SonicWall® NS_v Series on AWS

Getting Started Guide

(BYOL / PAYG)

SONICWALL®

Contents

1

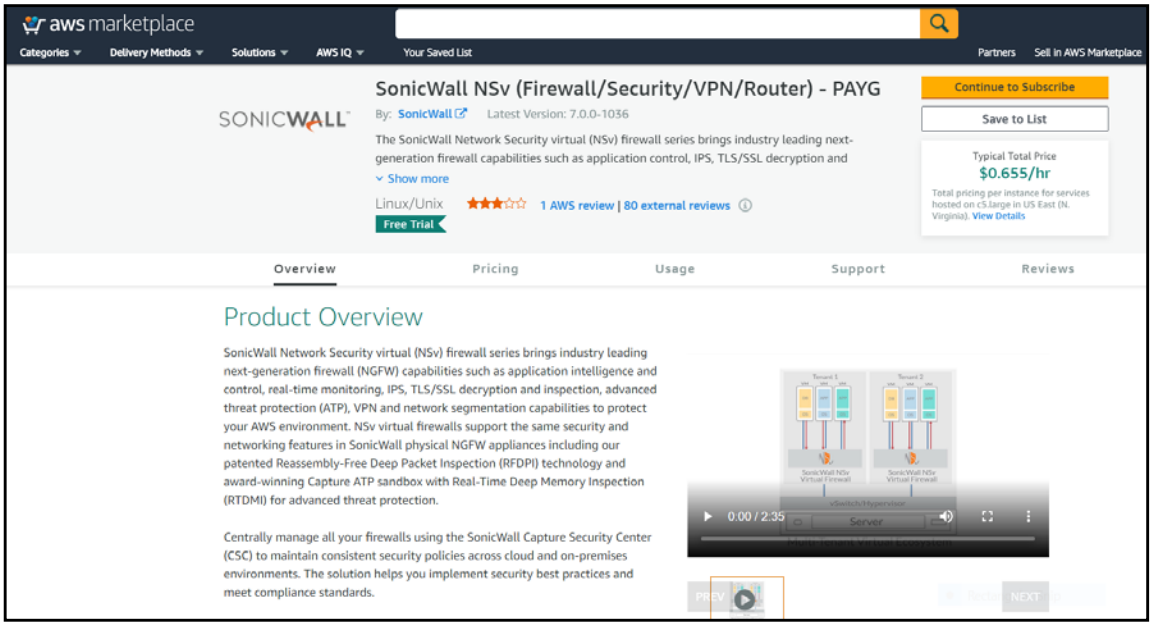
Introducing the NS$_v$ Series

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

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

IMPORTANT: You may choose to operate NS*v* on a "pay-as-you-go" basis (PAYG) or on a fixed fee per period basis — "bring your own license" (BYOL). This choice is made as you initiate subscription in the AWS Marketplace. Regardless of the pricing model choice, you can go to Installing NSv Series on AWS to start. Separate instructions for different pricing models are given in Deployment Options.

SonicWall NS*v* on AWS Marketplace



The SonicWall® Network Security Virtual Series (SonicWall® NS*v* Series) is SonicWall's virtualized next-generation firewall appliance that provides Deep Packet Inspection (DPI) security and segmentation in virtual environments. SonicOS running on the NS*v* 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* has nearly all the features and functionality of a SonicWall hardware appliance running SonicOS 6.5.4 firmware.

SonicWall Global Management System (GMS) 8.4 and higher versions are supported for management of SonicWall NS*v* series virtual appliances.

For information about supported features, refer to the *SonicOS 6.5 NSv Series* administration documentation. The *SonicOS 6.5 NSv Series About SonicOS* book contains the list of features not supported on NSv. This and other documents for the SonicWall NS*v* Series are available by selecting **NS*v*** Series as the **Product** at: https://www.sonicwall.com/support/technical-documentation.

NOTE: The AWS VPC does not support Layer 2 functionality. Therefore, the NS*v* interface to VPCs is restricted to the layer 3 network level and above. Consequently, DHCP services and VLAN interfaces are not supported on NS*v* appliances running in AWS.

The Key Feature Support of NSv for AWS table lists the key SonicOS features and whether they are supported or unsupported on deployments of the NSv for AWS.

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	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

Feature Support List

Component	Feature	Status
Anti-spam		Not supported
3G/4G Modem		Not supported
Wireless		Not supported
SonicPoints		Not supported
Virtual Assist		Not supported
High Availability	Active/Passive	Not supported
High Availability	Stateful Sync	Not supported
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

Node Counts Per Platform

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

Maximum Node Counts Per Platform

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

Node counts are calculated by SonicOS as follows:

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

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

Product Matrix and Requirements

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

Product Models	NSv 10	NSv 25	NSv 50	NSv 100	NSv 200	NSv 400	NSv 800	NSv 1600
Maximum Cores[1]	2	2	2	2	2	4	8	16
Minimum Total Cores	2	2	2	9	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 the number of cores defined in the above table, extra cores will be used as CPs. Multiple CP support is introduced in 6.5.4.v.

Github Repository

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

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

Backup and Recovery Information

In certain situations, it might be necessary to contact SonicWall , use SafeMode, or de-activate the NS*v* appliance:

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Please contact SonicWall for assistance.
- If the disk is not recoverable, then the NS*v* appliance needs to be de-activated. See De-activating Your NSv on page 39 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 the Management Console in SafeMode.
- 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 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

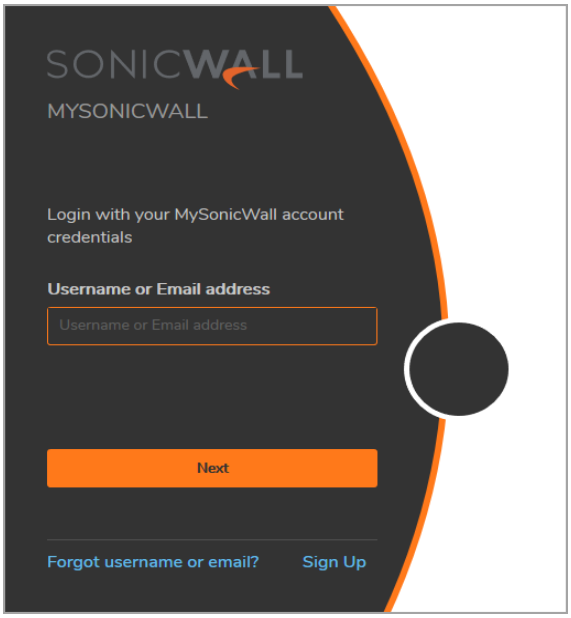
A MySonicWall account is required to obtain the image file for initial installation of the NS*v* Series virtual firewall, for product registration to enable full functionality of SonicOS features, and for access to licensed security services. For a High Availability configuration, MySonicWall provides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

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

To create a MySonicWall account:

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

2 In the login screen, click the **SIGN UP** link.



3 Complete the account information, including email and password.

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

4 Enable two-factor authentication if desired.

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

- **Email (one-time passcode)** where an email with a one-time passcode is sent each time you log into your MySonicWall account.
- **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code. Once 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 AWS on page 10
- Deployment Options on page 34.

2

Installing NS$_v$ Series on AWS

Topics:

Supported NS$_v$ Series Models on AWS

Determine the NS*v* instance type you will require before starting installation.

NS*v* Models (Instance Sizes) on AWS

SonicWall NS*v* Model	AWS EC2 Instance			
	Type	CPU Cores	Memory Gigabytes	Max Network Interfaces[1]
NS*v* 10	c5.large	2	4.0	3
NS*v* 25	c5.large	2	4.0	3
NS*v* 50	c5.large	2	4.0	3
NS*v* 100	c5.large	2	4.0	3
NS*v* 200	c5.large	2	6.0	3
NS*v* 400	c5.xlarge	4	8.0	4
NS*v* 800	c5.2xlarge	8	16.0	4
NS*v* 1600	c5.4xlarge	16	32.0	8

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

NOTE: The maximum number of NICs supported by SonicWall NS*v* is always eight for all models. But the total number of interfaces in an AWS instance maybe constrained by the AWS VM.

Task List for NS$_v$ Series AWS Instance Setup

1 Deploy a new VPC with NS*v* from the AWS Console

- Deploying NSv from Console on page 11
- Change Routing Tables for NSv Access on page 25

OR:

1 Deploy NS*v* to an existing VPC with AWS Cloud Formation Templates

- Deploying AWS from Cloud Template on page 20
- Change Routing Tables for NSv Access on page 25

THEN:

2 Register the NS*v* on MySonicWall

- Creating a MySonicWall Account on page 41

Deploying NS$_v$ from Console

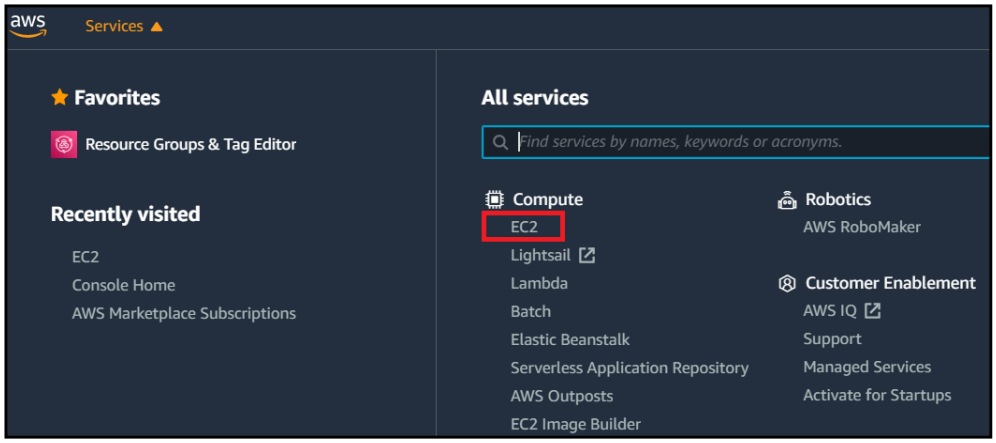
To deploy NSv from the AWS console, follow these steps:

1 Log into the AWS Console.

a Go to the AWS management console at https://aws.amazon.com.

