



SonicOS and SonicOSX 7

NSv Getting Started Guide

for KVM

SONICWALL®

Contents

Introducing the NSv Series	4
Feature Support Information	4
Node Counts Per Platform	7
Installation File / Supported Platforms	8
Hardware Compatibility	8
KVM/QEMU	8
Hardware-Assisted Full Virtualization	8
Paravirtualization	9
Product Matrix and Requirements	9
Backup and Recovery Information	10
Importing Firewall Configurations	10
High Availability Configurations	10
Upgrading from SonicOS 6.5	11
Upgrading to a Higher Capacity NSv Model	12
Creating a MySonicWall Account	12
 Installing SonicOS/X on the NSv Series	 15
Preparing the Linux Server System	15
Obtaining the NSv Image	15
Installing the NSv Series on Ubuntu-KVM/QEMU	16
Adding VLAN Parameters to the Network Card	22
Locating the img File	23
Using the CLI to Configure User Settings	24
Next Steps and Related Topics	24
Installing the NSv Series on CentOS-KVM/QEMU	25
Creating NSv with Virt-install	28
Editing a Virtual Machine Configuration File	29
Adding VLAN Parameters to the Network Card	29
Next Steps and Related Topics	31
 Licensing and Registering Your NSv	 32
Registering the NSv Virtual Machine with SonicOS/X	32
 SonicOS/X Management	 35
Managing SonicOS/X on the NSv Series	35
Using System Diagnostics	35

Using the Virtual Console and SafeMode	37
Connecting to the Management Console with SSH	37
Navigating the NSv Management Console	40
System Info	42
Management Network or Network Interfaces	43
Test Management Network	44
Diagnostics	46
NTP Server	47
Lockdown Mode	47
System Update	48
Reboot Shutdown	48
About	49
Logs	49
Using SafeMode on the NSv	50
How Management Console Differs in SafeMode	50
Entering SafeMode	50
Enabling SafeMode	51
Disabling SafeMode	52
Configuring the Management Network in SafeMode	52
Using the SafeMode Web Interface	56
Accessing the SafeMode Web Interface	57
Entering/Exiting SafeMode	58
Downloading the SafeMode Logs	59
Uploading a New Image in SafeMode	59
SonicWall Support	61
About This Document	62

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/X 7 running on the NSv offers the same feature functionality and security features of a physical appliance, with comparable performance. SonicOS/X Virtual is a fully featured 64-bit SonicOS/X 7 powered by SonicCore.

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/X 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/X 7 firmware.

For more information about supported features, go to the [Technical Documentation Portal](#).

The **Feature Support List** of NSv table shows the key SonicOS/X 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	
		AntiVirus Signature Object
		AntiSpyware Signature Object
	Rule Management	
		Cloning
		Shadow rule analysis
		In-cell editing
		Group editing
	Export of Rules	

Functional Category	Feature Area	Feature
		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	
	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	

Functional Category	Feature Area	Feature
	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/X 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
NSv 270	unlimited
NSv 470	unlimited
NSv 870	unlimited

Installation File / Supported Platforms

Release Version	Supported Linux / Kernel / KVM / VMM Versions
SonicOS/X 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.el7.x86_64
	• KVM version: 1.5.3
	• Virtual machine manager: 1.5.1

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/X) 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 subsystems, 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 270	NSv 470	NSv 870
Maximum Cores ¹	2	4	8
Minimum Total Cores	2	4	8
Minimum Management Cores	1	1	1
Data Plane Cores (fixed)	1	3	7
Network Interfaces	8	8	8
Supported IP/Nodes	Unlimited	Unlimited	Unlimited
Minimum Memory Required ²	8G	10G	12G
Minimum Hard Disk/Storage	60G	60G	60G

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 270	10G	8G
NSv 470	14G	10G
NSv 870	18G	12G

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

²Memory 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/X does not boot up, you can go into SafeMode and download the log files, upload a new SonicOS/X image, or take other actions. For more information about SafeMode, see [Using SafeMode on the NSv](#).
- If SonicOS/X 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/X 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/X 7 NSv installations. Note that there are console, API, and SonicOS/X web approaches to completing these configurations.

① **NOTE:** Upgrading to SonicOS/X 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 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 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.
① **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. Log into the SonicOS 7 NSv and import the configuration settings.
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/X 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](#).

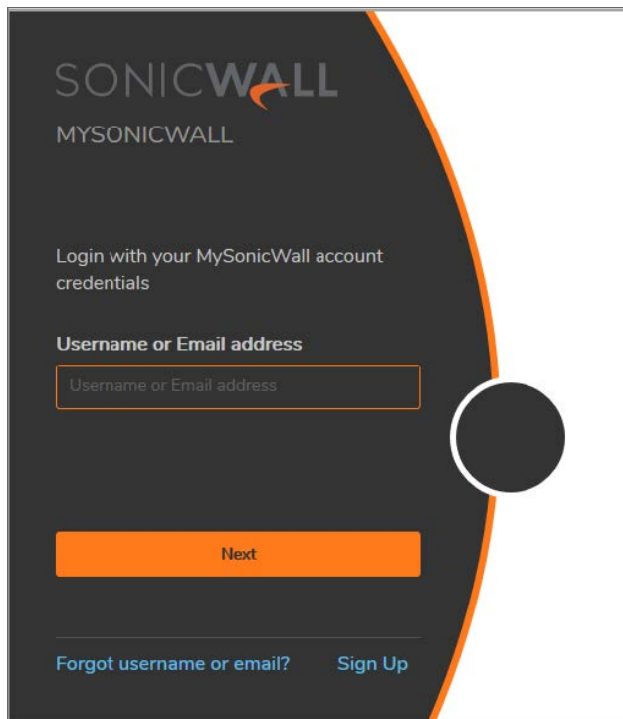
Creating a MySonicWall Account

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/X 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.



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.

Installing SonicOS/X 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:

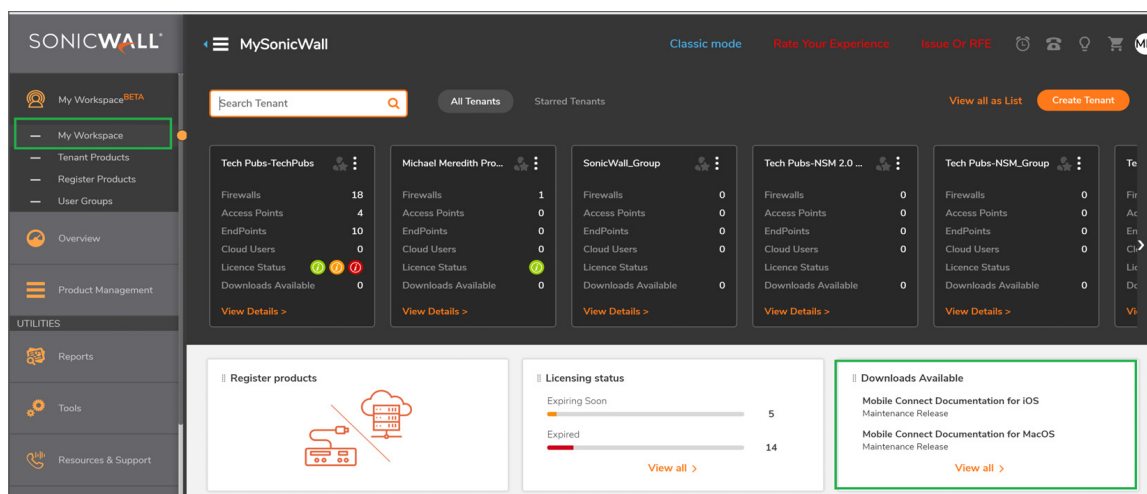
- Install Ubuntu or CentOS on the server. For version details refer to [Installation File / Supported Platforms](#).
- Install KVM and QEMU on server.
- Connect the Linux Server system to an external switch.

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**.



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 is installed. Refer to [Registering the NSv Appliance from SonicOS/X](#).

Installing the NSv Series on Ubuntu-KVM/QEMU

Topics:

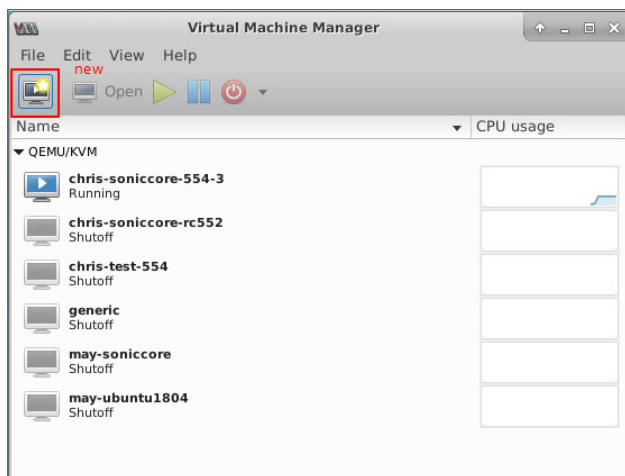
- [Adding VLAN Parameters to the Network Card](#)
- [Locating the img File](#)
- [Using the CLI to Configure User Settings](#)
- [Next Steps and Related Topics](#)

To install an NSv on Ubuntu-KVM/QEMU:

