SonicWall® NS$_v$ Series for KVM

Getting Started Guide

SONICWALL®

Contents

1

Introducing NS$_v$ Series for KVM/QEMU

The SonicWall® Network Security Virtual Series (SonicWall® NS*v* Series) is SonicWall's virtualized next-generation firewall appliance that provides Deep Packet Inspection (DPI) security and segmentation in virtual environments. The NS*v* Series KVM offers the same functionality and security features of a physical appliance, with comparable performance. SonicOS Virtual is a fully featured 64-bit SonicOS powered by SonicCore.

This section of the *NSv* Series KVM *Getting Started Guide* contains requirements, product matrix, feature information, and other useful information for deploying and using your SonicWall NS*v* Series virtual appliance.

Topics:

Installation File / Supported Platforms

Release Version	Supported Linux / Kernel / KVM / VMM Versions
SonicOS 6.5.4 for NS*v* Series KVM	Ubuntu 16.04-desktop • Kernel: 4.4.0-31-generic • KVM version: 2.5.0 • Virtual Machine Manager: 1.5.0
	CentOS-7 • Kernel: 3.10.0-693.e17.x86_64 • KVM version: 1.5.3 • Virtual Machine Manager: 1.5.0

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

Once you have received a purchase confirmation email, go to Obtaining the NSv Image on page 10 for download instructions.

Hardware Compatibility

SonicWall NS*v* Series is supported on x86-64 platforms supporting KVM/QEMU with sufficient resources. The following section, A log event is generated when the node count exceeds the limit., outlines core, interface, memory, and storage requirements for different NS*v* 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 OS (SonicOS*v*) 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

Node Counts Per Platform

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

Maximum Node Counts Per Platform

Platform	Maximum Node Count
NS*v* 10	10
NS*v* 25	25
NS*v* 50	50
NS*v* 100	100
NS*v* 200 and higher	Unlimited

Node counts are calculated by SonicOS as follows:

- Each unique IP address is counted.
- Only flow to the WAN side is counted.
- GVC and SSL VPN connections terminated to the WAN side are counted.
- Internal zone to zone is not counted.
- Guest users are not counted.

A log event is generated when the node count exceeds the limit.

Product Matrix and Requirements

The following tables show the hardware resource requirements for the SonicWall NS*v* Series virtual appliances.

NOTE: Jumbo packets are not currently supported in the NS*v* KVM/QEMU implementation.

Product Models	NS*v* 10	NS*v* 25	NS*v* 50	NS*v* 100
Maximum Cores[1]	2	2	2	2
Minimum Total Cores	2	2	2	2
Management Cores	1	1	1	1
Maximum Data Plane Cores	1	1	1	1
Minimum Data Plane Cores	1	1	1	1
Network Interfaces	8	8	8	8
Supported IP/Nodes	10	25	50	100
Minimum Memory Required	4G	4G	4G	4G
Minimum Hard Disk/Storage	60GB	60GB	60GB	60GB

1. If the actual number of cores allocated exceeds the number of cores defined in the above table, extra cores will be used as CPs. Multiple CP support is introduced in 6.5.4.v.

Product Models	NS*v* 200	NS*v* 300	NS*v* 400	NS*v* 800	NS*v* 1600
Maximum Cores[1]	2	3	4	8	16
Minimum Total Cores	2	2	2	2	2
Management Cores	1	1	1	1	1
Maximum Data Plane Cores	1	2	3	7	15
Minimum Data Plane Cores	1	1	1	1	1
Network Interfaces	8	8	8	8	8
Supported IP/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Minimum Memory Required	6G	8G	8G	10G	12G
Minimum Hard Disk/Storage	60G	60G	60G	60G	60G

1. If the actual number of cores allocated exceeds the number of cores defined in the above table, extra cores will be used as CPs. Multiple CP support is introduced in 6.5.4.v.

Backup and Recovery Information

In certain situations, it might be necessary to contact SonicWall for help as directed in SonicWall Support on page 55, or visit SonicWall, use SafeMode, or deregister the NS*v* appliance:

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Please contact SonicWall as directed in SonicWall Support on page 79.
- If the disk is not recoverable, then the NS*v* appliance needs to be deregistered with MySonicWall. See Deregistering Your NSv on page 27 for 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 information about SafeMode, see Using SafeMode on the NSv on page 46.

- If SonicOS fails three times during the boot process, it will boot into SafeMode. Verify that the minimum required memory is available and allocated based on the NS*v* model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall as directed in SonicWall Support on page 55.

Importing Firewall Configurations

Configuration settings import is ***not*** supported from SonicWall physical appliances to the NS*v*.

High Availability Configurations

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

For details, refer to SonicOS*v* documentation: https://www.sonicwall.com/support/technical-documentation/ enter Product as NSv Series and look under **Administration** for the SonicOS 6.5 NSv Series System Setup guide.

Upgrading to a Higher Capacity NS$_v$ Model

It is possible to move up to a higher capacity NSv model, but not down to a lower capacity model. For instructions refer to the *SonicOS 6.5.4 NSv Series Upgrade Guide* on the Technical Publications portal. Go to https://www.sonicwall.com/support/technical-documentation/ and select “NSv Series” as the product.

For details on the number of processors and memory to allocate to the VM to upgrade, refer to A log event is generated when the node count exceeds the limit. on page 6.

Creating a MySonicWall Account

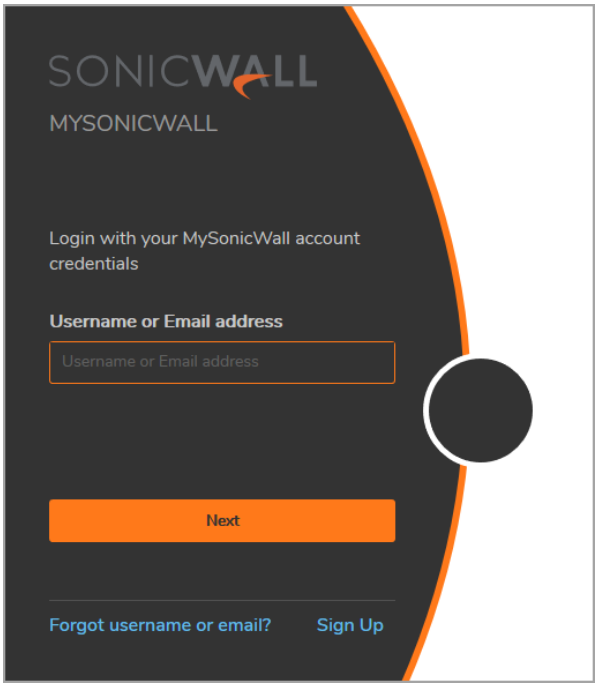
A MySonicWall account is required to obtain the image file for initial installation of the NS*v* Series KVM virtual firewall, for product registration to enable full functionality of SonicOS features, and for access to licensed security services. For a High Availability configuration, MySonicWall provides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

NOTE: 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.

NOTE: Your password must be at least 8 characters, but no more than 30 characters.

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. Once you have scanned the code, you need only click a button to confirm authentication.

6 Click on **CONTINUE** to go 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 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 **DONE**.

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. If you are using Microsoft or Google authenticator, scan the code or confirm authentication with a button.

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

2

Installing the NS*v* Series on KVM

Topics:

Preparing the Linux Server System

Before installing a SonicWall NS*v* Series virtual firewall on a Linux server, prepare the server:

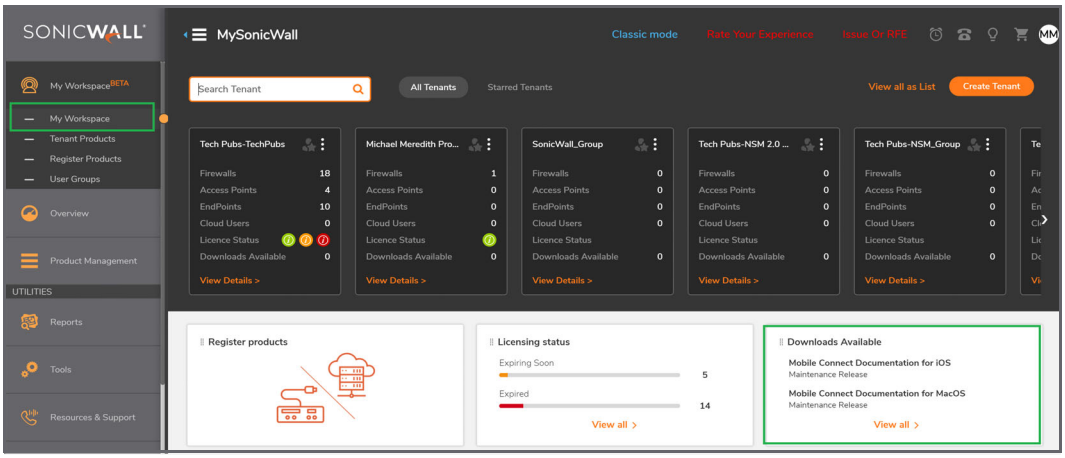
- Install Ubuntu or CentOS on the server. For version details refer to Installation File / Supported Platforms on page 4.
- Install KVM and QEMU on server.
- Connect the Linux Server system to an external switch.

Obtaining the NS*v* 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 on page 8) and go to the Download Center:

To download image:

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



2 Click on 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 on the download symbol to download: 

4 Keep the serial number and Authenitcation code from the purchase confirmation email to complete product registration after the virtual firewall in installed. Refer to Registering the NSv Appliance from SonicOS on page 24.

Installing the NSv Series on Ubuntu-KVM/QEMU

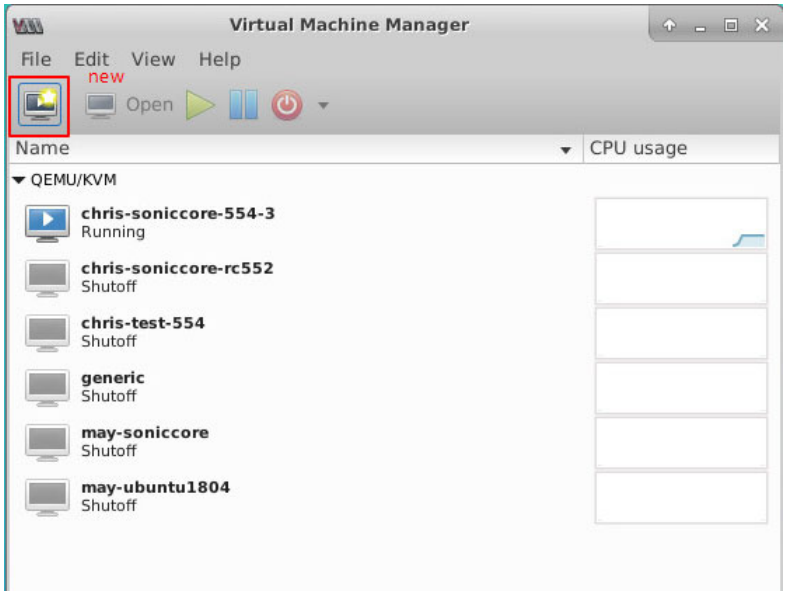
To install an NSv on Ubuntu-KVM/QEMU:

1 Download the NSv firewall ***img*** file to a local folder in the Linux Server system.

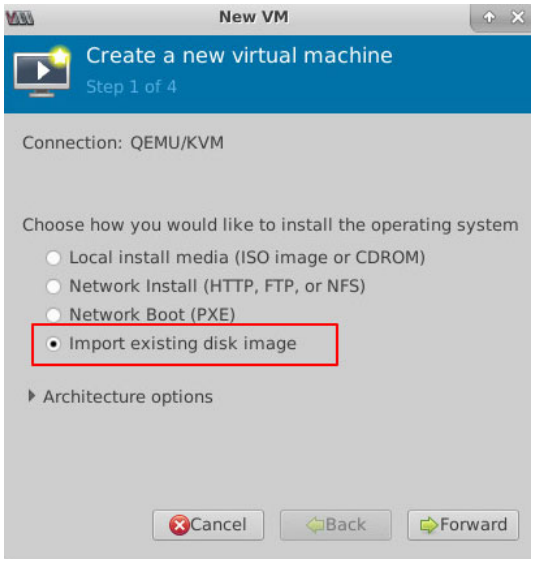
2 Copy image file (for example: “SonicWall_NSv_For_QEMU_VM.img”) into the directory **/var/lib/libvirt/images/**

3 Bring up the Virtual Machine Manager (VMM):

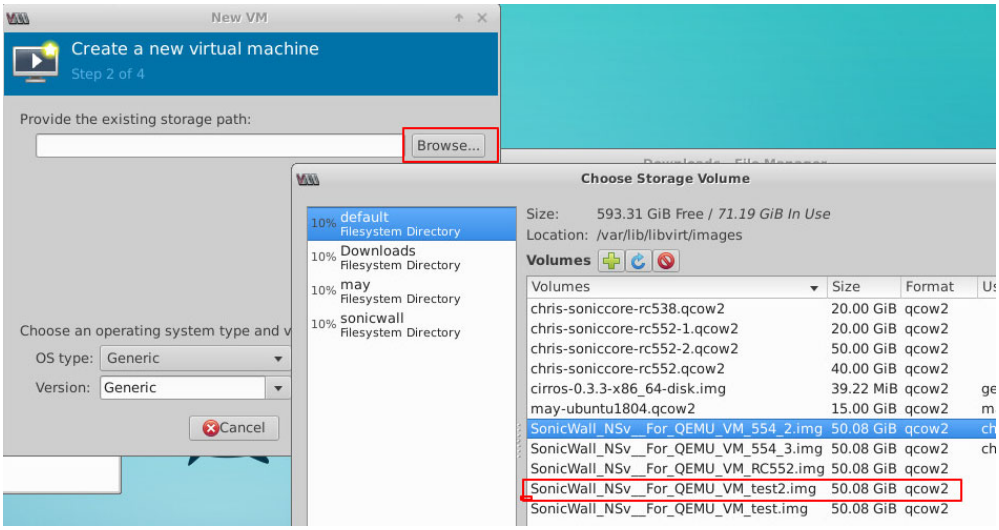
4 Create a VM in the Virtual Machine Manager to receive the image file:



