# SonicWall® NS*v* Series on Microsoft Azure

Getting Started Guide

SONICWALL®

# Contents

1

# Introducing NS$_v$ Series

This *SonicWall® NSv Series on Azure Getting Started Guide* describes how to install SonicWall NSv on Microsoft Azure and provides basic configuration information.

To jump directly to the installation instructions, go to Installing NSv Series on Azure on page 10.

### SonicWall NSv on Azure Marketplace


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

**Topics:**

# Feature Support Information

The SonicWall NS*v* Series on Azure has nearly all the features and functionality of a SonicWall NS*a* hardware appliance running SonicOS 6.5.4 firmware.

SonicWall GMS 8.4 and higher versions are supported for management of SonicWall NS*v* Series virtual appliances. The *SonicOS 6.5 NSv Series About SonicOS* book contains the list of features not supported on NSv.

The Feature Support List table lists key SonicOS features and whether or not they are supported in deployments of the NS*v* Series

**Feature Support List**

| Component | Feature | Status |
|---|---|---|
| Network Interfaces | Override MAC Address | Not supported |
| Network Interfaces | DHCPv6 Prefix Delegation (PD) | Not supported |
| Network Interfaces | IPv6 Management | ***Supported*** |
| Network Interfaces | 6rd | Not supported |
| Network Interfaces | Portshield Groups | Not supported |
| Network Interfaces | L2 Bridge Mode | Not supported |
| Network Interfaces | Native Bridge | Not supported |
| Network Interfaces | Wire Mode v4 | Not supported |
| Network Interfaces | Wire Mode v6 | Not supported |
| Network Interfaces | PPPoE | Not supported |
| Network Interfaces | PPTP | Not supported |
| Network Interfaces | L2TP | Not supported |
| Network Interfaces | Tap Mode | Not supported |
| Network Interfaces | Link Aggregation | Not supported |
| Network Interfaces | Port Redundancy | Not supported |
| Network Interfaces | IP Unnumbered | Not supported |
| Network Interfaces | VLAN Translation | Not supported |
| Network Interfaces | Users IPv6 | ***Supported*** |
| Network Interfaces | DHCP Server | Not supported |
| Network Interfaces | VLAN Interfaces | Not supported |
| Network Interfaces | Jumbo Frames | Not supported |
| Firewall Settings | Global BWM | Not supported |
| Firewall Settings | QoS Mapping | Not supported |
| Firewall Settings | Multicast | Not supported |
| Switching | | Not supported |
| Anti spam | | Not supported |
| 3G/4G Modem | | Not supported |
| Wireless | | Not supported |
| SonicPoints | | Not supported |
| VirtualAssist | | Not supported |
| High Availability | Active/Passive | **Supported** |
| High Availability | Stateful Sync | Not supported |

### Feature Support List

| Component | Feature | Status |
|---|---|---|
| High Availability | Firmware Sync | Not supported |
| High Availability | Active-Active DPI | Not supported |
| WAN Acceleration | | Not supported |
| SSL VPN | SSL VPN for IPv6 | ***Supported*** |
| VoIP | H.323 | ***Supported*** |
| VoIP | SIP | ***Supported*** |
| Diag Page | Unsupported Options | Partially supported |
| External Storage Support | | Not supported |

**NOTE:** Per Microsoft, "Azure does not support any Layer-2 semantics." Therefore, SonicOS Layer 2 functionality is disabled in NS*v* deployments in Azure. Consequently, NS*v* appliances operating in Azure 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 information about supported features, refer to the *SonicOS 6.5.4 NSv Series* administration documentation. This and other documents for the SonicWall NS*v* Series are available by selecting **NSv** Series as the **Product** at: https://www.sonicwall.com/support/technical-documentation.

# Node Counts per NS$_v$ Platform

The node count is the maximum number of nodes/users that can connect to the NS*v* at any one time, and is displayed on the **System Status** page in the **MONITOR** view.

### Maximum Node Counts Per Platform

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

For reference, node counts are calculated by SonicOS as follows:

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

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

# Product Matrix and Requirements

The following table shows the hardware resource requirements for the SonicWall NS*v* Series virtual appliances.

| Product Models | NS*v* 10 | NS*v* 25 | NS*v* 50 | NS*v* 100 | NS*v* 200 | NS*v* 400 | NS*v* 800 | NS*v* 1600 |
|---|---|---|---|---|---|---|---|---|
| Maximum Cores[1] | 2 | 2 | 2 | 2 | 2 | 4 | 8 | 16 |
| Minimum Total Cores | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 |
| Management Cores | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Maximum Data Plane Cores | 1 | 1 | 1 | 1 | 1 | 3 | 7 | 15 |
| Minimum Data Plane Cores | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| Network Interfaces | 2 | 2 | 2 | 2 | 2 | 4 | 8 | 8 |
| Supported IP/Nodes | 10 | 25 | 50 | 100 | No limit | No limit | No limit | No limit |
| Minimum Memory Required | 4G | 4G | 4G | 4G | 6G | 8G | 10G | 12G |
| Minimum Hard Disk/Storage | 35G | 35G | 35G | 35G | 35G | 35G | 35G | 35G |

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

# Github Repository

SonicWall NS*v* Azure templates are available in the github repository:

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

# Backup and Recovery Information

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

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Please contact SonicWall Technical Support for assistance.
- If the disk is not recoverable, then the NS*v* appliance needs to be deregistered with MySonicWall. See Deregistering Your NSv on page 46 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 65.
- If SonicOS fails three times during the boot process, it will boot into SafeMode. Verify that the minimum required memory is available and allocated based on the NS*v* model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall Technical Support for assistance.

# Exporting and Importing NS$_v$ Configurations

Moving configuration settings from SonicWall physical appliances to the NSv Series is not supported. However, configuration settings may be moved from one NSv to another. See the *SonicOS 6.5 NSv Series Updates* administration book and the *SonicOS 6.5.4 NSv Series Upgrade Guide* on 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 to a Higher Capacity NS$_v$ Model

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

For details on the number of processors and memory to allocate to the VM to upgrade, refer to Product Matrix and Requirements on page 7.

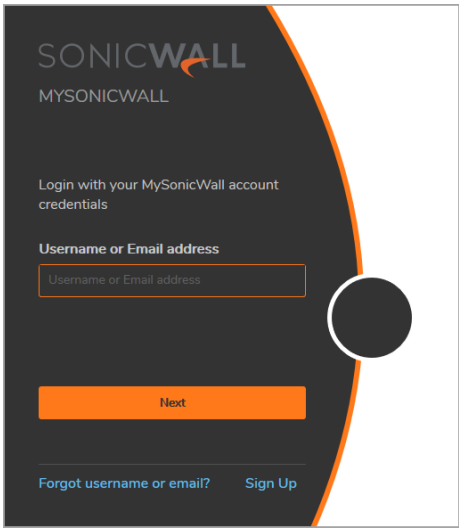
# Creating a MySonicWall Account

A MySonicWall account is required to obtain the image 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.

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

4 Enable two-factor authentication if desired.

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

- **Email (one-time passcode)** where an email with a one-time passcode is sent each time you log into your MySonicWall account.
- **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code. Once the code is scanned, you need only click on 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 new products.

10 Click **CONTINUE** to go to the **Extras** page.

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

12 If you opted for additional contacts, input the information and click **ADD CONTACT**.

13 Click **DONE**.

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

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

## Next Steps

- Installing NSv Series on Azure on page 10
- Licensing and Registering Your NSv on page 41

2

# Installing NS$_v$ Series on Azure

**Topics:**



# Supported NS$_v$ Series Models on Azure

**NSv Models (VM Sizes) on Azure**

| SonicWall NSv Model | Azure | Interface Count[1] | Core Count |
|---|---|---|---|
| NSv 10 | Standard D2 v2 | 2 | 2 |
| NSv 25 | Standard D2 v2 | 2 | 2 |
| NSv 50 | Standard D2 v2 | 2 | 2 |
| NSv 100 | Standard D2 v2 | 2 | 2 |
| NSv 200 | Standard D2 v2 | 2 | 2 |
| NSv 400 | Standard D3 v2 | 4 | 4 |
| NSv 800 | Standard D4 v2 | 8 | 8 |
| NSv 1600 | Standard D5 v2 | 8 | 16 |

1. The maximum number of interfaces supported on an NSv instance is defined by the type of Azure VM. For example, if more than 2 interfaces are required for an NSv 200, use the NSv200 with an Azure VM supporting a higher number of interfaces.

**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 maybe constrained by the Azure VM.

For Azure 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

# Task List for NS$_v$ Azure VM Setup

The process for setting up an NS*v* Azure virtual firewall is summarized in three main tasks:

1 Install the NS*v* Azure virtual firewall

- Installing NSv on Azure on page 11

2 Register the NS*v* on MySonicWall

- Registering the NSv Appliance from SonicOS on page 41

3 Configure traffic forwarding to the NS*v*

- Forwarding Traffic to Your NSv in Azure on page 32
- Testing Traffic Through Your NSv in Azure on page 36

# Installing NS$_v$ on Azure

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

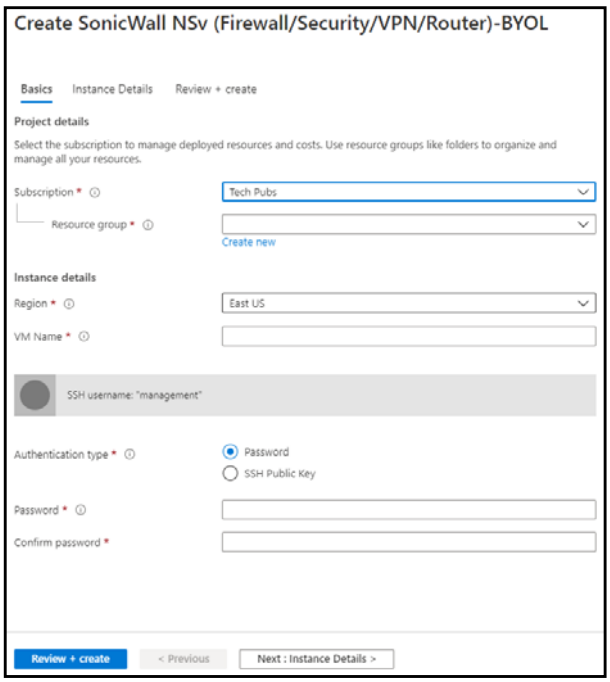
***To install from Azure Marketplace:***

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

2 Navigate to SonicWall NS*v* 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**.

The **Basics** screen of the NS*v* configuration window is displayed.




4 On the **Basics** screen, configure the following options:

- **Subscription** – Select the Azure subscription on which to deploy the resources for this NS*v* 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.
  - If you select **Use existing**, select the resource group to use from the associated drop-down list.
- **Region** – Select the Azure location where the resources will be deployed.
- **VM Name** – Type in a descriptive name for this NS*v* 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.

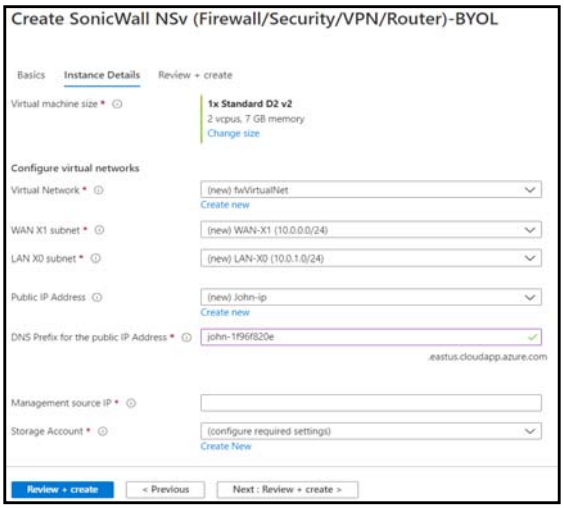
  ```
  The value for 'DNS Prefix for the public IP Address' must match the regular expression '^$|^[a-z][a-z0-9-]{1,61}[a-z0-9]$'
  ```

  **NOTE:** The **SSH username** is set to ***management*** by default. This is the user name for accessing the NS*v* console using SSH. This is not the NS*v* administrator user name, but is a user name created as part of an NS*v* Azure deployment.
- **Authentication type** – Select either ***SSH public key*** or ***Password*** as the authentication method for the above 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, e.g. !@#$%^&*()_+}{"|:>?<)
- 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.

5 Click **Next** to continue.

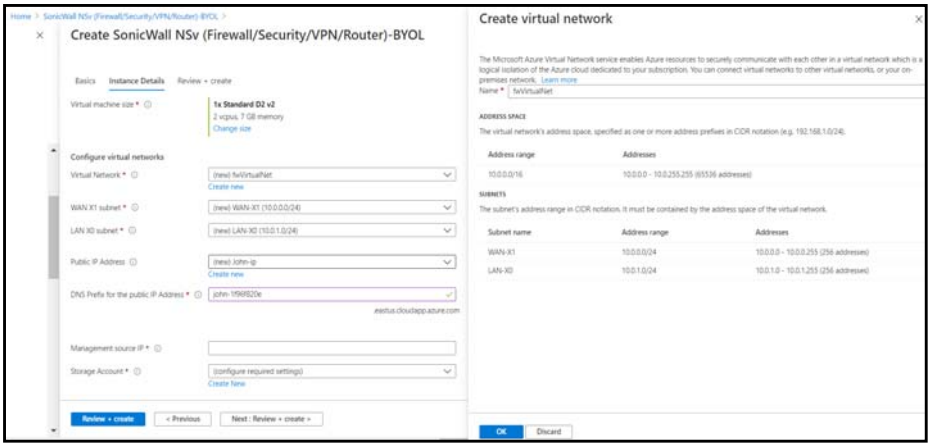
The **Instance Details** screen is displayed.




6 Select **Virtual machine size**, then select the row with the Azure equivalent for the NS*v* model you want to deploy in the **Choose a size** screen. Click **Select**.

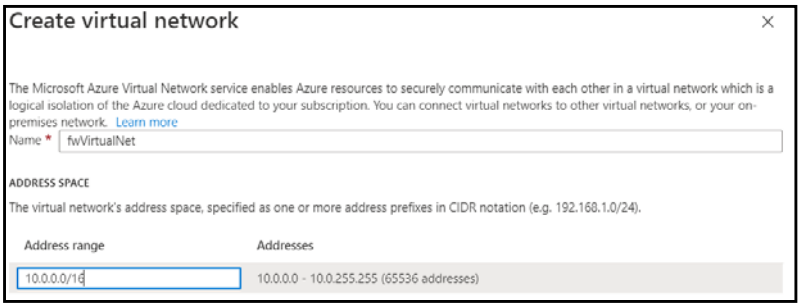
| VM Size in Azure | NS*v* Model |
|---|---|
| Standard_D2_v2 | NS*v* 10 |
| Standard_D2_v2 | NS*v* 25 |
| Standard_D2_v2 | NS*v* 50 |
| Standard_D2_v2 | NS*v* 100 |
| Standard_D2_v2 | NS*v* 200 |
| Standard_D3_v2 | NS*v* 400 |
| Standard_D4_v2 | NS*v* 800 |
| Standard_D5_v2 | NS*v* 1600 |

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 as displayed.




Under **Create virtual network**:

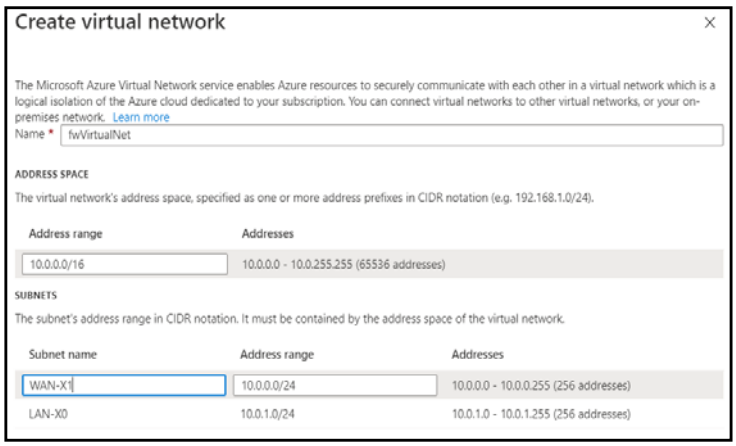
- **Name** – This is the name of virtual network the NS*v* will be deployed on. Leave the default, ***VNET***.
- **Address Space** – The template default is ***10.1.0.0/16***. This is a network address in CIDR format representing the virtual network address space. Accept the default or optionally configure a different address space, using the same format.




8 Click **OK**.

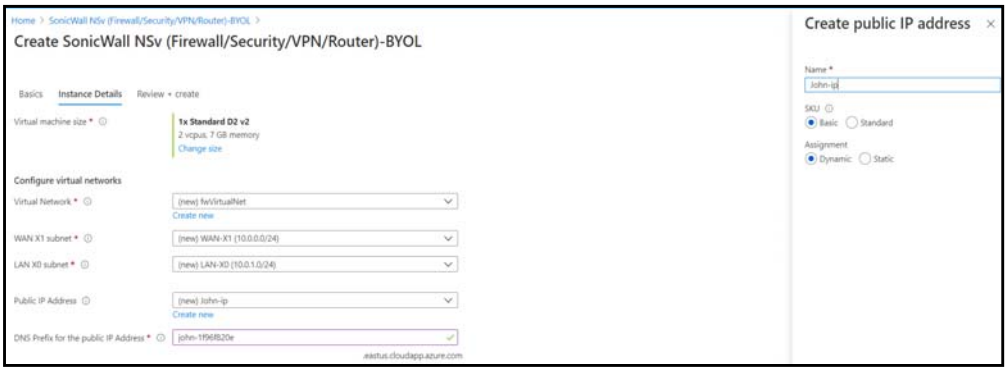
9 Select **Subnets** to configure the subnets for the WAN and LAN zones.

- **WAN subnet name** – The name of the WAN subnet. The default is ***WAN-X1***. If you have an existing network on Azure you may wish to change the value.
- **WAN-X1 Address range**– A sub-network of the **Address space** configured in Step 7, defined for WAN traffic. e.g. ***10.1.0.0/24***.
- **LAN subnet name** – The name of the LAN subnet. The default is ***LAN-X0***. If you have an existing network on Azure you may wish to change the value.
- **LAN- X0 Address range** – A sub-network of the **Address space** configured in Step 7, defined for LAN traffic. e.g. ***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 pre-populated 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**.

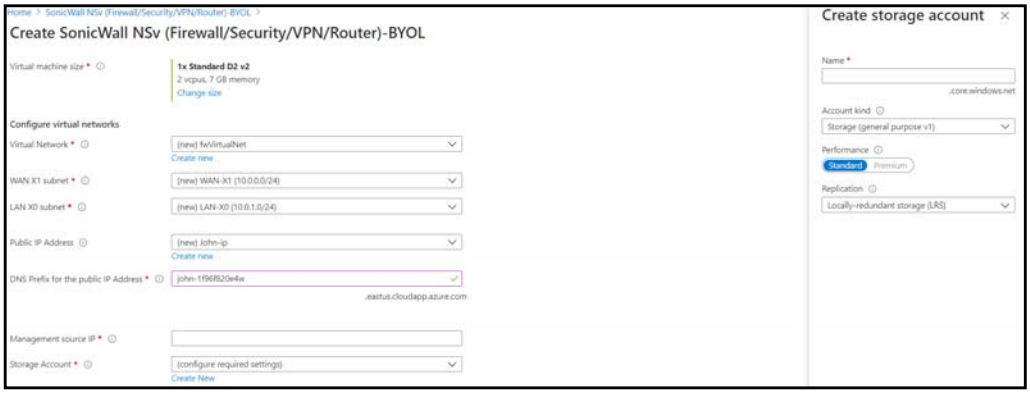
12 Click **OK**.

13 In the **DNS Prefix for the public IP Address** field, configure the DNS name for the NS*v*. This must be a unique DNS name for accessing the management interface of the NS*v* virtual firewall. When the NS*v* VM is created, the WAN will have a public IP and will be assigned the DNS name defined here.

14 In the **Management source IP** field, type in the public IP address that is allowed to access this NS*v* virtual firewall 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 **Review + create** at the bottom of the **Instance Details** screen.

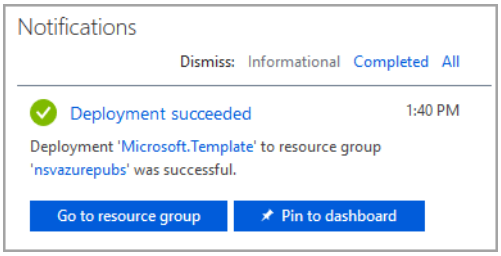
The Summary is displayed.