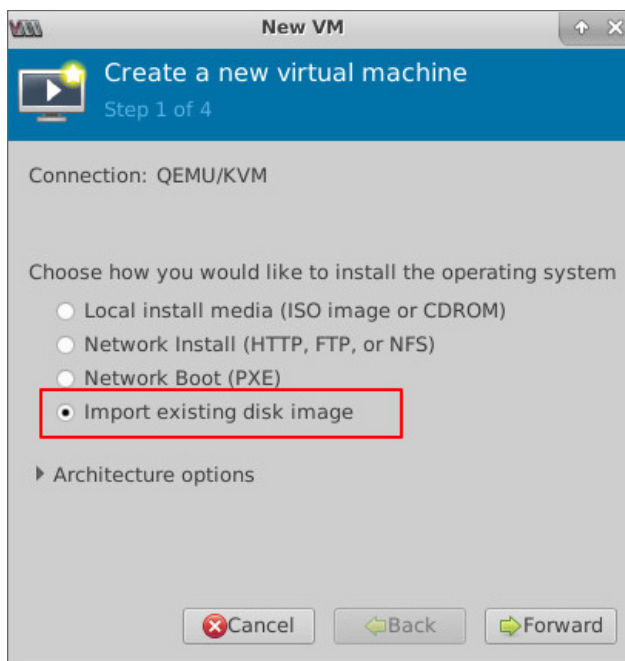
1. Download the NSv virtual machine **img** file to a local folder in the Linux Server system.
2. Copy image file (for example: "SonicWall_NSv_For_QEMU_VM.img") into the directory `/var/lib/libvirt/images/`.
3. Bring up the Virtual Machine Manager (VMM):



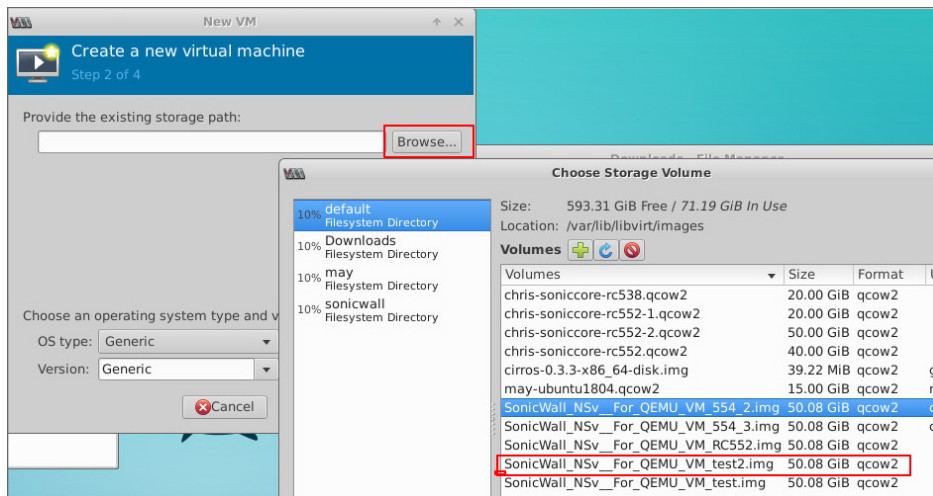
4. Create a virtual machine in the Virtual Machine Manager to receive the image file:



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



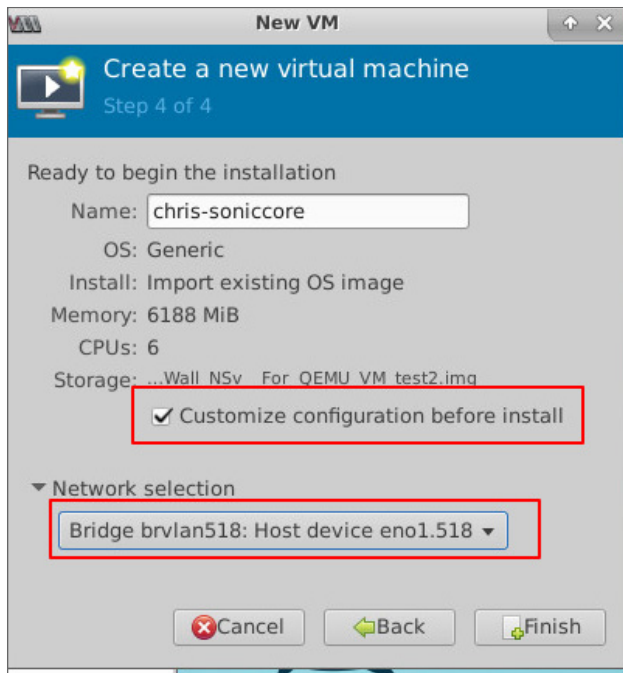
6. Choose storage volume:



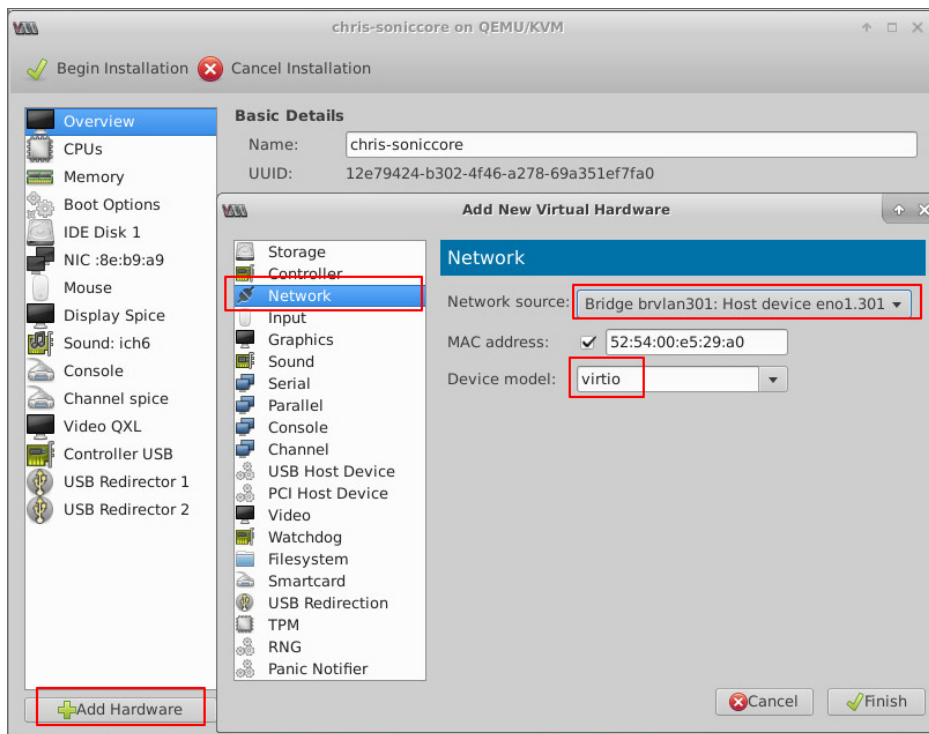
7. Configure CPU/Memory/Name/Network (default only one network interface attached), then click Finish to create. For hardware resources, refer to [Product Matrix and Requirements](#).



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

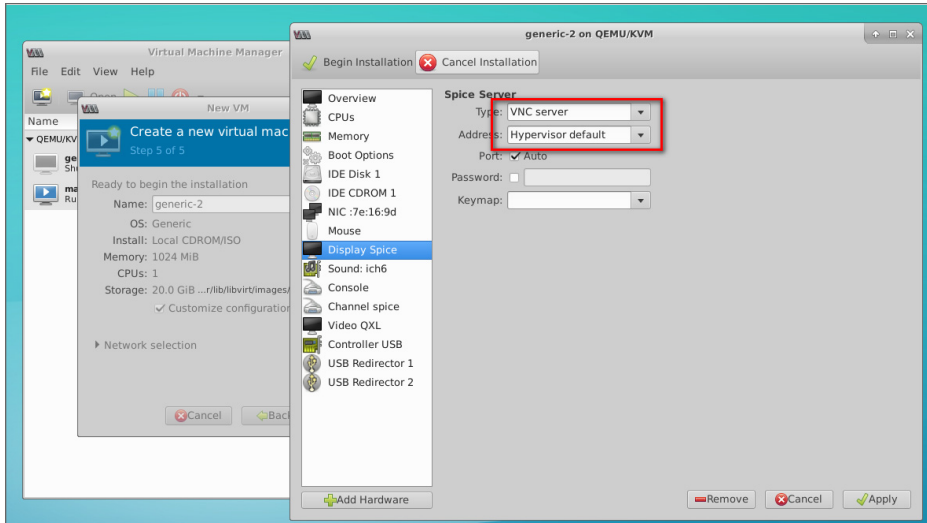


9. Another interface is required to serve as WAN port, or X1 of the virtual machine. Here we choose the interface 301:



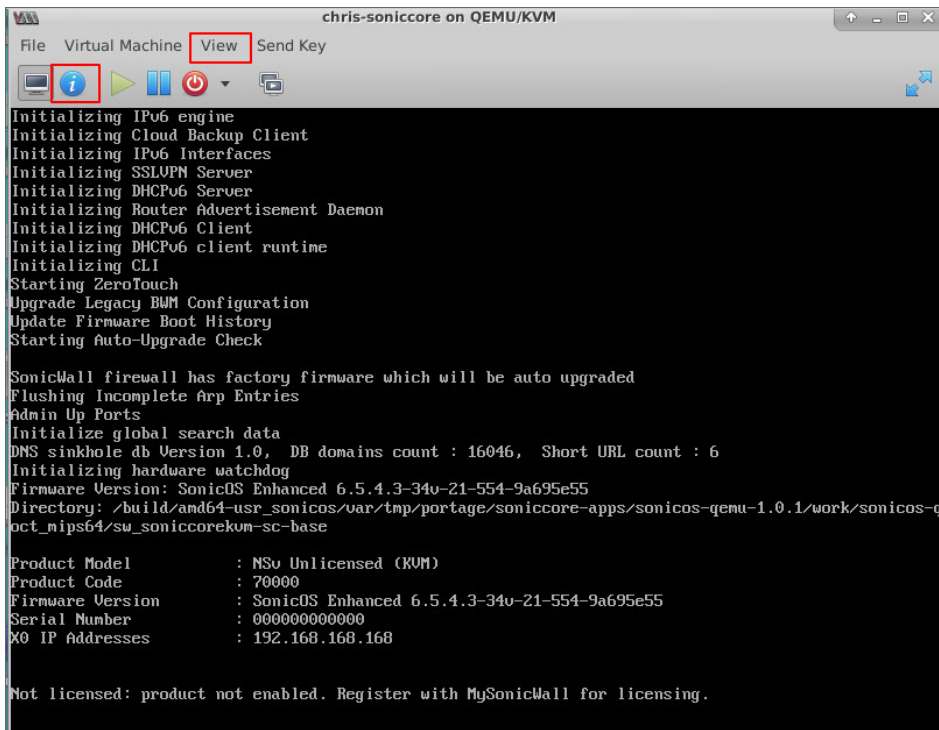
① **NOTE:** Both device models should choose **virtio**. By default, the first network card is X0, and the second one is X1. By choosing virtio, the VirtIO API is enabled. For more on VirtIO, see [Paravirtualization](#).

