



SonicWall® SonicOSX 7 NS_v Series on ESXi

Getting Started Guide

SONICWALL®

Contents

Introducing NSv Series	4
Feature Support Information	4
Node Counts Per Platform	7
Installation File / Supported Platforms	7
Hardware Compatibility	7
Support for SR-IOV	7
Product Matrix and Requirements	8
Backup and Recovery Information	8
Best Practices and Recommendations	9
High Availability Configurations	9
Exporting and Importing Firewall Configurations	10
Upgrading from SonicOS 6.5	10
Upgrading to a Higher Capacity NSv Model	10
Creating a MySonicWall Account	11
Installing NSv Series on ESXi	13
Obtaining the OVA from MySonicWall	13
Installing the NSv Appliance	14
Viewing and Editing Virtual Machine Settings	20
Troubleshooting Installation Configuration	22
Licensing and Registering Your NSv	26
Registering the NSv Appliance from SonicOS	26
SonicOS Management	28
Managing SonicOS on the NSv Series	28
Using System Diagnostics	29
Using the Virtual Console	30
Using the ESXi Remote Console to Configure the WAN or LAN Interfaces	30
Configuring SR-IOV	34
Using the NSv Management Console	48
System Info	50
Management Network	51
Test Management Network	51
Diagnostics	53
NTP Server	54
Lockdown Mode	54
Reboot Shutdown	55
About	55
Logs	56
Using SafeMode on the NSv	56
Enabling SafeMode	57
Disabling SafeMode	58

Configuring the Management Network in SafeMode	59
Installing a New SonicOS Version in SafeMode	62
Downloading Logs in SafeMode	63
SonicWall Support	64
About This Document	65

Introducing NS_v Series

This *SonicWall® SonicOSX 7 NSv Series on VMware ESXi Getting Started Guide* describes how to install SonicWall NSv on VMware ESXi and provides basic configuration information.

The SonicWall® Network Security Virtual Series (SonicWall® NSv Series) 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, SonicOSX 7 running on the NSv Series offers the same feature functionality and security features of a physical appliance, with comparable performance. SonicOSX Virtual is a fully featured 64-bit SonicOS 7 powered by SonicCore.

NOTE: vMotion is not supported.

Topics:

- [Feature Support Information](#) on page 4
- [Node Counts Per Platform](#) on page 7
- [Installation File / Supported Platforms](#) on page 7
- [Product Matrix and Requirements](#) on page 8
- [Backup and Recovery Information](#) on page 8
- [Best Practices and Recommendations](#) on page 9
- [High Availability Configurations](#) on page 9
- [Support for SR-IOV](#) on page 7
- [Exporting and Importing Firewall Configurations](#) on page 10
- [Upgrading to a Higher Capacity NSv Model](#) on page 10
- [Creating a MySonicWall Account](#) on page 11

Feature Support Information

The SonicWall NSv Series for VMware ESXi has nearly all the features and functionality of a SonicWall NSa hardware appliance running SonicOSX 7 firmware.

For information about supported features, go to the [technical publications portal](#).

The Feature Support List of NSv for ESXi table lists the key SonicOSX 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

Feature Support List

Functional Category	Feature Area	Feature
		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
		LiveCounters
	Managing views	
		Used/un-used rules
		Active/in-active rules
		Sections
		Customizable Grid/Layout
		Custom Grouping
TLS 1.3	Supporting TLS 1.3 with enhanced security	
SDWAN	SDWAN Scalability	

Feature Support List

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

Node Counts Per Platform

The supported node count varies by NSv platform. This is the maximum number of nodes/users that can connect to the NSv at any one time, and is displayed on the **System Status** page in the **MONITOR** view. 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 Hypervisor Versions
SonicOSX 7 for NSv Series	ESXi 6.7 and 7.0 or higher ¹

1. ESXi 6.5 or higher is recommended for production environments. The ESXi vswitch configuration should have the **MAC address changes** option enabled.

 **NOTE:** vMotion is not supported.

Hardware Compatibility

SonicWall NSv Series is supported on ESXi running on relatively modern chipsets, Intel Penryn and above (2008). If the chipset is too old, the installation will halt with the message, "This system does not support SSE4_1." For more information, see <https://kb.vmware.com/s/article/1005764>.

Support for SR-IOV

SonicWall NSv instances on VMware ESXi and on Linux KVM support Single-Root Input/Output Virtualization (SR-IOV). This feature allows a single PCI Express bus resource such as an SSD or NIC to be shared in a virtual environment. For details on configuration, see **Configuring SR-IOV** on page 34.

Product Matrix and Requirements

The following tables show the hardware resource requirements for the SonicWall NSv Series virtual appliances.

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

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

On NSv ESXi 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 below.

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

Backup and Recovery Information

In certain situations, it might be necessary to contact SonicWall Technical Support, use SafeMode, or deregister the NSv appliance:

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Please contact SonicWall Technical Support for assistance.
- If the disk is not recoverable, then the NSv appliance needs to be deregistered with MySonicWall. Contact technical support 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 56.
- 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 NSv model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall Technical Support for assistance.

Best Practices and Recommendations

- Configuration settings import is **not** supported from SonicWall physical appliances to NSv Series.
- SonicWall NSv Series supports the **vmxnet3** VMware Network Adapter Type. Exactly 8 virtual network interfaces (vNICs) are supported on each NSv platform. Adding and removing interfaces is supported, but the total must stay within the range of 2 to 8.
- To configure Virtual Interfaces in NSv on ESXi, map the NSv parent interface for the virtual interface to a port group with the VLAN ID 4095 (Trunk Port). ESXi treats a port group with VLAN 4095 as a Trunk Port.
- SonicWall recommends that you do **not** use the ESXi snapshot functionality. For more information, see <https://kb.vmware.com/s/article/1025279>.

High Availability Configurations

NSv virtual firewalls deployed on ESXi 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 may 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 failover 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, see [technical publications portal](#)

Exporting and Importing Firewall Configurations

Moving configuration settings from SonicWall physical appliances to the NSv Series is not supported. However, configuration settings may be moved from one SonicOSX 7 NSv to another. See the [technical publications portal](#) for more information about exporting and importing configuration settings.

Go to <https://www.sonicwall.com/support/technical-documentation/> and select “NSv Series” as the product.

Upgrading from SonicOS 6.5

SonicOS 7 NSv for VMware ESXi supports only fresh deployments. Under SonicOS 7, NSv supports only Unified Policy. Settings from SonicOS 6.5 NSv installations cannot be imported. Users must manually navigate policies, application rules, and content filtering rules for SonicOS 7 NSv installations.

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. Go to <https://www.sonicwall.com/support/technical-documentation/> and select “NSv Series” as the product.

For details on the number of process and memory to allocate to the VM to upgrade, refer to [Product Matrix and Requirements](#) on page 8.

To update the VM for processors and memory allocations, power-down the VM then right click on the VM and select "Edit Settings". The processor and memory settings then appear:

The screenshot shows the 'Edit Settings' dialog box for a VM. The 'Virtual Hardware' tab is selected. The settings are as follows:

Component	Value	Unit
CPU	2	
Memory	6	GB
Hard disk 1	50.080078125	GB
SCSI controller 0	LSI Logic Parallel	
Network adapter 1	10.203.26.X	
Network adapter 2	10.203.26.X	
Network adapter 3	10.203.26.X	
Network adapter 4	10.203.26.X	
Network adapter 5	10.203.26.X	

The CPU and Memory settings are highlighted with a red box. The 'ADD NEW DEVICE' button is in the top right. The 'CANCEL' and 'OK' buttons are at the bottom right.

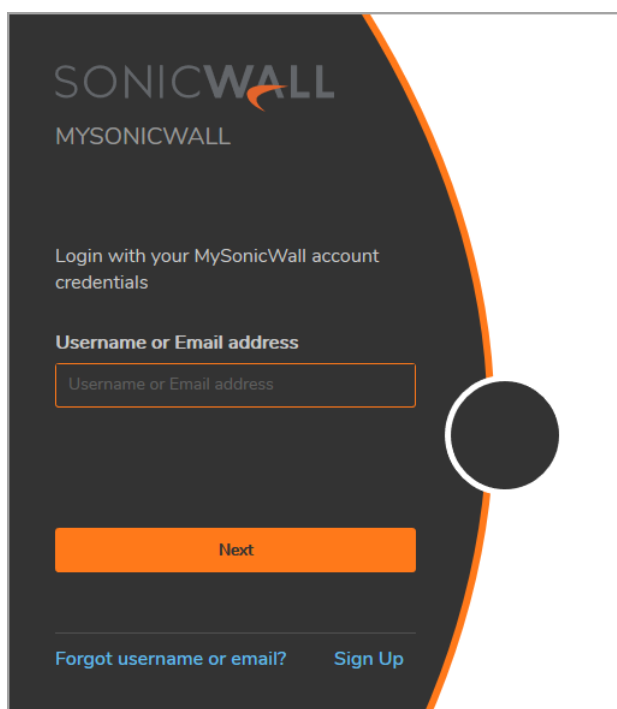
Creating a MySonicWall Account

A MySonicWall account is required to obtain the OVA file for initial installation of the NSv Series 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 NSv 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.
- 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 the code is scanned, you need only click a button.
- 6 Click on **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 NS_v Series on ESXi

Topics:

- [Obtaining the OVA from MySonicWall](#) on page 13
- [Installing the NSv Appliance](#) on page 14
- [Viewing and Editing Virtual Machine Settings](#) on page 20
- [Troubleshooting Installation Configuration](#) on page 22

Obtaining the OVA from MySonicWall

Refer to the purchase confirmation email for information about downloading the OVA files.

If you do not have a MySonicWall account, see [Creating a MySonicWall Account](#) on page 11 for information about creating one.

To perform initial registration and obtain the OVA file for deployment:

- 1 In a browser, log into your MySonicWall account.
- 2 Navigate to **My Products > Register Product**.
- 3 Fill in the **Serial Number**, **Friendly Name**, **Product Group**, and **Authentication Code** fields, and then click **Register**.

SONICWALL | MySonicWall

Register Product

Home

My Products

Product Management

Register Product

My Client Licenses

Free Trial Software

CFC Management

Get NFR Licenses

Bulk Activation

Bulk Activation Status

Register Anything

Add New

Fields marked by (*) are mandatory.

☒ Product ☐ Client Distribution Group

General Info

Serial Number: ? *

Friendly Name: SonicOS Virtual 209

Product Group: TechPubs Lab

Authentication Code: ?

Register

- 4 The **Registration Code** is displayed. Make a note of it.
You are now given access to the OVA file for your NSv model.
- 5 Download the OVA file and save it to your management computer.

You are now ready to deploy the OVA on your ESXi server. See [Installing the NSv Appliance](#) on page 14 for information.

After your NSv installation is complete, boot up SonicOS and log in. See [Managing SonicOS on the NSv Series](#) on page 28 for information.

Once you have connected and have internet access from the NSv, you must register your NSv Series instance using the **Registration Code** to complete the registration process. See [Registering the NSv Appliance from SonicOS](#) on page 26.

If your NSv is deployed in a closed network, see [Licensing and Registering Your NSv](#).

Installing the NS_v Appliance

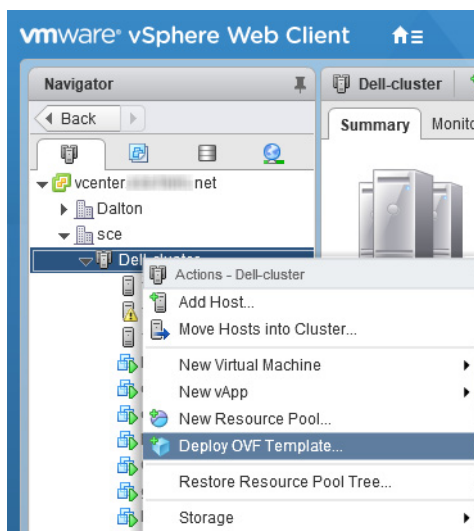
SonicWall NSv Series is installed by deploying an OVA file to your ESXi server. Each OVA file contains the software components needed. Deploy the OVA file by using the vSphere or vCenter client, which are available with ESXi.

NOTE: The elements of VMware must already be in place and the administrator must be familiar with the basics of deploying a virtual appliance on the ESXi server.

TIP: [Step 14](#) has some important information about selecting your networks. Even if you don't need all these step-by-step instructions, be sure to follow the instructions in [Step 14](#) to avoid connectivity issues after the deployment.

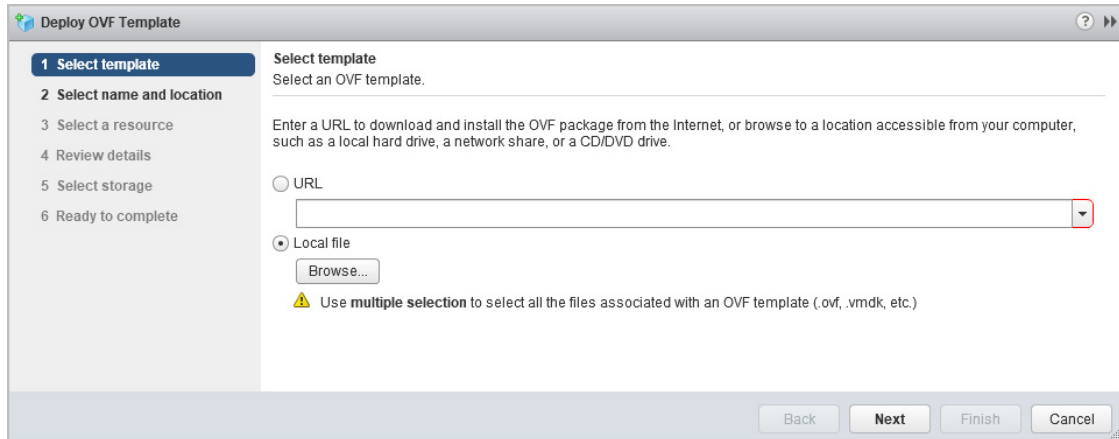
To perform a fresh install of NSv Series on ESXi:

- 1 Download the NSv Series OVA file from MySonicWall to a computer with vSphere / vCenter access.
- 2 Access vSphere or vCenter and log on to your ESXi server.
- 3 Navigate to the location where you want to install the virtual machine, and select the folder.
- 4 To begin the import process, click **Actions** and select **Deploy OVF Template**.



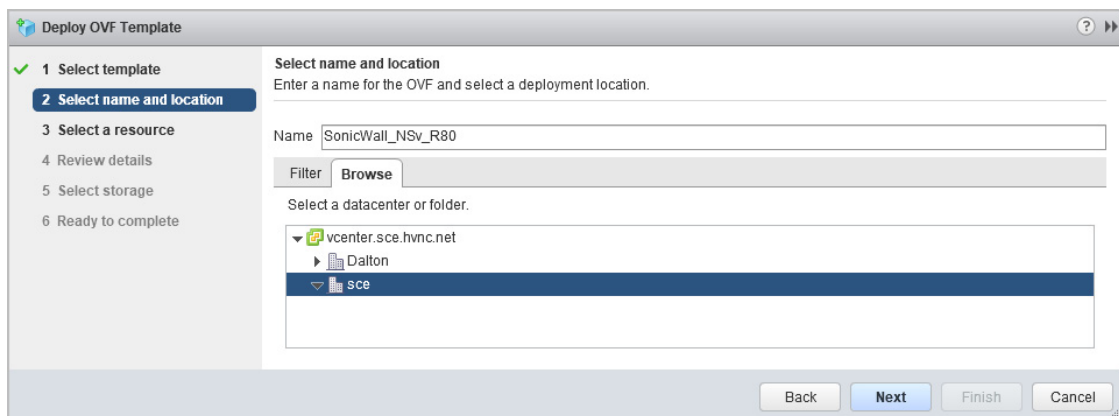
5 In the **Select template** screen, select **Local file**:

- **Local file** – Click **Browse** and navigate to the NSv Series OVA file that you previously downloaded.