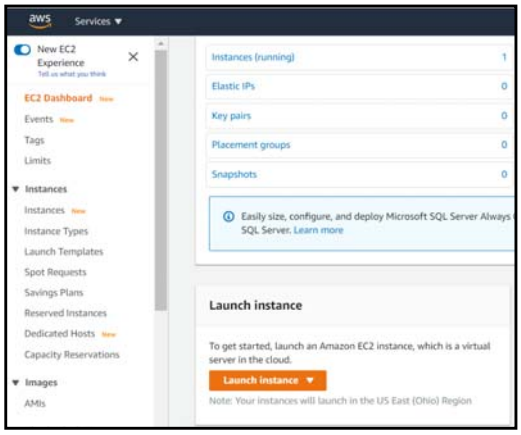
b Log into the AWS management console.

c From the Services menu select **EC2**.

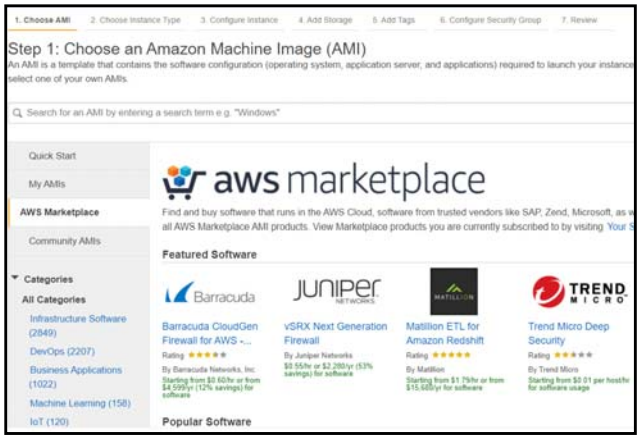


2 Follow these steps to launch the SonicWall NSv:

a From the EC2 Dashboard, select **Launch Instance**.

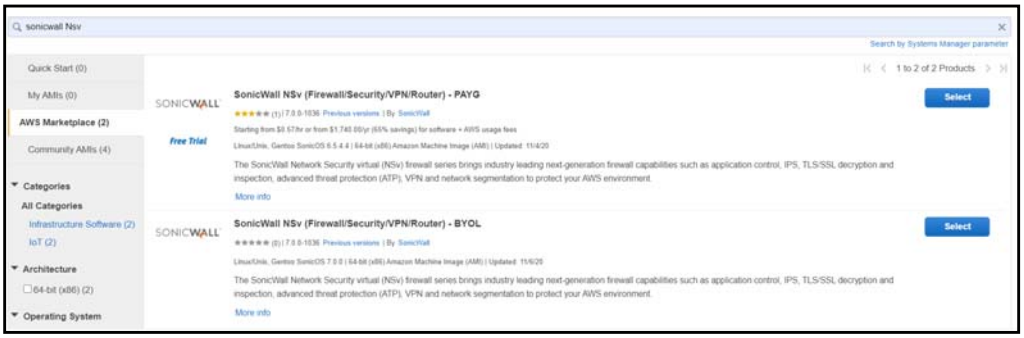


b From the left panel menu, click **AWS Marketplace** and enter **SonicWall NSv** into the search box.

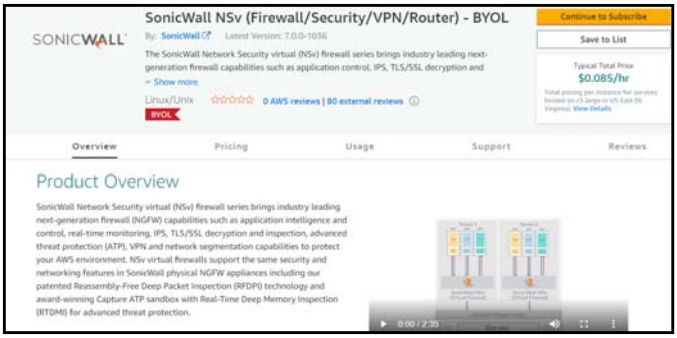


c Click the **Select** button next to the **SonicWall NSv (Firewall/Security/VPN/Router)**.

NOTE: This procedure applies to both BYOL and PAYG installations. You may choose to operate NSv on a "pay-as-you-go" basis (PAYG) or on a fixed fee per period basis — "bring your own license" (BYOL). This choice is made as you initiate subscription in the AWS Marketplace.

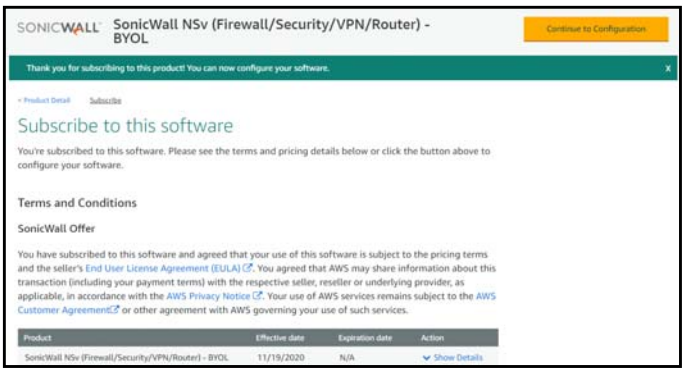


d Based on your selection, the product details screen is displayed. For reference, BYOL option is selected.



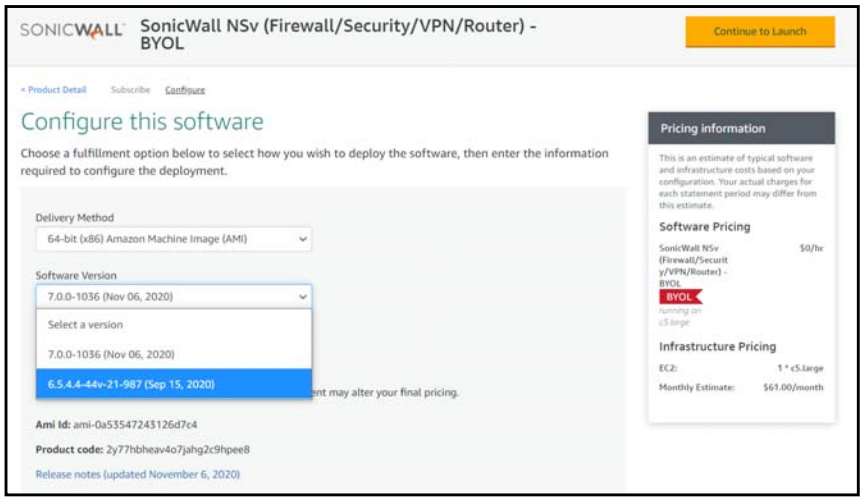
e Click **Continue to Subscribe** and accept the terms and conditions.

f On the next screen, click **Continue to Configuration**.



g On the next screen, select the following based on your requirements:

- Delivery Method
- Software Version
- Region



h Once you have made the selection, click **Continue to Launch**.

i In the Launch screen, select **Launch through EC2** option from the **Choose Action** drop-down and click **Launch**.

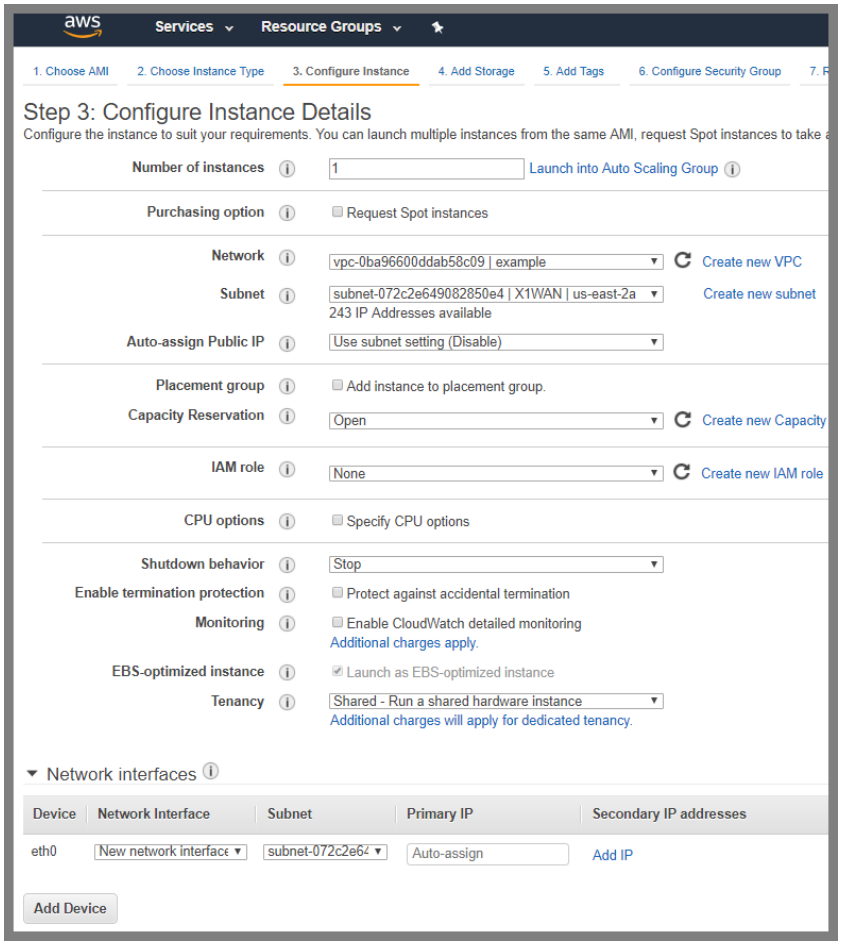
j Select the **Instance Type** corresponding to the SonicWall NSv model you require.