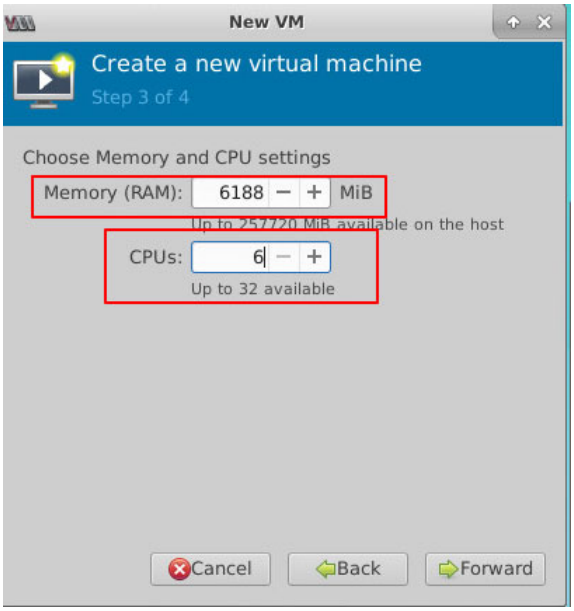
5 Starting creating a new virtual machine by importing a disk image:



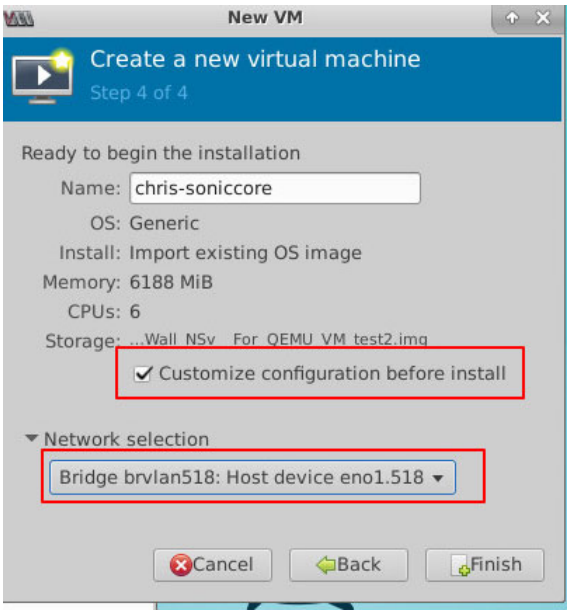
6 Choose storage volume:



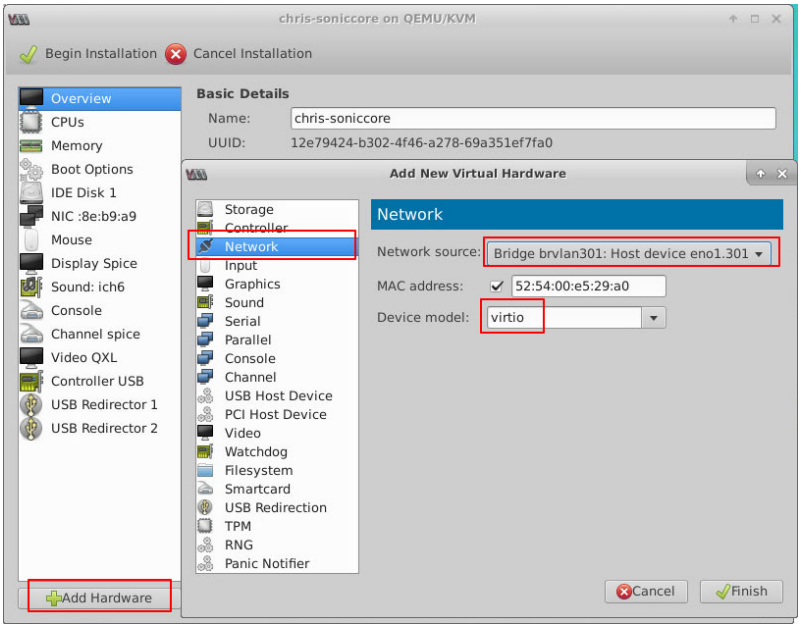
7 Configure CPU/Memory/Name/Network (default only one network interface attached), then click **Finish** to create. For hardware resources, refer to A log event is generated when the node count exceeds the limit. on page 6.



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

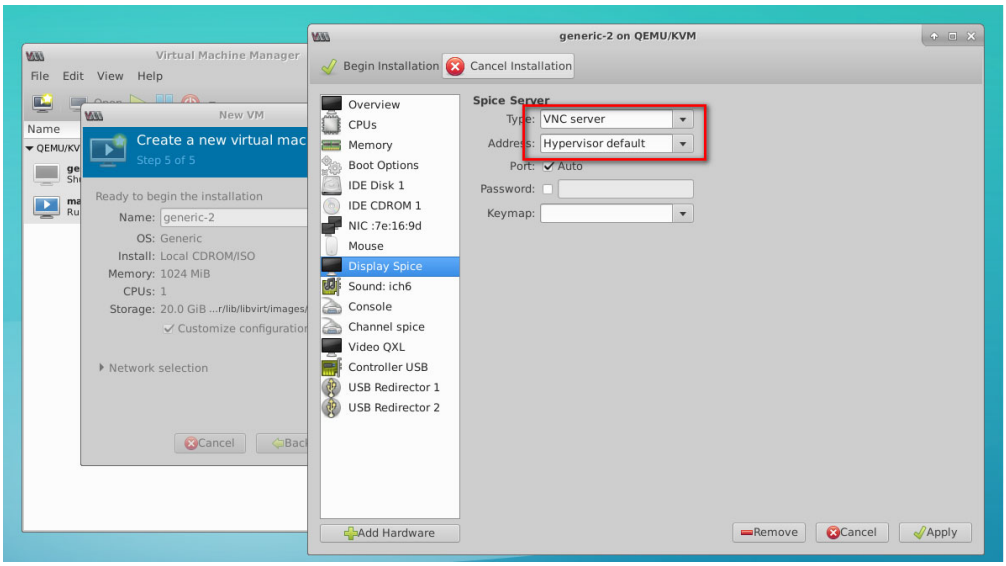


9 Another interface is required to serve as WAN port, or X1 of the firewall. Here we choose the *interface 301*:



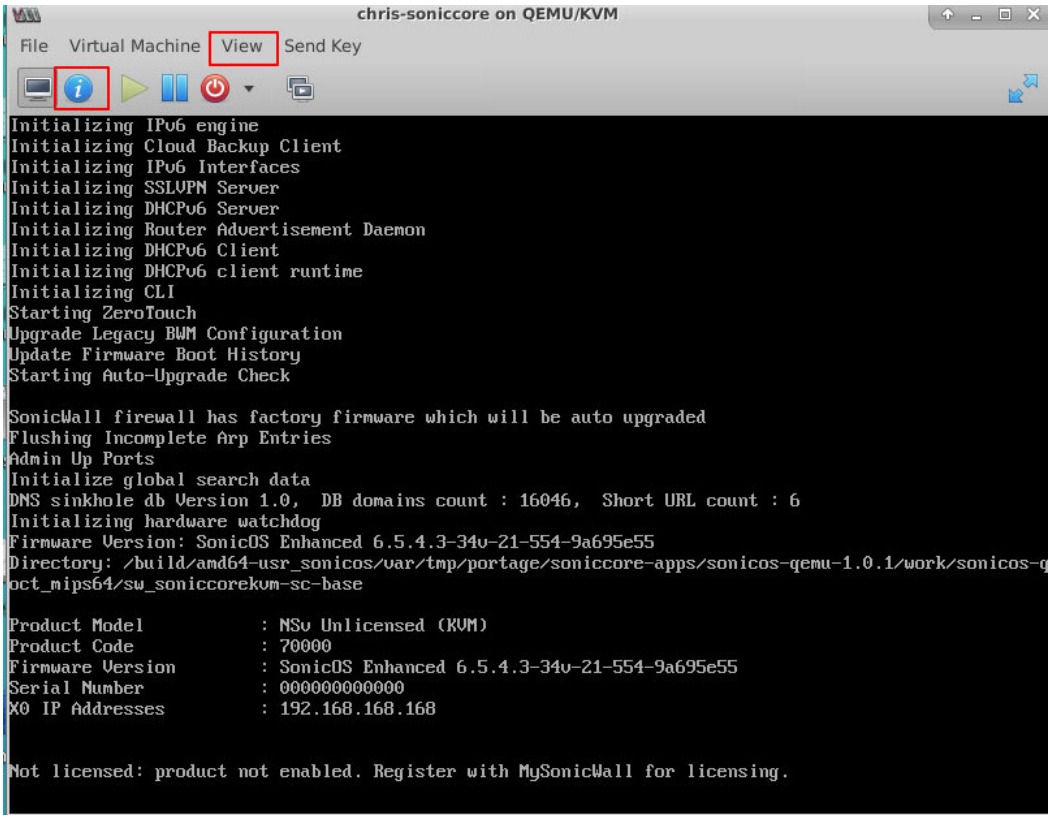
NOTE: Both device models should choose **virtio**. By default, the first network card is X0, and the second one is X1. By choosing virtio, the VirtIO API is enabled. For more on VirtIO, see Paravirtualization on page 5.

10 Create a new VM with the Display set as **VNC server**. Otherwise you may not be able to use the keyboard with the new VM.



NOTE: In the above 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 VM and select **View** to see NS*v* 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

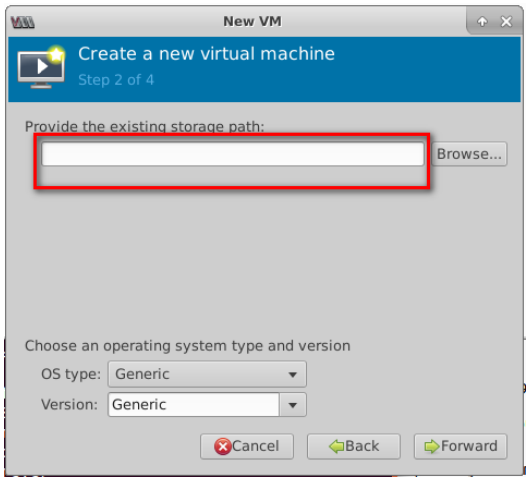
```
apt-get install vlan bridge-utils
edit /etc/network/interfaces:
#edit physical interface
auto eno 1
```

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 *img* file

If unable to locate through Browse as shown below, just 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:

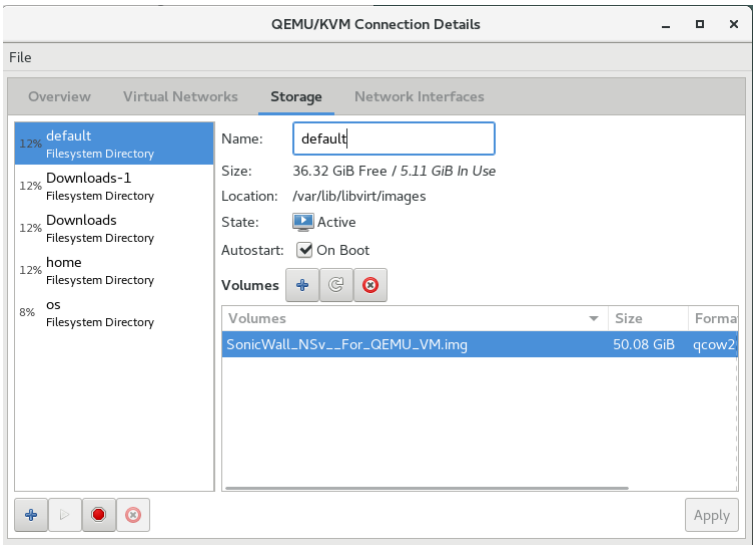
- Registering the NSv Appliance from SonicOS on page 24
- Registering an NSv in a Closed Network on page 26
- Managing SonicOS on the NSv Series on page 30
- Using System Diagnostics in SonicOS on page 33
- Using the Virtual Console and SafeMode on page 35

Installing the NS$_v$ Series on CentOS-KVM/QEMU

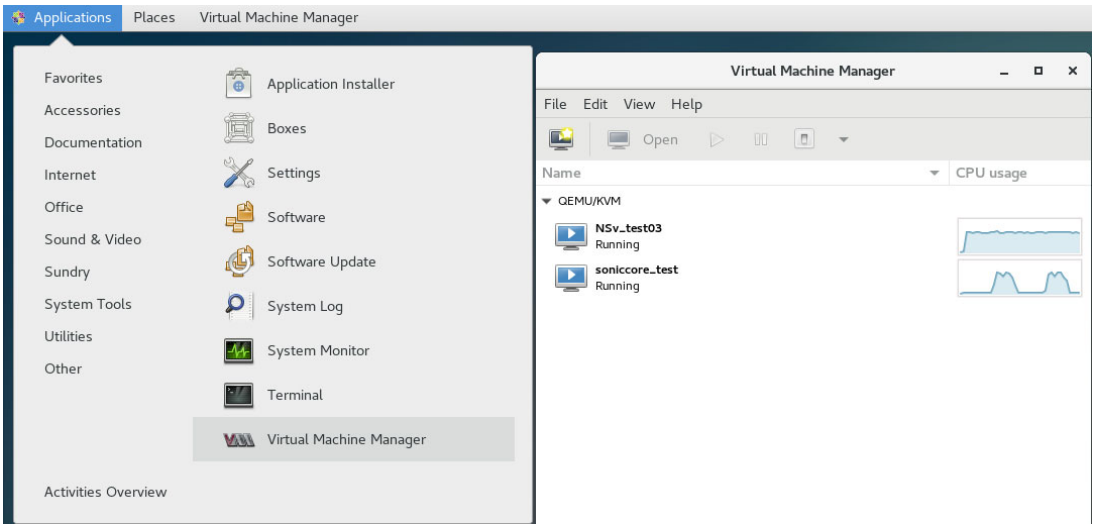
To install an NSv on CentOS-KVM/QEMU:

1 Download the NS*v* firewall ***img*** file to a local folder in the Linux Server system.

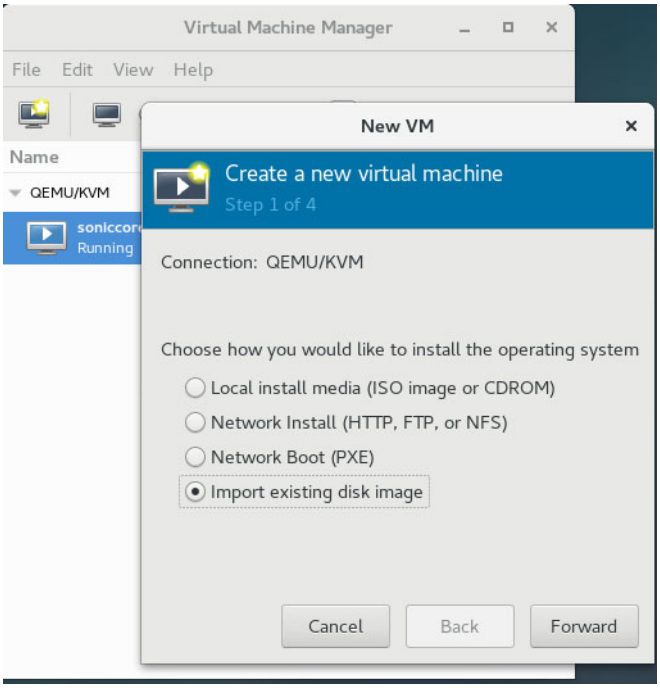
2 Copy image file (for example: “SonicWall_NSv_For_QEMU_VM.img”) into the directory **/var/lib/libvirt/images/**