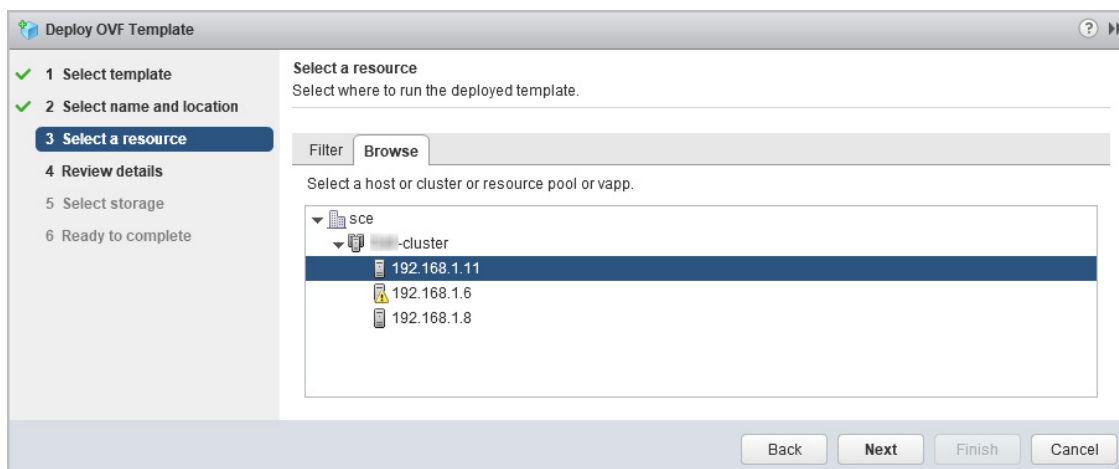
6 Click **Next**.

7 In the **Select name and location** screen, type a descriptive name for the NSv appliance into the **Name** field, and then select the location for it from the ESXi folder structure.



8 Click **Next**.

9 In the **Select a resource** screen, click **Next** to accept the default resource for the selected folder, or select a different resource and then click **Next**. Wait while the resource is validated. This is the resource pool where you want to deploy the template.



10 In the **Review details** screen, verify the template details and then click **Next**.

The screenshot shows the 'Deploy OVF Template' wizard at the 'Review details' step. The left sidebar lists steps 1 through 9, with '4 Review details' highlighted. The main area is titled 'Review details' and contains the instruction 'Verify the template details.' Below this is a table of template information:

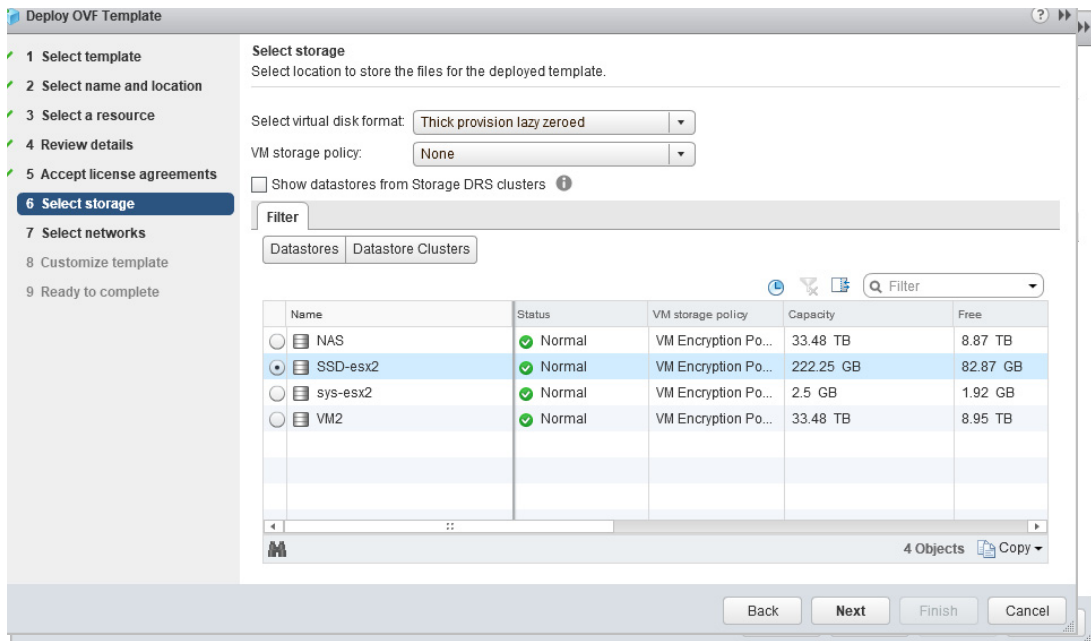
Publisher	✓ SonicWall Inc. (Trusted certificate)
Download size	1.0 GB
Size on disk	1.6 GB (thin provisioned) 66.3 GB (thick provisioned)
Description	SonicWall_NSv_R80

At the bottom of the wizard are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

11 In the **Accept license agreements** screen, read the agreement, click **Accept** and then click **Next**.

The screenshot shows the 'Deploy OVF Template' wizard at the 'Accept license agreements' step. The left sidebar lists steps 1 through 9, with '5 Accept license agreements' highlighted. The main area is titled 'Accept license agreements' and contains the instruction 'Read and accept the license agreements associated with this template before continuing.' Below this is a scrollable text area containing the 'SonicWall End User Product Agreement'. The agreement text includes a disclaimer and definitions for 'Affiliate', 'Appliance', and 'Documentation'. An 'Accept' button is located at the bottom left of the text area. At the bottom of the wizard are four buttons: 'Back', 'Next', 'Finish', and 'Cancel'.

- 12 In the **Select storage** screen, first select a datastore from the table. This is the location where you want to store the virtual machine files.



- 13 Leave the default settings for the datastore provisioning and click **Next**. The default is **Thick Provision Lazy Zeroed**.
- 14 In the **Select networks** screen, **first sort the list of interfaces** by clicking the **Source Network** column heading. Then select the vswitch networks that are mapped to the NSv appliance interfaces. The source networks are the NSv appliance interfaces (X0, X1, X2, X3, X4, X5, X6, X7), and the destination networks are the vswitch ports of your existing vswitch network configuration. If your vswitch networks are not fully configured, you can further adjust the interface/vswitch port pairs after the import.

NOTE: The ESXi vswitch configuration should have the option for **MAC address changes** enabled for the vswitch ports connected to the NSv.

For advanced configurations (DVS), consult the ESXi documentation on vswitch configuration.

Typically, the NSv Series is deployed between your internal network and a network with internet access, and therefore you map the source **X0** to your LAN network (vswitch port), and map the source **X1** to the WAN network (vswitch port) with connectivity to the internet.

IMPORTANT: **SONICOS_X1** (the default WAN Interface) is set to **DHCP** by default, with **HTTPS management** enabled for the NSv Series, as this configuration eases deployments in virtual/cloud environments.

NOTE: System defaults for the X0 and X1 interfaces are:

- X0 – Default LAN – 192.168.168.168
- X1 – Default WAN – DHCP addressing, with HTTPS and Ping management enabled

NOTE: Configuration settings import from physical firewalls to the NSv Series is not supported.

Deploy OVF Template

- 1 Select template
- 2 Select name and location
- 3 Select a resource
- 4 Review details
- 5 Accept license agreements
- 6 Select storage
- 7 Select networks**
- 8 Customize template
- 9 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
SONICOS_X0	VLAN 4 - DMZ
SONICOS_X6	VLAN 4 - DMZ
SONICOS_X5	VLAN 4 - DMZ
SONICOS_X7	VLAN 4 - DMZ
SONICOS_X2	VLAN 4 - DMZ
SONICOS_X1	VLAN 4 - DMZ
SONICOS_X4	VLAN 4 - DMZ
SONICOS_X3	VLAN 4 - DMZ

IP Allocation Settings
IP protocol: IPv4 IP allocation: Static - Manual ⓘ

Back Next Finish Cancel

Deploy OVF Template

- 1 Select template
- 2 Select name and location
- 3 Select a resource
- 4 Review details
- 5 Accept license agreements
- 6 Select storage
- 7 Select networks**
- 8 Customize template
- 9 Ready to complete

Select networks
Select a destination network for each source network.

Source Network	Destination Network
SONICOS_X0	VLAN 2 - main
SONICOS_X6	VLAN 100
SONICOS_X5	VLAN 100
SONICOS_X7	VLAN 100
SONICOS_X2	VLAN 100
SONICOS_X1	VLAN 4 - DMZ
SONICOS_X4	VLAN 100
SONICOS_X3	VLAN 100

Description - SONICOS_X1
SonicOS X1 Interface (Default: DHCP)

IP Allocation Settings
IP protocol: IPv4 IP allocation: Static - Manual ⓘ

Back Next Finish Cancel

15 Click **Next**.

- 16 In the **Ready to complete** screen, review the settings and click **Finish** to create the NSv appliance. To change a setting, click **Back** to navigate back through the screens to make a change.

Deploy OVF Template

Ready to complete
Review configuration data.

Name	SonicWall NSV
Source VM name	SonicWall_NSv_R80
Download size	1.0 GB
Size on disk	66.3 GB
Datacenter	sce
Resource	192.168.1.11
Storage mapping	1
Network mapping	8
IP allocation settings	IPv4, Static - Manual
Properties	SonicCore Hostname = SonicWall NSv

Back Next Finish Cancel

The name of the new NSv appliance appears in the left pane of the vSphere or vCenter window when complete.

The next step is to power on your NSv virtual firewall in the vSphere or vCenter interface. See [Viewing and Editing Virtual Machine Settings](#) on page 20 for information about powering on your NSv and related topics.

Once your NSv virtual firewall is powered on, the next step is to register it on MySonicWall. See [Registering the NSv Appliance from SonicOS](#) on page 26 for information about registering your NSv.

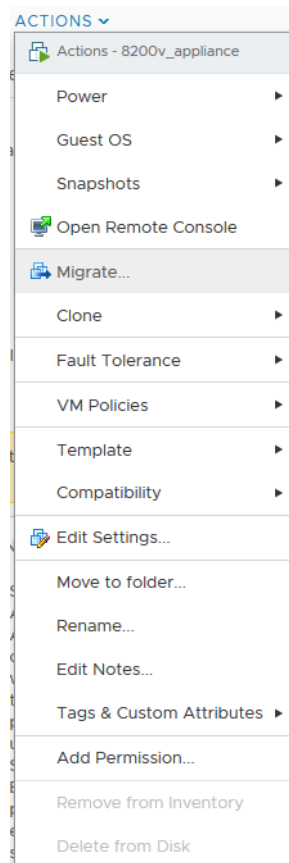
Other related topics are:

- [Managing SonicOS on the NSv Series](#) on page 28
- [Using System Diagnostics](#) on page 29
- [Using the Virtual Console](#) on page 30

Viewing and Editing Virtual Machine Settings

When logged into vSphere or vCenter, you can view and edit some basic information for your NSv Series instance.

With your NSv Series instance selected in the left pane, click **ACTIONS** to view the options.



Select **Power** to choose from **Power On**, **Power Off**, **Shut Down Guest OS**, **Restart Guest OS**, and other options.

Select **Open Remote Console** to launch the same *ESXi Remote Console* that you get with the **Launch Remote Console** link on the **Summary** screen.

Select **Edit Settings** to open the Edit Settings dialog where you can access settings for the number of CPUs, Memory size, Hard disk size, Network adapters, and other items in the ESXi configuration for this NSv Series instance.

Edit Settings | NSA_Virtual_288

Virtual Hardware | VM Options

[ADD NEW DEVICE](#)

> CPU	2		
> Memory	8	GB	
> Hard disk 1	68.4140625	GB	
> SCSI controller 0	LSI Logic Parallel		
> Network adapter 1	sonicosv_x0		<input checked="" type="checkbox"/> Connected
> Network adapter 2	10.203.26.X		<input checked="" type="checkbox"/> Connected
> Network adapter 3	sonicosv_x2		<input checked="" type="checkbox"/> Connected
> Network adapter 4	sonicosv_x3		<input checked="" type="checkbox"/> Connected
> Network adapter 5	sonicosv_x4		<input checked="" type="checkbox"/> Connected

[CANCEL](#) [OK](#)

The ESXi Network adapters are mapped to the NSv Series interfaces as follows:

Network Adapters to NSv Series Interfaces Mapping

Network Adapter #	NSv Series Interface	Default IP	Default Zone
Network adapter 1	x0	192.168.168.168	LAN
Network adapter 2	x1	DHCP	WAN
Network adapter 3	x2	N/A	LAN
Network adapter 4	x3	N/A	LAN
Network adapter 5	x4	N/A	LAN
Network adapter 6	x5	N/A	LAN
Network adapter 7	x6	N/A	LAN
Network adapter 8	x7	N/A	LAN

Troubleshooting Installation Configuration

If the NSv fails to come up, follow the instruction in [Configuring SR-IOV](#) on page 34 to go to the NSv Management Console window or the SonicOSX CLI window. Check the boot messages:

NOTE: The error messages shown below indicate that the virtual firewall cannot boot.

Insufficient Memory Assignment

The following messages will appear if the virtual machine has insufficient memory. This may occur when doing an NSv installation or a NSv product upgrade.

SonicOSX boot message:

Insufficient memory 4 GB, minimum memory required 10 GB for NSv model: "NSv 800 Beta"
Power off the Network Security virtual appliance and assign 10 GB to this virtual appliance.

This message can also appear in the Management Console logs as shown in the two following screen shots.

```
Mar 30 15:10:39 localhost Initializing SonicWall support services
Mar 30 15:10:39 localhost Completed configuring the operating environment for SonicOS
Mar 30 15:10:08 localhost Insufficient memory 4 GB, minimum memory required 10 GB.
Mar 30 15:10:08 localhost Insufficient memory 4 GB, minimum memory required 10 GB.
Mar 30 15:10:07 localhost Total memory installed 4160984 Kb
Mar 30 15:10:07 localhost CPU flags: fpu_ume de psc tsc mcr pae mce cx8 apic sep mtrr pge mca
Mar 30 15:10:07 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 15:10:07 localhost Configuring the operating environment for SonicOS
Mar 30 15:06:37 localhost Initializing SonicWall support services
Mar 30 15:06:36 localhost Completed configuring the operating environment for SonicOS
Mar 30 15:06:06 localhost Insufficient memory 4 GB, minimum memory required 10 GB.
Mar 30 15:06:05 localhost Total memory installed 4160984 Kb
Mar 30 15:06:05 localhost CPU flags: fpu_ume de psc tsc mcr pae mce cx8 apic sep mtrr pge mca
Mar 30 15:06:05 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 15:06:05 localhost Configuring the operating environment for SonicOS
Mar 30 15:02:31 localhost Unconfigure the operating environment for SonicOS
Mar 30 15:02:31 localhost Initializing SonicWall support services
Mar 30 15:02:31 localhost Completed configuring the operating environment for SonicOS
Mar 30 15:02:01 localhost Insufficient memory 4 GB, minimum memory required 10 GB.
Mar 30 15:02:01 localhost Total memory installed 4160984 Kb
Mar 30 15:02:00 localhost CPU flags: fpu_ume de psc tsc mcr pae mce cx8 apic sep mtrr pge mca
Mar 30 15:02:00 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 15:02:00 localhost Configuring the operating environment for SonicOS
Mar 30 15:01:48 localhost Unconfigure the operating environment for SonicOS
Mar 30 14:59:55 localhost Initializing SonicWall support services
Mar 30 14:59:54 localhost Completed configuring the operating environment for SonicOS
Mar 30 14:59:24 localhost Insufficient memory 4 GB, minimum memory required 10 GB.
Mar 30 14:59:24 localhost Total memory installed 4160984 Kb
Mar 30 14:59:24 localhost CPU flags: fpu_ume de psc tsc mcr pae mce cx8 apic sep mtrr pge mca
Mar 30 14:59:24 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 14:59:24 localhost Configuring the operating environment for SonicOS
Mar 30 14:59:11 localhost Unconfigure the operating environment for SonicOS
Mar 30 14:54:57 localhost Initializing SonicWall support services
Mar 30 14:54:56 localhost Completed configuring the operating environment for SonicOS
Mar 30 14:54:26 localhost Insufficient memory 4 GB, minimum memory required 10 GB.
Mar 30 14:54:26 localhost Total memory installed 4160984 Kb
Mar 30 14:54:26 localhost CPU flags: fpu_ume de psc tsc mcr pae mce cx8 apic sep mtrr pge mca
Mar 30 14:54:26 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 14:54:25 localhost Configuring the operating environment for SonicOS
Mar 30 14:54:12 localhost Unconfigure the operating environment for SonicOS
Mar 30 14:47:18 localhost Initializing SonicWall support services
```

NOTE: For details on navigating the NSv Management Console to troubleshoot the installation, see [Configuring SR-IOV](#) on page 34.

