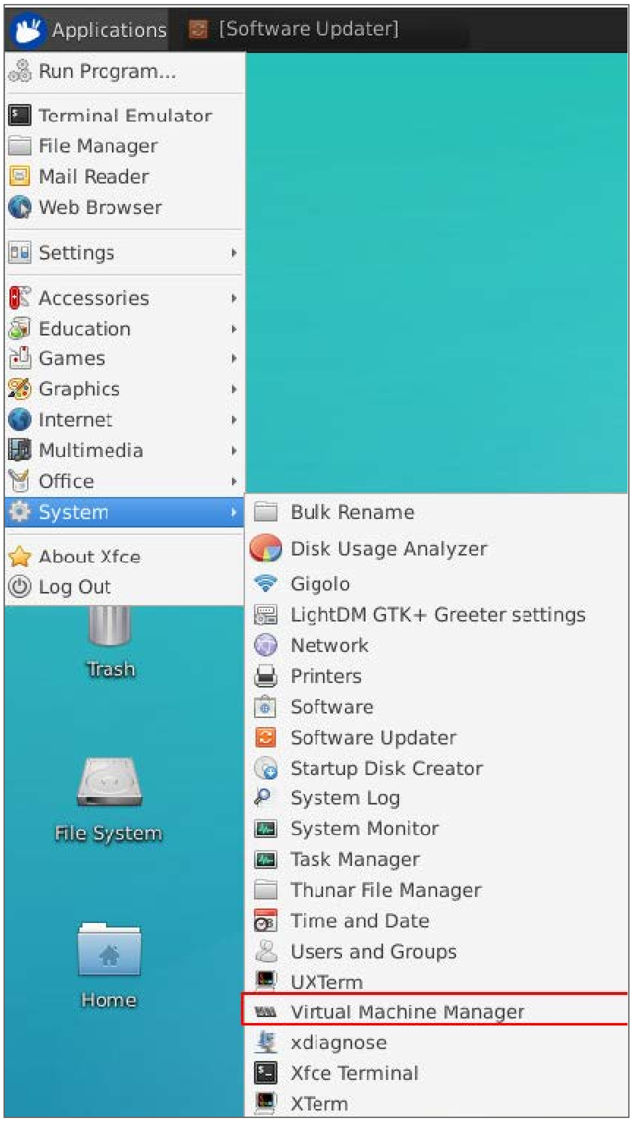
Installing the NSv Series on Ubuntu-KVM/QEMU

Topics:

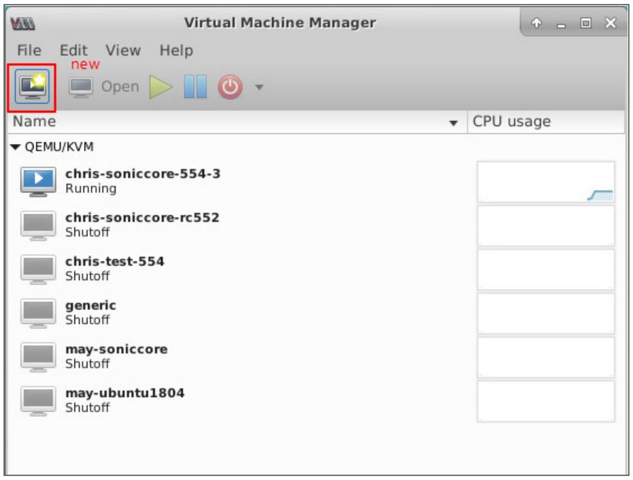
- Adding VLAN Parameters to the Network Card
- Locating the img File
- Using the CLI to Configure User Settings
- Next Steps and Related Topics

To install an NSv on Ubuntu-KVM/QEMU:

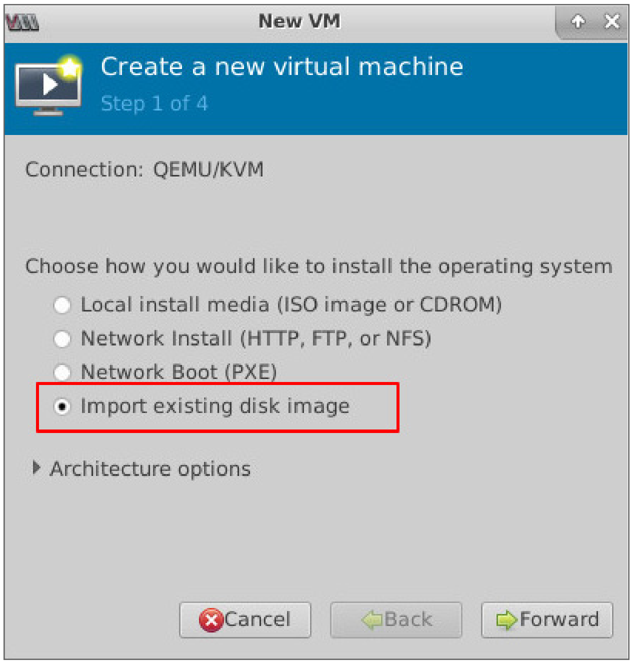
1. Download the NSv virtual machine ***img*** file to a local folder in the Linux Server system.
2. Copy image file (for example: “`SonicWall_NSv_For_QEMU_VM.img`”) into the directory `/var/lib/libvirt/images/`.
3. Bring up the Virtual Machine Manager (VMM):



4. Create a virtual machine in the Virtual Machine Manager to receive the image file:



5. Starting creating a new virtual machine by importing a disk image:



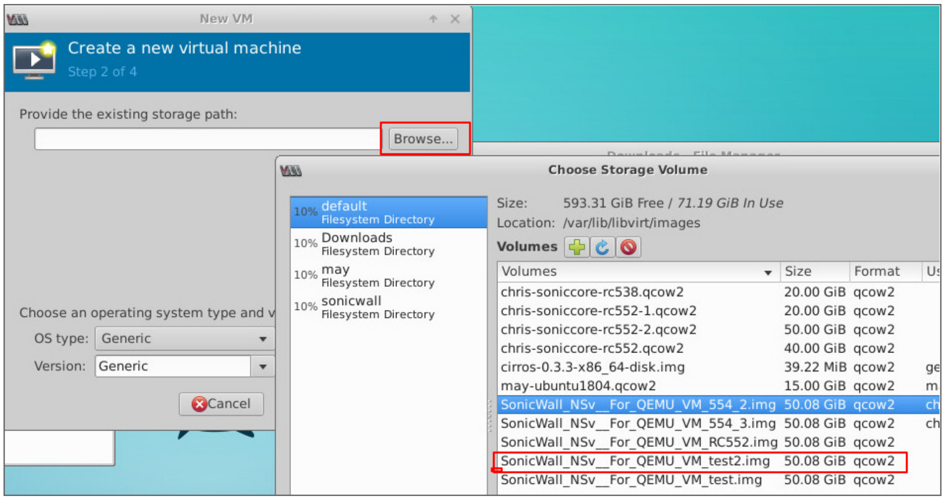
Connection: QEMU/KVM

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

Architecture options

6. Choose storage volume:



New VM

Create a new virtual machine

Step 2 of 4

Provide the existing storage path:

Browse...

Choose an operating system type and v

OS type: Generic

Version: Generic

Cancel

Choose Storage Volume

- 10% default — Filesystem Directory
- 10% Downloads — Filesystem Directory
- 10% may — Filesystem Directory
- 10% sonicwall — Filesystem Directory

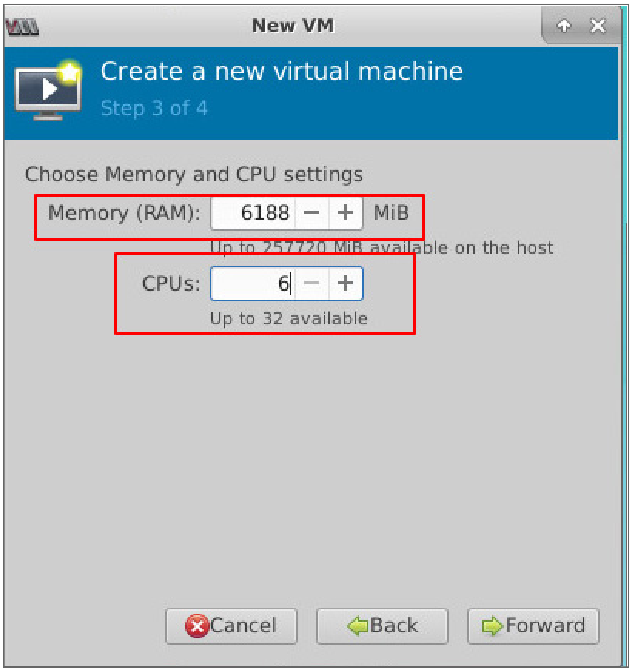
Size: 593.31 GiB Free / *71.19 GiB In Use*

Location: /var/lib/libvirt/images

Volumes

Volumes	Size	Format	Us
chris-soniccore-rc538.qcow2	20.00 GiB	qcow2	
chris-soniccore-rc552-1.qcow2	20.00 GiB	qcow2	
chris-soniccore-rc552-2.qcow2	50.00 GiB	qcow2	
chris-soniccore-rc552.qcow2	40.00 GiB	qcow2	
cirros-0.3.3-x86_64-disk.img	39.22 MiB	qcow2	ge
may-ubuntu1804.qcow2	15.00 GiB	qcow2	m
SonicWall_NSv__For_QEMU_VM_554_2.img	50.08 GiB	qcow2	ch
SonicWall_NSv__For_QEMU_VM_554_3.img	50.08 GiB	qcow2	ch
SonicWall_NSv__For_QEMU_VM_RC552.img	50.08 GiB	qcow2	
SonicWall_NSv__For_QEMU_VM_test2.img	50.08 GiB	qcow2	
SonicWall_NSv__For_QEMU_VM_test.img	50.08 GiB	qcow2	

7. Configure CPU/Memory/Name/Network (default only one network interface attached), then click Finish to create. For hardware resources, refer to Product Matrix and Requirements.



New VM

Create a new virtual machine

Step 3 of 4

Choose Memory and CPU settings

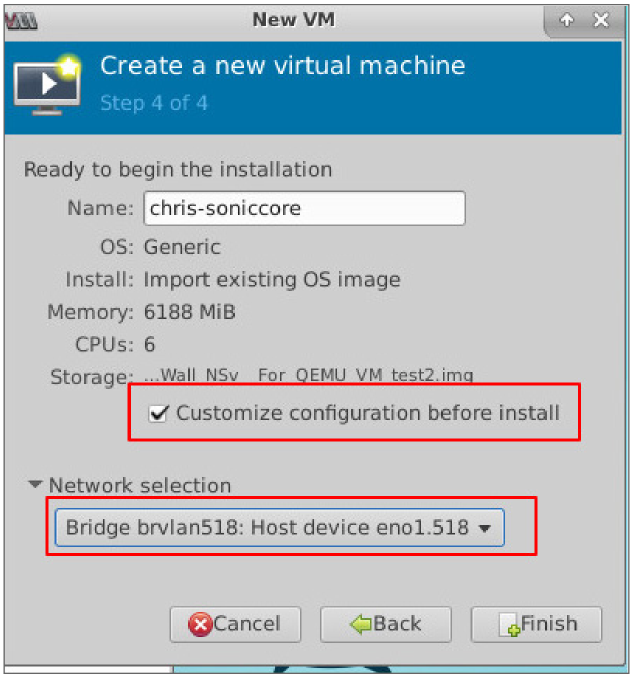
Memory (RAM): 6188 MiB

Up to 257720 MiB available on the host

CPUs: 6

Up to 32 available

8. The default interface corresponds to X0 of the virtual machine, here, for example, we choose a private VLAN 518 for network selection.



Ready to begin the installation

Name: chris-soniccore

OS: Generic

Install: Import existing OS image

Memory: 6188 MiB

CPUs: 6

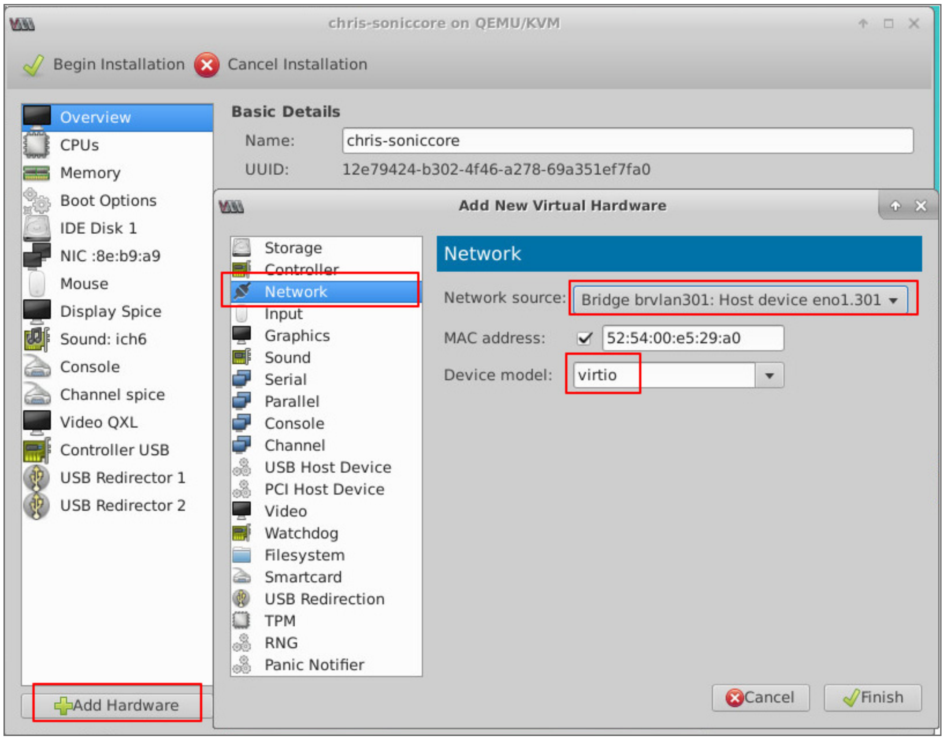
Storage: ...Wall NSv For QEMU VM test2.img

☑ Customize configuration before install

Network selection

Bridge brvlan518: Host device eno1.518

9. Another interface is required to serve as WAN port, or X1 of the virtual machine. Here we choose the interface 301:



Basic Details

Name: chris-soniccore

UUID: 12e79424-b302-4f46-a278-69a351ef7fa0

Network

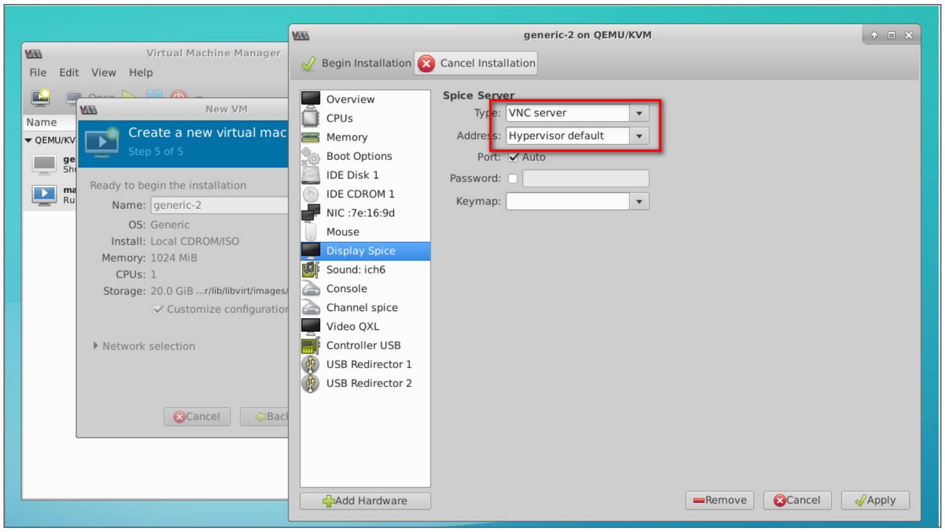
Network source: Bridge brvlan301: Host device eno1.301

MAC address: ☑ 52:54:00:e5:29:a0

Device model: virtio

> ⓘ **NOTE:** Both device models should choose **virtio**. By default, the first network card is X0, and the second one is X1. By choosing virtio, the VirtIO API is enabled. For more on VirtIO, see Paravirtualization.

10. Create a new virtual machine with the **Display** set as **VNC server**. Otherwise, you might not be able to use the keyboard with the new virtual machine.