17 Confirm the settings and then click **Create.**

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** message.




See Accessing Your NSv in the Azure Portal on page 27 for 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 firewall on MySonicWall. See Registering the NSv Appliance from SonicOS on page 41 for information about registering your NSv.

Once you have registered the NSv, see Forwarding Traffic to Your NSv in Azure on page 32 and Testing Traffic Through Your NSv in Azure on page 36 for information about forwarding traffic to it.

# Configuring HA in Azure

This section provides a step-by-step introduction on deploying NSv with High Availability (HA) on Azure. Currently NSv is only available as BYOL (Bring your own License) version. This means you must already have a license available where an user purchases a license outside of Azure, as is done with hardware appliances.

There are two different ways to implement HA on Azure, either Active/Passive, or Active/Active. Active/Passive closely resembles Active/Passive of a SonicWall appliance with the exception that the new primary has to signal to Azure that it is the primary to move the VIP (Virtual IP Addresses) – there are no MAC addresses in Azure.

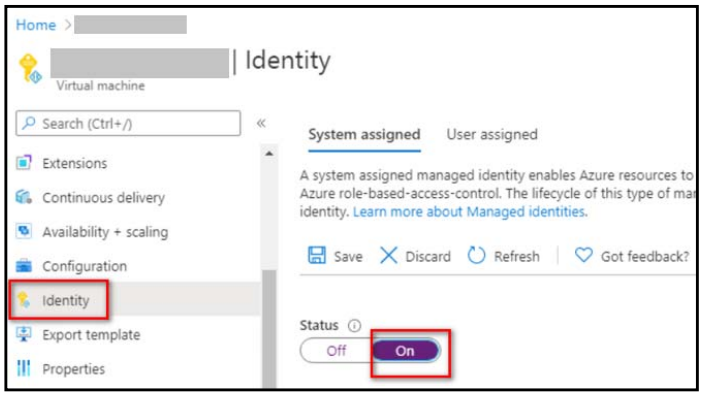
Likewise, the HA link needs to be terminated on L3 interfaces because of the lack of multicast support in Azure. Active/Passive HA supports both SPI state synchronization and config sync. As with other virtual firewall implementations of stateful high availability, failover may take several minutes.

The solution to slow failover is to deploy the NSv instance in Active/Active. Likewise in the non-virtual world, Active/Active does not support Stateful Packet Inspection (SPI) state sync, although this may not be as important anymore in a world of Deep Packet Inspection (DPI). But unlike Active/Active on a SonicWall hardware appliance, config sync is also not supported. HA Active/Active is more an architecture than a feature, and has some similarities to the Firewall Sandwich (FSW). An outside load balancer, preferably the Microsoft Azure Load Balancer, is used to direct traffic on the WAN side to one or multiple Active/Active high availability pairs. On egress, the NSv marks flows by swapping the src-ip with dynamic NAT. Config sync can be achieved via inheritance on Global Management Server (GMS) or Capture Security Center (CSC).

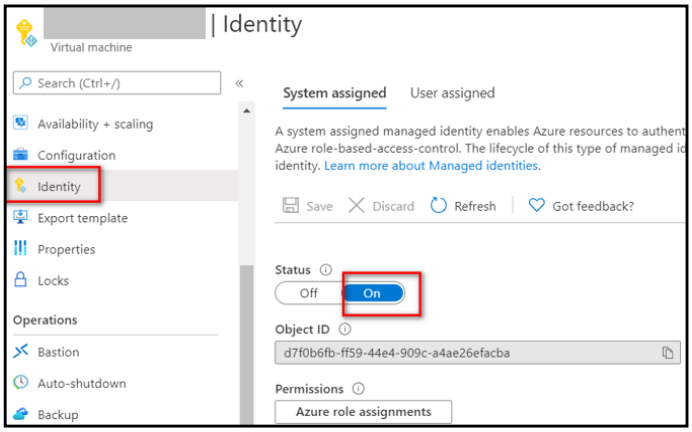
### *To Deploy an Active/Passive HA Pair:*

1 Ensure you have successfully deployed NSv on Azure. For information on how to deploy NSv on Azure, refer above section.

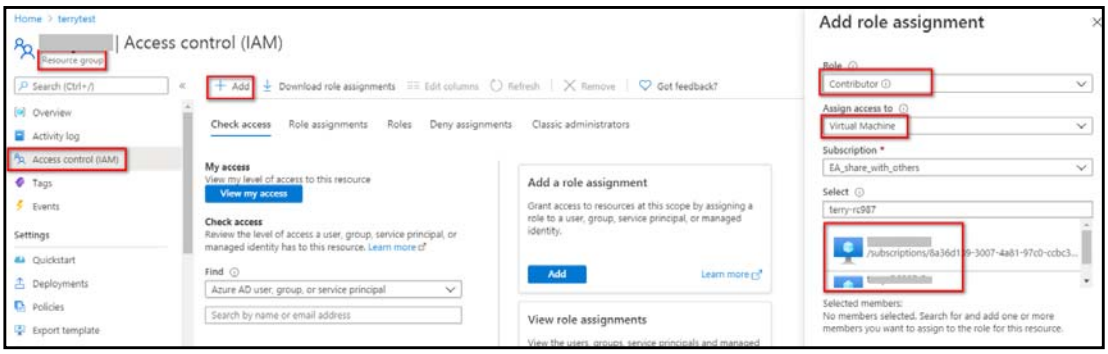
2 Enable Identity of Primary Virtual Machine. To enable, navigate to **Home > Virtual Machines** page, search for the primary virtual machine that you have created during deployment and on the left panel, select **Identity** and change the status to **On**.



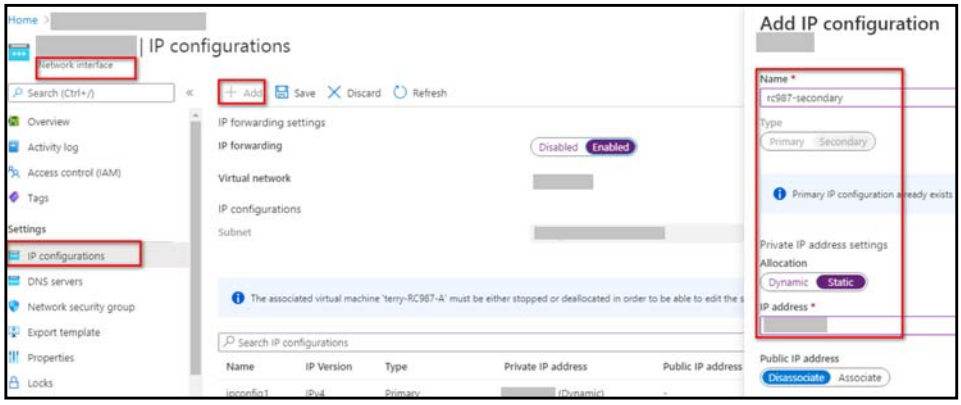

3 Enable Identity of Secondary Virtual Machine. To enable, navigate to **Home > Virtual Machines** page, search for the secondary virtual machine that you have created during deployment and on the left panel, select **Identity** and change the status to **On**.



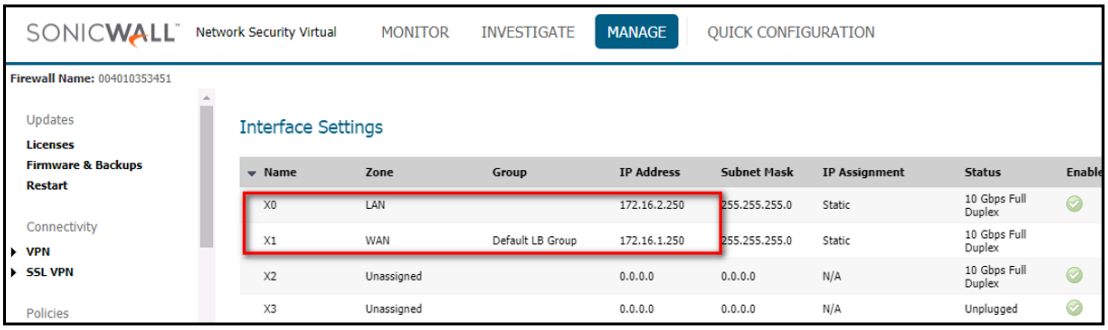
4 Add permissions to the Resource Group. To add contributor roles and permissions, navigate to **Home** page and search for the resource group that you have created during deployment and on the left panel, select **Access Control (IAM)** and click **Add** to provide permissions of virtual machines.



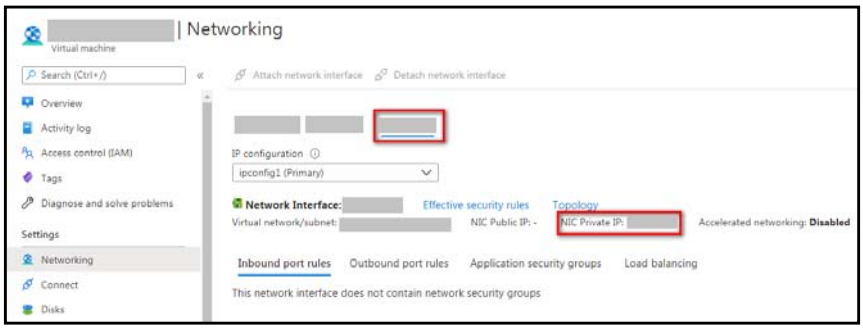

5 Add secondary IP address for the primary virtual machine. Navigate to **Home > Virtual Machines** page and select the primary virtual machine that you have created during deployment. On the left panel, select **Settings > IP Configurations > Add** to configure the IP address. By default, this address is set as 172.16.2.250 and allocated as Static.



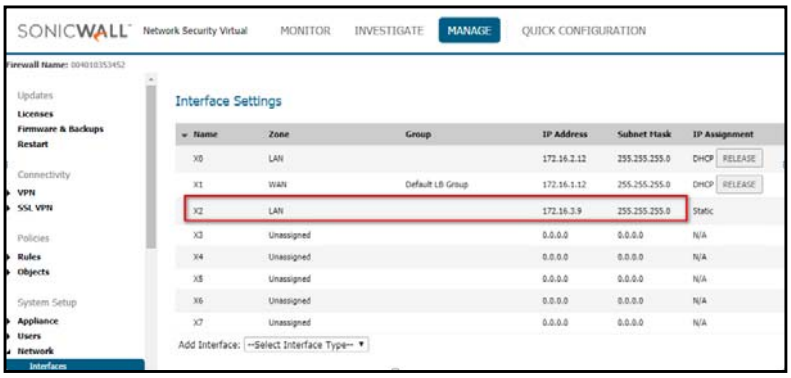

6 Log in to NSv firewall. On the **Manage > Interface Settings** page, change X0 first, and then X1 as shown below. You will lose access after you change X1.




7 Add secondary firewall HA interface. Navigate to **Home > Virtual Machines** page and select the secondary virtual machine that you have created during deployment. On the left panel, select **Settings > Networking,** configure **NIC Private IP** of **X2** as shown below.

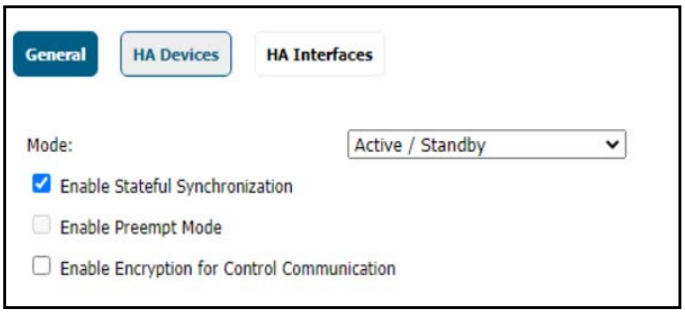



8 Log in to NSv firewall. Navigate to **Manage > Interface Settings** page, configure secondary firewall (X2) as shown below.



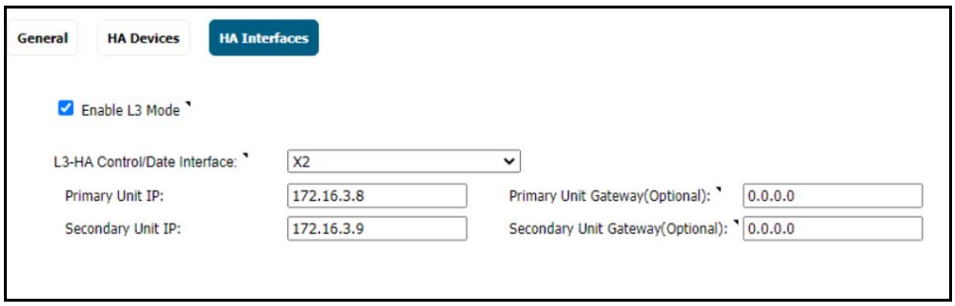

9 Navigate to **Manage > HA Interfaces** page, select **Enable L3 Mode** option on secondary firewall.

10 On the primary, configure HA to Active/Passive with L3 HA link. To configure, browse to **Manage > High Availability**, select **Enable Stateful Synchronization** option.

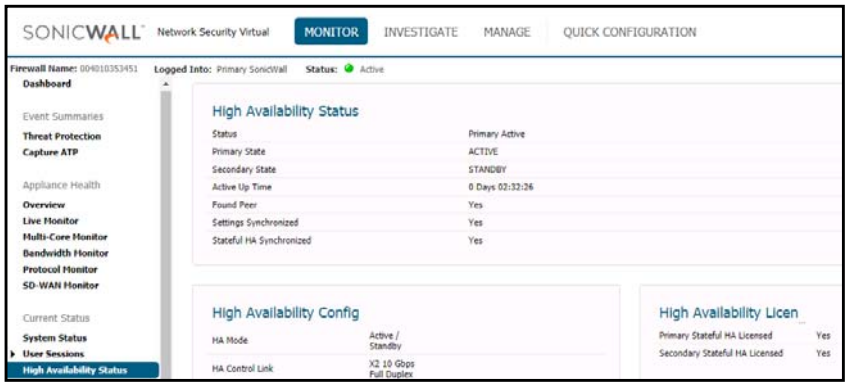



11 Click **HA Devices** tab and enter the serial number from the secondary. You can find the serial number in the **Monitor > System Status** page.


12 Click **HA interfaces** tab and switch the HA Control link to L3 mode. There is no need for gateway address, if two HA Interfaces are in the same subnet. If two HA interfaces are in different subnet, there is a need for proper gateway address and default is X.X.X.1 on Azure.




13 Navigate to **Monitor > High Availability Status** page to check whether the cluster is coming together. The secondary will reboot, and it may take a while to see the cluster up.




# Deploying an Active/Active HA Pair

Templates are a means to deploy VMs in Azure while also creating/modifying existing resources. There are a few different types of templates: Quick, Solution and Simple.

The below is an example of a Simple template which creates the following resources and defines their interconnections.

- Virtual Machine
- Storage Group
- Public IP
- 2 x Network Interfaces
- Virtual Network
- Network Security Policy

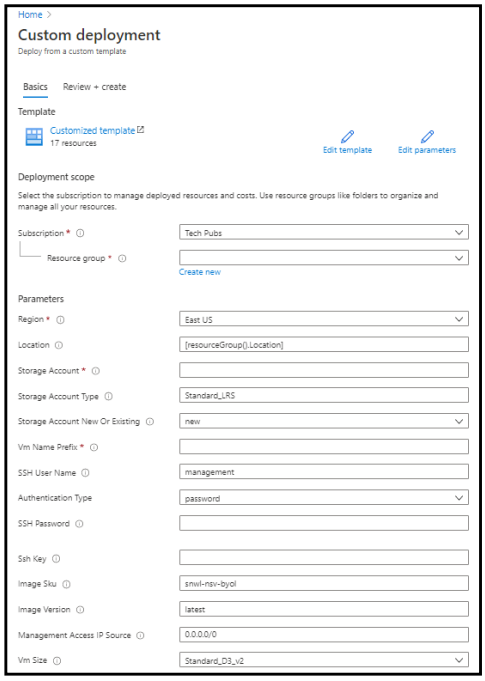
***To deploy an Active/Active HA Pair:***

1 Log into Azure.

2 Click to load the web page: https://github.com/sonicwall-nsv/azure-template/tree/feature/HA

3 Click the **Deploy to Azure Button**: 


4 The **Custom Deployment** page should come up:




Enter information to define the custom deployment:

- **Subscription**: Select the Azure subscription on which to deploy the resources for this NS*v* 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.
  - If you select **Use existing**, select the resource group to use from the associated drop-down list.
- **Region:** Select the Azure location where the resources will be deployed.
- **Location:** The geo location where you wish to deploy.
- **Storage Account:** A new or existing storage account (we recommend you create a new storage account). Type a name for the 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 storage account**.**
- **Vm Name Prefix:** Type in a descriptive name for this NS*v* instance.
- **SSH User Name:** 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 Azure deployment.
- **Authentication Type:** Select either ***SSH public key*** or ***Password*** as the authentication method for the above management **SSH username**. The default for the template is ***Password***.

- If you selected ***Password*** for **Authentication Type**, type the desired password into the **SSH Password** field. 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, e.g. !@#$%^&*()_+}{"|:>?<)
- If you selected ***SSH public key*** for **Authentication Type**, type the SSH RSA public key file name as a string into the **Ssh Key** field.

- **Image Sku:** The name of the Azure product SKU to load. It is not recommended to modify the default image Sku.
- **Image Version:** The version of the loaded NSv image. The default is set as **latest**. Replace **latest** with **987**.
- **Management Access IP Source:** Public IP address to allowed access to SonicWall NSv HTTPS & SSH management.
- **VM Size:** Select the VM you wish to deploy:

| SonicWall NS*v* Model | Azure |
|---|---|
| NS*v* 10 | Standard D2 v2 |
| NS*v* 25 | Standard D2 v2 |
| NS*v* 50 | Standard D2 v2 |
| NS*v* 100 | Standard D2 v2 |
| NS*v* 200 | Standard D2 v2 |
| NS*v* 400 | Standard D3 v2 |
| NS*v* 800 | Standard D4 v2 |
| NS*v* 1600 | Standard D5 v2[1] |

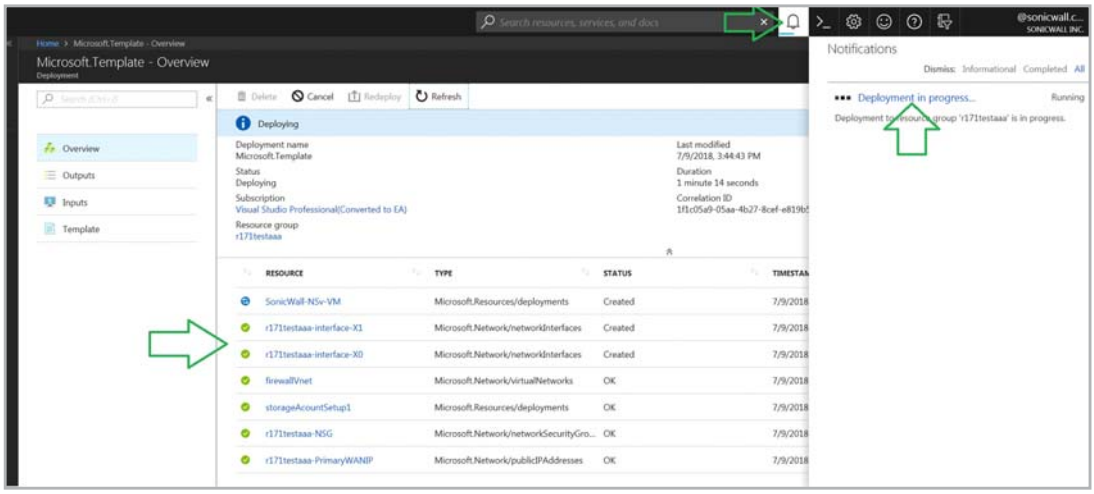
1. Supported only in the "U.S. East Location."