For guidance, refer to Node Counts Per Platform on page 6 and Supported NSv Series Models on AWS on page 10. Choose instance size from the table displayed:

NSv Models and AWS Image Types

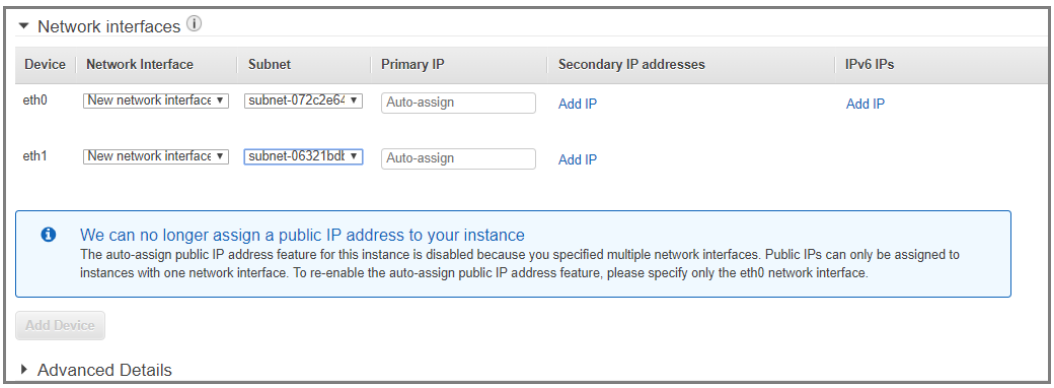
SonicWall NSv Model	AWS EC2 Instance Type
NSv 10	c5.large
NSv 25	c5.large
NSv 50	c5.large
NSv 100	c5.large
NSv 200	c5.large
NSv 400	c5.xlarge
NSv 800	c5.2xlarge
NSv 1600	c5.4xlarge

k Click on **Configure Instance Details**. From the **Network** drop down select a VPC to deploy the firewall on. Select the subnet which is to be the public or WAN interface (X1) of the firewall.



l To add additional Elastic Network Interfaces click **Add Device**. The firewall MUST at minimum have 2 ENI attached. The ENI interfaces MUST be on separate subnets. The eth0 ENI device will be connected to the SonicWall NSv X1 interface that is the public interface. The eth1 ENI device will be connected to the SonicWall NSv X0 interface that is the private interface.

NOTE: If you get a response from the system offering only two interfaces with the same subnet, check all subnets in the VPC with the VPC availability board to ensure that they are in the same availability zone.



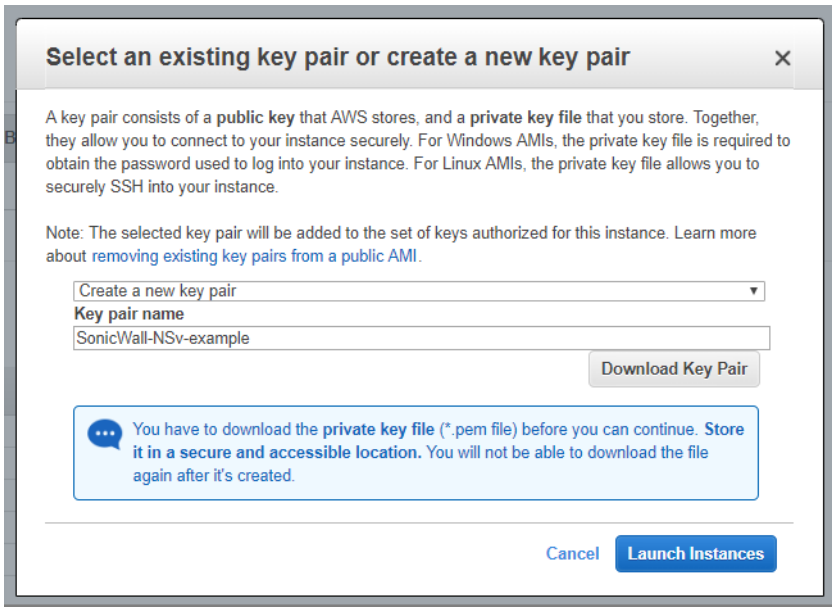
m Accept the default storage options by clicking the **Add Storage** button.

n Click the **Add tags** button. Add metadata to the instance configuration to assist in identifying the SonicWall NS*v* instance.

o Click the: **Configure Security Group** button. At minimum, allow SSH and HTTPS from a predefined source.

p Click the **Review** and **Launch** buttons. Review the instance details.

q You will be prompted to select either **Key-Pair** or **Create a new key pair**. Ensure you have access to the key pair.



r Click the **Launch Instances** button to deploy the SonicWall NS*v* instance. Deployment will take between 5 to 8 minutes. You can monitor the progress by viewing the instance in the EC2 Dashboard.

3 Disable source/destination checking:

a Select **Network Interfaces** from the left menu of the EC2 Dashboard.

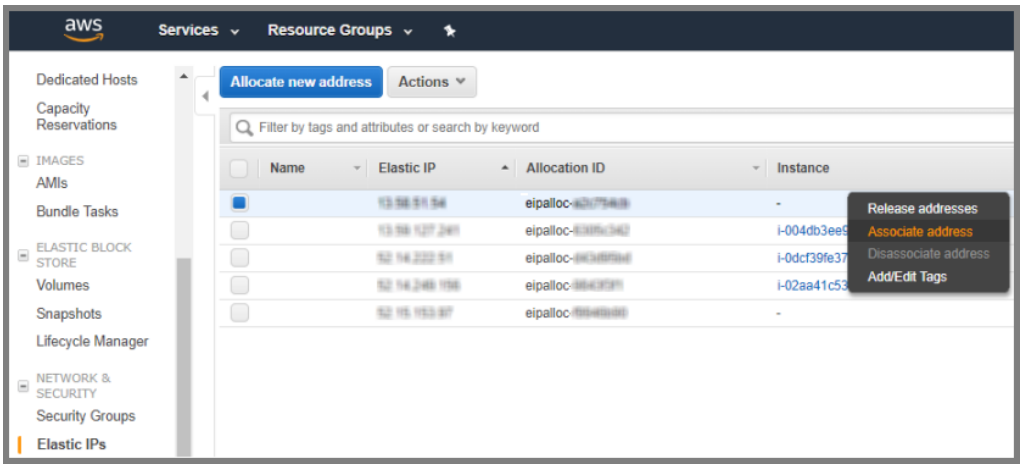
b For each network interface connected to the new SonicWall NS*v* instance, disable the source and destination check.
To do this, right click on the network interface and select **Change Source/Dest Check**.

c Select the **Disabled** checkbox and press **Save**.

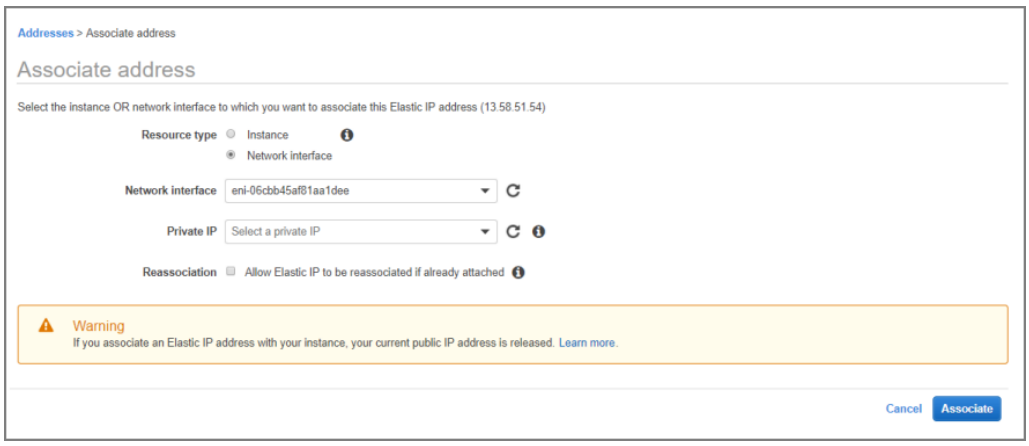
4 To assign an Elastic IP, follow these steps:

a From the EC2 Dashboard left hand menu select **Elastic IPs**.

b Right click on a free Elastic IP and select **Associate**. If no Elastic IPs are available, then click on **Allocate new address**.



c Choose the **Resource type** and **Network Interface**. In the **Network Interface** drop down choose the first ENI (eth0) connected to the SonicWall NSv Instance. That is the ENI connected to the public subnet. Refer to **Instance** details page to help identify the ENI.



d Click **Associate**. This IP address can now be used to connect to the SonicWall NS*v* web management interface.

5 Connect to the firewall web management interface:

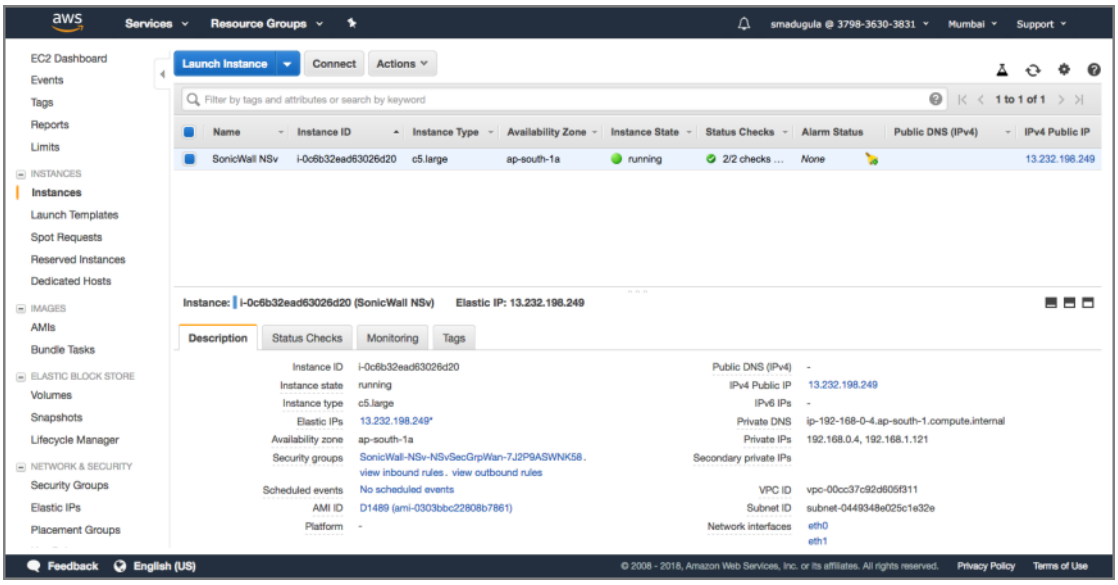
a Now that you have associated an Elastic IP to the SonicWall NS*v* instance you will be able to connect to the web management interface by entering the IP address into your browser.

b Enter the username "admin" and the password is the AWS instance ID of the newly created SonicWall NSv instance such as i-02axxxxxxxxxxxxx.