Ready to begin the installation

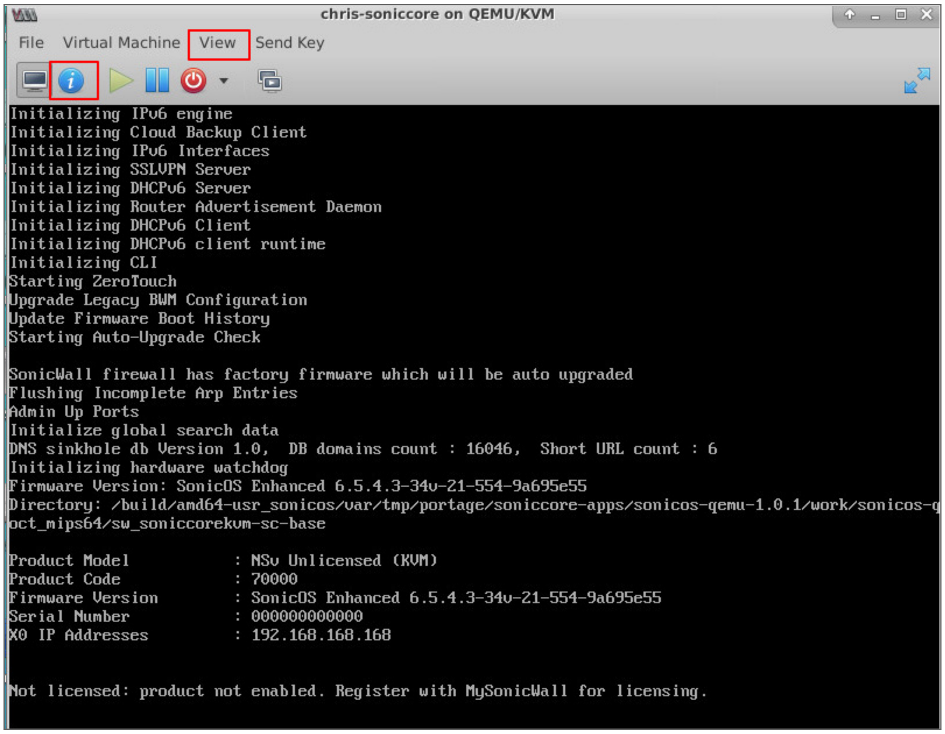
Name: generic-2
OS: Generic
Install: Local CDROM/ISO
Memory: 1024 MiB
CPUs: 1
Storage: 20.0 GiB ...r/lib/libvirt/images/
✓ Customize configuration

Network selection

Spice Server
Type: VNC server
Address: Hypervisor default
Port: ✓ Auto
Password: □
Keymap:

> ⓘ **NOTE:** In the previous dialog box, Spice refers to the Simple Protocol for Independent Computing Environment. In this context a Spice Display is one that can be accessed remotely through a standard protocol.

11. Open the newly created virtual machine and select **View** to see NSv boot messages:



```
Initializing IPv6 engine
Initializing Cloud Backup Client
Initializing IPv6 Interfaces
Initializing SSLVPN Server
Initializing DHCPv6 Server
Initializing Router Advertisement Daemon
Initializing DHCPv6 Client
Initializing DHCPv6 client runtime
Initializing CLI
Starting ZeroTouch
Upgrade Legacy BWM Configuration
Update Firmware Boot History
Starting Auto-Upgrade Check

SonicWall firewall has factory firmware which will be auto upgraded
Flushing Incomplete Arp Entries
Admin Up Ports
Initialize global search data
DNS sinkhole db Version 1.0,  DB domains count : 16046,  Short URL count : 6
Initializing hardware watchdog
Firmware Version: SonicOS Enhanced 6.5.4.3-34v-21-554-9a695e55
Directory: /build/amd64-usr_sonicos/var/tmp/portage/soniccore-apps/sonicos-qemu-1.0.1/work/sonicos-q
oct_mips64/sw_soniccorekvm-sc-base

Product Model          : NSv Unlicensed (KVM)
Product Code           : 70000
Firmware Version       : SonicOS Enhanced 6.5.4.3-34v-21-554-9a695e55
Serial Number          : 000000000000
X0 IP Addresses        : 192.168.168.168


Not licensed: product not enabled. Register with MySonicWall for licensing.
```

Adding VLAN Parameters to the Network Card

- Web Management Interface

  For best results, X0: 518 and X1: 201 are recommended.

  Access settings through **Virtual Machine Manager | Connection Details > Network Interface**

- Command Line Interface

```
apt-get install vlan bridge-utils

edit /etc/network/interfaces:

#edit physical interface

auto eno 1
```

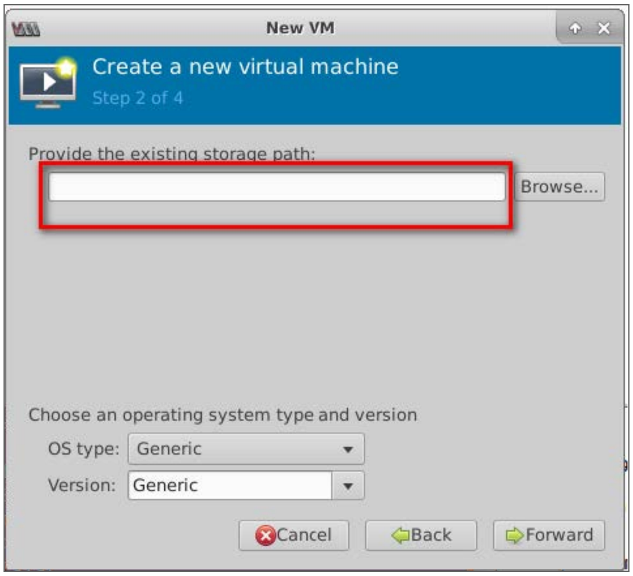
ⓘ | **NOTE:** Where eno 1 is the network server on the Ubuntu interface.

```
iface eno 1 inet manual



#add sub-interface, the number is vlan to be added
```

```
auto eno 1.301
iface eno 1.301. inet manual
vlan-raw-device eno 1

#add bridge
auto brvlan301
iface brvlan301 inet static
bridge_stp off
bridge_waitport 0
bridge_fd 0
bridge_ports eno 1_301
address 10.103.4.19
netmask 255.255.255.0
gatewar 10.103.64.1
dns_nameserver 10.196.2020.200

systemctl restart network
```

Locating the image file

If unable to locate using **Browse** as shown in the following image, input the full path (including the file name) manually:



Provide the existing storage path:

Choose an operating system type and version

OS type: Generic

Version: Generic

Using the CLI to Configure User Settings

Create user and input password:

```
sudo adduser <user>
```

Add user group so they can remote to desktop:

```
sudo adduser <user> tsusers
```

Add user to group so they can work with KVM:

```
sudo adduser <user> libvirtd
```

Add user to sudo so they can add vlans:

```
sudo adduser ,user> sudo
```

Create .xsession file for the user:

```
su -<user>

echo xfce4-session>.xsession
```

Next Steps and Related Topics

- Registering the NSv Appliance from SonicOS
- Managing SonicOS on the NSv Series

- Using System Diagnostics
- Using the Virtual Console and SafeMode

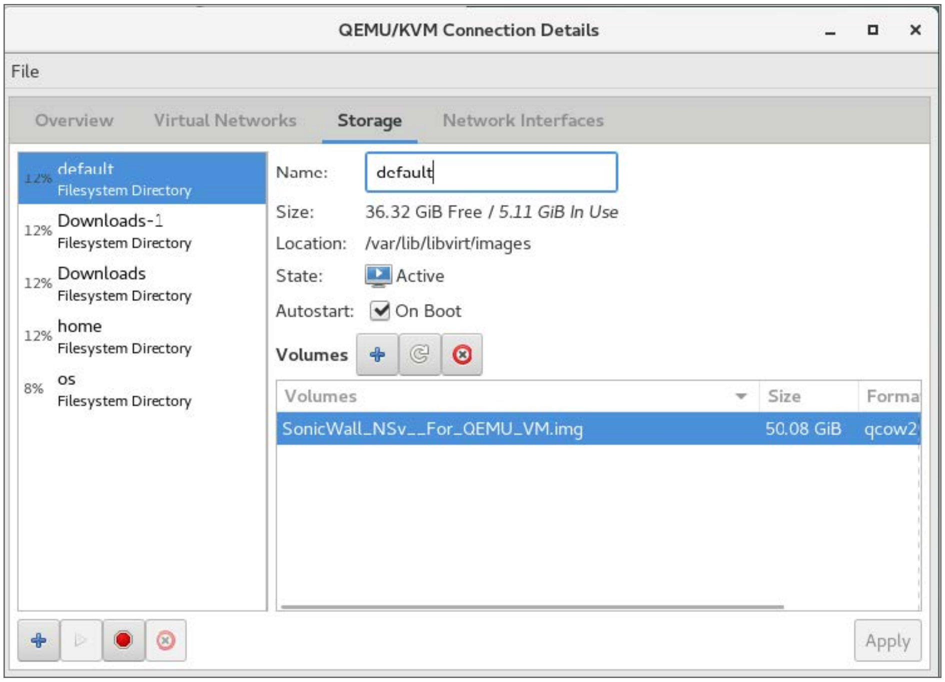
Installing the NSv Series on CentOS-KVM/QEMU

Topics:

- Creating NSv with Virt-install
- Editing a VM Config File
- Adding VLAN Parameters to the Network Card
- Next Steps and Related Topics

To install an NSv on CentOS-KVM/QEMU:

1. Download the NSv virtual machine ***img*** file to a local folder in the Linux Server system.
2. Copy image file (for example: “`SonicWall_NSv_For_QEMU_VM.img`”) into the directory `/var/lib/libvirt/images/`.



Usage	Pool
12%	default Filesystem Directory
12%	Downloads-1 Filesystem Directory
12%	Downloads Filesystem Directory
12%	home Filesystem Directory
8%	os Filesystem Directory

Name: default

Size: 36.32 GiB Free / *5.11 GiB In Use*

Location: /var/lib/libvirt/images

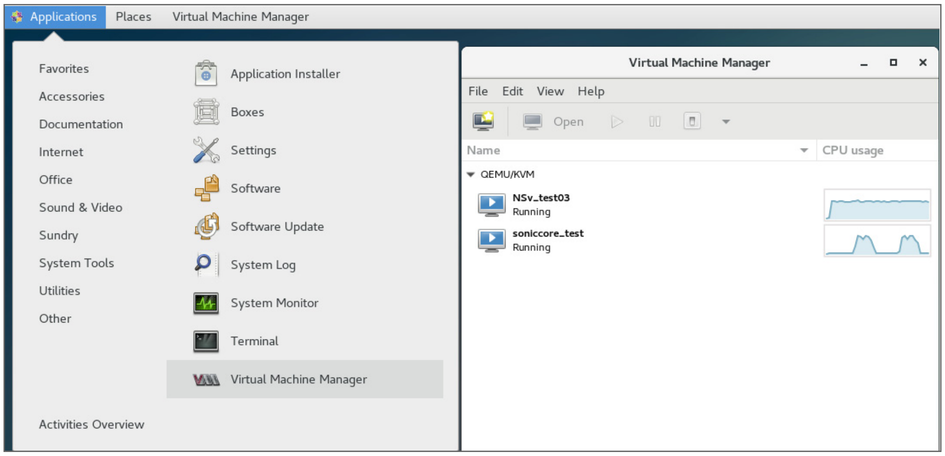
State: Active

Autostart: ☑ On Boot

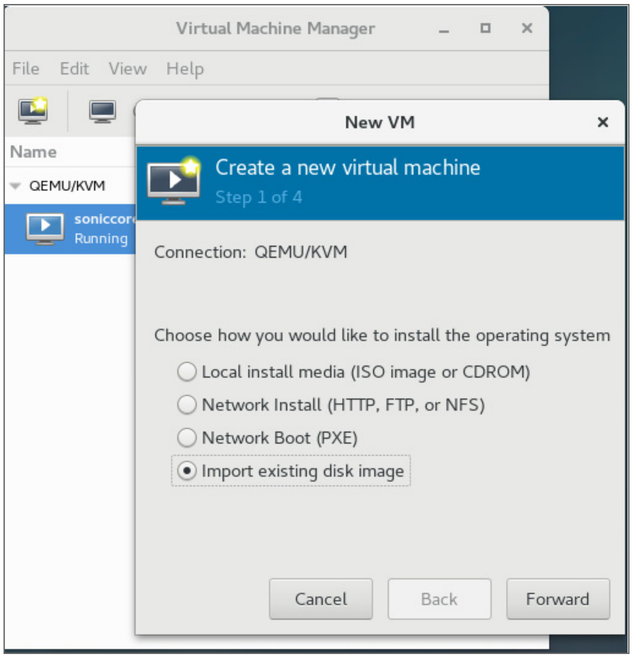
Volumes

Volumes	Size	Forma
SonicWall_NSv__For_QEMU_VM.img	50.08 GiB	qcow2

3. Bring up the Virtual Machine Manager (VMM):



4. Create a virtual machine and select the corresponding image file format (NSv is an existing disk image).



Create a new virtual machine

Step 1 of 4

Connection: QEMU/KVM

Choose how you would like to install the operating system

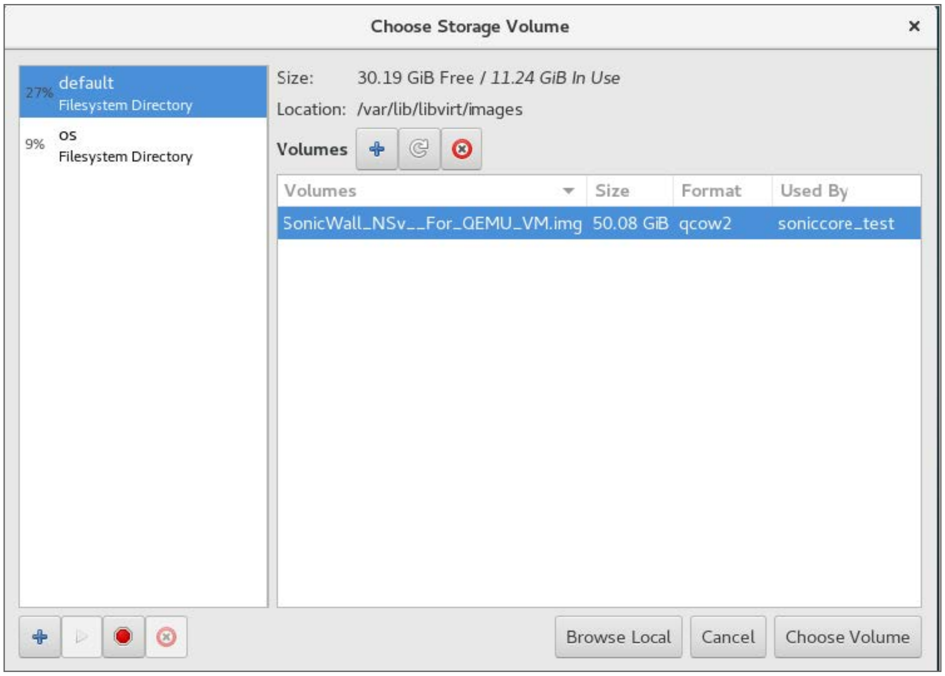
○ Local install media (ISO image or CDROM)

○ Network Install (HTTP, FTP, or NFS)

○ Network Boot (PXE)

● Import existing disk image

5. Choose the storage volume:



Choose Storage Volume

27% default Filesystem Directory

9% os Filesystem Directory

Size: 30.19 GiB Free / *11.24 GiB In Use*

Location: /var/lib/libvirt/images

Volumes	Size	Format	Used By
SonicWall_NSv__For_QEMU_VM.img	50.08 GiB	qcow2	soniccore_test

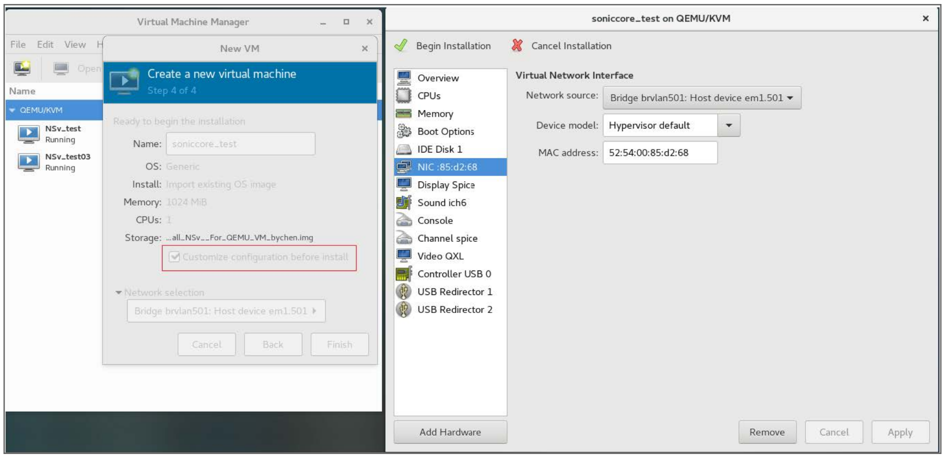
6. Configure CPU/Memory/Name/Network (default only one network interface attached), then finish to create.

   a. The default interface corresponds to X0 of the virtual machine, here we choose **a private VLAN 518**.

   b. We need to add another network interface as WAN port, that is X1 of the virtual machine, here we choose the **interface 301**.

      ⓘ **NOTE:** Both device models should choose **virtio**. By default, the first network card is X0, and the second one is X1.

   c. Create a new virtual machine with Display set as VNC otherwise you might not be able to use keyboard with new virtual machine.