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.



① **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:



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
```

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

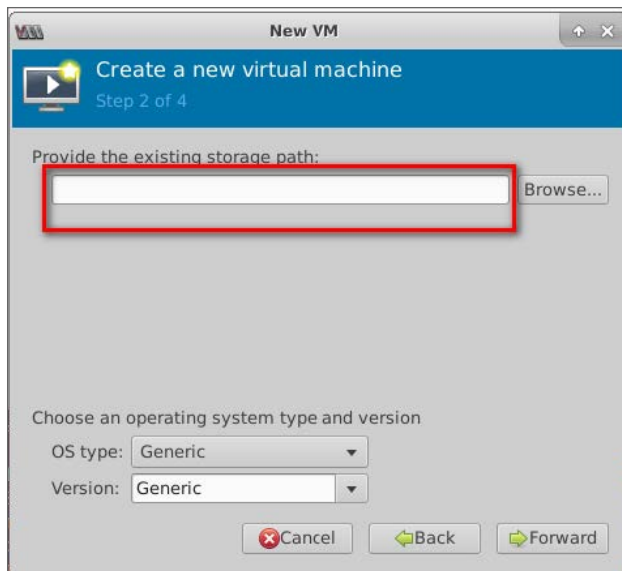
gateway 10.103.64.1

dns_nameserver 10.196.2020.200


systemctl restart network
```

Locating the *img* File

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



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/X](#)
- [Managing SonicOS/X on the NSv Series](#)

- [Using System Diagnostics](#)
- [Using the Virtual Console and SafeMode](#)

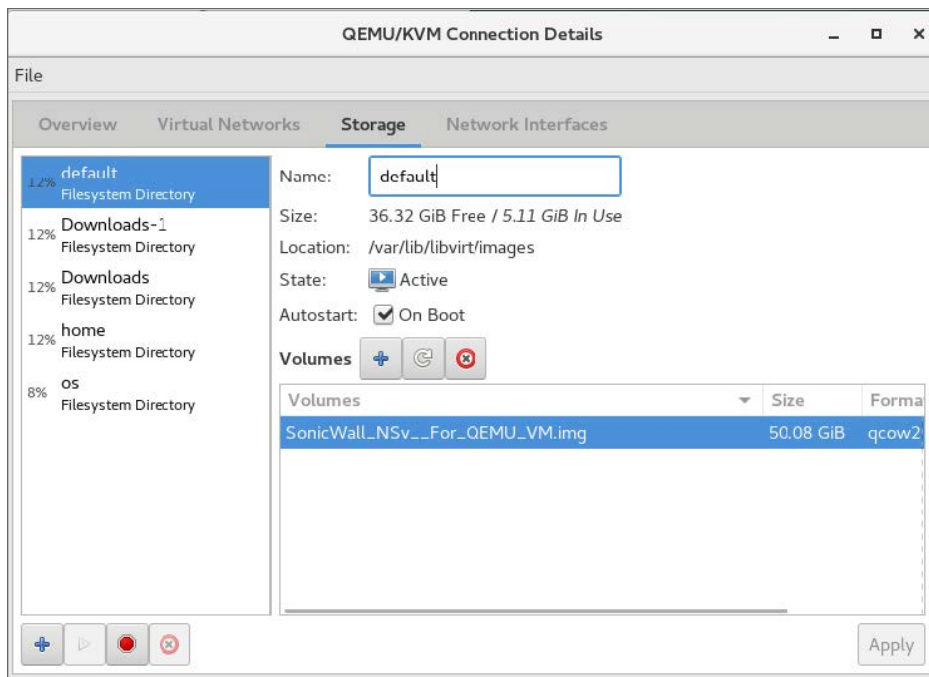
Installing the NSv Series on CentOS-KVM/QEMU

Topics:

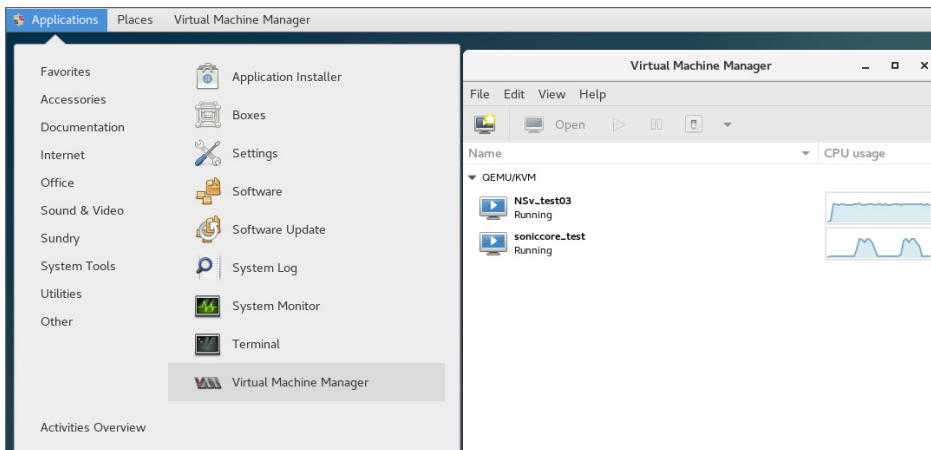
- [Creating NSv with Virt-install](#)
- [Editing a VM Config File](#)
- [Adding VLAN Parameters to the Network Card](#)
- [Next Steps and Related Topics](#)

To install an NSv on CentOS-KVM/QEMU:

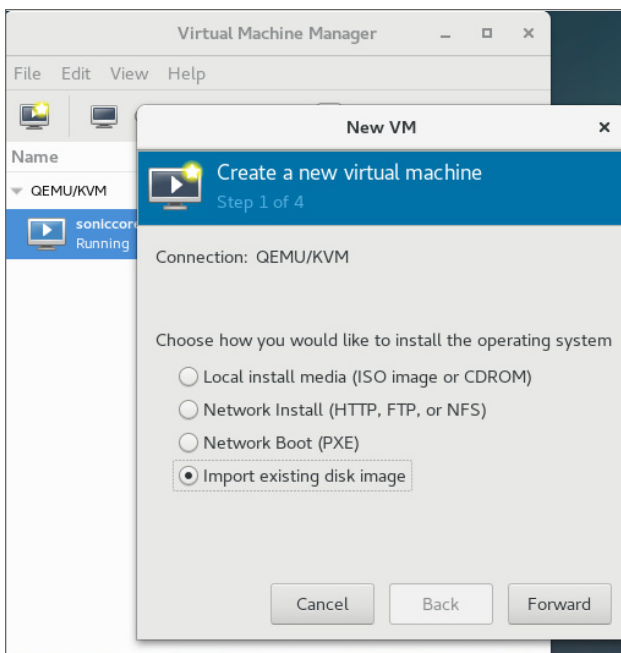
1. Download the NSv virtual machine **img** file to a local folder in the Linux Server system.
2. Copy image file (for example: "SonicWall_NSv_For_QEMU_VM.img") into the directory /var/lib/libvirt/images/.



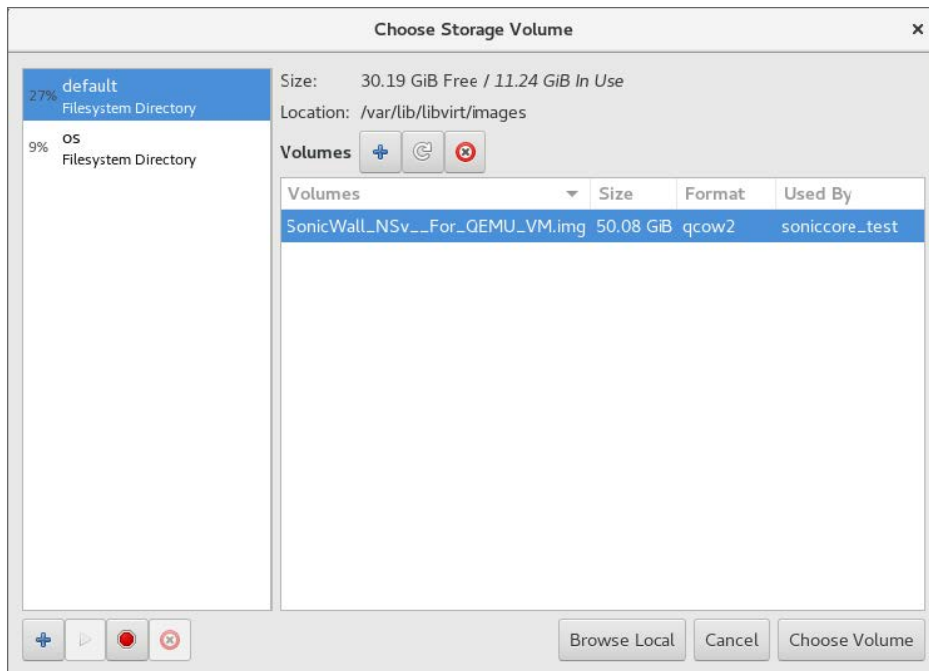
3. Bring up the Virtual Machine Manager (VMM):