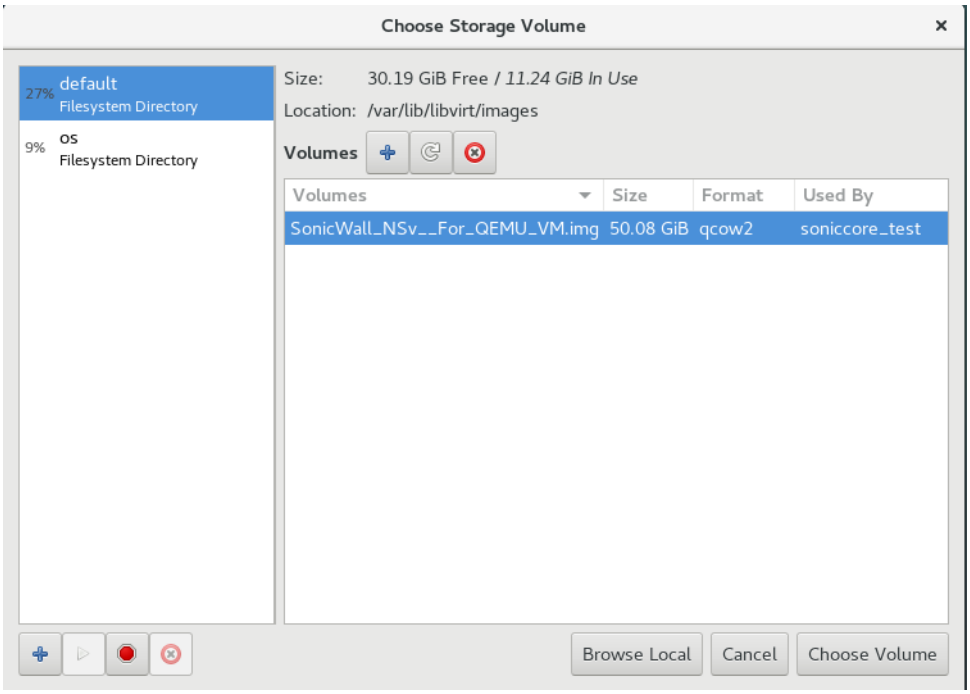
3 Bring up the Virtual Machine Manager (VMM):



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



5 Choose the storage volume:



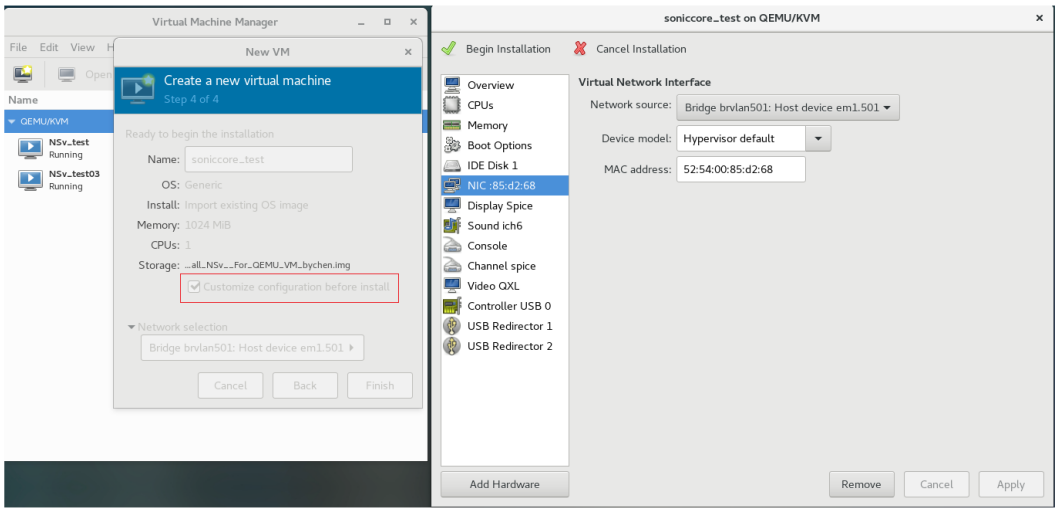
6 Configure CPU/Memory/Name/Network (default only one network interface attached), then finish to create.

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

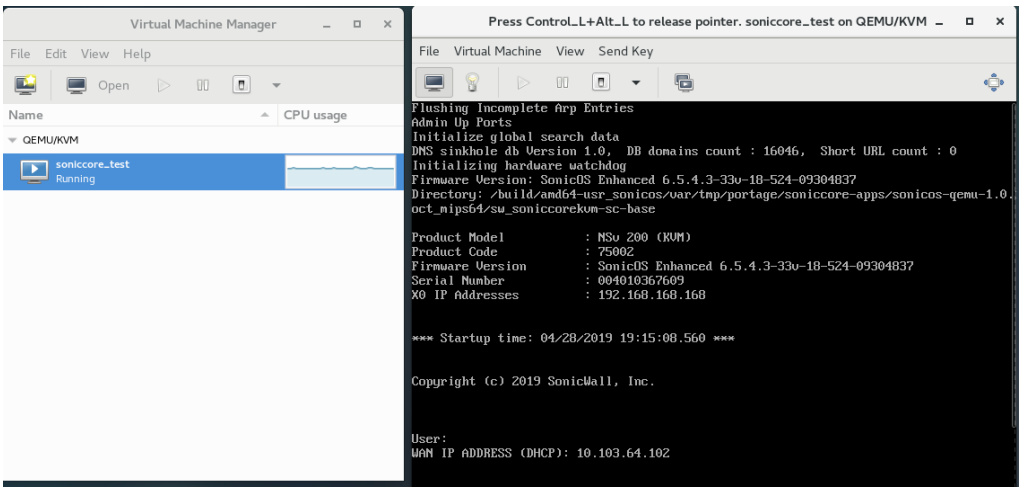
b We need to add another network interface as WAN port, that is X1 of the firewall, here we choose the **interface 301.**

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

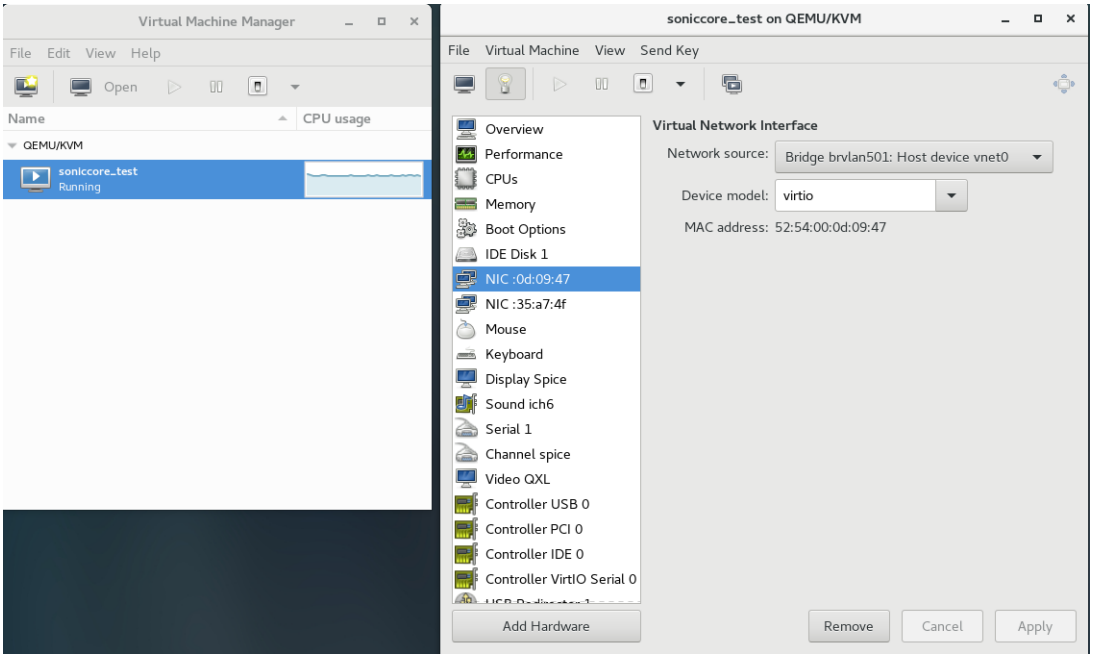
c Create new VM with Display set as VNC otherwise you may not be able to use keyboard with new vm.



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



8 Add interfaces and select virtio type:



Creating NS$_v$ 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 VM Config File

Following "virsh" command need root right:

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

Edit vm config file with following command:

```
virsh  edit  <your_vmname>
```

You can check vm info by:

```
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 VMs.

Next steps and related topics:

- Registering the NSv Appliance from SonicOS on page 24
- Registering an NSv in a Closed Network on page 26
- Managing SonicOS on the NSv Series on page 30
- Using System Diagnostics in SonicOS on page 33
- Using the Virtual Console and SafeMode on page 35

3

Licensing and Registering Your NS$_v$

Topics:

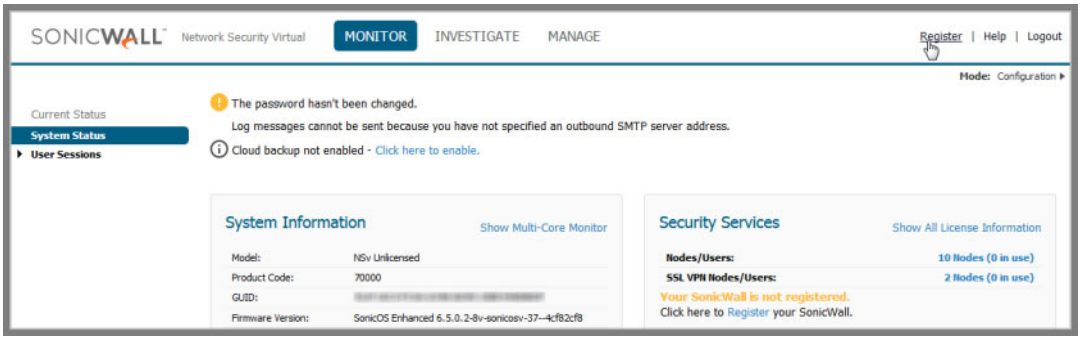
Registering the NS$_v$ Appliance from SonicOS

Once you have installed and configured network settings for your NS*v* Series KVM appliance, you can log into SonicOS management and register it in your MySonicWall account. Registration of your SonicWall NS*v* Series follows the same process as for SonicWall hardware-based appliances.

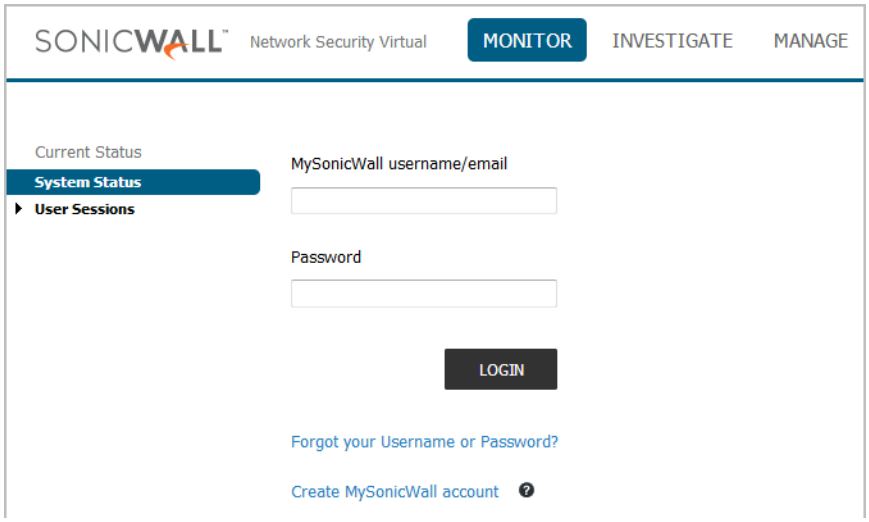
NOTE: System functionality is extremely limited if registration is not completed. See Using SonicOS on an Unregistered NSv on page 30 for more information.

To register your NSv appliance:

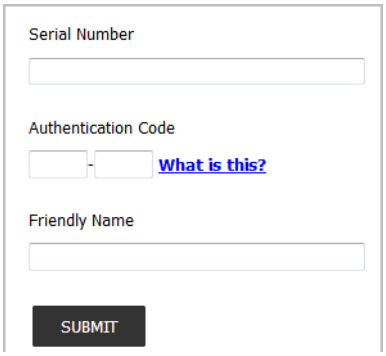
1. Point your browser to your NS*v* Series KVM WAN or LAN IP address and log in as the administrator (default *admin / password*).
2. Click the **Register** link in the top banner or on the **MONITOR | System > Status** page.



3 Enter your MySonicWall credentials and click **LOGIN** to log into MySonicWall.



4 In the **Serial Number** and **Authentication Code** fields, enter the corresponding values you received in your purchase confirmation email.



5 Type a descriptive name for the NS*v* into the **Friendly Name** field.

6 Click **SUBMIT**.

7 The licensing server acquires the necessary information from the NS*v* Series KVM appliance and your MySonicWall account.

8 Acknowledge the registration completion notification by clicking **CONTINUE**.

SonicOS automatically restarts and then displays the login page.

9 Log into SonicOS.

On the **MANAGE** view under **Updates**, the **Licenses** page now shows your NS*v* appliance as **Licensed**.

10 In the **Licenses** page, you can activate security service free trials, enable available services, and click to purchase other services you want.

Registering an NS$_v$ in a Closed Network

NOTE: This registration method uses Manual Upgrade and is **not** recommended for normal product registration on products that have internet access. See Registering the NSv Appliance from SonicOS on page 24 for the recommended registration method on products with internet access.

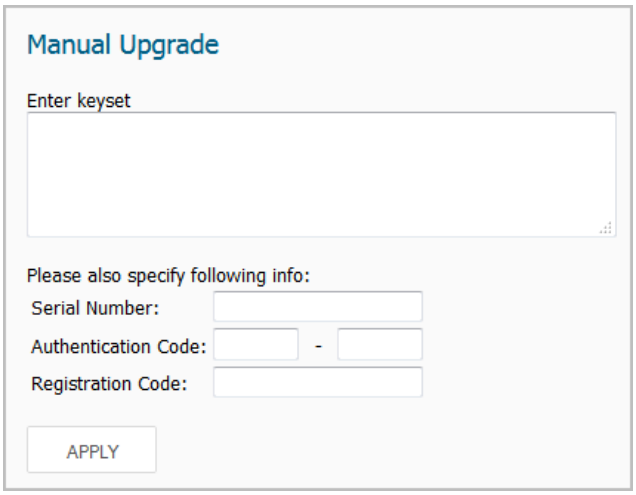
NOTE: Only an NS*v* which was registered online can be deregistered. If the NS*v* was registered using the offline method, deregistration is not supported.

In a closed network, your NS*v* does not have internet access and cannot communicate directly with the SonicWall licensing server. To complete the registration process, you need to obtain information from MySonicWall and then log into SonicOS on your NS*v* and enter that information.

NOTE: System functionality is extremely limited if registration is not completed. See Using SonicOS on an Unregistered NSv on page 30 for more information.

To register an NSv virtual firewall in a closed network environment:

1. Log into your NS*v* appliance and navigate to the **MONITOR | System Status** page.
2. Make a note of the **GUID**, or leave the page open in your browser. The **GUID** is displayed in the **System Information** section.
3. In another browser tab or window, log into your MySonicWall account.
4. Navigate to **My Products** and click on the entry for your NS*v* appliance.
5. To get the **License Keyset**, first click the key icon.
6. Enter the **GUID** into the dialog box and click **Update**. The **License Keyset** is displayed. This is a binary representation of all the service licenses activated on your NS*v*.
7. Select the **License Keyset** and copy it to your clipboard.
8. Log into your NS*v* appliance or return to that browser window if still logged in.
9. Navigate to the **MANAGE | Licenses** page in SonicOS.
10. Under **Manual Upgrade**, paste the **License Keyset** into the **Enter keyset** field.



11. In the **Serial Number** and **Authentication Code** fields, enter the corresponding values you received after purchasing your NS*v* Series KVM virtual firewall.

12 In the **Registration Code** field, enter the registration code you received when you did the initial registration in MySonicWall to obtain the NSv image file. See Obtaining the NSv Image on page 10 for more information.

13 Click **APPLY** to register the NSv and activate the licensed services.

14 Click **ACCEPT**.

Your NS*v* virtual firewall is now registered.

Deregistering Your NS*v*

You can deregister your NS*v* directly from the SonicOS management interface. Deregistration puts the virtual appliance into the unregistered state and deletes the binding between it and its serial number in MySonicWall. Then you can use the serial number to register the same or another NS*v* instance. Only one NS*v* instance is allowed per serial number.

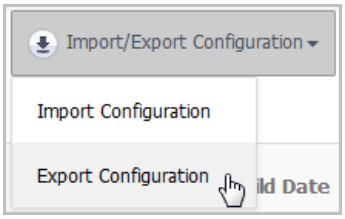
NOTE: Only an NS*v* which was registered online can be deregistered. If the NS*v* was registered using the offline method, deregistration is not supported.

To deregister an NSv:

1 Log into the SonicOS management interface on your NS*v* virtual appliance.

2 Navigate to the **Updates | Setting** page in the **MANAGE** view.

3 Select **Export Configuration** from the **Import/Export Configuration** drop-down list to export your current configuration settings before deregistering your NS*v*.