- **Virtual Network New Or Existing:** A new or existing virtual network account (we recommend you create a new virtual network account). Select **new**.
- **Virtual Network Name:** The name of the virtual network the NSv will be deployed on. It is not recommended to modify the default name. Template creates a new VNet whenever it is run.
- **Virtual Network Address Prefix:** The virtual network "Address space**"**. If you have an existing network on Azure, and wish to install the NSv on this network then this field should be populated with the network name. e.g. 192.168.0.0/16
- **Virtual Network Resource Group Name:** Name of the resource group for the existing virtual network.
- **Subnet WAN name:** Unique Name for Subnet.
- **Subnet LAN name:** Unique Name for Subnet.
- **Subnet HA name:** Unique Name for HA link network.
- **Subnet WAN prefix:** Must fit into Virtual Network Address Prefix defined in the above step.
- **Subnet LAN prefix:** Must fit into Virtual Network Address Prefix defined in the above step.
- **Subnet HA prefix:** Must fit into Virtual Network Address Prefix defined in the above step.

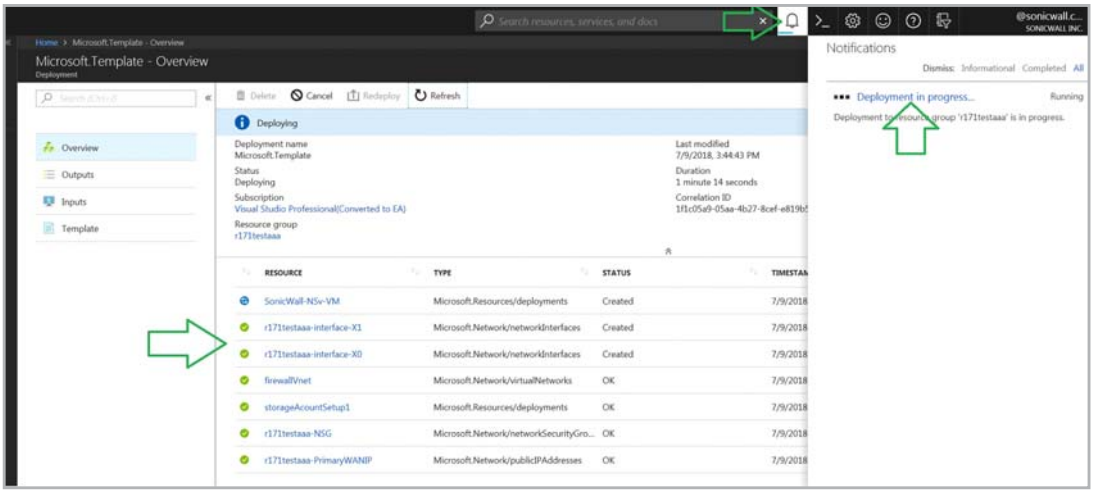
- **HA1Public Ip New or Existing:** A new or existing public IP. The default is set as **new**.
- **HA1Public Ip name:** Name of public WAN IP of primary.
- **HA1Public Ip Dns:** Host name that is entered into Azure DNS for public WAN IP of primary.
- **HA1Public Ip Resource Group Name:** Name of the resource group for the public IP address.
- **HA1Public IP Allocation Method:** Allocation method for the public IP address. The default is **Dynamic**. Choose static in production, and dynamic for lab.
- **HA1Public Ip Sku:** Name of the resource group for the public ip address. The default is **Basic**.
- **HA2Public Ip New or Existing:** A new or existing public IP of secondary. The default is set as **new**.
- **HA2Public Ip name:** Name of public WAN IP of secondary.
- **HA2Public Ip Dns:** Host name that is entered into Azure DNS for public WAN IP of secondary.
- **HA2Public Ip Resource Group Name:** Name of the resource group for the public IP address.
- **HA2Public IP Allocation Method:** Choose static in production, and dynamic for lab.
- **HA2Public Ip Sku:** Name of the resource group for the public ip address.
- **HA Float Public Ip New or Existing:** Public WAN IP of VIP. The default is set as **new**.
- **HA Float Public Ip name:** Name of public WAN IP of VIP**.**
- **HA Float Public Ip Dns:** Host name that is entered into Azure DNS for public WAN IP of VIP.
- **HA Float Public Ip Resource group name:** Name of the resource group for public WAN IP of VIP.
- **HA Float Public Ip Allocation Method:** Choose static in production, and dynamic for lab.
- **HA Float Public Ip Sku:** Name of the resource group for public WAN IP of VIP.

5 After filling in all the values you will need to click "I agree to the terms and conditions stated above" then click the "Purchase" button in order to deploy the template and create the SonicWall NS*v* instance.

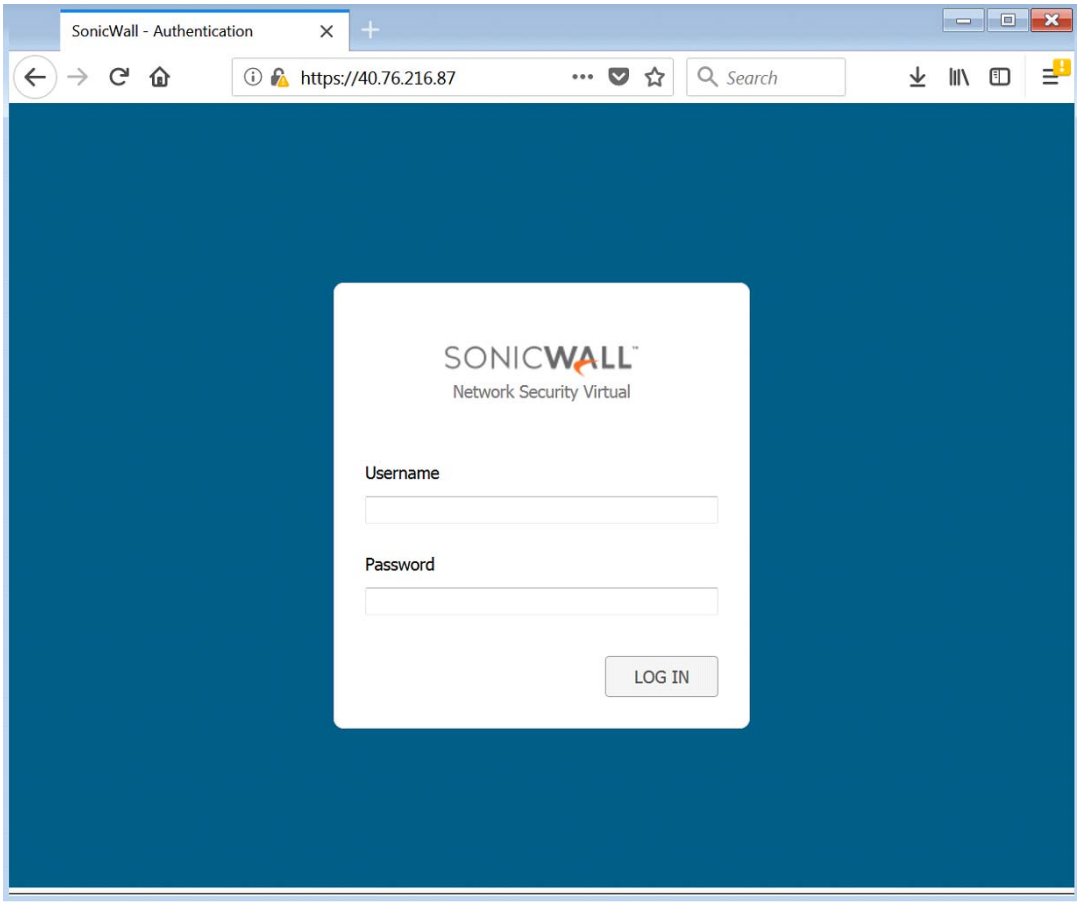
It will take approximately 10 minutes to deploy NS*v* respective resources. You can view the progress by clicking the icons indicated below:



6 To connect to the SonicWall NSv management GUI click “Virtual Machines” from the left hand menu. Then select the NSv VM name, in the overview section a public IP address is displayed, In the example below, 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 Series on Azure on page 10.

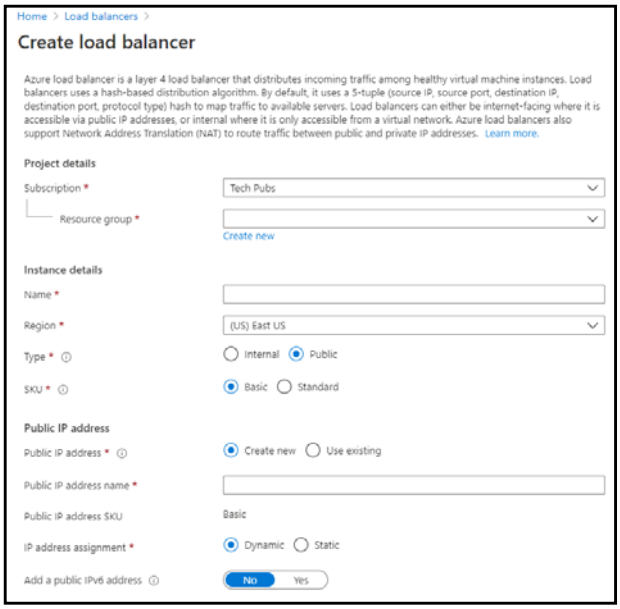
# Deploying a Load Balancer

We are using the default Microsoft Load Balancer – this is an **optional** step as you can chose at the bottom of the template to have two load-balancers automatically deployed.


### *To deploy load balancers, configure the following:*

1 In the Azure Services **Home** page, select **Load Balancers** option.

2 Click **Add** or **Create Load Balancer** button.




3 Configure the following options:

- **Subscription** – This value is pre-populated unless you have more than one subscription like, one via MSDN and an Enterprise Account.
- **Resource group** – Chose the resource group that you create when installing the template.
- **Name** – The name of the load balancer.
- **Region** – Chose the same location that you chose for the template.
- **Type** – The default type is set as **Public**.
- **SKU** – The default SKU is set as **Basic**.
- **Public IP address** – Select **Use Existing** option.
- **Choose public IP address** – Chose the one that was created by the template.
- **Add a public IPv6 address** – Select **No.**

4 Click **Review + create**. The deployment process will begin. Once deployment is complete, configure the load balancer properties.

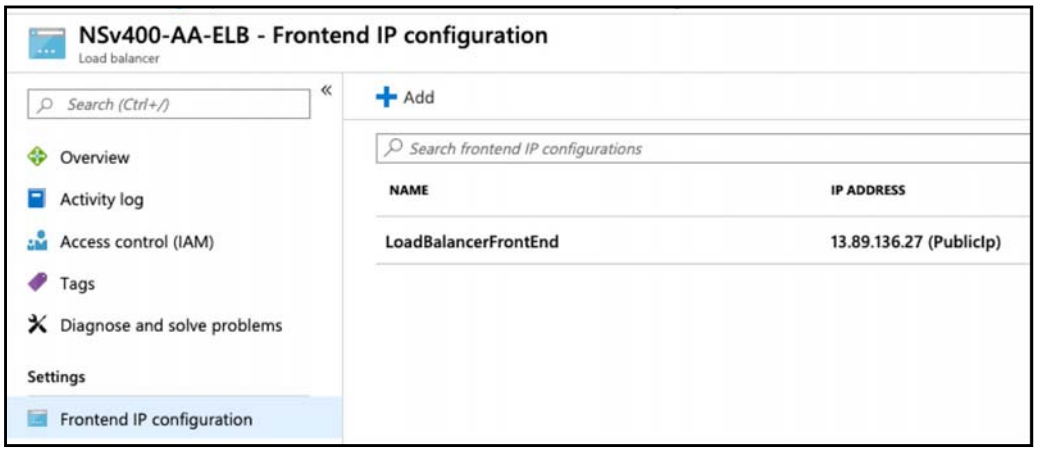
## Configuring the Load Balancer

The load balancer is already pre-configured in the template. There is an external and an internal deployed. The default Azure load balancers cannot sync connections among each other, meaning the when traffic comes in from the outside, its hits the external LB, is then forwarded to one of the firewalls. The internal firewall cannot see this traffic and direct it back to the same firewall where it came from. In order to make this work, the processing firewall needs to tag the traffic on egress. The way we do this is by doing src-nat translation so that each firewall puts itself into the source address of the IP packet. Load balancers have a frontend and backend configuration. On the frontend is the Virtual IP (VIP) and on the backend are the collection of firewalls across we load share. The frontend IP must be a public IP.

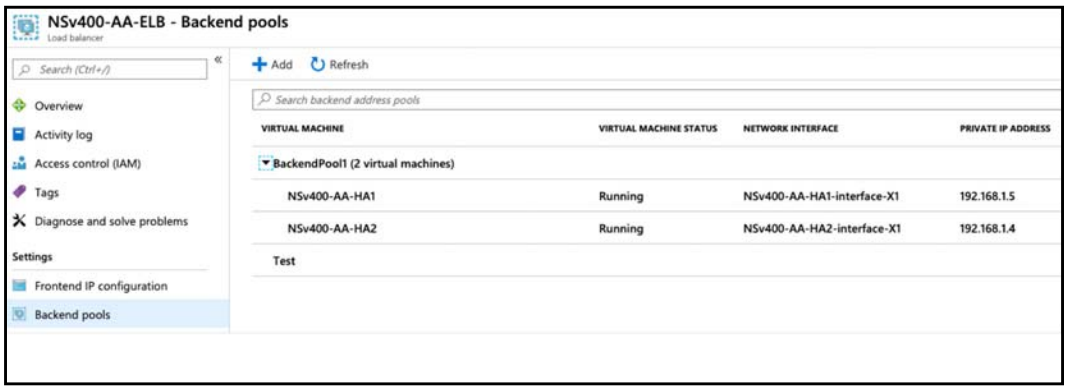
### *To configure the Load Balancer:*

1 On the Azure **Home** page, select **Load Balancers** and select the Load Balancer that you have created.

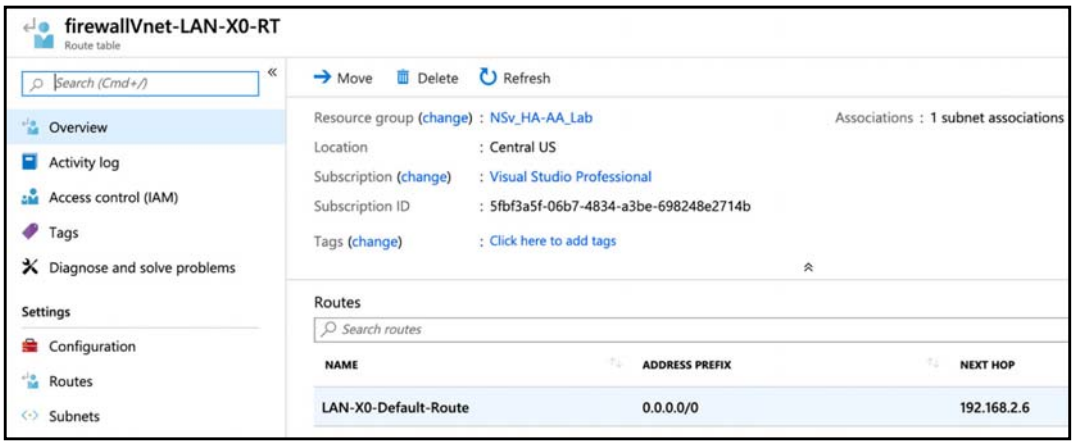
2 On the **Settings > Frontend IP configuration** page, configure the front end IP. The frontend IP must be a public IP.




3 On the **Settings > Backend pools** page, configure the backend IPs. For the Backend pools, add two or more firewalls.




4 If the internal load-balancer is configured, a UDR needs to be configured to point to the LB instead of the FW.




# Accessing Your NS$_v$ in the Azure Portal

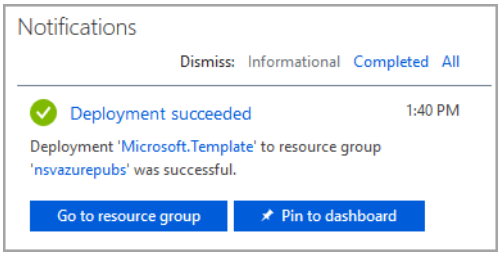
There are a number of pages and settings for your NSv virtual machine available in the Azure portal.

**Topics:**

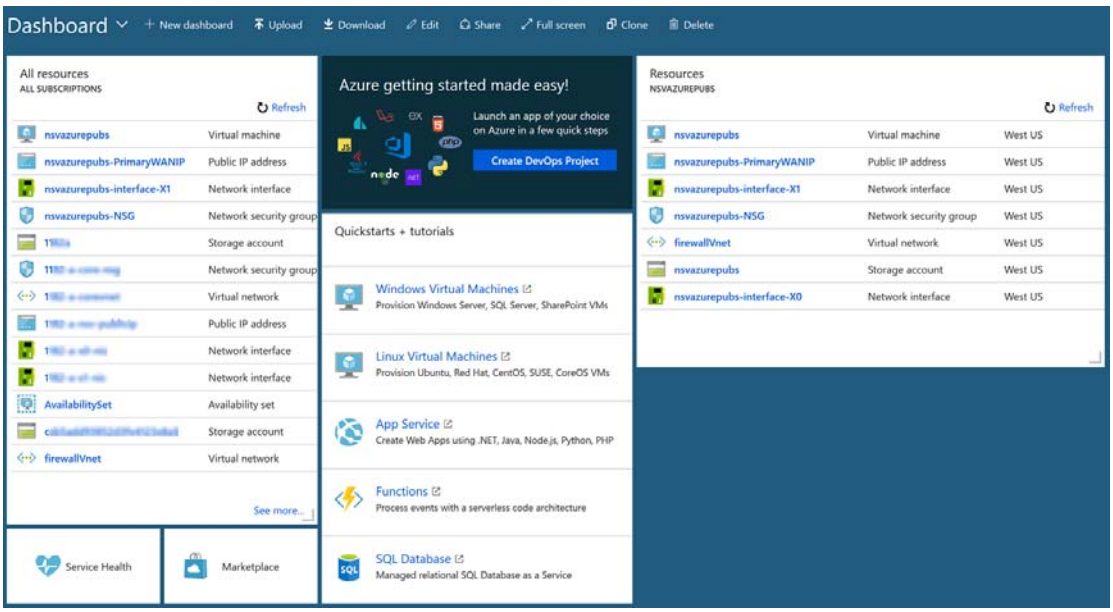


# Updating Your Dashboard and Accessing the NS$_v$ Resource Group

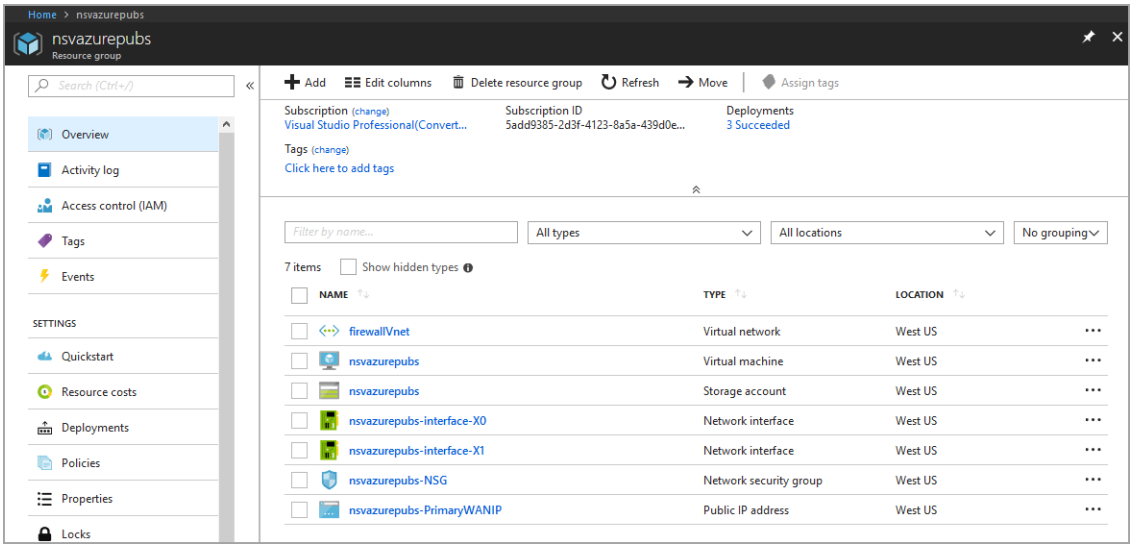
The notification window for **Deployment succeeded** provides two buttons for your immediate use.



- Click the **Pin to dashboard** button 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**.