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

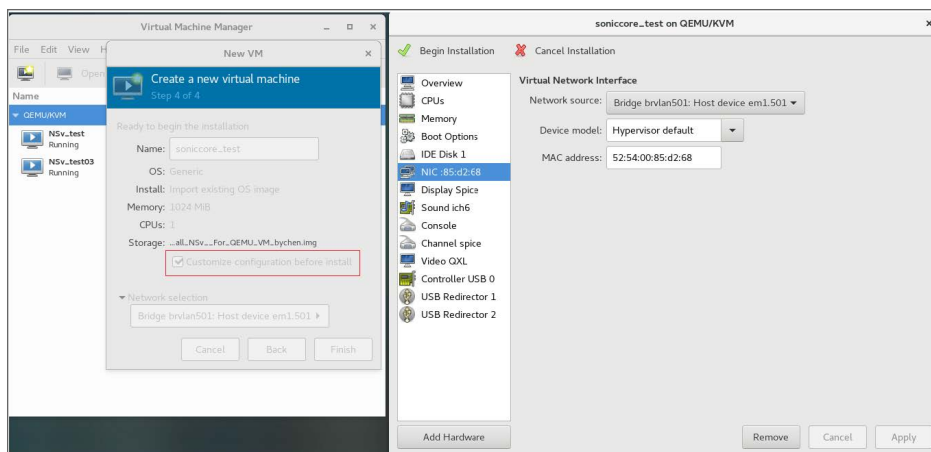


5. Choose the storage volume:

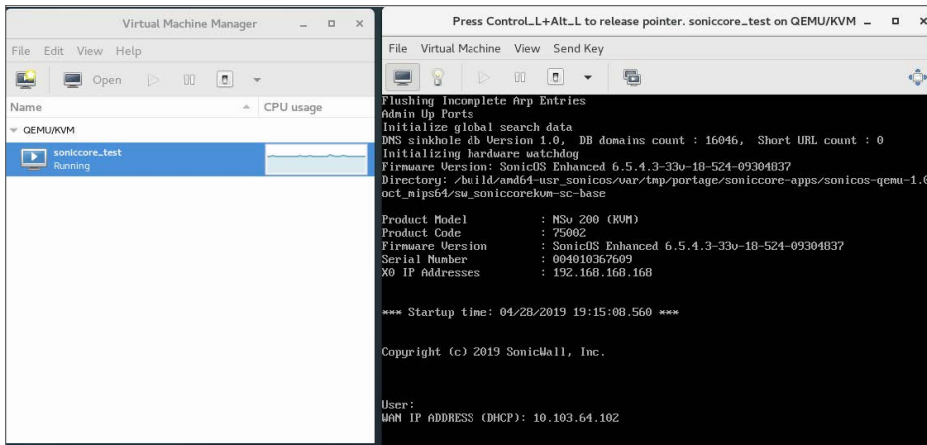


6. Configure CPU/Memory/Name/Network (default only one network interface attached), then finish to create.
 - a. The default interface corresponds to X0 of the virtual machine, here we choose **a private VLAN 518**.
 - b. We need to add another network interface as WAN port, that is X1 of the virtual machine, here we choose the **interface 301**.

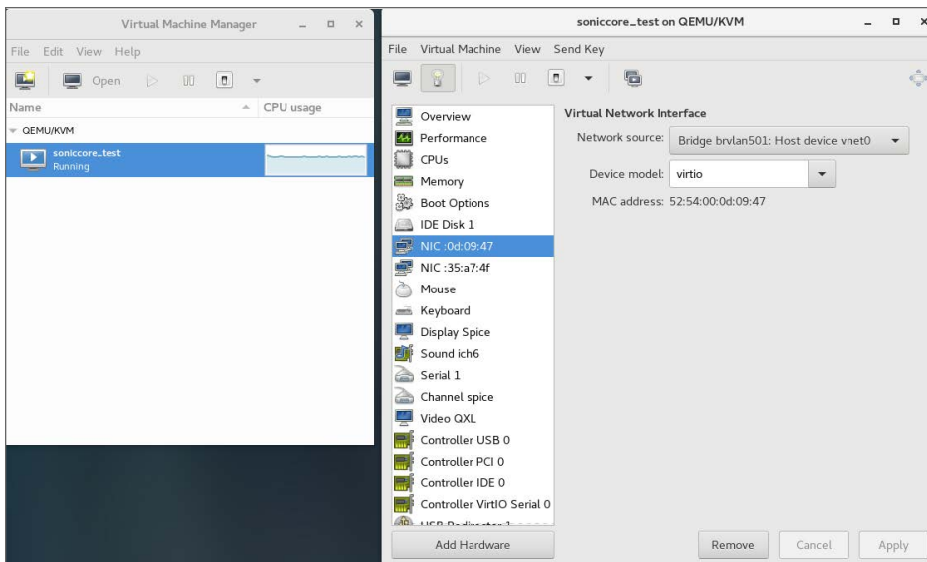
① **NOTE:** Both device models should choose **virtio**. By default, the first network card is X0, and the second one is X1.
 - c. Create a new virtual machine with Display set as VNC otherwise you might not be able to use keyboard with new virtual machine.



- 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.



- Add interfaces and select virtio type:



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 domaininfo <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/X](#)
- [Managing SonicOS/X on the NSv Series](#)
- [Using System Diagnostics](#)
- [Using the Virtual Console and SafeMode](#)

Licensing and Registering Your NSv

Topics:

- [Registering the NSv Appliance from SonicOS/X](#)

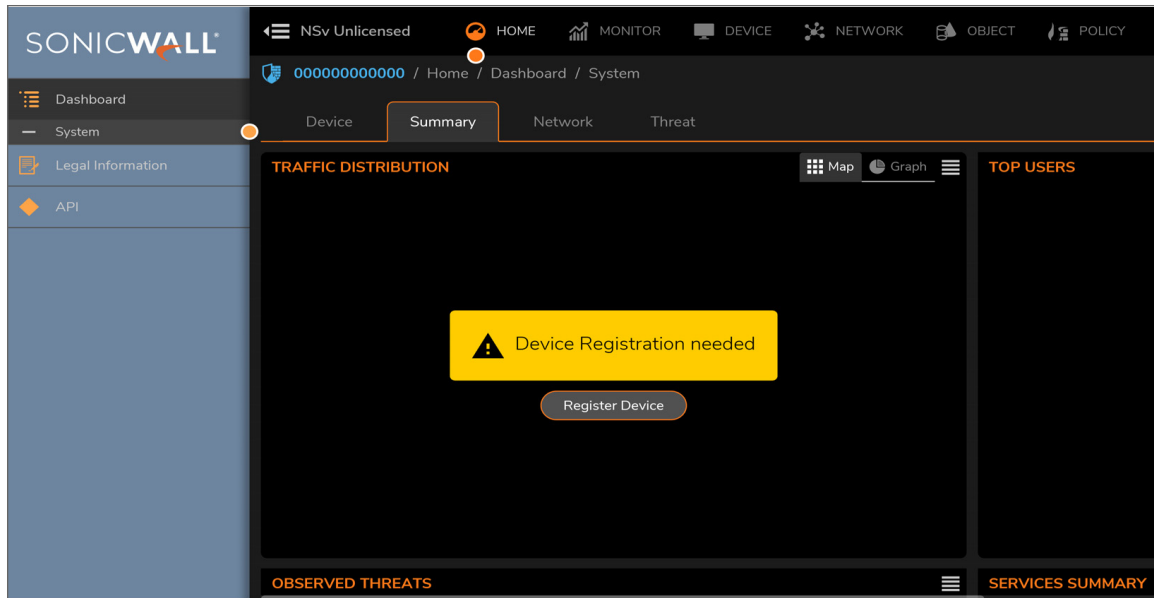
Registering the NSv Virtual Machine with SonicOS/X

After you have installed and configured the network settings for your NSv Series virtual machine, you can log into SonicOS/X 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.

① **NOTE:** System functionality is extremely limited when registration is not complete. See [Using 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**.



- 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

Register

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.

The screenshot displays the SonicOS/X 7 web interface. At the top, a navigation bar includes links for NSv Unlicensed, HOME, MONITOR, DEVICE, NETWORK, OBJECT, and POLICY. Below this, a breadcrumb trail shows '000000000000 / Device / Settings / Licenses'. The 'Settings' tab is active, showing two main sections: 'MANAGE SECURITY SERVICES ONLINE' and 'MANUAL UPGRADE'. The 'MANAGE SECURITY SERVICES ONLINE' section contains instructions on how to activate, upgrade, or renew services, followed by a 'Register' button. The 'MANUAL UPGRADE' section includes a large text area for 'Enter keyset', and three input fields for 'Serial Number', 'Auth Code', and 'Registration Code', each marked with a red asterisk. An 'Apply' button is located at the bottom right of the 'MANUAL UPGRADE' section.

Click **Apply** to complete the registration.

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

SonicOS/X Management

Topics:

- [Managing SonicOS/X on the NSv Series](#)
- [Using System Diagnostics](#)

Managing SonicOS/X 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/X 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/X 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/X 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.

The screenshot displays the SonicWall management interface. The left sidebar contains navigation options: Settings, High Availability, Users, AppFlow, Log, and Diagnostics. The main content area is titled '00401038B524 / Device / Diagnostics / Check Network Settings'. It shows the 'GENERAL NETWORK CONNECTION' section with a table of test results for IPv4. The table has columns: SERVER, IP ADDRESS, TEST RESULTS, NOTES, TIMESTAMP, and PROGRESS. The results show successful tests for the Default Gateway (X1) and DNS Servers 1 and 2. Below this, the 'SECURITY MANAGEMENT' section is also visible.

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)

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.