Virtual Machine Manager

QEMU/KVM

NSv_test Running

NSv_test03 Running

New VM

Create a new virtual machine

Step 4 of 4

Ready to begin the installation

Name: soniccore_test

OS: Generic

Install: Import existing OS image

Memory: 1024 MiB

CPUs: 1

Storage: ...all_NSv__For_QEMU_VM_bychen.img

☑ Customize configuration before install

Network selection

Bridge brvlan501: Host device em1.501

soniccore_test on QEMU/KVM

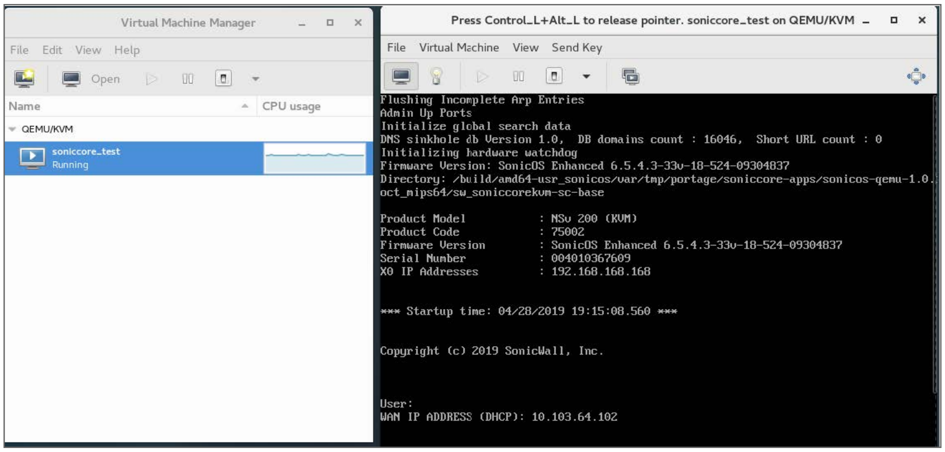
Virtual Network Interface

Network source: Bridge brvlan501: Host device em1.501

Device model: Hypervisor default

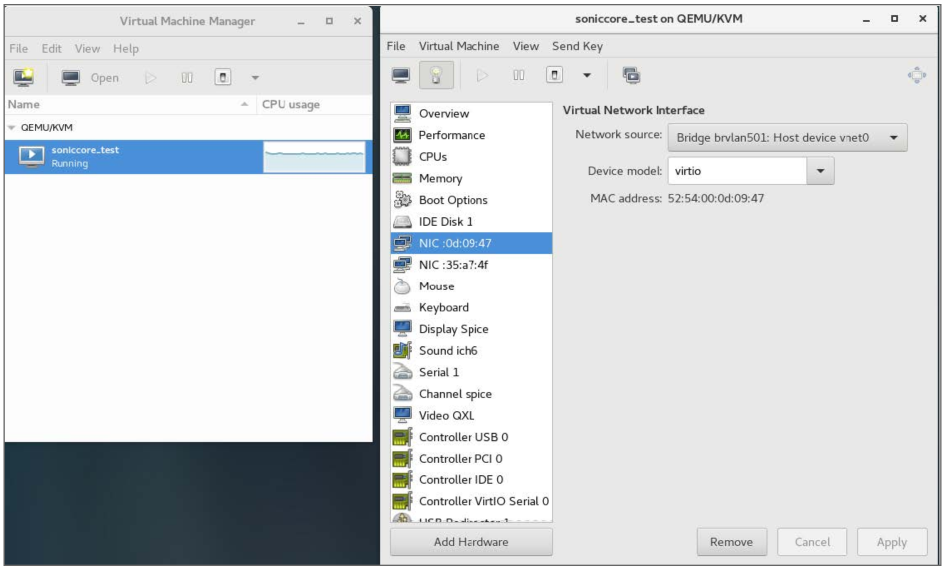
MAC address: 52:54:00:85:d2:68

7. Open the new virtual machine. Select **View > Details** and check details of configuration after boot messages. Use **View > Snapshots** to take a snapshot of the virtual machine.


Virtual Machine Manager
File Edit View Help
Open
Name
CPU usage
QEMU/KVM
soniccore_test
Running
Press Control_L+Alt_L to release pointer. soniccore_test on QEMU/KVM
File Virtual Machine View Send Key

```
Flushing Incomplete Arp Entries
Admin Up Ports
Initialize global search data
DNS sinkhole db Version 1.0,  DB domains count : 16046,  Short URL count : 0
Initializing hardware watchdog
Firmware Version: SonicOS Enhanced 6.5.4.3-33v-18-524-09304837
Directory: /build/amd64-usr_sonicos/var/tmp/portage/soniccore-apps/sonicos-qemu-1.0.
oct_mips64/sw_soniccorekvm-sc-base

Product Model            : NSv 200 (KVM)
Product Code             : 75002
Firmware Version         : SonicOS Enhanced 6.5.4.3-33v-18-524-09304837
Serial Number            : 004010367609
X0 IP Addresses          : 192.168.168.168


*** Startup time: 04/28/2019 19:15:08.560 ***


Copyright (c) 2019 SonicWall, Inc.



User:
WAN IP ADDRESS (DHCP): 10.103.64.102
```

8. Add interfaces and select virtio type:



Virtual Network Interface

Network source: Bridge brvlan501: Host device vnet0

Device model: virtio

MAC address: 52:54:00:0d:09:47

Creating NSv with Virt-install

```
# install a virtual machine from existing virtual disk image

virt-install \

--name NSv_test \ # NSv name

--memory 6144 \ # NSv memory

--vcpus 2 \ # NSv cpu counts
```

```
--disk /var/lib/libvirt/images/SonicWall_NSv__For_QEMU_VM_test.img \ # image path

--import \

--os-variant Generic \

--network bridge=brvlan501,model=virtio \ # X0

--network bridge=brvlan301,model=virtio # X1
```

Editing a Virtual Machine Configuration File

Following a "Virsh" command, you need a root right:

```
vm config file located on /etc/libvirt/qemu/<your_vmname.xml>
```

Edit the virtual machine configuration file with the following command:

```
Virsh edit <your_vmname>
```

You can check your virtual machine information using:

```
Virsh dominfo <your_vmname>
```

Adding VLAN Parameters to the Network Card

- Web Management Interface
  For best results, X0: 518 and X1: 201 is recommended.
  Access settings through **Virtual Machine Manager | Connection Details > Network Interface**
- Command Line Interface
  1. Enter:
     ```
     /etc/sysconfig/network-scripts/
     ```
  2. Execute the following commands:
     ```
     modprobe 8021q



     [root@server02 network-scripts]# cat ifcfg-enp14s0

     DEVICE=enp14s0

     TYPE=Ethernet

     BOOTPROTO=none
     ```

```
ONBOOT=yes
NM_CONTROLLED=no

[root@server02 network-scripts]# cat ifcfg-enp14s0.35
DEVICE=enp14s0.35
TYPE=Ethernet
BOOTPROTO=none
ONBOOT=yes
VLAN=yes
BRIDGE=br35
NM_CONTROLLED=no

[root@server02 network-scripts]# cat ifcfg-br35
DEVICE=br35
TYPE=Bridge
BOOTPROTO=none
ONBOOT=yes
IPADDR=10.64.35.92
PREFIX=24
GATEWAY=10.64.35.1
DNS1=10.64.28.200
DNS2=10.64.28.201
DOMAIN=acme.com
NM_CONTROLLED=no
```

```
            systemctl restart network
```

These network definitions can be selected by virtual machines.

Next Steps and Related Topics

- Registering the NSv Appliance from SonicOS
- Managing SonicOS on the NSv Series
- Using System Diagnostics
- Using the Virtual Console and SafeMode

3

Licensing and Registering Your NSv

Topics:

- Registering the NSv Appliance from SonicOS

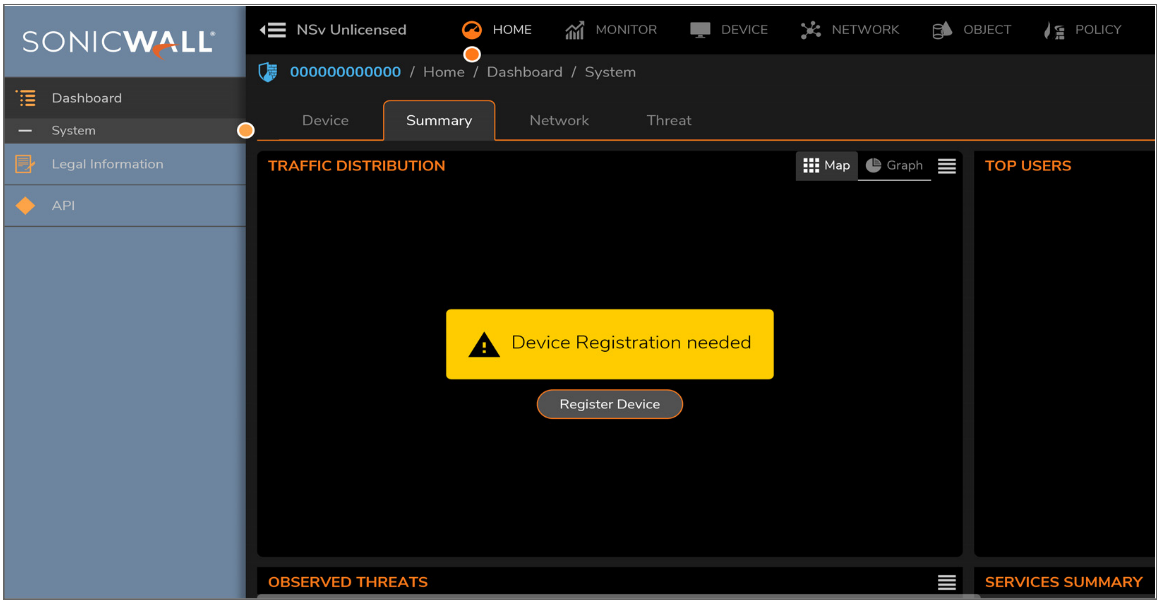
Registering the NSv Virtual Machine with SonicOS

After you have installed and configured the network settings for your NSv Series virtual machine, you can log into SonicOS management and register it in your MySonicWall account. Registration of your SonicWall NSv Series virtual machine follows the same process as for SonicWall hardware-based appliances.

ⓘ **NOTE:** System functionality is extremely limited when registration is not complete. SeeUsing System Diagnostics for more information.

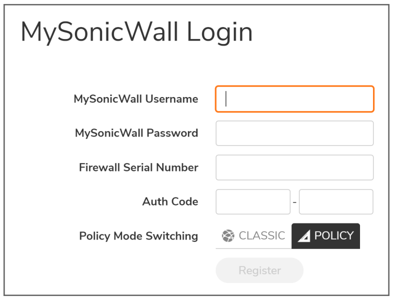
To register your NSv virtual machine:

1. Point your browser to your NSv Series WAN or LAN IP address and log in as the administrator (default admin / password).
2. Go to **Dashboard | System > Summary** and click **Register Device**.



Device Registration needed

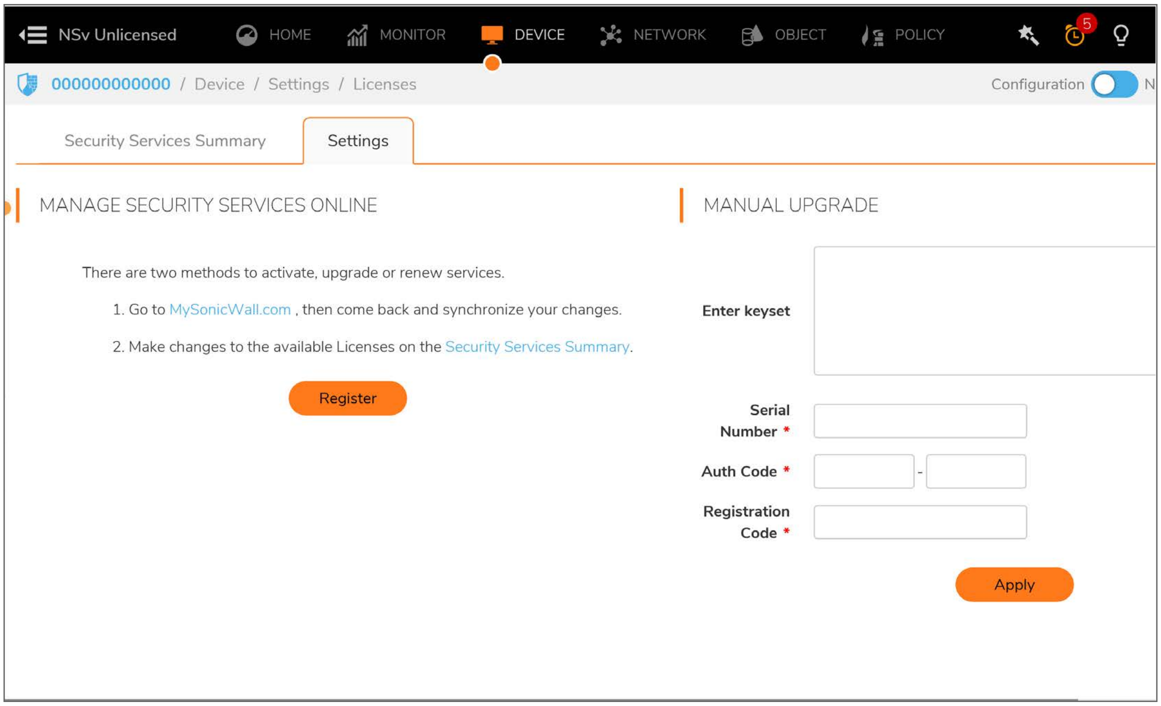
3. At this point you can log into MySonicWall and name the NSv installation while providing the **Firewall Serial Number** and authorization code (**Auth Code**), and select a **Policy Mode Switching** option (**Classic** or **Policy**). Click **Register** to complete the registration.



MySonicWall Login

MySonicWall Username
MySonicWall Password
Firewall Serial Number
Auth Code -
Policy Mode Switching CLASSIC POLICY

If you are unable to reach MySonicWall, use the **Keyset**, **Serial Number**, **Auth Code**, and **Registration Code** provided by your SonicWall representative in the **Settings** tab.



MANAGE SECURITY SERVICES ONLINE

There are two methods to activate, upgrade or renew services.

1. Go to MySonicWall.com , then come back and synchronize your changes.
2. Make changes to the available Licenses on the Security Services Summary.

MANUAL UPGRADE

Enter keyset

Serial Number *

Auth Code * -

Registration Code *

Click **Apply** to complete the registration.

4. Log in to SonicOS and check that the licensing is enabled.

4

SonicOS Management

Topics:

- Managing SonicOS on the NSv Series
- Using System Diagnostics

Managing SonicOS on the NSv Series

The X1 interface is the default WAN Interface and is set to use DHCP addressing by default, with HTTPS management enabled. To ease testing, you can utilize a DHCP server on the X1 connected network. If DHCP is not available, use the console to access the CLI and configure a static IP address.

The X0 interface is the default LAN interface, and also has HTTPS management enabled. Its IP address is set to `192.168.168.168` by default. You can map this interface to your own network during initial deployment of the OVF template. After deployment, you can reconfigure the IP address to an address in your network.

To log into SonicOS for management of the NSv:

1. Point your browser to either the LAN or WAN IP address. The login screen is displayed.

   When the X1 WAN interface is using DHCP addressing, DNS is also enabled. You can generally access the WAN address from any machine in your network.

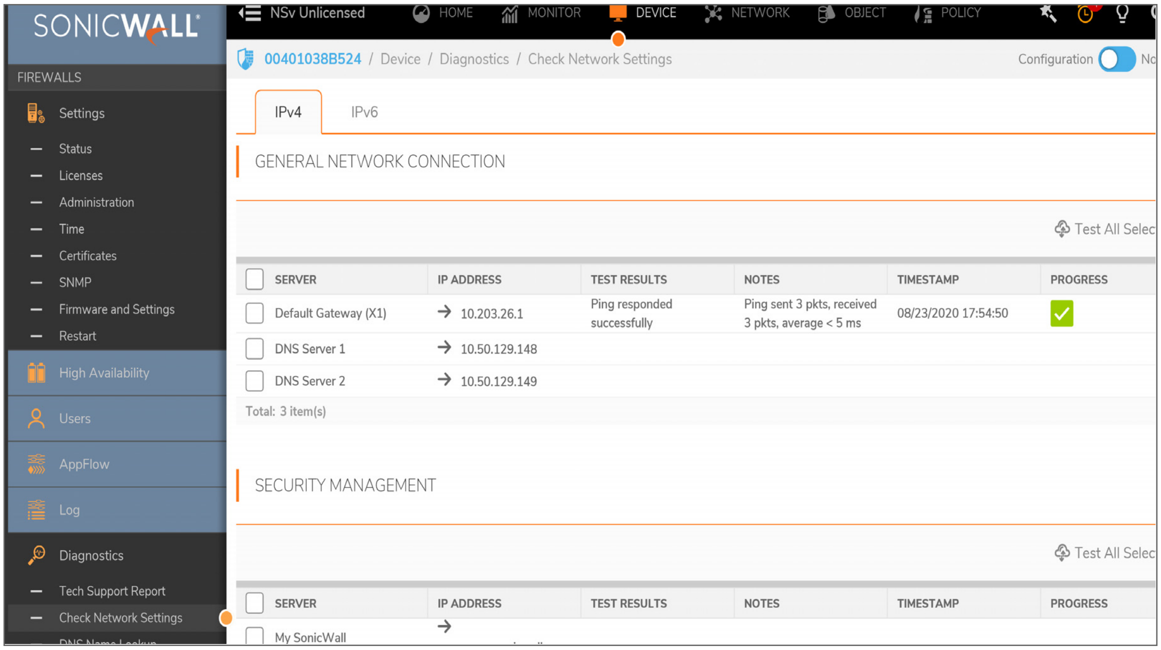
   If you have an existing network on `192.168.168.0/24` in your environment, you can access the default IP address of the X0 LAN interface of your NSv Series from a computer on that network for SonicOS management. The NSv Series X0 IP address is `192.168.168.168` by default.

2. Enter the administrator credentials (default admin / password) and press **Enter**.

   The SonicOS management interface is displayed. You can navigate and update the configuration just as you would with any SonicWall network security virtual machine

Using System Diagnostics

Check Network Settings, at **DEVICE | Diagnostics > Check Network Settings**. is a diagnostic tool that automatically checks the network connectivity and service availability of several predefined functional areas of the NSv Series, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.



