SonicOS and SonicOSX 7

NSv Getting Started Guide

for Azure

SONIC**WALL**®

Contents

Introducing the NSv Series

This SonicWall® SonicOS/X 7 NSv Getting Started Guide describes how to install SonicWall NSv and provides basic configuration information.

To jump directly to the installation instructions, go to Installing SonicOS/X on the NSv Series.

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

Topics:

- Feature Support Information
- Product Matrix and Requirements
- Github Repository
- Backup and Recovery Information
- Exporting and Importing Firewall Configurations
- Upgrading from SonicOS 6.5
- Upgrading to a Higher Capacity NSv Model
- Creating a MySonicWall Account

Feature Support Information

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

For more information about supported features, go to the *Technical Documentation Portal*.

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

FEATURE SUPPORT LIST

Functional Category	Feature Area	Feature
Unified Security Policy	Unified Policy combining Layer 4 to Layer 3 Rules	Source/Destination IP/Port/Service
		Application based Control
		CFS/Web Filtering
		Botnet
		Geo-IP/country
		Single Pass Security
		Services enforcement
		Decryption Policy
		DoS Policy
		EndPoint Security Policy
		Rule Diagram
	Profile Based Objects	
		Endpoint Security
		Bandwidth Management
		QoS Marking
		Content Filter
		Intrusion Prevention
		DHCP Option
		AWS VPN
	Action Profiles	
		Security Profile
		DoS Profile
	Signature Objects	
		AntiVirus Signature Object
		AntiSpyware Signature Object
	Rule Management	
		Cloning
		Shadow rule analysis
		In-cell editing
		Group editing
		Export of Rules
		LiveCounters
	Managing Views	

Functional Category	Feature Area	Feature
		Used/unused rules
		Active/inactive rules
		Sections
		Customizable Grid/Layout
		Custom Grouping
TLS 1.3	**Supporting TLS 1.3 with enhanced security**	
SDWAN	**SDWAN Scalability**	
	SDWAN Usability Wizard	
API	**API Driven Management**	
	Full API Support	
Dashboard	**Enhanced Home Page**	
		Actionable Dashboard
		Enhanced Device View
		Top Traffic and User summary
		Insights to threats
		Policy/Object Overview
		Profiles and Signatures Overview
		Zero-Day Attack Origin Analysis
	Notification Center	
Debugging	**Enhanced Packet Monitoring**	
	UI based System Logs Download	
	SSH Terminal on UI	
	System Diagnostic Utility Tools	
	Policy Lookup	
Capture Threat Assessment (CTA 2.0)	**Executive Template**	
	Customizable Logo/Name/Company	
	Industry and Global Average Statistics	
	Risky File Analysis	
	Risky Application Summary	

Functional Category	Feature Area	Feature
	Malware Analysis	
	Glimpse of Threats	
Monitoring	Risky Application Summary	
	Enhanced AppFlow Monitoring	
Management	CSC Simple Reporting	
	ZeroTouch Registration and Provisioning	
General	SonicCoreX and SonicOS/X Containerization	
	Data Encryption using AES-256	
	Enhanced Online Help	

ⓘ **NOTE:** Per Microsoft, "Azure does not support any Layer-2 semantics." Therefore, SonicOS/X Layer 2 functionality is disabled in NSv deployments. Consequently, NSv virtual machines do not support VLAN interfaces and DHCP Server functionality. See https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq and https://support.microsoft.com/en-us/help/2721672/microsoft-server-software-support-for-microsoft-azure-virtual-machines for more information.

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

Product Matrix and Requirements

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

Product Models	NSv 270	NSv 470	NSv 870
Maximum Cores[1]	2	4	8
Minimum Total Cores	2	2	2
Management Cores	1	1	1
Maximum Data Plane Cores	1	3	7
Minimum Data Plane Cores	1	1	1
Network Interfaces	2	4	8
Supported IP/Nodes	Unlimited	Unlimited	Unlimited
Minimum Memory Required [2]	6G	8G	10G
Minimum Hard Disk/Storage	35G	35G	35G

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

MEMORY REQUIREMENTS ON NSV WITH JUMBO FRAMES ENABLED VS DISABLED

NSv Model	Minimum Memory – Jumbo Frames Enabled	Minimum Memory – Jumbo Frames Disabled
NSv 270	10G	8G
NSv 470	14G	10G
NSv 870	18G	12G

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

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

Backup and Recovery Information

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

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Contact SonicWall Technical Support for assistance.

- If the disk is not recoverable, then the NSv virtual machine needs to be deregistered with MySonicWall. Contact technical support for more information.

- If SonicOS/X does not boot up, you can go into SafeMode and download the log files, upload a new SonicOS/X image, or take other actions. For more information about SafeMode, see Using SafeMode on the NSv.

- If SonicOS/X fails three times during the boot process, it boots into SafeMode. Verify that the minimum required memory is available and allocated based on the NSv model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall Technical Support for assistance.

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

Exporting and Importing Firewall Configurations

Moving configuration settings from SonicWall physical appliances to the NSv is not supported. However, configuration settings can be moved from one SonicOS/X 7 NSv to another or from an NSv running SonicOS

6.5.4.4 to an NSv running SonicOS 7.0.1 or higher (but not SonicOSX).

Go to https://www.sonicwall.com/support/technical-documentation/ for more information about exporting and importing configuration settings. Search for **SonicOS/X 7 updates and upgrades**.

Github Repository

SonicWall NSv templates are available in the Github repository:

- https://github.com/sonicwall
- https://github.com/sonicwall/sonicwall-nsv-azure-templates

Upgrading from SonicOS 6.5

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

ⓘ | **NOTE:** Upgrading to SonicOS/X 7 from SonicOS 6.5.4 requires a Secure Upgrade Path key that must be purchased separately. You can choose from any of the following:
- SONICWALL NSV 270 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 470 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 870 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 270 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 470 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 870 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)

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

1. Purchase a Secure Upgrade license key.

2. Log into MySonicWall and register the Secure Upgrade serial number. Enter a descriptive "friendly" name in the available field, shown here as "SecureUpgrade1."

3. Click **Choose management options**.

4. In the **Secure Upgrade** popup window, select **Register Only** at the top.

5. Select the Trade-In Unit from the list of registered NSv instances. This is the SonicOS 6.5.4.v NSv instance to be upgraded to SonicOS 7.

6. Click **Done** after selecting the Trade-In Unit. The Secure Upgrade serial number is then registered to your MySonicWall account.

7. The action item Secure Upgrade Transfer is added to the To do list at the bottom of the page.

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

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

   ⓘ | **NOTE:** If you do not perform the service transfer within 60 days, the transfer is performed automatically.

8. Deploy a new SonicOS 7 NSv instance with the desired model and platform.

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

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

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

11. Log into the SonicOS 7 NSv and import the configuration settings.

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

Upgrading to a Higher Capacity NSv Model

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

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

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

Creating a MySonicWall Account

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

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

To create a MySonicWall account:

1. In your web browser, navigate to https://www.mysonicwall.com.

2. In the login screen, click the **Sign Up** link.
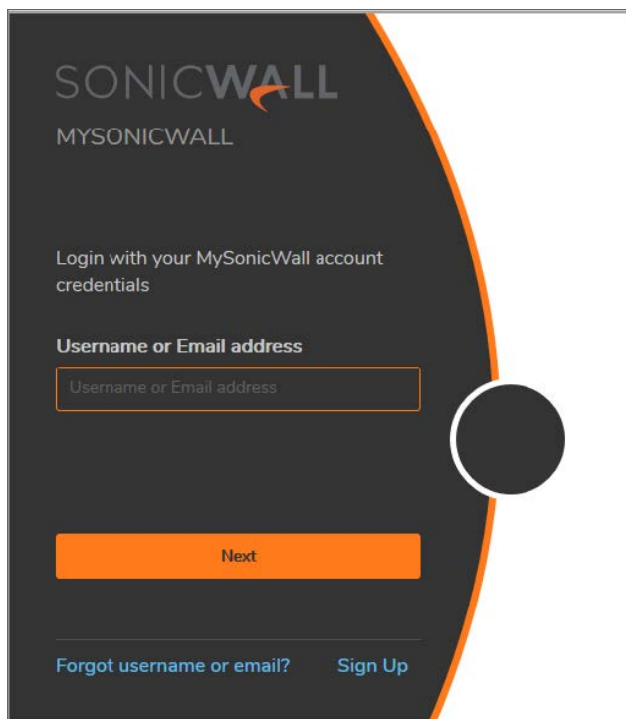
3. Complete the account information, including email and password.

4. Enable two-factor authentication if desired.

5. If you enabled two-factor authentication, select one of the following authentication methods:

    - **Email (one-time passcode)** where an email with a one-time passcode is sent each time you log into your MySonicWall account.

    - **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code. After the code is scanned, you need only click a button.

6. Click **Continue** to go to the **COMPANY** page.

7. Complete the company information and click **Continue**.

8. On the **YOUR INFO** page, select whether you want to receive security renewal emails.

9. Identify whether you are interested in beta testing of new products.

10. Click **Continue** to go to the **EXTRAS** page.

11. Select whether you want to add additional contacts to be notified for contract renewals.

12. If you opted for additional contacts, input the information and click **Add Contact**.

13. Click **Finish**.

14. Check your email for a verification code and enter it in the **Verification Code** field. If you did not receive a code, contact Customer Support by clicking on the link.

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

Installing SonicOS/X on the NSv Series

Topics:

- Supported NSv Models
- Task List for an NSv Virtual Machine Setup
- Installing NSv on Azure
- Accessing Your NSv in the Azure Portal
- Forwarding Traffic to Your NSv
- Testing Traffic Through Your NSv
- Troubleshooting Installation Configuration

Supported NSv Models

Determine the NSv instance type required before starting installation.

NSV MODELS (VIRTUAL MACHINE SIZES)

SonicWall NSv Model	Azure	Interface Count[1]	Core Count
NSv 270	Standard D2 v2	2	2
NSv 470	Standard D3 v2	4	4
NSv 870	Standard D4 v2	8	8

ⓘ **NOTE:** The maximum number of NICs supported by SonicWall NSv is always eight for all models. But the total number of interfaces in an NSv instance could be constrained by the NSv virtual machine.

For NSv sizing and pricing information, see:

- https://azure.microsoft.com/en-us/pricing/details/virtual-machines/linux/
- https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes-general

[1]The maximum number of interfaces supported on an NSv instance is defined by the type of Azure virtual machine. For example, if more than two interfaces are required for an NSv 270, use the NSv 270 with an Azure virtual machine supporting a higher number of interfaces.

Task List for an NSv Virtual Machine Setup

The process for setting up an NSv virtual machine is summarized in three main tasks:

1. Install the NSv virtual machine

    • Installing NSv on Azure

2. Register the NSv on MySonicWall

    • Registering the NSv Appliance from SonicOS/X

3. Configure traffic forwarding to the NSv

    • Forwarding Traffic to Your NSv in Azure

    • Testing Traffic Through Your NSv in Azure

Installing NSv on Azure

SonicWall NSv is deployed on Azure by using a solution template. The template is a JSON file, which is loaded into Azure through a web page. Templates are a means to deploy virtual machines in Azure while also creating/modifying existing resources. Templates use the Azure Resource managers to support not just the deployment of the NSv but also of other virtualized network functions.

This section details two deployment procedures:

    • To install from Azure Marketplace

    • To Install from an Azure template

To install from Azure Marketplace:

1. In your browser, navigate to https://portal.azure.com/ and log into your Microsoft Azure account.

2. Navigate to SonicWall NSv on Azure Marketplace at https://azuremarketplace.microsoft.com/en-us/marketplace/apps/sonicwall-inc.sonicwall-nsv-firewall-security-vpn-router, click **GET IT NOW**, and then click **Continue** to display the *SonicWall NSv (Firewall/Security/VPN/Router)-BYOL* page.

3. On the **SonicWall NSv (Firewall/Security/VPN/Router)-BYOL** page, click **Create** at the bottom to get started.

The **Basics** screen of the NSv configuration window displays.
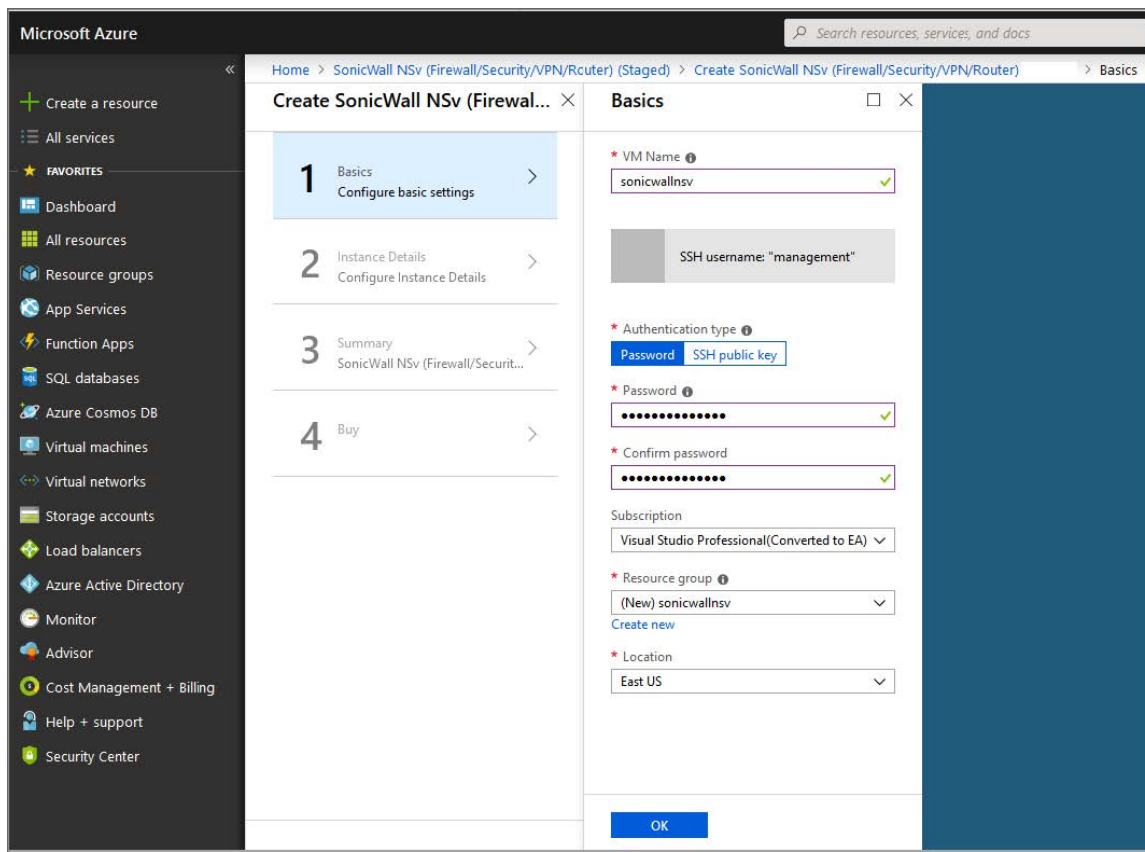
4. On the **Basics** screen, configure the following options:

    - **VM Name** – Type in a descriptive name for this NSv instance. Consider using lowercase letters, numbers and hyphens, as this name is used to create the default DNS Prefix, which has some restrictions. You can, however, adjust the DNS Prefix as needed.

      The value for 'DNS Prefix for the public IP Address' must match the regular expression '^$|^[a-z][a-z0-9-]{1,61}[a-z0-9]$'

      (i) **NOTE:** The **SSH username** is set to *management* by default. This is the user name for accessing the NSv console using SSH. This is not the NSv administrator user name, but is a user name created as part of an NSv deployment.

- **Authentication type** – Select either **SSH public key** or **Password** as the authentication method for the previous management **SSH username**. The default for the template is **Password**.

    - If you selected **Password** for **Authentication Type**, type the desired password into the **Password** and **Confirm password** fields. The password must be between 12 and 72 characters in length and contain at least three of the following character types:

        - Uppercase character
        - Lowercase character

- Number

- Special character (non-alpha-numeric, such as !@#$%^&*()_+}{"|:>?<)

- If you selected **SSH public key** for **Authentication Type**, type the SSH RSA public key file name as a string into the **SSH Public Key** field.

- **Subscription** – Select the Azure subscription on which to deploy the resources for this NSv instance.

- **Resource group** – **Create new** or select an existing resource group from the list.

  A resource group is a user defined friendly name for a collection of resources. If you are deploying on Azure for the first time, click **Create new**. If you already have a network configured and some virtual machines, then you might wish to use an existing resource group. If you are deploying for test purposes, consider creating a new resource group so you can easily delete the resources, if needed.