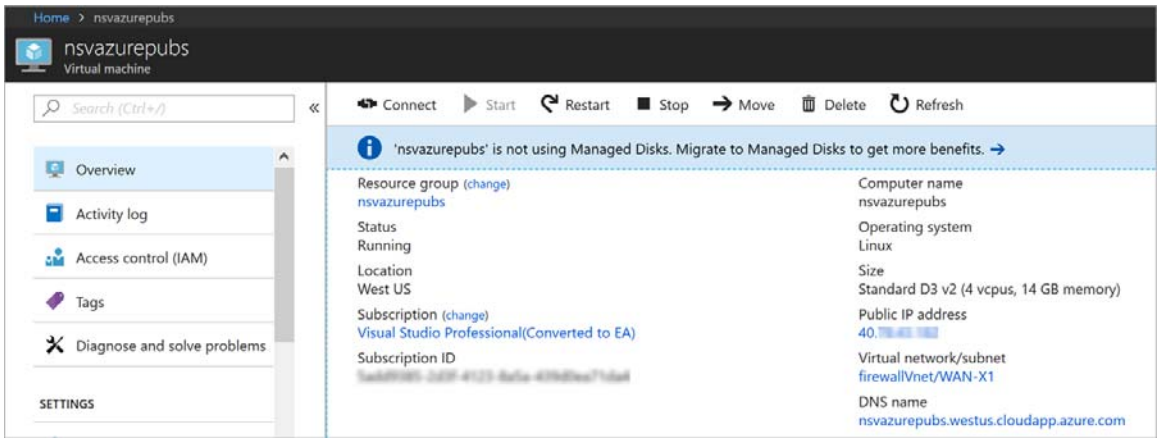



- Click **Go to resource group** to display the **Resource group** page.



# Finding the Public IP Address of Your NS*v*

On the **Dashboard** page or the **Resource group** page, click the VM name link to display the **Public IP address** of your NS*v* virtual firewall. The VM name link has a description or type of ***Virtual machine***.

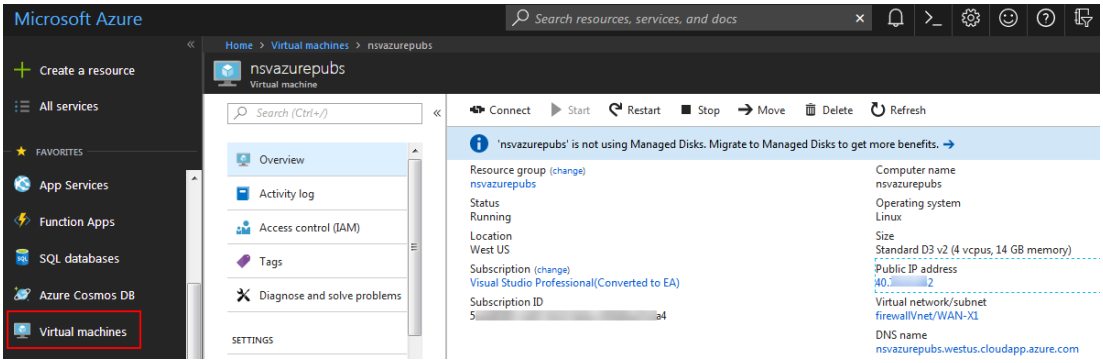



**TIP:** Log into the NS*v* at the displayed public IP address for SonicOS management and to register the NSv on MySonicWall.

# Logging into Your NS*v* for SonicOS Management

***To log into your NSv for SonicOS management:***

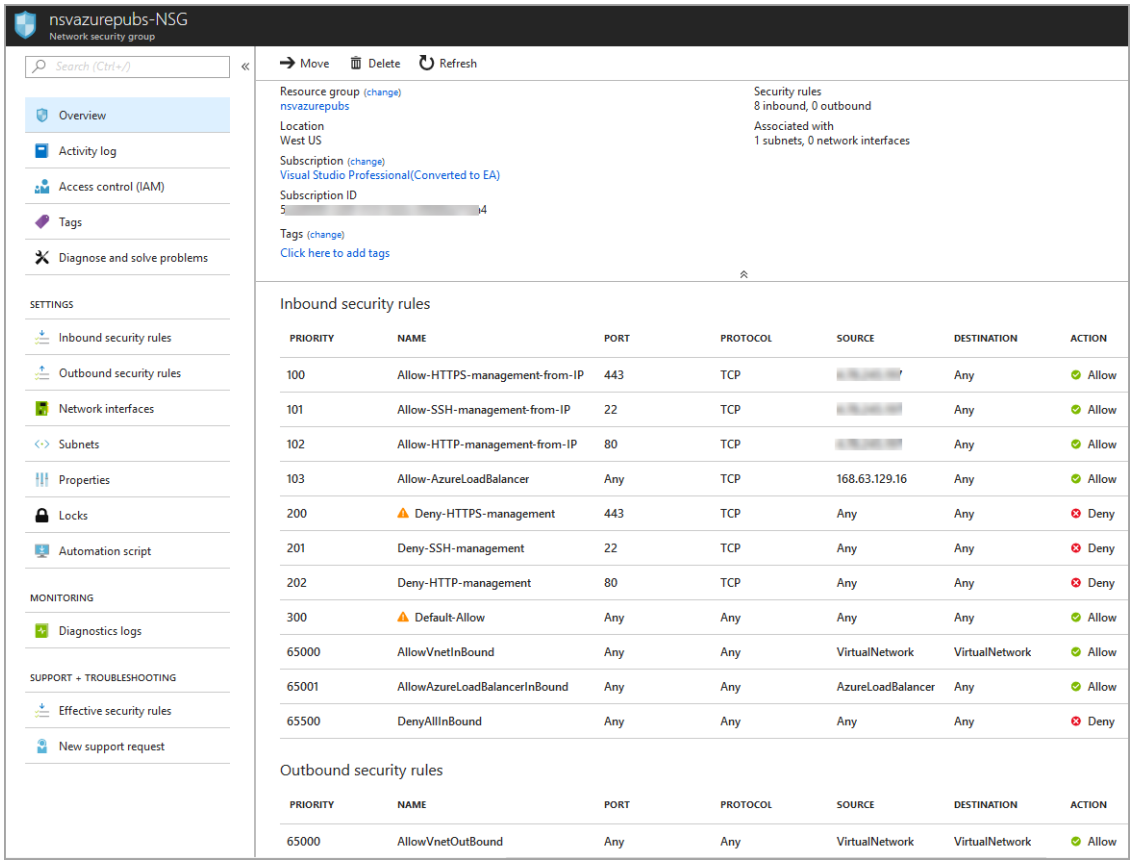
1. In the left navigation pane of Azure, click **Virtual Machines**.
2. Click the name of your NS*v*.
3. In the **Overview** screen, the IP address of the NS*v* is displayed under **Public IP address.**




4. Point your browser to **https://*<Public IP address>***, using the public IP address of your NS*v*.
5. Log into SonicOS (default credentials: *admin/password*).

# Viewing and Configuring Security Rules

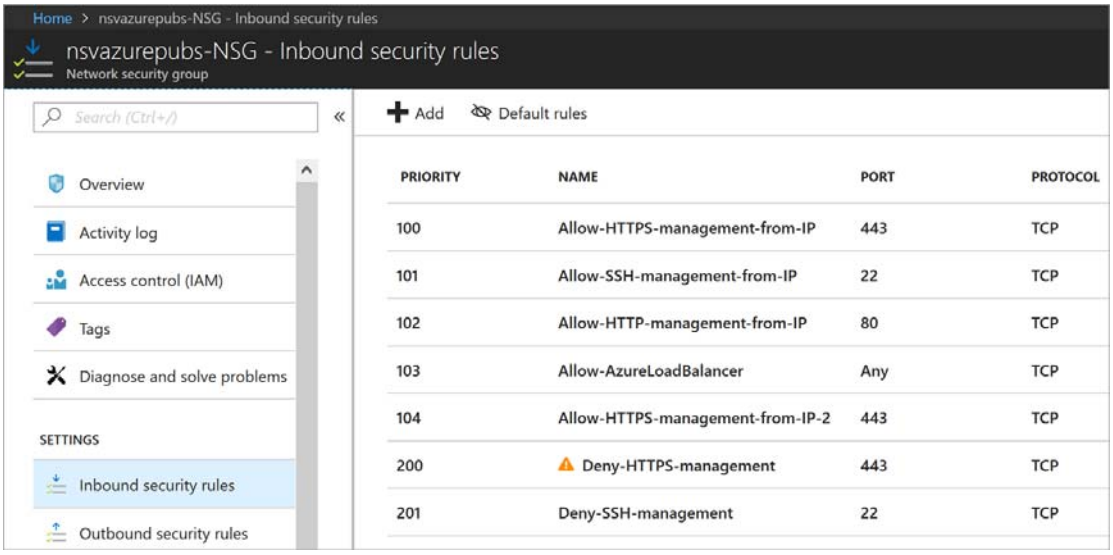
On the **Dashboard** page or the **Resource group** page, click the **NSG** link to view the inbound and outbound security rules. The NSG link has a description or type of ***Network security group***.



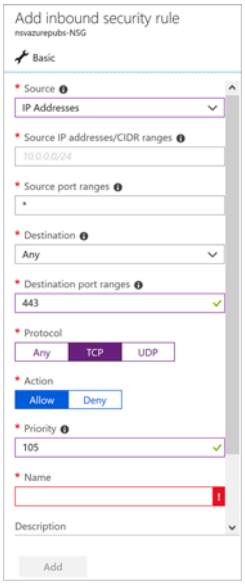

The inbound rules control management access to the NS*v*. The Source for these rules is initially set to your public IP address, that you entered during the installation process for **Management Access IP Source**. To manage the NS*v* from another location, you need to add an inbound rule.

*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 the **Add** button. 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 NS*v* in Azure

This section describes how to configure a route on your SonicWall NS*v* Series virtual firewall so that you can pass traffic though the NS*v*.

If you have not yet registered your NS*v* on MySonicWall, do that now. See Registering the NSv Appliance from SonicOS on page 41 for information. Your NS*v* must be registered to enable full functionality.

### *To configure a route on your NSv Azure firewall:*

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

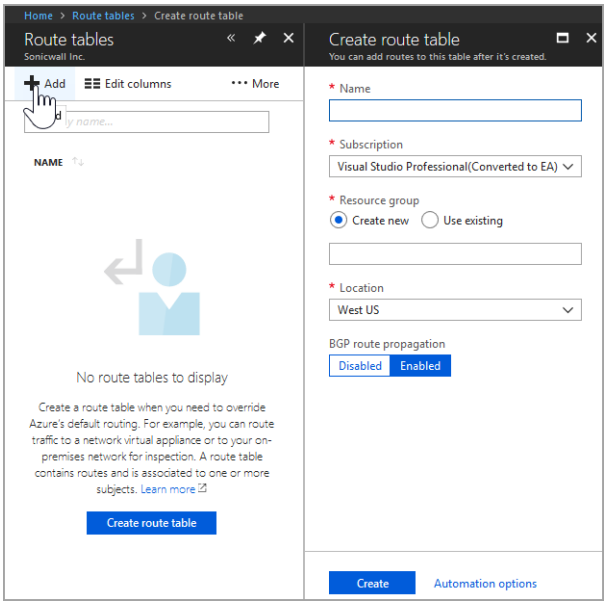
2 In the Azure left navigation pane, click **All services**.


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 is displayed.



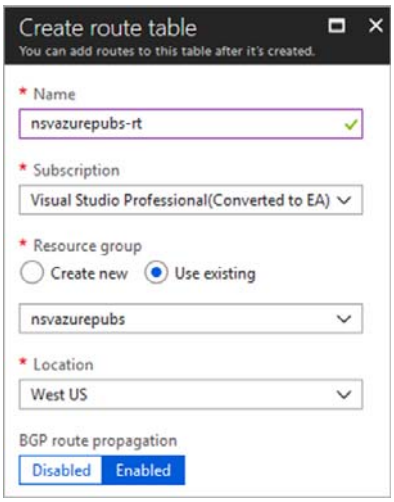

6 In the **Name** field, type in a name for this route table.

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

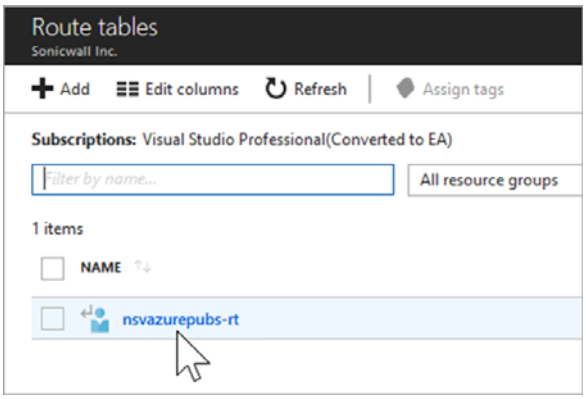
8 For **Resource group**, select **Create new** if you will use the route table for other networks, or select **Use existing** if you will use the route table for this network only. If you select **Use existing**, you can use the drop-down list to select the same resource group you are using for your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

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

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

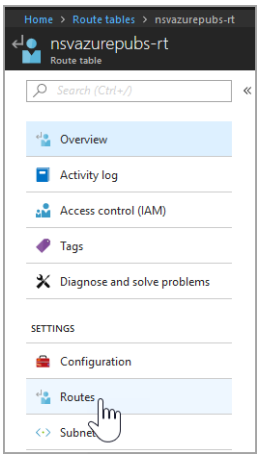


11 Click **Create** to create the route table. After a brief wait, **Notifications** displays ***Deployment succeeded*** and the new route table appears in the **Route tables** screen.




12 Click on the route table name.

13 In the route table screen, under **SETTINGS**, click **Routes**.



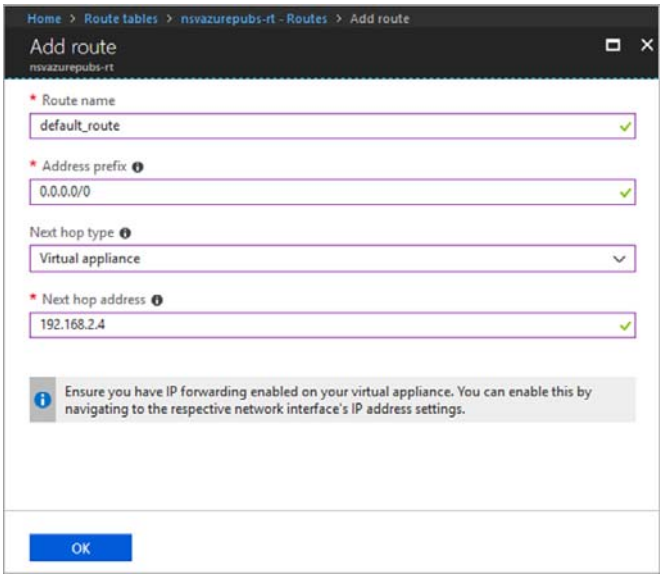

14 On the **Routes** screen, click **Add** to add a route to the route table.

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.

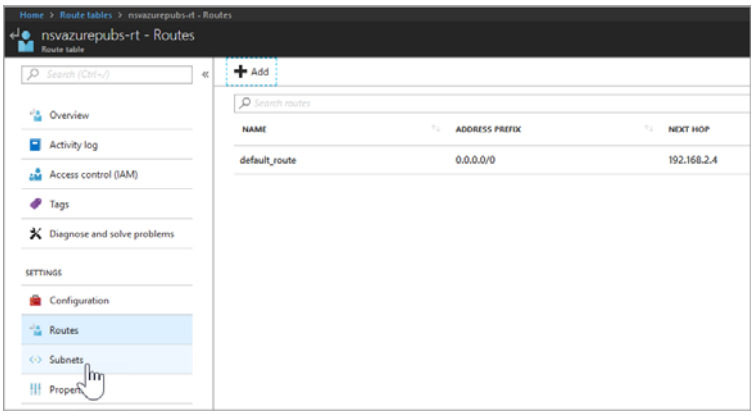
17 For **Next hop type**, select **Virtual appliance** from the drop-down list.

18 For **Next hop address**, type in the IP address of the NSv X0 interface.

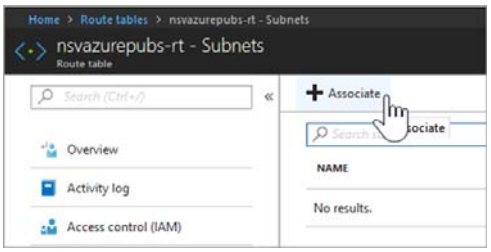



19 Click **OK**. This creates the route.

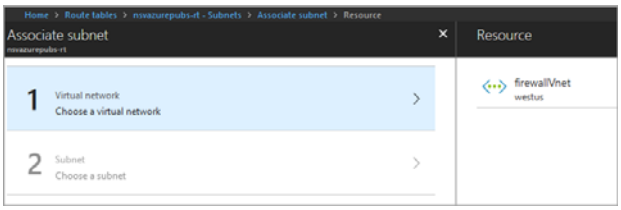
20 Next, you need to associate the route table. In the **Route table** options, click **Subnets**.



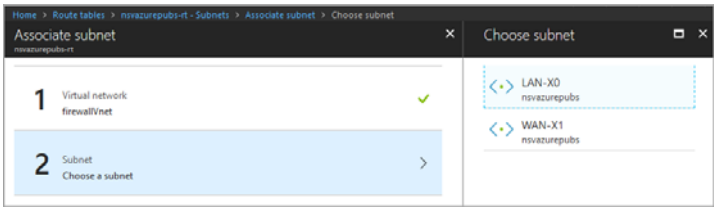

21 In the **Subnets** screen, click **Associate**.



22 In the **Associate subnet** screen, click **Virtual network**. The resources with possible virtual networks are displayed to the right under **Resource**.

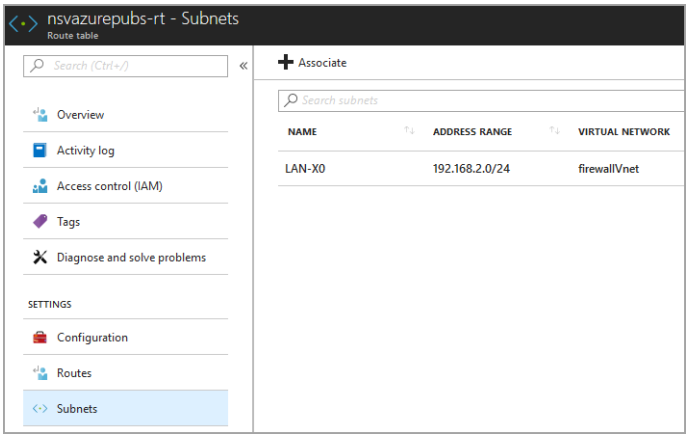



23 Click on the desired resource. The display on the right changes to the **Choose subnet** screen and shows the possible subnets available for that resource.




24 Under **Choose subnet**, click **LAN-X0**. Since we entered the X0 IP address above 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 in Azure on page 36.

# Testing Traffic Through Your NS$_v$ in Azure

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:

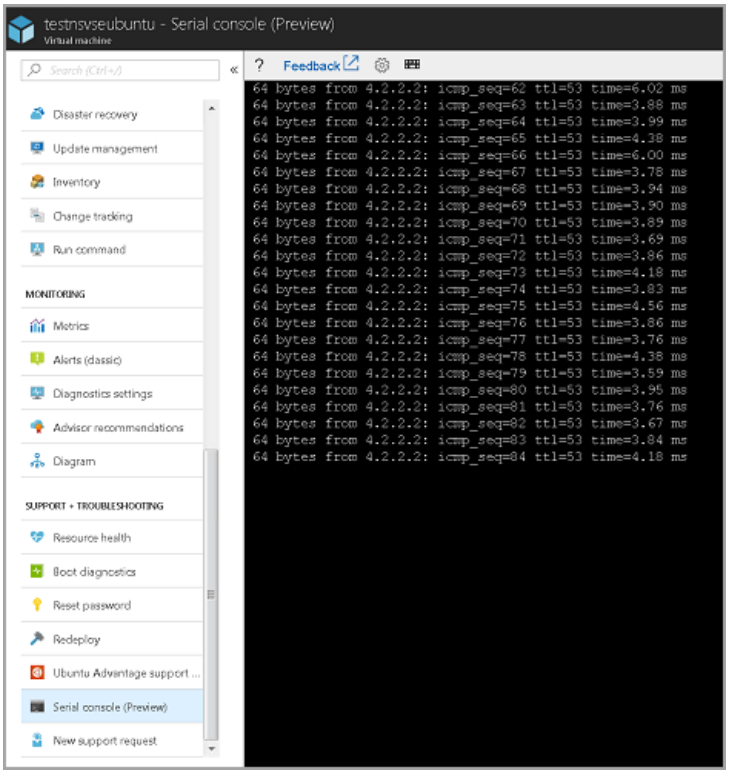
- Subscription
- Resource group

- 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 VM (Ubuntu, for example), open a console window. For an Ubuntu VM on Azure, click **Serial Console** in the **Virtual machine** options.