00401038B524 / Device / Diagnostics / Check Network Settings

GENERAL NETWORK CONNECTION

□ SERVER	IP ADDRESS	TEST RESULTS	NOTES	TIMESTAMP	PROGRESS
□ Default Gateway (X1)	→ 10.203.26.1	Ping responded successfully	Ping sent 3 pkts, received 3 pkts, average < 5 ms	08/23/2020 17:54:50	✓
□ DNS Server 1	→ 10.50.129.148				
□ DNS Server 2	→ 10.50.129.149				

Total: 3 item(s)

SECURITY MANAGEMENT

□ SERVER	IP ADDRESS	TEST RESULTS	NOTES	TIMESTAMP	PROGRESS
□ My SonicWall	→				

Specifically, Check Network Settings automatically tests the following functions:

- Default Gateway settings
- DNS settings
- MySonicWall server connectivity
- License Manager server connectivity
- Content Filter server connectivity

To use the **Check Network Settings** tool, first select it in the **Diagnostics** drop-down menu and then click the check box in the row for the item that you want to test. The results are displayed in the same row. A green check mark signifies a successful test, and a red X indicates that there is a problem.

To test multiple items at the same time, select the **Server** checkbox at the top of the table to select all items or select the checkbox for each desired item and then click **TEST ALL SELECTED**.

If the probes fail, you can click the arrow to the left of the **IP Address** field of the failed item to jump to the configuration page to investigate the root cause.

5

Using the Virtual Console and SafeMode

Topics:

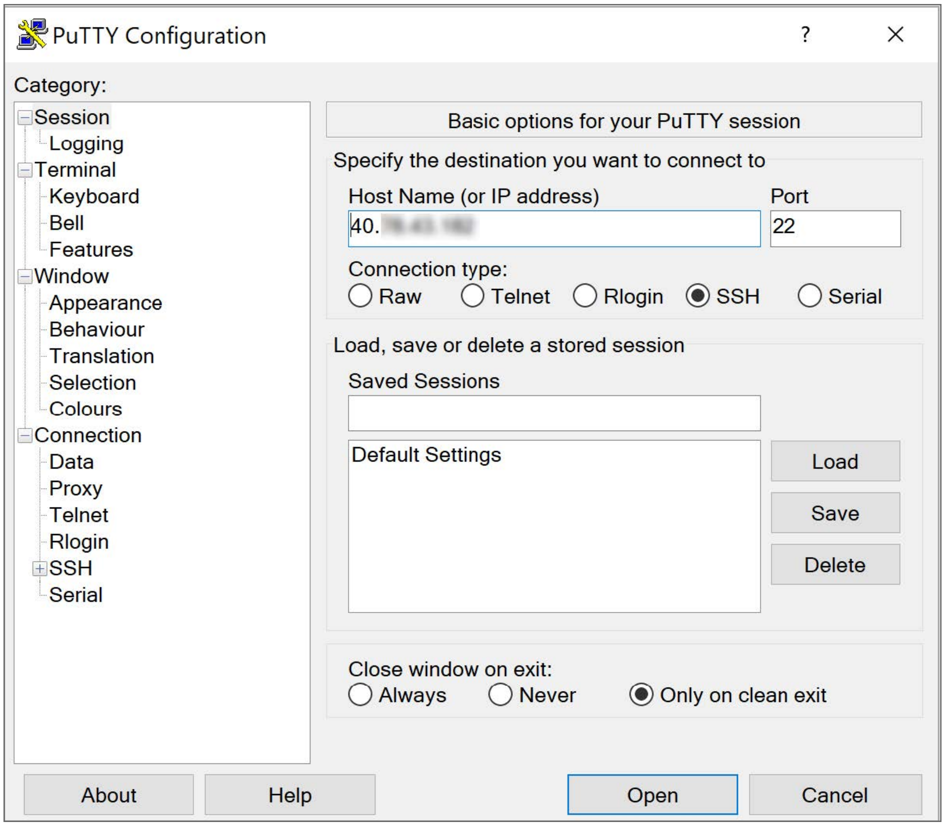
Connecting to the Management Console with SSH

There are two ways to connect to the management console:

- Use SSH or PuTTY to access the public IP address of the NSv.
- Use the Virtual Machine Manager (VMM) to access the NSv command line interface.

To connect to the management console using SSH:

1. Launch PuTTY and type in the public IP address of the NSv/QEMU.



Specify the destination you want to connect to

Host Name (or IP address): 40.[redacted]

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions:

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

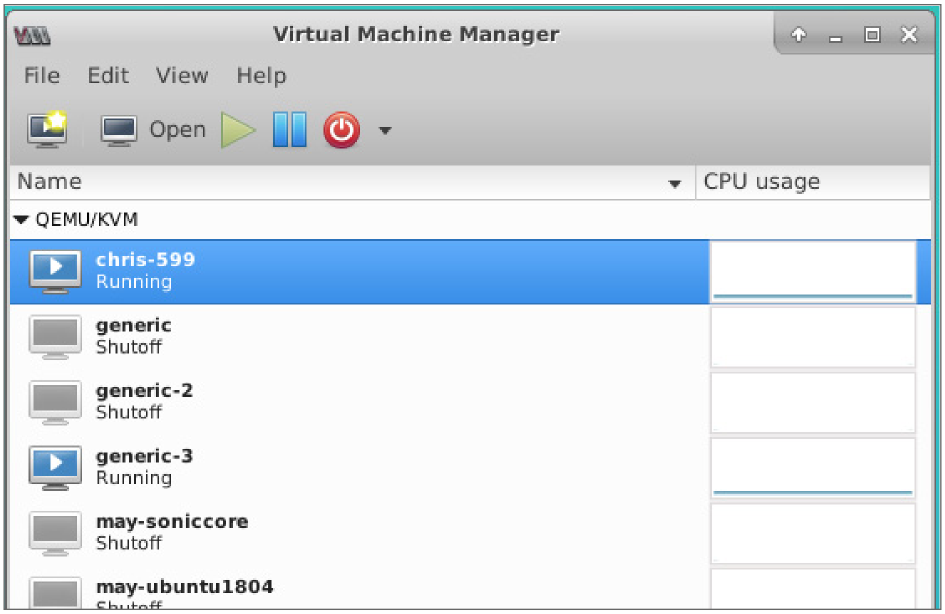
2. For **Port**, type in `22` if it is not already set.

   ⓘ **NOTE:** Changing the SSH port to anything other than 22 can prevent access to the SonicCore management console and the SonicOS CLI console.

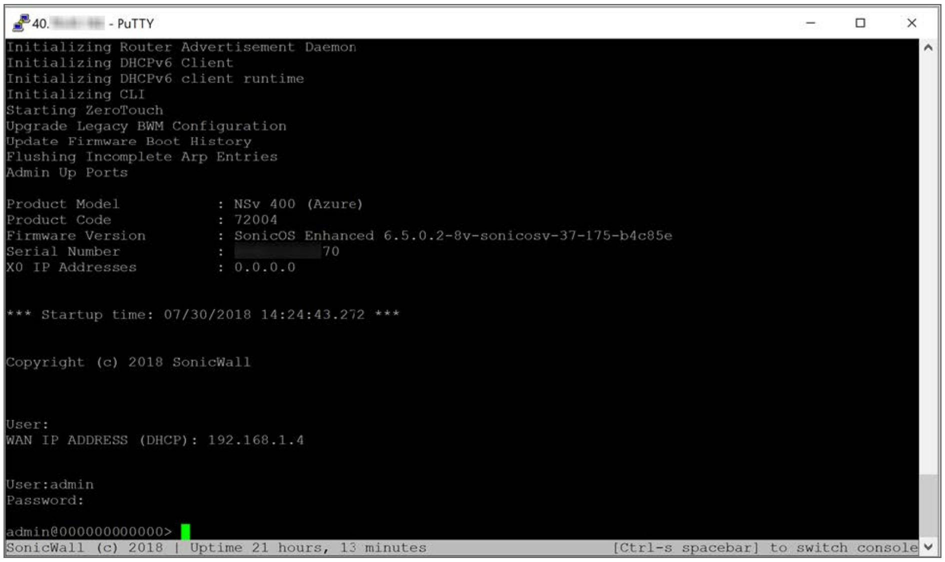
3. For **Connection type**, **SSH** should already be selected by specifying port 22.
4. Click **Open** to open a console connection.
5. When you are prompted to log in at the **User** prompt, enter the SonicOS administrator credentials (default: *admin* / *password*).

To connect to the management console through the Virtual Machine Manager:

1. Open the VMM and then double-click on the virtual machine with the NSv.



2. Wait for the NSv to boot to the command line in the **Virtual Machine Connection** window and then login as ***admin*** with the password: ***password***.



```
Initializing Router Advertisement Daemon
Initializing DHCPv6 Client
Initializing DHCPv6 client runtime
Initializing CLI
Starting ZeroTouch
Upgrade Legacy BWM Configuration
Update Firmware Boot History
Flushing Incomplete Arp Entries
Admin Up Ports

Product Model            : NSv 400 (Azure)
Product Code             : 72004
Firmware Version         : SonicOS Enhanced 6.5.0.2-8v-sonicosv-37-175-b4c85e
Serial Number            : [redacted]70
X0 IP Addresses          : 0.0.0.0

*** Startup time: 07/30/2018 14:24:43.272 ***

Copyright (c) 2018 SonicWall


User:
WAN IP ADDRESS (DHCP): 192.168.1.4

User:admin
Password:

admin@000000000000>
SonicWall (c) 2018 | Uptime 21 hours, 13 minutes                    [Ctrl-s spacebar] to switch console
```

See Navigating the NSv Management Console for more information about the options in the NSv management console.

To use the CLI to change the default X0 IP address:

1. At the CLI prompt:

   ```
   config(2CB8ED694DF8)# interface X0

   (edit-interface[X0])# ip-assignment LAN static

   (edit-LAN-static[X0])# ip 192.168.1.1 netmask 255.255.255.0

   (edit-LAN-static[X0])# commit

   % Applying changes...

   % Status returned processing command:

   commit

   Changes made
   ```

2. When IP address configuration and management settings are complete, type `restart` to reboot the NSv with the new settings.

   ⓘ | **NOTE:** Press **Ctrl+Alt** to regain control of your mouse.

After configuring an IP address and enabling management, you can log in to SonicOS on your NSv instance from a browser, or ping the virtual machine from a command window or other application.

Navigating the NSv Management Console

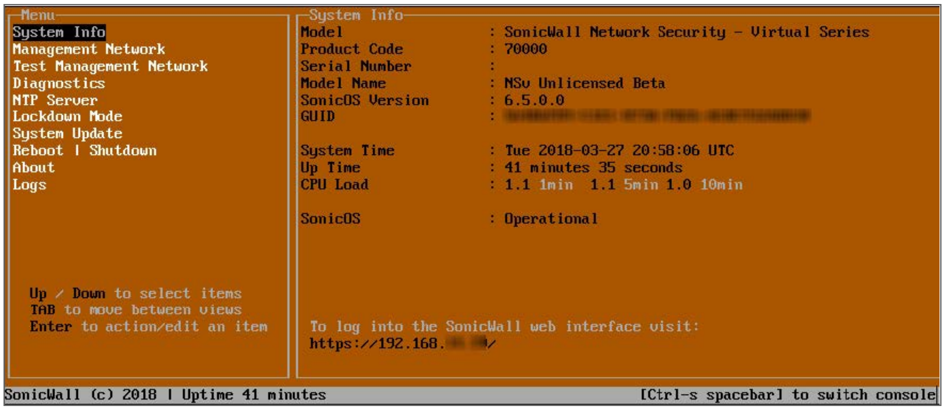
The NSv management console provides options for viewing and changing system and network settings, running diagnostics, rebooting SonicOS, and other functions.

You can connect to the NSv management console by using PuTTY or a similar application to SSH to the public IP address of an NSv.

To navigate and use the management console:

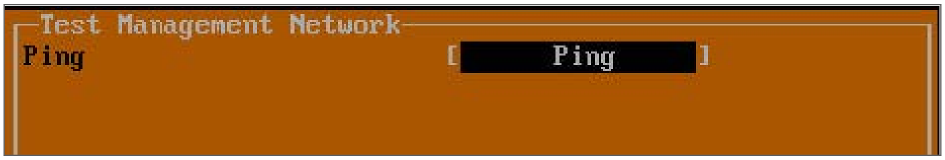
1. Press **Ctrl+s** and then press the **spacebar** to toggle between the SSH virtual console or NSv remote console and the NSv management console. That is, press the Ctrl key and ‘s’ key together, then release

and press the **spacebar**. The NSv management console has an orange background.



```
-Menu--------------------------------  -System Info-----------------------------------------------------
System Info                            Model                   : SonicWall Network Security - Virtual Series
Management Network                     Product Code            : 70000
Test Management Network                Serial Number           :
Diagnostics                            Model Name              : NSv Unlicensed Beta
NTP Server                             SonicOS Version         : 6.5.0.0
Lockdown Mode                          GUID                    : [redacted]
System Update
Reboot | Shutdown                      System Time             : Tue 2018-03-27 20:58:06 UTC
About                                  Up Time                 : 41 minutes 35 seconds
Logs                                   CPU Load                : 1.1 1min  1.1 5min 1.0 10min

                                       SonicOS                 : Operational




  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item           To log into the SonicWall web interface visit:
                                         https://192.168.[redacted]/

SonicWall (c) 2018 | Uptime 41 minutes                          [Ctrl-s spacebar] to switch console
```

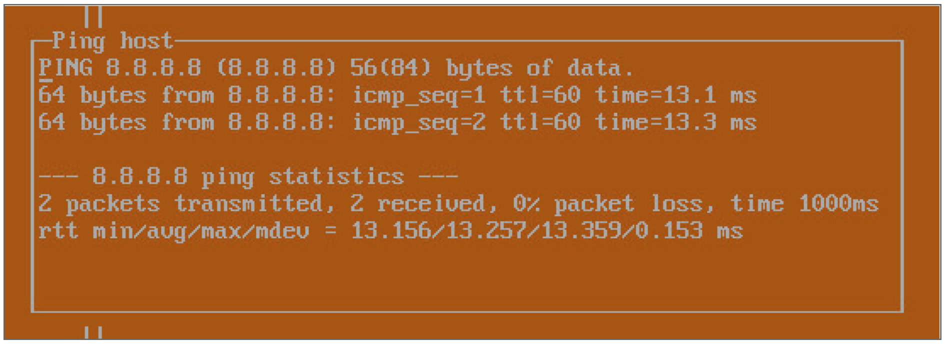
2. The main menu is displayed in the side menu (left pane). Use the up/down arrow keys to move the focus between menu items. As the focus shifts, the right pane displays the options and information for that menu item. The currently selected item is highlighted in black.
3. Press the **Tab** key to move the focus from side menu to the main view (right pane), or vice versa.
4. In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.



```
-Test Management Network-
Ping                                       [        Ping        ]
```

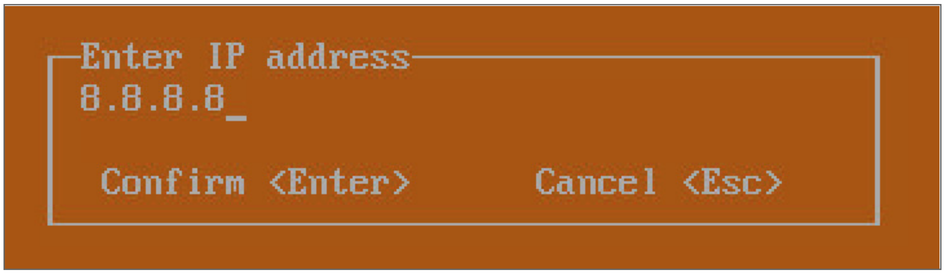
5. To select an option for editing or to choose the associated action, use the up/down arrow keys to move the focus to the editable/actionable items and press the **Enter** key.

   An edit/selection dialog is displayed in the middle of the main view following the option list. Some dialogs have selectable actions and some are information only:



```
-Ping host-
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=60 time=13.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=60 time=13.3 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 13.156/13.257/13.359/0.153 ms
```

Some dialogs are for input:



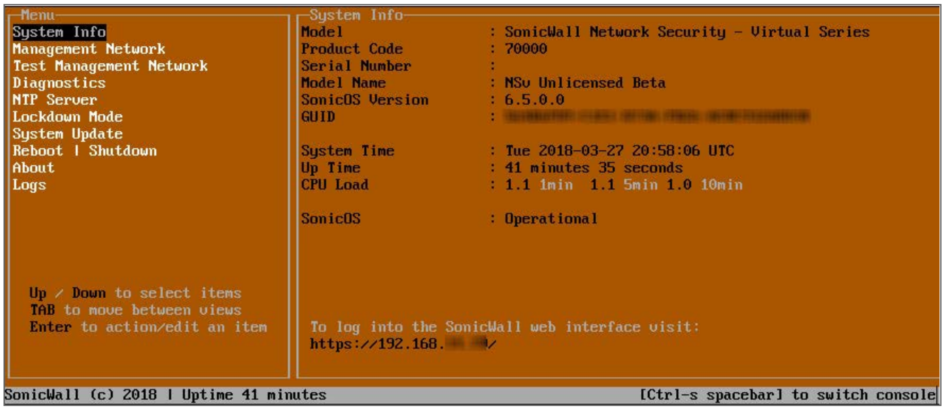
```
Enter IP address
8.8.8.8_

 Confirm <Enter>        Cancel <Esc>
```

6. Use the arrow keys as needed to move between selections in the dialog. To change a value, press **Backspace** to erase each character, then type in the new value. When ready, press **Enter** to commit the change or perform the selected action. You can dismiss the dialog by pressing **Esc**.