  - If you select **Create new**, type a name for this resource group into the associated text field, and then select a location for it from the **Location** drop-down menu.

  - If you select **Use existing**, select the resource group to use from the associated drop-down menu.

- **Location** – Select the Azure location where the resources are deployed.

5. Click **OK** to continue.

   The **Instance Details** screen displays.
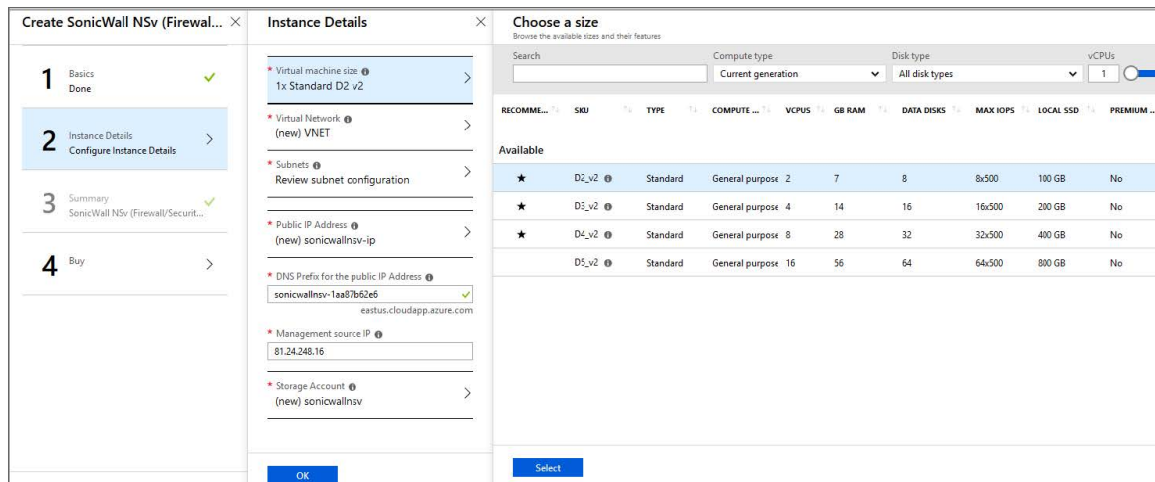
6. Select **Virtual machine size**, then select the row with the equivalent for the NSv model you want to deploy in the **Choose a size** screen. Click **Select**.

Virtual Machine Size in NSv	NSv Model
Standard_D2_v2	NSv 270
Standard_D3_v2	NSv 470
Standard_D4_v2	NSv 870

7. Select **Virtual Network** to configure the virtual network. **Create new** under **Choose virtual network** is selected by default and the **Create virtual network** settings are displayed.
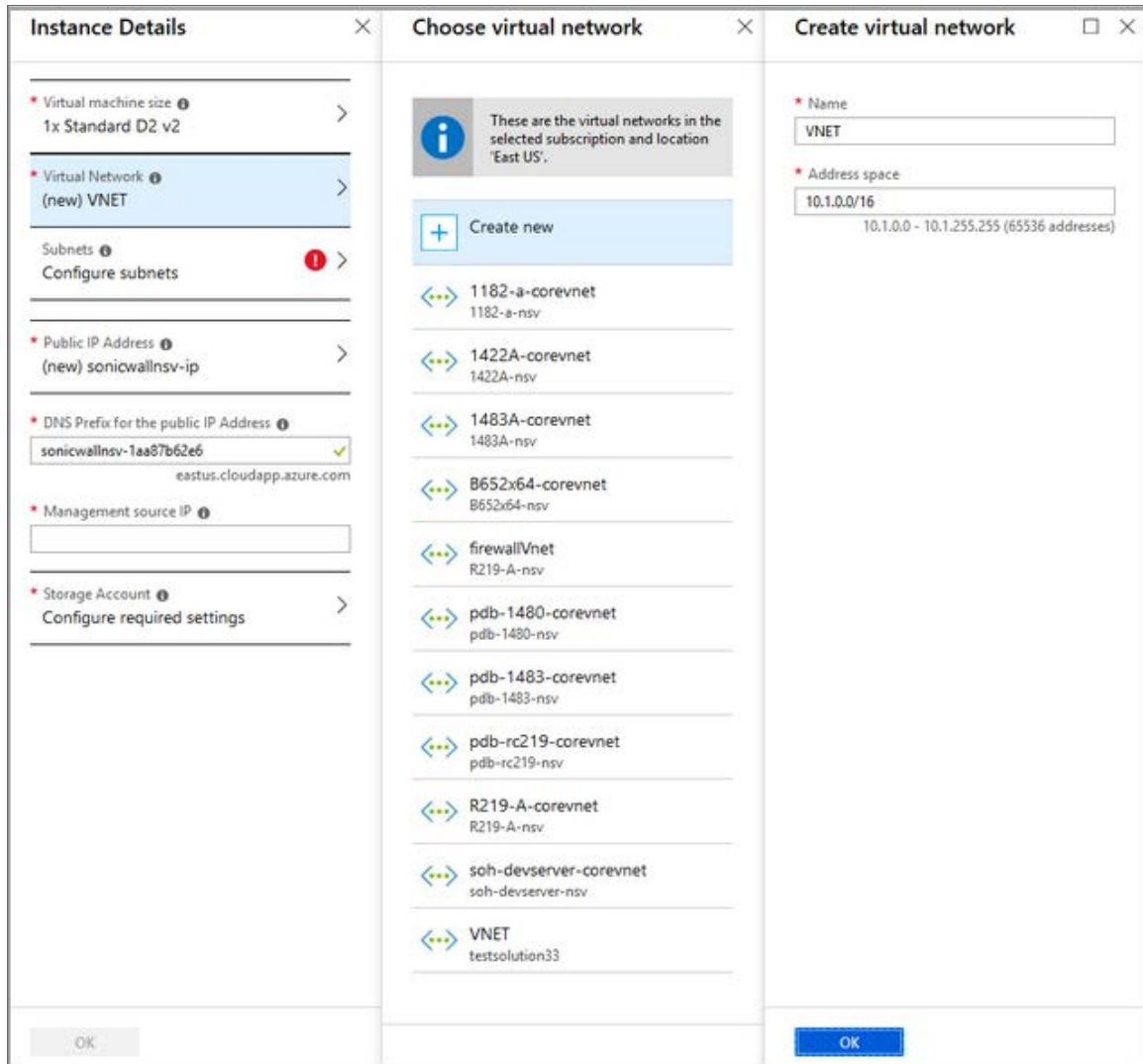
Under **Create virtual network**:

- **Name** – This is the name of virtual network the NSv is deployed on. Leave the default, **VNET**.

- **Address space** – The template default is `10.1.0.0/16`. This is a network address in CIDR format representing the virtual network address space. Accept the default or optionally configure a different address space, using the same format.

8. Click **OK**.

9. Select **Subnets** to configure the subnets for the WAN and LAN zones.
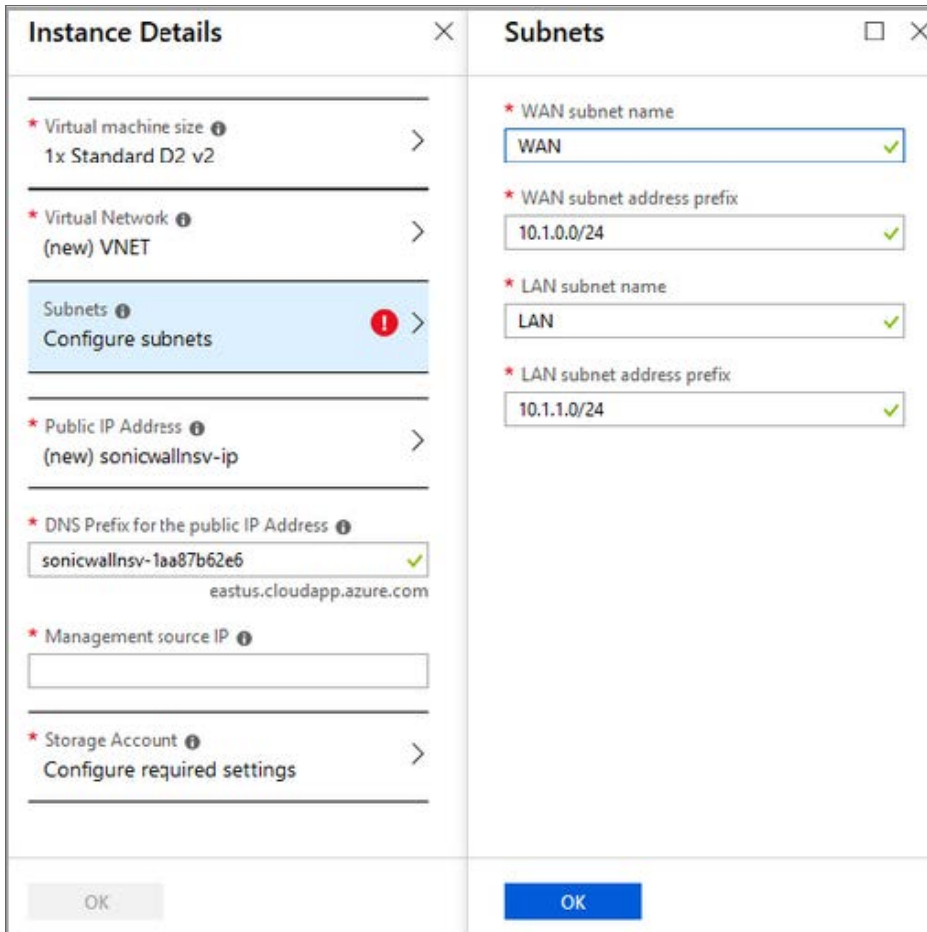
- **WAN subnet name** – The name of the WAN subnet. The default is WAN. If you have an existing network on Azure you might want to change the value.

- **WAN subnet address prefix** – A sub-network of the Address space configured in Step 7, defined for WAN traffic. For example, `10.1.0.0/24`.

- **LAN subnet name** – The name of the LAN subnet. The default is LAN. If you have an existing network on Azure you might want to change the value.

- **LAN subnet address prefix** – A sub-network of the Address space configured in Step 7, defined for LAN traffic. For example, `10.1.1.0/24`.

10. Click **OK**.

11. Select **Public IP Address**. **Create new** is selected by default and the **Create public IP address** settings are displayed. You also have the option to select an existing public IP address to reassign it for use with your NSv.
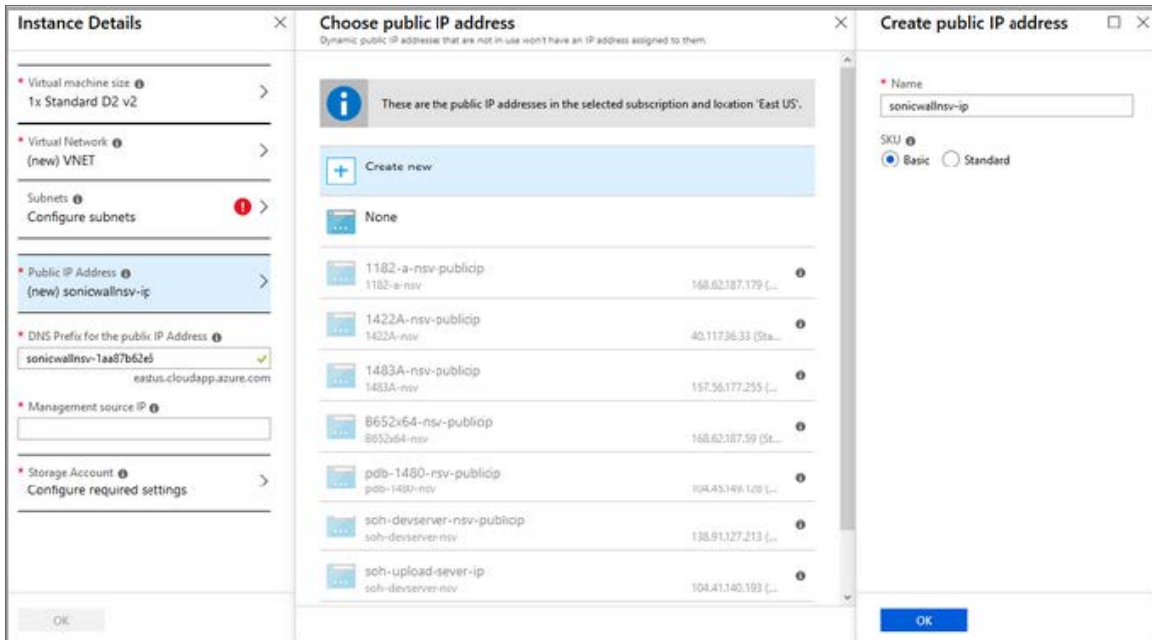
- Under **Create public IP address**, accept the prepopulated name or type a different name into the **Name** field.

- For **SKU**, select **Basic** or **Standard**. The default is **Basic**.

- For **Assignment** (if displayed), select **Dynamic** or **Static**. The default is **Dynamic**.

12. Click **OK**.

13. In the **DNS Prefix for the public IP Address** field, configure the DNS name for the NSv. This must be a unique DNS name for accessing the management interface of the NSv virtual machine. When the NSv virtual machine is created, the WAN uses a public IP and is assigned the DNS name defined here.

Instance Details ☐ ✕

---

* Virtual machine size ℹ   ❯
1x Standard D2 v2

---

* Virtual Network ℹ   ❯
(new) VNET

---

* Subnets ℹ   ❯
Review subnet configuration

---

* Public IP Address ℹ   ❯
(new) sonicwallnsv-ip

---

* DNS Prefix for the public IP Address ℹ
| sonicwallnsv-1aa87b62e6 ✓ |

eastus.cloudapp.azure.com

* Management source IP ℹ
| 81.24.248.16 ✓ |

---

* Storage Account ℹ   ❯
Configure required settings

OK
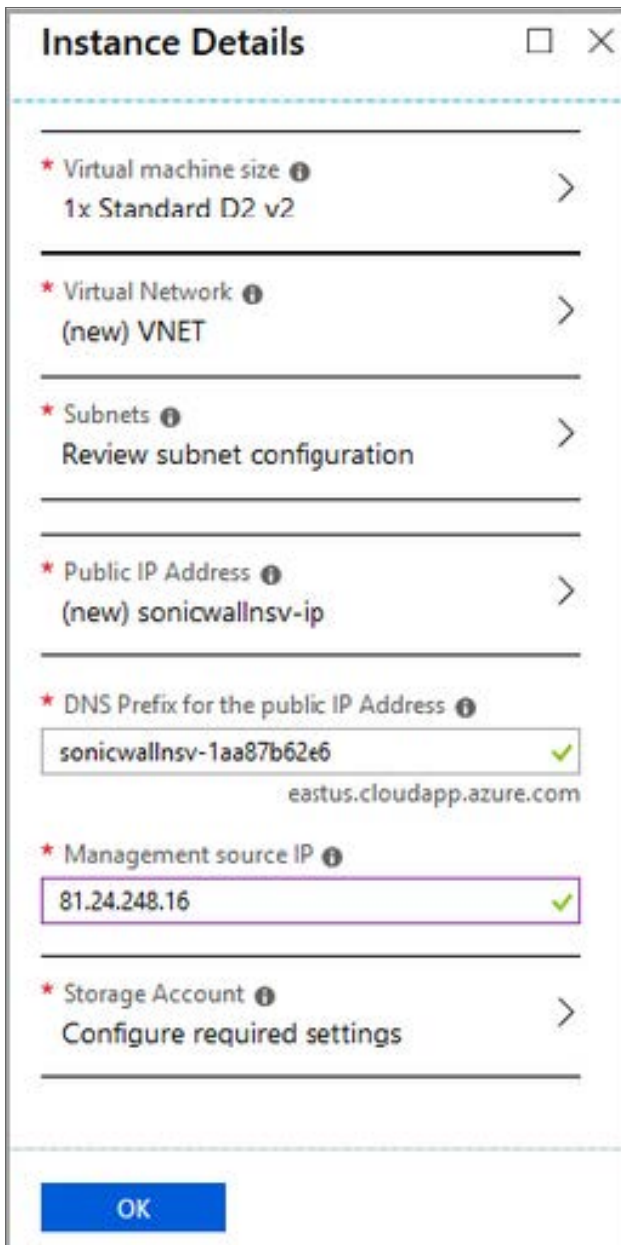
14. In the **Management source IP** field, type in the public IP address that is allowed to access this NSv virtual machine for HTTPS and SSH management.

    You can find out your public IP address by typing **what is my IP** into Google or another search engine in a different browser window/tab. Additional addresses can be added later in Azure.