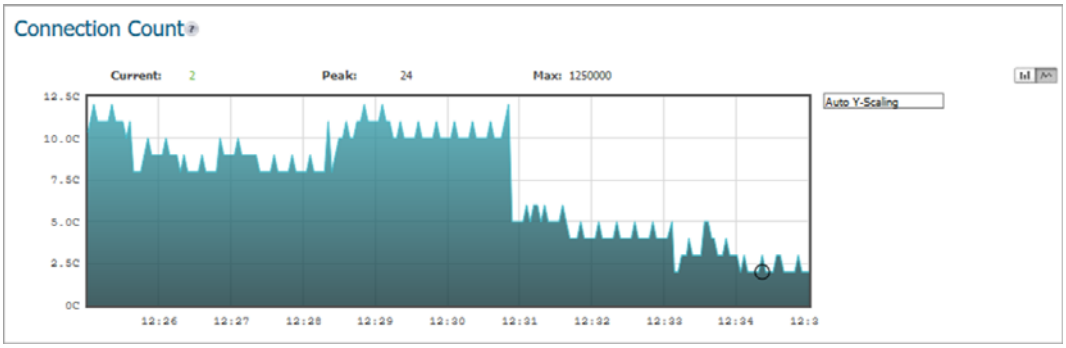
2 Type ***ping 192.168.2.4*** on the command line.




The pings should succeed.

3 Log into your NS*v* 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 will also show activity. This verifies that traffic can be forwarded to the NS*v*.

# Troubleshooting Installation Configuration

If the NSv fails to come up, follow the instruction in Using the Virtual Console on page 54 to go to the NSv Management Console window or the SonicOS CLI window. Check the boot messages:

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

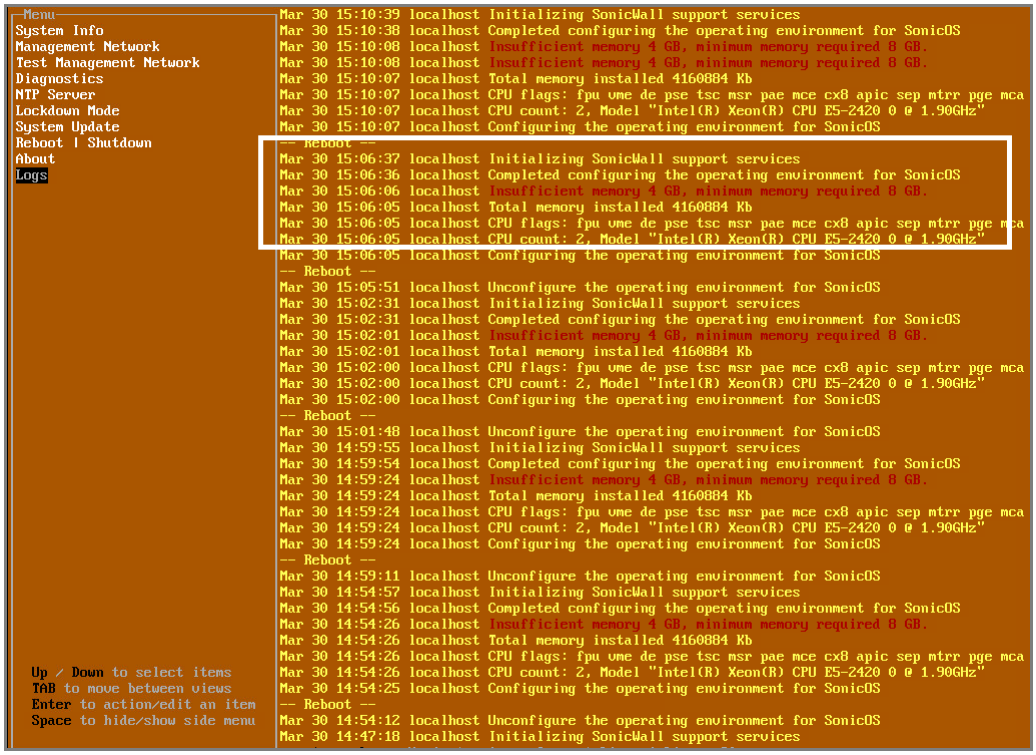
## Insufficient Memory Assignment

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.

SonicOS boot message:

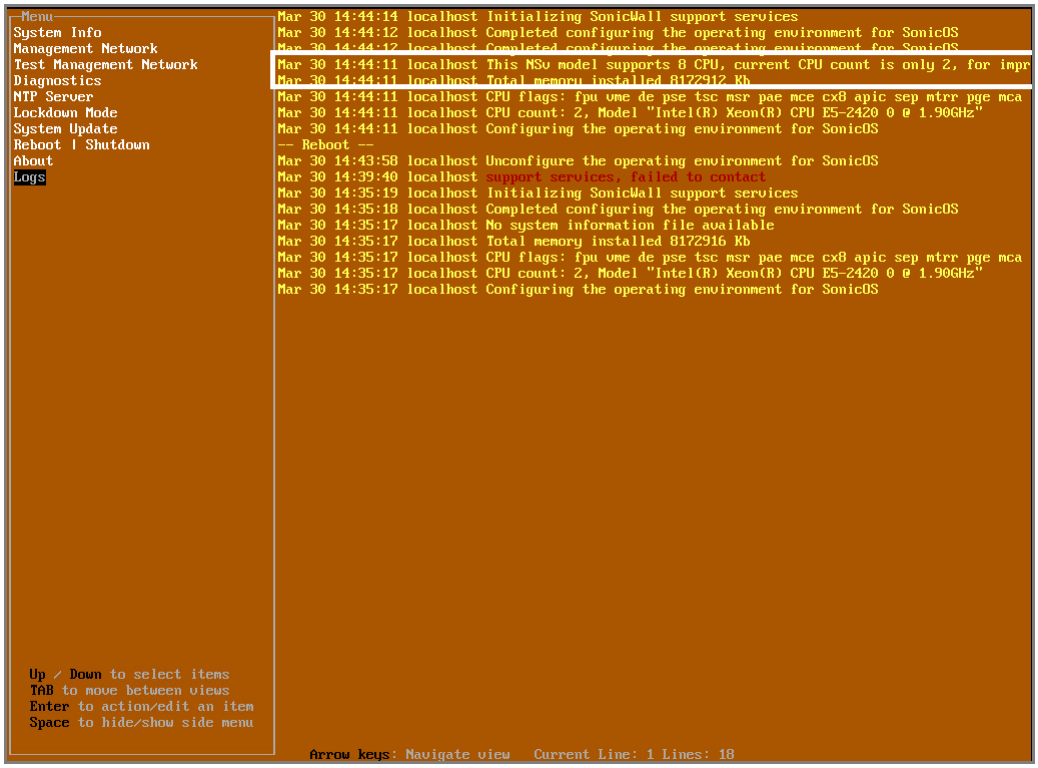
```
Insufficient memory 4 GB, minimum memory required 10 GB for NSv model: “NSv 800 Beta”
Power off the Network Security virtual appliance and assign 10 GB to this virtual appliance.
```

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




**NOTE:** For details on navigating the NSv Management Console to troubleshoot the installation, see Using the Virtual Console on page 54.

Memory may be insufficient without an insufficient memory log entry:

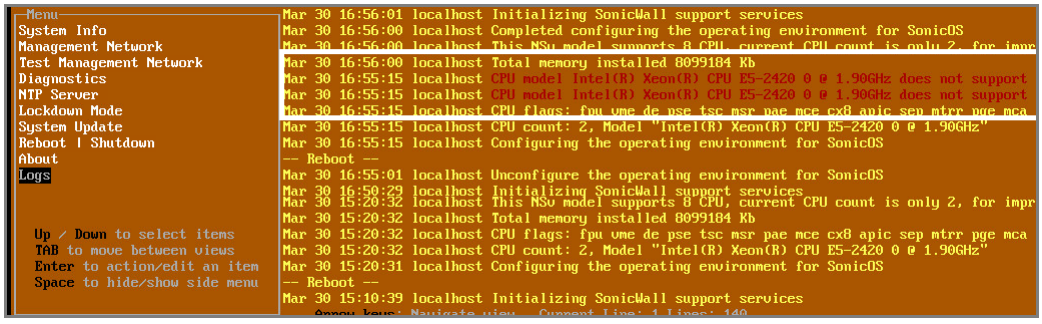



# Incompatible CPU

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:




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
```

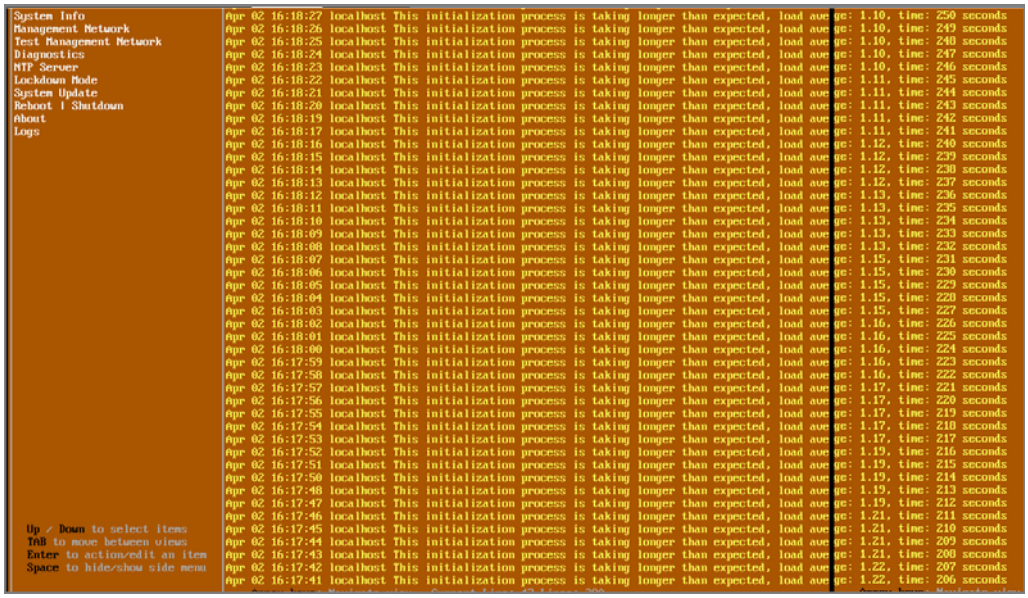
**NOTE:** The above error may occur when EVC masks the CPU capability.
https://communities.vmware.com/thread/536227 resolution is to disabled EVC.

# 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:



3

# Licensing and Registering Your NS$_v$

**Topics:**



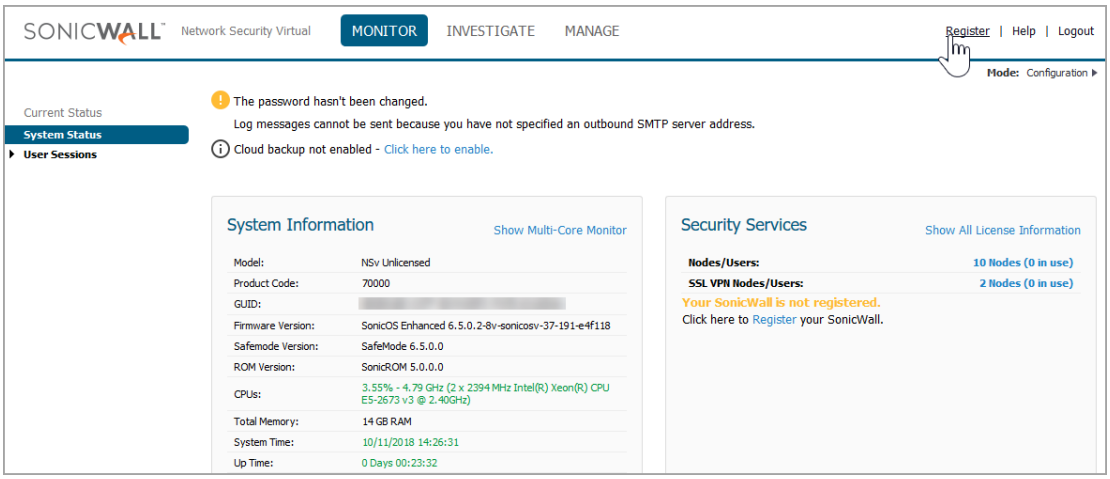
## Registering the NS$_v$ Appliance from SonicOS

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

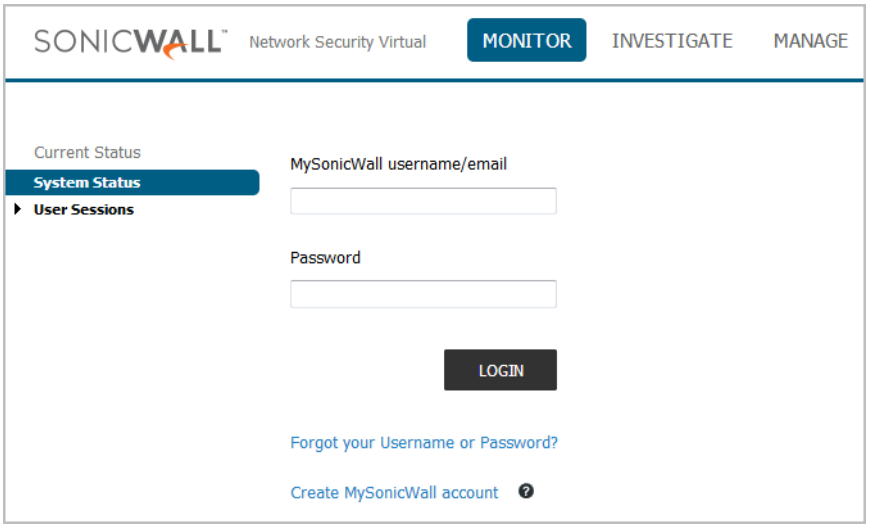
**NOTE:** System functionality is extremely limited if registration is not completed. See Using SonicOS on an Unregistered NSv on page 49 for more information.

***To register your NSv appliance:***

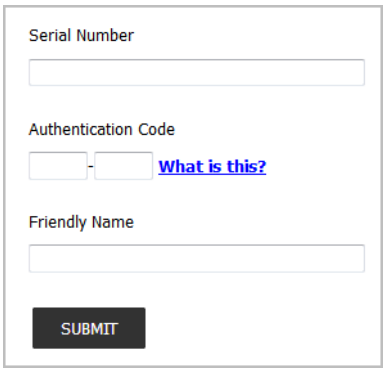
1. Point your browser to your NS*v* WAN or LAN IP address and log in as the administrator (default *admin / password*).
2. Click the **Register** link in the top banner or on the **MONITOR | System > Status** page.



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




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




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

6 Click **SUBMIT**.

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

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

SonicOS automatically restarts and then displays the login page.

9 Log into SonicOS.

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

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

# Registering with Zero Touch Deployment

The SonicWall NS*v* Series for ESXi is Zero-touch enabled. Zero-Touch makes it easy to register your unit and add it to SonicWall Capture Security Center or SonicWall GMS On-Premises for management and reporting.

**Topics:**



# Deploying from CSC Management

## 1) Register:

- Point your browser to https://cloud.sonicwall.com and log into your MySonicWall account or create an account.
- In **Capture Security Center**, click the **mySonicWall** tile to launch the **MySonicWall Dashboard**.
- Click the **Add Product** button  to launch the **QUICK REGISTER** dialog and then type in the serial number of your SonicWall NS*v*. Click **Confirm**.

  You should receive the NS*v* serial number and authentication code with your purchase confirmation email.
- In the **REGISTER A PRODUCT** dialog, fill in the **Friendly name** and **Authentication code**, and select the **Tenant Name**. By default, all products are placed under ***SonicWall Products Tenant***.
- Click **Register**.

## 2) Enable Zero Touch and CSC Management and Reporting:

- MySonicWall recognizes your appliance model and displays the **Zero Touch** option. Enable **Zero Touch** and then click **Register** again. A success message is displayed to indicate Zero Touch readiness.
- In MySonicWall, navigate to **Product Management > My Products**, select the appliance, and click the **Try** button to enable the license for **CSC Management and Reporting** (if not enabled already). A success message displays.

## 3) Connect and Power On the VM:

**NOTE:** The NS*v* must be able to obtain an IP address via DHCP from the WAN connection. You may use as static IP address. For details on using the NSv Management Console to setup a static IP address, see Using the Virtual Console on page 54.

**CSC Management** automatically acquires the unit (it can take up to 30 minutes for initial acquisition). Once the unit is acquired, you can begin management.

To view the status of your NS*v* instance:

- In MySonicWall, pull down the curtain for **Capture Security Center**.
- Using the same Tenant as you selected during registration, click the **Management** tile.
- Click the appliance serial number or friendly name under **DEVICE MANAGER** to display its status.

## Getting the Latest Firmware for the NSv

1 In **Capture Security Center,** click the **mySonicWall** tile.

2 Navigate to **Resources & Support > My Downloads** and select your product firmware from the **Product Type** drop-down menu.

3 Click the link for the firmware you want and save the file to a location on your computer.

4 Pull down the curtain for **Capture Security Center**.

5 Using the same Tenant as you selected during registration, click the **Management** tile.

6 In **DEVICE MANAGER**, click on the NS*v* instance in the left pane.

7 In the center pane, go to the **Register/Upgrades > Firmware Upgrade** page.

8 Click the **Choose File** button to select the firmware you just downloaded, then click **Upgrade from Local File**.

# Deploying from GMS On-Premises

**PREREQUISITE:** GMS 8.7 or higher is required. Be sure that your GMS system is <Short Product Name> enabled. Refer to the knowledge base article at:
https://www.sonicwall.com/support/knowledge-base/?sol_id=190205183052590

## 1) Register:

- Log into your MySonicWall account or create an account at www.mysonicwall.com.
- Click the **Add Product** button to launch the **QUICK REGISTER** dialog and then type in the serial number of your SonicWall appliance. Click **Confirm**.

  You can find the serial number and authentication code on the shipping box or appliance label.
- In the **REGISTER A PRODUCT** dialog, fill in the **Friendly name** and **Authentication code**, and select the **Tenant Name**. By default, all products are placed under ***SonicWall Products Tenant***.
- Click **Register**.

## 2) Enable Zero Touch:

- MySonicWall recognizes your NS*v* model and displays the **Zero Touch** option. Enable **Zero Touch**.
- Select the desired GMS Public IP from the **GMS Server Public IP/FQDN** drop-down list. The **ZeroTouch Agent Public IP/FQDN** field is populated with the associated IP address.

  **IMPORTANT:** Verify that both of these IP addresses are the same as those you configured during the prerequisite process.
- Click **Register**.

## 3) Connect and Power On VM:

**NOTE:** The NSv must be able to obtain an IP address via DHCP from the WAN connection. If you need to use a static IP address, refer to the details on using the NSv Management Console, see Using the Virtual Console on page 54.

**GMS** automatically acquires the unit (it can take up to 30 minutes for initial acquisition). Once the unit is acquired, you can begin management.

To view the status of your NSv instance:

- Log into GMS and navigate to the **FIREWALL** view.
- Click on the appliance in the left pane to display the status.

## Getting the Latest Firmware for the NS$_v$

1 In a web browser, navigate to www.mysonicwall.com.

2 Navigate to **Resources & Support > My Downloads** and select your product firmware from the **Product Type** drop-down menu.

3 Click the link for the firmware you want and save the file to a location on your computer.

4 In GMS, navigate to the **FIREWALL** view and click on the NSv instance in the left pane.

5 In the center pane, go to the **Manage > Register/Upgrades > Firmware Upgrade** page.

6 Click the **Choose File** button to select the firmware you just downloaded, then click **Upgrade from Local File**.

# Registering an NS$_v$ Manually in a Closed Network

**NOTE:** This registration method uses Manual Upgrade and is **not** recommended for normal product registration on products that have internet access. See Registering the NSv Appliance from SonicOS on page 41 for the recommended registration method on products with internet access.

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

**NOTE:** System functionality is extremely limited if registration is not completed. See Using SonicOS on an Unregistered NSv on page 49 for more information.

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

1 Log into your NSv appliance and navigate to the **MONITOR | System Status** page.

2 Make a note of the **GUID**, or leave the page open in your browser. The **GUID** is displayed in the **System Information** section.

**NOTE:** If the **GUID** is already updated on MySonicWall, it is necessary to de-register and restart the NSv. See Deregistering Your NSv on page 46. If your NSv cannot connect with MySonicWall, contact Technical Support to de-register the **GUID** from MySonicWall.

3 In another browser tab or window, log into your MySonicWall account.

4 Navigate to **My Products** and click on the entry for your NSv appliance.

5 Click on the **+** next to **GUID**.Enter the **GUID** into the dialog box and click **Update**.

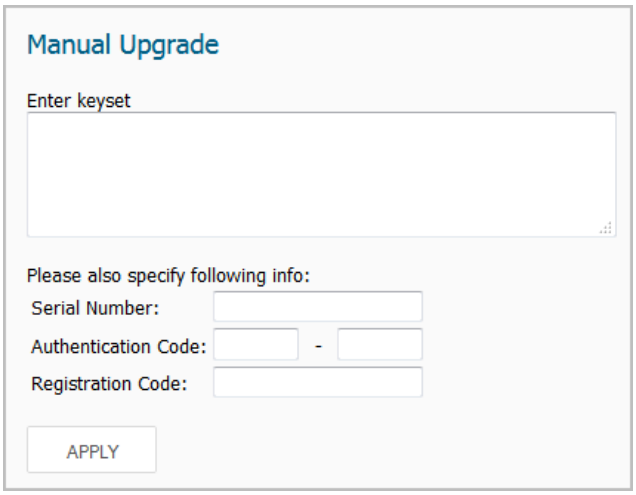
6 To get the **License Keyset**, first click the key icon. The **License Keyset** is displayed. This is a binary representation of all the service licenses activated on your NSv.

7 Select the **License Keyset** and copy it to your clipboard.

8 Log into your NSv appliance or return to that browser window if still logged in.

9 Navigate to the **MANAGE | Licenses** page in SonicOS.

10 Under **Manual Upgrade**, paste the **License Keyset** into the **Enter keyset** field.




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

12 In the **Registration Code** field, enter the registration code you received when you did the initial registration in MySonicWall to obtain the OVA file.

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

14 Click **ACCEPT**.

Your NS*v* virtual firewall is now registered.

# Deregistering Your NS$_v$

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

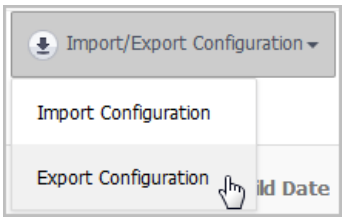
**NOTE:** Only an NS*v* which was registered online can be deregistered. If the NS*v* was registered using the offline method, deregistration is not supported. For assistance, contact technical support.

***To deregister an NSv:***

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

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

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

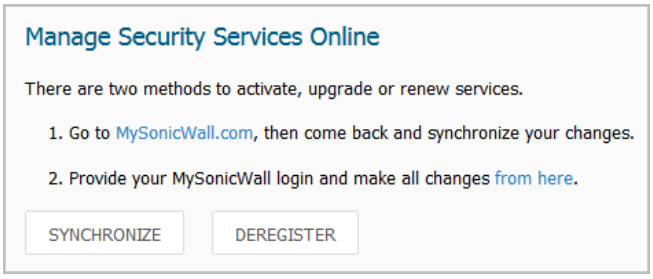


This makes it possible to import the settings to another NS*v* instance.

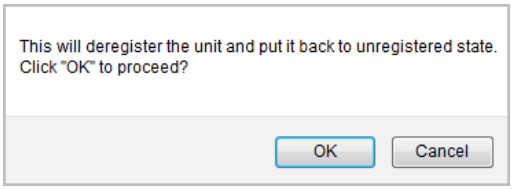
**CAUTION: Be sure to export your configuration settings before deregistering your NS*v*. You cannot recover them after deregistration.**

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

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




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




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

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

# Converting a Free Trial License to Full License

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

***To convert your free trial to a production version:***

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