The NSv management menu choices are described in the following sections:

- System Info
- Management Network or Network Interfaces
- Test Management Network
- Diagnostics
- NTP Server
- Lockdown Mode
- System Update
- Reboot | Shutdown
- About
- Logs

System Info



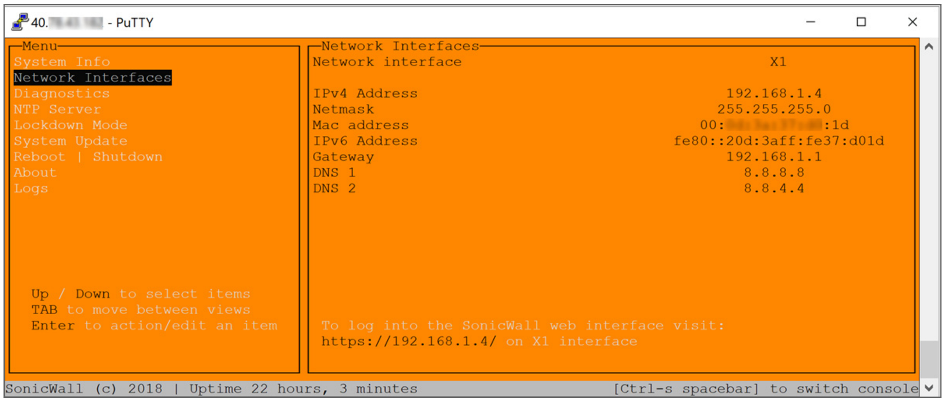
```
Menu                              System Info
System Info                       Model                  : SonicWall Network Security - Virtual Series
Management Network                Product Code           : 70000
Test Management Network           Serial Number          :
Diagnostics                       Model Name             : NSv Unlicensed Beta
NTP Server                        SonicOS Version        : 6.5.0.0
Lockdown Mode                     GUID                   : [redacted]
System Update
Reboot | Shutdown                 System Time            : Tue 2018-03-27 20:58:06 UTC
About                             Up Time                : 41 minutes 35 seconds
Logs                              CPU Load               : 1.1 1min  1.1 5min 1.0 10min

                                  SonicOS                : Operational



  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item     To log into the SonicWall web interface visit:
                                   https://192.168.[redacted]/

SonicWall (c) 2018 | Uptime 41 minutes                       [Ctrl-s spacebar] to switch console
```

Some of the information in the **System Info** screen is dynamic. The following information is displayed:

- **Model** – This is the model of the NSv virtual machine.
- **Product code** – This is the product code of the NSv virtual machine.
- **Serial Number** – The serial number for the virtual machine; this is a number unique to every NSv instance deployed. This number can be used to identify the NSv virtual machine on MySonicWall.
- **Model Name** – This is the model name of the NSv virtual machine.
- **SonicOS Version** – This is the currently running SonicOS version of the NSv virtual machine.
- **GUID** – Every NSv instance has a GUID that is displayed here.
- **System Time** – This is the current system time on the NSv virtual machine.
- **Up Time** – This is the total time that the NSv virtual machine has been running.
- **Average Load** – This shows the average CPU load for the last 1 minute, 5 minutes and 10 minutes. You can change the Average load time durations to view the CPU load over longer or shorter time periods.
- **SonicOS** – This presents the current state of the SonicOS service on the NSv. ***Operational*** is displayed here when the SonicOS service is running normally, ***Not Operational*** when there is a problem with the service and ***Operational (debug)*** if the service is currently running in debug mode.

Management Network or Network Interfaces

NETWORK INTERFACES SCREEN



```
─Menu──────────────────────────  ─Network Interfaces──────────────────────────────────────
System Info                      Network interface                               X1
Network Interfaces
Diagnostics                      IPv4 Address                                192.168.1.4
NTP Server                       Netmask                                   255.255.255.0
Lockdown Mode                    Mac address                              00:[redacted]:1d
System Update                    IPv6 Address                        fe80::20d:3aff:fe37:d01d
Reboot | Shutdown                Gateway                                     192.168.1.1
About                            DNS 1                                         8.8.8.8
Logs                             DNS 2                                         8.8.4.4



   Up / Down to select items
   TAB to move between views
   Enter to action/edit an item     To log into the SonicWall web interface visit:
                                    https://192.168.1.4/ on X1 interface

SonicWall (c) 2018 | Uptime 22 hours, 3 minutes                 [Ctrl-s spacebar] to switch console
```

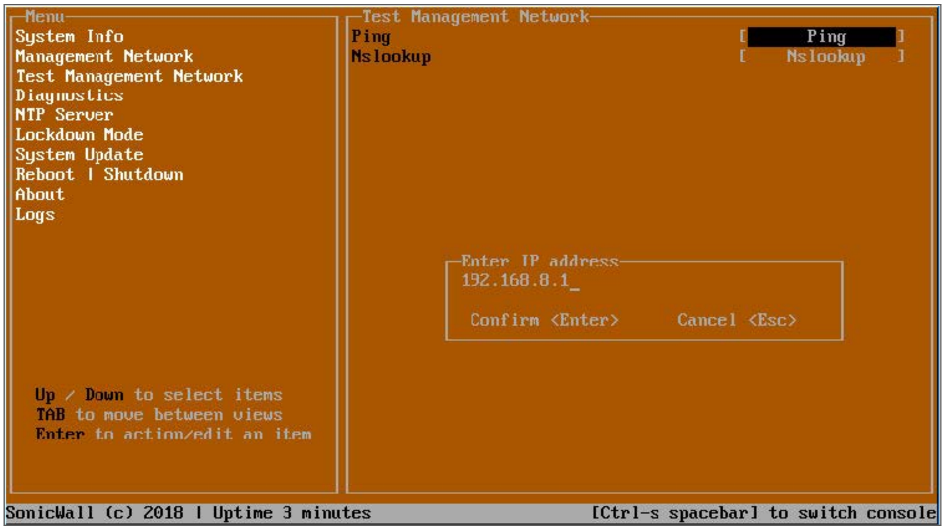
In this screen, the network settings are read-only except when the management console is in SafeMode. In SafeMode, you can configure these settings.

- **Management Interface** – This is the current interface serving as the management interface. This defaults to X1.
- **IPv4 Address** – This is the IPv4 address currently assigned to the management interface.
- **Netmask** – This is the netmask currently assigned to the management interface.
- **Mac Address** – This is the MAC address of the management interface.
- **IPv6 address** – This is the IPv6 address currently assigned to the management interface.

- **Gateway** – This is the default gateway currently in use by the NSv virtual machine.
- **DNS** – This is a list of the DNS servers currently being used by the NSv virtual machine.

Test Management Network

The **Test Management Network** screen is displayed for an NSv, but not for an NSv. In an NSv, the **Ping** and **Nslookup** commands are available on the **Diagnostics** screen.



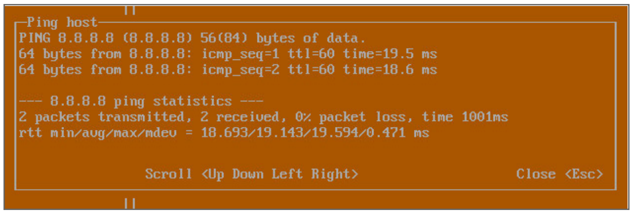
```
Menu                                 Test Management Network
System Info                          Ping                                [    Ping    ]
Management Network                   Nslookup                            [  Nslookup  ]
Test Management Network
Diagnostics
NTP Server
Lockdown Mode
System Update
Reboot | Shutdown
About
Logs

                                              Enter IP address
                                              192.168.0.1_

                                               Confirm <Enter>      Cancel <Esc>

   Up / Down to select items
   TAB to move between views
   Enter to action/edit an item

SonicWall (c) 2018 | Uptime 3 minutes                           [Ctrl-s spacebar] to switch console
```

The **Test Management Network** screen provides the **Ping** and **Nslookup** tools to test connectivity between the management interface and the local network. **Ping** is used to test whether hosts in the network are reachable. **Nslookup** is available for sending DNS queries from the NSv virtual machine.

To use Ping:

1. Select **Test Management Network** in the Menu and press **Tab** to move the focus into the **Test Management Network** screen.
2. Select **Ping** to highlight it and then press **Enter** to display the **Enter IP address** dialog.
3. Navigate into the dialog, press **Backspace** to clear the current value, and then type in the IP address that you want to ping.
4. Press **Enter**.

   The ping output is displayed in the **Ping host** dialog.

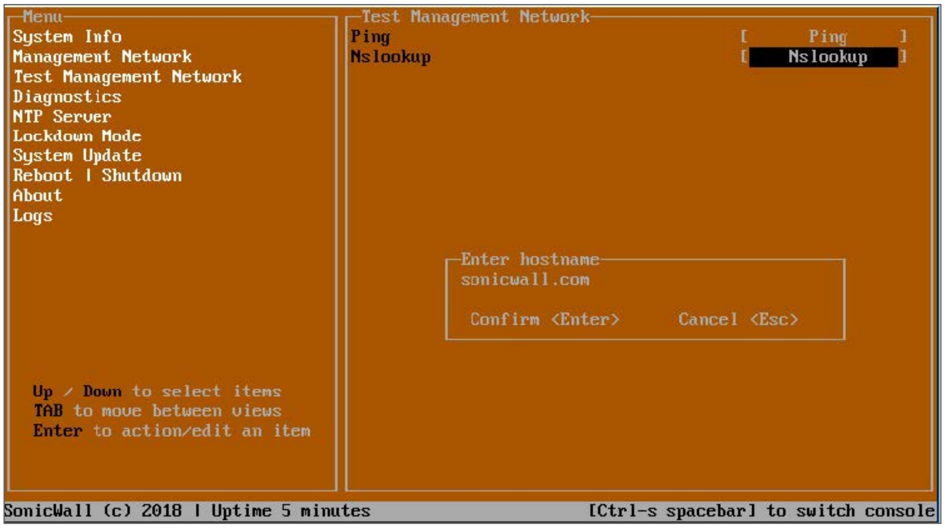


```
Ping host
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=60 time=19.5 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=60 time=18.6 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 18.693/19.143/19.594/0.471 ms
```

5. Press the **Esc** key to close the dialog.

To use Nslookup:

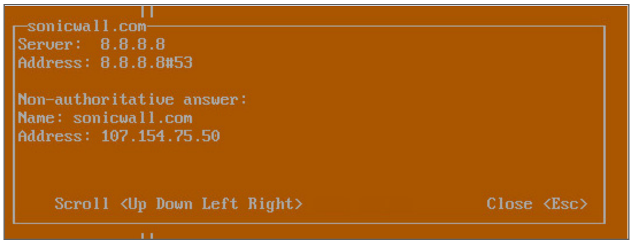
1. Select **Test Management Network** in the Menu and press **Tab** to move the focus into the **Test Management Network** screen.
2. Select **Nslookup** to highlight it and press **Enter** to display the **Enter hostname** dialog.



Enter hostname
sonicwall.com

3. Navigate into the dialog, press **Backspace** to clear the current value, and then type in the hostname that you want to look up with a DNS query.
4. Press **Enter**.

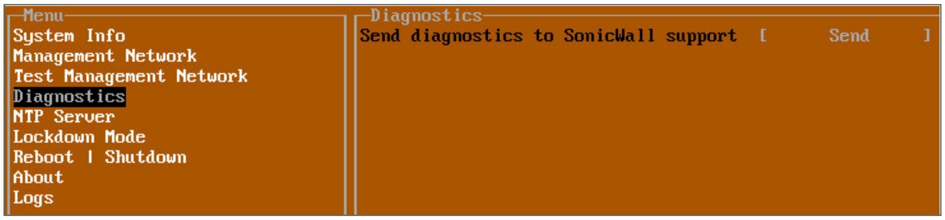
   The Nslookup query results are displayed in an information dialog. You can scroll up and down within the dialog by using the up/down arrow keys.



```
sonicwall.com
Server:  8.8.8.8
Address: 8.8.8.8#53

Non-authoritative answer:
Name: sonicwall.com
Address: 107.154.75.50
```

5. Press the **Esc** key to close the dialog.

Diagnostics

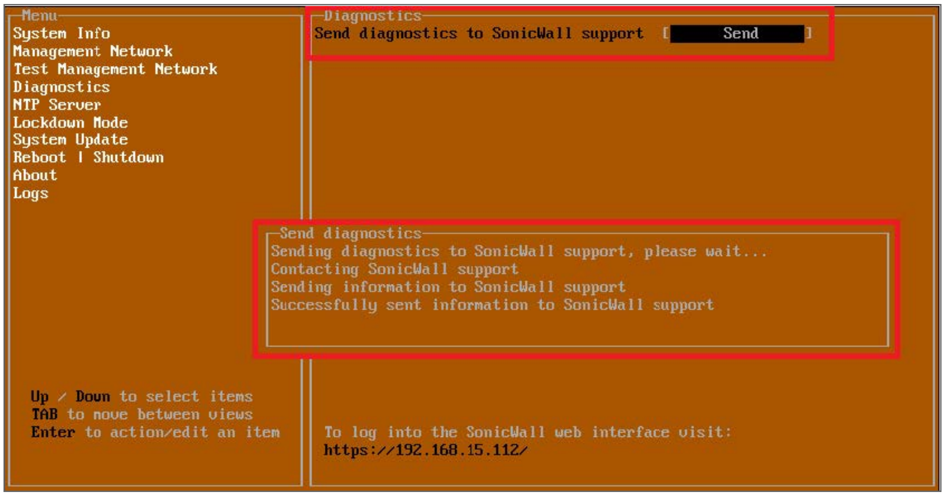


```
Menu                            Diagnostics
System Info                     Send diagnostics to SonicWall support  [      Send      ]
Management Network
Test Management Network
Diagnostics
NTP Server
Lockdown Mode
Reboot | Shutdown
About
Logs
```

In the **Diagnostics** screen, you can send diagnostics to SonicWall Technical Support. This has the same functionality as clicking **SEND DIAGNOSTIC REPORTS TO SUPPORT** in the **INVESTIGATE | Tools | System Diagnostics** page of the SonicOS web management interface.

ⓘ | **NOTE:** Your NSv virtual machine must have internet access to send the diagnostics report to SonicWall Support.

To send the diagnostics report, select **Send** in the main view to highlight it, then press **Enter**. A dialog box showing the diagnostics send output is displayed. The last message indicates success or failure.



```
Menu                         Diagnostics
System Info                  Send diagnostics to SonicWall support  [      Send      ]
Management Network
Test Management Network
Diagnostics
NTP Server
Lockdown Mode
System Update
Reboot | Shutdown
About
Logs
                          Send diagnostics
                          Sending diagnostics to SonicWall support, please wait...
                          Contacting SonicWall support
                          Sending information to SonicWall support
                          Successfully sent information to SonicWall support


  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item   To log into the SonicWall web interface visit:
                                 https://192.168.15.112/
```

Press the **Esc** key to close the dialog.

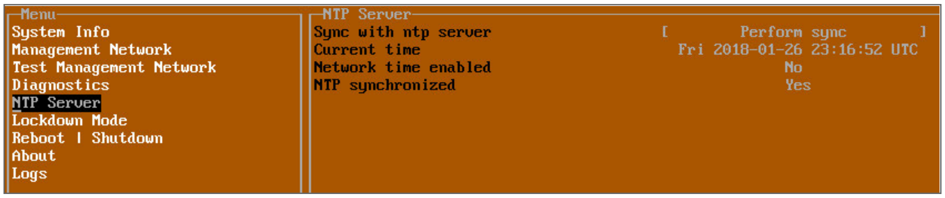
Any errors during the Send process are displayed in the **Send diagnostics** dialog box.

Common reasons for the report failing to send include:

- Misconfigured/missing default gateway
- Misconfigured/missing DNS servers
- Inline proxy

ⓘ | **NOTE:** The **Send Diagnostics** tool does not currently work through HTTP proxies.

NTP Server



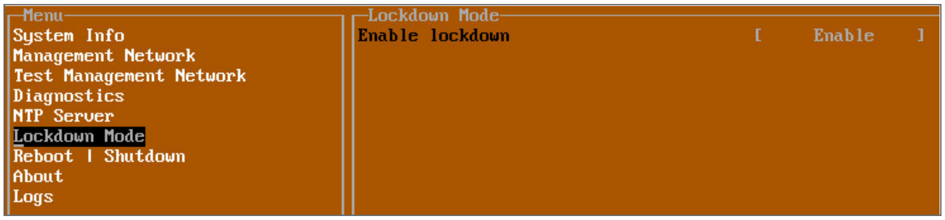
```
┌Menu──────────────────────────┐┌NTP Server─────────────────────────────────────────────────┐
System Info                      Sync with ntp server              [        Perform sync       ]
Management Network               Current time                        Fri 2018-01-26 23:16:52 UTC
Test Management Network          Network time enabled                          No
Diagnostics                      NTP synchronized                              Yes
NTP Server
Lockdown Mode
Reboot | Shutdown
About
Logs
```

In the **NTP Server** screen, you can synchronize with an NTP server. For complete NTP Server configuration options, log into the SonicOS management interface and navigate to the **MANAGE | Appliance > System Time** page.