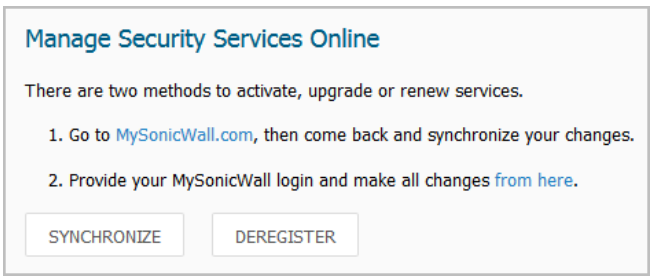


This makes it possible to import the settings to another NS*v* instance.

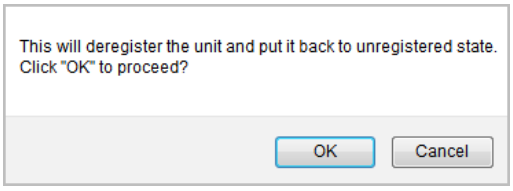
CAUTION: Be sure to export your configuration settings before deregistering your NSv. You cannot recover them after deregistration.

4 Navigate to the **Updates | Licenses** page in the **MANAGE** view.

5 Under **Manage Security Services Online**, click the **DEREGISTER** button.



6 Click **OK** in the confirmation dialog.



If deregistration is successful, the virtual appliance will return to the unregistered state. You can see the **Register** link in the top banner of SonicOS and the message “Your SonicWall is not registered” on the **MONITOR | System > Status** page.

If deregistration fails, an error message is displayed in the status bar at the bottom of the SonicOS management interface.

Converting a Free Trial License to Full License

A SonicWall NS*v* instance installed as a 30-day free trial can easily be converted to a full production licensed NS*v* instance.

To convert your free trial to a production version:

1 Purchase a SonicWall NS*v* license from a distributor. You will receive a fulfillment email with the new serial number and authentication code.

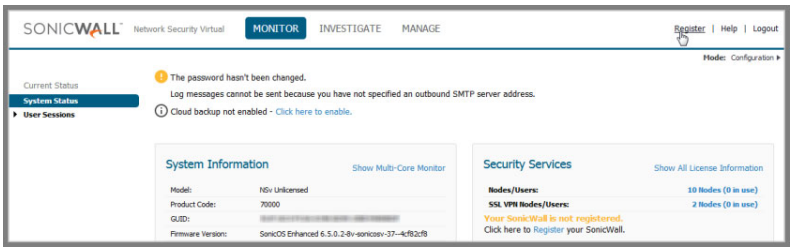
2 Log into SonicOS on your free trial instance.

3 Navigate to the **Updates | Licenses** page in the **MANAGE** view.

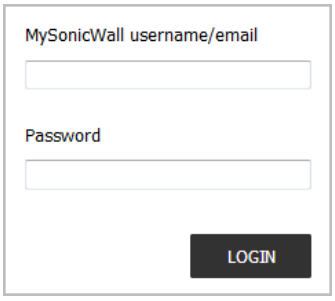
4 Under **Manage Security Services Online**, click the **DEREGISTER** button.

5 Click **OK** in the confirmation dialog. The virtual firewall returns to the unregistered state.

6 Click the **Register** link in the top banner or on the **MONITOR | System > Status** page.



7 Enter your MySonicWall credentials and then click **LOGIN**.



8 Enter the **Serial Number** and **Authentication Code** you received after purchasing your NS*v* Series KVM instance.

9 Click **SUBMIT**.

10 The licensing server acquires the necessary information from the NS*v* Series KVM appliance and your MySonicWall account. If asked, you can specify a **Friendly Name** or **Product Group** for the NS*v* Series KVM appliance.

11 Acknowledge the registration completion notification by clicking **CONTINUE**.

SonicOS automatically restarts and then displays the login page.

12 Log into SonicOS.

In the **MONITOR** view, the **System > Status** page now shows your licensed security services, and the **Register** link is no longer displayed.

13 In the **MANAGE** view on the **Updates | Licenses** page, you can activate security service free trials, enable available services, and click to purchase other services you want.

4

SonicOS Management

Topics:

Managing SonicOS on the NS*v* Series

The X1 interface is the default WAN Interface and is set to use DHCP addressing by default, with HTTPS management enabled. 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 by default 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. After deployment, you can reconfigure the IP address to an address in your network.

To log into SonicOS for management of the NS*v*:

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 NS*v* from a computer on that network for SonicOS management. The NS*v* 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 appliance.

Using SonicOS on an Unregistered NS*v*

The SonicOS management interface provides fewer features on an unregistered NS*v* Series KVM appliance than on a registered NS*v*. The Available SonicOS Pages on Unregistered NS*v* table provides a summary of the available features on an unregistered NS*v*.

Available SonicOS Pages on Unregistered NS*v*

Top Level View	Page Group	Page Within Group	Description
MONITOR	System Status	n/a	System information, Node license, Alerts, Network interface settings
	User Sessions	SSL-VPN Sessions	User sessions connected via SSL VPN

Available SonicOS Pages on Unregistered NSv

Top Level View	Page Group	Page Within Group	Description
		Active Users	Active user session information; Logout button for users
		Active Guest Users	Active guest user session information; Logout button for guest users
		User Monitor	Graph of logged in users over time for client logins and web based logins
INVESTIGATE	Event Logs	n/a	Log event table, dynamically updated, filterable, searchable, one-click details
	Connection Logs	n/a	Connection log, source/destinations, protocols, bytes transferred, filterable, searchable, flush option
	Appflow Logs	n/a	Requires App Visualization license, which requires registration
	System Diagnostics	n/a	TSR access and Diagnostic tools:  See Using System Diagnostics in SonicOS on page 33 for information.
MANAGE	Licenses	n/a	Node license information, MySonicWall access, Manual Upgrade
	Settings	n/a	Firmware versions, Local Backup, Settings import/export, Settings options to send to SonicWall Support
	Restart	n/a	Restarts the virtual firewall after confirmation
	Appliance	Base Settings	Firewall name, Admin username and password, Login security, Multiple administrator, Web/SSH/GMS management, Client certificate checks, and Language settings

Available SonicOS Pages on Unregistered NSv

Top Level View	Page Group	Page Within Group	Description
		SNMP	Enable SNMP
		Certificates	View and Import certificates, Generate certificate signing requests, SCEP for issuing certificates to endpoint devices
		System Time	Time and time zone, NTP server settings
		System Schedules	Schedule settings
	Network	Interfaces	Interface settings, Traffic statistics
		Failover & Load Balancing	Enable load balancing, LB Group configuration, Statistics
		Zones	Zone settings
		VLAN Translation	VLAN Translation configuration