Memory may be insufficient without a insufficient memory log entry:

```
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
Space to hide/show side menu

Mar 30 14:44:14 localhost Initializing SonicWall support services
Mar 30 14:44:12 localhost Completed configuring the operating environment for SonicOS
Mar 30 14:44:12 localhost Completed configuring the operating environment for SonicOS
Mar 30 14:44:11 localhost This NSv model supports 8 CPU, current CPU count is only 2, for impr
Mar 30 14:44:11 localhost Total memory installed 8172912 Kb
Mar 30 14:44:11 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 14:44:11 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 14:44:11 localhost Configuring the operating environment for SonicOS
-- Reboot --
Mar 30 14:43:58 localhost Unconfigure the operating environment for SonicOS
Mar 30 14:39:40 localhost support services, failed to contact
Mar 30 14:35:19 localhost Initializing SonicWall support services
Mar 30 14:35:18 localhost Completed configuring the operating environment for SonicOS
Mar 30 14:35:17 localhost No system information file available
Mar 30 14:35:17 localhost Total memory installed 8172916 Kb
Mar 30 14:35:17 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 14:35:17 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 14:35:17 localhost Configuring the operating environment for SonicOS

Arrow keys: Navigate view Current Line: 1 Lines: 18
```

Incompatible CPU

If the CPU does not support AES instructions the following message will appear:

CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz is not supported by SonicWall Network Security Virtual

CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does not support the Advanced Encryption Standard(AES) instructions

Refer to Getting Started Guide and install the SonicWall Network Virtual on a supported platform

The message can also be seen in the logs provided by the management console:

```
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
Space to hide/show side menu

Mar 30 16:56:01 localhost Initializing SonicWall support services
Mar 30 16:56:00 localhost Completed configuring the operating environment for SonicOS
Mar 30 16:56:00 localhost This NSv model supports 8 CPU, current CPU count is only 2, for impr
Mar 30 16:56:00 localhost Total memory installed 8099184 Kb
Mar 30 16:55:15 localhost CPU model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does not support
Mar 30 16:55:15 localhost CPU model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does not support
Mar 30 16:55:15 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 16:55:15 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 16:55:15 localhost Configuring the operating environment for SonicOS
-- Reboot --
Mar 30 16:55:01 localhost Unconfigure the operating environment for SonicOS
Mar 30 16:50:29 localhost Initializing SonicWall support services
Mar 30 15:20:32 localhost This NSv model supports 8 CPU, current CPU count is only 2, for impr
Mar 30 15:20:32 localhost Total memory installed 8099184 Kb
Mar 30 15:20:32 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 15:20:32 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 15:20:31 localhost Configuring the operating environment for SonicOS
-- Reboot --
Mar 30 15:10:39 localhost Initializing SonicWall support services

Arrow keys: Navigate view Current Line: 1 Lines: 140
```

If the CPU does not support SSE 4.1 or 4.2 instructions the following message will appear:

CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz is not supported by SonicWall Network Security Virtual

CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does support SSE 4.1 or 4.2 instructions

Refer to Getting Started Guide and install the SonicWall Network Virtual on a supported platform

Incorrect CPU Configuration

All cores must be on the same socket. Customer needs to change the CPU configuration in settings.

The SonicWall Network Security requires all virtual CPU to reside on a single socket. Power down the virtual machine and adjust the CPU configuration such that all CPU reside on the same socket

NOTE: The above error may occur when EVC masks the CPU capability.
<https://communities.vmware.com/thread/536227> resolution is to disabled EVC.

Insufficient Resources at Time of Configuration

If the ESXi infrastructure where the NSv is being installed has poor performance the following message may appear at time of installation:

```
*****
Initializing services: IMPORTANT, DO NOT POWEROFF OR REBOOT
                        -- Warning --
This initialization is taking longer than expected.
Please ensure sufficient compute resources are available to the SonicWall Network Security
Virtual.
*****
```

If the above message occurs during initialization, more information is available in the logs:

System Info	Apr 02 16:18:27 localhost This initialization process is taking longer than expected, load avg ge: 1.10, time: 250 seconds
Management Network	Apr 02 16:18:26 localhost This initialization process is taking longer than expected, load avg ge: 1.10, time: 249 seconds
Test Management Network	Apr 02 16:18:25 localhost This initialization process is taking longer than expected, load avg ge: 1.10, time: 248 seconds
Diagnostics	Apr 02 16:18:24 localhost This initialization process is taking longer than expected, load avg ge: 1.10, time: 247 seconds
NTP Server	Apr 02 16:18:23 localhost This initialization process is taking longer than expected, load avg ge: 1.10, time: 246 seconds
Lockdown Mode	Apr 02 16:18:22 localhost This initialization process is taking longer than expected, load avg ge: 1.11, time: 245 seconds
System Update	Apr 02 16:18:21 localhost This initialization process is taking longer than expected, load avg ge: 1.11, time: 244 seconds
Reboot Shutdown	Apr 02 16:18:20 localhost This initialization process is taking longer than expected, load avg ge: 1.11, time: 243 seconds
About	Apr 02 16:18:19 localhost This initialization process is taking longer than expected, load avg ge: 1.11, time: 242 seconds
Logs	Apr 02 16:18:17 localhost This initialization process is taking longer than expected, load avg ge: 1.11, time: 241 seconds
	Apr 02 16:18:16 localhost This initialization process is taking longer than expected, load avg ge: 1.12, time: 240 seconds
	Apr 02 16:18:15 localhost This initialization process is taking longer than expected, load avg ge: 1.12, time: 239 seconds
	Apr 02 16:18:14 localhost This initialization process is taking longer than expected, load avg ge: 1.12, time: 238 seconds
	Apr 02 16:18:13 localhost This initialization process is taking longer than expected, load avg ge: 1.12, time: 237 seconds
	Apr 02 16:18:12 localhost This initialization process is taking longer than expected, load avg ge: 1.13, time: 236 seconds
	Apr 02 16:18:11 localhost This initialization process is taking longer than expected, load avg ge: 1.13, time: 235 seconds
	Apr 02 16:18:10 localhost This initialization process is taking longer than expected, load avg ge: 1.13, time: 234 seconds
	Apr 02 16:18:09 localhost This initialization process is taking longer than expected, load avg ge: 1.13, time: 233 seconds
	Apr 02 16:18:08 localhost This initialization process is taking longer than expected, load avg ge: 1.13, time: 232 seconds
	Apr 02 16:18:07 localhost This initialization process is taking longer than expected, load avg ge: 1.15, time: 231 seconds
	Apr 02 16:18:06 localhost This initialization process is taking longer than expected, load avg ge: 1.15, time: 230 seconds
	Apr 02 16:18:05 localhost This initialization process is taking longer than expected, load avg ge: 1.15, time: 229 seconds
	Apr 02 16:18:04 localhost This initialization process is taking longer than expected, load avg ge: 1.15, time: 228 seconds
	Apr 02 16:18:03 localhost This initialization process is taking longer than expected, load avg ge: 1.15, time: 227 seconds
	Apr 02 16:18:02 localhost This initialization process is taking longer than expected, load avg ge: 1.16, time: 226 seconds
	Apr 02 16:18:01 localhost This initialization process is taking longer than expected, load avg ge: 1.16, time: 225 seconds
	Apr 02 16:18:00 localhost This initialization process is taking longer than expected, load avg ge: 1.16, time: 224 seconds
	Apr 02 16:17:59 localhost This initialization process is taking longer than expected, load avg ge: 1.16, time: 223 seconds
	Apr 02 16:17:58 localhost This initialization process is taking longer than expected, load avg ge: 1.16, time: 222 seconds
	Apr 02 16:17:57 localhost This initialization process is taking longer than expected, load avg ge: 1.17, time: 221 seconds
	Apr 02 16:17:56 localhost This initialization process is taking longer than expected, load avg ge: 1.17, time: 220 seconds
	Apr 02 16:17:55 localhost This initialization process is taking longer than expected, load avg ge: 1.17, time: 219 seconds
	Apr 02 16:17:54 localhost This initialization process is taking longer than expected, load avg ge: 1.17, time: 218 seconds
	Apr 02 16:17:53 localhost This initialization process is taking longer than expected, load avg ge: 1.17, time: 217 seconds
	Apr 02 16:17:52 localhost This initialization process is taking longer than expected, load avg ge: 1.19, time: 216 seconds
	Apr 02 16:17:51 localhost This initialization process is taking longer than expected, load avg ge: 1.19, time: 215 seconds
	Apr 02 16:17:50 localhost This initialization process is taking longer than expected, load avg ge: 1.19, time: 214 seconds
	Apr 02 16:17:49 localhost This initialization process is taking longer than expected, load avg ge: 1.19, time: 213 seconds
	Apr 02 16:17:47 localhost This initialization process is taking longer than expected, load avg ge: 1.19, time: 212 seconds
	Apr 02 16:17:46 localhost This initialization process is taking longer than expected, load avg ge: 1.21, time: 211 seconds
	Apr 02 16:17:45 localhost This initialization process is taking longer than expected, load avg ge: 1.21, time: 210 seconds
	Apr 02 16:17:44 localhost This initialization process is taking longer than expected, load avg ge: 1.21, time: 209 seconds
	Apr 02 16:17:43 localhost This initialization process is taking longer than expected, load avg ge: 1.21, time: 208 seconds
	Apr 02 16:17:42 localhost This initialization process is taking longer than expected, load avg ge: 1.22, time: 207 seconds
	Apr 02 16:17:41 localhost This initialization process is taking longer than expected, load avg ge: 1.22, time: 206 seconds

Incorrect Network Adapter Configuration

If the user adds a non-VMXNET3 driver the following error will appear on boot.

The SonicWall Network Security Virtual network adapters have been modified
NSv configuration supports 8 VMXNET ethernet adapters
Currently 1 non VMXNET3 ethernet adapters are configured
Power down the virtual machine and remove the 1 non VMXNET3 network adapters

Incorrect Number of Network Adapters

The NSv supports exactly 8 VMXNET3 Network adapters. If the customer adds or removes a VMXNET3 Network adapter the below error message will appear.

```
The SonicWall Network Security Virtual network adapters have been modified
NSv requires 8 ethernet adapters, currently 7 are configured
Power down the virtual machine and configure the additional 1 VMXNET network adapters
```

Insufficient Memory When Jumbo Frames Enabled

The below error message appears on boot when Jumbo frames have been enabled and there is insufficient memory. Resolution is to power off the VM and increase the memory.

```
Insufficient memory 5 GB. The minimum memory required is 10 GB for NSv model: "NSv 400" with
the jumbo frame feature enabled
Power off the Network Security virtual appliance and assign 10 GB of memory to this virtual
appliance
```

Licensing and Registering Your NS_v

Topics:

- [Registering the NSv Appliance from SonicOS](#) on page 26

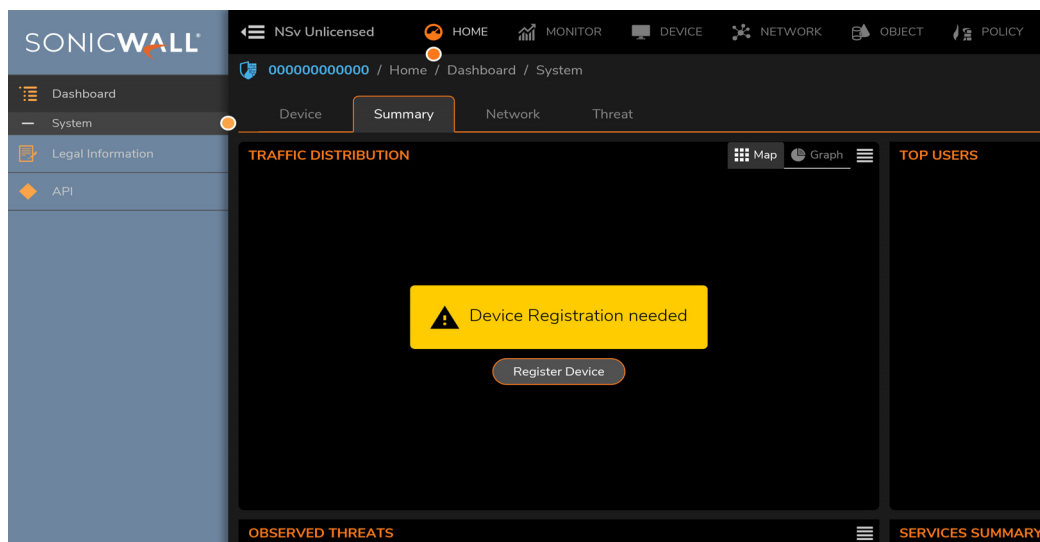
Registering the NS_v Appliance from SonicOS

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

NOTE: System functionality is extremely limited if registration is not completed. See [Using System Diagnostics](#) on page 29 for more information.

To register your NSv appliance:

- 1 Point your browser to your NSv Series WAN or LAN IP address and log in as the administrator (default *admin / password*).
- 2 [Licensing and Registering Your NSv](#)



- 3 At this point you may log into **MySonicWall** and name the NSv installation while providing the serial number and authorization code to complete registration. Or, if you are unable to reach **MySonicWall**, use the **Keyset**, **Serial Number** and **Authorization** and **Registration** codes provided by your SonicWall representative.

NSv Unlicensed | HOME | MONITOR | **DEVICE** | NETWORK | OBJECT | POLICY

000000000000 / Device / Settings / Licenses | Configuration

Security Services Summary | **Settings**

MANAGE SECURITY SERVICES ONLINE

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

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

Register

MANUAL UPGRADE

Enter keyset

Serial Number *

Auth Code * -

Registration Code *

Apply

- 4 Once complete log into SonicOS and check that licensing is complete.

SonicOS Management

Topics:

- [Managing SonicOS on the NSv Series](#) on page 28
- [Using System Diagnostics](#) on page 29
- [Using System Diagnostics](#) on page 29

Managing SonicOS on the NSv Series

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

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

To change the configuration of either X1 or X0, refer to [Using the ESXi Remote Console to Configure the WAN or LAN Interfaces](#) on page 30.