Using the Virtual Console and SafeMode

Topics:

- [Connecting to the Management Console with SSH](#)
- [Navigating the NSv Management Console](#)
- [Using SafeMode on the NSv](#)

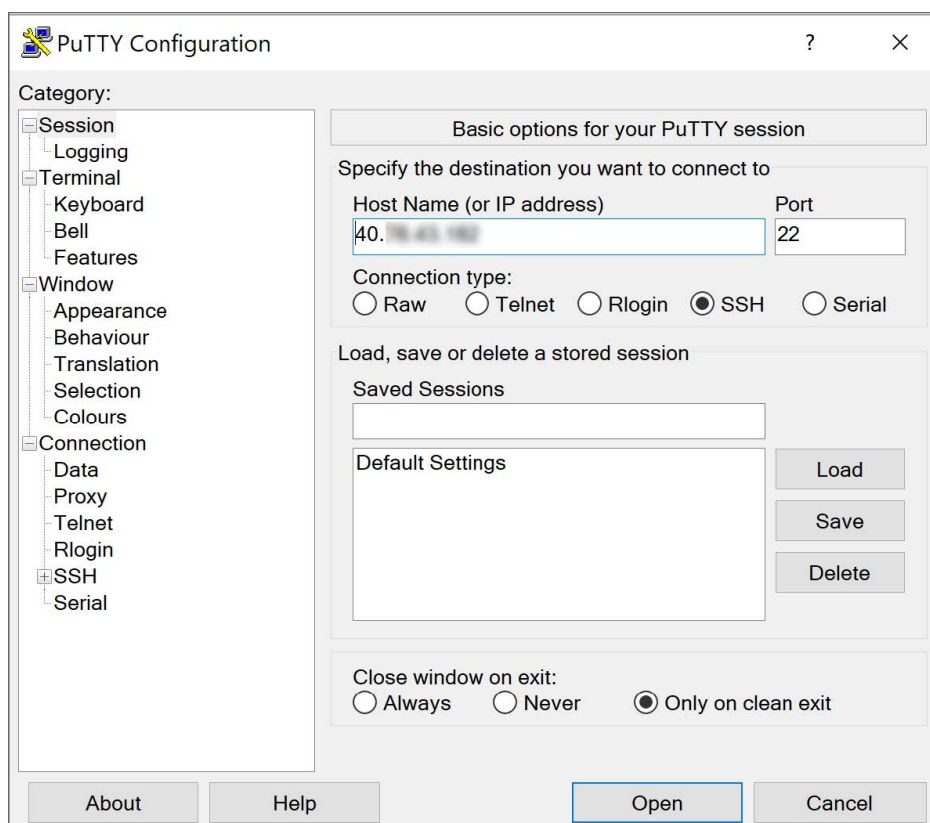
Connecting to the Management Console with SSH

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:

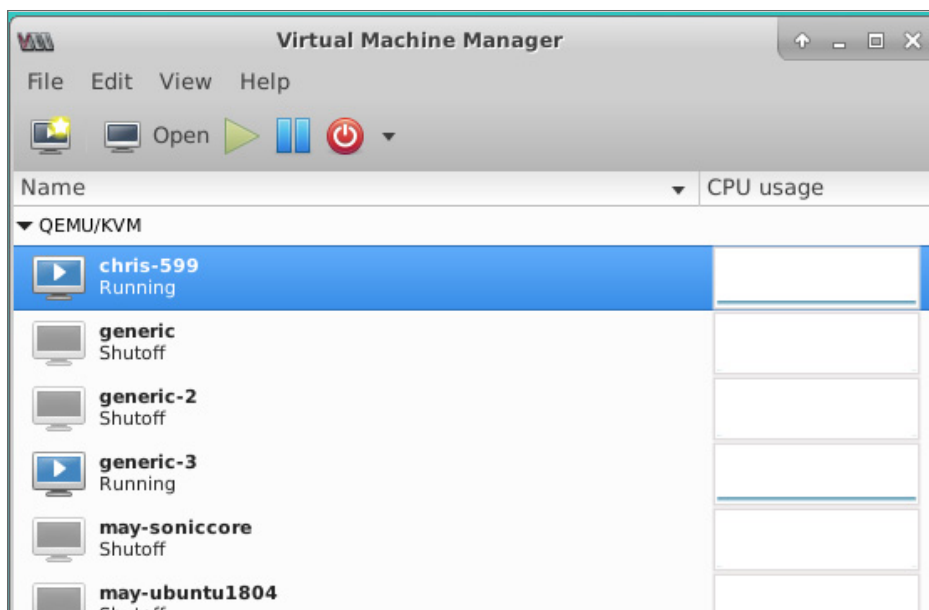
1. Launch PuTTY and type in the public IP address of the NSv/QEMU.



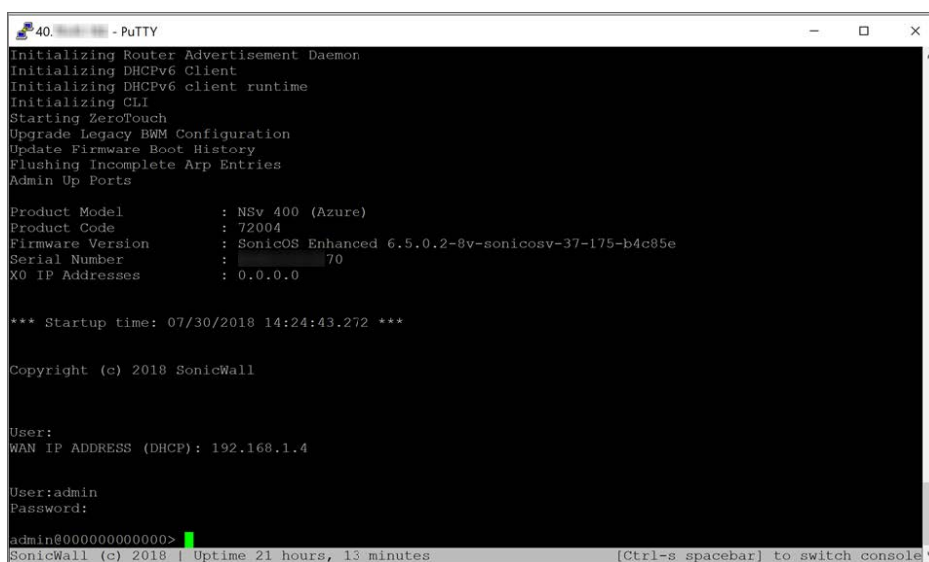
2. For **Port**, type in 22 if it is not already set.
NOTE: Changing the SSH port to anything other than 22 can prevent access to the SonicCore management console and the SonicOS/X CLI console.
3. For **Connection type**, **SSH** should already be selected by specifying port 22.
4. Click **Open** to open a console connection.
5. When you are prompted to log in at the **User** prompt, enter the SonicOS/X 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**.



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.

① | **NOTE:** Press **Ctrl+Alt** to regain control of your mouse.

After configuring an IP address and enabling management, you can log in to SonicOS/X 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/X, 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
Management Network
Test Management Network
Diagnostics
NTP Server
Lockdown Mode
System Update
Reboot | Shutdown
About
Logs

System Info
Model          : SonicWall Network Security - Virtual Series
Product Code   : 70000
Serial Number  :
Model Name     : NSv Unlicensed Beta
SonicOS Version : 6.5.0.0
GUID          : [REDACTED]

System Time    : Tue 2018-03-27 20:58:06 UTC
Up Time       : 41 minutes 35 seconds
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://192.168.1.1/

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:

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
Management Network
Test Management Network
Diagnostics
NTP Server
Lockdown Mode
System Update
Reboot | Shutdown
About
Logs

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

System Info
Model          : SonicWall Network Security - Virtual Series
Product Code   : 70000
Serial Number   :
Model Name     : NSu Unlicensed Beta
SonicOS Version : 6.5.0.0
GUID           : 00000000-0000-0000-0000-000000000000

System Time    : Tue 2018-03-27 20:58:06 UTC
Up Time        : 41 minutes 35 seconds
CPU Load       : 1.1 1min 1.1 5min 1.0 10min
SonicOS        : Operational

To log into the SonicWall web interface visit:
https://192.168.1.1/

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:

- ## Management Network or Network Interfaces

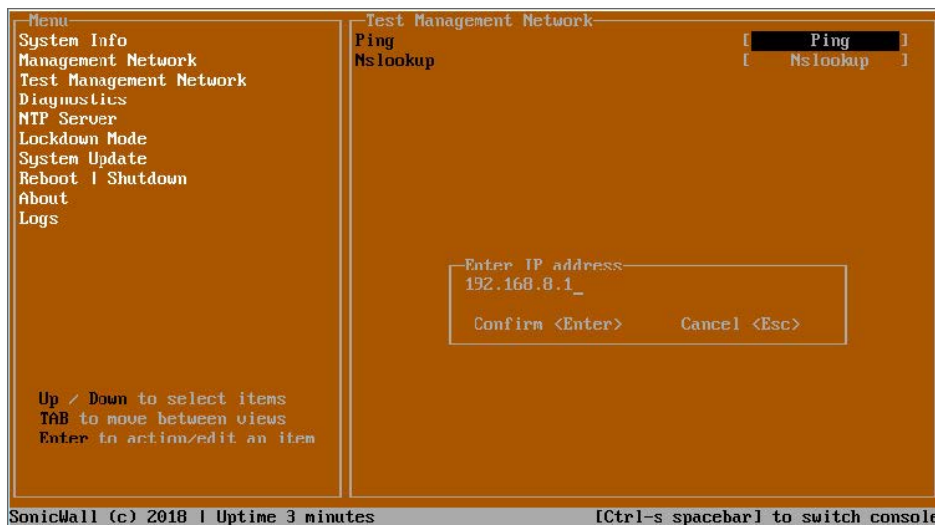
A screenshot of a PuTTY terminal window titled "40. [redacted] - PuTTY". The terminal displays a menu-driven interface for configuring a SonicWall device. On the left, a vertical menu lists options: Menu, System Info, Network Interfaces (highlighted), Diagnostics, VPN Server, Lockdown Mode, System Update, Reboot | Shutdown, About, and Logs. Below this menu are instructions: "Up / Down to select items", "TAB to move between views", and "Enter to action/edit an item". The main area shows the "Network Interfaces" configuration for "X1". It lists various network parameters: IPv4 Address (192.168.1.4), Netmask (255.255.255.0), Mac address (00:00:00:00:00:ld), IPv6 Address (fe80::20d:3aff:fe37:d01d), Gateway (192.168.1.1), DNS 1 (8.8.8.8), and DNS 2 (8.8.4.4). At the bottom right, there is a note: "To log into the SonicWall web interface visit: https://192.168.1.4/ on X1 interface". The footer of the terminal shows "SonicWall (c) 2018 | Uptime 22 hours, 3 minutes" and "[Ctrl-s spacebar] to switch console".