The **NTP Server** screen displays the following information:

- **Sync with NTP server** – This button forces the NSv virtual machine's NTP client to perform a sync with the configured NTP server(s).
- **Current time** – The current time on the NSv virtual machine.
- **Network time enabled** – A Yes/No value determining whether the NTP client is currently configured to keep in sync with an NTP server.
- **NTP synchronized** – A Yes/No value determining if the NSv virtual machine is currently synchronized with the configured NTP server(s).

Lockdown Mode



```
┌Menu──────────────────────────┐┌Lockdown Mode──────────────────────────────┐
System Info                      Enable lockdown              [     Enable     ]
Management Network
Test Management Network
Diagnostics
NTP Server
Lockdown Mode
Reboot | Shutdown
About
Logs
```

In the **Lockdown Mode** screen, you can enable ***Strict Lockdown*** mode. When enabled, the management console is effectively disabled. A dialog box that cannot be closed is permanently displayed on the management console. This prevents any person from accessing the management console.

To enable Strict Lockdown mode, select **Enable** and then press **Enter**.

△ **CAUTION: Be careful about enabling Strict Lockdown mode. Strict Lockdown mode cannot be disabled.**

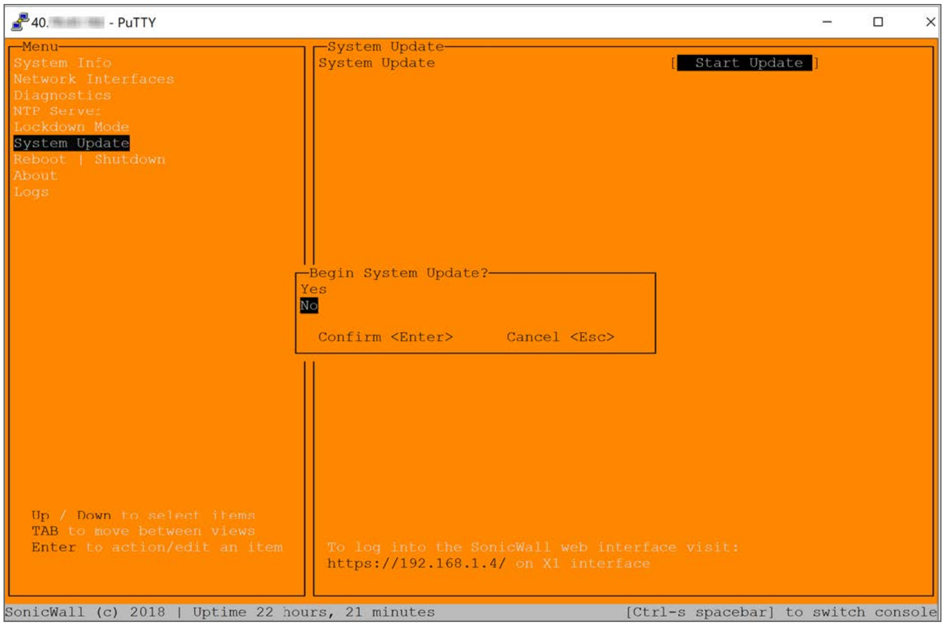
Temporary Lockdown Mode

A temporary lockdown mode can be enabled and disabled in SonicOS on the **MANAGE | Appliance > Base Settings** page. You can enable lockdown mode by clearing the **Enable management console** checkbox under the **Advanced Management** section, and can disable lockdown mode by selecting the checkbox. Click **ACCEPT** after each change.

The management console is automatically enabled/disabled a few seconds after it has been enabled/disabled in the SonicOS web interface page.

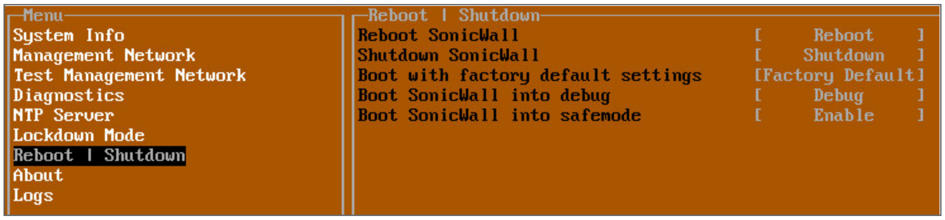
System Update

The **System Update** screen is available on NSv.



```
Menu                                 System Update
System Info                          System Update                       [ Start Update ]
Network Interfaces
Diagnostics
NTP Serve:
Lockdown Mode
System Update
Reboot | Shutdown
About
Logs

                                   Begin System Update?
                                   Yes
                                   No

                                     Confirm <Enter>       Cancel <Esc>


  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item          To log into the SonicWall web interface visit:
                                        https://192.168.1.4/ on X1 interface
SonicWall (c) 2018 | Uptime 22 hours, 21 minutes             [Ctrl-s spacebar] to switch console
```

Reboot | Shutdown



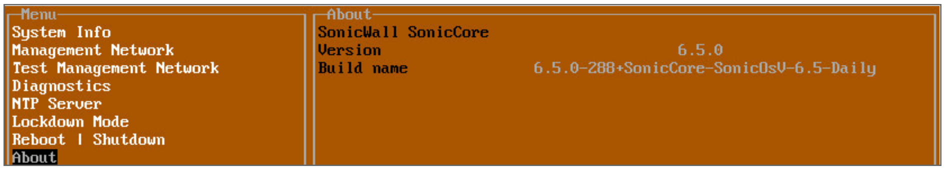
```
Menu                          Reboot | Shutdown
System Info                   Reboot SonicWall                      [     Reboot     ]
Management Network            Shutdown SonicWall                    [    Shutdown    ]
Test Management Network       Boot with factory default settings    [Factory Default]
Diagnostics                   Boot SonicWall into debug             [     Debug      ]
NTP Server                    Boot SonicWall into safemode          [     Enable     ]
Lockdown Mode
Reboot | Shutdown
About
Logs
```

The **Reboot | Shutdown** screen provides functions for rebooting the NSv virtual machine, enabling debug mode, and enabling SafeMode. To perform an action, position the focus and then press **Enter** to select the desired action. Select **Yes** in the confirmation dialog, then press **Enter** again.

The actions available on the **Reboot | Shutdown** screen are:

- **Reboot SonicWall** – Restarts the NSv Series virtual machine with current configuration settings.
- **Shutdown SonicWall** – Powers off the NSv Series virtual machine.
- **Boot with factory default settings** – Restarts the NSv Series virtual machine using factory default settings. All configuration settings are erased.
- **Boot SonicWall into debug** – Restarts the NSv Series virtual machine into debug mode. Normally this operation is performed under the guidance of SonicWall Technical Support.
- **Boot SonicWall into safemode** – Puts the NSv Series virtual machine into SafeMode. For more information, see Using SafeMode on the NSv.

About

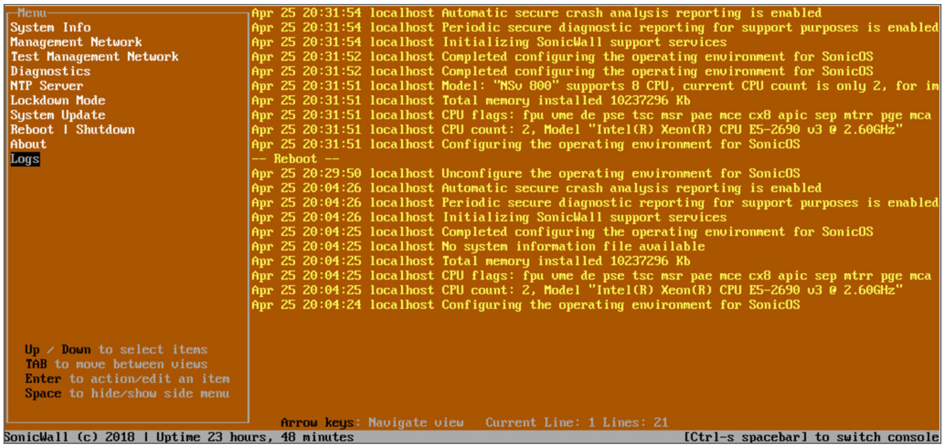


```
SonicWall SonicCore
Version                       6.5.0
Build name          6.5.0-288+SonicCore-SonicOsV-6.5-Daily
```

The **About** screen provides information about the software version and build.

Logs

The **Logs** screen displays log events for the NSv virtual machine.



```
Apr 25 20:31:54 localhost Automatic secure crash analysis reporting is enabled
Apr 25 20:31:54 localhost Periodic secure diagnostic reporting for support purposes is enabled
Apr 25 20:31:54 localhost Initializing SonicWall support services
Apr 25 20:31:52 localhost Completed configuring the operating environment for SonicOS
Apr 25 20:31:52 localhost Completed configuring the operating environment for SonicOS
Apr 25 20:31:51 localhost Model: "NSv 800" supports 8 CPU, current CPU count is only 2, for im
Apr 25 20:31:51 localhost Total memory installed 10237296 Kb
Apr 25 20:31:51 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Apr 25 20:31:51 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz"
Apr 25 20:31:51 localhost Configuring the operating environment for SonicOS
-- Reboot --
Apr 25 20:29:50 localhost Unconfigure the operating environment for SonicOS
Apr 25 20:04:26 localhost Automatic secure crash analysis reporting is enabled
Apr 25 20:04:26 localhost Periodic secure diagnostic reporting for support purposes is enabled
Apr 25 20:04:26 localhost Initializing SonicWall support services
Apr 25 20:04:25 localhost Completed configuring the operating environment for SonicOS
Apr 25 20:04:25 localhost No system information file available
Apr 25 20:04:25 localhost Total memory installed 10237296 Kb
Apr 25 20:04:25 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Apr 25 20:04:25 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz"
Apr 25 20:04:24 localhost Configuring the operating environment for SonicOS
```

Up / Down to select items
TAB to move between views
Enter to action/edit an item
Space to hide/show side menu
Arrow keys: Navigate view   Current Line: 1 Lines: 21
SonicWall (c) 2018 | Uptime 23 hours, 48 minutes
[Ctrl-s spacebar] to switch console

Using SafeMode on the NSv

The NSv virtual machine enters SafeMode when SonicOS restarts three times unexpectedly within 200 seconds. When the NSv virtual machine is in SafeMode, the virtual machine starts with a very limited set of services and features enabled. This is useful when trying to troubleshoot issues. The NSv virtual machine can also be configured to boot into SafeMode by using the **Reboot | Shutdown** screen in the NSv management console.

Topics:

- How Management Console Differs in SafeMode
- Entering SafeMode

How Management Console Differs in SafeMode

In SafeMode, some of the features the management console provides are different in the following ways:

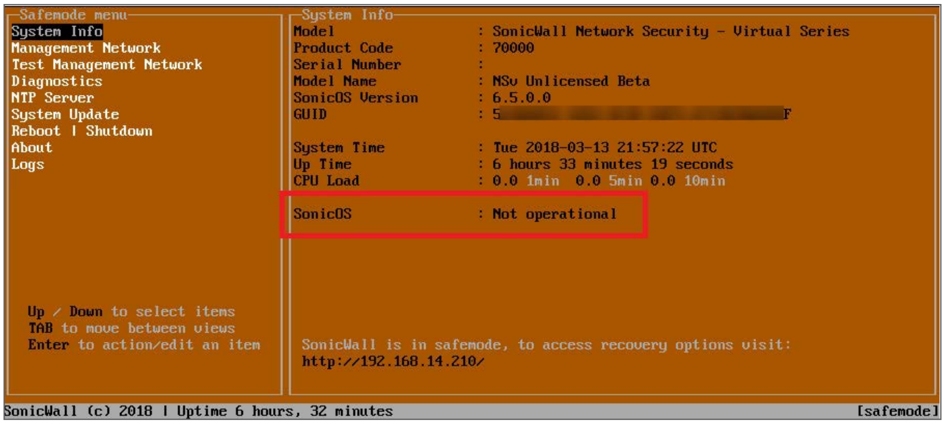
- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

  ⓘ | **NOTE:** Changes made to interfaces in SafeMode are ***not*** persistent between reboots.

When the NSv is in SafeMode, the SonicOS service is one of the services that is not enabled and is shown as Not operational on the SafeMode **System Info** screen.

Entering SafeMode

After booting into SafeMode, the Management Console always starts with the **System Info** screen.



```
Safemode menu                         System Info
System Info                           Model              : SonicWall Network Security - Virtual Series
Management Network                    Product Code       : 70000
Test Management Network               Serial Number      :
Diagnostics                           Model Name         : NSv Unlicensed Beta
NTP Server                            SonicOS Version    : 6.5.0.0
System Update                         GUID               : 5[redacted]F
Reboot | Shutdown
About                                 System Time        : Tue 2018-03-13 21:57:22 UTC
Logs                                  Up Time            : 6 hours 33 minutes 19 seconds
                                      CPU Load           : 0.0 1min  0.0 5min 0.0 10min

                                      SonicOS            : Not operational



  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item         SonicWall is in safemode, to access recovery options visit:
                                       http://192.168.14.210/

SonicWall (c) 2018 | Uptime 6 hours, 32 minutes                                         [safemode]
```

ⓘ **NOTE:** To exit SafeMode, disable it on the **Reboot | Shutdown** screen or deploy a new firmware image. See Disabling SafeMode and Installing a New SonicOS Version in SafeMode for more information.

Topics:

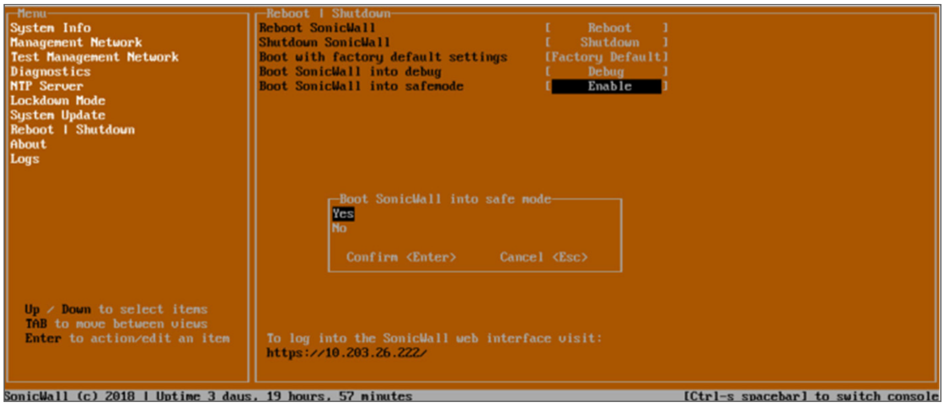
- Enabling SafeMode
- Disabling SafeMode
- Configuring the Management Network in SafeMode

Enabling SafeMode

SafeMode can be enabled from the management console.

To enable SafeMode:

1. Access the NSv management console as described in one of:
   - For NSv, see: Connecting to the Console with SSH
2. In the console, select the **Reboot | Shutdown** option and then press **Enter**.
3. Navigate down to the **Boot SonicWall into safemode** option to highlight **Enable**, and then press **Enter**.



```
Menu                           Reboot | Shutdown
System Info                    Reboot SonicWall                  [     Reboot     ]
Management Network             Shutdown SonicWall                [    Shutdown    ]
Test Management Network        Boot with factory default settings [Factory Default]
Diagnostics                    Boot SonicWall into debug         [     Debug      ]
NTP Server                     Boot SonicWall into safemode      [     Enable     ]
Lockdown Mode
System Update
Reboot | Shutdown
About
Logs

                                         Boot SonicWall into safe mode
                                         Yes
                                         No

                                           Confirm <Enter>      Cancel <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item   To log into the SonicWall web interface visit:
                                 https://10.203.26.222/

SonicWall (c) 2018 | Uptime 3 days, 19 hours, 57 minutes          [Ctrl-s spacebar] to switch console
```

4. Select **Yes** in the confirmation dialog.
5. Press **Enter**.

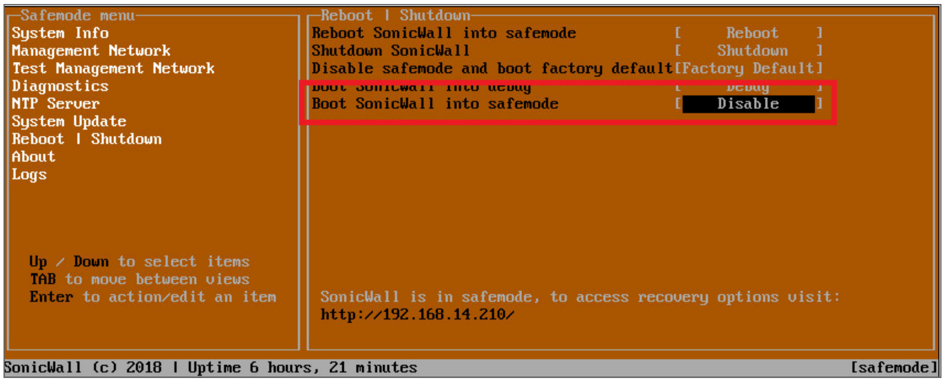
   The NSv immediately reboots and comes back up in SafeMode.

   ⓘ **NOTE:** In SafeMode, the web interface is served from an HTTP server. The HTTPS server is not started in SafeMode.

Disabling SafeMode

To disable SafeMode:

1. In the SafeMode menu in the NSv management console, select the **Reboot | Shutdown** option and press **Enter**.
2. In the **Reboot | Shutdown** screen, navigate down to the **Boot SonicWall into safemode** option to highlight **Disable**, and then press **Enter**.