To log into SonicOS for management of the NSv:

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

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

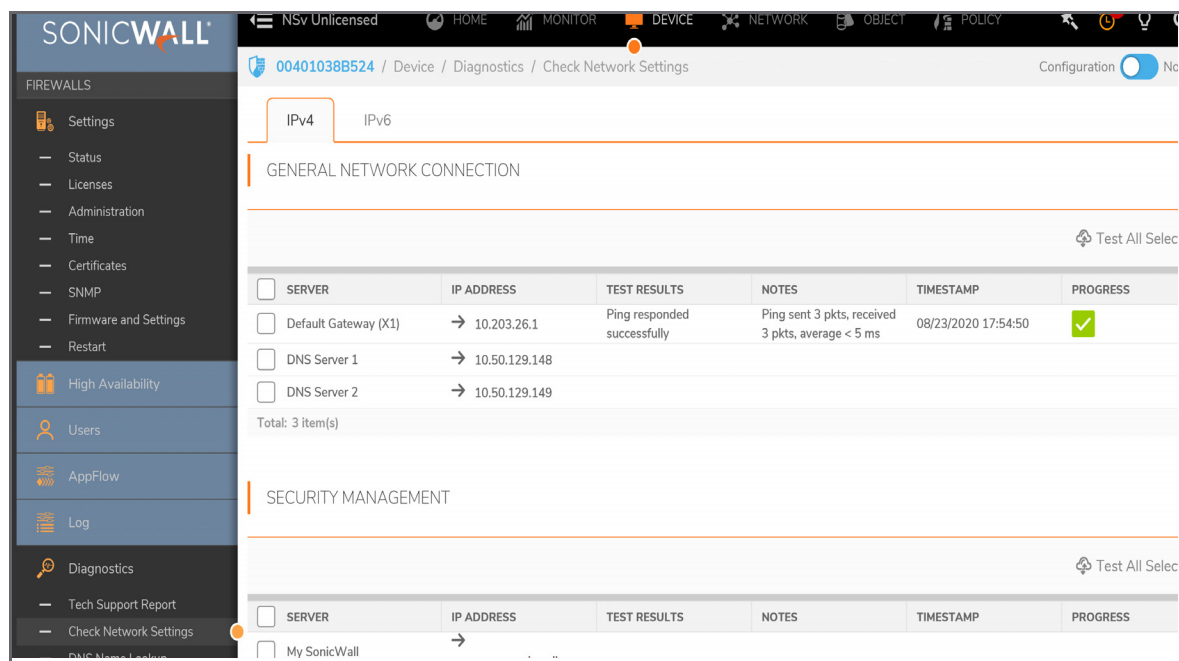
If you have an existing network on 192.168.168.0/24 in your environment, you can access the default IP address of the X0 LAN interface of your NSv Series from a computer on that network for SonicOS management. The NSv Series X0 IP address is 192.168.168.168 by default.

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

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

Using System Diagnostics

Check Network Settings, at Device | Diagnostic > Check Network Setting. is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined 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 shows the SonicWall NSv Series VMware ESXi Getting Started Guide interface. The left sidebar contains a navigation menu with options like Settings, Status, Licenses, Administration, Time, Certificates, SNMP, Firmware and Settings, Restart, High Availability, Users, AppFlow, Log, and Diagnostics. The main content area is titled 'Check Network Settings' and shows a table of network connection tests for IPv4. The table has columns for SERVER, IP ADDRESS, TEST RESULTS, NOTES, TIMESTAMP, and PROGRESS. The tests include Default Gateway (X1), DNS Server 1, and DNS Server 2. The results show that the Default Gateway (X1) test was successful, while the DNS Server 1 and DNS Server 2 tests failed. The table also includes a 'Total: 3 item(s)' summary and a 'Test All Selected' button.

SERVER	IP ADDRESS	TEST RESULTS	NOTES	TIMESTAMP	PROGRESS
<input type="checkbox"/> 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	<input checked="" type="checkbox"/>
<input type="checkbox"/> DNS Server 1	→ 10.50.129.148				<input type="checkbox"/>
<input type="checkbox"/> DNS Server 2	→ 10.50.129.149				<input type="checkbox"/>

Total: 3 item(s)

Test All Selected

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 list 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 probes fail, you can click the blue 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

Topics:

- [Using the ESXi Remote Console to Configure the WAN or LAN Interfaces](#) on page 30
- [Configuring SR-IOV](#) on page 34
- [Using SafeMode on the NSv](#) on page 56

Using the ESXi Remote Console to Configure the WAN or LAN Interfaces

You can use the ESXi remote console to set the IP address and network settings of the NSv Series interfaces, to change between static and DHCP addressing, and to enable SonicOS management on your NSv Series instance.

For example, depending on your network environment, you might need to configure a static IP address on your NSv Series X1 WAN interface. If you do so, you need to configure HTTPS management to allow remote management over the WAN.

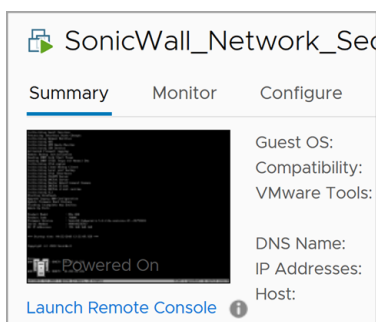
The NSv Series X0 IP address is 192.168.168.168 by default. If your LAN network uses a different IP address range, then you may want to configure your NSv Series X0 IP address with an address in your existing LAN network. This will allow you to manage SonicOS from a computer on your LAN.

The *ESXi Remote Console* allows you to log into the NSv Series console and use the command line interface (CLI) to configure these network settings.

NOTE: To type within the console window, click your mouse inside the window. To regain control of your mouse, press **Ctrl+Alt**.

To use the console to enable SonicOS management:

- 1 Log into vSphere or vCenter and select your NSv Series instance in the left pane.
- 2 Do one of the following to open the ESXi remote console:
 - Click on the image of the console to access the console in browser window.



- Click **Launch Remote Console**.

- Click **Actions > Open Remote Console**.
- 3 Click inside the console window.
 - i** | **NOTE:** Press **Ctrl+Alt** to regain control of your mouse, or with the browser access method simply move your mouse away from the console area.
 - 4 Log in using the administrator credentials.

```
Product Model      : NSv Unlicensed
Product Code       : 70000
Firmware Version   : SonicOS Enhanced 6.5.0.2-8v-sonicosv-37--25793204
Serial Number      : 000000000000
X0 IP Addresses    : 192.168.168.168

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

*** Startup time: 04/25/2018 18:14:27.048 ***

Copyright (c) 2018 SonicWall

User:
```

- 5 To use a static IP address for the WAN, type the following sequence of commands to enable a static IP and management access on the X1 WAN interface. The command prompt will change as you enter or exit different command levels. This command sequence shown below uses example IP address settings in the 10.203.26.0 network, which should be replaced with the correct settings for your environment.

```
configure t
interface x1
ip-assignment WAN static
ip 10.203.26.228 netmask 255.255.255.0
gateway 10.203.26.1
exit
management https
management ping
management ssh
exit
commit
```

After entering `commit`, the console displays `Applying changes` and other status information, then displays the `config` prompt. Type `exit` to return to the `admin` command level and prompt.

```
admin@00000000000000> configure t
config(00000000000000)# interface x1
(edit-interface[X1])# ip-assignment WAN static
(edit-WAN-static[X1])# ip 10.203.26.228 netmask 255.255.255.0
(edit-WAN-static[X1])# gateway 10.203.26.1
(edit-WAN-static[X1])# exit
(edit-interface[X1])# management https
(edit-interface[X1])# management ping
(edit-interface[X1])# management ssh
(edit-interface[X1])# exit
config(00000000000000)# commit
% Applying changes...
% Status returned processing command:
    commit
% Changes made.
config(00000000000000)#
```

- 6 To return to DHCP for the WAN address, type the following sequence of commands to enable DHCP and management access on the X1 WAN interface. The command prompt will change as you enter or exit different command levels.

```
configure t
interface x1
ip-assignment WAN dhcp
exit
management https
management ping
management ssh
exit
commit
```

After entering `commit`, the console displays `Applying changes` and other status information, then displays the `config` prompt. After a few seconds, the assigned DHCP address is displayed. You can access the SonicOS web management interface at that address.

```
admin@00000000000000> configure t
config(00000000000000)# interface x1
(edit-interface[X1])# ip-assignment WAN dhcp
(edit-WAN-dhcp[X1])# exit
(edit-interface[X1])# management https
(edit-interface[X1])# management ping
(edit-interface[X1])# management ssh
(edit-interface[X1])# exit
config(00000000000000)# commit
% Applying changes...
% Status returned processing command:
    commit
% Changes made.
config(00000000000000)#
WAN IP ADDRESS (DHCP): 10.203.26.229
```


- 7 You can use the `show status` command at the `admin` prompt to view the assigned IP address for the X1 (WAN) interface and other information.

```
admin@000000000000> show status

=====
System Information:
=====

Model:                               NSv Unlicensed
Product Code:                        70000
Serial Number:
Authentication Code:
GUID:
Firmware Version:                    SonicOS Enhanced 6.5.0.2-8u-sonicosu-37--25793204
Safemode Version:                    6.5.0.0
ROM Version:                         5.0.0.0
CPUs:                               3.35% - 2 x 2599 MHz Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz
Total Memory:                        6 GB RAM
System Time:                         04/26/2018 12:41:46
Up Time:                             0 Days 18:30:02
Connections:                         Peak: 77 Current: 0 Max: 512
Connection Usage:                    0.000%
Last Modified By:                    admin CLI 04/26/2018 12:37:45

=====
Security Services:
=====

Nodes/Users:                         10 Nodes(0 in use)
SSL VPN Nodes/Users:                 2 Nodes(0 in use)
Virtual Assist Nodes/Users:          1 Nodes(0 in use)
Registration Status:                 Your SonicWall is not registered

=====
Network Interfaces:
=====

Name          IP Address      Link Status
X0(LAN)       192.168.168.168 10 Gbps Full Duplex
X1(WAN)       10.203.26.229   10 Gbps Full Duplex
X2(Unassigned) 0.0.0.0         10 Gbps Full Duplex
X3(Unassigned) 0.0.0.0         10 Gbps Full Duplex
X4(Unassigned) 0.0.0.0         10 Gbps Full Duplex
X5(Unassigned) 0.0.0.0         10 Gbps Full Duplex
X6(Unassigned) 0.0.0.0         10 Gbps Full Duplex
X7(Unassigned) 0.0.0.0         10 Gbps Full Duplex
admin@000000000000>
```

- 8 To change the X0 LAN static IP address, use the following commands:

NOTE: SonicOS HTTPS management is enabled by default on the X0 interface.

For a static IP address in an example 10.10.10.0/24 LAN network, enter:

```
configure t
interface x0
ip 10.10.10.100 netmask 255.255.255.0
exit
exit
commit
```

An alternative approach to changing the X0 IP address to 192.168.1.1 at the CLI follows:

```
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
```

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

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

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

Configuring SR-IOV

For high performance requirements in the virtual environment, VMWARE ESXi provides 2 options for exposing the HW level NIC as PCI device directly into VM Guest OS. One is the "pass-through" mode. The other one is "SR-IOV". For "pass-through" mode, the HW NIC will be directly exposed as a PCI device into VM Guest OS. We need to add "PCI device" in the VM configuration settings. And the "pass-through" mode NIC can only be used by one VM and can in no way to share this HW NIC with other VMs on the same Host. For the "SR-IOV" mode, if the NIC supports this mode, it can expose the "Virtual Function (VF)" virtualized PCI devices into the Guest VM as Network Adapters. So multiple VMs can use different VF NICs from the same HW PF (Physical Function) NIC.

Prerequisites

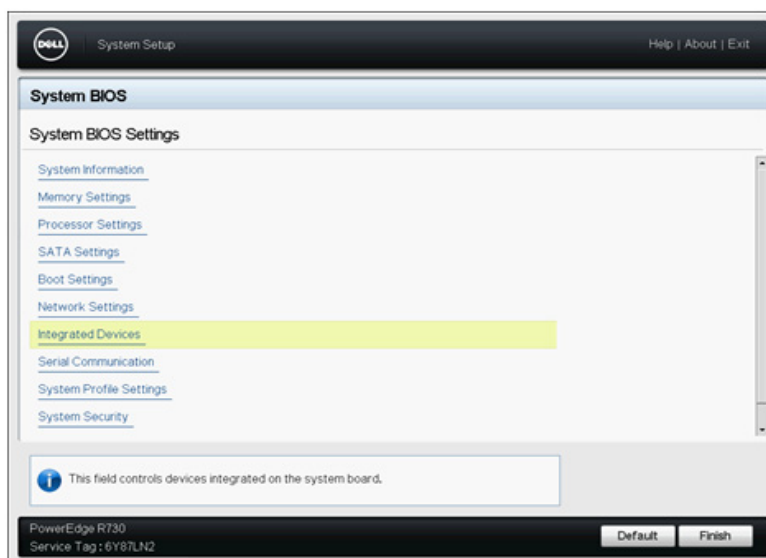
This document (especially the screenshots) is based on Dell R740 server with Intel X520 NIC. For other servers and NICs, the settings may be different.

- Get the iDrac access to your host server (for enabling SR-IOV settings in BIOS). Note, you may need use old IE as the iDrac virtual console as a JAVA SE applet and may not able to pop out on some modern browsers.
- Get the vCenter access to configure the host server and VMs on the server.

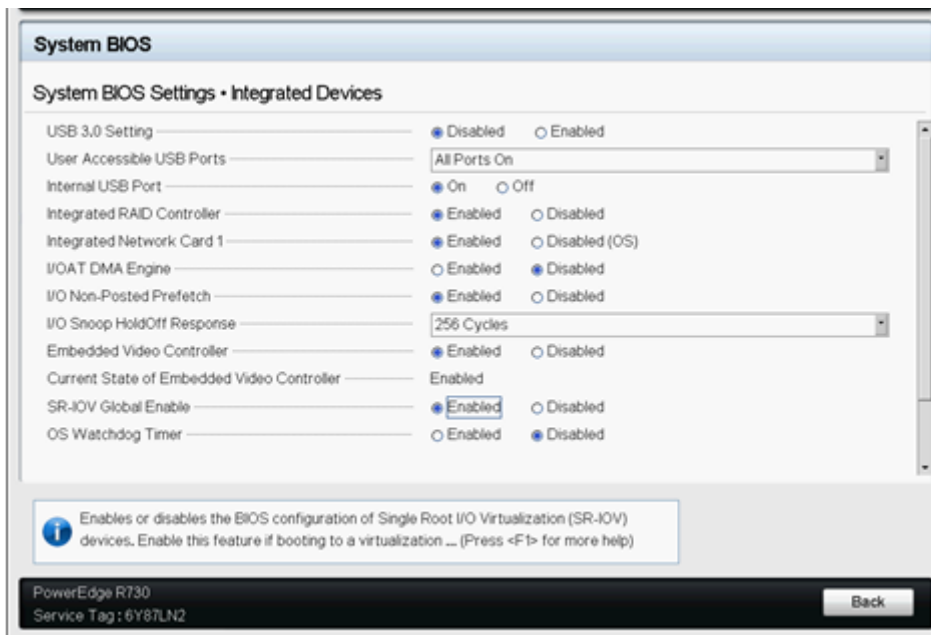
Procedures

To enable SR-IOV in BIOS:

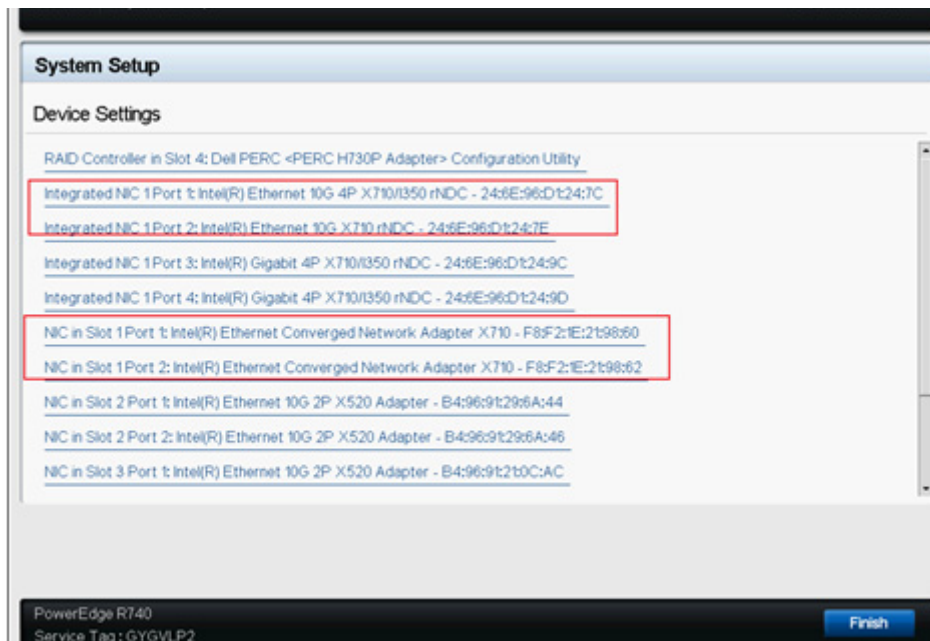
- 1 Goto "System BIOS Settings > Integrated Devices".