- **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.



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

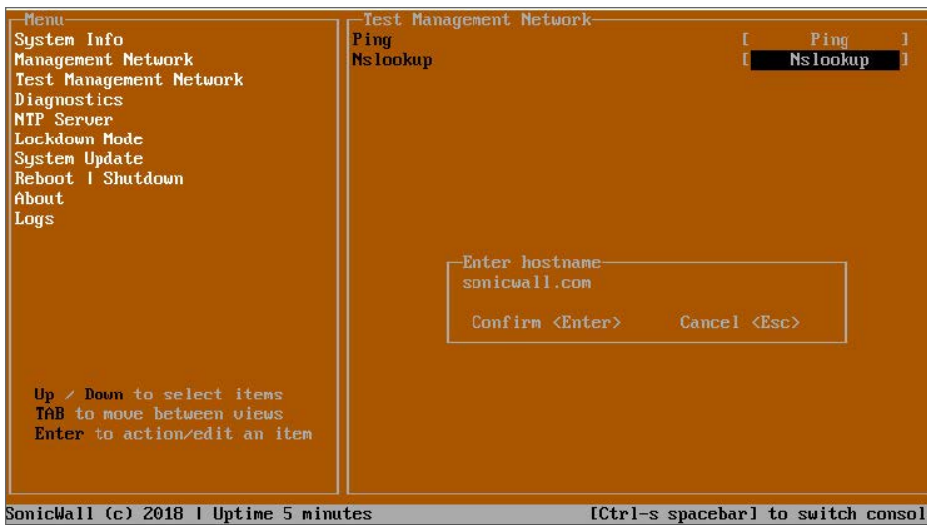
Scroll <Up Down Left Right>          Close <Esc>

```

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.



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

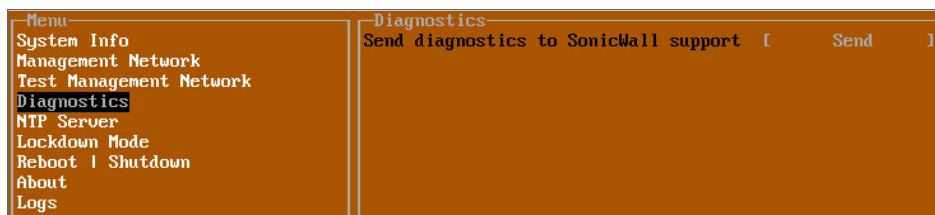
Non-authoritative answer:
Name: sonicwall.com
Address: 107.154.75.50

Scroll <Up Down Left Right>          Close <Esc>

```

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

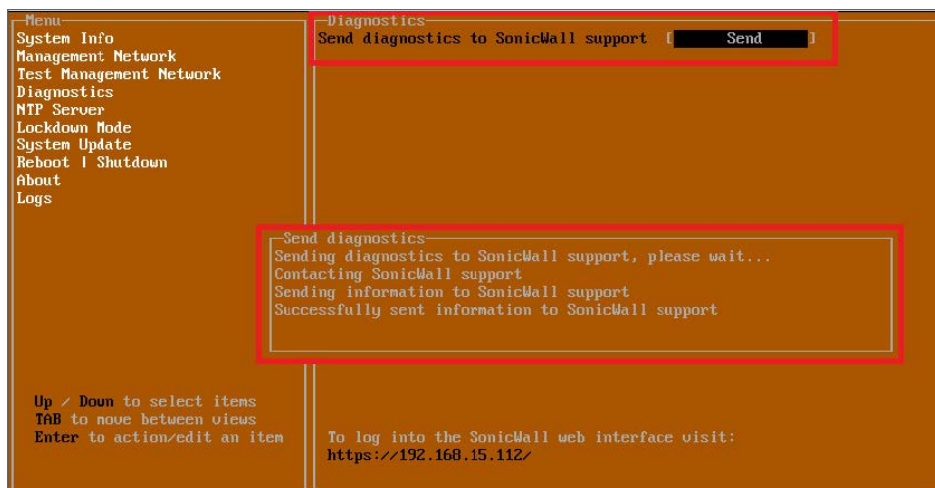
Diagnostics



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/X web management interface.

① | **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.



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

① | **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/X 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/X 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.

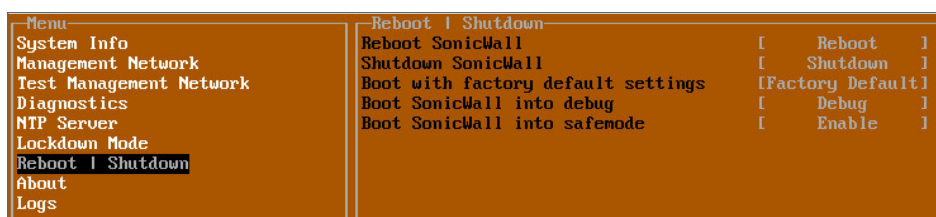
The management console is automatically enabled/disabled a few seconds after it has been enabled/disabled in the SonicOS/X web interface page.

System Update

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



Reboot | Shutdown

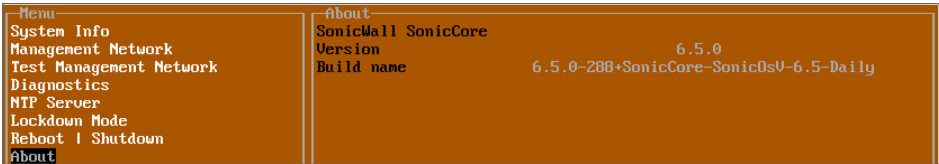


The **Reboot | Shutdown** screen provides functions for rebooting the NSv virtual machine, enabling debug mode, and enabling SafeMode. To perform an action, position the focus and then press **Enter** to select the desired action. Select **Yes** in the confirmation dialog, then press **Enter** again.

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](#).

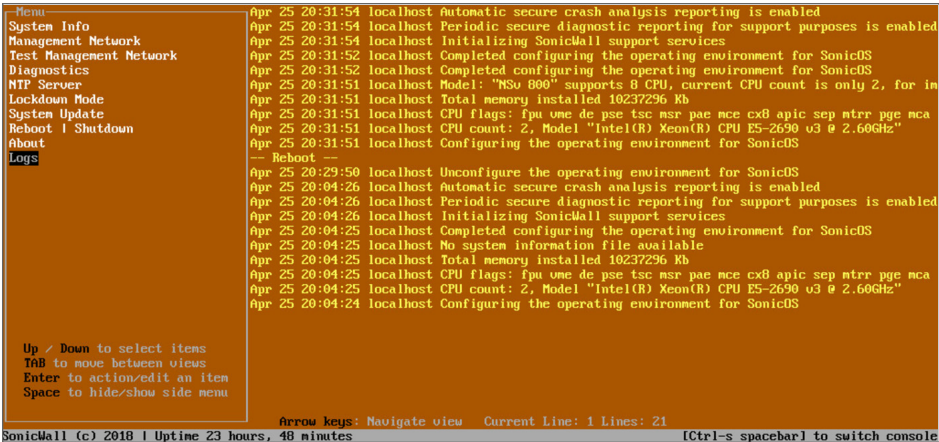
About



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

Logs

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



Using SafeMode on the NSv

The NSv virtual machine enters SafeMode when SonicOS/X 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:

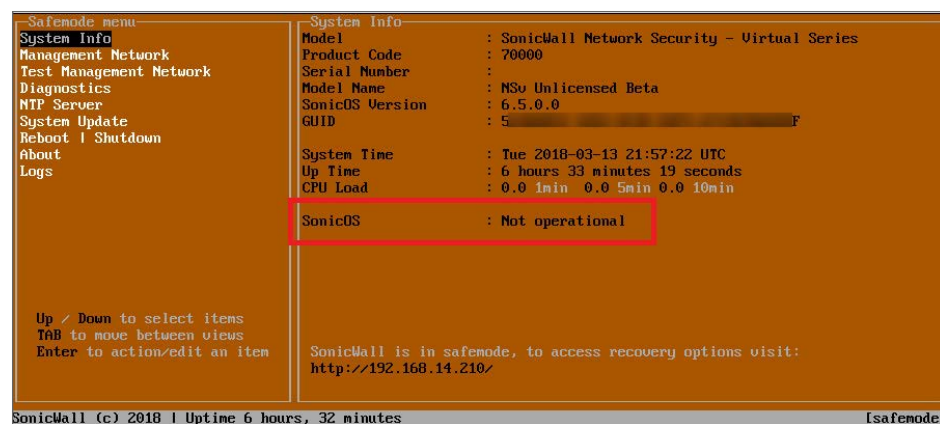
- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

① | **NOTE:** Changes made to interfaces in SafeMode are **not** persistent between reboots.

When the NSv is in SafeMode, the SonicOS/X 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.



- ① **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/X Version in SafeMode](#) for more information.