   ```
   Safemode menu                   Reboot | Shutdown
   System Info                     Reboot SonicWall into safemode           [     Reboot     ]
   Management Network              Shutdown SonicWall                       [    Shutdown    ]
   Test Management Network         Disable safemode and boot factory default[Factory Default]
   Diagnostics                     Boot SonicWall into debug                [     Debug      ]
   NTP Server                      Boot SonicWall into safemode             [    Disable     ]
   System Update
   Reboot | Shutdown
   About
   Logs



     Up / Down to select items
     TAB to move between views
     Enter to action/edit an item   SonicWall is in safemode, to access recovery options visit:
                                    http://192.168.14.210/

   SonicWall (c) 2018 | Uptime 6 hours, 21 minutes                                  [safemode]
   ```

3. Select **Yes** in the confirmation dialog.
4. Press **Enter**.

   The NSv immediately reboots and boots up in normal mode.

Configuring the Management Network in SafeMode

When the Management Console is in SafeMode, the **Management Network** screen in the NSv management console provides features to configure the NSv virtual machine interfaces:

- **Management Interface** – This is the currently selected interface. This defaults to X1. Use this to select any of the NSv virtual machine interfaces.
- **IPv4 Address** – The current IPv4 address currently assigned to the Management Interface.
- **Netmask** – The current Netmask assigned to the Management Interface.
- **Mac Address** – The MAC address of the Management Interface.
- **IPv6 Address** – The currently assigned IPv6 address of the Management Interface.
- **Gateway** – The current Default Gateway currently in use by the NSv virtual machine.
- **DNS** – A list of the current DNS servers currently being used by the NSv virtual machine.

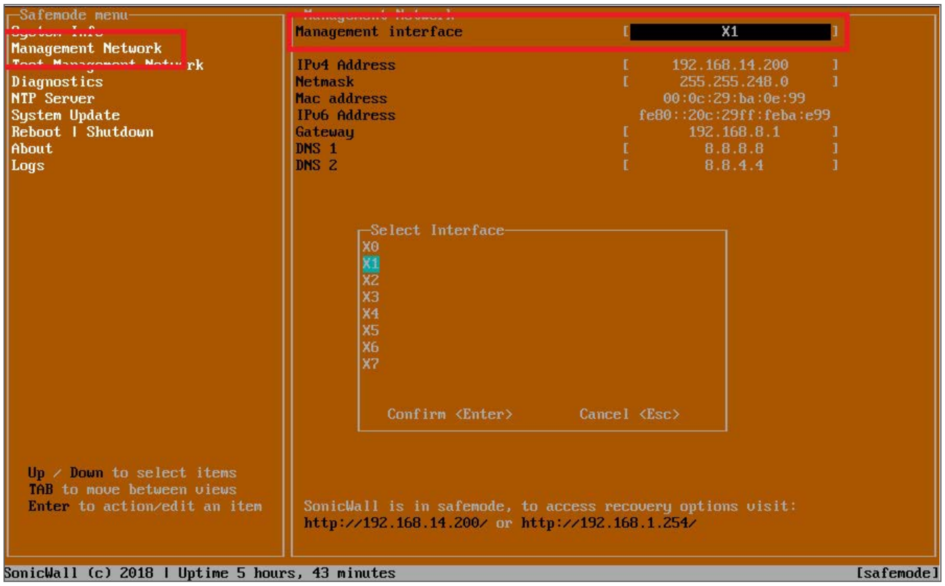
Changes made to interfaces in SafeMode are ***not*** persistent between reboots.

Topics:

- Configuring Interface Settings
- Disabling an Interface

Configuring Interface Settings

In SafeMode, the **Management Network** screen includes editable and actionable items that are read-only when the management console is in normal mode.

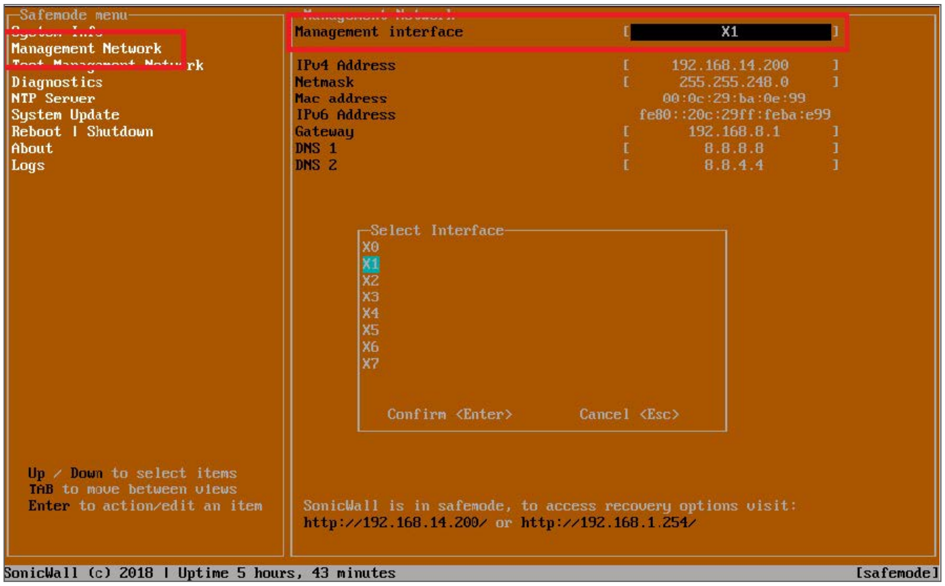


```
Safemode menu                          Management Network
System Info                            Management interface                          [          X1          ]
Management Network
Test Management Network                IPv4 Address                                  [     192.168.14.200     ]
Diagnostics                            Netmask                                       [      255.255.248.0     ]
NTP Server                             Mac address                                       00:0c:29:ba:0e:99
System Update                          IPv6 Address                                   fe80::20c:29ff:feba:e99
Reboot | Shutdown                      Gateway                                       [       192.168.8.1      ]
About                                  DNS 1                                         [         8.8.8.8        ]
Logs                                   DNS 2                                         [         8.8.4.4        ]

                                                 Select Interface
                                                 X0
                                                 X1
                                                 X2
                                                 X3
                                                 X4
                                                 X5
                                                 X6
                                                 X7

                                                    Confirm <Enter>          Cancel <Esc>

   Up / Down to select items
   TAB to move between views
   Enter to action/edit an item          SonicWall is in safemode, to access recovery options visit:
                                         http://192.168.14.200/ or http://192.168.1.254/

SonicWall (c) 2018 | Uptime 5 hours, 43 minutes                                                        [safemode]
```

To edit an interface:

1. In the SafeMode **Management Network** screen, select the **Management interface** option and then press **Enter**.

   The **Select Interface** list appears, displaying all of the interfaces available on the NSv.



```
Safemode menu                          Management Network
System Info                            Management interface          [          X1           ]
Management Network
Test Management Network                IPv4 Address                  [     192.168.14.200     ]
Diagnostics                            Netmask                       [     255.255.248.0      ]
NTP Server                             Mac address                        00:0c:29:ba:0e:99
System Update                          IPv6 Address                     fe80::20c:29ff:feba:e99
Reboot | Shutdown                      Gateway                       [      192.168.8.1       ]
About                                  DNS 1                         [        8.8.8.8         ]
Logs                                   DNS 2                         [        8.8.4.4         ]

                                            Select Interface
                                            X0
                                            X1
                                            X2
                                            X3
                                            X4
                                            X5
                                            X6
                                            X7

                                               Confirm <Enter>          Cancel <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item           SonicWall is in safemode, to access recovery options visit:
                                         http://192.168.14.200/ or http://192.168.1.254/

SonicWall (c) 2018 | Uptime 5 hours, 43 minutes                                        [safemode]
```

2. Select the interface you wish to edit and press **Enter**.

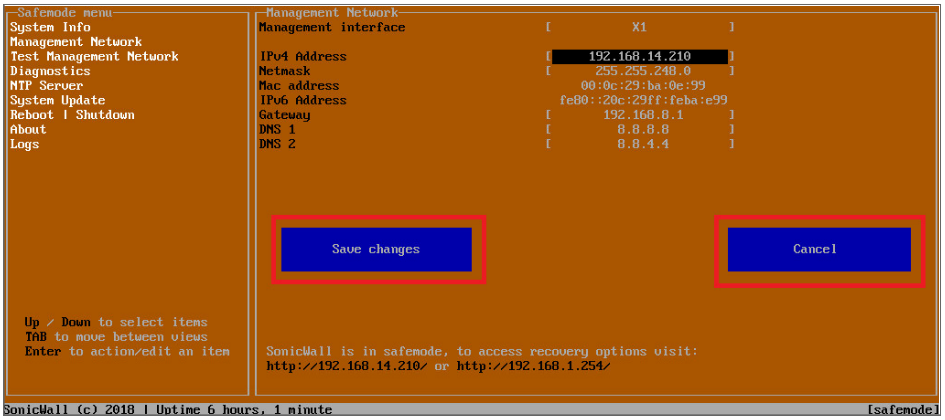
   The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

3. To edit the IPv4 address, select **IPv4 Address** on the screen and press **Enter**.

   The on-screen dialog displays the current IP address.

4. Navigate into the dialog and make the desired changes, then press **Enter** to close the dialog or press **Esc** to cancel and close the dialog.

5. Two new buttons appear on the screen after you make changes to an interface setting: **Save changes** or **Cancel**. You can use the **Tab** key to navigate to these buttons.



```
Safemode menu                          Management Network
System Info                            Management interface          [          X1           ]
Management Network
Test Management Network                IPv4 Address                  [     192.168.14.210     ]
Diagnostics                            Netmask                       [     255.255.248.0      ]
NTP Server                             Mac address                        00:0c:29:ba:0e:99
System Update                          IPv6 Address                     fe80::20c:29ff:feba:e99
Reboot | Shutdown                      Gateway                       [      192.168.8.1       ]
About                                  DNS 1                         [        8.8.8.8         ]
Logs                                   DNS 2                         [        8.8.4.4         ]


                                          Save changes                              Cancel


  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item           SonicWall is in safemode, to access recovery options visit:
                                         http://192.168.14.210/ or http://192.168.1.254/

SonicWall (c) 2018 | Uptime 6 hours, 1 minute                                          [safemode]
```

ⓘ **NOTE:** You cannot navigate to the left navigation pane until you either save changes or cancel using these buttons.

Do one of the following:

- To make changes to other settings for this interface, navigate to the desired setting, press **Enter**, make the changes in the dialog, then press **Enter** to close the dialog for that setting. Repeat for other settings, as needed.
- If finished making changes to the settings for this interface, press **Tab** to navigate to the **Save changes** button and then press **Enter** to save your changes.
- Press **Tab** to navigate to the **Cancel** button and then press **Enter** to cancel all changes to the settings for this interface.

Disabling an Interface

You can disable an interface while in SafeMode.

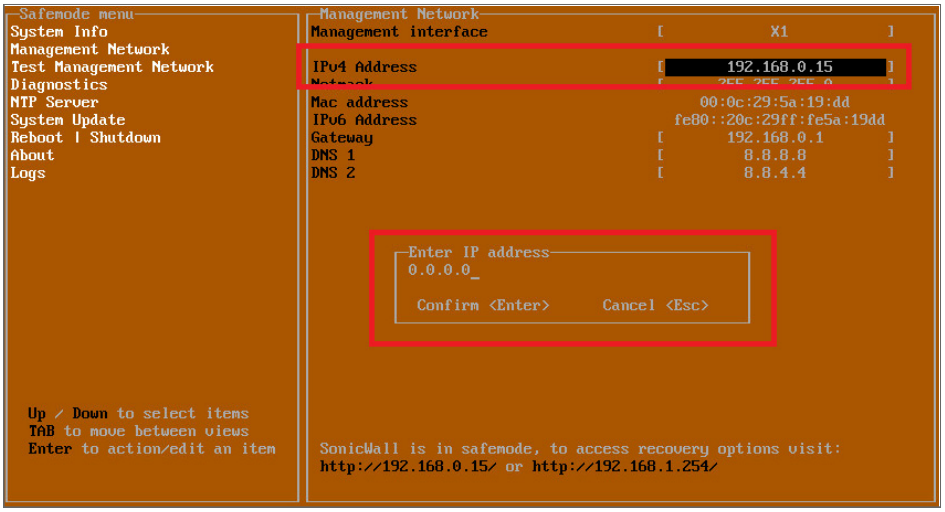
To disable an interface:

1. In the SafeMode **Management Network** screen, select the **Management interface** option.
2. Press **Enter**.

   The **Select Interface** list appears, displaying all of the interfaces available on the NSv.
3. Select the interface you wish to edit and press **Enter**.

   The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed previously on the interface selection dialog.
4. Select **IPv4 Address** and press **Enter**.

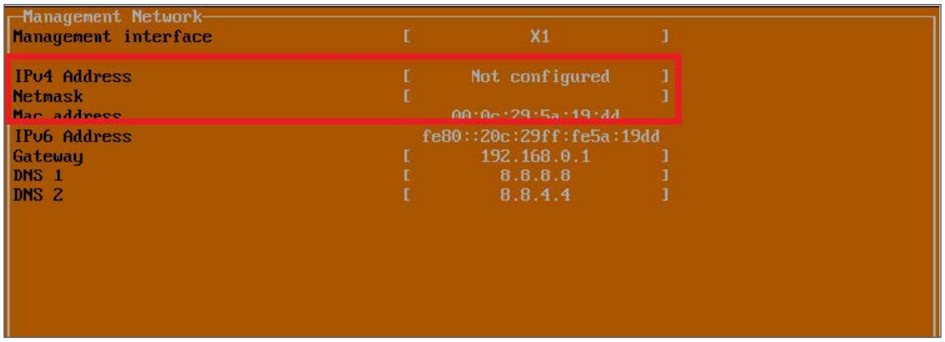
   The onscreen dialog displays the current IP address.
5. Navigate into the dialog and change the IP address to `0.0.0.0`, then press **Enter**.



```
Safemode menu                  Management Network
System Info                    Management interface            [        X1          ]
Management Network
Test Management Network        IPv4 Address                    [    192.168.0.15    ]
Diagnostics                    Netmask                         [    255.255.255.0   ]
NTP Server                     Mac address                       00:0c:29:5a:19:dd
System Update                  IPv6 Address                    fe80::20c:29ff:fe5a:19dd
Reboot | Shutdown              Gateway                         [    192.168.0.1     ]
About                          DNS 1                           [      8.8.8.8       ]
Logs                           DNS 2                           [      8.8.4.4       ]

                                     Enter IP address
                                     0.0.0.0_

                                      Confirm <Enter>        Cancel <Esc>

  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item   SonicWall is in safemode, to access recovery options visit:
                                 http://192.168.0.15/ or http://192.168.1.254/
```

   Save changes displays.
6. Press **Tab** to navigate to **Save changes** and then press **Enter**.

The interface is disabled.



```
Management Network
Management interface                    [          X1          ]

IPv4 Address                            [    Not configured    ]
Netmask                                 [                      ]
Mac address                                00:0c:29:5a:19:dd
IPv6 Address                              fe80::20c:29ff:fe5a:19dd
Gateway                                 [      192.168.0.1     ]
DNS 1                                   [        8.8.8.8       ]
DNS 2                                   [        8.8.4.4       ]
```

Using the SafeMode Web Interface

In addition to SafeMode in the NSv management console, there is also a SafeMode web interface that provides image upgrade and log download functions. You can also lock or unlock the NSv management console from the SafeMode web interface.