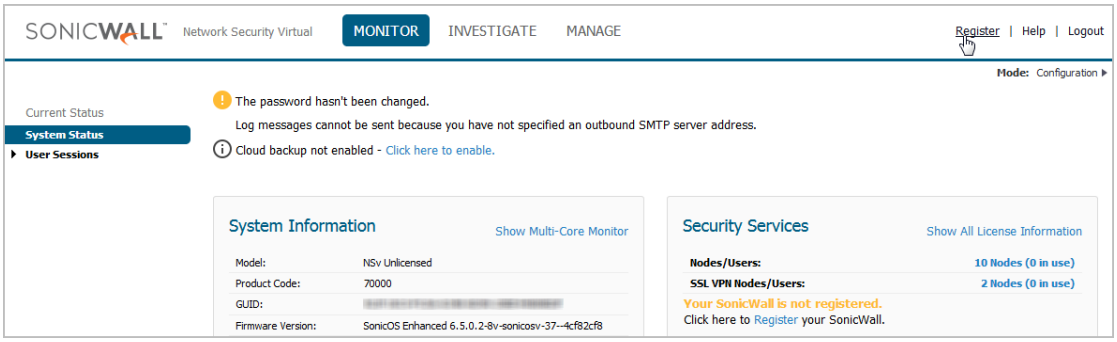
2 Log into SonicOS on your free trial instance.

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

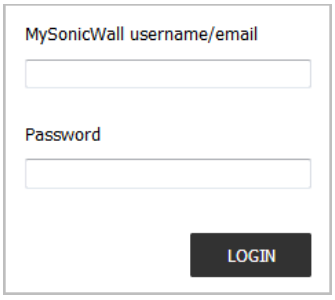
4 Under **Manage Security Services Online**, click the **DEREGISTER** button.

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

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




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




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

9 Click **SUBMIT**.

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

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

SonicOS automatically restarts and then displays the login page.

12 Log into SonicOS.

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

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

4

# SonicOS Management

**Topics:**



## Managing SonicOS on the NS$_v$ Series

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

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

***To log into SonicOS for management of the 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 NS*v* from a computer on that network for SonicOS management. The NS*v* X0 IP address is 192.168.168.168 by default.

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

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

**NOTE:** To upgrade your release of NS*v*, either use the management interface as described in *SonicOS 6.5 for NSv Series Updates* documentation available on the SonicWall portal, or use the SafeMode web interface as described in Installing a New SonicOS Version in SafeMode on page 71.

## Using SonicOS on an Unregistered NS$_v$

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

### Available SonicOS Pages on Unregistered NSv

| Top Level View | Page Group | Page Within Group | Description |
|---|---|---|---|
| **MONITOR** | System Status | n/a | System information, Node license, Alerts, Network interface settings |
| | User Sessions | SSL-VPN Sessions | User sessions connected via SSL VPN |
| | | Active Users | Active user session information; Logout button for users |
| | | Active Guest Users | Active guest user session information; Logout button for guest users |
| | | User Monitor | Graph of logged in users over time for client logins and web based logins |
| **INVESTIGATE** | Event Logs | n/a | Log event table, dynamically updated, filterable, searchable, one-click details |
| | Connection Logs | n/a | Connection log, source/destinations, protocols, bytes transferred, filterable, searchable, flush option |
| | Appflow Logs | n/a | Requires App Visualization license, which requires registration |
| | System Diagnostics | n/a | TSR access and Diagnostic tools:<br>  <br>See Using System Diagnostics in SonicOS on page 52 for information. |
| **MANAGE** | Licenses | n/a | Node license information, MySonicWall access, Manual Upgrade |
| | Settings | n/a | Firmware versions, Local Backup, Settings import/export, Settings options to send to SonicWall Support |
| | Restart | n/a | Restarts the virtual firewall after confirmation |

### Available SonicOS Pages on Unregistered NSv

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

# Using System Diagnostics in SonicOS

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

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

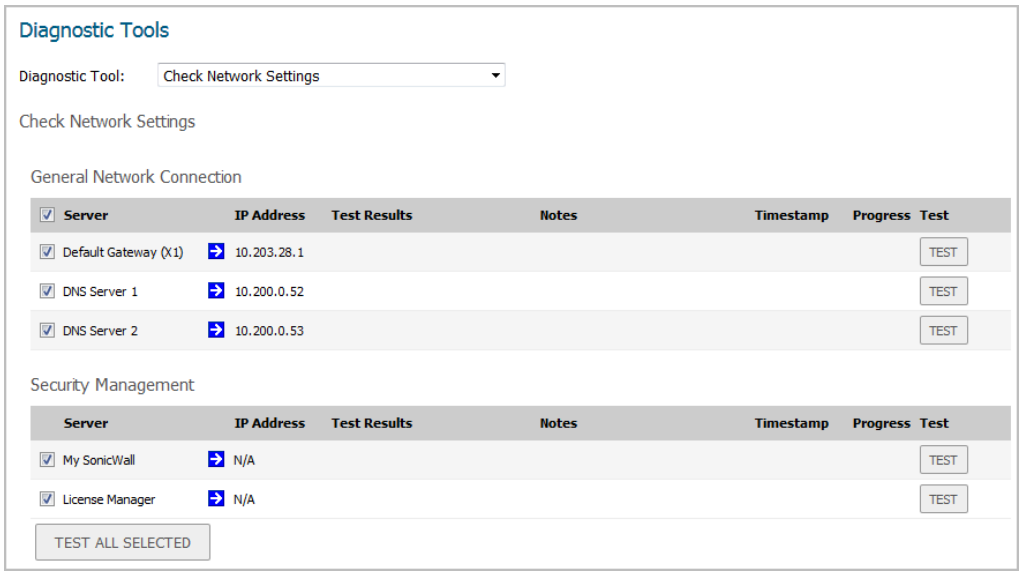

| Button | Function |
|---|---|
| **ACCEPT** | Saves any changes you made to the diagnostic support report or diagnostic tool. |
| **CANCEL** | Cancels any changes you initially made to the diagnostic support report or diagnostic tool. |
| **REFRESH** | Refreshes the data being displayed in the **Diagnostic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

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

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

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

# Check Network Settings




**Check Network Settings** is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined functional areas of the NS*v* Series, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.

Specifically, **Check Network Settings** automatically tests the following functions:

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

The return data consists of two parts:

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

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

`diagTestPolicyAuto_<IP_address/Domain_name>_0`

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

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

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

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

5

# Using the Virtual Console

**Topics:**



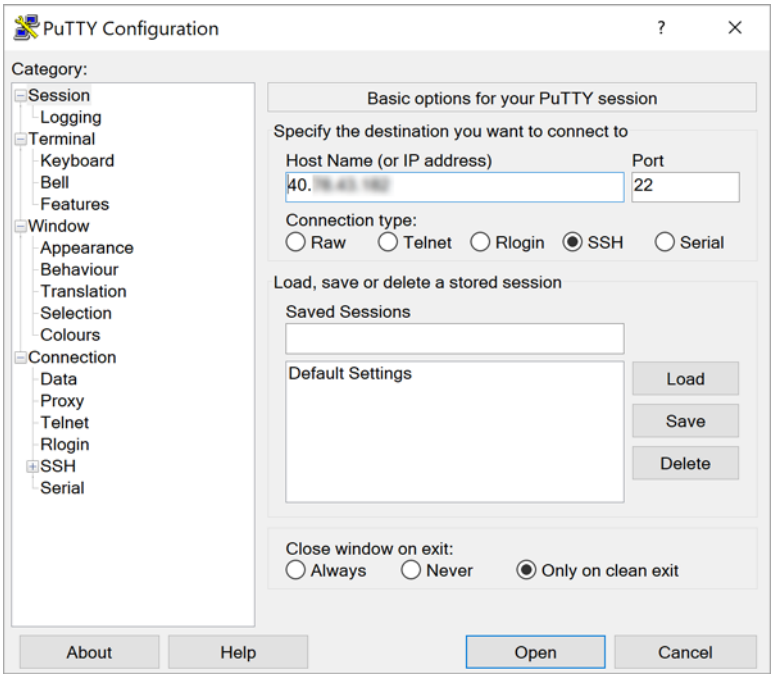
# Connecting to the Console with SSH

SSH is used to connect to the virtual console of an NS*v* deployed on Azure.

***To connect to the management console using SSH:***

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

You can find the public IP by clicking **Virtual Machines** in the Azure portal, then clicking the name of your NS*v* and locating the public IP on the **Overview** screen.



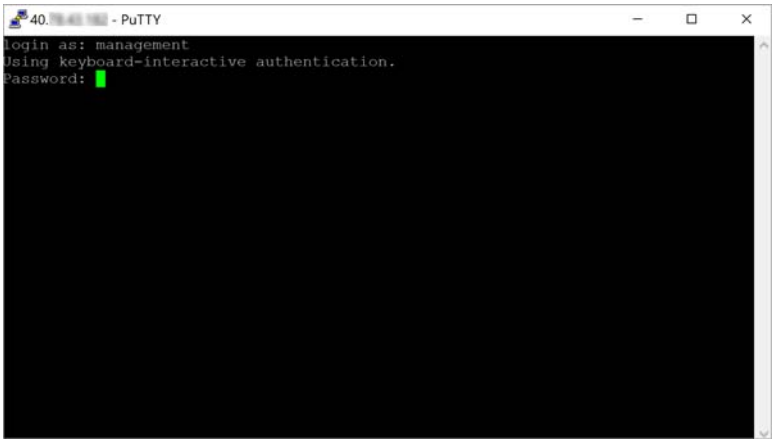

2 For **Port**, type in ***22*** if it is not already set.

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

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

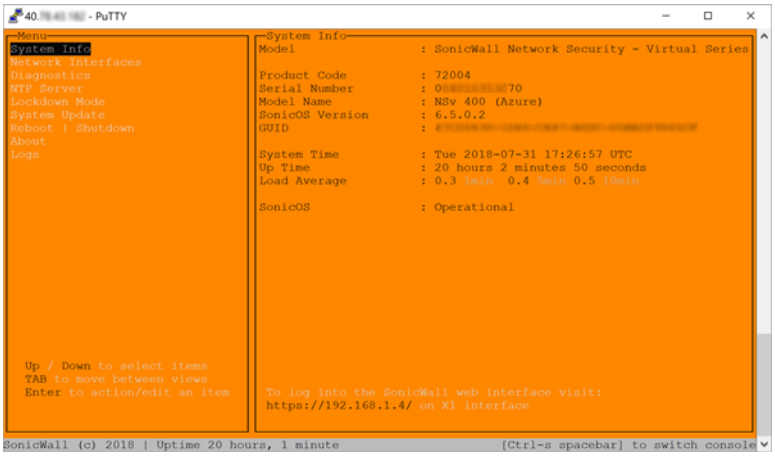
4 Click **Open** to open a console connection.

5 In the console window at the **login as** prompt, type in ***management***, which is the SSH management user name defined during the NS*v* deployment.

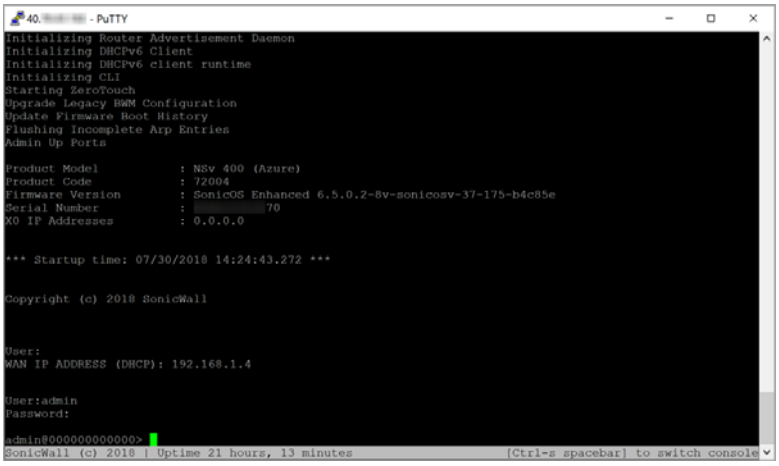



6 At the ***Password*** prompt, type in the SSH management password you defined during deployment.

The orange NS*v* management console displays.




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



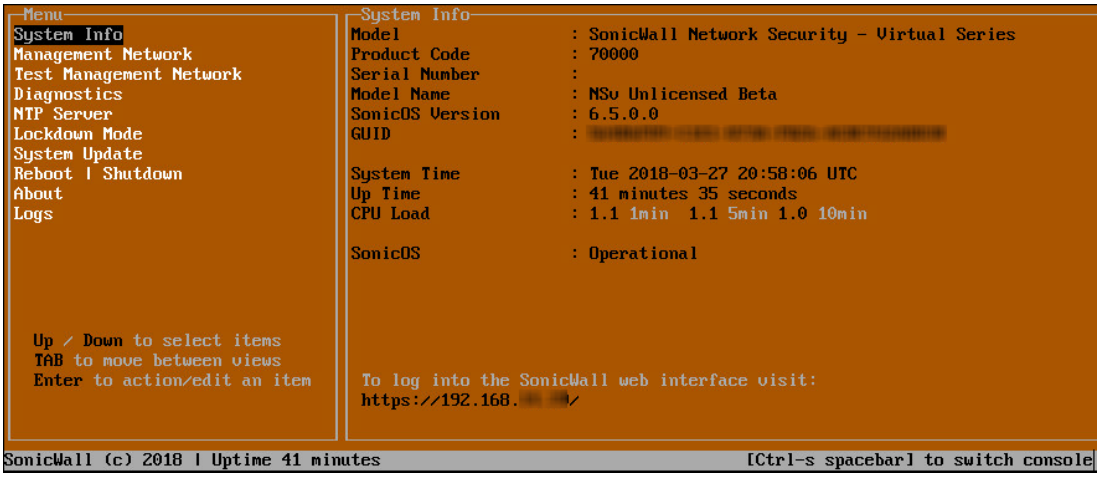
See Navigating the NSv Management Console on page 56 for information about the options in the NSv management console.

# Navigating the NSv Management Console

The NSv management console provides options for viewing and changing system and network settings, running diagnostics, rebooting SonicOS, 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 on Azure. See Connecting to the Console with SSH on page 54.

***To navigate and use the management console:***

1 Press **Ctrl+s** and then press the **spacebar** to toggle between the SSH virtual console or VMware 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.



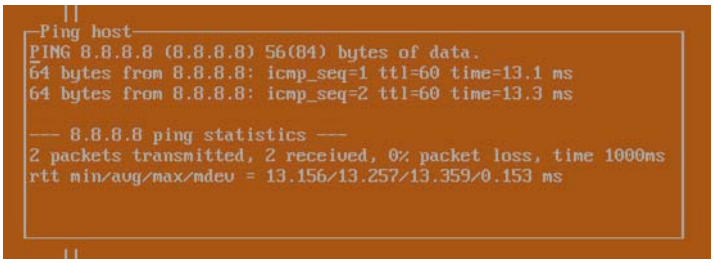

2 The main menu is displayed in the side menu (left pane). Use the up/down arrow keys to move the focus between menu items. As the focus shifts, the right pane displays the options and information for that menu item. The currently selected item is highlighted in black.

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

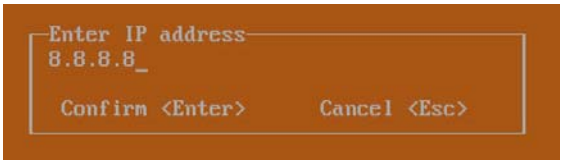
4 In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.


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




Some dialogs are for input:

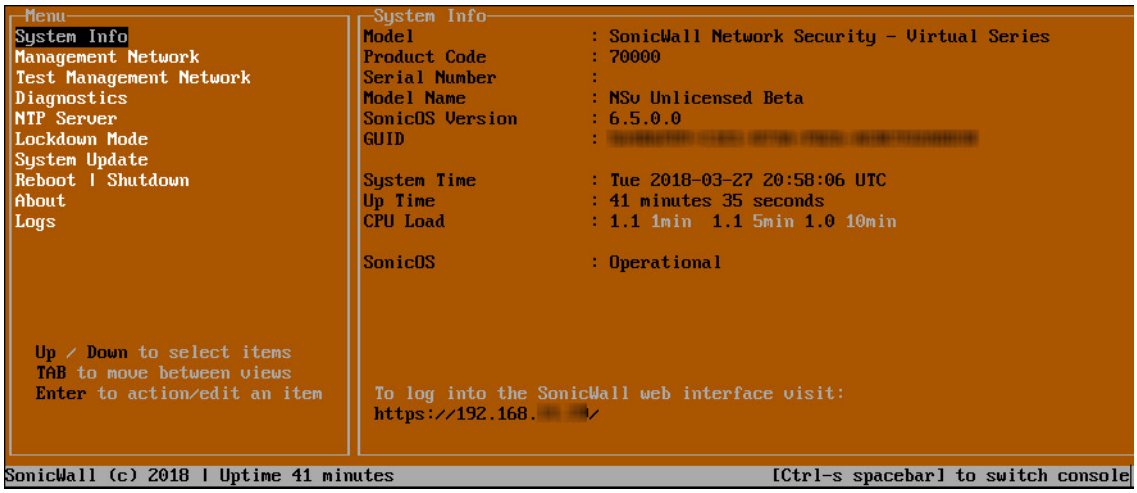



6 Use the arrow keys as needed to move between selections in the dialog. To change a value, press **Backspace** to erase each character, then type in the new value. When ready, press **Enter** to commit the change or perform the selected action. You can dismiss the dialog by pressing **Esc**.

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

- System Info on page 58
- Management Network or Network Interfaces on page 59
- Test Management Network on page 60
- Diagnostics on page 61
- NTP Server on page 62
- Lockdown Mode on page 63
- System Update on page 64
- Reboot | Shutdown on page 64
- About on page 65
- Logs on page 65

# System Info




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

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

# Management Network or Network Interfaces

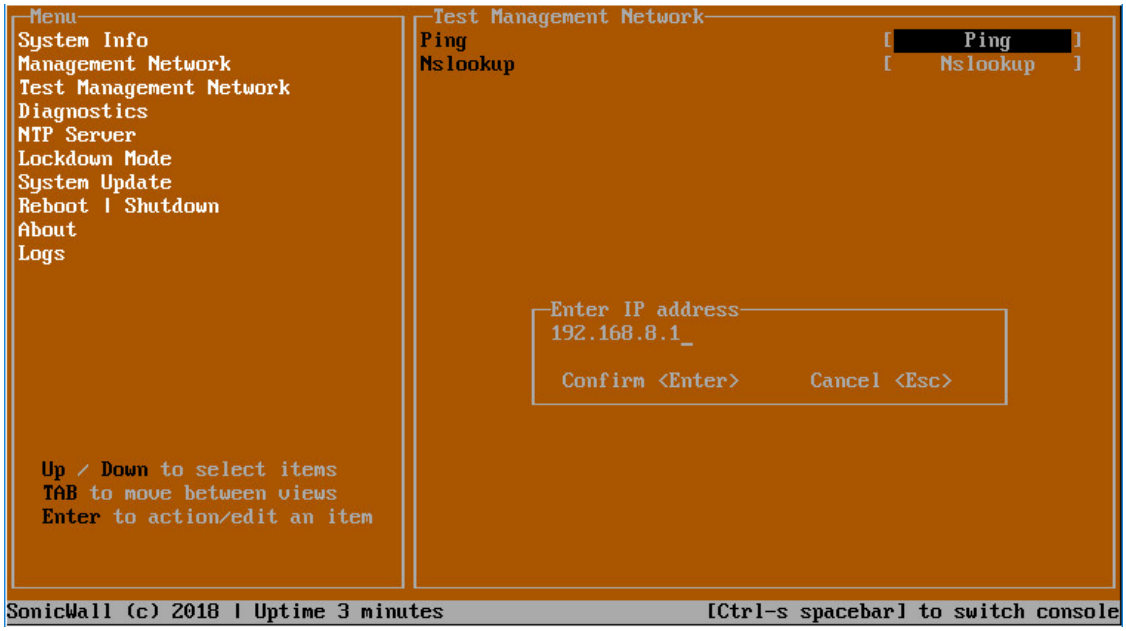
### Network Interfaces screen (Azure)


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 NS*v* appliance.
- **DNS** – This is a list of the DNS servers currently being used by the NS*v* appliance.

# Test Management Network

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

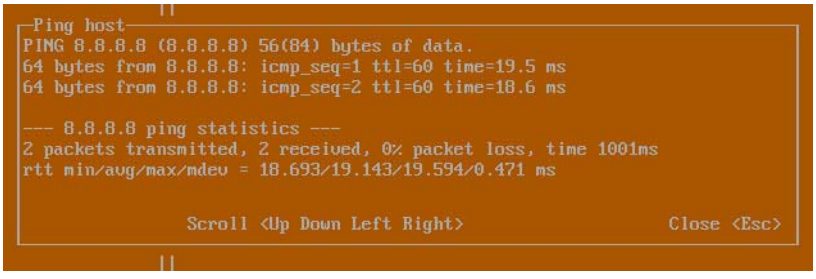



The **Test Management Network** screen provides the **Ping** and **Nslookup** tools to test connectivity between the management interface and the local network. **Ping** is used to test whether hosts in the network are reachable. **Nslookup** is available for sending DNS queries from the NSv appliance.

### *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.

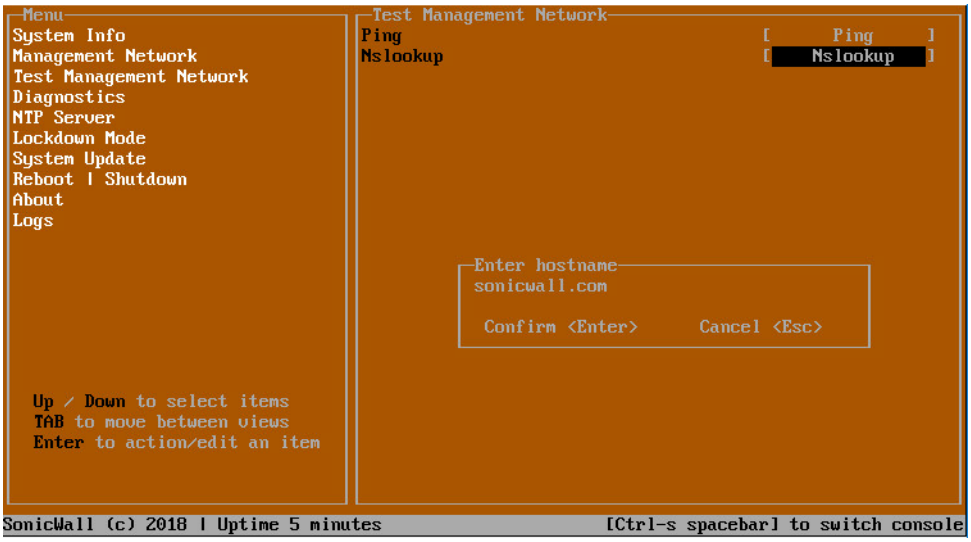



5. Press the **Esc** key to close the dialog.

### *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.



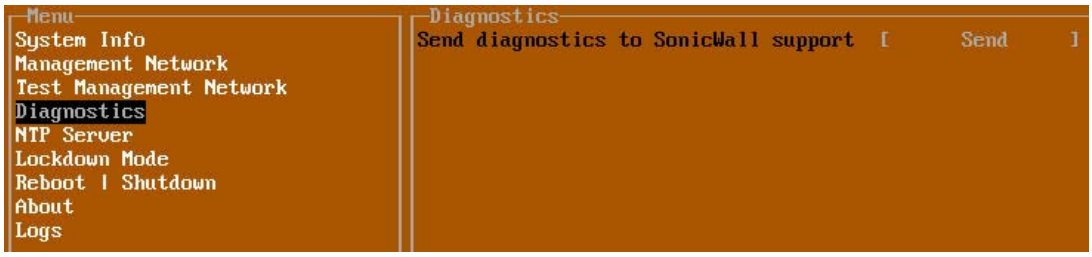

3 Navigate into the dialog, press **Backspace** to clear the current value, and then type in the hostname that you want to look up with a DNS query.

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.


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

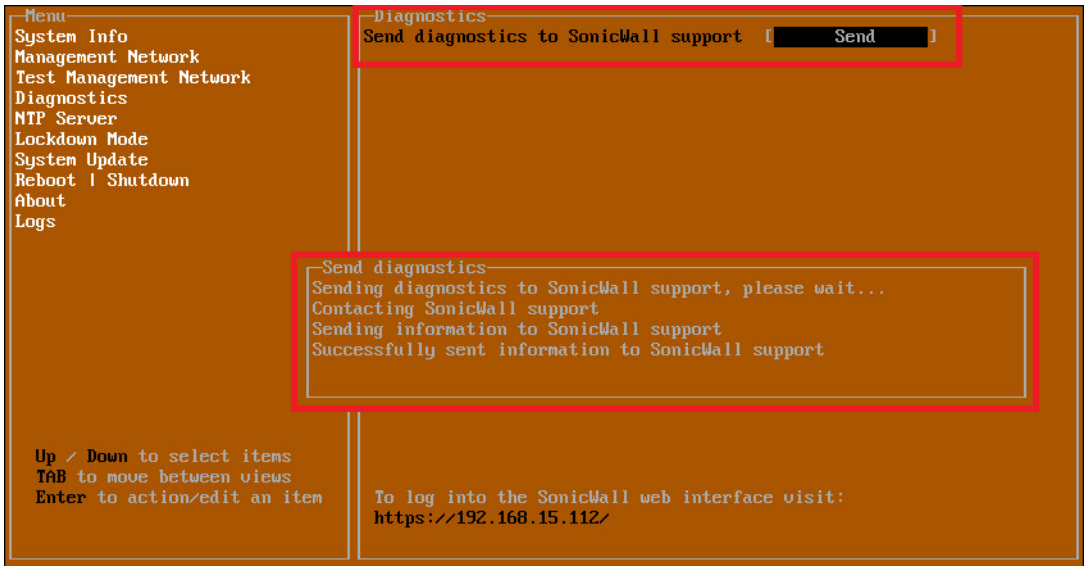
# Diagnostics




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.

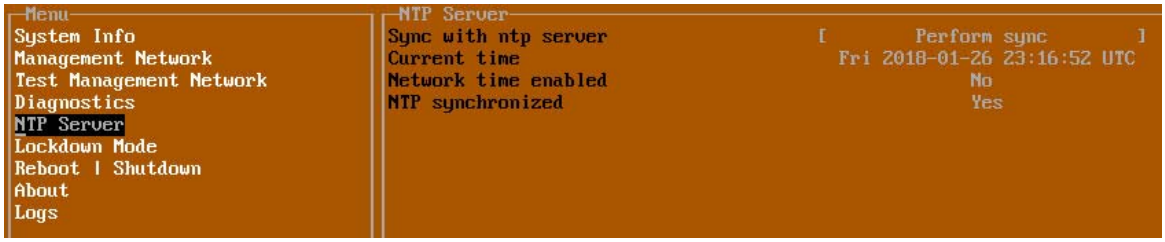
Any errors during the Send process are displayed in the **Send diagnostics** dialog box.

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




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

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

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

- **Network time enabled** – A Yes/No value determining whether the NTP client is currently configured to keep in sync with an NTP server.
- **NTP synchronized** – A Yes/No value determining if the NS*v* appliance is currently synchronized with the configured NTP server(s).

# Lockdown Mode


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

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

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

# Temporary Lockdown Mode

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

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

# System Update

The **System Update** screen is available on NS*v* in Azure.


# Reboot | Shutdown


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

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

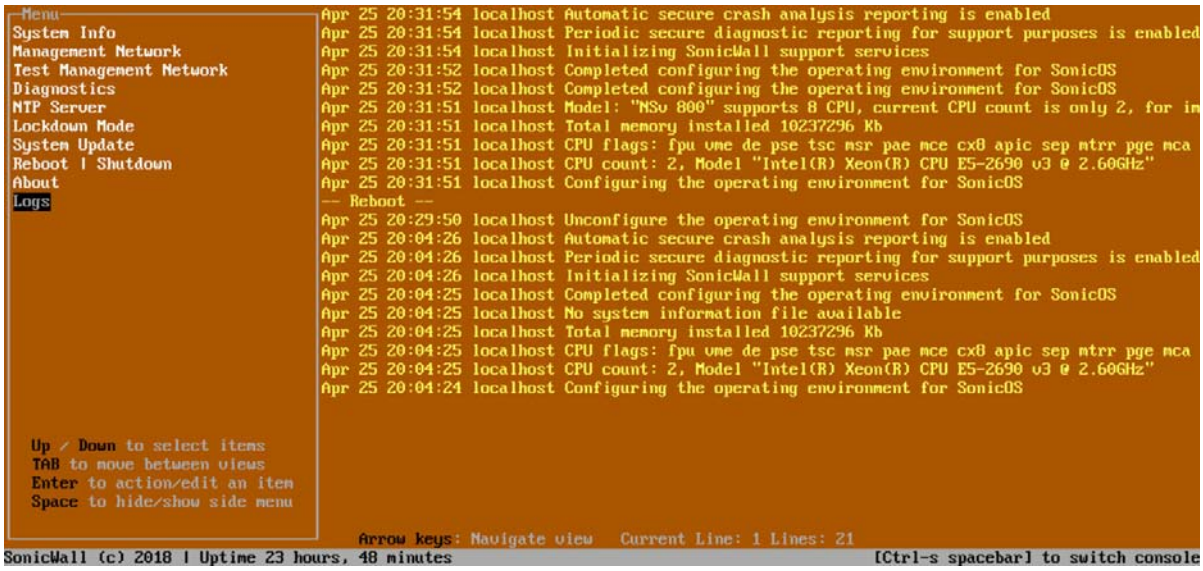