Now, connect the NSv with the internet and LAN by setting up routing tables as described in Modify Routing Tables for NSv Access on page 18.

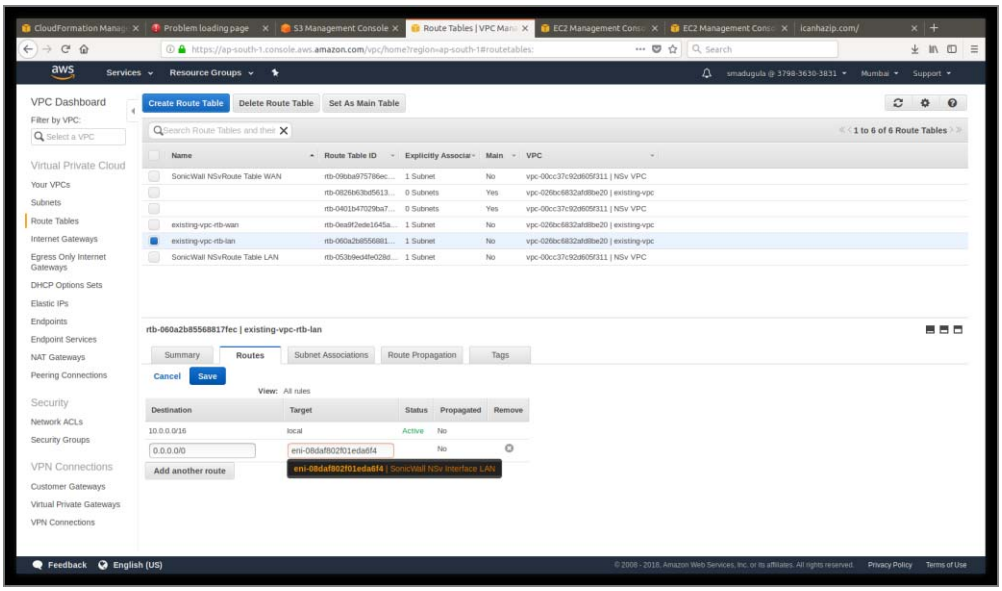
Modify Routing Tables for NS$_v$ Access

1 Wait at EC2 Dashboard for **Instance State — running**, AND **Status checks — 2/2 checks passed**.

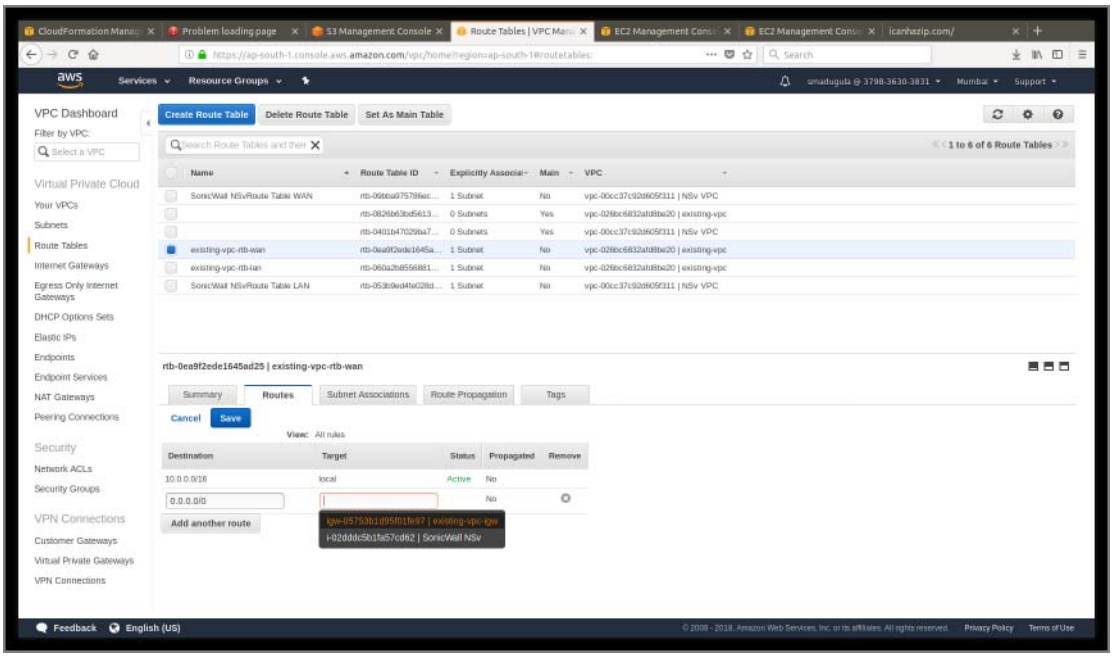


2 Change Routing Tables:

a Change Your LAN routing table to add a route with **Destination** 0.0.0.0/0 with **Target** to NS*v*'s LAN Interface. This routes all your LAN traffic to the NS*v* X0 interface.



b Change your WAN routing table to add a route with **Destination** 0.0.0.0/0 with **Target** to your Internet Gateway (igw-xxxxx). This routes NS*v* WAN traffic to the Internet Gateway (IGW).



3 Your NS*v* should now be operational. Next, register your NS*v*, see: Deployment Options on page 34. The following section details how to set up access to the NSv from the public internet.

Deploying AWS from Cloud Template

This section describes how to deploy NS*v* to an existing VPC using AWS Cloud Formation Templates. This is referred to as a ***Launch Stack*** deployment.

Pre-requisites include:

- AMI ID of NSv
- A key pair
- A VPC with:
    1) Two subnets:
        - WAN subnet.
        - LAN subnet.
    2) Two routing tables (in addition to main routing table - main routing table is automatically created when you created your VPC):
        - WAN routing table (with WAN subnet associated with it).
        - LAN routing table (with LAN subnet associated with it).
    3) An Internet Gateway attached to the VPC.

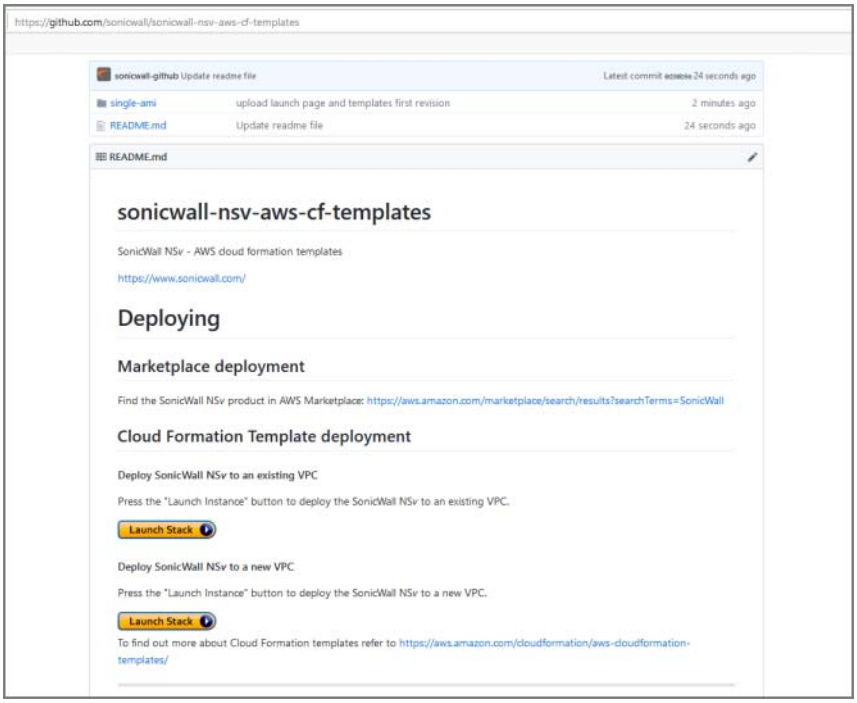
Populate the routing tables after the stack has been deployed successfully.

Steps:

1 Go to:

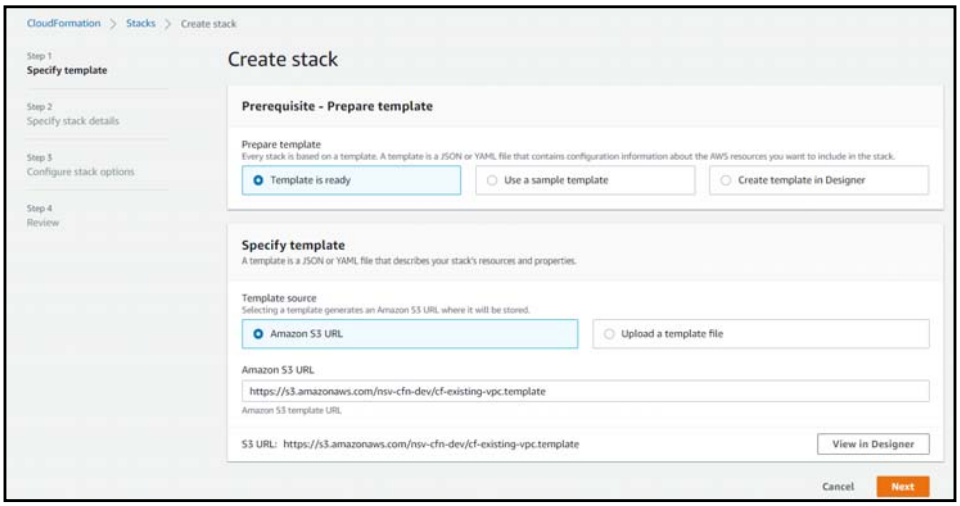
https://github.com/sonicwall/sonicwall-nsv-aws-cf-templates