Topics:

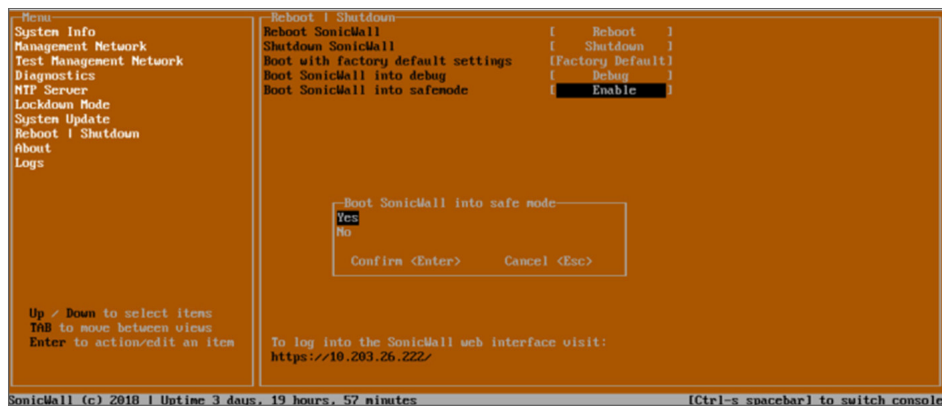
- [Enabling SafeMode](#)
- [Disabling SafeMode](#)
- [Configuring the Management Network in SafeMode](#)

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**.



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

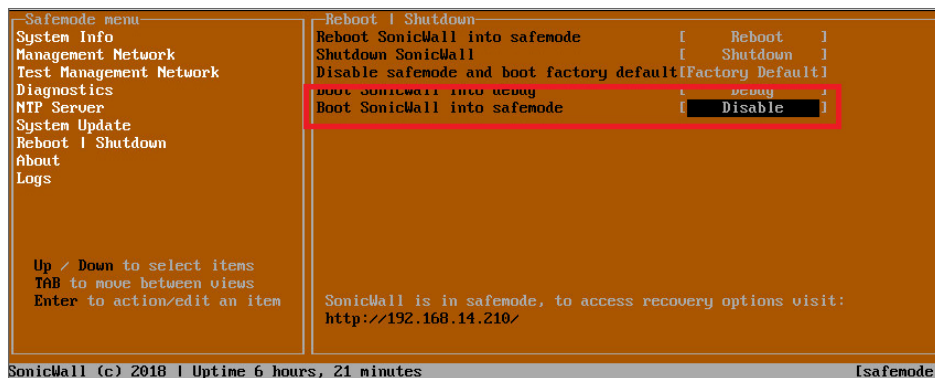
The NSv immediately reboots and comes back up in SafeMode.

- ① **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**.



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.

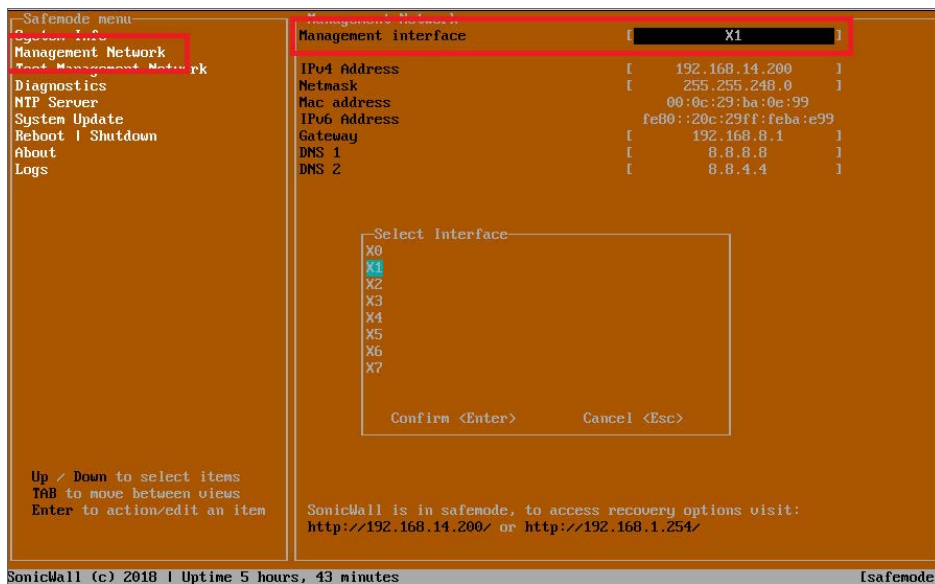
Changes made to interfaces in SafeMode are **not** persistent between reboots.

Topics:

- [Configuring Interface Settings](#)
- [Disabling an Interface](#)

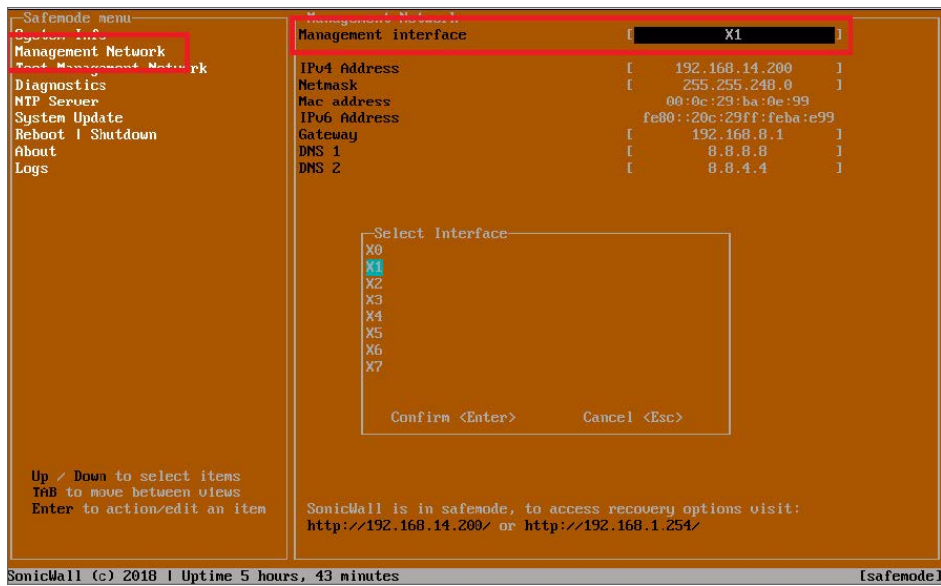
Configuring Interface Settings

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

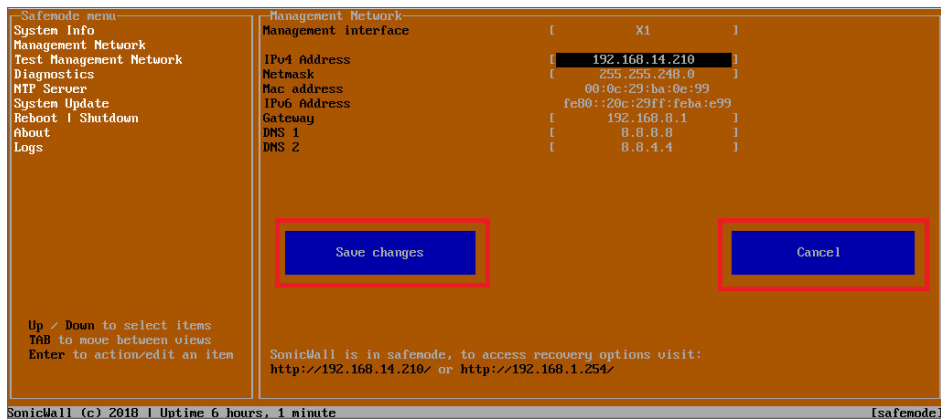


To edit an interface:

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.



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.



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

Do one of the following:

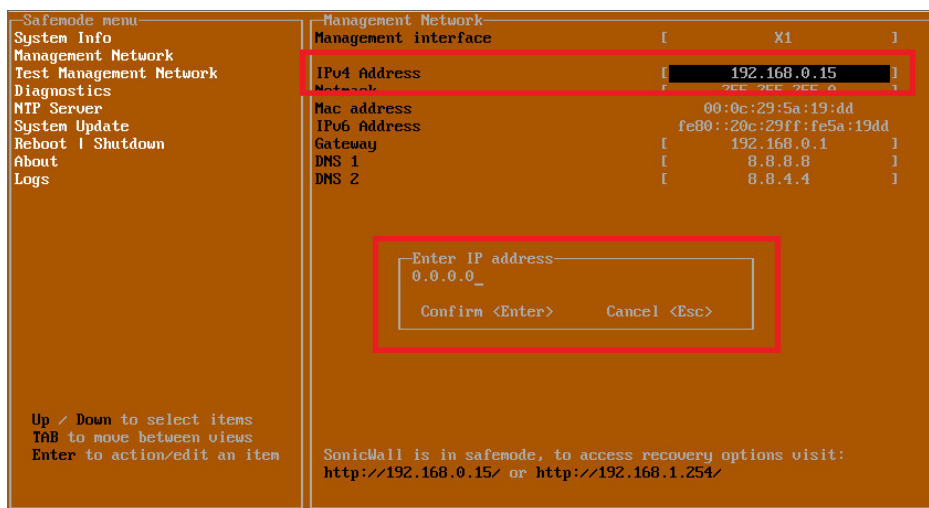
- To make changes to other settings for this interface, navigate to the desired setting, press **Enter**, make the changes in the dialog, then press **Enter** to close the dialog for that setting. Repeat for other settings, as needed.
- If finished making changes to the settings for this interface, press **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**.



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:19:4d	
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.