15. Select **Storage Account**. **Create new** is selected by default, displaying the **Create storage account** settings. You also have the option to select an existing storage account.
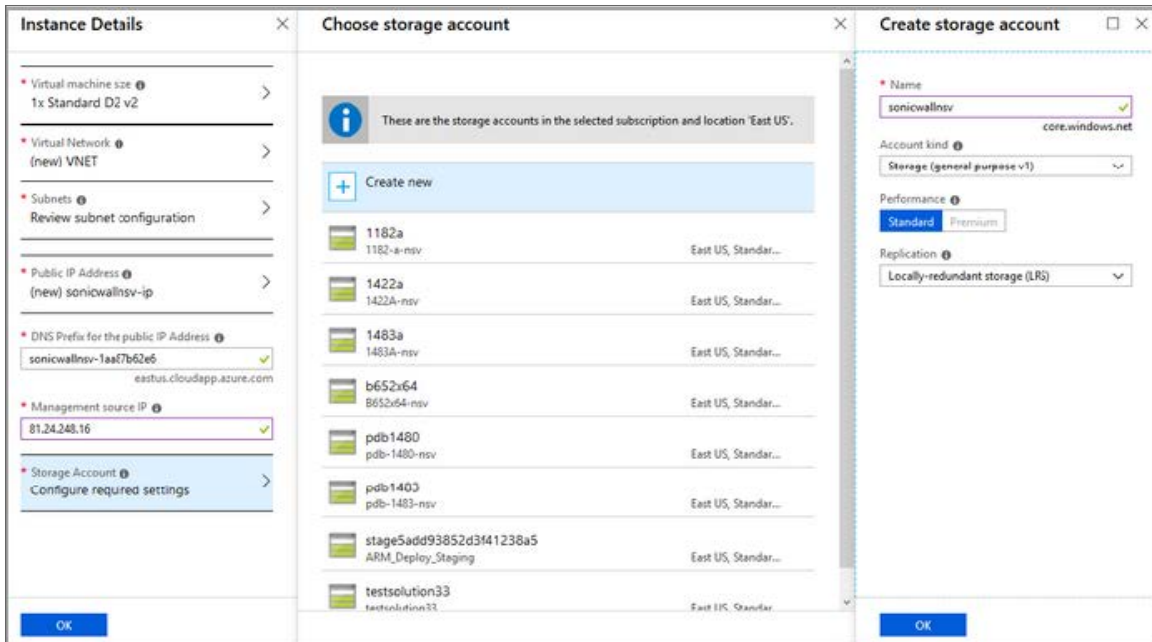
- For a new storage account, type in a unique **Name** for the storage account using only lowercase letters and numbers.

- Select the desired options for **Account kind**, **Performance**, and **Replication**.

- Click **OK**.

16. Click **OK** at the bottom of the **Instance Details** pane.

The **Summary** screen displays.
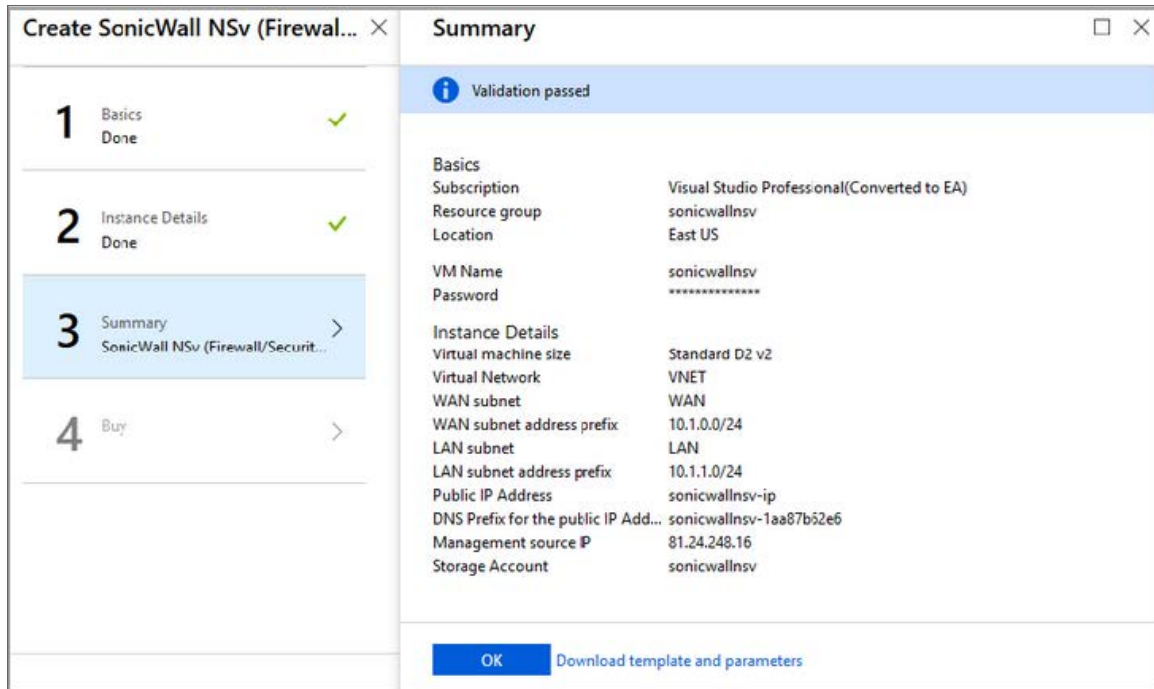
17. Confirm the settings and then click **OK**.

    The **Buy** screen displays.
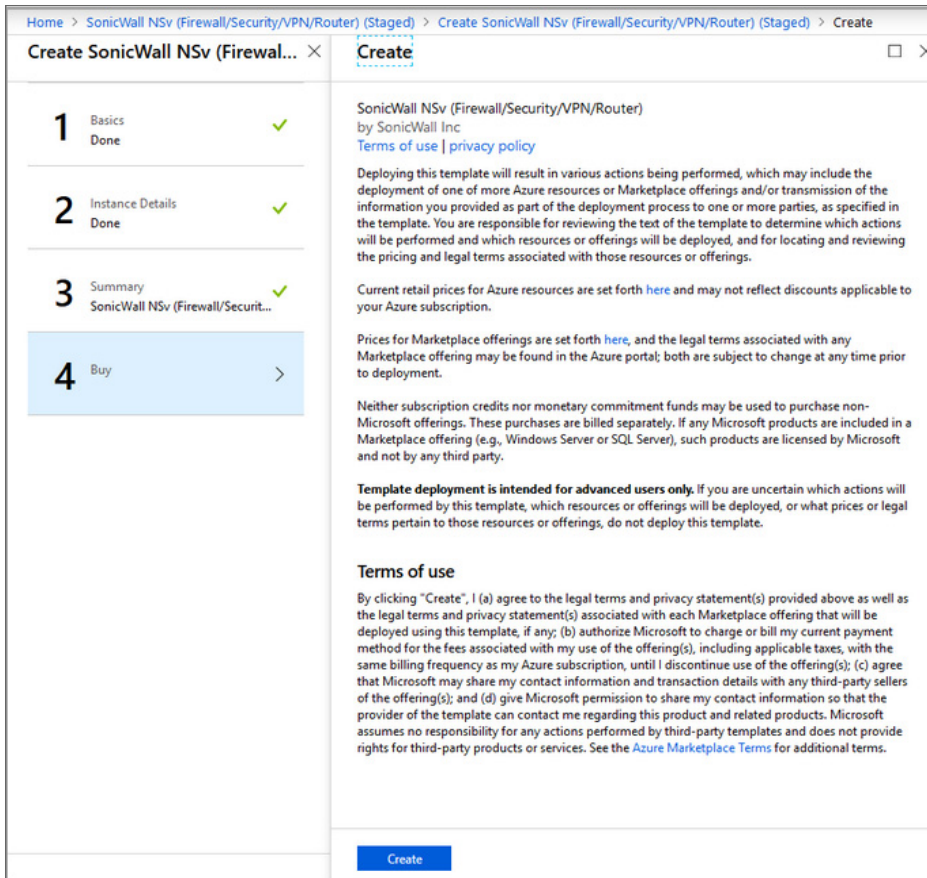
18. Read the **Azure Terms of use | privacy policy** and then click **Create** to agree to the terms and purchase the NSv instance.

    Azure begins the deployment process and displays the Azure **Dashboard** page.

    You can click the **Notifications** icon at the top to display the **Deployment in progress** notification window, then click **Deployment in progress** to view the progress.
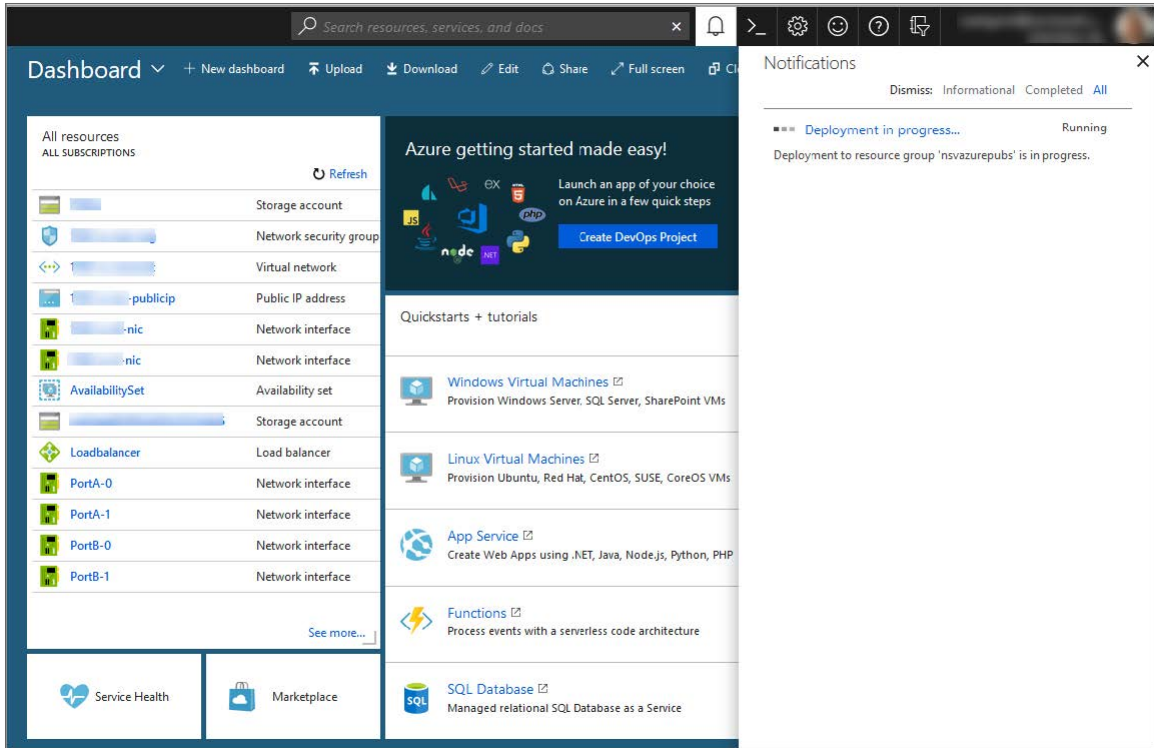
When finished, the notification window displays **Deployment succeeded**.
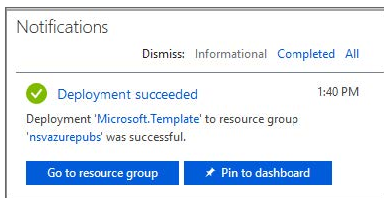
See Accessing Your NSv in the Azure Portal for more information about accessing the pages and settings for your NSv virtual machine available in the Azure portal.

The next step is to register your NSv virtual machine on MySonicWall. See Registering the NSv Virtual Machine with SonicOS/X for more information about registering your See Accessing Your NSv in the Azure Portal for more information about accessing the pages and settings for your NSv virtual machine available in the Azure portal.

After you have registered the NSv, see Forwarding Traffic to Your NSv for more information about accessing the pages and settings for your NSv virtual machine.

To Install from an Azure template:

Templates are a means to deploy virtual machines in Azure while also creating/modifying exiting resources. There are a few different types of templates: Quick, Solution and Simple. The following is an example of a Simple template that creates resources and defines their interconnections.

- Virtual Machine
- Storage Group

- Public IP

- 2 x Network Interfaces

- Virtual Network

- Network Security Policy

Deploying NSv by way of Templates:

1. Log into Azure.

2. Click to load the webpage: https://github.com/sonicwall/sonicwall-nsv-azure-templates

3. Click **Deploy to Azure.**

4. The **Custom Deployment** page should come up:
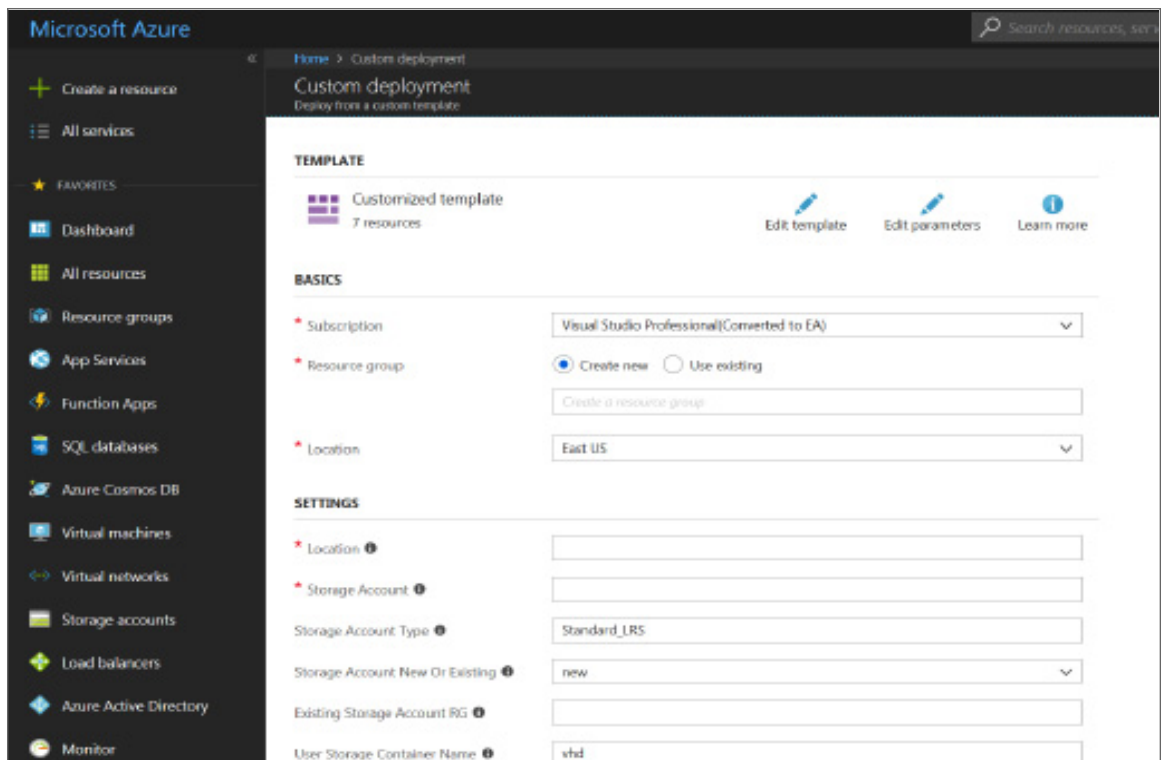
Enter information to define the custom deployment:

- **Resource Group**: The user-defined friendly name for a group of resources.

  If you are deploying on a Azure for the first time, use "Create New," however, if you already have a network configured, and some virtual machines then you might wish to use an existing resource group. If you are deploying for test purposes, we suggest you create a new resource group so you can easily delete the resources later if needed.

- **Location**: The region where you wish to deploy.

- **Storage Account**: A new or existing storage account (we recommend you create a new storage account).

- **Storage Account Type**: The type of storage account you wish to use or create.

  Currently only "Standard_LRS" is recommended.

- **Storage Account New or Existing**: Whether you wish to create or use an existing stage account.

- **User Storage Container Name**: The name of the container where the VHD file is stored.

- **DNS Name for Public IP**: When the See Accessing Your NSv in the Azure Portal for more information about accessing the pages and settings for your NSv virtual machine available in the Azure portal.

- The next step is to register your NSv virtual machine on MySonicWall. See Registering the NSv Virtual Machine with SonicOS/X for more information about registering your NSv.

- After you have registered the NSv, see Forwarding Traffic to Your NSv and Testing Traffic Through Your NSv for more information about forwarding traffic to it.