		DNS	IPv4 DNS settings
		DNS Proxy	Enable DNS Proxy, DNS proxy and cache settings
		Routing	Route policies, OSPF, RIP
		ARP	Static ARP entries, ARP settings and cache
		Neighbor Discovery	Static NDP entries, NDP settings and cache
		MAC-IP Anti-spoof	Interface anti-spoof settings, cache, detected list
		DHCP Server	Enable DHCPv4 Server, Configure lease scopes, View current leases
		IP Helper	Enable IP Helper, Configure relay protocols and policies, Refresh DHCP relay leases
		Web Proxy	Proxy forwarding, User proxy servers
		Dynamic DNS	DDNS Profile settings
	Log Settings	Base Setup	Logging and alert levels, per-category settings
		SYSLOG	Syslog settings, servers
		Automation	Email settings for sending logs and alerts, Solera Capture Stack
		Name Resolution	DNS and NetBios methods
		Analyzer	Requires Analyzer license, which requires registration
	Legal	n/a	End User Product Agreement

Using System Diagnostics in SonicOS

The **Tools | System Diagnostics** page on the **INVESTIGATE** view provides several diagnostic tools that help troubleshoot various kinds of network problems and process monitors, to help you resolve many of the common issues you might face. Each tool is different from the others so the display changes with the tool. However, some of the data management functions are common among the tools.

Nearly all the tools have these buttons at the bottom of the window:

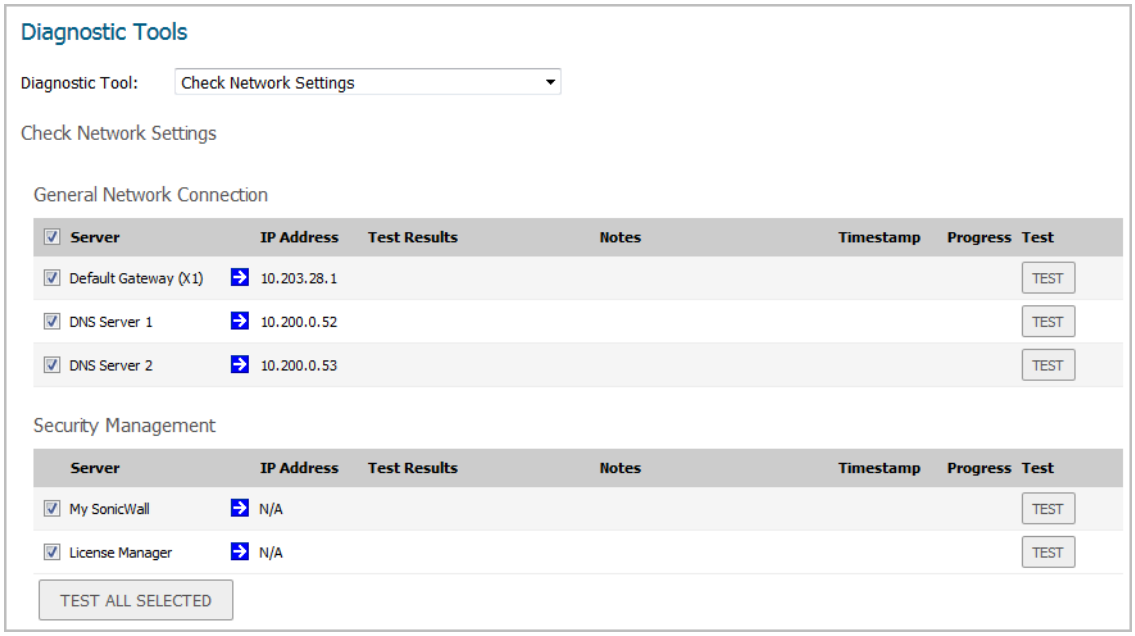
Button	Function
ACCEPT	Saves any changes you made to the diagnostic support report or diagnostic tool.
CANCEL	Cancels any changes you initially made to the diagnostic support report or diagnostic tool.
REFRESH	Refreshes the data being displayed in the **Diagnostic Tools** section.

Some tools have management functions to help you manage lists of data. These operate much like the options on the other logs and reports.

- Search
- Filter
- Toggling between views (IPv4 vs. IPv6, for example)
- Refresh
- Export
- Clear

Select the tool you want from the **Diagnostic Tool** drop-down menu in the **Tools | System Diagnostics** page. The Check Network Settings tool is described below. See the *SonicOS 6.5 NSv Series Investigate* administration documentation for complete information about the available diagnostic tools.

Check Network Settings



Check Network Settings is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined functional areas of the NS*v* Series KVM, 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.

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

The return data consists of two parts:

- **Test Results** – Provides a summary of the test outcome
- **Notes** – Provides details to help determine the cause if any problems exist

The Check Network Settings tool is dependent on the **Network Monitor** feature available on the **Tools | Network Probes** on the **INVESTIGATE** view. Whenever the **Check Network Settings** tool is being executed (except during the Content Filter test), a corresponding Network Monitor Policy appears on the **Tools | Network Probes** page, with a special diagnostic tool policy name in the form:

`diagTestPolicyAuto_<IP_address/Domain_name>_0`

NOTE: Log messages show the up/down status of some of these special network objects. These objects, however, live for only three seconds and then are deleted automatically.

To use the **Check Network Settings** tool, first select it in the **Diagnostic Tools** drop-down list and then click the **Test** button 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 probes fail, you can click the blue arrow to the left of the I**P 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:

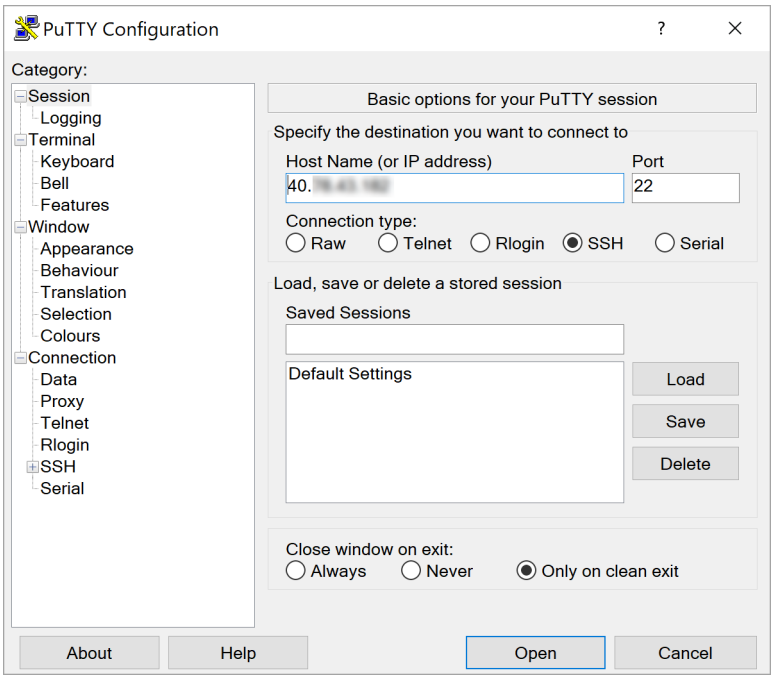
Connecting to the Console

There are two ways to connect to the management console:

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

To connect to the management console using SSH:

1 Launch PuTTY and type in the public IP address of the NS*v* on KVM/QEMU.



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

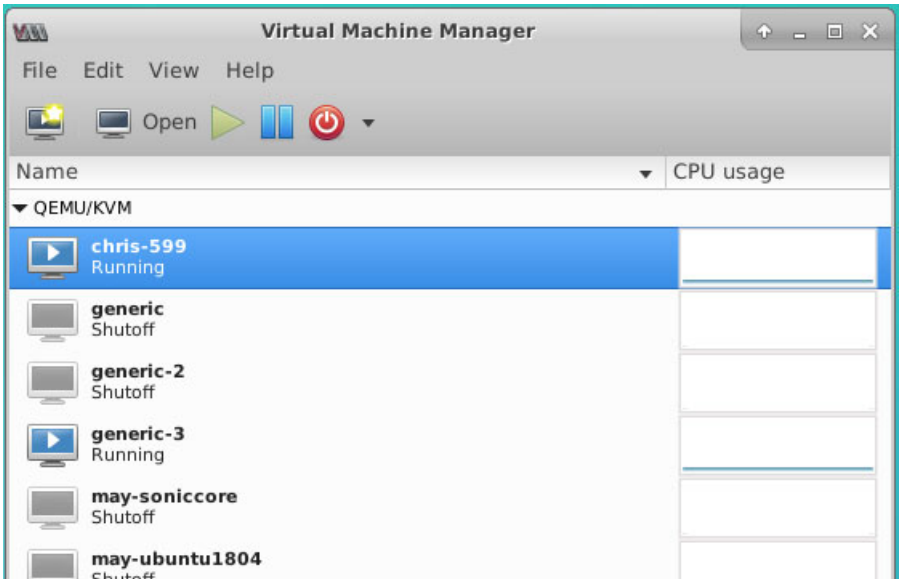
3 For **Connection type**, **SSH** should already be selected by specifying port 22.

4 Click **Open** to open a console connection.

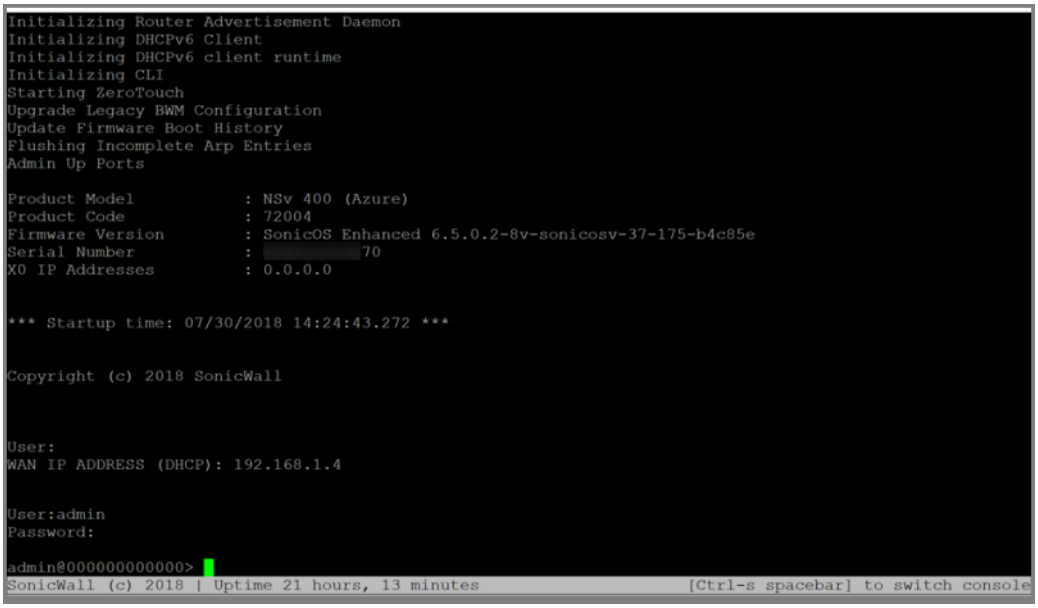
5 When you are prompted to log in at the **User** prompt, enter the SonicOS administrator credentials (default: *admin / password*).

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

1 Bring up the VMM, then double click on the VM with the NS*v*.



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

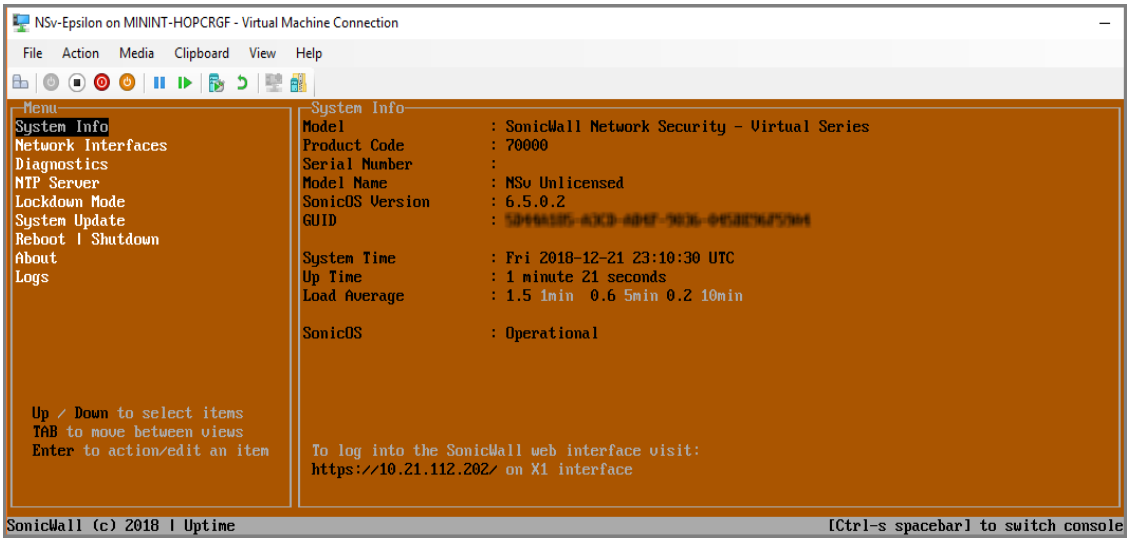


See Navigating the NSv Management Console on page 37 for information about the options in the NS*v* management console.

Navigating the NS*v* Management Console

Once you have arrived at the NS*v* CLI, bring up the management console window by pressing **Ctrl+s** and then the **spacebar**. To navigate and use the management console:

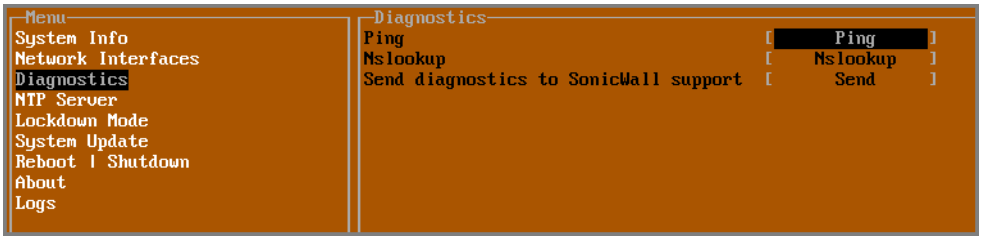
1 Press **Ctrl+s** and then press the **spacebar** to toggle between the SSH virtual console or Virtual Machine Manager console and the NS*v* management console. That is, press the **Ctrl** key and '**s**' key together, then release and press the **spacebar**.



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.

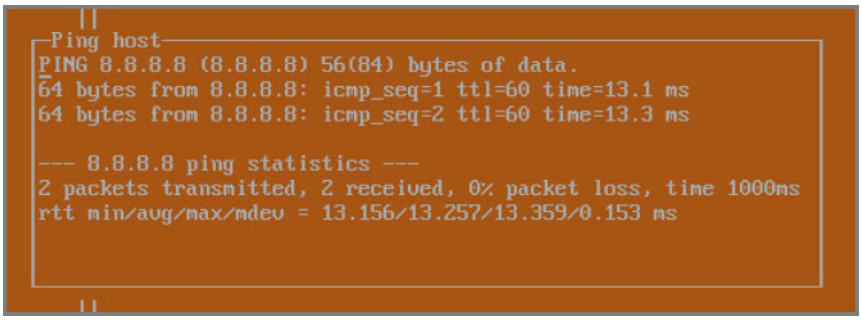
3 Press the **Tab** key to move the focus from side menu to the main view (right pane), or vice versa.

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.



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 below the option list. Some dialogs have selectable actions and some are only for information:

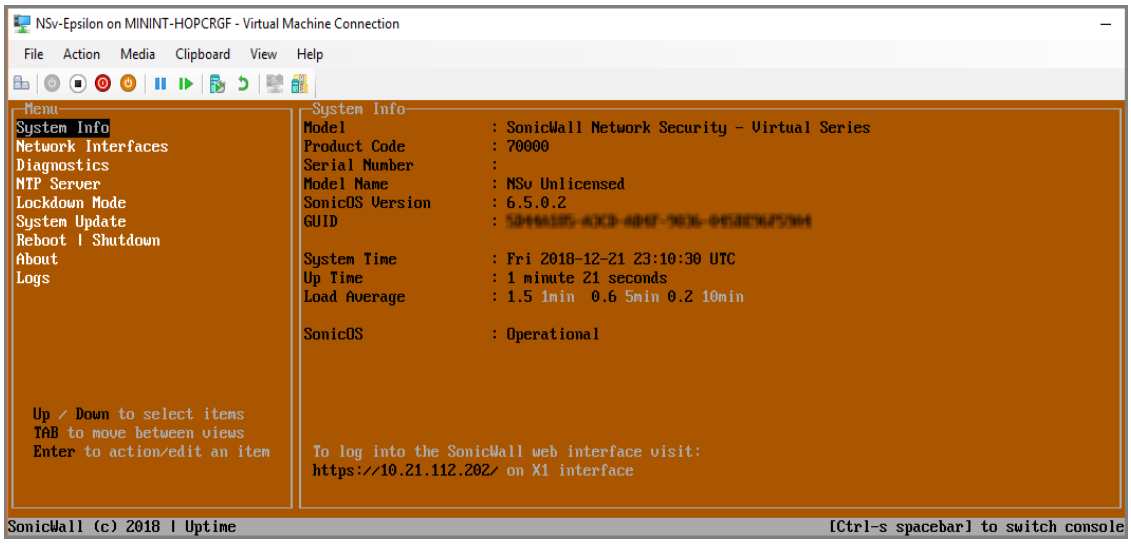


Some dialogs are for input:

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 NS*v* management menu choices are described in the following sections:

System Info



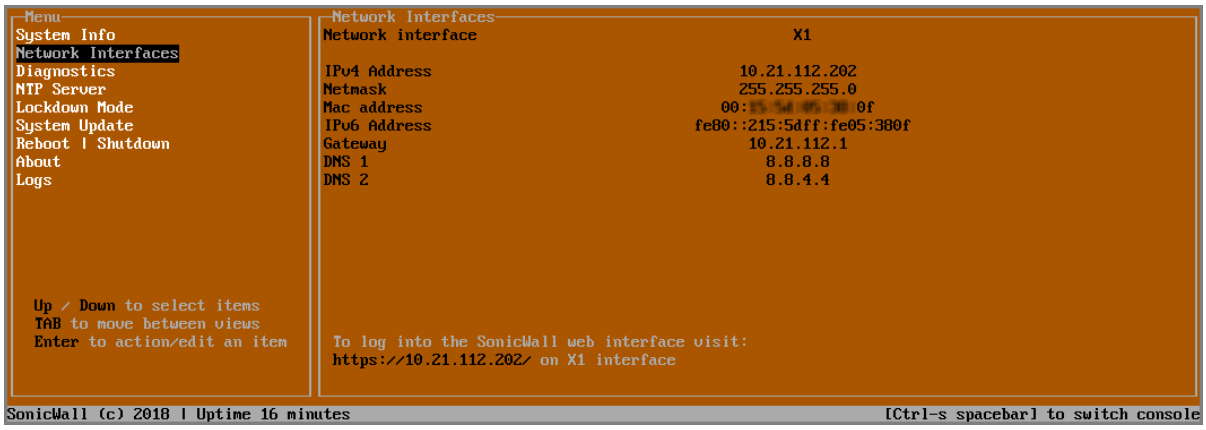
Some of the information in the **System Info** screen is dynamic. The following information is displayed:

- **Model** – This is the model of the NS*v* appliance.
- **Product code** – This is the product code of the NS*v* appliance.
- **Serial Number** – The serial number for the appliance; this is a number unique to every NS*v* instance deployed. This number can be used to identify the NS*v* appliance on MySonicWall.
- **Model Name** – This is the model name of the NS*v* appliance.
- **SonicOS Version** – This is the currently running SonicOS version of the NS*v* appliance.
- **GUID** – Every NS*v* instance has a GUID which is displayed here.
- **System Time** – This is the current system time on the NS*v* appliance.
- **Up Time** – This is the total time that the NS*v* appliance 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 NS*v*. ***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

The **Management Network** screen on an NSv deployed in KVM/QEMU displays:

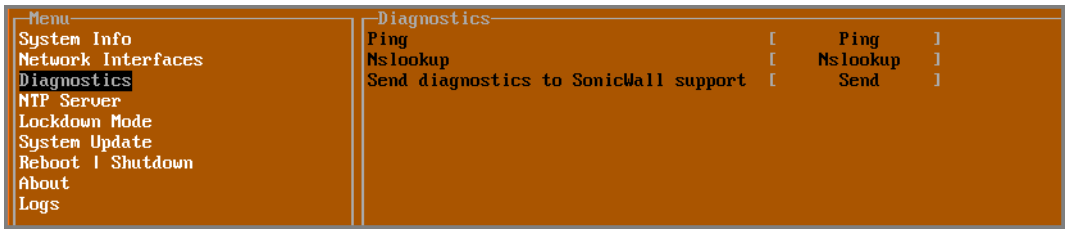
Network Interfaces screen



In these screens, 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 appliance.
- **DNS** – This is a list of the DNS servers currently being used by the NSv appliance.

Diagnostics



In the **Diagnostics** screen, you can run **ping** and **nslookup** tests as well as send diagnostics to SonicWall Technical Support.

The Send diagnositcs... option 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 appliance must have internet access to send the diagnostics report to SonicWall Support.

To use Ping:

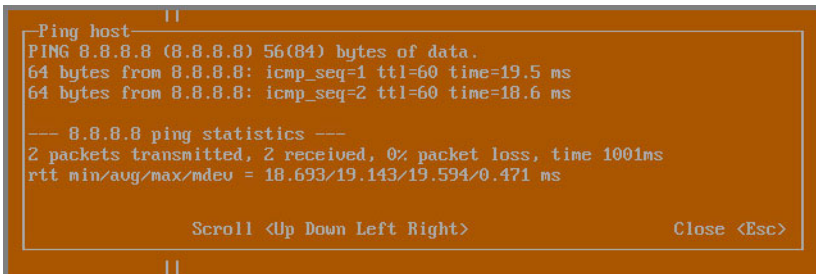
1 Select **Diagnostics** in the Menu and press **Tab** to move the focus into the **Diagnostics** screen.

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.

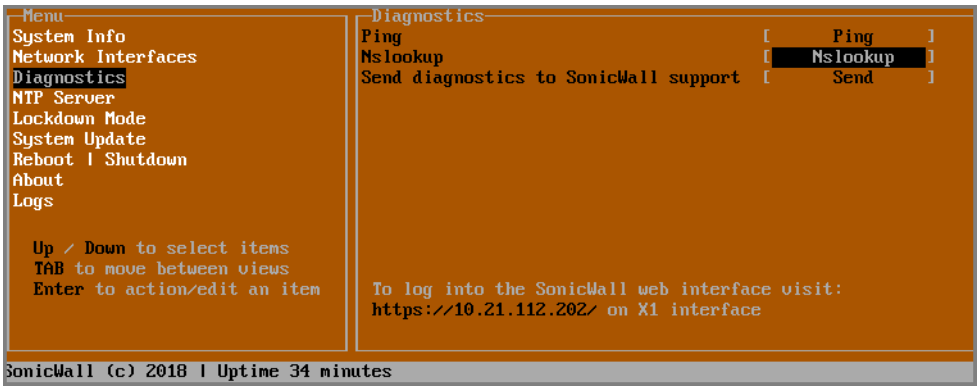


5 Press the **Esc** key to close the dialog.

To use Nslookup:

1 Select **Diagnostics** in the Menu and press **Tab** to move the focus into the **Diagnostics** screen.

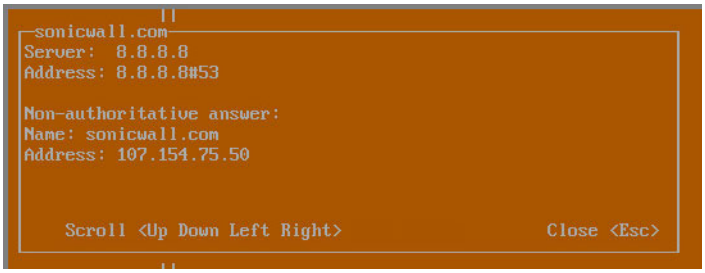
2 Select **Nslookup** to highlight it and press **Enter** to display the **Enter hostname** dialog.



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**.

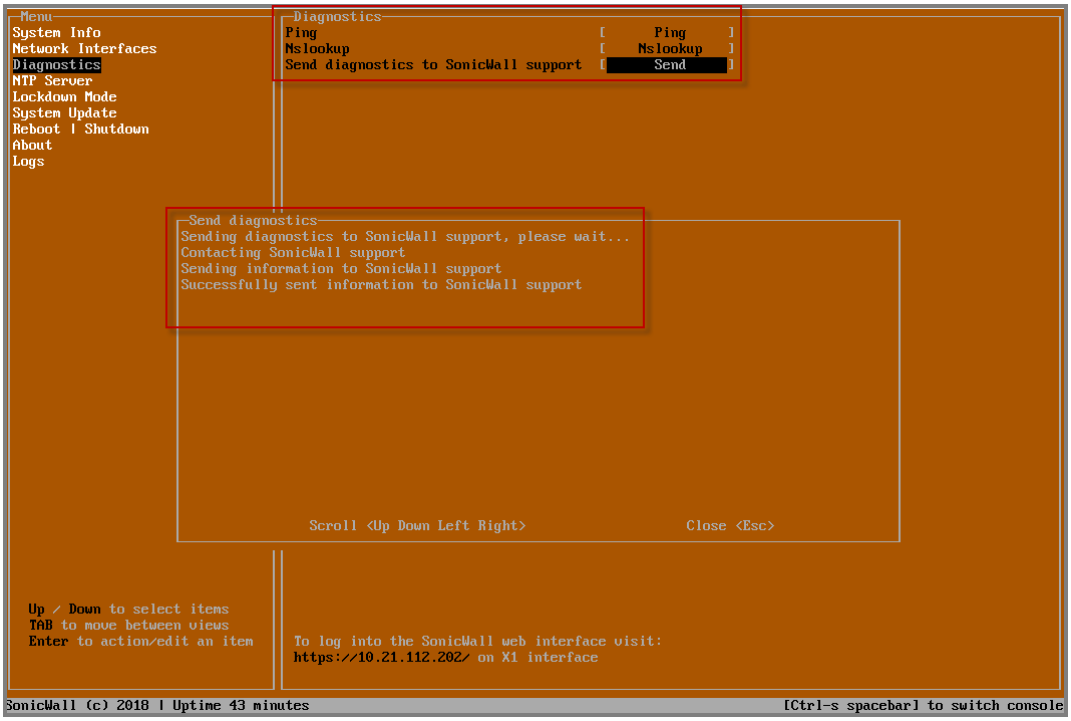
The Nslookup query results are displayed in an information dialog. You can scroll up and down within the dialog by using the up/down arrow keys.



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

To send the diagnostics report:

1 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.



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

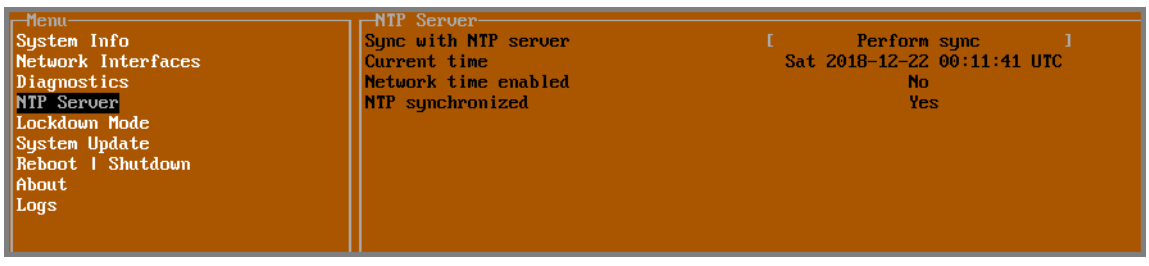
3 Any errors during the Send process are displayed in the **Send diagnostics** dialog box.

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

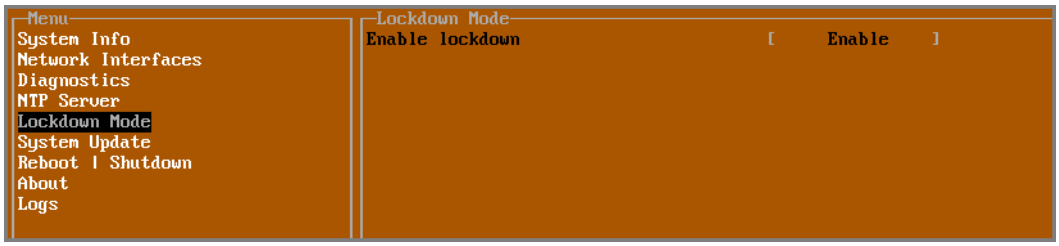


In the **NTP Server** screen, you can synchronize with an NTP server. For complete NTP Server configuration options, log into the SonicOS management interface and navigate to the **MANAGE | Appliance > System Time** page.

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

- **Sync with NTP server** – This button forces the NS*v* appliance's NTP client to perform a sync with the configured NTP server(s).
- **Current time** – The current time on the NS*v* appliance.
- **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 NS*v* appliance is currently synchronized with the configured NTP server(s).

Lockdown Mode



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.

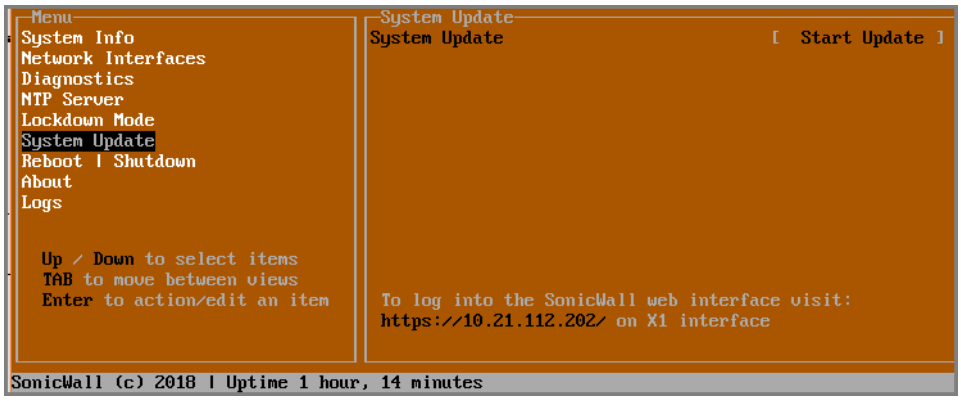
Temporary Lockdown Mode

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.

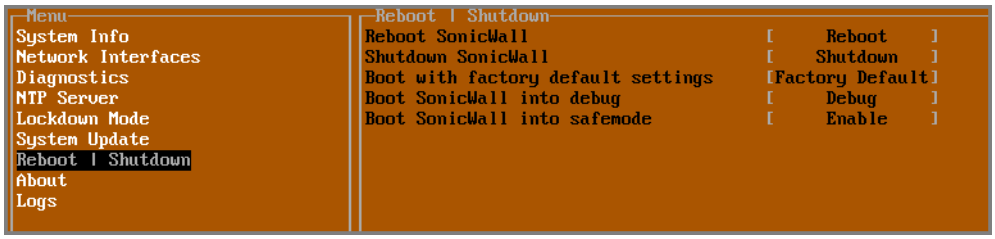
The management console will automatically be enabled/disabled a few seconds after it has been enabled/disabled in the SonicOS web interface page.

System Update

The **System Update** screen is available on NS*v*. This screen allows update of both the versions of SonicOS and SonicCore supporting NS*v*. Updates are announced via notification on MySonicWall. If an update is attempted, the management console will report if no updates are available.



Reboot | Shutdown



The **Reboot | Shutdown** screen provides functions for rebooting the NS*v* appliance, 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:

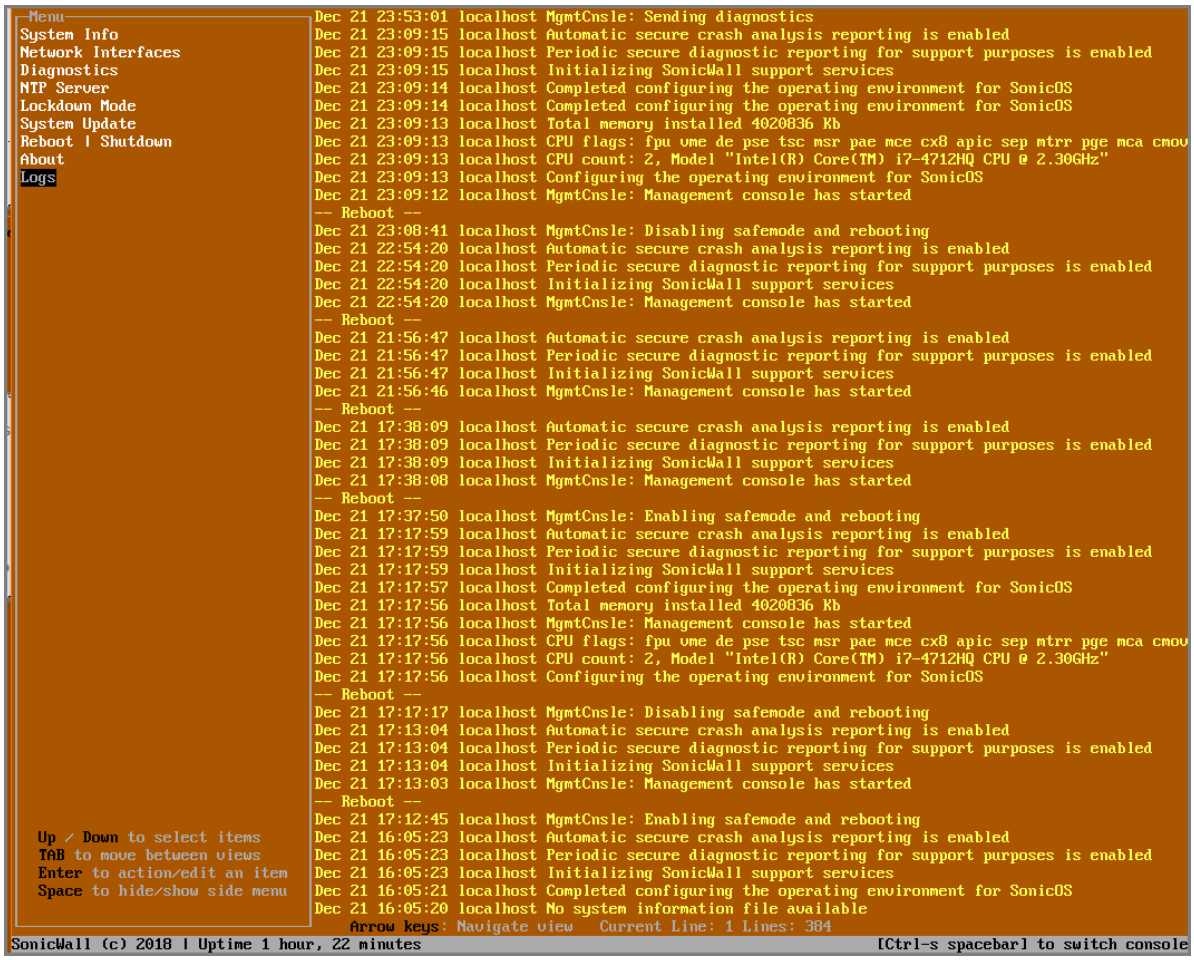
- **Reboot SonicWall** – Restarts the NS*v* Series KVM virtual appliance with current configuration settings.
- **Shutdown SonicWall** – Powers off the NS*v* Series KVM virtual appliance.
- **Boot with factory default settings** – Restarts the NS*v* Series KVM virtual appliance using factory default settings. All configuration settings will be erased.
- **Boot SonicWall into debug** – Restarts the NS*v* Series KVM virtual appliance into debug mode. Normally this operation is performed under the guidance of SonicWall Technical Support.
- **Boot SonicWall into safemode** – Puts the NS*v* Series KVM virtual appliance into SafeMode. For more information, see Using SafeMode on the NSv on page 46.

About

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

Logs

The **Logs** screen displays log events for the NS*v* appliance.



Using SafeMode on the NS*v*

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

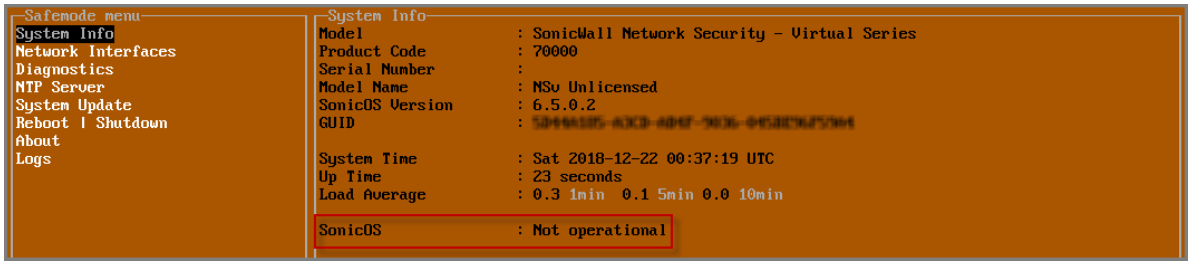
In SafeMode, some of the features the management console provides are different in the following ways:

- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

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

When the NS*v* 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.