2 Click the **Launch Stack** button below the **Deploy SonicWall NSv to an existing VPC**.

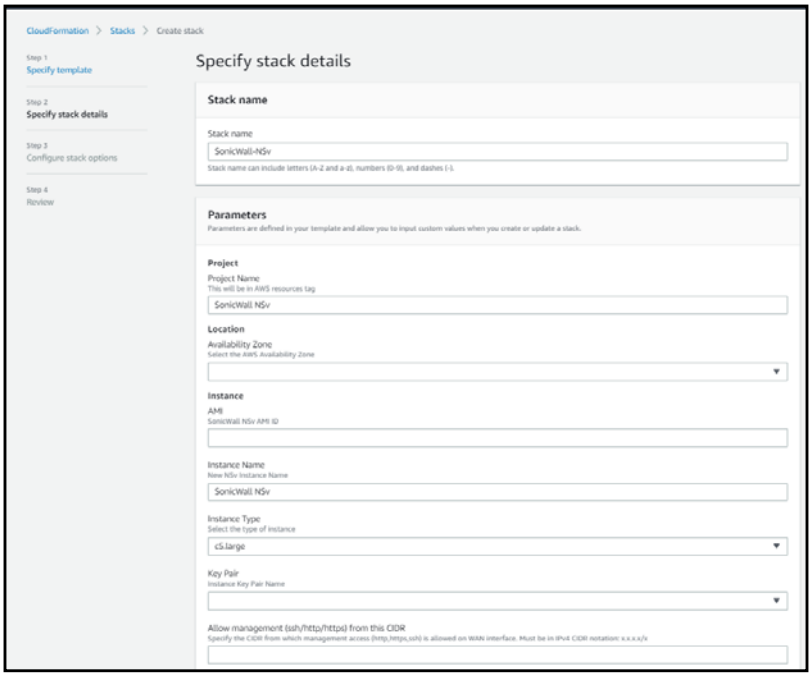


3 To select a Region, identify the region into which you wish to deploy NS*v*. Note: You must copy the AMI to the chosen region and have its ID ready.

4 Click on **Launch Stack** button under **Deploy NSv to an existing VPC**.



5 Click **Next**.



6 Specify **Stack Name**: Name for your stack. The name helps you find a particular stack from a list of stacks.

7 Set the following parameters:

- **Project Name**: A name which will be added to the resources tag.
- **Location**

  Availability Zone: Select the Availability Zone into which NS*v* is launched.
- **Instance**

  AMI: AMI ID of SonicWall NSv.

  Instance Name: A descriptive name for the NSv instance.

  Instance Type: Select the type of the instance from the drop-down menu.

  Key Pair: Select the key pair. This is the key pair available in AWS that can be used to SSH to the SonicWall NSv management console. See:
  https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

  Allow management (ssh/http/https) from this CIDR: Specify the IP address from which management access is allowed on the WAN interface. Must be in IPv4 CIDR notation x.x.x.x/x. Open HTTP, HTTPS, and SSH ports for this address in the Ingress Security Group.

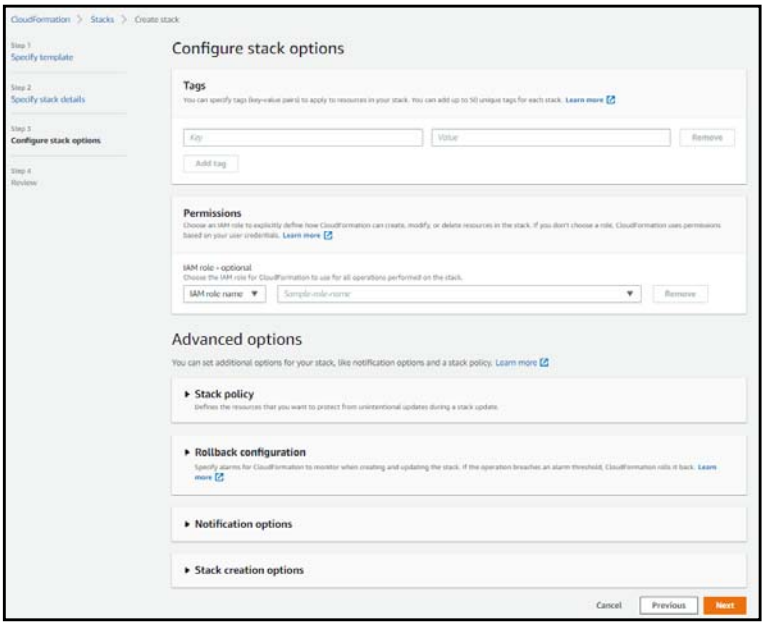
  WAN Interface Subnet ID: Select the subnet id for your WAN interface.

  LAN Interface Subnet ID: Select the subnet id for your LAN interface.

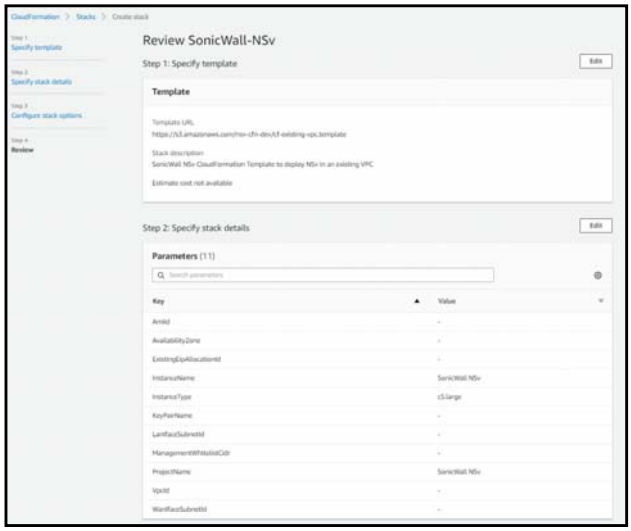
  Optional Existing Elastic IP Address (EIP). You can specify Allocation ID of an existing Elastic IP address. This EIP can connect to the WAN interface of the NS*v*. If this field is left blank, the system allocates a new EIP.
- **VPC**

  VpcId: Select existing VPC to which to deploy NS*v*.

8 Click **Next.**

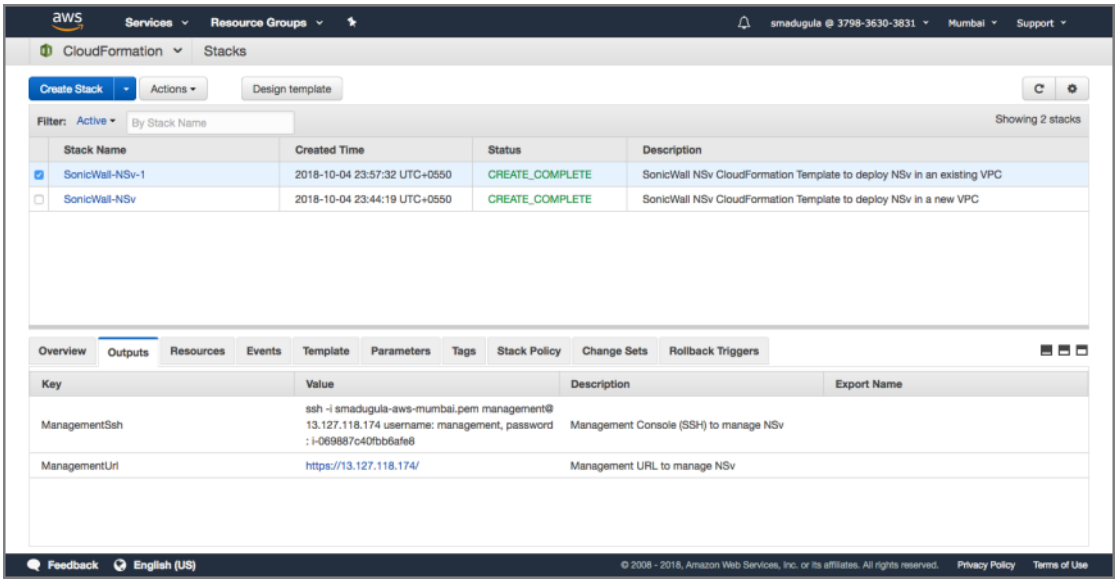

CloudFormation > Stacks > Create stack
Step 1
Specify template
Step 2
Specify stack details
Step 3
Configure stack options
Step 4
Review
Configure stack options
Tags
Key
Value
Remove
Add tag
Permissions
IAM role - optional
IAM role name
Sample-role-name
Remove
Advanced options
Stack policy
Rollback configuration
Notification options
Stack creation options
Cancel
Previous
Next

9 Click **Next**.



10 Review details and click **Create Stack**.

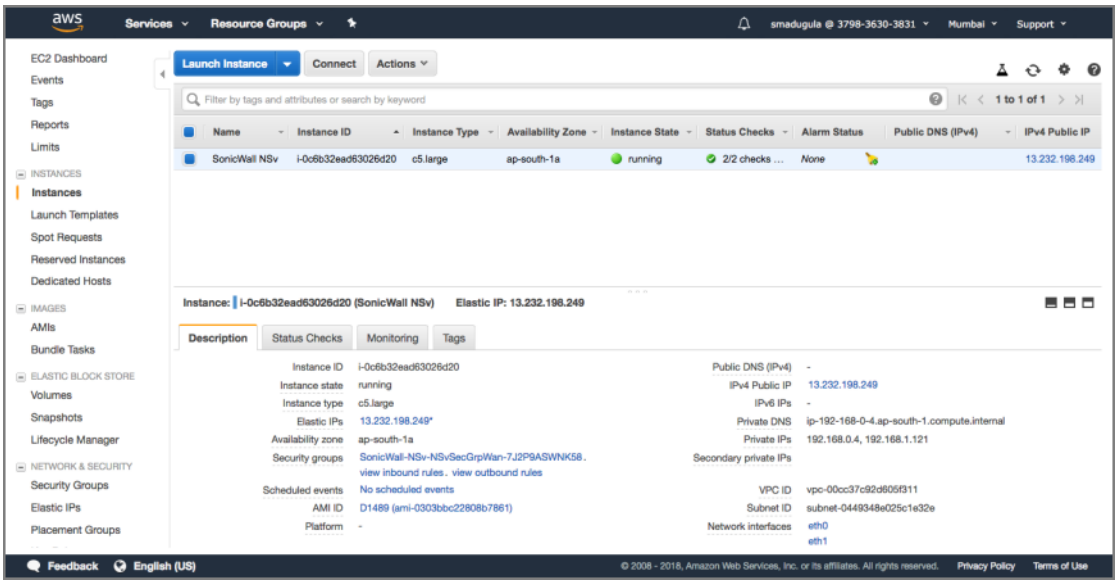
11 Status changes to **CREATE_COMPLETE**.