- 2 Enable "SR-IOV Global Enable" option.



NOTE: If the NIC has some separate SR-IOV settings, you may also need to check them in the BIOS settings. For example, for the Intel 710 NICs, you need to enable the SR-IOV for each NIC in BIOS settings.




NIC in Slot 1 Port 1: Intel(R) Ethernet Converged Network Adapter X710 - F8F21E:2t98:60

Main Configuration Page • Device Level Configuration

Virtualization Mode SR-IOV

NParEP Mode ☒ Disabled ☐ Enabled

 View and configure global device level parameters.

PowerEdge R740
Service Tag : GYGVLP2

[Back](#)

NIC in Slot 1 Port 2: Intel(R) Ethernet Converged Network Adapter XL710-Q2 - F8F21E:8B:A5:71

Main Configuration Page

[Firmware Image Properties](#)

[NIC Configuration](#)

[iSCSI Configuration](#)

[Device Level Configuration](#)

Blink LEDs 0

Adapter PBA H71024-016


Device Name Intel(R) Ethernet Converged Network Adapter XL710-Q2

Chip Type Intel XL710

PCI Device ID 1583

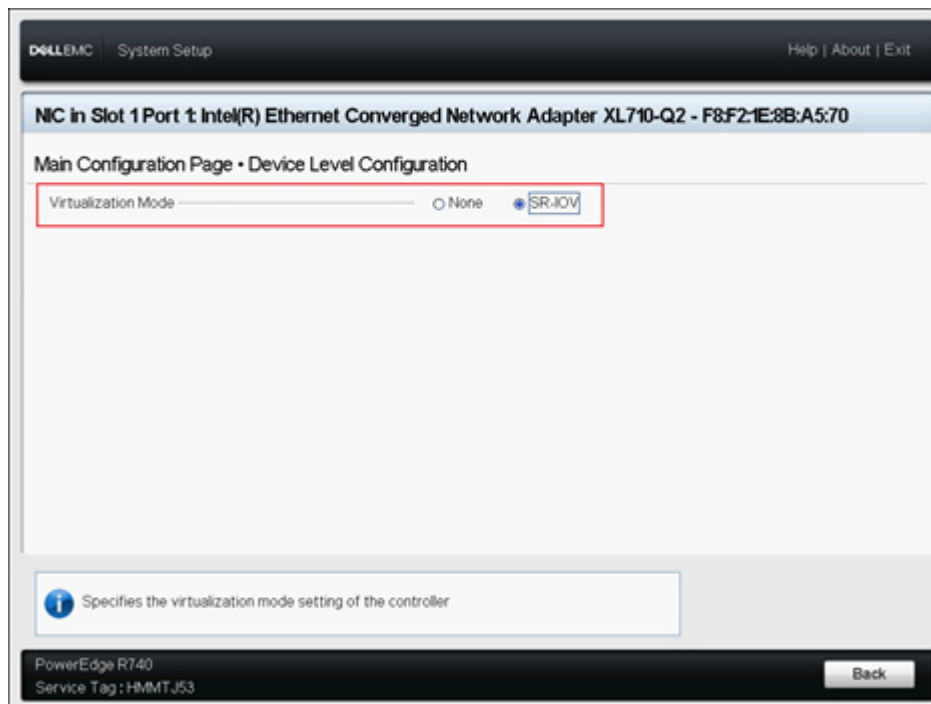
PCI Address 65:00:01

Link Status ☐ Disconnected ☒ Connected

 View and configure global device level parameters.

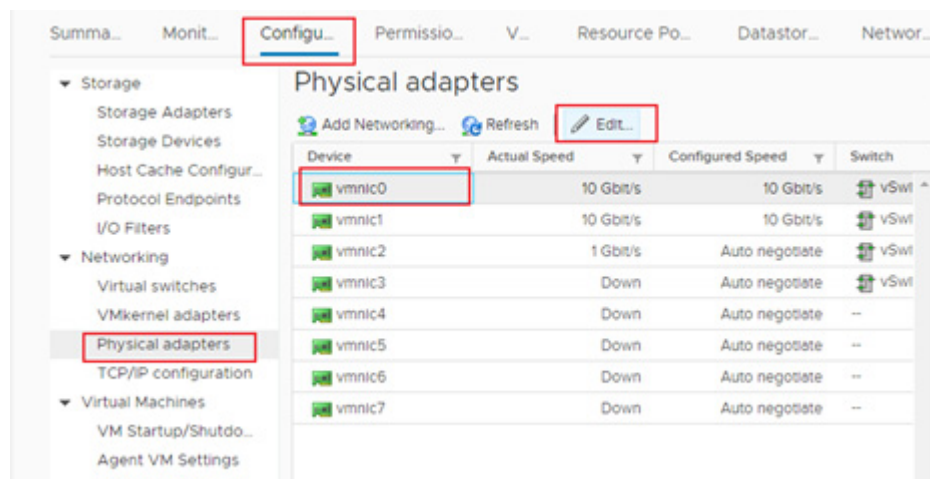
PowerEdge R740
Service Tag : HMMTJ53

[Default](#) [Finish](#)



To enable SR-IOV in VMWARE Host NIC settings:

- 1 Go to the Host's **Configuration > Networking > Physical adapters**, find your NIC that supports SR-IOV, click **Edit**.



- 2 In **SR-IOV** section, set the **Status** to **Enabled** and set the value of **Number of virtual functions** to some value that is larger than 0. (Note there would be some max VF number for different NICs, you need check NIC specification or BIOS settings for this max number).

Edit Settings

vmnic0

×

Configured speed, Duplex

10000 Mbit/s, Full Duplex

SR-IOV

SR-IOV is a technology that allows multiple virtual machines to use the same PCI device as a virtual pass-through device.

Status

Enabled

Number of virtual functions

4

- 3 After configure the SR-IOV settings for all the NICs that you want to use, you need reboot the "Host" and then check the SR-IOV status of those NICs to make sure it's all available.

The screenshot displays the vSphere Client configuration interface for physical network adapters. The left-hand navigation pane is expanded to 'Networking' > 'Physical adapters'. The main content area shows a table of physical adapters and their properties.

Device	Actual Speed	Configured Speed	Switch
vmnic0	10 Gbit/s	10 Gbit/s	vSwi
vmnic1	10 Gbit/s	10 Gbit/s	vSwi
vmnic2	1 Gbit/s	Auto negotiate	vSwi
vmnic3	Down	Auto negotiate	vSwi
vmnic4	Down	Auto negotiate	--
vmnic5	Down	Auto negotiate	--
vmnic6	Down	Auto negotiate	--
vmnic7	Down	Auto negotiate	--

Below the table, the configuration for 'Physical network adapter: vmnic0' is shown. The 'SR-IOV' section is highlighted with a red box, indicating the status and number of virtual functions.

Physical network adapter: vmnic0	
Adapter: Intel Corporation 82599EB 10-Gigabit SFI/SFP+ Network Connection	
Name	vmnic0
Location	PCI 0000:01:00.0
Driver	ixgben
Status	
Status	Connected
Actual speed, Duplex	10 Gbit/s, Full Duplex
Configured speed, Duplex	10 Gbit/s, Full Duplex
Networks	No networks
SR-IOV	
Status	Enabled
Number of virtual functions	4

Below the SR-IOV section, the 'Cisco Discovery Protocol' and 'Link Layer Discovery Protocol' are listed as not available on this physical network adapter.

Now the Host settings are all fine. We will configure the NSv VM to add the SR-IOV interfaces.

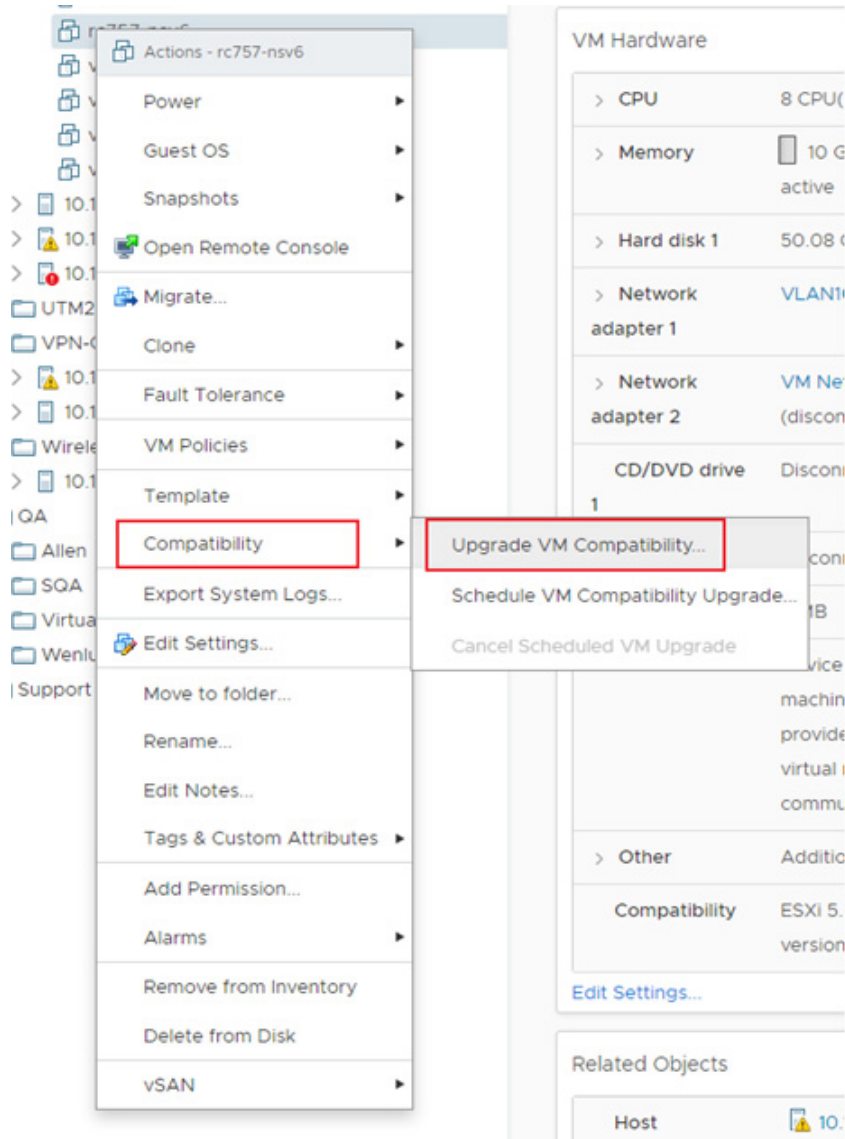
If the vCenter GUI reports error and not work, there is a CLI command in ESXi ssh that can do the same for configuring SR-IOV VF number:

- 1 Use "esxcli network nic list" to find the driver name of your NICs.
- 2 Use "esxcfg-module ixgben -s max_vfs=4,4,4,4". The "ixgben" is the driver name in this case. And the "4,4,4,4" means configure all 4 ports with 4 max VF number.

To add SR-IOV Network Adapters into your VM:

- 1 Set the "VM compatibility" of your NSv VM (right click the VM and see the "Compatibility" option). Please note, this is the very "key" step to be able to add the SR-IOV network adapter in your VM. See the "Prerequisites"

in <https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vsphere.networking.doc/GUID-898A3D66-9415-4854-8413-B40F2CB6FF8D.html>



VM Compatibility Upgrade | rc757-nsv6

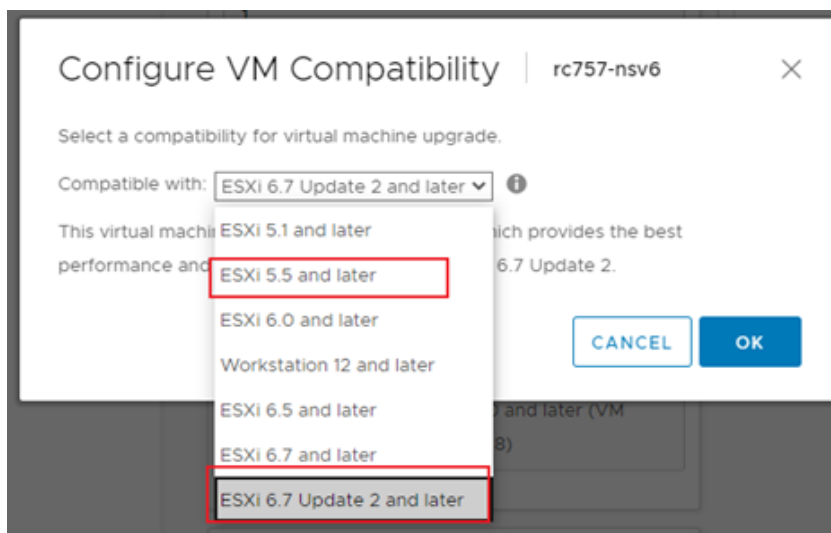


This operation changes the compatibility of your virtual machine. It is an irreversible operation that makes your virtual machine incompatible with earlier versions of VMware software products. Make a backup copy of your virtual machine files before proceeding. Upgrade your compatibility?