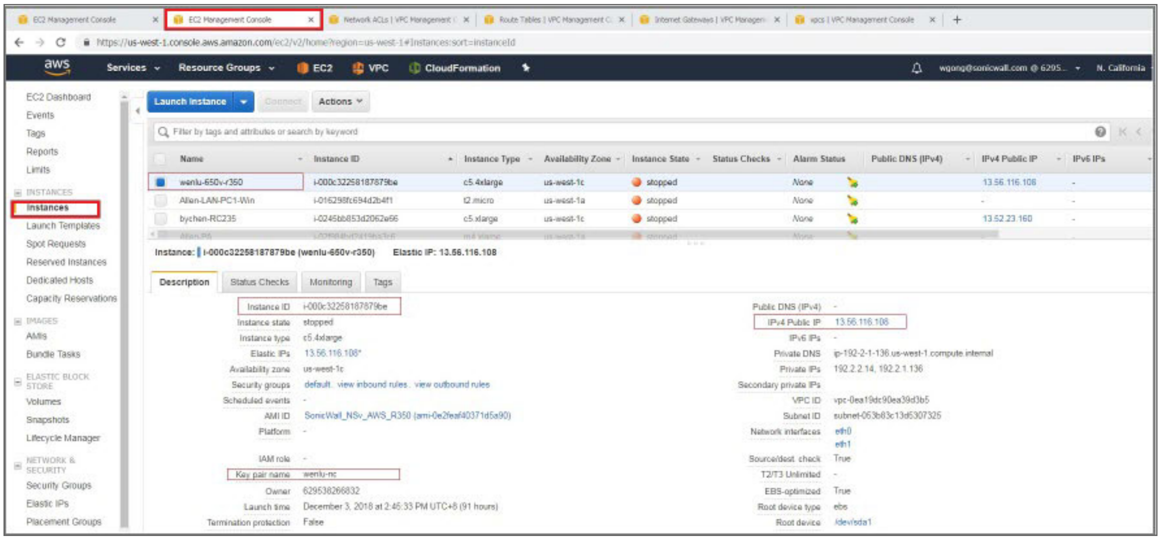
Topics:

- Accessing the SafeMode Web Interface
- Entering/Exiting SafeMode
- Locking and Unlocking the Management Console
- Downloading the SafeMode Logs
- Uploading a New Image in SafeMode

Accessing the SafeMode Web Interface

To access the SafeMode web interface:

1. Navigate to the **AWS E2C Management Console** page and view the **Instances** page for your NSv.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
wenlu-650v-r350	i-000c32258187879be	c5.4xlarge	us-west-1c	stopped		None		13.56.116.108	-
Allen-LAN-PC1-Win	i-016298fc694d2b4f1	t2.micro	us-west-1a	stopped		None		-	-
bychen-RC235	i-0245bb853d2062e66	c5.xlarge	us-west-1c	stopped		None		13.52.23.160	-

Instance: i-000c32258187879be (wenlu-650v-r350)   Elastic IP: 13.56.116.108

Instance ID	i-000c32258187879be
Instance state	stopped
Instance type	c5.4xlarge
Elastic IPs	13.56.116.108*
Availability zone	us-west-1c
Security groups	default. view inbound rules. view outbound rules
Scheduled events	-
AMI ID	SonicWall_NSv_AWS_R350 (ami-0e2feaf40371d5a90)
Platform	-
IAM role	-
Key pair name	wenlu-nc
Owner	629538266832
Launch time	December 3, 2018 at 2:46:33 PM UTC+8 (91 hours)
Termination protection	False

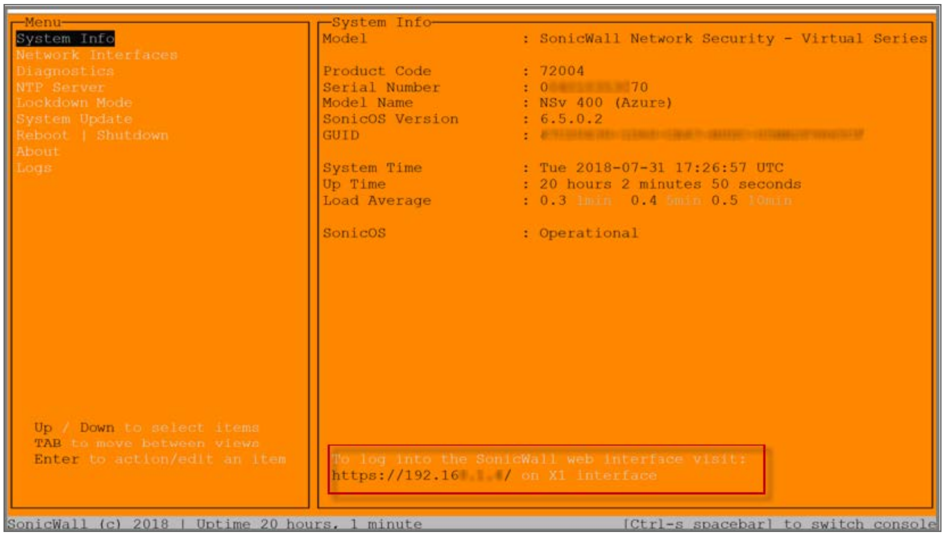
Public DNS (IPv4)	-
IPv4 Public IP	13.56.116.108
IPv6 IPs	-
Private DNS	ip-192-2-1-136.us-west-1.compute.internal
Private IPs	192.2.2.14, 192.2.1.136
Secondary private IPs	
VPC ID	vpc-0ea19dc90ea39d3b5
Subnet ID	subnet-053b83c13d5307325
Network interfaces	eth0 eth1
Source/dest. check	True
T2/T3 Unlimited	-
EBS-optimized	True
Root device type	ebs
Root device	/dev/sda1

2. In the **Instances** page, locate the public IP address assigned to the NSv and the Instance ID for your NSv.

   You can access the SafeMode web interface at the public IP address of the NSv, and you must authenticate to gain access.

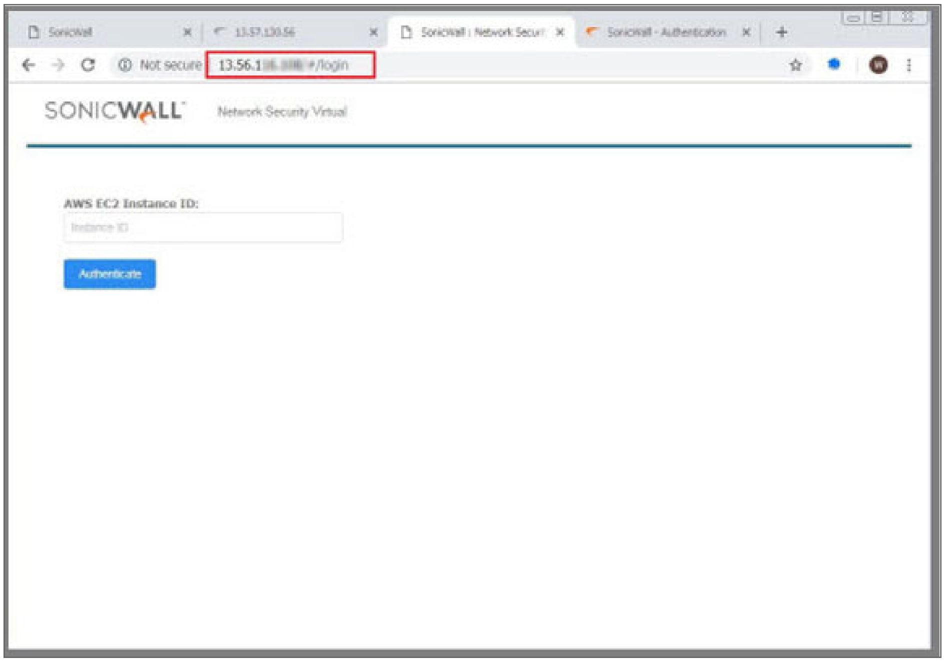
   ⓘ | **NOTE:** In SafeMode, the web management interface is only available by way of **http** (not https).

   The web interface address is also given on the management console screen as shown in the following image.



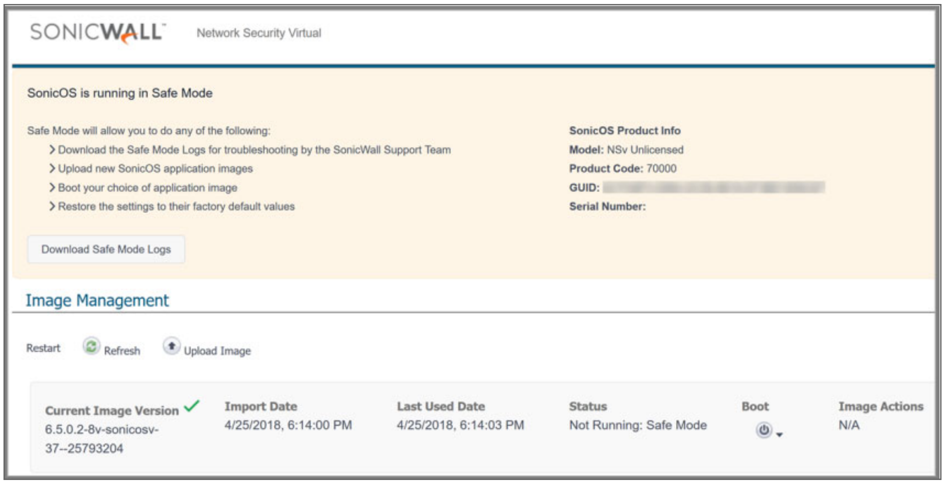
```
-Menu-                          -System Info-
System Info                     Model            : SonicWall Network Security - Virtual Series
Network Interfaces
Diagnostics                     Product Code     : 72004
NTP Server                      Serial Number    : 0[redacted]70
Lockdown Mode                   Model Name       : NSv 400 (Azure)
System Update                   SonicOS Version  : 6.5.0.2
Reboot | Shutdown               GUID             : [redacted]
About
Logs                            System Time      : Tue 2018-07-31 17:26:57 UTC
                                Up Time          : 20 hours 2 minutes 50 seconds
                                Load Average     : 0.3 1min  0.4 5min  0.5 10min

                                SonicOS          : Operational




  Up / Down to select items
  TAB to move between views
  Enter to action/edit an item  To log into the SonicWall web interface visit:
                                https://192.16[redacted]/ on X1 interface

SonicWall (c) 2018 | Uptime 20 hours, 1 minute            [Ctrl-s spacebar] to switch console
```

3. Go into the management console and boot into SafeMode. See **Entering SafeMode** under Using SafeMode on the NSv.
4. In a web browser, navigate to `http://<NSv public IP address>`, using the applicable IP address. The SafeMode authentication screen displays.



AWS EC2 Instance ID:

5. In the **AWS EC2 Instance ID** field, enter the Instance ID for the NSv.
6. Click **Authenticate**. The SafeMode web interface displays.



SonicOS is running in Safe Mode

Safe Mode will allow you to do any of the following:

- Download the Safe Mode Logs for troubleshooting by the SonicWall Support Team
- Upload new SonicOS application images
- Boot your choice of application image
- Restore the settings to their factory default values

SonicOS Product Info
Model: NSv Unlicensed
Product Code: 70000
GUID: [redacted]
Serial Number:

Image Management

Current Image Version ✓	Import Date	Last Used Date	Status	Boot	Image Actions
6.5.0.2-8v-sonicosv-37--25793204	4/25/2018, 6:14:00 PM	4/25/2018, 6:14:03 PM	Not Running: Safe Mode	⏻ ▾	N/A

Entering/Exiting SafeMode

Enter SafeMode as described in Accessing the SafeMode Web Interface.

Exit by either uploading a new SonicOS images or by going to the management console and rebooting into normal mode (see Enabling SafeMode and Disabling SafeMode).

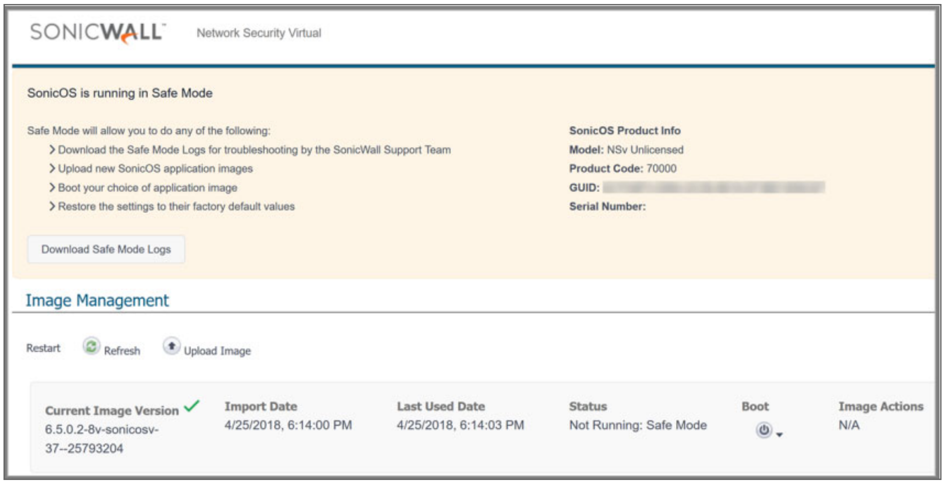
Downloading the SafeMode Logs

You can download logs of SafeMode activity.

ⓘ | **NOTE:** In SafeMode, the web management interface is only available by way of**http** (not **https**).

To download logs from SafeMode:

1. Access the web interface in SafeMode as described. The SafeMode web management interface displays:



SonicOS is running in Safe Mode

Safe Mode will allow you to do any of the following:

- Download the Safe Mode Logs for troubleshooting by the SonicWall Support Team
- Upload new SonicOS application images
- Boot your choice of application image
- Restore the settings to their factory default values

SonicOS Product Info
Model: NSv Unlicensed
Product Code: 70000
GUID: [redacted]
Serial Number:

Current Image Version ✓	Import Date	Last Used Date	Status	Boot	Image Actions
6.5.0.2-8v-sonicosv-37--25793204	4/25/2018, 6:14:00 PM	4/25/2018, 6:14:03 PM	Not Running: Safe Mode	⏻	N/A

2. Click **Download Safe Mode Logs**. A compressed file is downloaded that contains a number of files, including a `console_logs` file that contains detailed logging information.

Uploading a New Image in SafeMode

SWI files are used to upgrade SonicOS. You can download the latest SWI image file from MySonicWall.

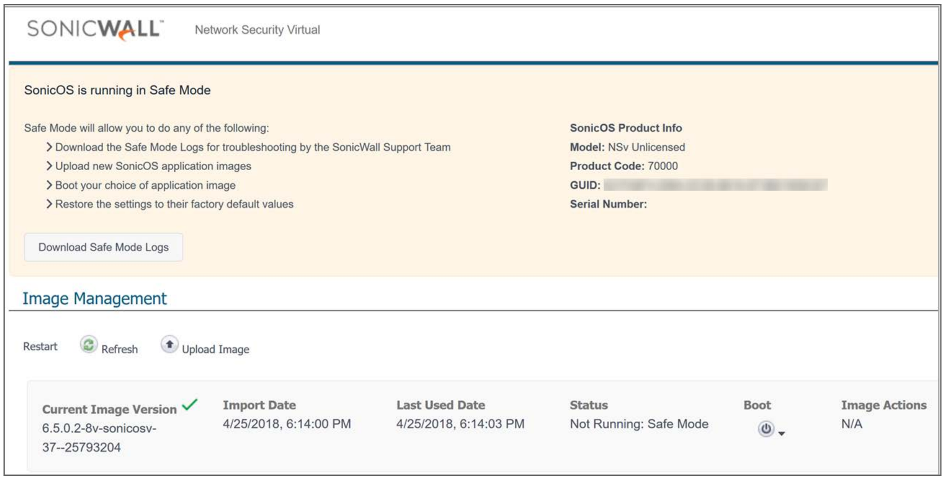
For additional information on uploading a new image, refer to: https://www.sonicwall.com/support/knowledge-base/?sol_id=180404172741874

In SafeMode, you can upload a new SonicOS SWI image and apply it to the NSv virtual machine. The SafeMode web management interface is used to perform an upgrade, rather than SafeMode in the NSv management console. When viewing the NSv management console in SafeMode, the URL for the SafeMode web interface is displayed at the bottom of the screen.

ⓘ | **NOTE:** In SafeMode, the web management interface is only available by way of **http** (not **https**).

To install a new SonicOS from SafeMode:

1. In the SafeMode web interface, click **Upload Image** to select an SWI file and then click **Upload** to upload the image to the virtual machine. A progress bar provides feedback on the file upload progress. After the upload completes, the image is available in the **Image Management** list in the SafeMode web interface.



SONICWALL Network Security Virtual

SonicOS is running in Safe Mode

Safe Mode will allow you to do any of the following:

- Download the Safe Mode Logs for troubleshooting by the SonicWall Support Team
- Upload new SonicOS application images
- Boot your choice of application image
- Restore the settings to their factory default values

SonicOS Product Info
Model: NSv Unlicensed
Product Code: 70000
GUID: [redacted]
Serial Number:

Download Safe Mode Logs

Image Management

Restart Refresh Upload Image

Current Image Version ✓	Import Date	Last Used Date	Status	Boot	Image Actions
6.5.0.2-8v-sonicosv-37--25793204	4/25/2018, 6:14:00 PM	4/25/2018, 6:14:03 PM	Not Running: Safe Mode	⏻ ▾	N/A

2. In the row with the uploaded image file, click **Boot** and select one of the following:
   - **Boot Uploaded Image with Current Configuration**
   - **Boot Uploaded Image with Factory Default Configuration**

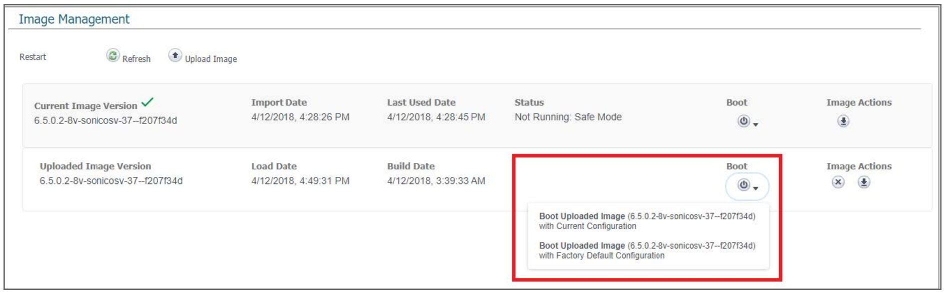


Image Management

Restart Refresh Upload Image

Current Image Version ✓	Import Date	Last Used Date	Status	Boot	Image Actions
6.5.0.2-8v-sonicosv-37--f207f34d	4/12/2018, 4:28:26 PM	4/12/2018, 4:28:45 PM	Not Running: Safe Mode	⏻ ▾	⬇

Uploaded Image Version	Load Date	Build Date		Boot	Image Actions
6.5.0.2-8v-sonicosv-37--f207f34d	4/12/2018, 4:49:31 PM	4/12/2018, 3:39:33 AM		⏻ ▾	✕ ⬇

Boot Uploaded Image (6.5.0.2-8v-sonicosv-37--f207f34d) with Current Configuration

Boot Uploaded Image (6.5.0.2-8v-sonicosv-37--f207f34d) with Factory Default Configuration

The NSv virtual machine reboots with the new image.

6

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

ⓘ | **NOTE:** A NOTE icon indicates supporting information.

ⓘ | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

ⓘ | **TIP:** A TIP icon indicates helpful information.

△ | **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**

⚠ | **WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.**

SonicOS NSv Getting Started Guide for the KVM Series
Updated - November 2022
Software Version - 7
232-005385-00 Rev C

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