- A virtual machine is created, the WAN uses a public IP, this WAN IP is assigned a DNS name defined here.

- **SSH User Name**: The user name required to SSH into the NSv virtual machine.

  This is not the NSv administrator's user name, but rather a username created as part of an NSv deployment.

- **Authentication Type**: Select either "password" or "sshPublicKey" as the authentication method.

- **SSH Password**: The password for the previously mentioned SSH user.

  Password must contain one non alpha-numeric character (such as !@#$%^&*()_+}{"|: >?<), one uppercase alphanumeric character and one numeric character.

- **Management Access IP Source**: Public IP address to allowed access to SonicWall NSv HTTPS & SSH management.

- **VM Size**: Select the virtual machine you wish to deploy:

SonicWall NSv Model	Azure
NSv 270	Standard D2 v2
NSv 470	Standard D3 v2
NSv 870	Standard D4 v2

- **Base URL**: This is the location of the template resources.

  This should remain at the default value unless you are creating your own template.

- **Virtual Network Name**: The name of the virtual network the NSv is deployed on.

  If you have an existing network on Azure, and would like to install the NSv on this network then this field should be populated with the network name. For example, `192.168.0.0/26`.

- **Virtual Network Address Prefix**: The virtual network "Address space."

- **Subnet WAN Name**: The name of the WAN subnet.

  If you have an existing network on Azure, you might want to change the default value or it can remain at the default.

- **Subnet LAN Name**: The name of the LAN subnet.

  If you have an existing network on Azure you might want to change the default value else it can remain at default.

- **Subnet WAN prefix**: A sub-network of the previous "Virtual Network Address Prefix" defined for WAN traffic, such as `192.168.2.0/24`.

- **Subnet LAN prefix**: A sub-network of the previous "Virtual Network Address Prefix" defined for LAN traffic, such as `192.168.2.0/24`.

- **Subnet WAN Start Address**: The starting address from which the virtual network provides through DHCP addresses to host on the WAN subnet.

- **Subnet LAN Start Address**: The starting address from which the virtual network provides through DHCP addresses to host on the LAN subnet.

5. After filling in all the values, click **I agree to the terms and conditions stated above** and then click **Purchase** to deploy the template and create the SonicWall NSv instance.

It takes approximately 10 minutes to deploy NSv respective resources. You can view the progress by clicking the icons indicated in the following image:
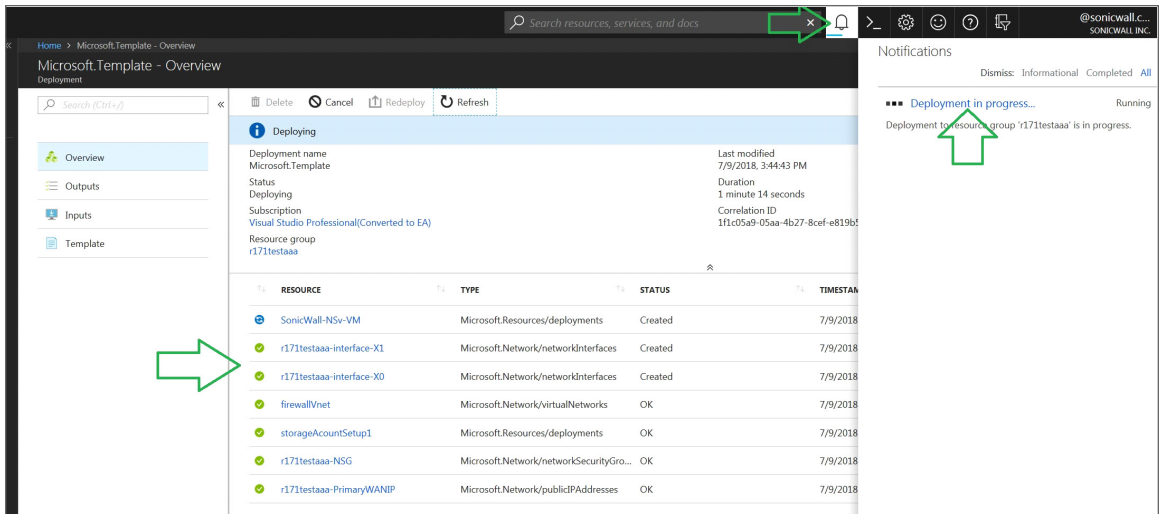
6. To connect to the SonicWall NSv management GUI click **Virtual Machines** from the left menu. Then select the NSv virtual machine name, in the overview section a public IP address is displayed, In the example that follows, that is `http://40.76.216.87/.`
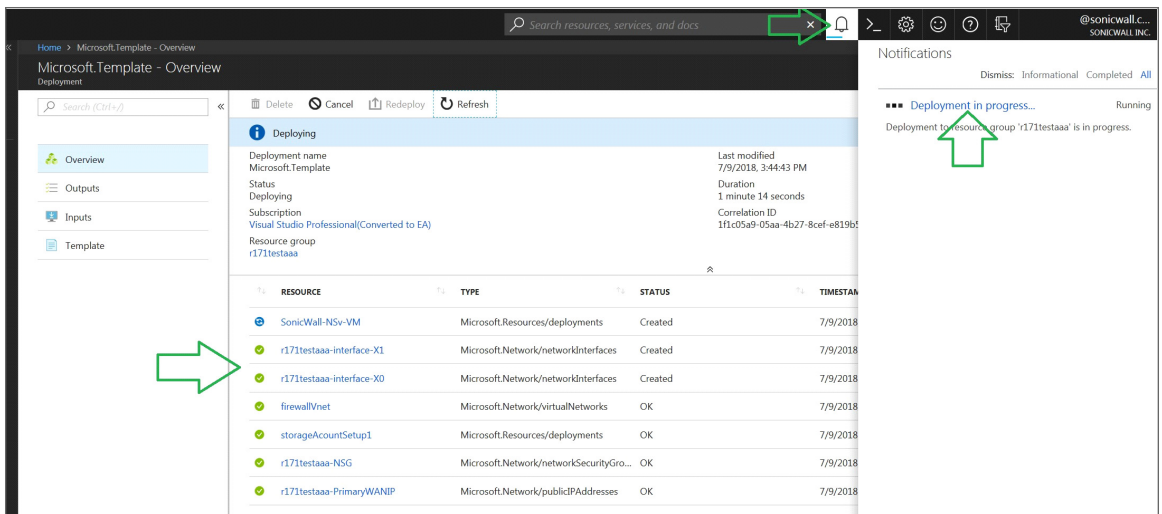
7. Login with the default SonicWall credentials "`admin/sonicwall`."
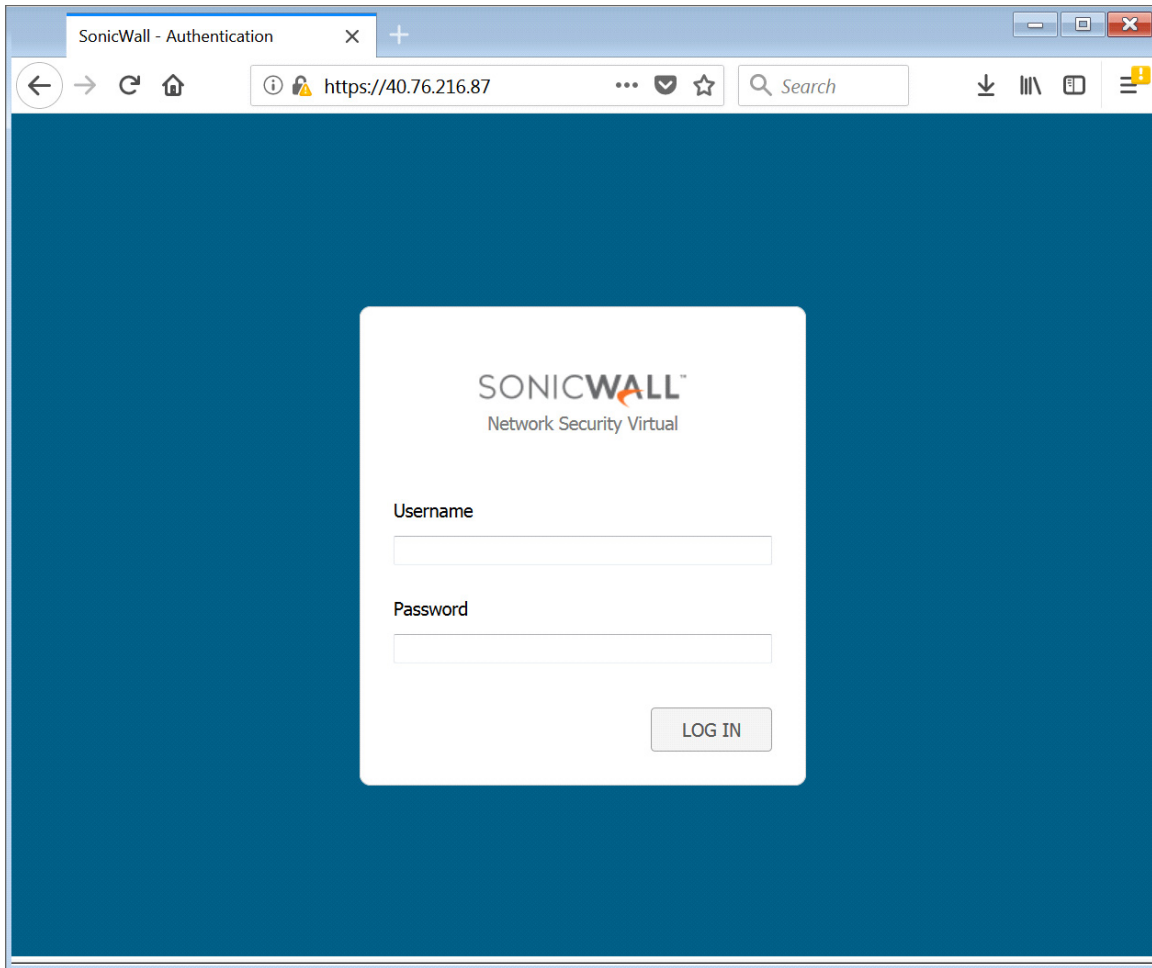
8. Now continue with the following section,Accessing Your NSv in the Azure Portal, or go on to Installing NSv on Azure.

Accessing Your NSv in the Azure Portal

There are a number of pages and settings for your NSv virtual machine available in the Azure portal.

Topics:

- Updating Your Dashboard and Accessing the NSv Resource Group
- Finding the Public IP Address of Your NSv
- Logging into Your NSv for SonicOS/X Management
- Viewing and Configuring Security Rules

Updating Your Dashboard and Accessing the NSv Resource Group

The notification window for **Deployment succeeded** provides two buttons for your immediate use.
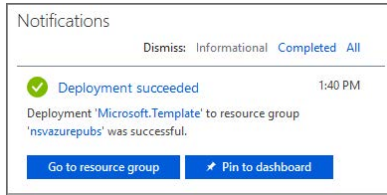
- Click **Pin to dashboard** to add links to your new NSv and its Azure configuration pages to your Azure **Dashboard** page. Click **Refresh** on the **Dashboard** page to view your new virtual machine, storage account, and network interface on the **Dashboard**.
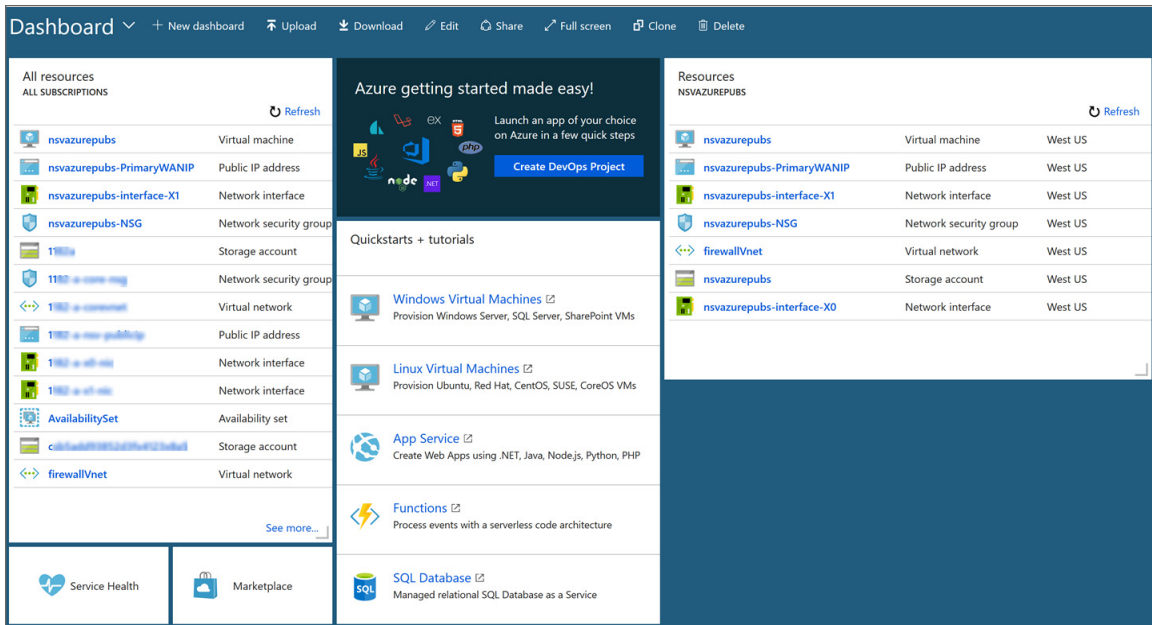
- Click **Go to resource group** to display the **Resource group** page.
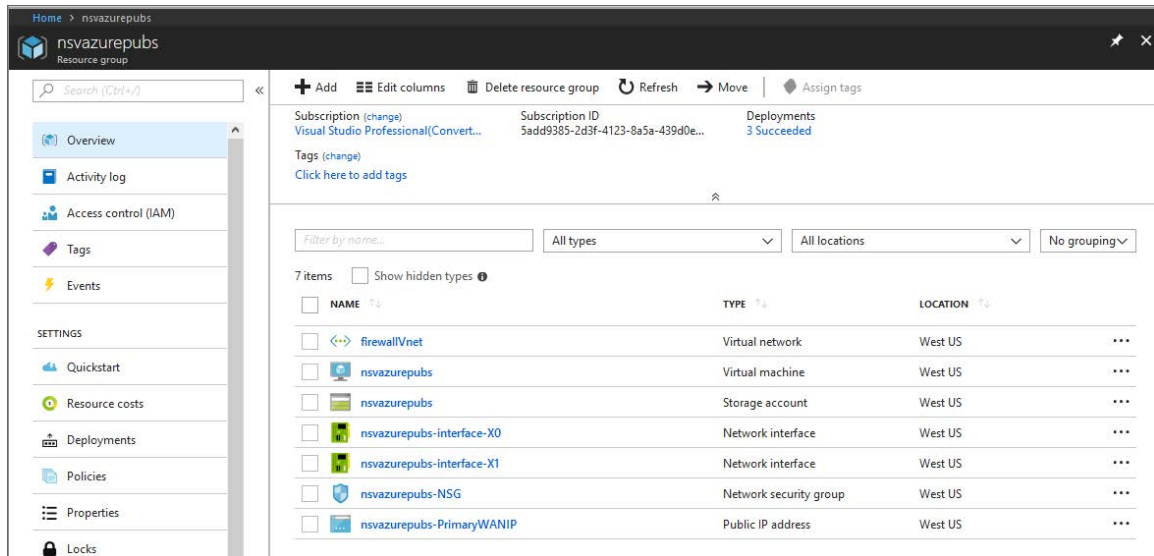
Finding the Public IP Address of Your NSv

On the **Dashboard** page or the **Resource group** page, click the virtual machine name link to display the **Public IP address** of your NSv virtual machine. The virtual machine name link has a description or type of **_Virtual machine_**.
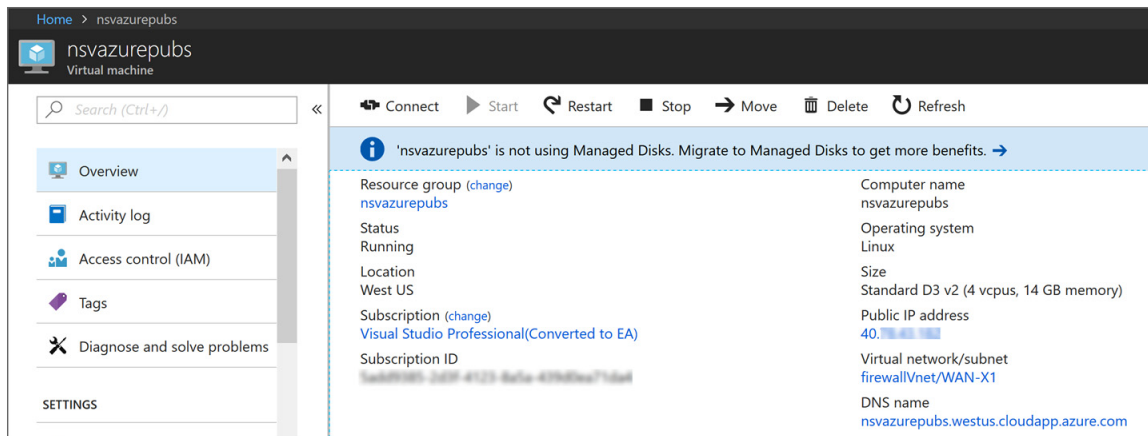
ⓘ **TIP:** Log into the NSv at the displayed public IP address for SonicOS/X management and to register the NSv on MySonicWall.