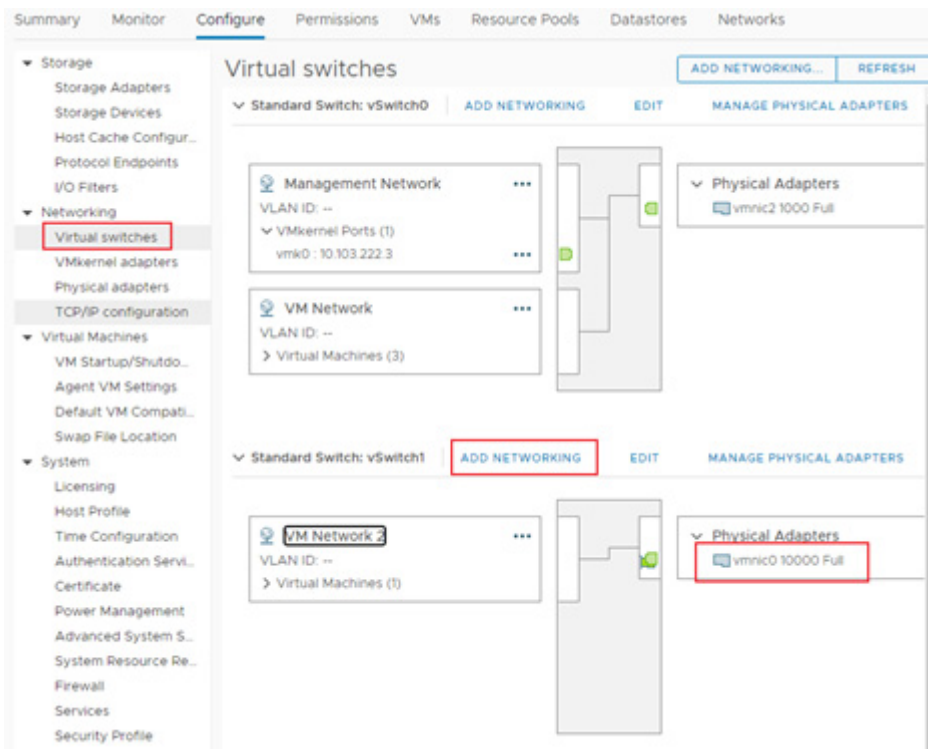
NO

YES

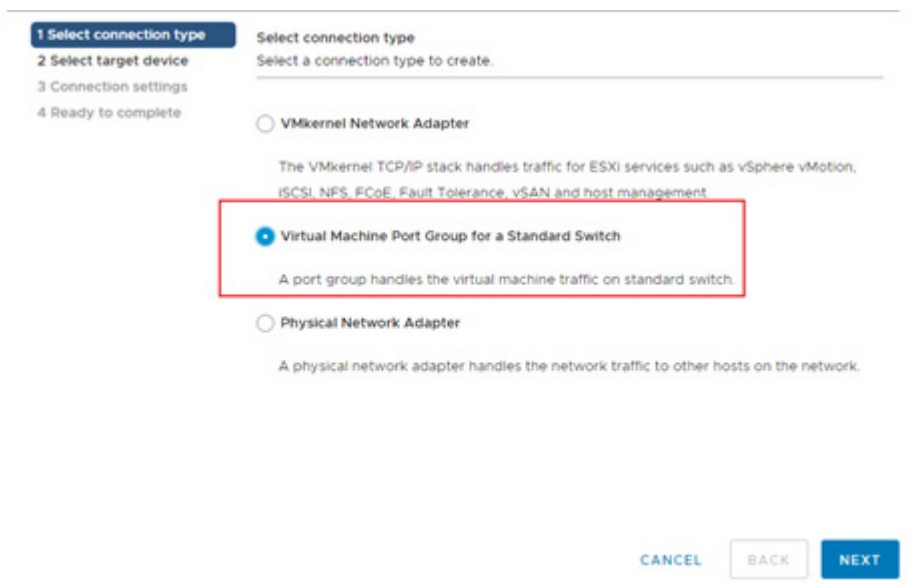
- 2 According to VMWARE's guide, the compatibility should be "ESXi 5.5 or later". It is suggested to use the latest version that the Host support. So select the default "ESXi 6.7 Update 2 and later" for this host.



- 3 You may would like to add new "virtual networking" to the vSwitches with your physical adapters.



- 4 Make sure you select the vSwitch of your SR-IOV physical adapter.



- 5 To make the multiple SR-IOV VF can be used by multiple different VMs, set different VLAN IDs for different networks. Then you can select different networks for different VMs.

✓ 1 Select connection type
2 Select target device
3 Connection settings
4 Ready to complete

Select target device
Select a target device for the new connection.

Select an existing standard switch

vSwitch1 [BROWSE ...](#)

☐ New standard switch

MTU (Bytes) 1500

To configure the VM to add the SR-IOV Network Adapters:

- 1 Open the **Edit Settings** of your NSv VM. Click the **ADD NEW DEVICE** and **Select Network Adapter**.

Edit Settings | 953-nsv7

Virtual Hardware VM Options

[ADD NEW DEVICE](#)

CD/DVD Drive
Host USB Device
Hard Disk
RDM Disk
Existing Hard Disk
Network Adapter
SCSI Controller
USB Controller
SATA Controller
NVMe Controller
Shared PCI Device
PCI Device
Serial Port

8	10	GB	
50.080078125	GB		
LSI Logic Parallel			
VLAN1000			<input checked="" type="checkbox"/> Connect...
VM Network			<input checked="" type="checkbox"/> Connect...
VLAN1000			<input checked="" type="checkbox"/> Connect...
> Network adapter 4	VLAN1000		<input checked="" type="checkbox"/> Connect...
> SR-IOV network adapter 1	VM Network 2		<input checked="" type="checkbox"/> Connect...
> CD/DVD drive 1	Client Device		<input type="checkbox"/> Connect...
> Video card	Specify custom settings		
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface		
> Other	Additional Hardware		

- 2 Edit your newly added Network Adaptor by: changing the **Adapter Type** to **SR-IOV passthrough** and select the **Physical Function** to the physical NIC and select your virtual Network.

New Network *	VLAN1000
Status	<input checked="" type="checkbox"/> Connect At Power On
Adapter Type	SR-IOV passthrough
<p>⚠ Some operations are unavailable when SR-IOV passthrough devices are present. Suspending, migrating with vMotion, or taking/restoring snapshots of the virtual machine are not possible.</p>	
Physical Function	vmnic0 0000:01:00:0 82599EB 10-Gigabit SFI/SFP+ Network Co
MAC Address	Automatic
Allow Guest MTU Change	Disallow

You can add multiple SR-IOV adapters to the same VM if your total NIC number does not exceed the "maximum physical interfaces supported in NSv". Now you're done with all the SR-IOV settings in VMWARE. You may need to configure your real physical switch that connected to the physical function NIC port to add the VLANs for supporting different VF sending traffics with different VLAN ID.

- 3 Enable "Reserve all guest memory (All locked)" option in VM Memory part.

Virtual Hardware		VM Options	
ADD NEW DEVICE			
CPU	8		
Memory *	10	GB	
Reservation	10240	MB	
	<input checked="" type="checkbox"/> Reserve all guest memory (All locked)		
Limit	Unlimited	MB	
Shares	Normal	102400	
Memory Hot Plug	<input type="checkbox"/> Enable		

IMPORTANT: Otherwise, the VM with SR-IOV devices cannot boot up due to memory error.

Performance Enhancement Configurations

In the screenshots in above sections on configuration, we use the Intel 82599 (or X520) NIC as an example. But due to the limitations with these NICs, the RSS configurations can only be configured by the PF driver side. And after some testing and investigations, both the "ixgben" and "ixgbe" drivers from VMWARE cannot fully enable the multi-queue RSS feature in NSv's VF side. So all packets goes to only one RX queue for each NIC port. This may result some multi-core contentions on the RX side (may male more CPU time visible on the ODP scheduler when doing the performance profiling).

To achieve the best performance for NSv, make sure the RSS feature on the VF side inside the NSv works as expected (multiple RX queue can all evenly get packets when we have multiple traffic flows running through NSv). Currently, only the i40e (Intel 7xx NICs) driver can work as expected and get the best performance.

Replace the default VMWARE Native driver (ends with "n") with original driver

Before going into the steps for enabling RSS on the PF driver side, enable the original Intel NIC drivers (i.e. "i40e" for Intel 7xx NICs) and disable the native VMWARE drivers (i.e. the "i40en" for Intel 7xx NICs).

The main reason for replacing the driver is that the "native" driver does NOT work with DPDK's VF driver and will cause SonicOSv always fails at the early stages on configuring VF drivers.

Firstly, you can use the following command to check which driver is in use.

```
[root@ESXi-10D7D100D252:~] esxcfg-nics -l | grep i40e

vmnic0 0000:18:00.0 i40en      Up    10000Mbps Full   24:6e:96:d1:24:7c 1500   Intel
Corporation Ethernet Controller X710 for 10GbE SFP+

vmnic1 0000:18:00.1 i40en      Up    10000Mbps Full   24:6e:96:d1:24:7e 1500   Intel
Corporation Ethernet Controller X710 for 10GbE SFP+

vmnic4 0000:3b:00.0 i40en      Up    10000Mbps Full   f8:f2:1e:21:98:60 1500   Intel
Corporation Ethernet Controller X710 for 10GbE SFP+

vmnic5 0000:3b:00.1 i40en      Up    10000Mbps Full   f8:f2:1e:21:98:62 1500   Intel
Corporation Ethernet Controller X710 for 10GbE SFP+
```

If the 3rd column says "i40en", then it means you need to replace it with "i40e".

Then check if the "i40e" drivers are available in your system. If not, you may need to search and download from VMWARE's website.

```
[root@ESXi-10D7D100D252:~] esxcli system module list | grep i40e
i40en_ens      true      true
i40e           true      true
i40en          true      true
```

As you can see from above, we have both "i40e" and "i40en" drivers and all enabled and loaded by default. Now we need to disable the "i40en" and make sure enable the "i40e" driver module.

```
esxcli system module set -e=true -m=i40e
esxcli system module set -e=false -m=i40en
```

Then we need reboot the Host server to apply this change. After the system boots up, you can check with "esxcfg-nics -l | grep i40e" to see if all those X710 NICs are using the "i40e" driver module instead of the "i40en".

Set the RSS and max_vfs parameters for i40e driver

There're some parameters can be set for "i40e" driver. You can use the following command to see the list of these parameters and the brief descriptions.

```
[root@ESXi-10D7D100D252:~] esxcli system module parameters list --module i40e
Name                Type                Value              Description
-----
RSS                  array of int        4,4,4,4           Number of Receive-Side Scaling Descriptor Queues: 0 =
disable/default, 1-4 = enable (number of cpus)

VMDQ                 array of int        0/1 = disable,
2-16 enable (default = 8)

debug               int                 Debug level (0=none,...,16=all)
heap_initial        int                 Initial heap size allocated for the driver.
heap_max            int                 Maximum attainable heap size for the driver.
max_vfs             array of int        4,4,4,4           Number of Virtual Functions: 0 = disable (default),
1-128 = enable this many VFs
```

skb_mpool_initial int Driver's minimum private socket buffer memory pool size.

skb_mpool_max int Maximum attainable private socket buffer memory pool size for the driver.

There are only 2 parameters that we need to set for enabling SR-IOV and RSS features: "max_vfs" and "RSS". As the maximum RSS queues are 4 for current i40e and we set the maximum number of VFs to 4 as example, then you can use the following command to set the values.

```
esxcli system module parameters set --module i40e -p "RSS=4,4,4,4 max_vfs=4,4,4,4"
```

Please note that we set four numbers for both parameters. This is because we have four NICs in "esxcfg-nics" results and we would like to enable these features for all these four NICs.

After this command, then you need to reboot the Host again to apply these changes.

After the system boots up, you can change your NSv's NIC settings to setup the SR-IOV interfaces upon the X710 physical NIC and do the performance testing.

Note on Test Methods

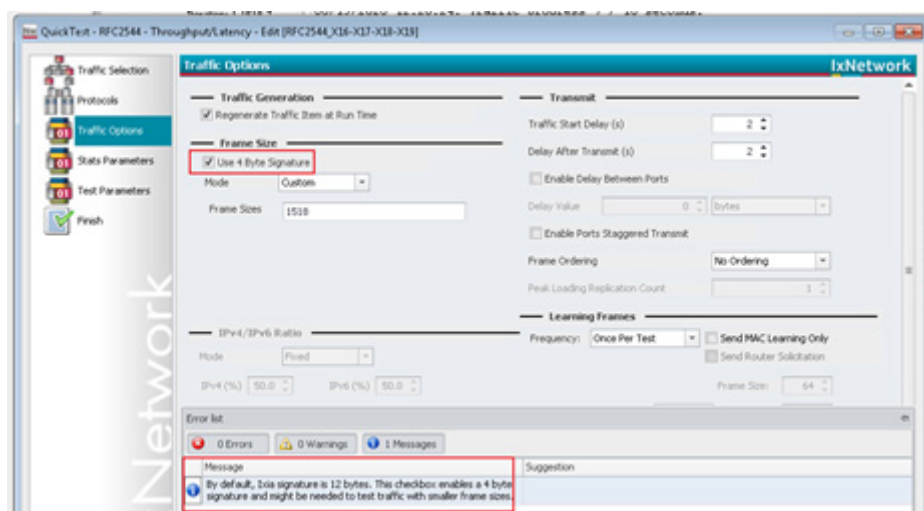
- **Always use multiple flows to test the performance**

Due to our multi-core processing design, always use multiple traffic flow when testing the throughput.

And for these flows, we should make sure only 1 of the 4 tuples (srcIP/dstIP/srcPort/dstPort) changes for each flow. This can make sure the RSS hash and our connection tag hash to work perfectly to distribute the flows to different cores.

- **Disable the "Use 4 Byte Signature" feature in IXIA**

In IxNetwork RFC2544 test settings, the following configuration may affect the result.



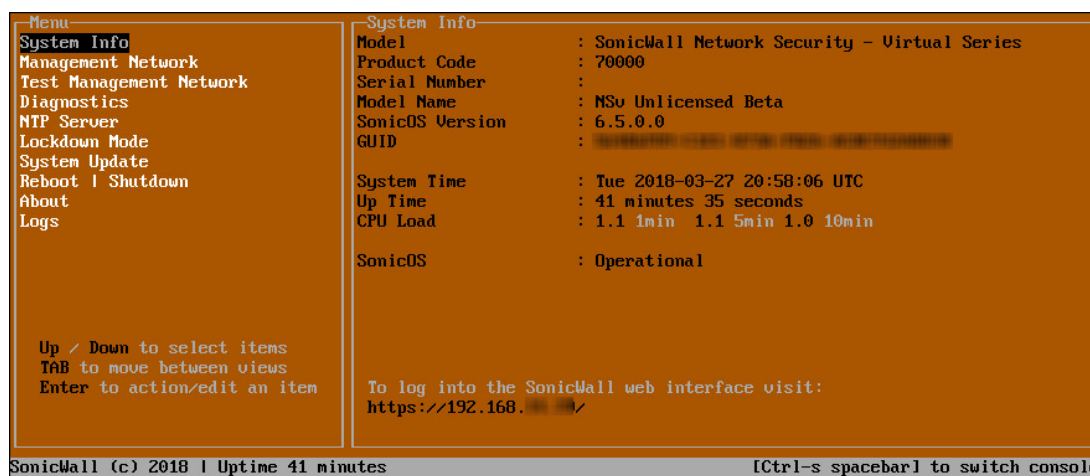
This "Use 4 Byte Signature" shall only be used in testing the packets with 64 bytes size. Otherwise, disable this.

Using the NS_v Management Console

The NS_v management console provides options for viewing and changing system and network settings, running diagnostics, rebooting SonicOS, and other functions. The NS_v management console can be accessed after you log into the ESXi remote console.

To access and navigate the management console:

- 1 Log into the ESXi remote console by selecting your NS_v in the vSphere or vCenter interface and clicking **Actions > Open Remote Console**, then clicking inside the console window. Use your initial login credential (admin / password) to get to the SonicOS prompt.
- 2 Press **Ctrl+s** and then press the **spacebar** to toggle between the ESXi remote console and the NS_v management console. That is, press the **Ctrl** key and 's' key together, then release and press the **spacebar**.



- 3 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.
- 4 Press the **Tab** key to move the focus from side menu to the main view (right pane), or vice versa.
- 5 In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.