- **Reboot SonicWall** – Restarts the NS*v* Series virtual appliance with current configuration settings.
- **Shutdown SonicWall** – Powers off the NS*v* Series virtual appliance.
- **Boot with factory default settings** – Restarts the NS*v* Series virtual appliance using factory default settings. All configuration settings will be erased.
- **Boot SonicWall into debug** – Restarts the NS*v* Series virtual appliance into debug mode. Normally this operation is performed under the guidance of SonicWall Technical Support.
- **Boot SonicWall into safemode** – Puts the NS*v* Series virtual appliance into SafeMode. For more information, see Using SafeMode on the NSv on page 65.

# About


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

# Logs

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




# Using SafeMode on the NS*v*

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

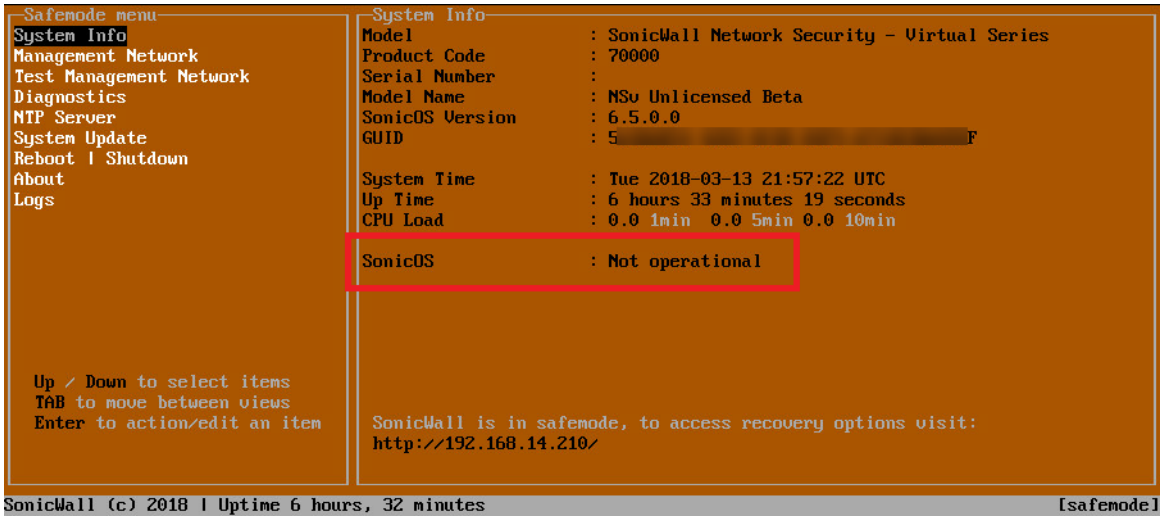
In SafeMode, some of the features the management console provides are different in the following ways:

- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

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

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

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




**NOTE:** To exit SafeMode, disable it on the **Reboot | Shutdown** screen or deploy a new firmware image. See Disabling SafeMode on page 67 and Installing a New SonicOS Version in SafeMode on page 71 for more information.

**Topics:**



# Enabling SafeMode

SafeMode can be enabled from the management console.

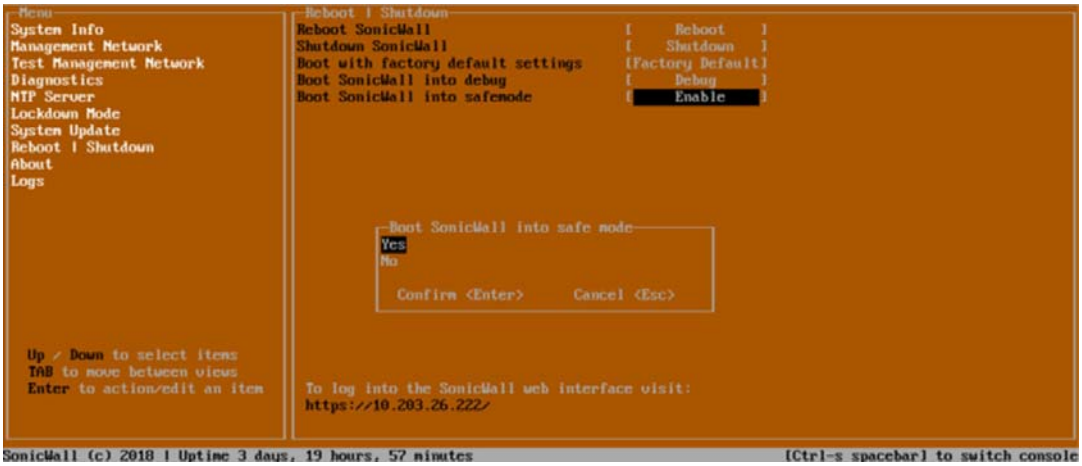
***To enable SafeMode:***

1 Access the NS*v* management console as described in one of:

- For NS*v* on Azure, see: Connecting to the Console with SSH on page 54

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

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




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

5 Press **Enter**.

The NS*v* immediately reboots and comes back up in SafeMode.

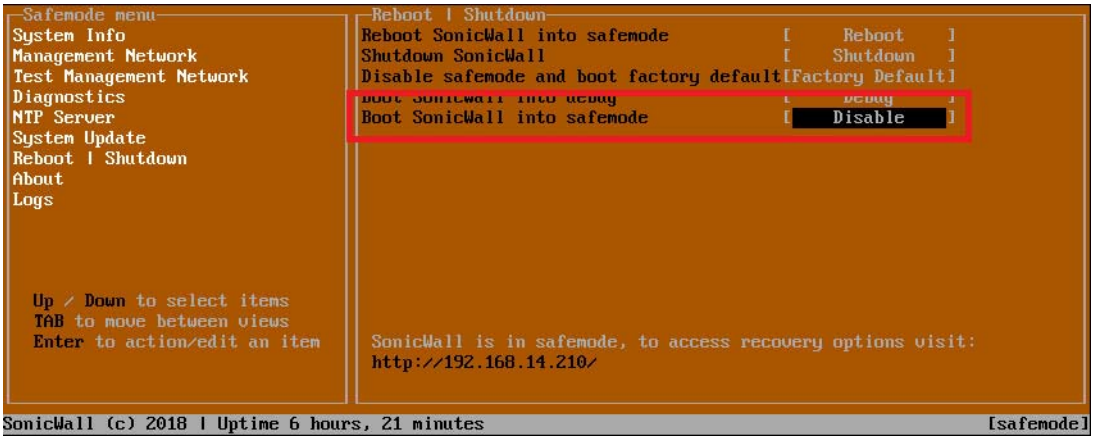
**NOTE:** In SafeMode, the web interface is served from an HTTP server. The HTTPS server is not started in SafeMode.

# Disabling SafeMode

***To disable SafeMode:***

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

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




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

4 Press **Enter**.

The NS*v* immediately reboots and boots up in normal mode.

# Configuring the Management Network in SafeMode

When the Management Console is in SafeMode, the **Management Network** screen in the NSv management console 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.

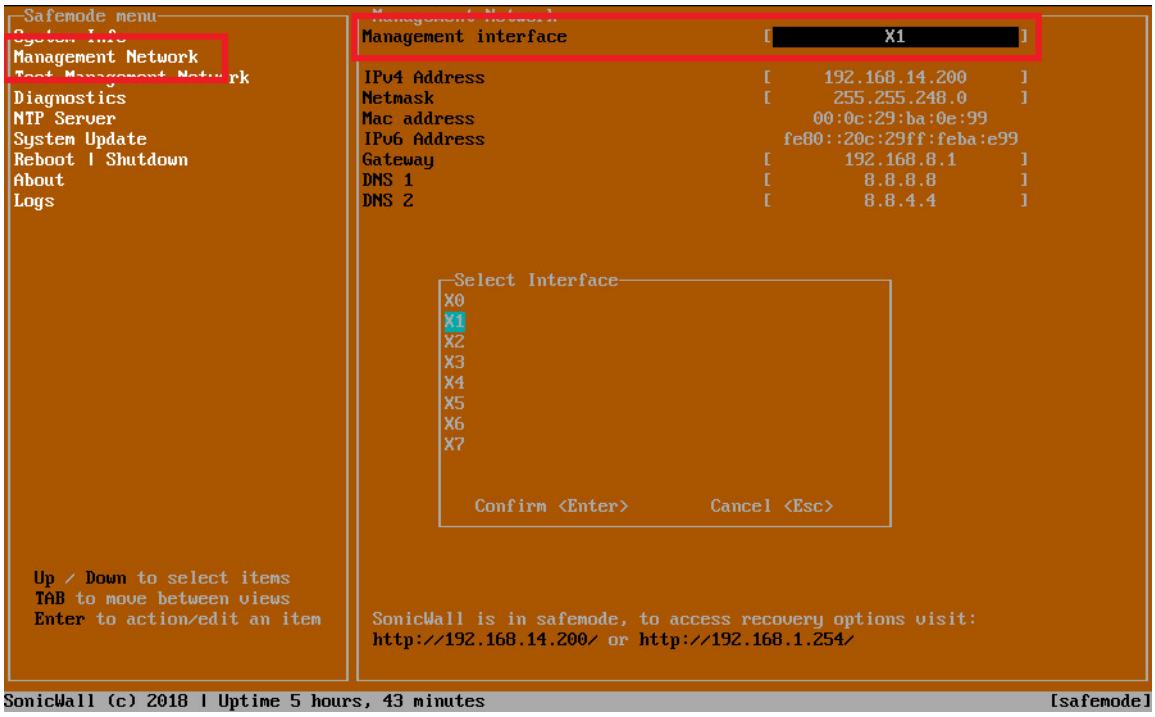
**NOTE:** Changes made to interfaces in SafeMode are ***not*** persistent between reboots.

**Topics:**



## Configuring Interface Settings

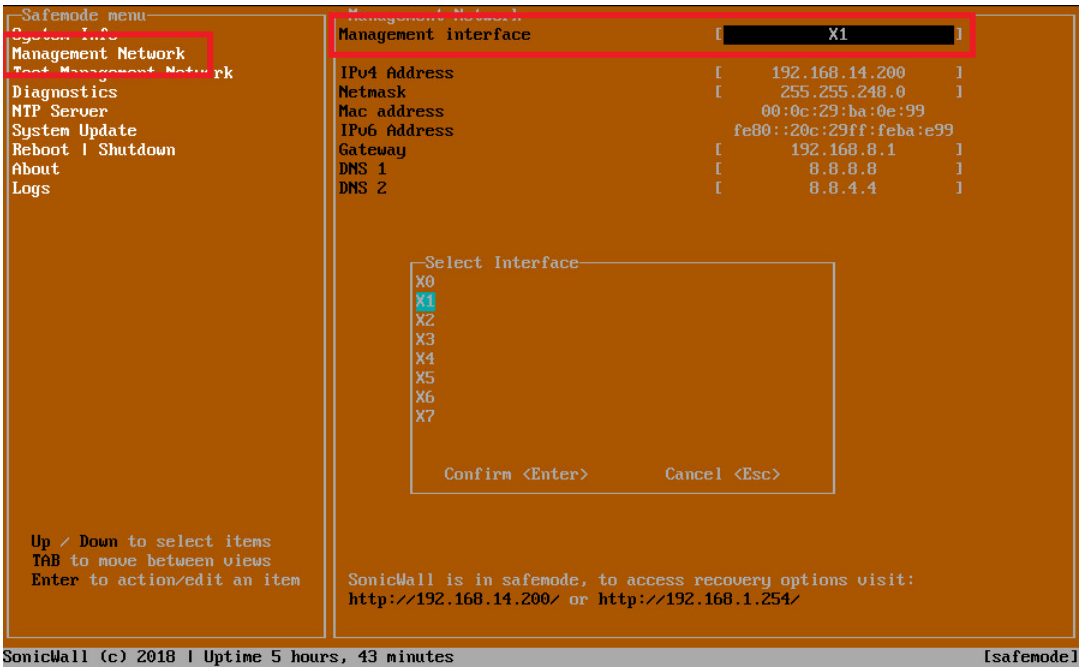
In SafeMode, the **Management Network** screen includes editable and actionable items which are read-only when the management console is in normal mode.



*To edit an interface:*

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

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




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

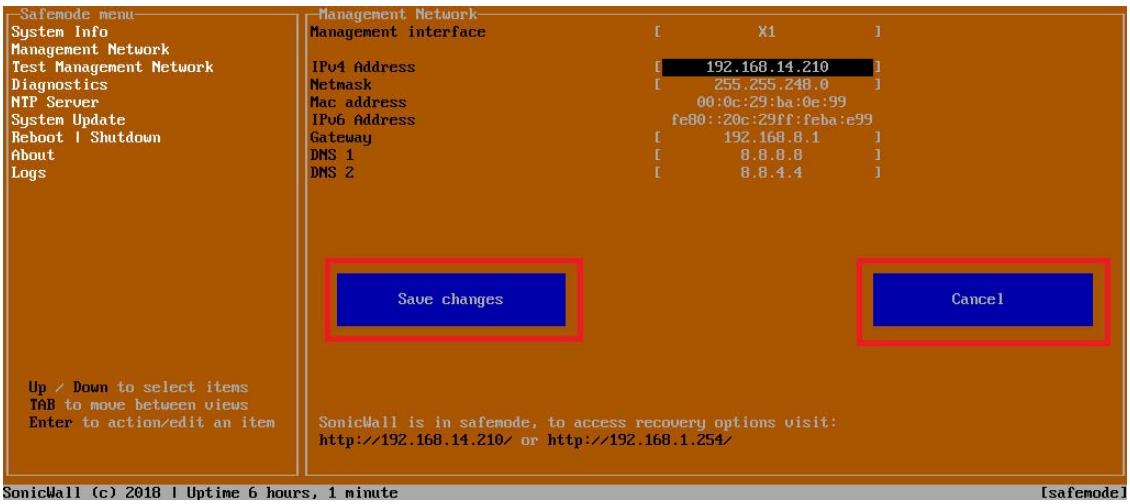
The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

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

The on-screen dialog displays the current IP address.

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

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



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

Do one of the following:

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

# Disabling an Interface

You can disable an interface while in SafeMode.

***To disable an interface:***

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

2 Press **Enter**.

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

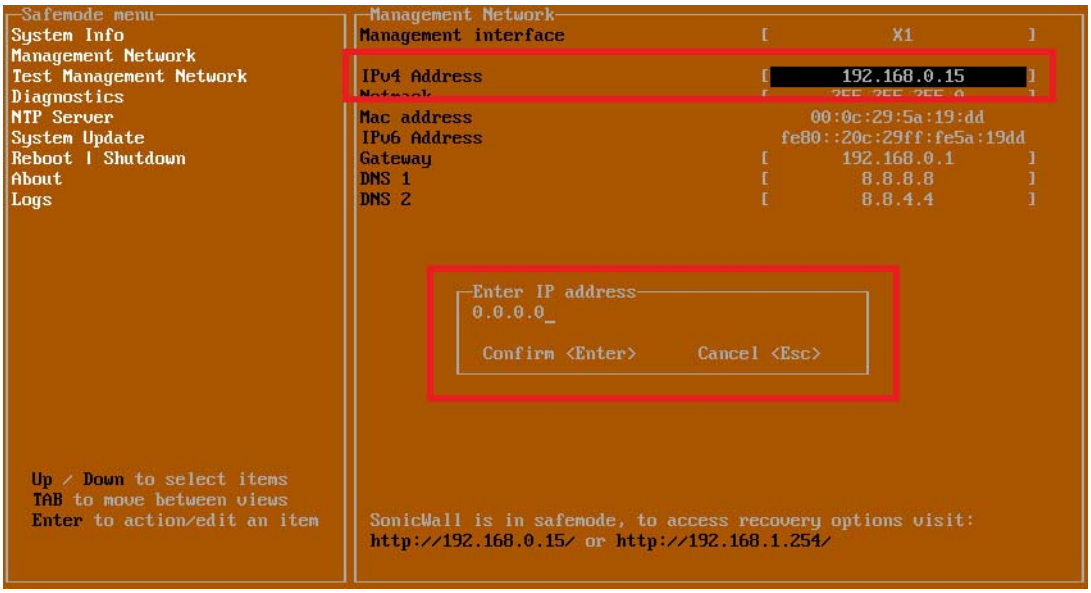
3 Select the interface you wish to edit and press **Enter**.

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.

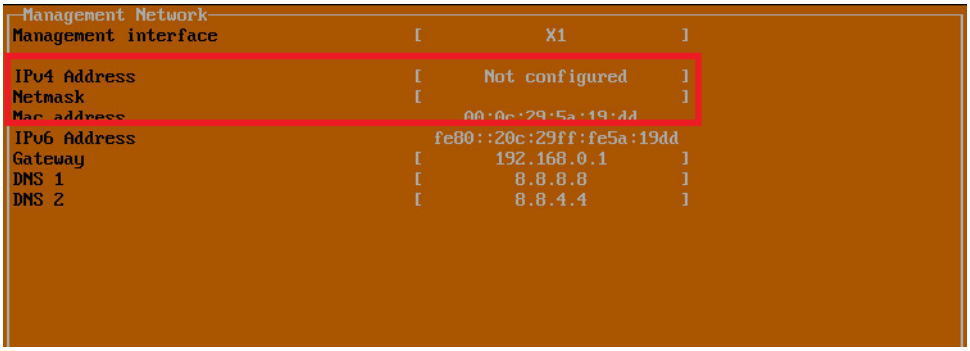
5 Navigate into the dialog and change the IP address to **0.0.0.0**, then press **Enter**.




The **Save changes** button is displayed.

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

The interface is disabled.




# 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 NS*v* appliance. The SafeMode web management interface is used to perform an upgrade, rather than SafeMode in the NS*v* management console. When viewing the NS*v* management console in SafeMode, the URL for the SafeMode web interface is displayed at the bottom of the screen.

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

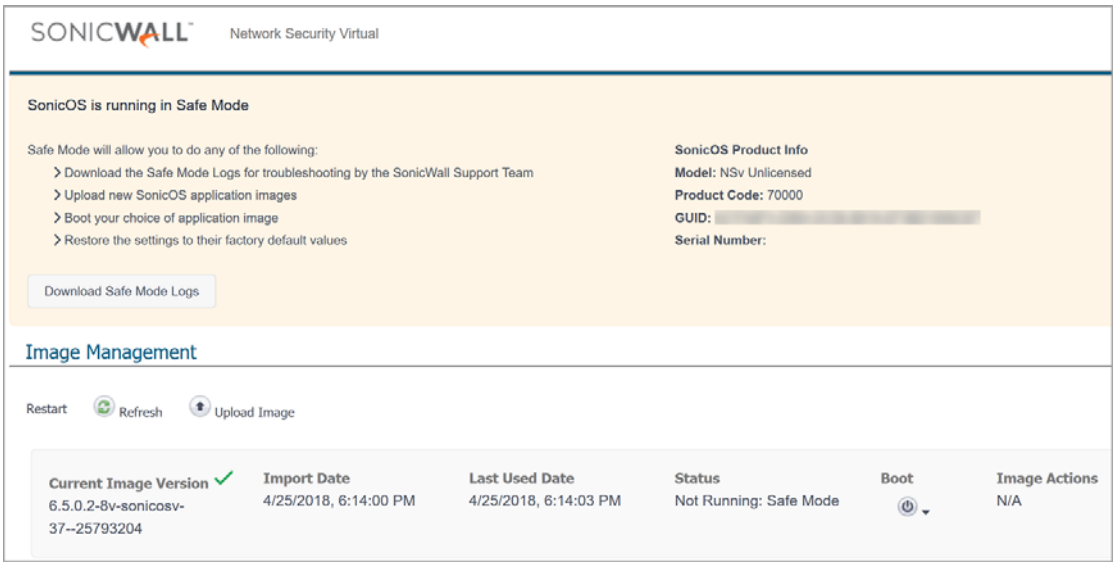
**NOTE:** In SafeMode, the web management interface is only available via **http** (not **https**).

***To install a new SonicOS from SafeMode:***

1 Depending on the type of NS*v* deployment, determine the IP address to use to access the SafeMode web management interface:

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

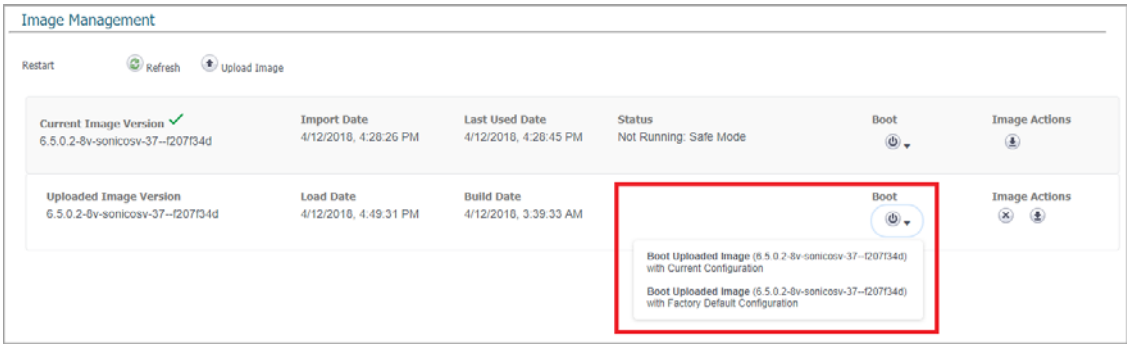
2 In a browser, navigate to **http://*<IP address>***, using the applicable IP address. The SafeMode web management interface displays.




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 NS*v* appliance reboots with the new image.

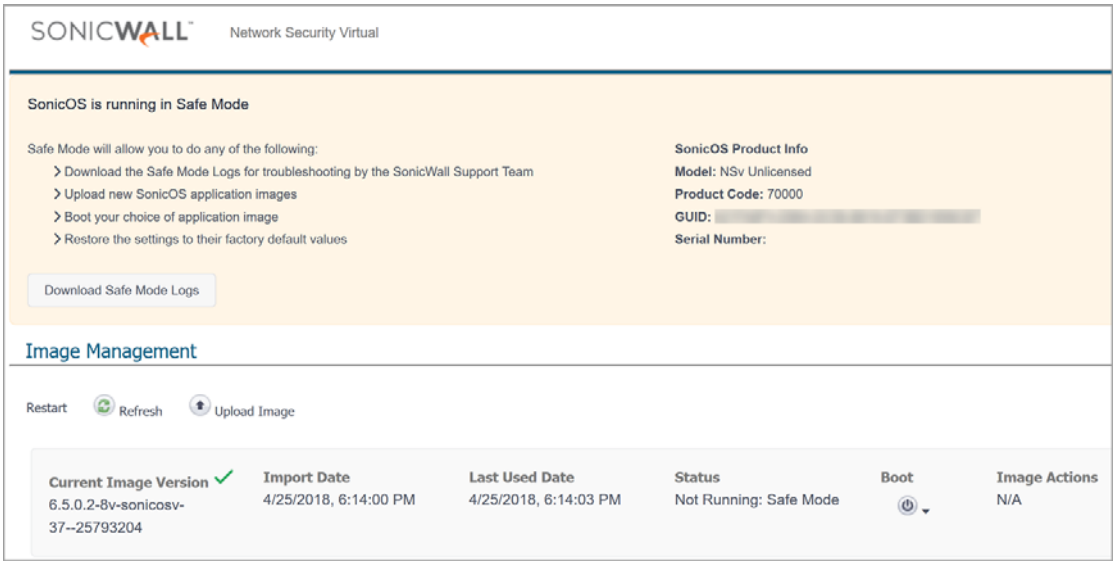
# Downloading Logs in SafeMode

When the NS*v* 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 public IP address of an NS*v* on Azure.

**NOTE:** In SafeMode, the web management interface is only available via **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.




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

6

# Glossary: Azure Networking

Azure takes a different approach to networking when compared to classic networking infrastructure.

**VNet**

A virtual network in Azure is more comparable to a VRF (virtual route-forwarding instance) then to a Vlan. A Vnet is defined over an *Address Space*. All networks within a VNet need to be sub-networks of this Address Space. VNets within same location or different location must not have overlapping Address Spaces. The Address Space has to be defined within RFC1918 space. A VNet contains one or multiple Subnets that are more alike to Vlans on a switch. The VNet routes between all Subnets within the same VNet by default. All Subnets have NATed outbound access to the Internet. If a Public IP has been defined for an interface, all attached hosts have automatic inbound access from the Internet, regardless in which Subnet they are. VNets among each other are connected via VNet-to-VNet VPN, Site-to-Site IPsec VPN, or VNet peering, all of which is being charged and metered.

**UDR**

A *User-Defined Route (UDR)* is a routing table that can be attached to a Subnet. Its purpose is to overwrite the default behavior of the VNet. One of the most common uses is to overwrite the default route out to a virtual public network, instead, to a gateway like a router or firewall (virtual) appliance.

**NSG**

A *Network Security Group* is a collection of simple stateful access-control socket rules. UDRs can be applied to a Subnet or an Interface. Their main purpose is to secure access to Resources from the Internet and to each other.

**NVA**

A *Network Virtual Appliance* in Azure has the function of a router, VPN gateway, or a firewall. Unlike their nonvirtual cousins, NVAs typically only have two interfaces. Azure encourages the deployment of multiple NVAs in spot solutions, rather than of a large collapsed solution we see in brick-and-mortar datacenters. NVA redundancy is provided by Azure's built-in load-balancing function.

**Express Routes**

*Express Routes* are not routes, but are VPN circuits between datacenters and via partners to on-premises running of private infrastructure, instead of the public Internet. Express Routes are very expensive. Instead an NVA like the Sonicwall NSv is able to pride this service much more cost effectively.

**Network Interfaces**

*Network Interfaces* are virtual NIC (Network Interface Card). Unlike with VMware where virtual NICs appear like real NICs within the guest, and are configured there like real interfaces, in Azure, all addressing happens on the Network Interface, and is learned via DHCP by the guest. Unlike VMware, machine sizes typically support a low number of Network Interfaces, one or two, sometimes four.

Addressing of Network Interfaces is typically dynamic, but can be done static. If left to dynamic, the next available IP address is being allocated. Within each /24 Subnet, the first available address is .4 in the last octet. The first three addresses in each Subnet are reserved by Azure.

Network Interfaces may or may not have public IP addresses attached. Network Interfaces can have secondary IPs configured, which do not have be configured within the guest since Azure attaches the same MAC from the primary to its secondaries.

**Public IP**

A *Public IP* is typically a routable but randomly assigned public IP address that is attached to a Network Interface or a Load-balancer resource. Public IP re-address each time when a virtual machine is allocated, unless set to static. When a virtual machine is stopped, from within Azure in order to stop machine billing, the Public IP is being lost. Public IPs can enter DNS hostnames so that references stay the same after restart of the machine. Both primary and secondary IPs within a Network Interface can have Public IPs attached.

We are going to discuss two design choices for implementing a NVA in the next chapter. From a general design perspective, special about Azure is:

- A NVA (firewall) is placed within a VNet, not in-between VNets
- All Subnets within a VNet have access to each other. All hosts have automatic access to the Internet. In order to force traffic through the firewall, a UDR has to be configured and attached to the LAN side Subnet.
- A NVA has typically only two interfaces
- Public IPs from Network Interfaces of machines on the LAN side have to be moved.
- NSGs are configured by default and would need to be loosened, or removed, when access should be controlled by the firewall. NSGs are important to limit public access to the firewall's management interface.

7

# 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 Azure Getting Started Guide*
Updated - December 2020
Software Version - 6.5.4
232-004957-00 Rev E