Logging into Your NSv for SonicOS/X Management

To log into your NSv for SonicOS/X management:

1. In the left navigation pane of Azure, click **Virtual Machines**.

2. Click the name of your NSv.

3. In the **Overview** screen, the IP address of the NSv is displayed under **Public IP address**.
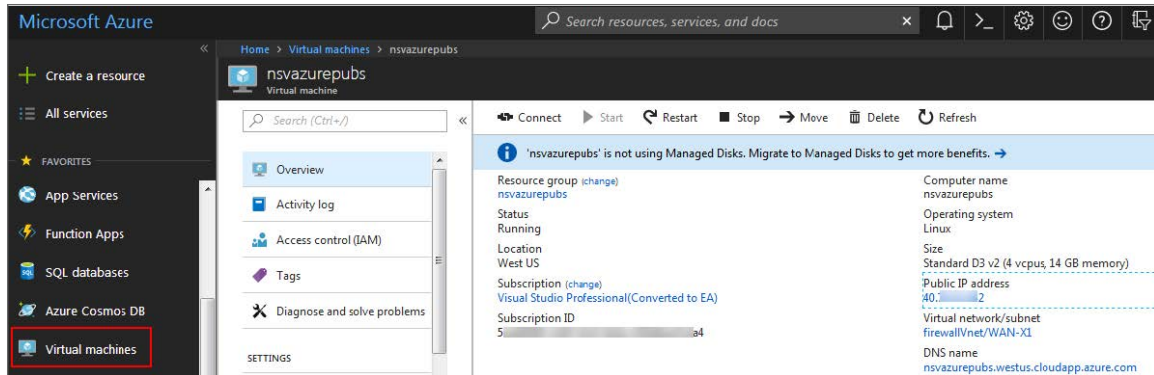
4. Point your browser to `https://<Public IP address>`, using the public IP address of your NSv.

5. Log into SonicOS/X (default credentials: ***admin/password***).

Viewing and Configuring Security Rules

On the **Dashboard** page or the **Resource group** page, click the **NSG** link to view the inbound and outbound security rules. The NSG link has a description or type of ***Network security group***.

The inbound rules control management access to the NSv. The Source for these rules is initially set to your public IP address, that you entered during the installation process for **Management Access IP Source**. To manage the NSv from another location, you need to add an inbound rule.

To add a new inbound rule for NSv HTTPS management access from another public IP address:

1. Click **Inbound security rules** in the left navigation pane of the Azure NSG page. The **Inbound security rules** page displays.
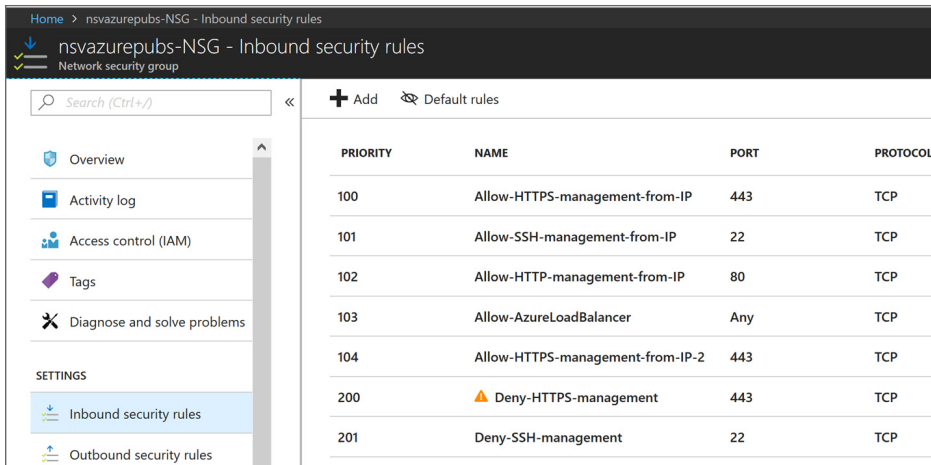
2. Click **Add**. The **Add inbound security rule** dialog appears.
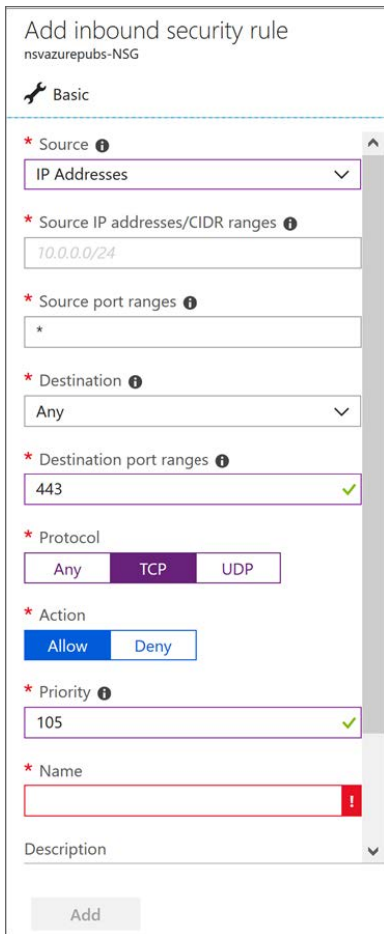
3. For **Source**, select **IP Addresses**.

4. For **Source IP addresses/CIDR ranges**, type in your new public IP address or an address range in CIDR format.

5. Optionally fill in **Source port ranges** if you want to specify the port(s).

6. For **Destination**, select **Any**.

7. For **Destination port ranges**, type in **443** for HTTPS access.

8. For **Protocol**, select **TCP**.

9. For **Action**, select **Allow**.

10. For **Priority**, type in an available number that is less than (higher priority than) the number for the first **Deny** rule.

11. For **Name**, type in a descriptive name for this rule.

12. Optionally fill in the **Description** field.

13. Click **Add**.

Forwarding Traffic to Your NSv

This section describes how to configure a route on your SonicWall NSv Series virtual machine so that you can pass traffic though the NSv.

If you have not yet registered your NSv on MySonicWall, do that now. See Registering the NSv Virtual Machine with SonicOS/X for more information. Your NSv must be registered to enable full functionality.

To configure a route on your NSv virtual machine:

1. If not already logged into the Azure portal, navigate to https://portal.azure.com/ and log into your Azure account.

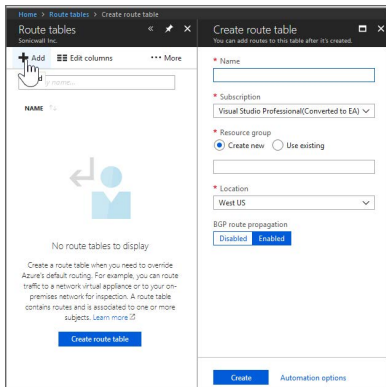2. In the Azure left navigation pane, click **All services**.
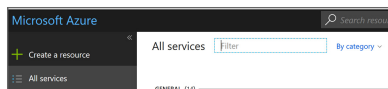
3. In the **All services Filter** field, type **Route**. The display changes to show only services with "Route" in their names.
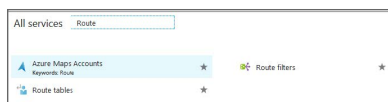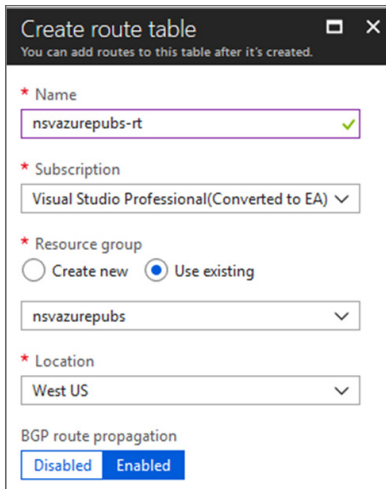

4. Click **Route tables**.

5. On the **Route tables** page, click **Add** to create a new route table.

The **Create route table** dialog displays.

6. In the **Name** field, type in a name for this route table.

7. For **Subscription**, select the subscription you are using in Azure.

8. For **Resource group**, select **Create new** if you are using the route table for other networks, or select **Use existing** if you are using the route table for this network only. If you select **Use existing**, you can use the drop-down menu to select the same resource group you are using for your NSv.

9. The **Location** field should already display the same location you selected for your NSv.

10. For **BGP route propagation**, accept the default of **Enabled**.


11. Click **Create** to create the route table. After a brief wait, **Notifications** displays *Deployment succeeded* and the new route table appears in the **Route tables** screen.
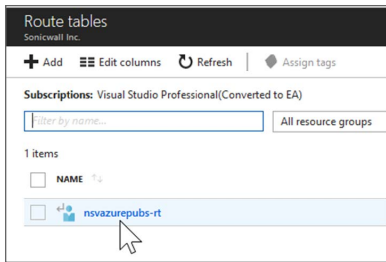
12. Click on the route table name.

13. In the route table screen, under **SETTINGS**, click **Routes**.
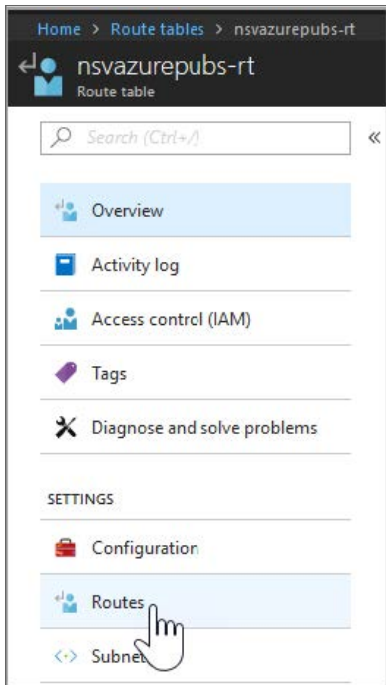
14. On the **Routes** screen, click **Add** to add a route to the route table.

15. In the **Add route** screen, for **Route name**, type in a descriptive name such as `default_route`.

16. For **Address prefix**, type in `0.0.0.0/0` to elect all traffic to be forwarded to the NSv.

17. For **Next hop type**, select **virtual machine** from the drop-down menu.

18. For **Next hop address**, type in the IP address of the NSv X0 interface.
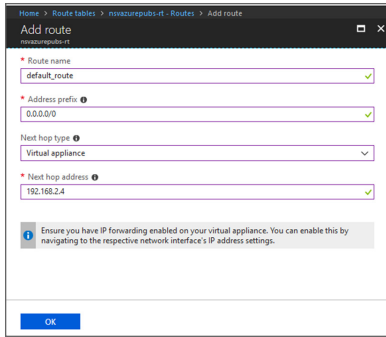
19. Click **OK**. This creates the route.

20. Next, you need to associate the route table. In the **Route table** options, click **Subnets**.
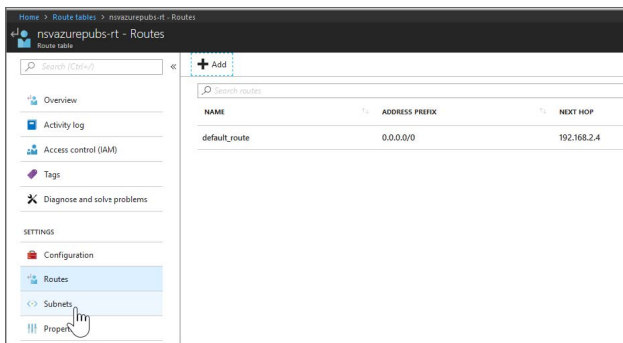
21. In the **Subnets** screen, click **Associate**.
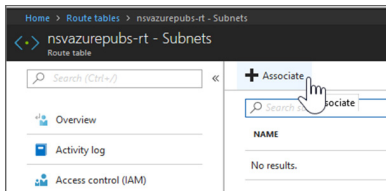
22. In the **Associate subnet** screen, click **Virtual network**. The resources with possible virtual networks are displayed to the right under **Resource**.
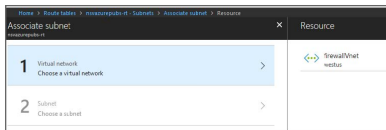
23. Click the desired resource. The display on the right changes to the **Choose subnet** screen and shows the possible subnets available for that resource.

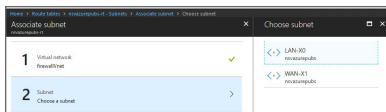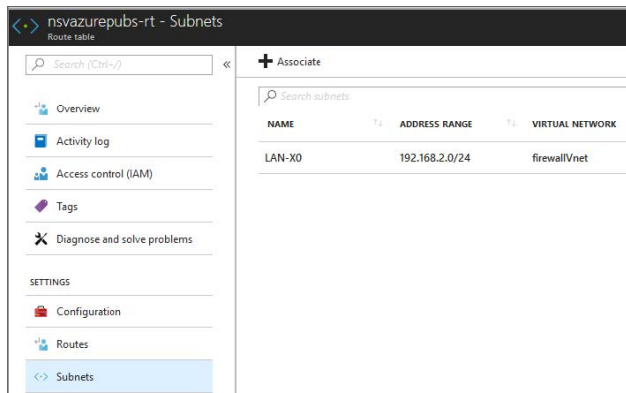24. Under **Choose subnet**, click **LAN-X0**. Because we entered the X0 IP address previously for **Next hop address**, the X0 subnet must be selected here.

25. Click **OK** at the bottom of the screen. Azure performs the association and the **LAN-X0** subnet appears on the screen.

This completes the configuration required for forwarding traffic through the NSv. Continue to Testing Traffic Through Your NSv.

Testing Traffic Through Your NSv

After configuring a route for forwarding traffic on your NSv, you can verify it with some test traffic. You can send traffic from any client machine or virtual machine on the same subnet as the route you configured. In our configuration, this is the LAN-X0 subnet, or `192.168.2.0/24`.

For example, you could create an Ubuntu virtual machine in Azure, using the same options as your NSv for the following settings:

- Subscription
- Resource group
- Location
- Virtual network
- Subnet (such as LAN-X0 or `192.168.2.0/24`)

To send traffic through your NSv:

1. On your client machine or virtual machine (Ubuntu, for example), open a console window. For an Ubuntu virtual machine on Azure, click **Serial Console** in the **Virtual machine** options.