The SafeMode Management Console always starts with the **System Info** screen.



NOTE: To exit SafeMode, disable it on the **Reboot | Shutdown** screen or deploy a new firmware image. See Disabling SafeMode on page 47 and Using the SafeMode Web Interface on page 51 for more information.

Topics:

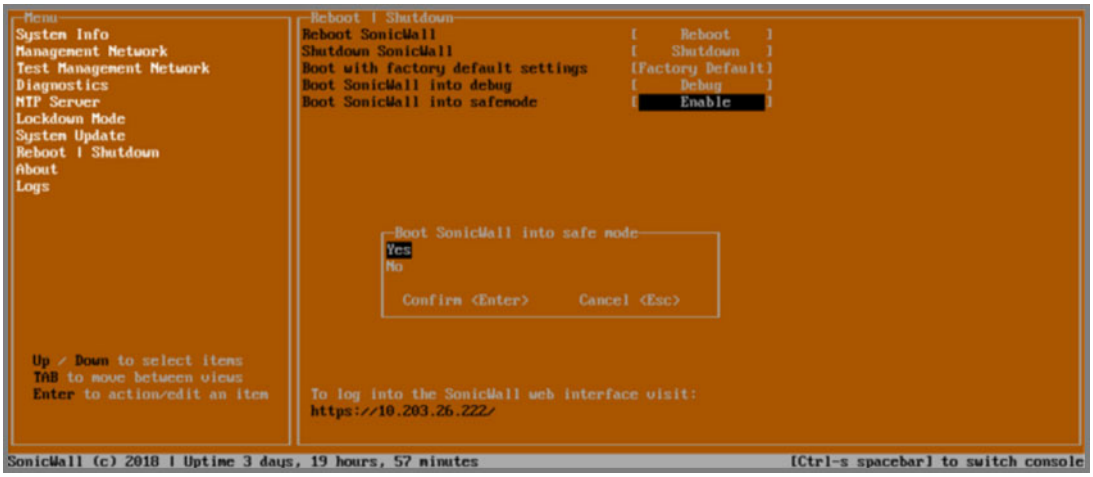
Enabling SafeMode

SafeMode can be enabled from the management console.

To enable SafeMode:

1. Access the NS*v* management console:
   - To connect to the management console using SSH: on page 35
   - To connect to the management console through the Virtual Machine Manager: on page 36
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 NS*v* immediately reboots and comes back up in SafeMode.

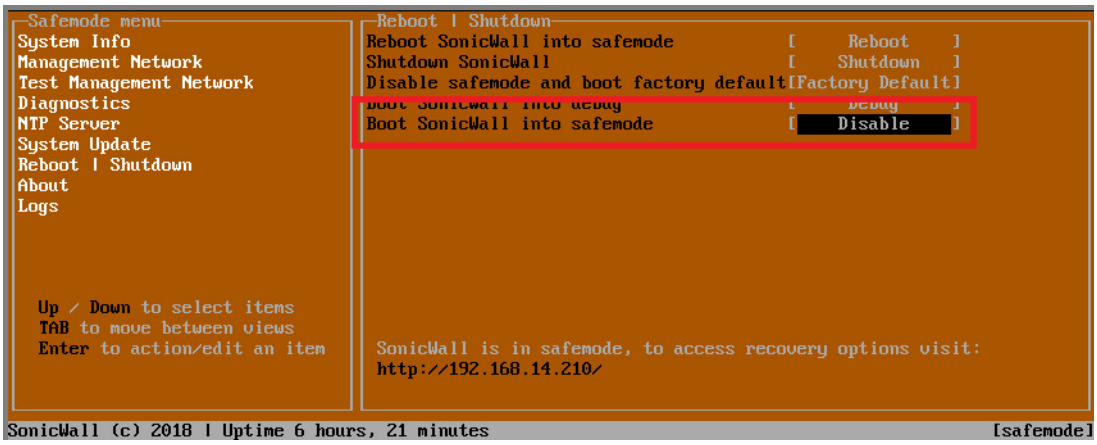
NOTE: In SafeMode, the web interface is served from an HTTP server. The HTTPS server is not started in SafeMode.

Disabling SafeMode

To disable SafeMode:

1 In the SafeMode menu in the NS*v* 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 NS*v* 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 NS*v* management console provides features to configure the NS*v* appliance interfaces:

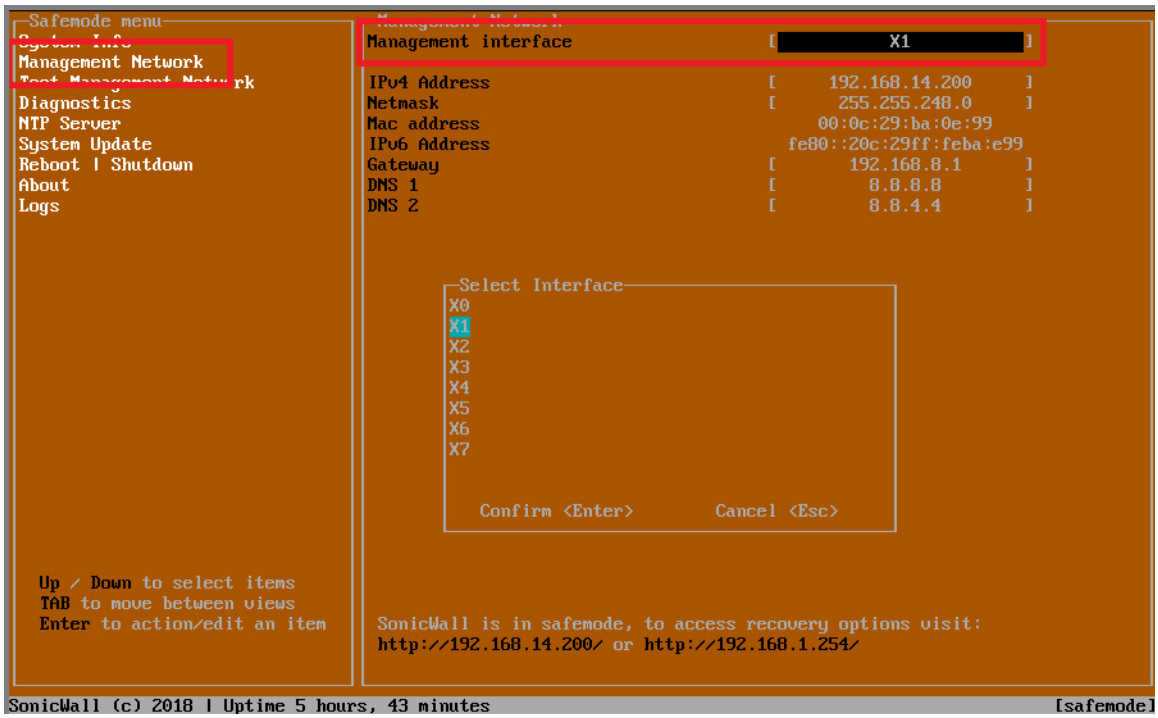
- **Management Interface** – This is the currently selected interface. This defaults to X1. Use this to select any of the NS*v* appliance interfaces.
- **IPv4 Address** – The current IPv4 address currently assigned to the Management Interface.
- **Netmask** – The current Netmask assigned to the Management 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 NS*v* appliance.
- **DNS** – A list of the current DNS servers currently being used by the NS*v* appliance.

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

Topics:

Configuring Interface Settings

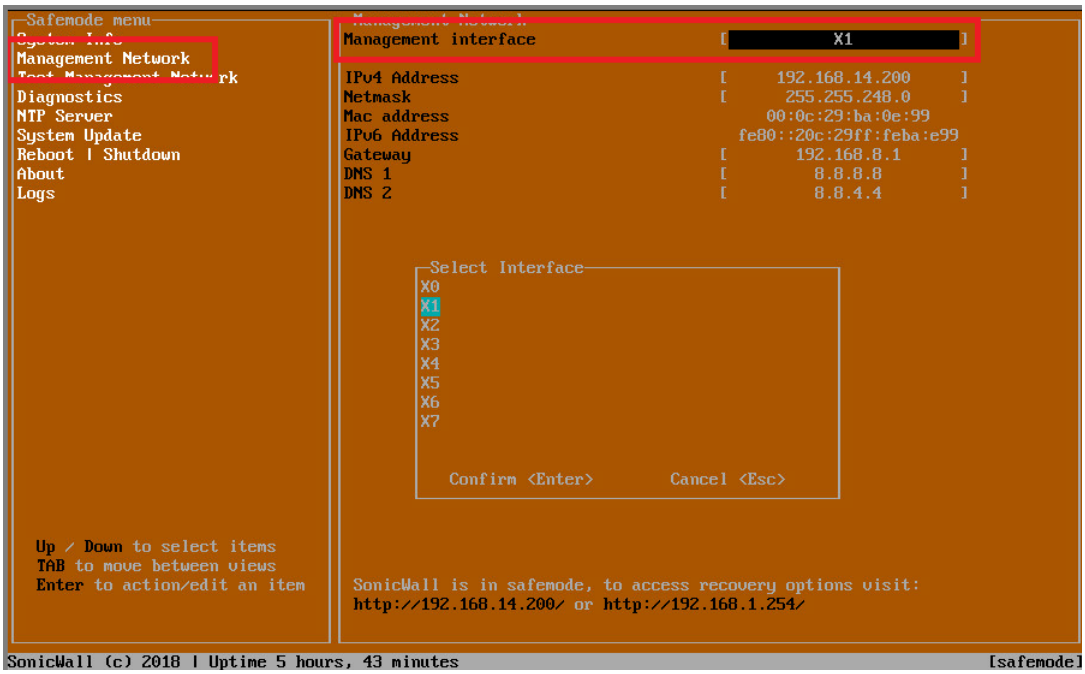
In SafeMode, the **Management Network** screen includes editable and actionable items which are read-only when the management console is in normal mode.



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 NS*v*.



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

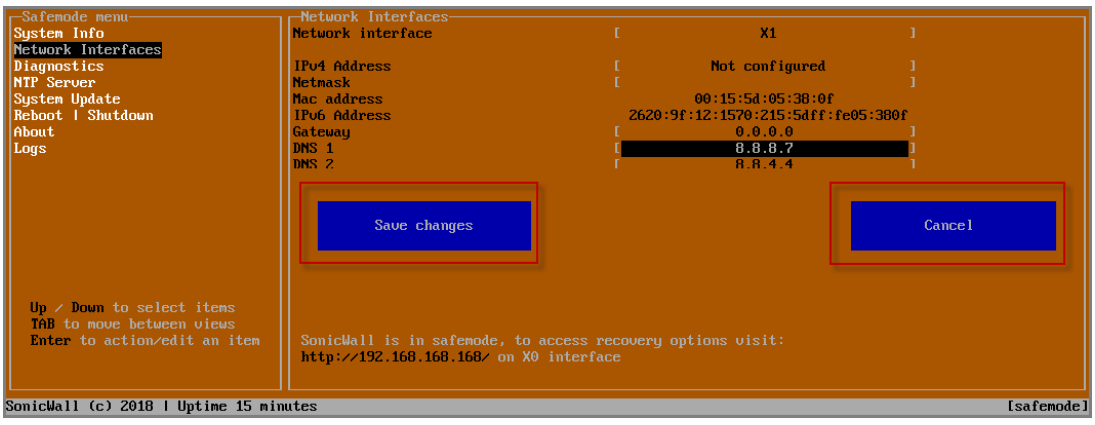
The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

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** and **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.

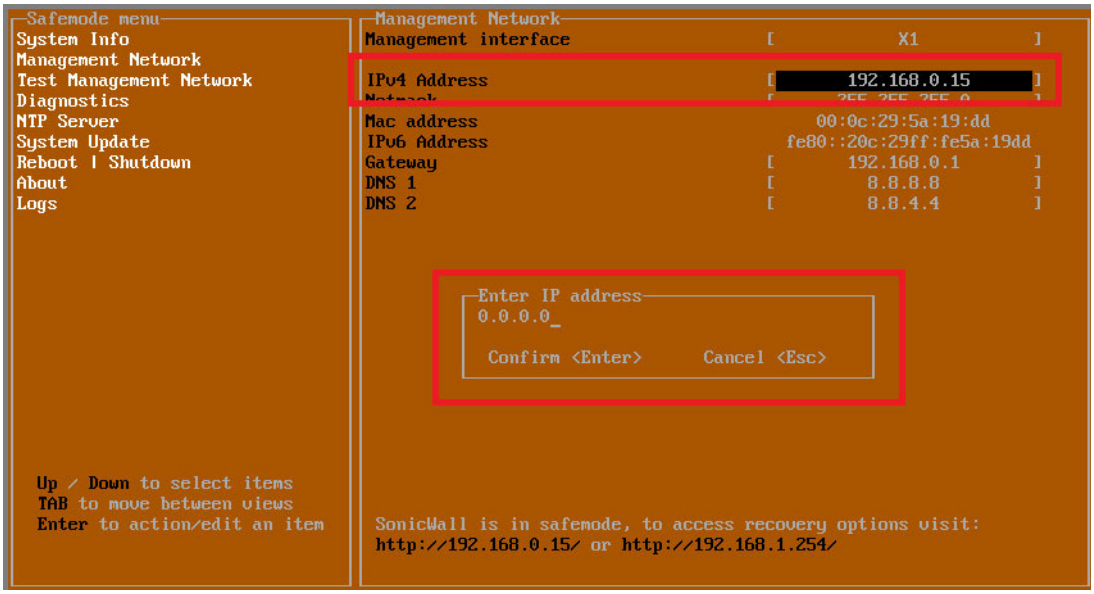
3 Select the interface you wish to edit and press **Enter**.

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

4 Select **IPv4 Address** and press **Enter**.

The on-screen dialog displays the current IP address.

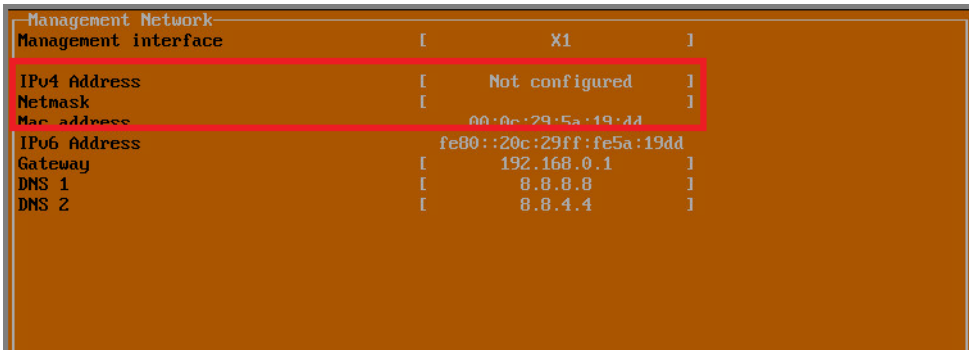
5 Navigate into the dialog and change the IP address to **0.0.0.0**, then press **Enter**.



The **Save changes** button is displayed.

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

The interface is disabled.



Using the SafeMode Web Interface

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

Topics:

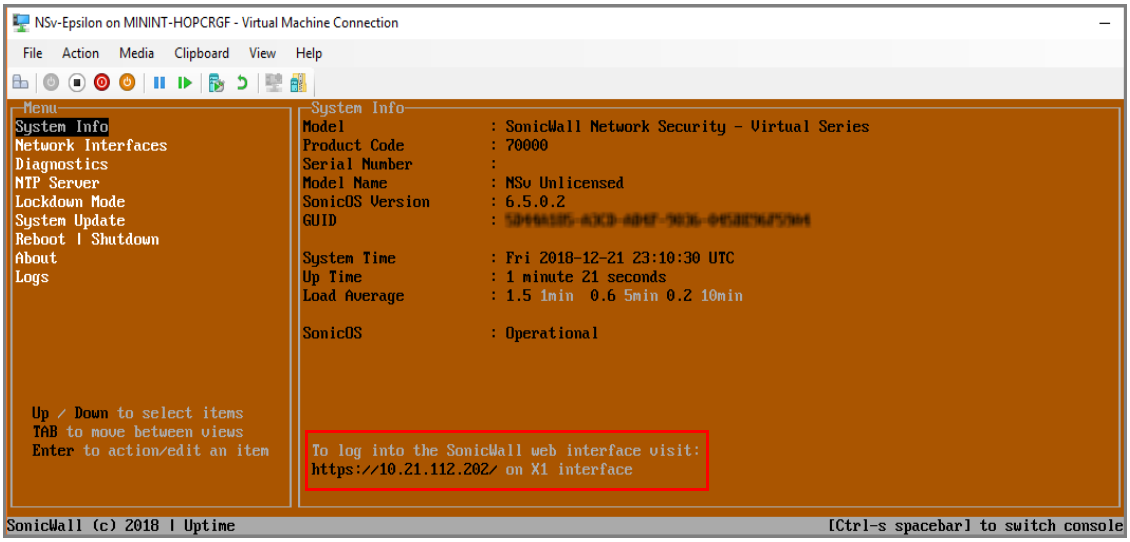
Accessing the SafeMode Web Interface

To access the SafeMode web interface:

1 You can access the SafeMode web interface at the public IP address of the NSv

NOTE: In SafeMode, the web management interface is only available via **http** (not **https**).

The web interface address is also given on the management console screen as shown below.



2 Go into the management console and boot into SafeMode. See Entering/Exiting SafeMode on page 52.

3 In a web browser, navigate to ***http://<NSv IP address>***, using the applicable IP address. The SafeMode web interface displays.

NOTE: You may want to switch browsers to ensure you log in to SafeMode via **http** (not **https**).

Entering/Exiting SafeMode

Enter SafeMode as described in Accessing the SafeMode Web Interface on page 51.

Exit by either uploading a new SonicOS images or by going to the management console and rebooting into normal mode (see Enabling SafeMode on page 46).

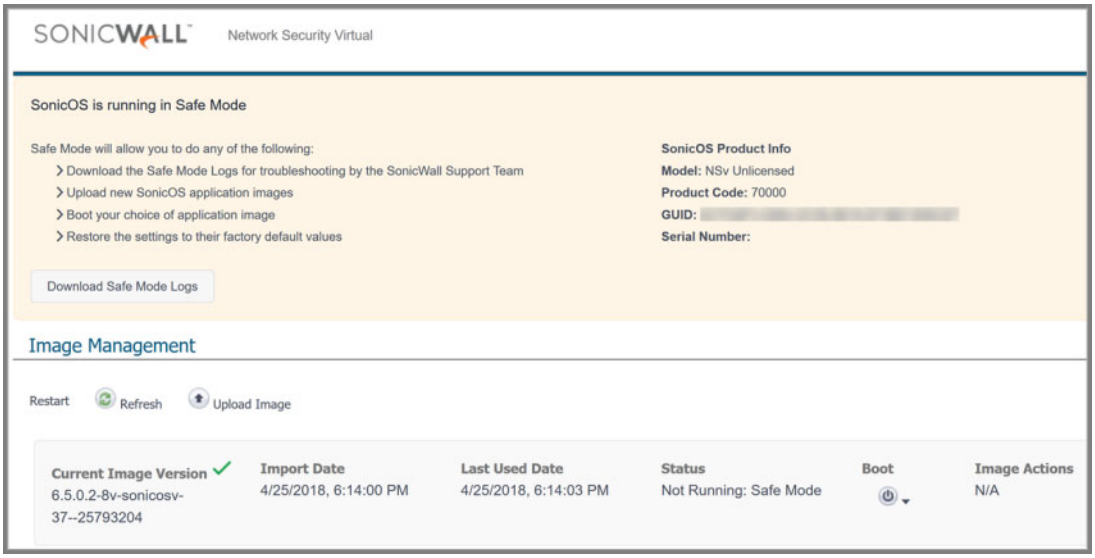
Downloading the SafeMode Logs

You can download logs of SafeMode activity.

NOTE: In SafeMode, the web management interface is only available via **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 the **Download Safe Mode Logs** button. A compressed file is downloaded which contains a number of files, including a ***console_logs*** file that contains detailed logging information.

Uploading a New Image in SafeMode

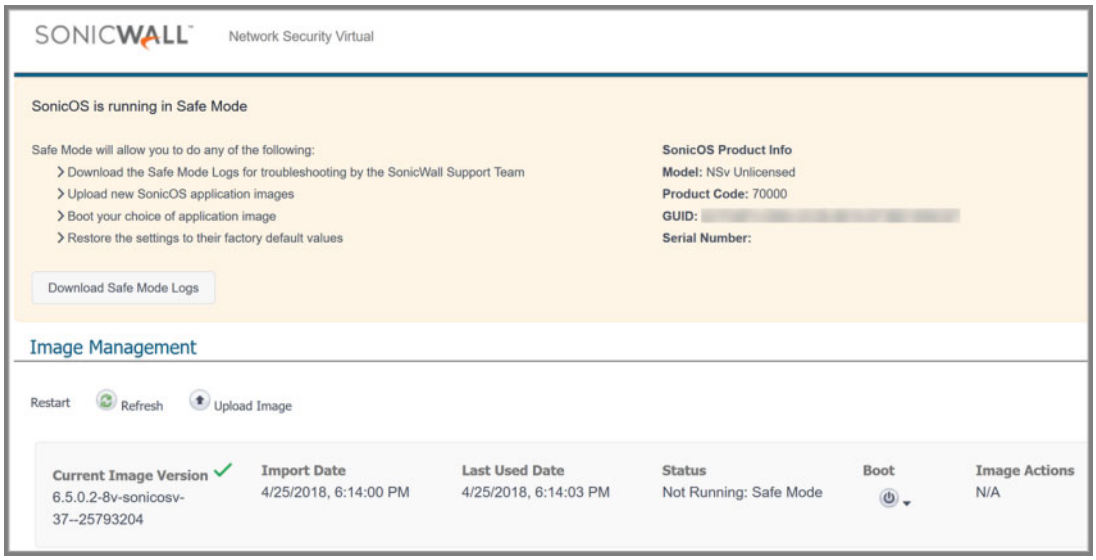
SWI files are used to upgrade SonicOS. You can download the latest SWI image file from MySonicWall. In SafeMode, you can upload a new SonicOS SWI image and apply it to the NS*v* appliance. The SafeMode web interface is used to perform an upgrade, rather than SafeMode in the NS*v* management console.

NOTE: In SafeMode, the web management interface is only available via **http** (not **https**).

To install a new SonicOS from SafeMode:

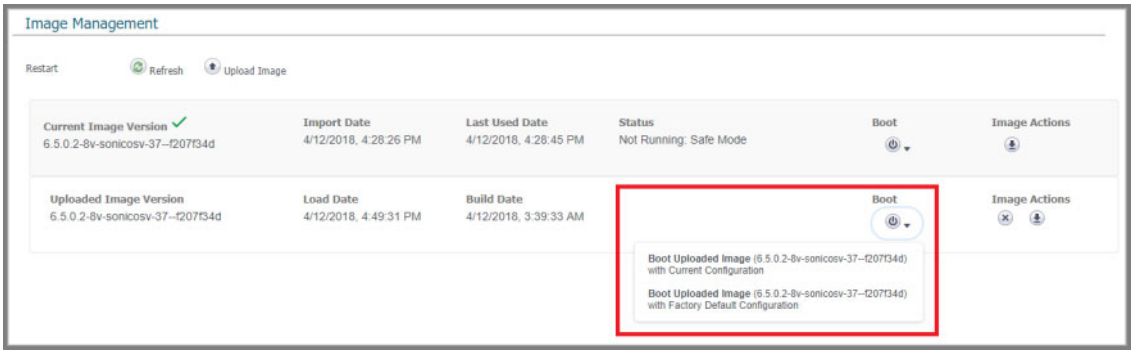
1 In the SafeMode web interface, click the **Upload Image** button to select an SWI file and then click **Upload** to upload the image to the appliance. A progress bar provides feedback on the file upload progress. Once

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 the **Boot** button and select one of the following:

- **Boot Uploaded Image with Current Configuration**
- **Boot Uploaded Image with Factory Default Configuration**



The NSv 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 MySonicWall
- 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

Legend

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

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

NSv Series KVM Getting Started Guide
Updated - June 2020
Software Version 6.5.4
232-004959-00 Rev B