- 6 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:

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

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

Some dialogs are for input:

```
Enter IP address
8.8.8.8_
Confirm <Enter>      Cancel <Esc>
```

- 7 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](#) on page 50
- [Management Network](#) on page 51
- [Test Management Network](#) on page 51
- [Diagnostics](#) on page 53
- [NTP Server](#) on page 54
- [Lockdown Mode](#) on page 54
- [Reboot | Shutdown](#) on page 55
- [About](#) on page 55
- [Logs](#) on page 56

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 : NSv 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

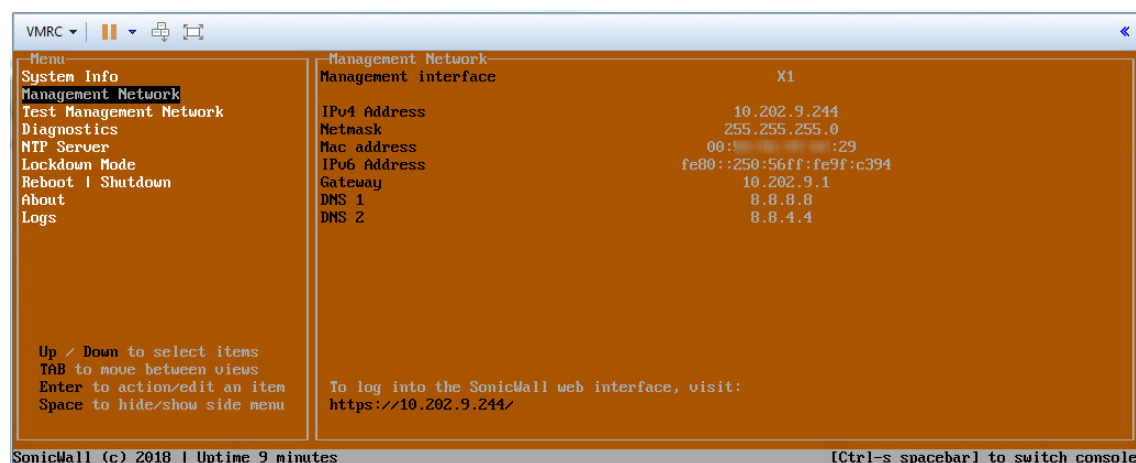
To log into the SonicWall web interface visit:
https://192.168.1.1/

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:

- **Model** – This is the model of the NSv appliance.
- **Product code** – This is the product code of the NSv appliance.
- **Serial Number** – The serial number for the appliance; this is a number unique to every NSv instance deployed. This number can be used to identify the NSv appliance on MySonicWall.
- **Model Name** – This is the model name of the NSv appliance.
- **SonicOS Version** – This is the currently running SonicOS version of the NSv appliance.
- **GUID** – Every NSv instance has a GUID which is displayed here.
- **System Time** – This is the current system time on the NSv appliance.
- **Up Time** – This is the total time that the NSv 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 NSv. **Operational** is displayed here when the SonicOS service is running normally, **Not Operational** when there is a problem with the service and **Operational (debug)** if the service is currently running in debug mode.

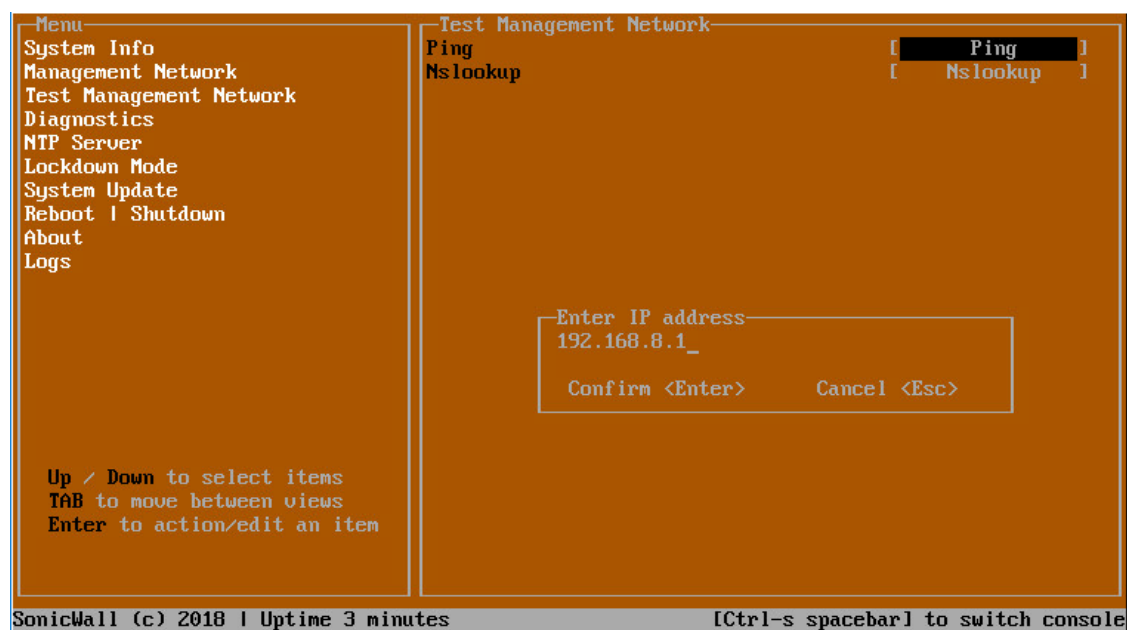
Management Network



In the **Management Network** screen, the network settings displayed in the white text 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.

Test Management Network



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 appliance.

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

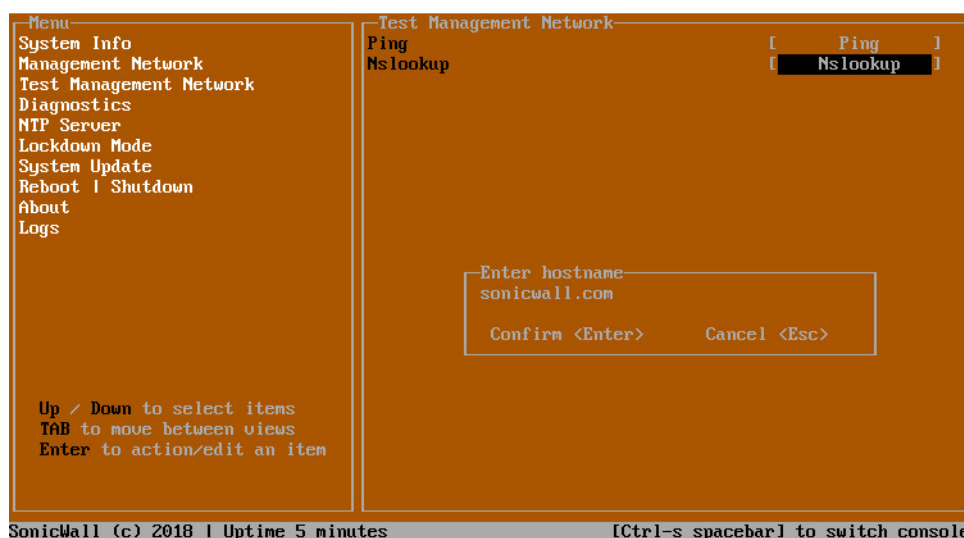
                                Scroll <Up Down Left Right>                                Close <Esc>

```

- 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.

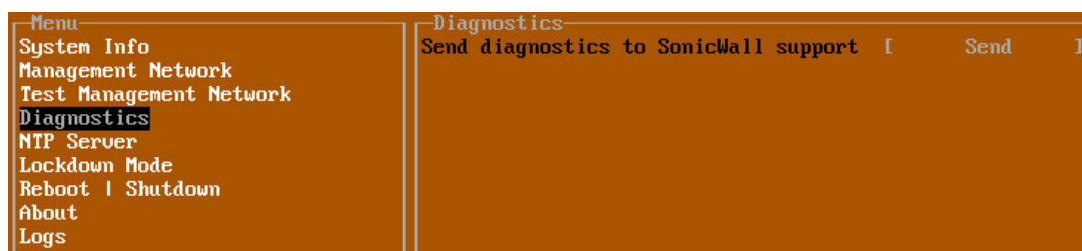
```
sonicwall.com
Server: 8.8.8.8
Address: 8.8.8.8#53

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.

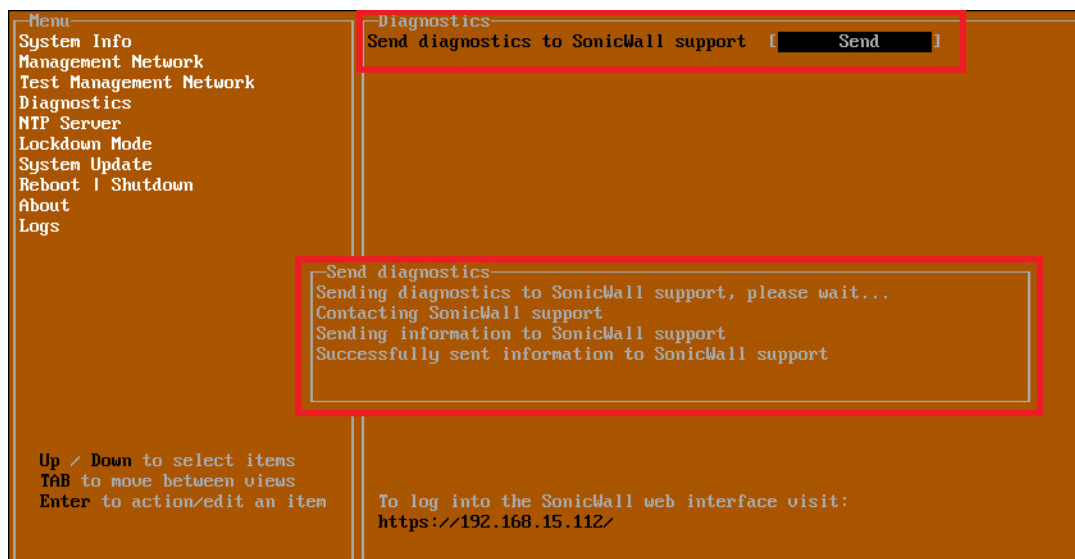
Diagnostics



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 web management interface.

NOTE: Your NSv appliance 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

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

NTP Server

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

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

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

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

Lockdown Mode

Menu	Lockdown Mode
System Info	Enable lockdown [Enable]
Management Network	
Test Management Network	
Diagnostics	
NTP Server	
Lockdown Mode	
Reboot Shutdown	
About	
Logs	

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

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

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

Temporary Lockdown Mode

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

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

Reboot | Shutdown

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

The **Reboot | Shutdown** screen provides functions for rebooting the NSv 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 NSv Series virtual appliance with current configuration settings.
- **Shutdown SonicWall** – Powers off the NSv Series virtual appliance.
- **Boot with factory default settings** – Restarts the NSv Series virtual appliance using factory default settings. All configuration settings will be erased.
- **Boot SonicWall into debug** – Restarts the NSv Series virtual appliance into debug mode. Normally this operation is performed under the guidance of SonicWall Technical Support.
- **Boot SonicWall into safemode** – Puts the NSv Series virtual appliance into SafeMode. For more information, see [Using SafeMode on the NSv](#) on page 56.

About

Menu	About
System Info	SonicWall SonicCore
Management Network	Version 6.5.0
Test Management Network	Build name 6.5.0-288+SonicCore-SonicOSV-6.5-Daily
Diagnostics	
NTP Server	
Lockdown Mode	
Reboot Shutdown	
About	

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

Logs

The **Logs** screen displays log events for the NSv appliance.

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

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

Up / Down to select items
TAB to move between views
Enter to action/edit an item
Space to hide/show side menu

Arrow keys: Navigate view   Current Line: 1 Lines: 21
SonicWall (c) 2018 | Uptime 23 hours, 48 minutes   [Ctrl-s spacebar] to switch console
```

Using SafeMode on the NS_v

The NSv appliance will enter SafeMode if SonicOS restarts three times unexpectedly within 200 seconds. When the NSv 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 NSv appliance can also be configured to boot into SafeMode by using the **Reboot | Shutdown** screen.

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

- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

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

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

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

```
-Safemode menu-
System Info
Management Network
Test Management Network
Diagnostics
NTP Server
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   : NSv Unlicensed Beta
SonicOS Version : 6.5.0.0
GUID        : 5
System Time  : Tue 2018-03-13 21:57:22 UTC
Up Time      : 6 hours 33 minutes 19 seconds
CPU Load     : 0.0 1min 0.0 5min 0.0 10min
SonicOS      : Not operational

SonicWall is in safemode, to access recovery options visit:
http://192.168.14.210/

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

NOTE: To exit SafeMode, disable it on the **Reboot | Shutdown** screen or deploy a new firmware image. See [Disabling SafeMode](#) on page 58 and [Installing a New SonicOS Version in SafeMode](#) on page 62 for more information.

Topics:

- [Enabling SafeMode](#) on page 57
- [Disabling SafeMode](#) on page 58
- [Configuring the Management Network in SafeMode](#) on page 59
- [Installing a New SonicOS Version in SafeMode](#) on page 62
- [Downloading Logs in SafeMode](#) on page 63

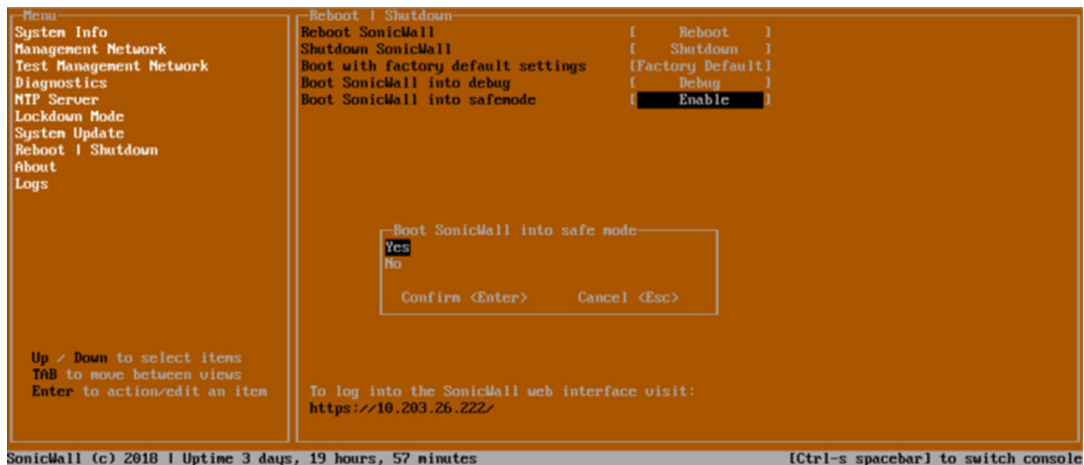
Enabling SafeMode

SafeMode can be enabled from the management console.

To enable SafeMode:

- 1 Access the NSv management console as described in [Configuring SR-IOV](#) on page 34.
- 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**.

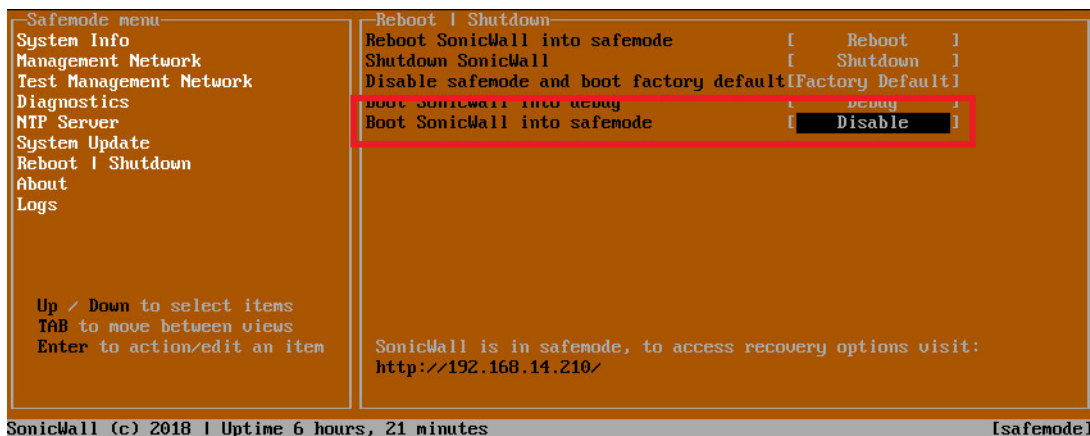
The NSv immediately reboots and comes back up in SafeMode.