12 When the stack creation is complete (**Status** changes to **CREATE_COMPLETE**). You can get the management and access details in the **Outputs** section.

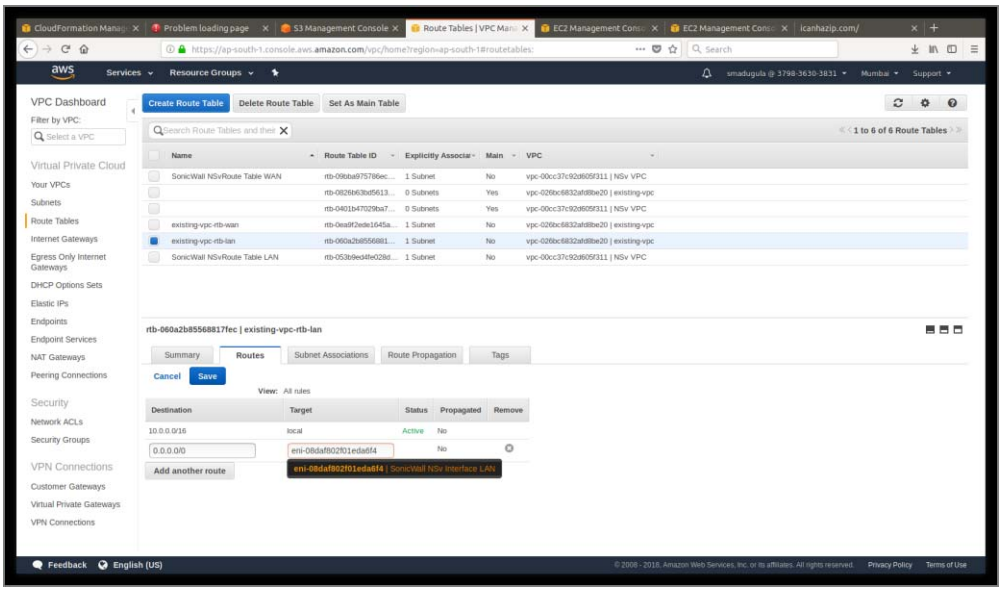
Change Routing Tables for NS$_v$ Access

1 Wait at EC2 Dashboard for **Instance State** — **running**, AND **Status checks** — **2/2 checks passed**.

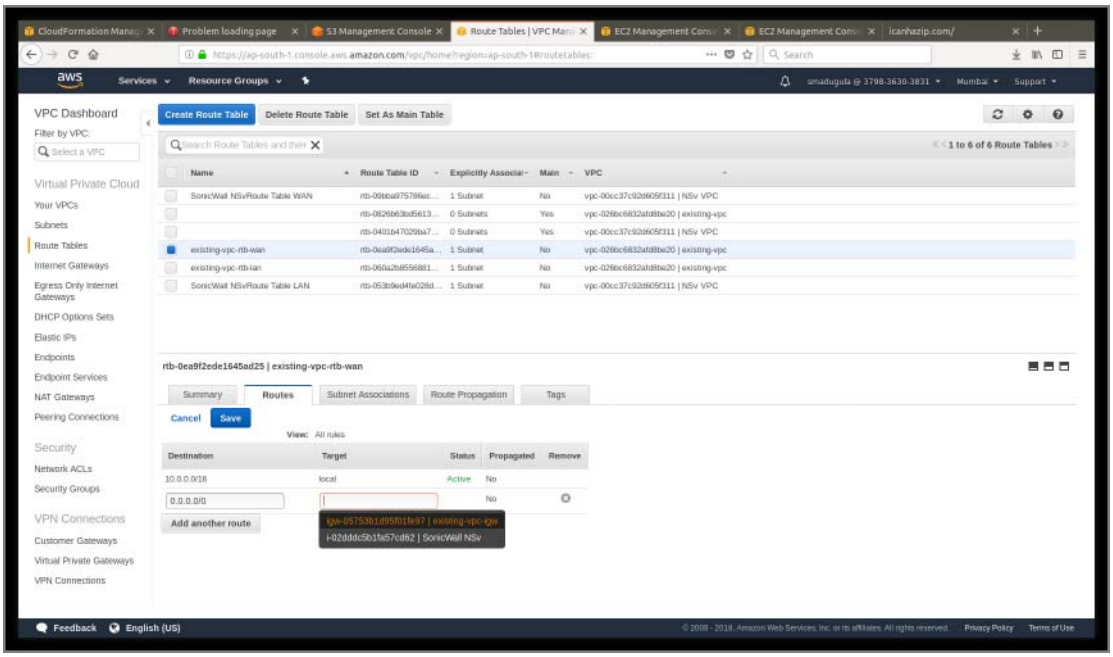


2 Change Routing Tables:

a Change Your LAN routing table to add a route with **Destination** 0.0.0.0/0 with **Target** to NS*v*'s LAN Interface. This routes all your LAN traffic to the NS*v* X0 interface.



b Change your WAN routing table to add a route with **Destination** 0.0.0.0/0 with **Target** to your Internet Gateway (igw-xxxxx). This routes NS*v* WAN traffic to the Internet Gateway (IGW).



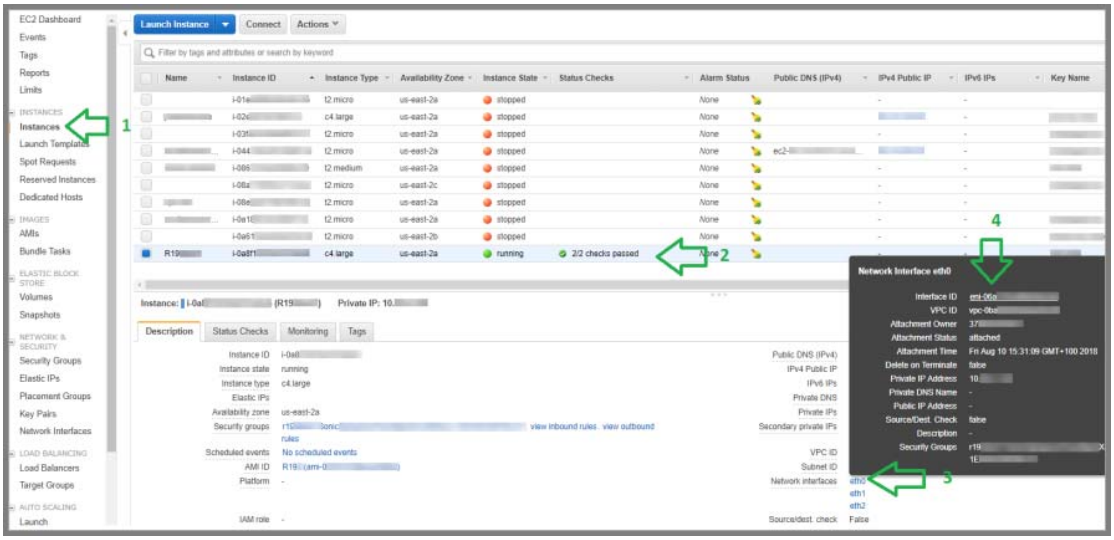
3 Your NS*v* should now be operational. Next, register your NS*v*, see: Deployment Options on page 34. The following section details how to set up access to the NSv from the public internet.

Accessing the SonicWall NS$_v$ Web Interface

To access the SonicWall NS*v* web interface, you need to assign an Elastic IP (EIP) to the NS*v* management interface. For this, you need to use the management Elastic Network Interface (ENI).

To locate the management ENI:

1 In your browser, navigate to **EC2 > Instances**.



2 Select the SonicWall NS*v* instance.

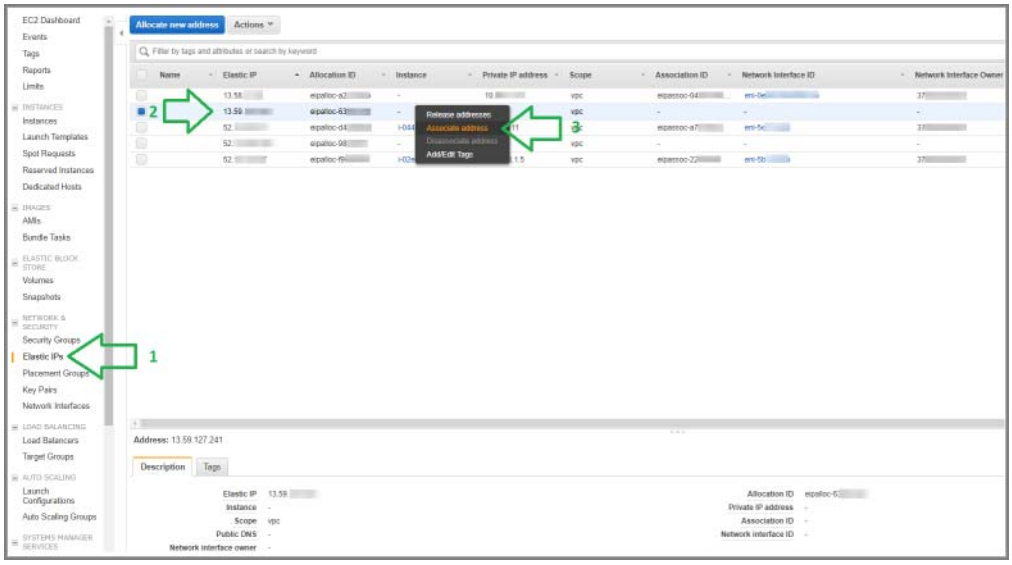
3 Select **eth0** in the lower pane.