2. Type `ping 192.168.2.4` on the command line.
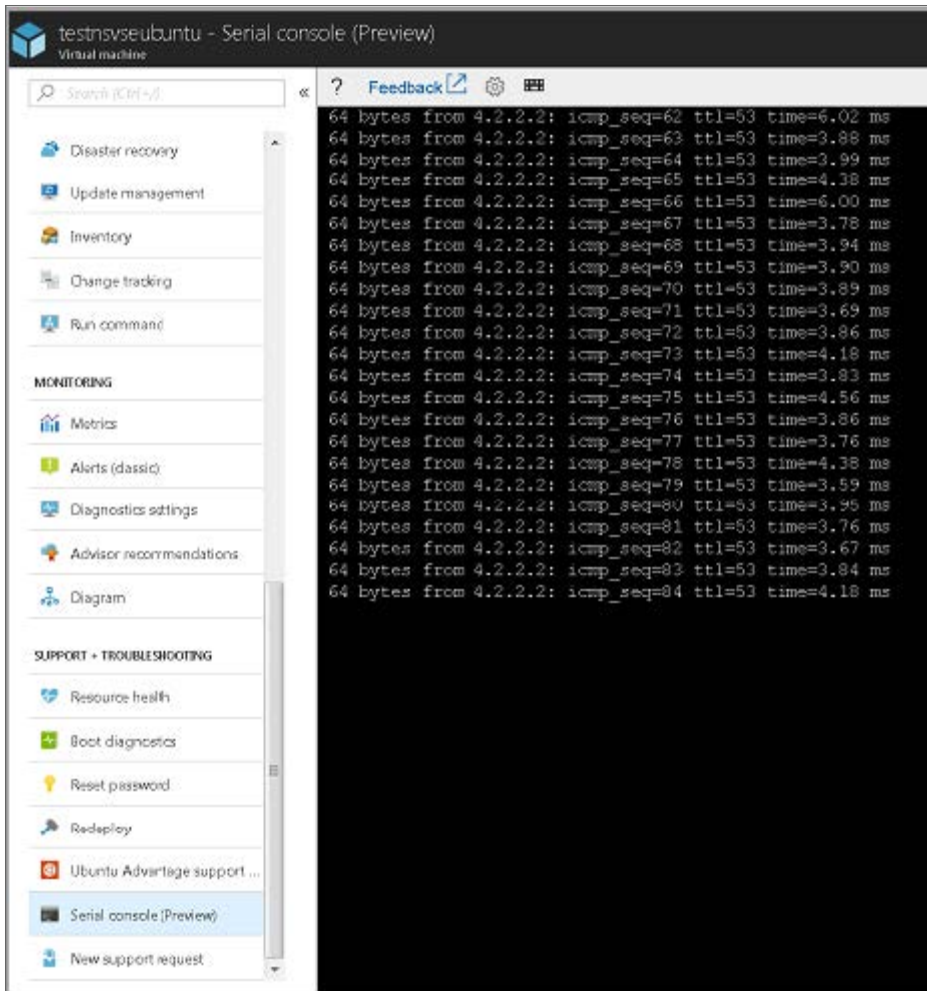
The pings should succeed.

3. Log into your NSv and navigate to the **MONITOR | Appliance Health | Live Monitor** page.

4. Scroll down to view the **Connection Count** chart. It should show a positive count, caused by the pings.
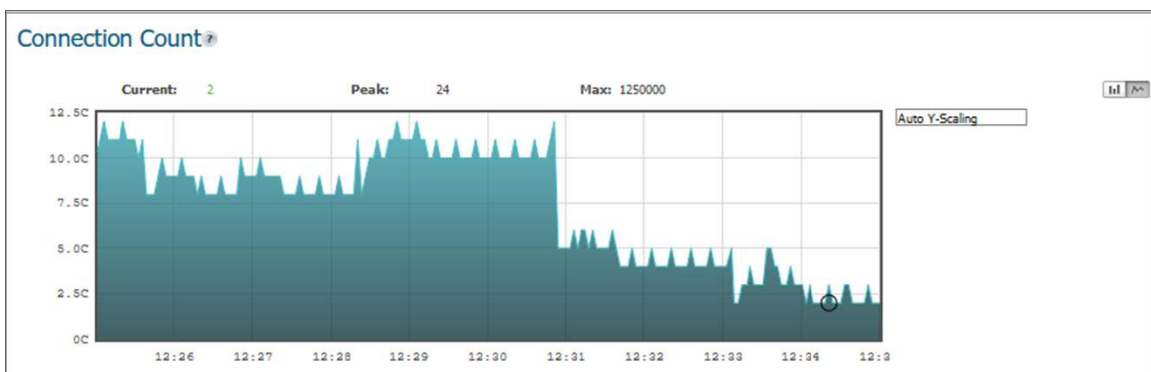
Other charts on the page also show activity. This verifies that traffic can be forwarded to the NSv.

Troubleshooting Installation Configuration

If the NSv fails to come up, follow the instruction in Using the Virtual Console and SafeMode to go to the NSv Management Console window or the SonicOS/X CLI window. Check the boot messages:

ⓘ | **NOTE:** The error messages that follow indicate that the virtual machine cannot boot.
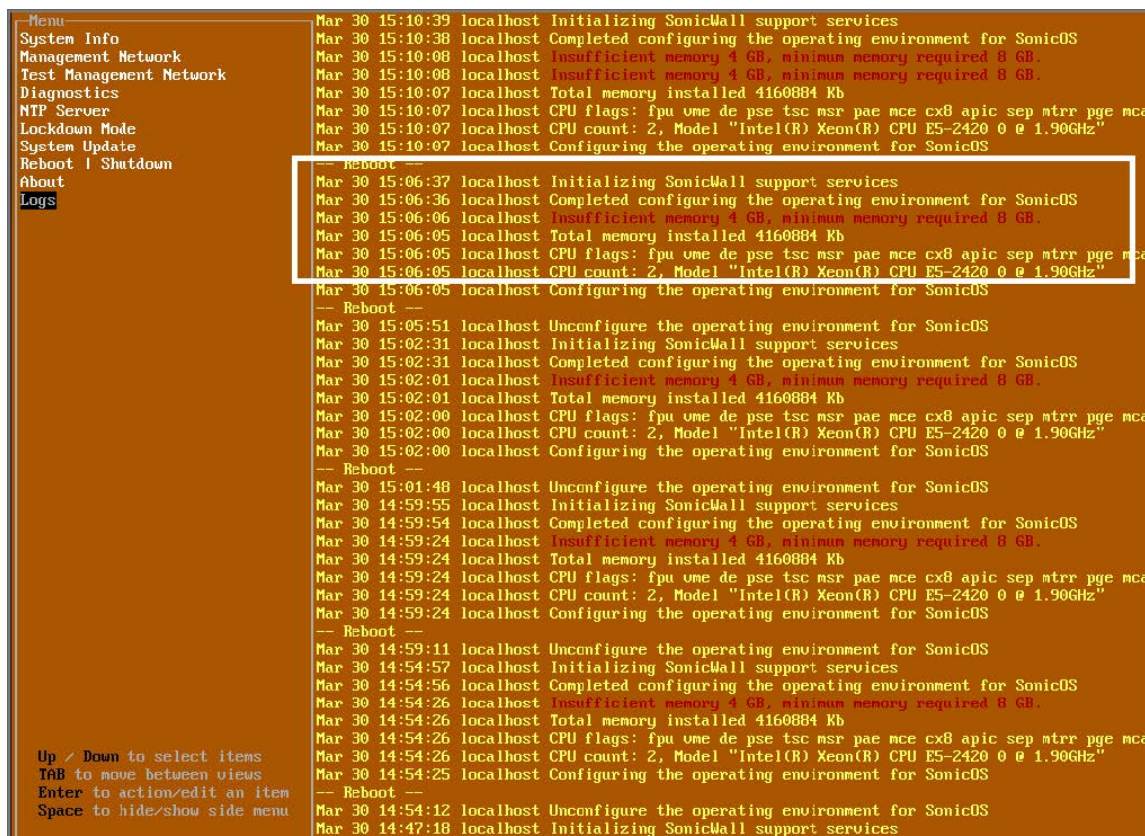
Insufficient Memory Assignment

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

SonicOS/X boot message:

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

This message can also appear in the Management Console logs as shown in the following images.

Memory might be insufficient without an insufficient memory log entry:

```
┌─Menu─────────────────────┐  Mar 30 14:44:14 localhost  Initializing SonicWall support services
│ System Info              │  Mar 30 14:44:12 localhost  Completed configuring the operating environment for SonicOS
│ Management Network       │  Mar 30 14:44:12 localhost  Completed configuring the operating environment for SonicOS
│ Test Management Network  │ ┌─────────────────────────────────────────────────────────────────────────────────┐
│ Diagnostics              │ │Mar 30 14:44:11 localhost  This NSv model supports 8 CPU, current CPU count is only 2, for impr│
│ NTP Server               │ └Mar 30 14:44:11 localhost  Total memory installed 8172912 Kb──────────────────────────┘
│ Lockdown Mode            │  Mar 30 14:44:11 localhost  CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
│ System Update            │  Mar 30 14:44:11 localhost  CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
│ Reboot | Shutdown        │  Mar 30 14:44:11 localhost  Configuring the operating environment for SonicOS
│ About                    │  ── Reboot ──
│ Logs                     │  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
│                          │
│                          │
│ 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: 18
```

Licensing and Registering Your NSv

Topics:

- Registering the NSv Appliance from SonicOS/X

Registering the NSv Virtual Machine with SonicOS/X

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

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

To register your NSv virtual machine:

1. Point your browser to your NSv Series WAN or LAN IP address and log in as the administrator (default admin / password).
2. Go to **Dashboard | System > Summary** and click **Register Device**.
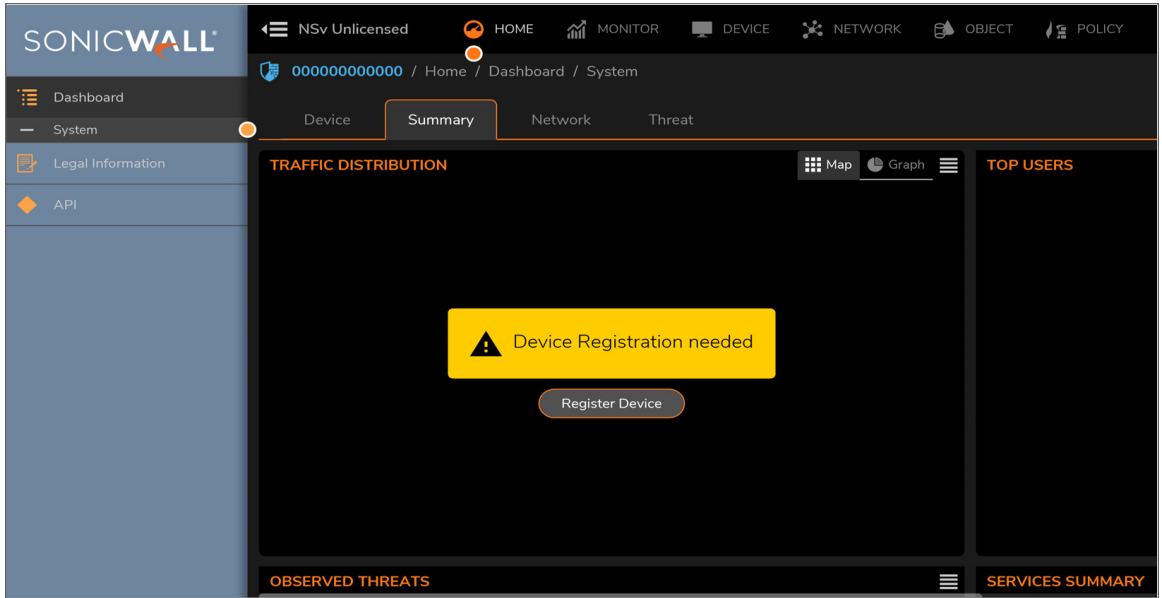
3. At this point you can log into MySonicWall and name the NSv installation while providing the **Firewall Serial Number** and authorization code (**Auth Code**), and select a **Policy Mode Switching** option (**Classic** or **Policy**). Click **Register** to complete the registration.

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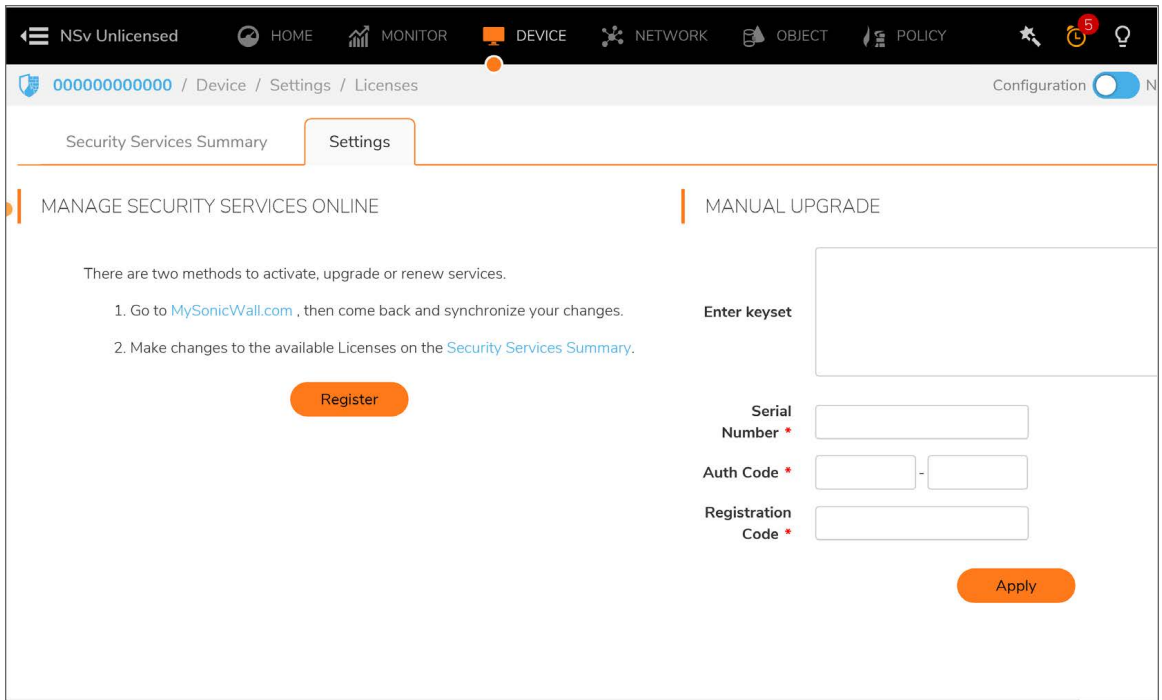
Click **Apply** to complete the registration.

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

SonicOS/X Management

Topics:

- Managing SonicOS/X on the NSv Series
- Using System Diagnostics

Managing SonicOS/X on the NSv Series

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

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

To log into SonicOS/X for management of the NSv:

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

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

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

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

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

Using System Diagnostics

Check Network Settings, at **DEVICE | Diagnostics > Check Network Settings**. is a diagnostic tool that automatically checks the network connectivity and service availability of several predefined functional areas of

the NSv Series, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.
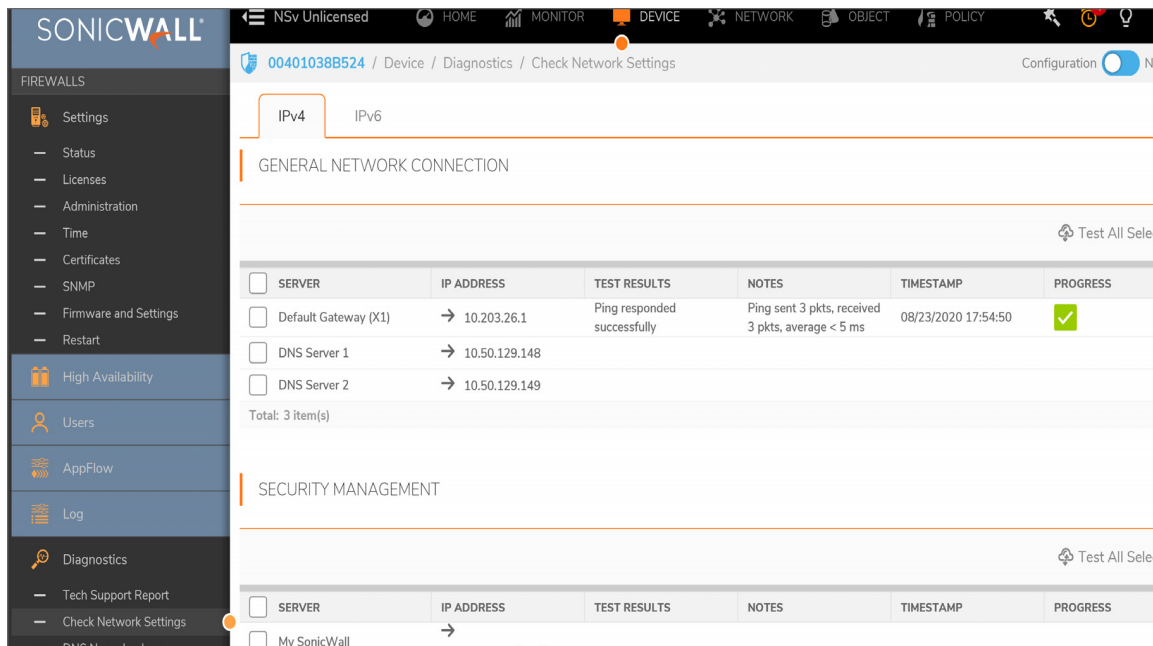
Specifically, Check Network Settings automatically tests the following functions:

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

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

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

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

Using the Virtual Console and SafeMode

Topics:

- Connecting to the Console with SSH
- Navigating the NSv Management Console
- Using SafeMode on the NSv

Connecting to the Console with SSH

SSH is used to connect to the virtual console of an NSv deployed on Azure.