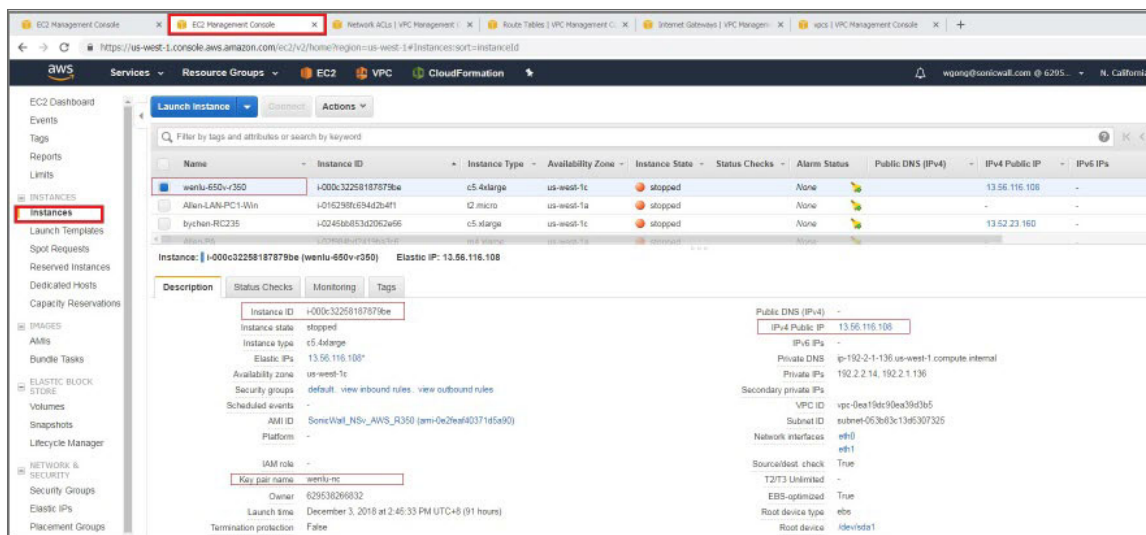
Topics:

- [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.



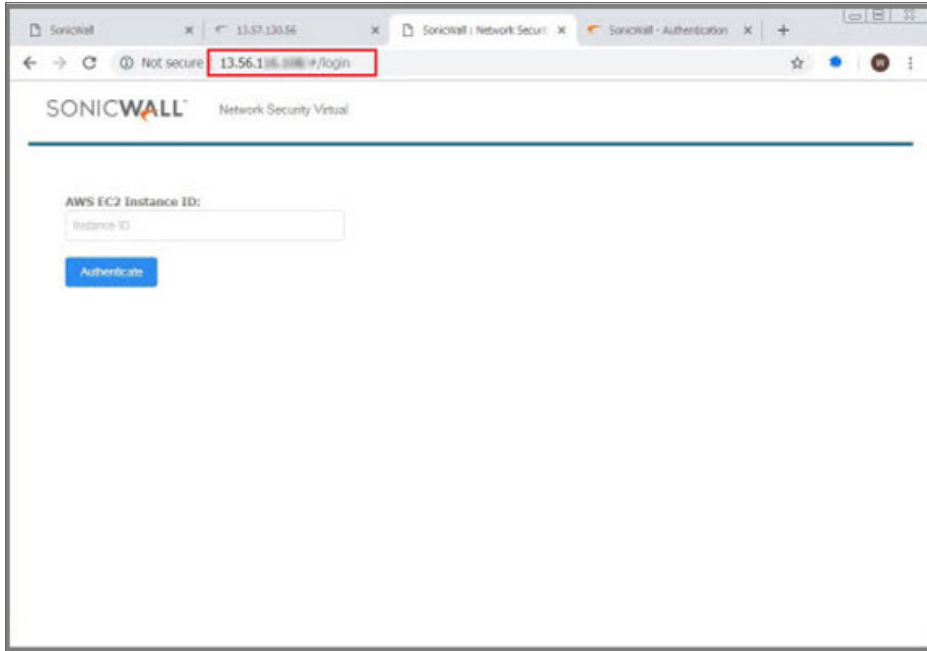
2. In the **Instances** page, locate the public IP address assigned to the NSv and the Instance ID for your NSv. You can access the SafeMode web interface at the public IP address of the NSv, and you must authenticate to gain access.

① | **NOTE:** In SafeMode, the web management interface is only available by way of **http** (not https).

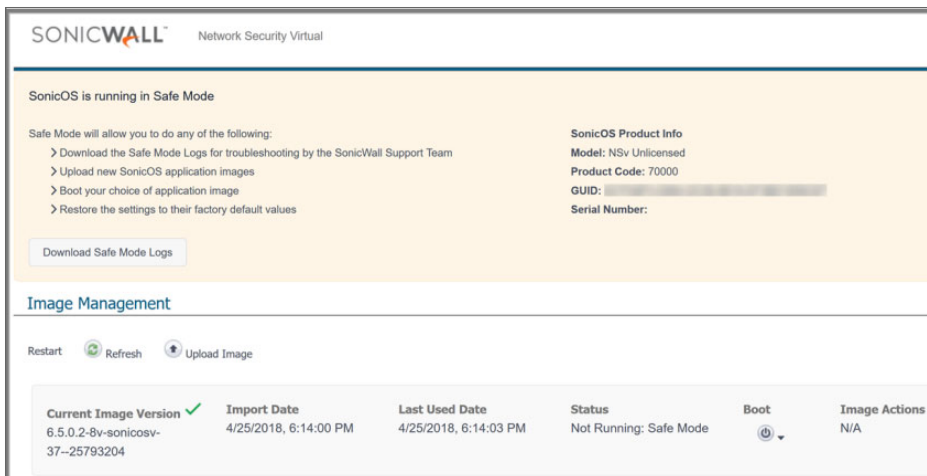
The web interface address is also given on the management console screen as shown in the following image.



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



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



Entering/Exiting SafeMode

Enter SafeMode as described in [Accessing the SafeMode Web Interface](#).

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

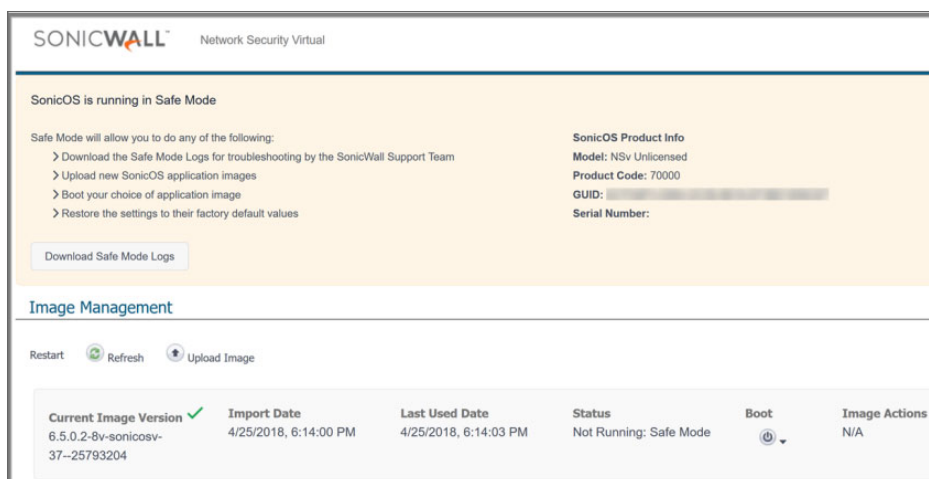
Downloading the SafeMode Logs

You can download logs of SafeMode activity.

① | **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:



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/X. You can download the latest SWI image file from MySonicWall.

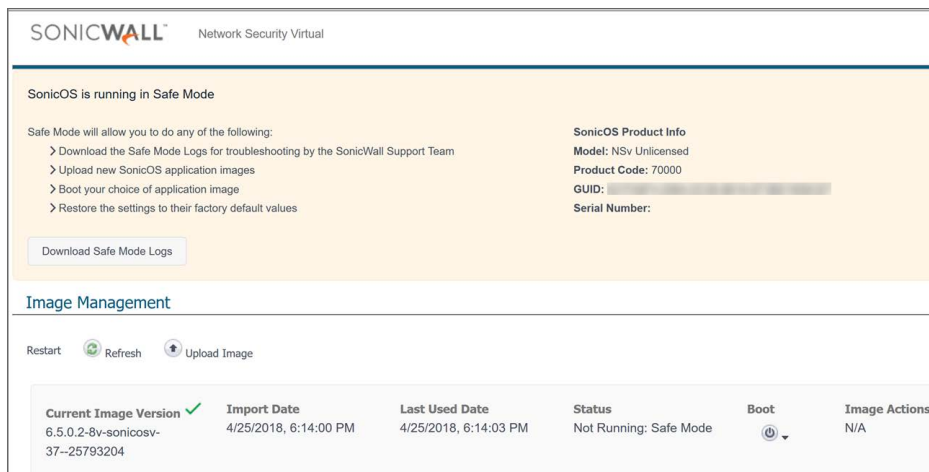
For additional information on uploading a new image, refer to: https://www.sonicwall.com/support/knowledge-base/?sol_id=180404172741874

In SafeMode, you can upload a new SonicOS/X 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.

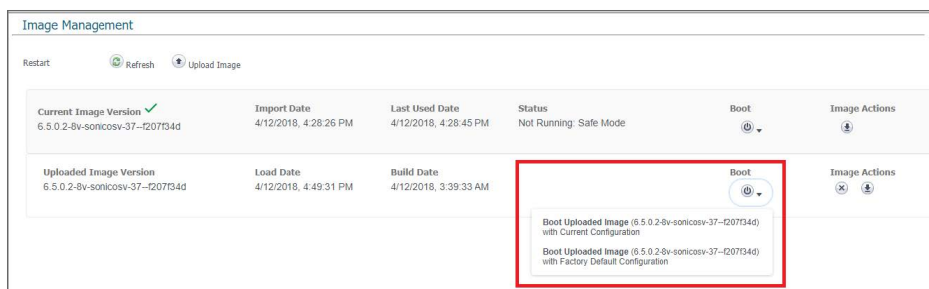
① | **NOTE:** In SafeMode, the web management interface is only available by way of **http** (not **https**).

To install a new SonicOS/X 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.



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**



The NSv virtual machine reboots with the new image.

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

① | **NOTE:** A NOTE icon indicates supporting information.

① | **IMPORTANT:** An IMPORTANT icon indicates supporting information.

① | **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 and SonicOSX NSv Getting Started Guide for the KVM Series

Updated - October 2021

Software Version - 7

232-005385-00 Rev B

Copyright © 2021 SonicWall Inc. All rights reserved.

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

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

End User Product Agreement

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

Open Source Code

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

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