4 Copy the **Interface ID** value into your clipboard (eni-xxxxxxxxxxxxxxxxx). This is the management ENI.

5 Paste the value into a temporary file, so you can refer to it during the next procedure.

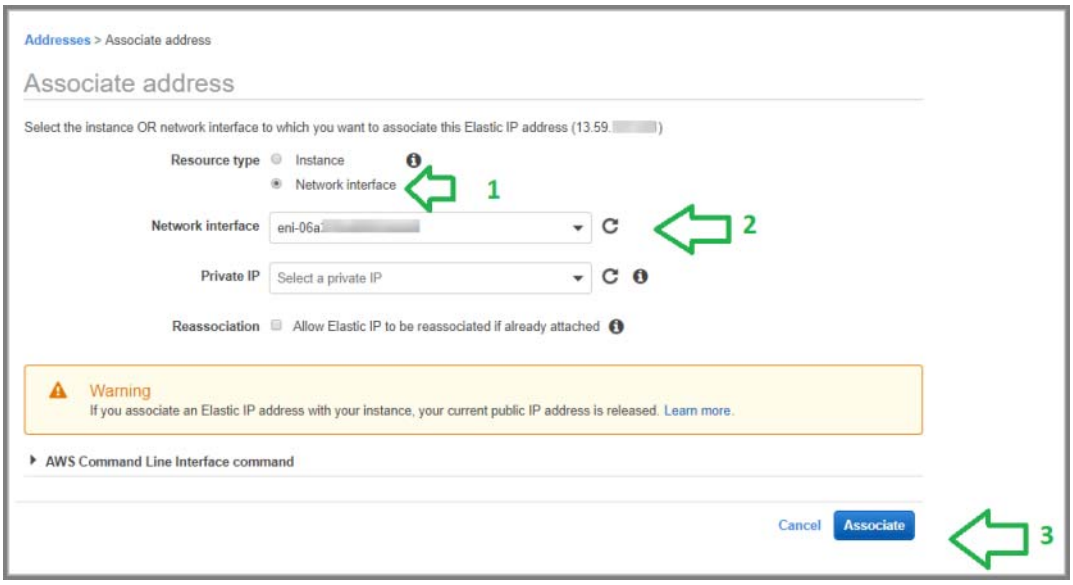
To locate or create the Elastic IP (EIP) and associate it with the management interface:

1 In the left nav pane, click **Elastic IPs**.



2 Select an IP address that is “free”, or if no addresses are available, then click the **Allocate new address** button at the top of the screen.

3 Right-click on the address row and select **Associate Address** from the right-click menu. The **Associate address** screen is displayed.



4 For **Resource type**, select **Network interface**.

5 In the **Network interface** drop-down list, select the ENI of the management interface that you located in the previous procedure.

6 Click **Associate**.

At this point you can point your browser to the Elastic IP (EIP) address that you just associated to the ENI of the NS*v* management interface, by typing in the URL consisting of the IPv4 EIP address (for example: ***https://xx.xx.xxx.xxx***).

To locate the EIP address, see Step 1 on page 27.

The SonicWall NS*v* login page is displayed. Log in using the default credentials (*admin / password where the password* is the AWS instance ID of the newly created SonicWall NSv instance e.g. i-02aaxxxxxxxxxxxx.

If you have not already registered, register your NS*v* virtual firewall MySonicWall. See Deployment Options on page 34.

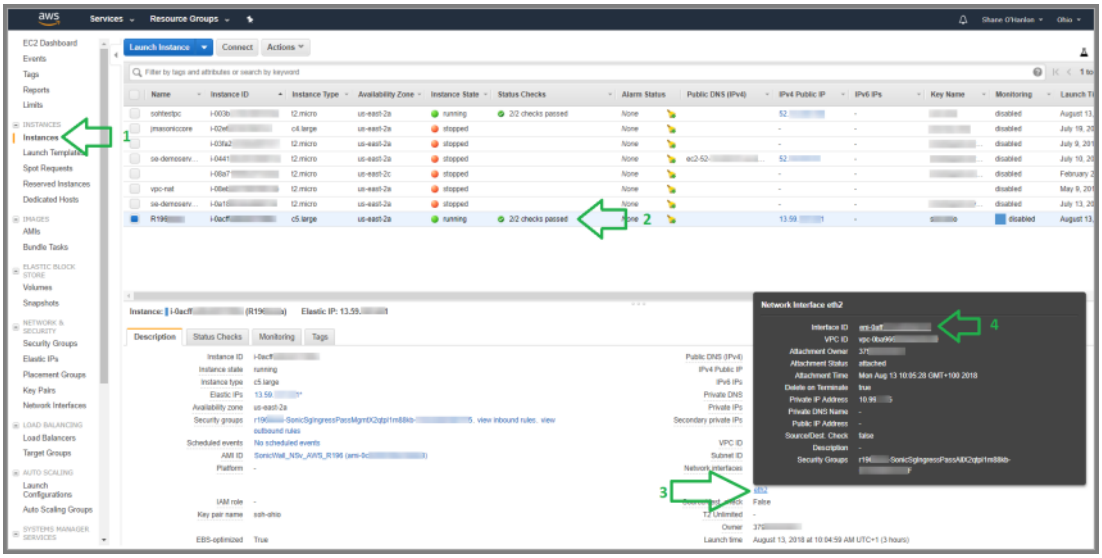
Configuring Internet/Public Access Through the NS$_v$

The X1 interface typically needs egress/ingress access to the public internet. To allow access, the X1 interface must be configured with an ***Elastic IP (EIP)***. Otherwise, traffic from the X1 interface is directed to a NAT Instance.

To assign an EIP to the NS*v* X1 interface, you need to use the Elastic Network Interface (ENI).

To locate the ENI:

1 In your browser, navigate to **EC2 > Instances**.



2 In the top pane, select the NS*v* instance.

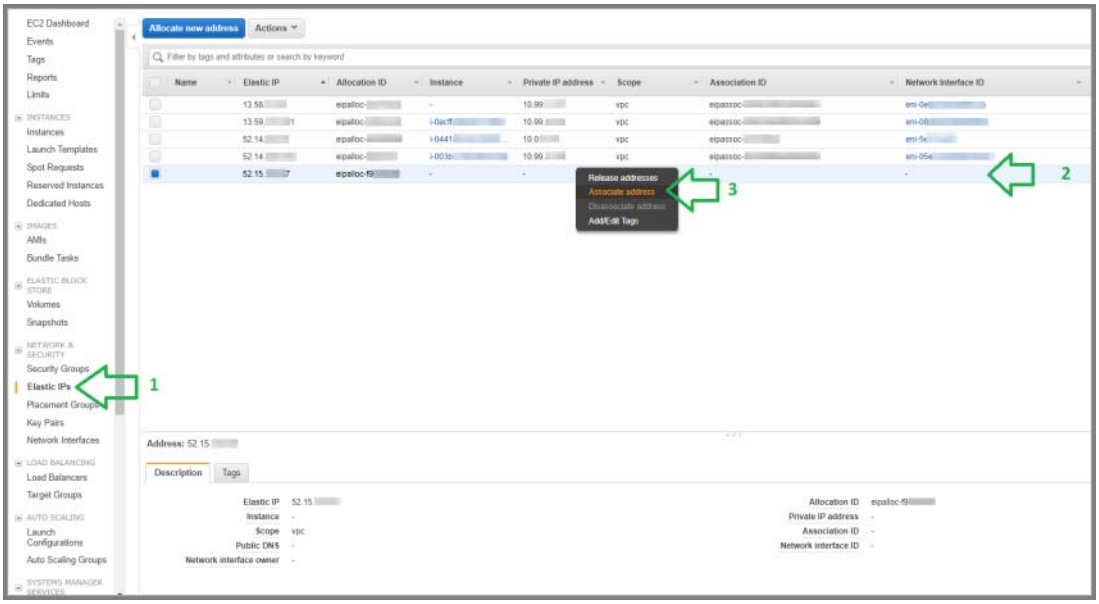
3 In the lower pane, click on **eth0** to display the **Network Interface eth0** popup.

4 Copy the **Interface ID** from the popup. This is the X1 ENI.

5 Paste the value into a temporary file, so you can refer to it during the next procedure.

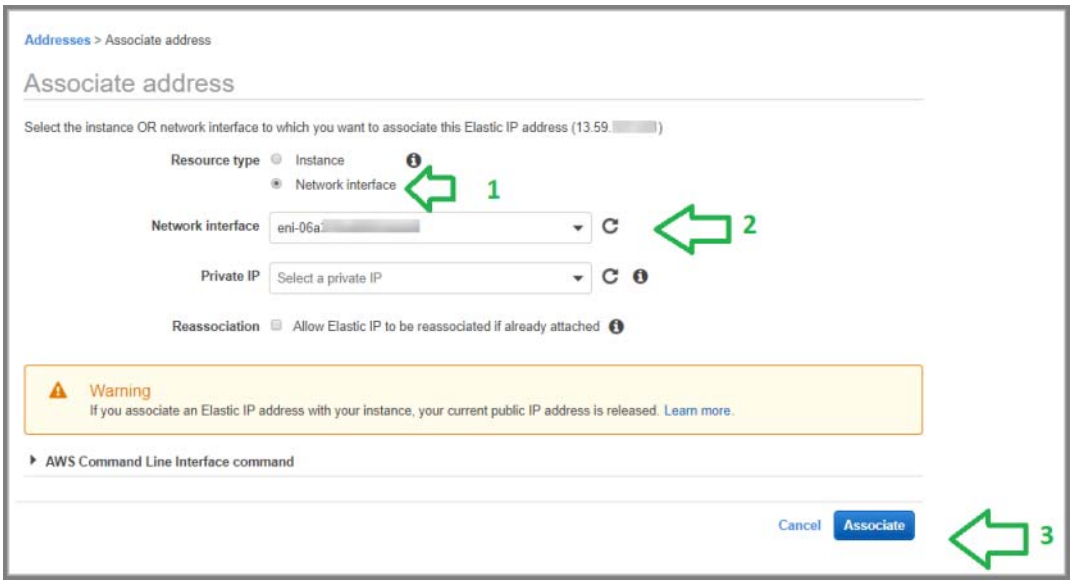
To locate or create the Elastic IP (EIP) and associate it with the X1 interface:

1 In the left nav pane, click **Elastic IPs**.



2 Select an IP address that is “free”, or if no addresses are available, then click the **Allocate new address** button at the top of the screen.