To connect to the management console using SSH:

1. Launch PuTTY and type in the public IP address of the NSv on Azure.

   You can find the public IP by clicking **Virtual Machines** in the Azure portal, then clicking the name of your NSv and locating the public IP on the **Overview** screen.
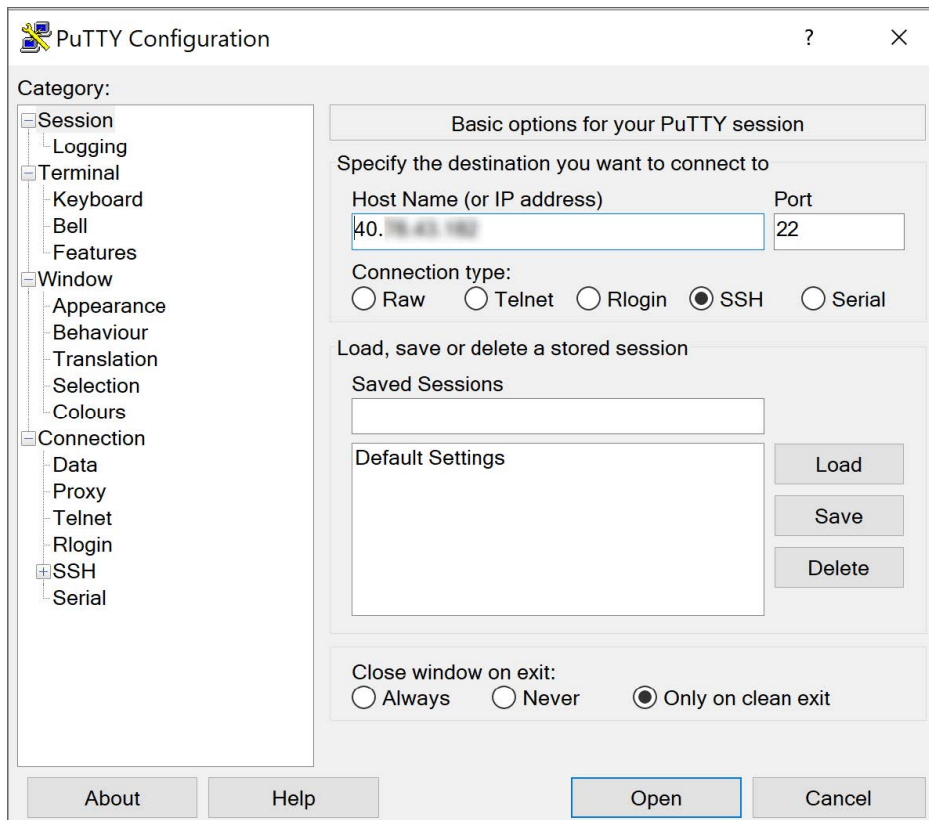
2. For **Port**, type in `22` if it is not already set.

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

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

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

5. In the console window at the **login as** prompt, type in `management`, which is the SSH management user name defined during the NSv deployment.
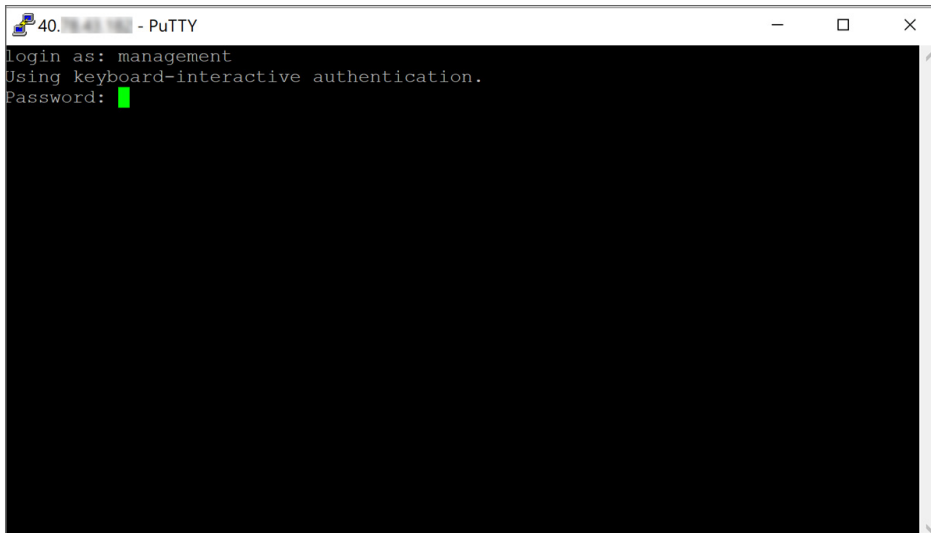
6. At the **Password** prompt, type in the SSH management password you defined during deployment.

    The orange NSv management console displays.
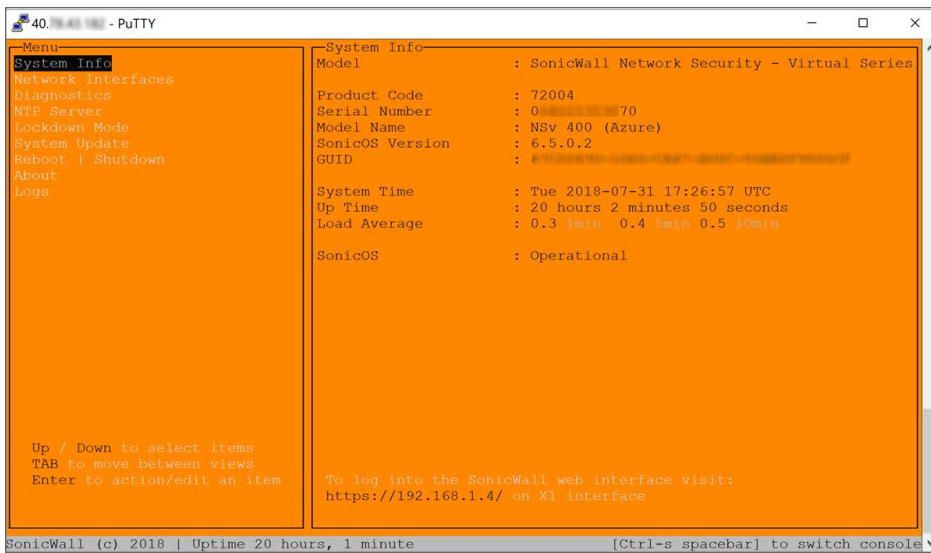
You can switch to the black SSH console window by pressing **Ctrl+s** and then the **space bar**. If you are prompted to log in at the **User** prompt, enter the SonicOS/X administrator credentials (default: *admin / password*).

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

Navigating the NSv Management Console

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

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

See Connecting to the Console with SSH.

To navigate and use the management console:

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

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

2. The main menu is displayed in the side menu (left pane). Use the up/down arrow keys to move the focus between menu items. As the focus shifts, the right pane displays the options and information for that menu item. The currently selected item is highlighted in black.

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

4. In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.

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

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

Some dialogs are for input:

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

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

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

System Info

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

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

Management Network or Network Interfaces

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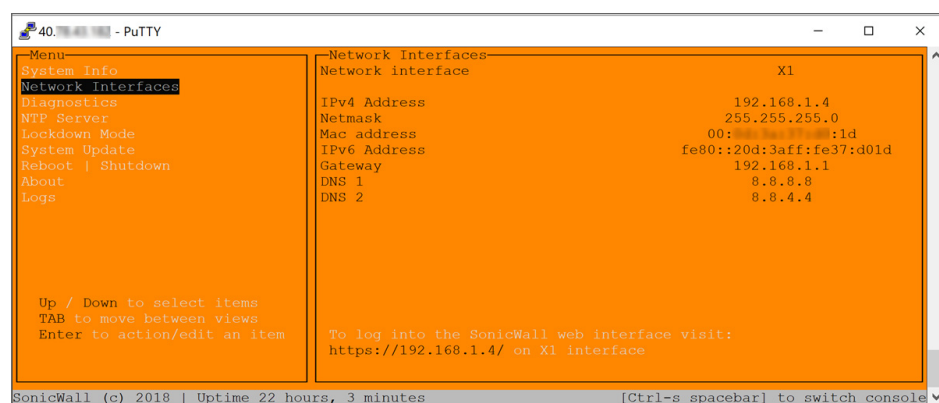
In this screen, the network settings are read-only except when the management console is in SafeMode. In SafeMode, you can configure these settings.

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

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

Test Management Network

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

```
┌Menu──────────────────┐  ┌Test Management Network──────────────────────────────┐
│ System Info           │  │ Ping                        [      Ping         ]   │
│ Management Network    │  │ Nslookup                    [      Nslookup      ]  │
│ Test Management Network│ │                                                     │
│ Diagnostics           │  │                                                     │
│ NTP Server            │  │                                                     │
│ Lockdown Mode         │  │                                                     │
│ System Update         │  │                                                     │
│ Reboot | Shutdown     │  │                                                     │
│ About                 │  │                                                     │
│ Logs                  │  │        ┌Enter IP address┐                           │
│                       │  │        │ 192.168.8.1_   │                           │
│                       │  │        │                │                           │
│                       │  │        │ Confirm <Enter>     Cancel <Esc>           │
│                       │  │        └────────────────┘                           │
│                       │  │                                                     │
│ Up / Down to select items                                                      │
│ TAB to move between views                                                      │
│ Enter to action/edit an item                                                   │
└───────────────────────┘  └─────────────────────────────────────────────────────┘
 SonicWall (c) 2018 | Uptime 3 minutes          [Ctrl-s spacebar] to switch console
```
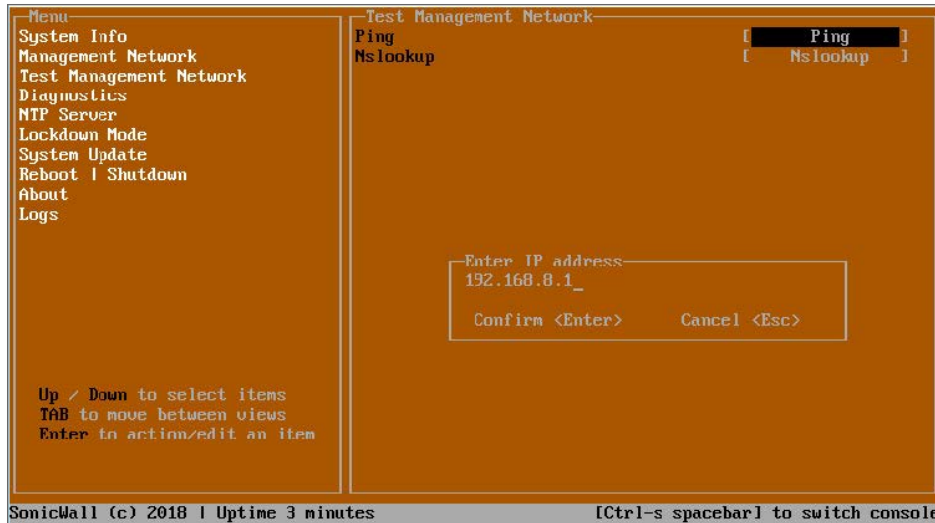
The **Test Management Network** screen provides the **Ping** and **Nslookup** tools to test connectivity between the management interface and the local network. **Ping** is used to test whether hosts in the network are reachable. **Nslookup** is available for sending DNS queries from the NSv virtual machine.

To use Ping:

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

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

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


              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.

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

                                        Confirm <Enter>     Cancel <Esc>




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

SonicWall (c) 2018 | Uptime 5 minutes              [Ctrl-s spacebar] to switch console
```

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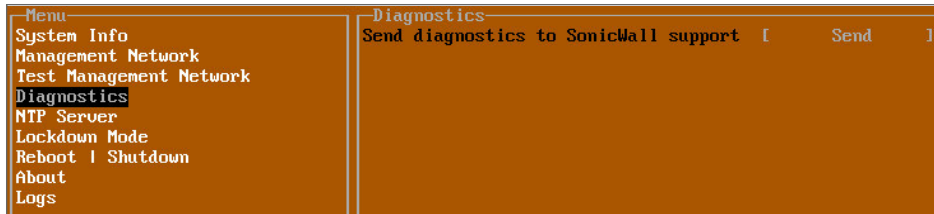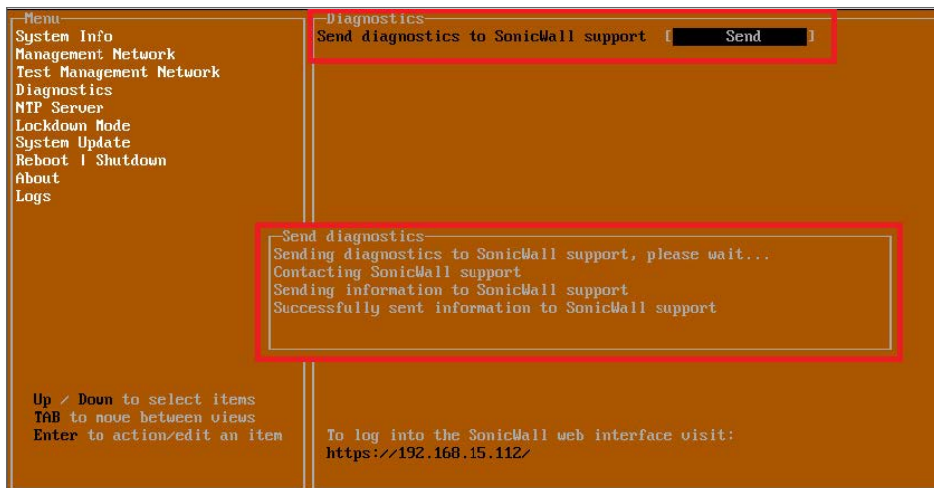
5. Press the **Esc** key to close the dialog.

Diagnostics

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

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

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

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

```
┌─Menu──────────────────────┐ ┌─Diagnostics─────────────────────────────────
│ System Info               │ │ Send diagnostics to SonicWall support  [     Send     ]
│ Management Network        │ │
│ Test Management Network   │ │
│ Diagnostics               │ │
│ NTP Server                │ │
│ Lockdown Mode             │ │
│ System Update             │ │
│ Reboot | Shutdown         │ │
│ About                     │ │
│ Logs                      │ │
│                           │ │ ┌─Send diagnostics──────────────────────────
│                           │ │ │ Sending diagnostics to SonicWall support, please wait...
│                           │ │ │ Contacting SonicWall support
│                           │ │ │ Sending information to SonicWall support
│                           │ │ │ Successfully sent information to SonicWall support
│                           │ │ │
│                           │ │ │
│ Up / Down to select items │ │
│ TAB to move between views │ │
│ Enter to action/edit an item │ To log into the SonicWall web interface visit:
│                           │ │ https://192.168.15.112/
```

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

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

Common reasons for the report failing to send include:

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

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

NTP Server

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

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

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

Lockdown Mode

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

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

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

Temporary Lockdown Mode

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

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

System Update

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

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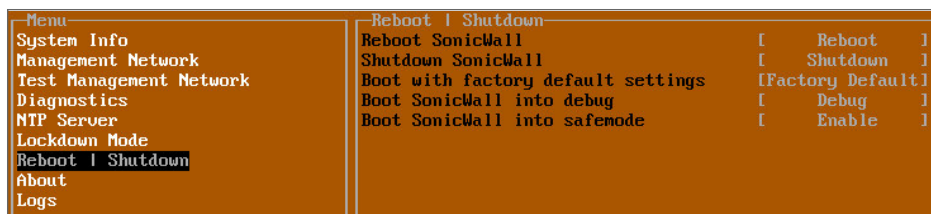
The **Reboot | Shutdown** screen provides functions for rebooting the NSv virtual machine, enabling debug mode, and enabling SafeMode. To perform an action, position the focus and then press **Enter** to select the desired action. Select **Yes** in the confirmation dialog, then press **Enter** again.

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

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

About

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

Logs

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

Using SafeMode on the NSv

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

Topics:

- How Management Console Differs in SafeMode
- Entering SafeMode

How Management Console Differs in SafeMode

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

- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers
  ⓘ | **NOTE:** Changes made to interfaces in SafeMode are *not* persistent between reboots.

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

Entering SafeMode

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

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

Topics:

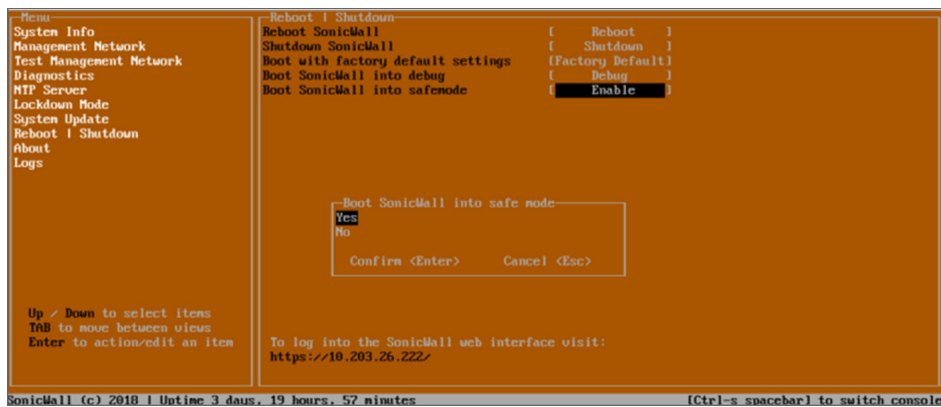- Enabling SafeMode
- Disabling SafeMode
- Configuring the Management Network in SafeMode
- Installing a New SonicOS/X Version in SafeMode
- Downloading Logs in SafeMode

Enabling SafeMode

SafeMode can be enabled from the management console.

To enable SafeMode:

1. Access the NSv management console as described in one of:

   - For NSv, see: Connecting to the Console with SSH

2. In the console, select the **Reboot | Shutdown** option and then press **Enter**.

3. Navigate down to the **Boot SonicWall into safemode** option to highlight **Enable**, and then press **Enter**.

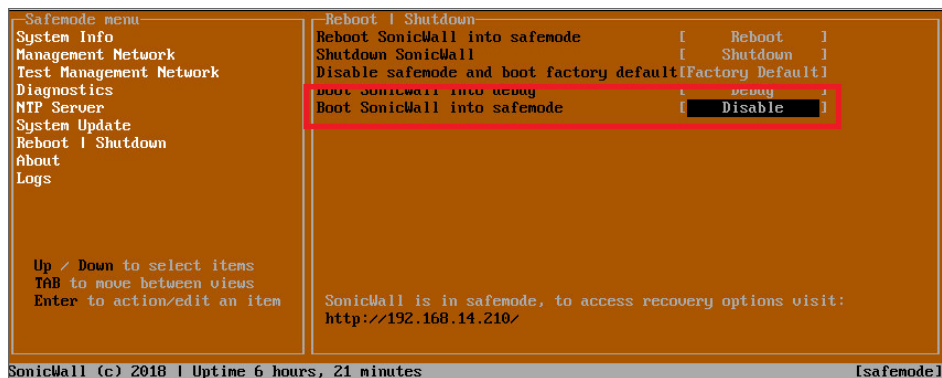4. Select **Yes** in the confirmation dialog.

5. Press **Enter**.

   The NSv immediately reboots and comes back up in SafeMode.

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

Disabling SafeMode

To disable SafeMode:

1. In the SafeMode menu in the NSv management console, select the **Reboot | Shutdown** option and press **Enter**.

2. In the **Reboot | Shutdown** screen, navigate down to the **Boot SonicWall into safemode** option to highlight **Disable**, and then press **Enter**.