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 provides features to configure the NSv appliance interfaces:

- **Management Interface** – This is the currently selected interface. This defaults to X1. Use this to select any of the NSv 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 NSv appliance.
- **DNS** – A list of the current DNS servers currently being used by the NSv appliance.

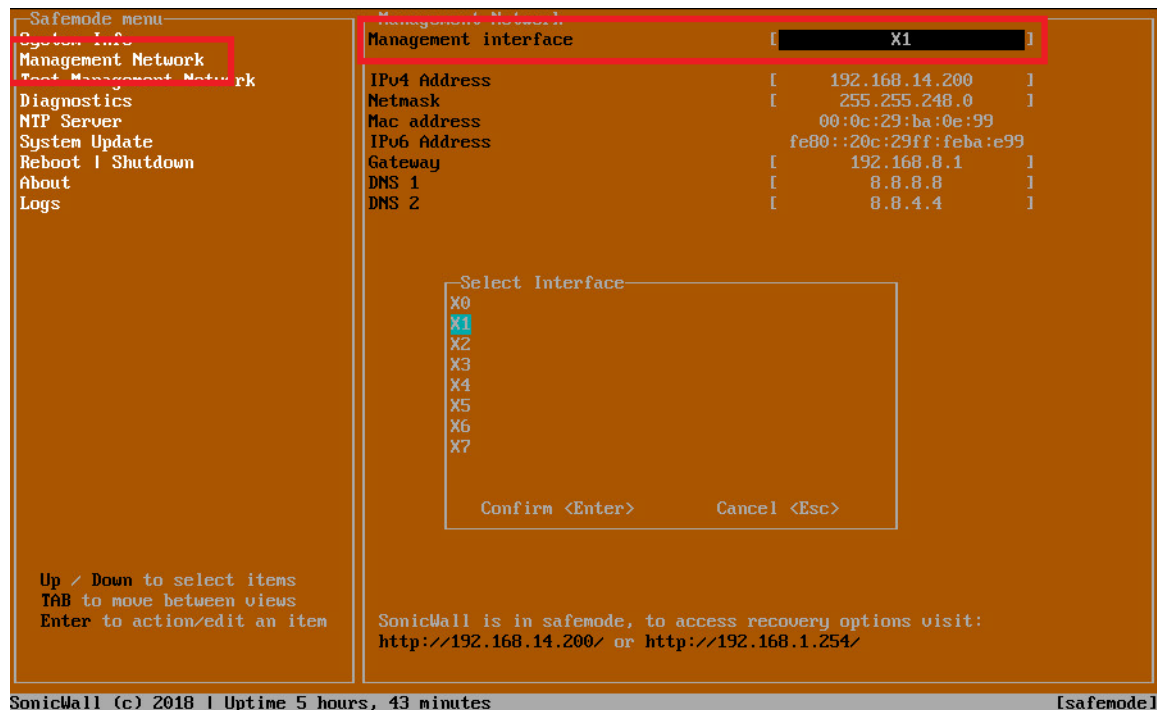
NOTE: Changes made to interfaces in SafeMode are *not* persistent between reboots.

Topics:

- [Configuring Interface Settings](#) on page 59
- [Disabling an Interface](#) on page 61

Configuring Interface Settings

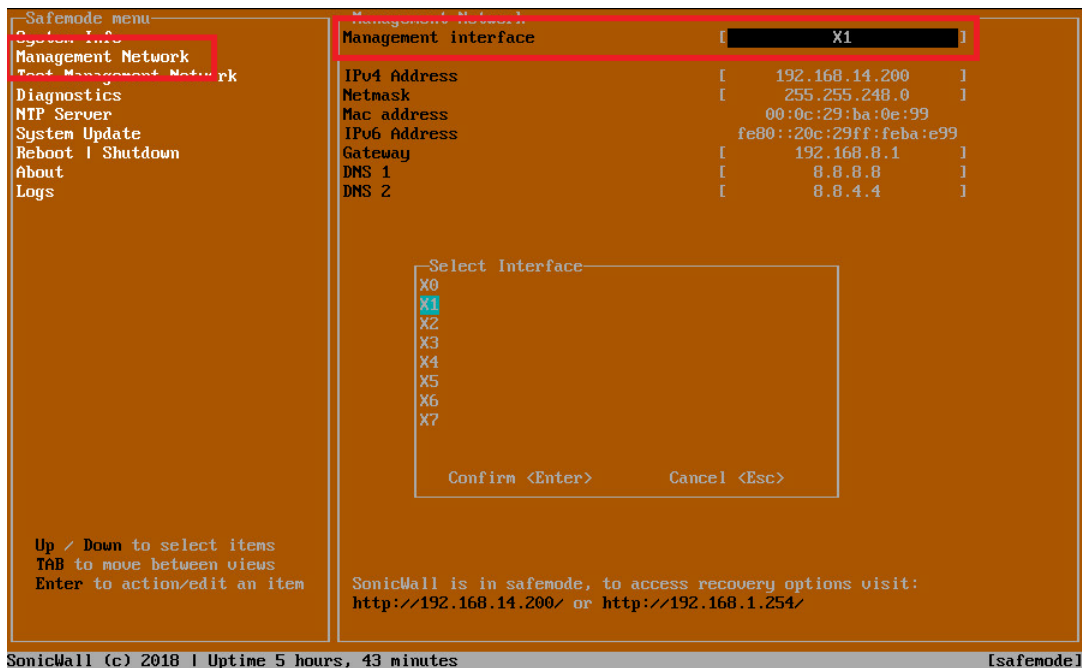
In SafeMode, the **Management Network** screen includes editable and actionable items which are read-only when the management console is in normal mode.



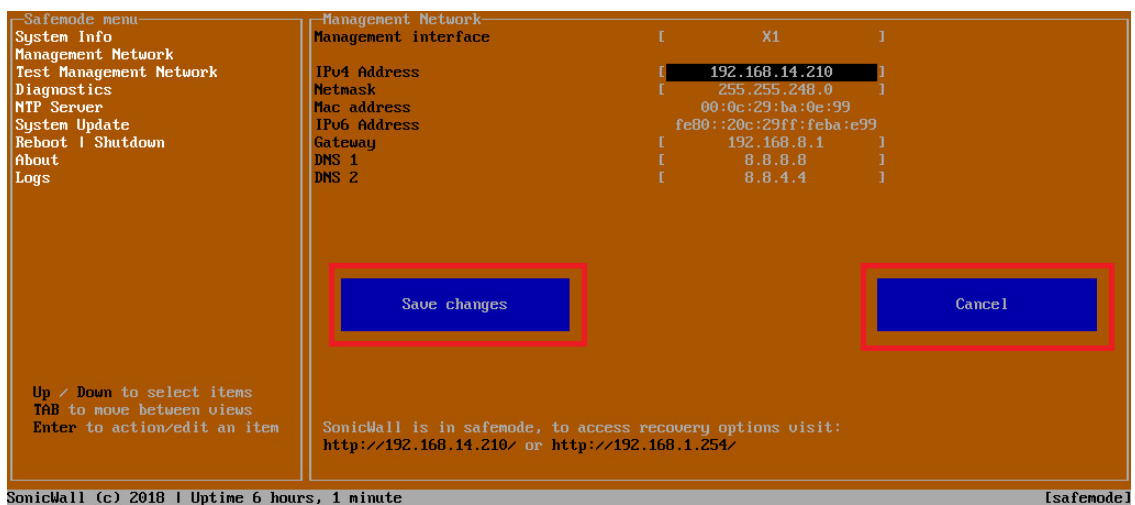
To edit an interface:

- 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 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** 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.

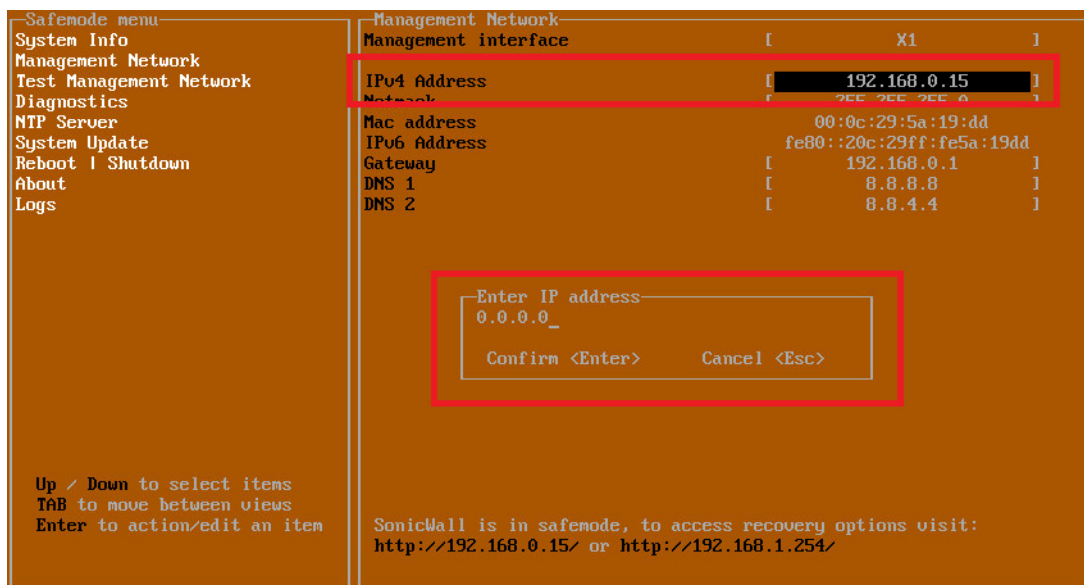
- 3 Select the interface you wish to edit and press **Enter**.

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.

Management Network		
Management interface	[X1]
IPv4 Address	[Not configured]
Netmask	[]
Mac address	00:0c:29:5a:19:dd	
IPv6 Address	fe80::20c:29ff:fe5a:19dd	
Gateway	[192.168.0.1]
DNS 1	[8.8.8.8]
DNS 2	[8.8.4.4]

Installing a New SonicOS Version 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 NSv appliance. The SafeMode web management interface is used to perform an upgrade, rather than SafeMode in the NSv management console. When viewing the NSv management console in SafeMode, the URL for the SafeMode web interface is displayed at the bottom of the screen.

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

To install a new SonicOS from SafeMode:

- 1 With the NSv in SafeMode, view the NSv management console. At the bottom of the screen, the URL for the SafeMode web management interface is displayed.
- 2 In a browser, navigate to the URL provided at the bottom of the Management Console screen. The SafeMode web management interface displays.

SONICWALL™ Network Security Virtual

SonicOS is running in Safe Mode

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

> Download the Safe Mode Logs for troubleshooting by the SonicWall Support Team

> Upload new SonicOS application images

> Boot your choice of application image

> Restore the settings to their factory default values

Download Safe Mode Logs

SonicOS Product Info

Model: NSv Unlicensed

Product Code: 70000

GUID:

Serial Number:

Image Management

Restart

Refresh

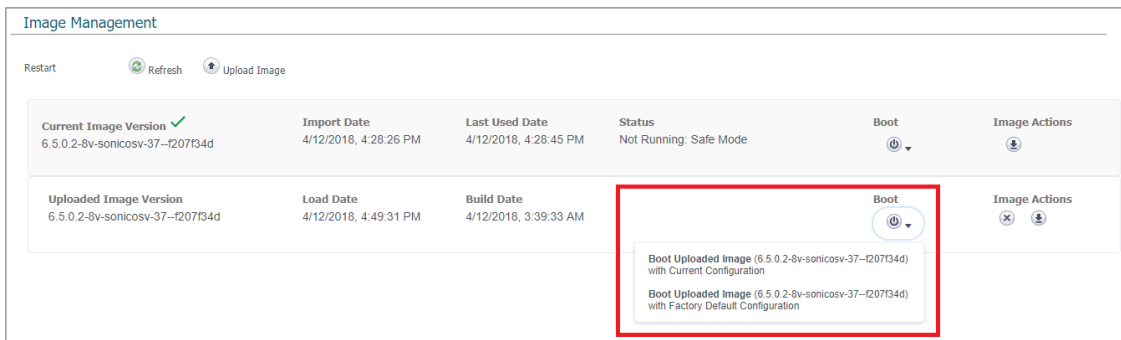
Upload Image

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

- 3 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.

4 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 appliance reboots with the new image.

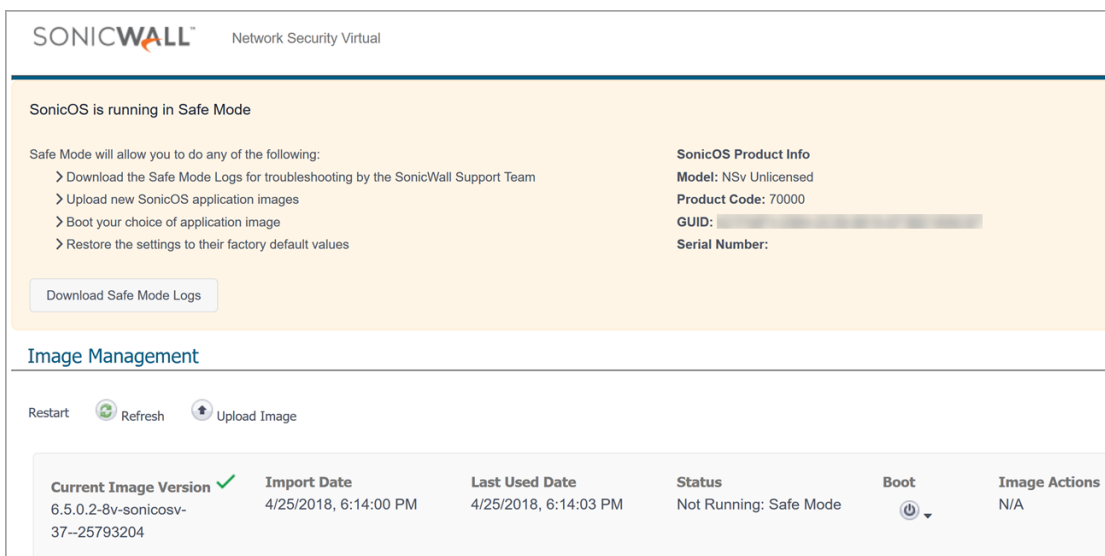
Downloading Logs in SafeMode

When the NSv appliance is in SafeMode, extra logging information is kept that can be downloaded. The logs are available from the SafeMode web management interface, which can be accessed via the URL provided at the bottom of the Management Console screen.

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

To download logs from SafeMode:

- 1 With the NSv in SafeMode, view the NSv management console. At the bottom of the screen, the URL for the SafeMode page in the web UI is displayed.
- 2 In a browser, navigate to the URL provided at the bottom of the Management Console screen. The SafeMode web management interface displays.



- 3 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.

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 on ESXi Getting Started Guide

Updated - August 2020

Software Version - 7.0.0

232-005388-01 Rev A

Copyright © 2020 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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. SonicWall Inc. 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/en-us/legal/license-agreements>. Select the language based on your geographic location to see the EUPA that applies to your region.

Open Source Code

SonicWall 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
SonicWall Inc. Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035