```
┌─Safemode menu──────────┐┌─Reboot | Shutdown──────────────────────────────────────┐
│ System Info            ││ Reboot SonicWall into safemode        [     Reboot     ]│
│ Management Network     ││ Shutdown SonicWall                    [    Shutdown    ]│
│ Test Management Network││ Disable safemode and boot factory default[Factory Default]│
│ Diagnostics            ││ Boot SonicWall into debug             [     Debug      ]│
│ NTP Server             ││ Boot SonicWall into safemode          [    Disable    ]│
│ System Update          ││                                                         │
│ Reboot | Shutdown      ││                                                         │
│ About                  ││                                                         │
│ Logs                   ││                                                         │
│                        ││                                                         │
│                        ││                                                         │
│                        ││                                                         │
│   Up / Down to select items ││                                                    │
│   TAB to move between views ││                                                    │
│   Enter to action/edit an item ││ SonicWall is in safemode, to access recovery options visit:│
│                        ││ http://192.168.14.210/                                  │
│                        │└─────────────────────────────────────────────────────────┘
SonicWall (c) 2018 | Uptime 6 hours, 21 minutes                        [safemode]
```

3. Select **Yes** in the confirmation dialog.

4. Press **Enter**.

   The NSv immediately reboots and boots up in normal mode.

Configuring the Management Network in SafeMode

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

- **Management Interface** – This is the currently selected interface. This defaults to X1. Use this to select any of the NSv virtual machine interfaces.

- **IPv4 Address** – The current IPv4 address currently assigned to the Management Interface.

- **Netmask** – The current Netmask assigned to the Management Interface.

- **Mac Address** – The MAC address of the Management Interface.

- **IPv6 Address** – The currently assigned IPv6 address of the Management Interface.

- **Gateway** – The current Default Gateway currently in use by the NSv virtual machine.

- **DNS** – A list of the current DNS servers currently being used by the NSv virtual machine.

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

Topics:

- Configuring Interface Settings
- Disabling an Interface

Configuring Interface Settings

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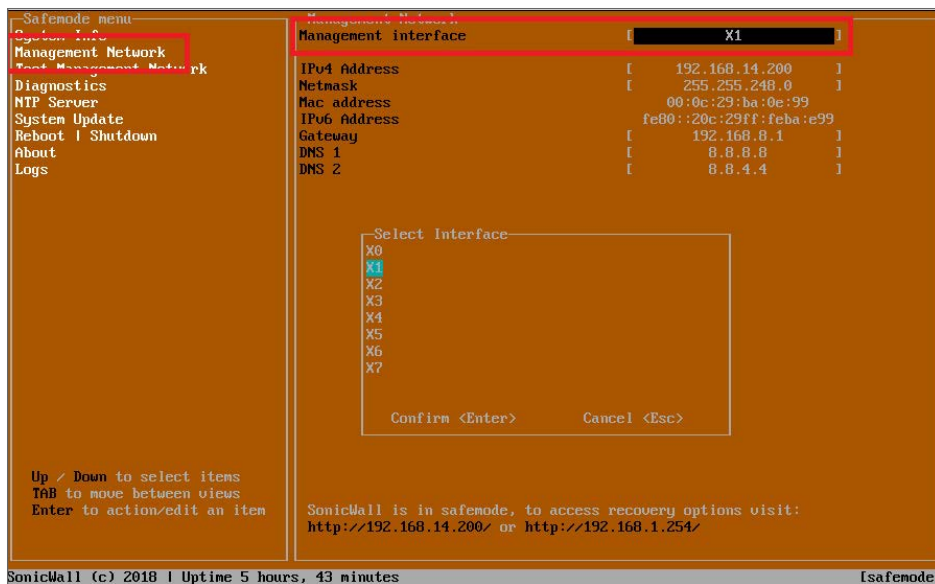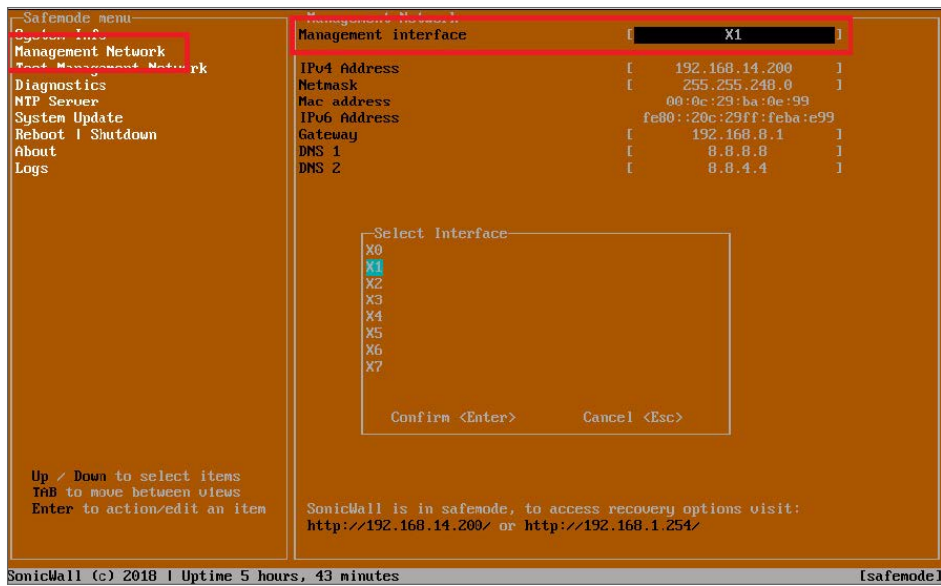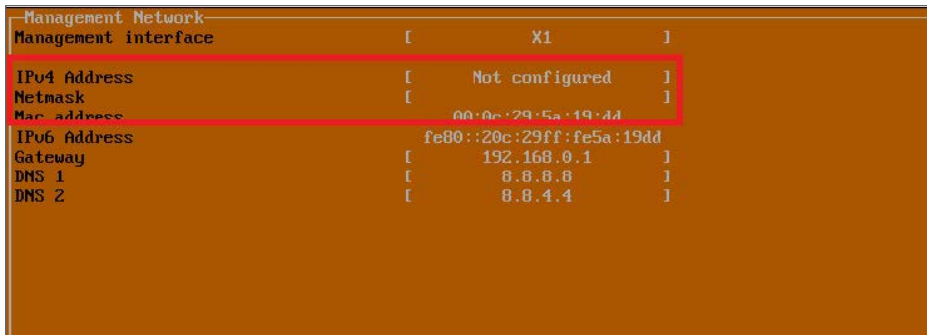

To edit an interface:

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

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

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

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

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

   The on-screen dialog displays the current IP address.

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

5. Two new buttons appear on the screen after you make changes to an interface setting: **Save changes** or **Cancel**. You can use the **Tab** key to navigate to these buttons.
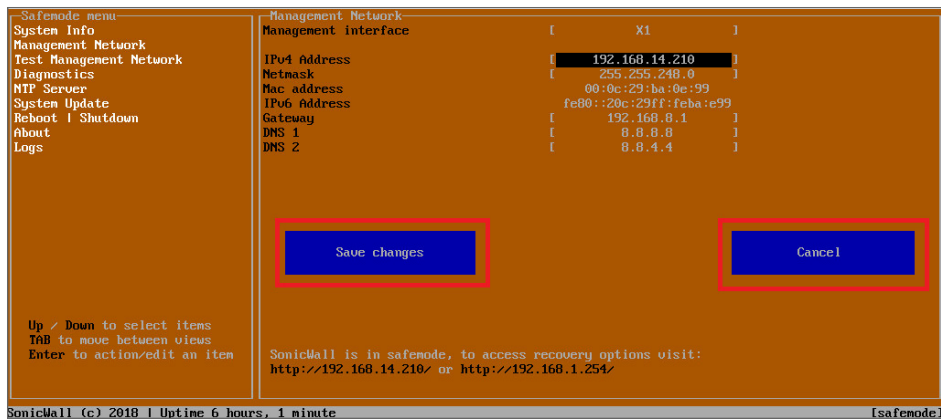
ⓘ | **NOTE:** You cannot navigate to the left navigation pane until you either save changes or cancel using these buttons.

Do one of the following:

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

- If finished making changes to the settings for this interface, press **Tab** to navigate to the **Save changes** button and then press **Enter** to save your changes.

- Press **Tab** to navigate to the **Cancel** button and then press **Enter** to cancel all changes to the settings for this interface.

Disabling an Interface

You can disable an interface while in SafeMode.

To disable an interface:

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

2. Press **Enter**.

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

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

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

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

   The onscreen dialog displays the current IP address.

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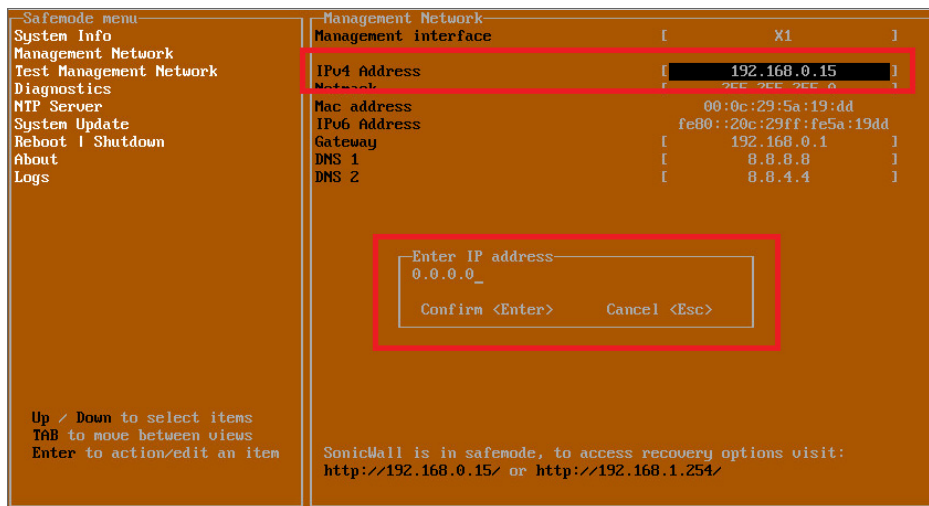
   Save changes displays.

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

The interface is disabled.

Installing a New SonicOS/X Version in SafeMode

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

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

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

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

To install a new SonicOS/X from SafeMode:

1. Depending on the type of NSv deployment, determine the IP address to use to access the SafeMode web management interface:

   - On an NSv deployed in Azure, you can access the Safemode web interface at the public IP address assigned to the NSv.

2. In a browser, navigate to `http://<IP address>`, using the applicable IP address. The SafeMode web management interface displays.
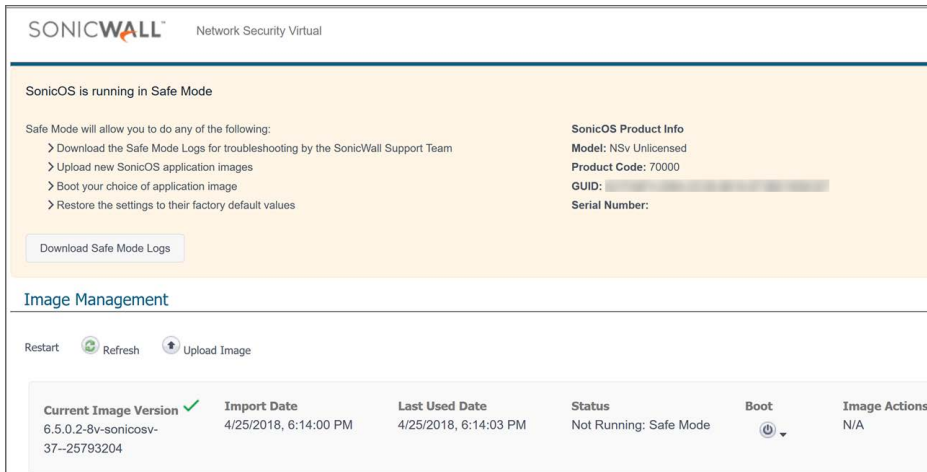
3. Click **Upload Image** to select an SWI file and then click **Upload** to upload the image to the virtual machine. A progress bar provides feedback on the file upload progress. After the upload completes, the image is available in the **Image Management** list in the SafeMode web interface.

4. In the row with the uploaded image file, click **Boot** and select one of the following:

    -   **Boot Uploaded Image with Current Configuration**
    -   **Boot Uploaded Image with Factory Default Configuration**
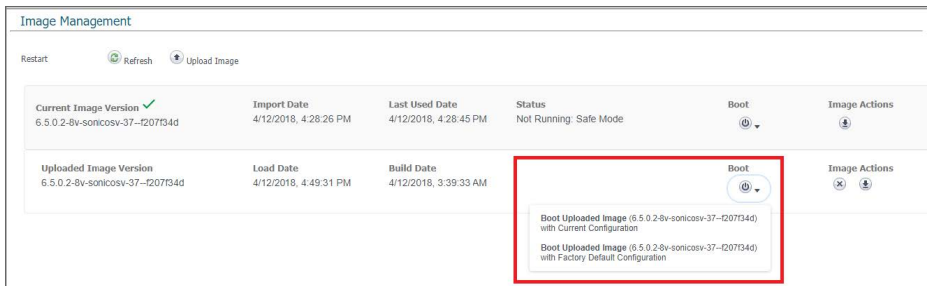
The NSv virtual machine reboots with the new image.

Downloading Logs in SafeMode

When the NSv virtual machine is in SafeMode, extra logging information is kept that can be downloaded. The logs are available from the SafeMode web management interface that can be accessed through the URL provided at the public IP address of an NSv.

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

To download logs from SafeMode:

1. In a browser, navigate to `http://<IP address>`, using the applicable IP address. 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

SonicOS Product Info
Model: NSv Unlicensed
Product Code: 7C000
GUID:
Serial Number:

Download Safe Mode Logs

Image Management

Restart   ⟳ Refresh   ⬆ Upload Image

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

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

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

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

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

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

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

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

End User Product Agreement

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

Open Source Code

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

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