3 Right-click on the address row and select **Associate Address** from the right-click menu. The **Associate address** screen is displayed.



4 For **Resource type**, select **Network interface**.

5 In the **Network interface** drop-down list, select the ENI of the X1 interface that you located in the previous procedure.

6 Click **Associate**.

Troubleshooting Installation Configuration

If the NSv fails to come up, follow the instruction in Navigating the NSv Management Console on page 50 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.

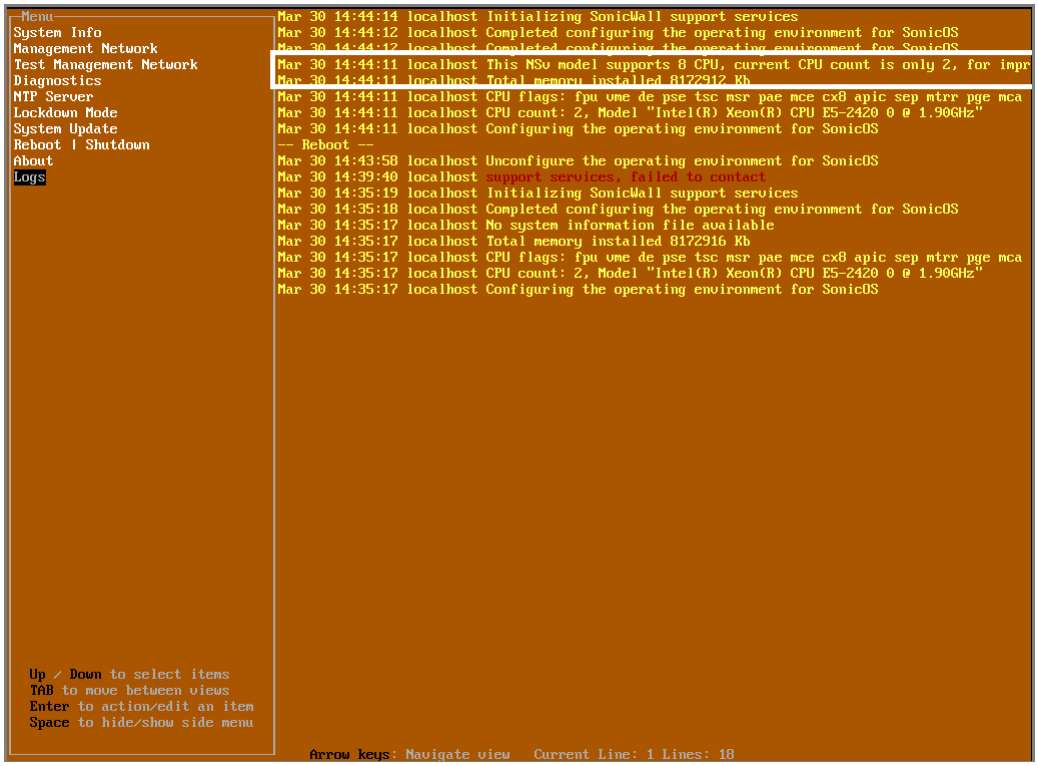
```
Menu
System Info
Management Network
Test Management Network
Diagnostics
NTP Server
Lockdown Mode
System Update
Reboot | Shutdown
About
Logs

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

Mar 30 15:10:39 localhost Initializing SonicWall support services
Mar 30 15:10:38 localhost Completed configuring the operating environment for SonicOS
Mar 30 15:10:08 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
Mar 30 15:10:08 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
Mar 30 15:10:07 localhost Total memory installed 4160884 Kb
Mar 30 15:10:07 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 15:10:07 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 15:10:07 localhost Configuring the operating environment for SonicOS
-- Reboot --
Mar 30 15:06:37 localhost Initializing SonicWall support services
Mar 30 15:06:36 localhost Completed configuring the operating environment for SonicOS
Mar 30 15:06:06 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
Mar 30 15:06:05 localhost Total memory installed 4160884 Kb
Mar 30 15:06:05 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 15:06:05 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 15:06:05 localhost Configuring the operating environment for SonicOS
-- Reboot --
Mar 30 15:05:51 localhost Unconfigure the operating environment for SonicOS
Mar 30 15:02:31 localhost Initializing SonicWall support services
Mar 30 15:02:31 localhost Completed configuring the operating environment for SonicOS
Mar 30 15:02:01 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
Mar 30 15:02:01 localhost Total memory installed 4160884 Kb
Mar 30 15:02:00 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 15:02:00 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 15:02:00 localhost Configuring the operating environment for SonicOS
-- Reboot --
Mar 30 15:01:48 localhost Unconfigure the operating environment for SonicOS
Mar 30 14:59:55 localhost Initializing SonicWall support services
Mar 30 14:59:54 localhost Completed configuring the operating environment for SonicOS
Mar 30 14:59:24 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
Mar 30 14:59:24 localhost Total memory installed 4160884 Kb
Mar 30 14:59:24 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 14:59:24 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 14:59:24 localhost Configuring the operating environment for SonicOS
-- Reboot --
Mar 30 14:59:11 localhost Unconfigure the operating environment for SonicOS
Mar 30 14:54:57 localhost Initializing SonicWall support services
Mar 30 14:54:56 localhost Completed configuring the operating environment for SonicOS
Mar 30 14:54:26 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
Mar 30 14:54:26 localhost Total memory installed 4160884 Kb
Mar 30 14:54:26 localhost CPU flags: fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Mar 30 14:54:26 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Mar 30 14:54:25 localhost Configuring the operating environment for SonicOS
-- Reboot --
Mar 30 14:54:12 localhost Unconfigure the operating environment for SonicOS
Mar 30 14:47:18 localhost Initializing SonicWall support services
```

NOTE: For details on navigating the NSv Management Console to troubleshoot the installation, see Navigating the NSv Management Console on page 50.

Memory may be insufficient without a insufficient memory log entry:

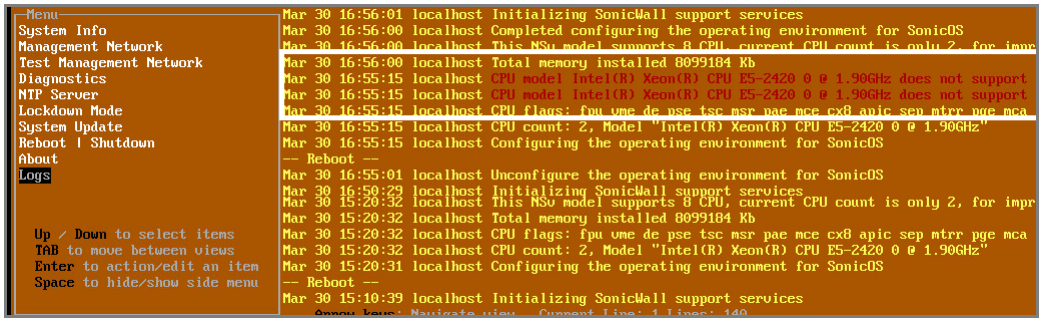


Incompatible CPU

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.

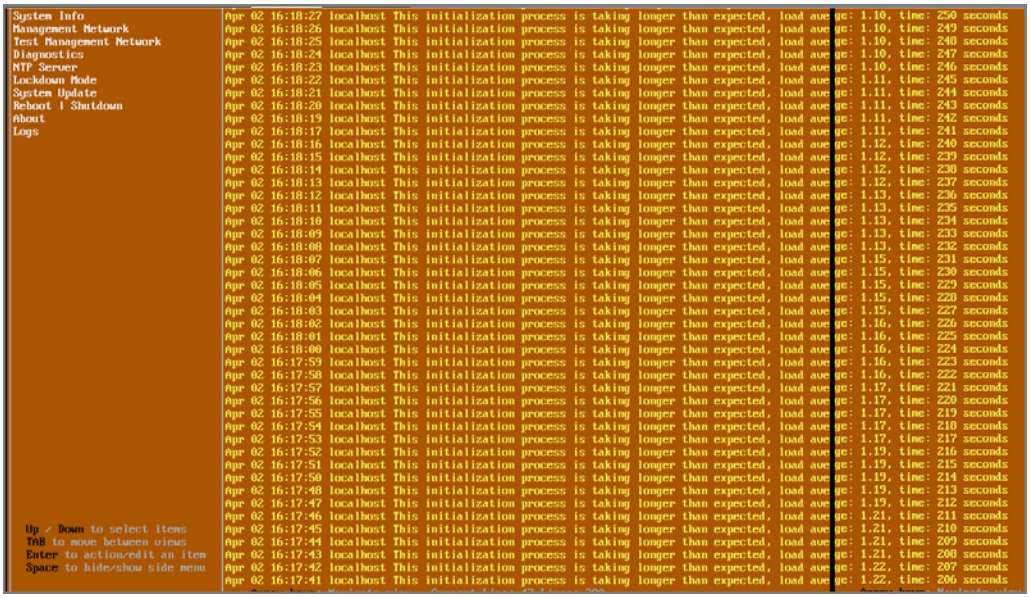
```
The SonicWall Network Security requires all virtual CPU to reside on a single socket.
Power down the virtual machine and adjust the CPU configuration such that all CPU reside on the
same socket
```

Insufficient Resources at Time of Configuration

If the 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

Deployment Options

You may choose to pre-pay for a fixed license period, or pay a recurring fee. You make this choice when selecting the subscription type in the AWS marketplace. Installation procedures for these two options are identical, but completion steps differ.

The following subsections detail these two approaches: BYOL (Bring Your Own License) and PAYG (Pay As You Go).

IMPORTANT: There is no migration path between BYOL and PAYG options, so if you choose to change the licensing model, it will be necessary to first export the configuration data from the NS*v* instance and then disable it. You can then import the configuration data into a new NS*v* instance with the preferred licensing model.

Topics:

Deploying the NS$_v$ as PAYG

This section presents the steps to complete deployment of a PAYG or “Pay as you go” NS*v* instance.

To complete deployment:

1 Once you have installed and configured network settings for your NSv Series appliance, log into the firewall management interface.
To find the IPv4 address for the firewall management interface, log into the Management Console as described in Connecting to the Management Console with SSH.

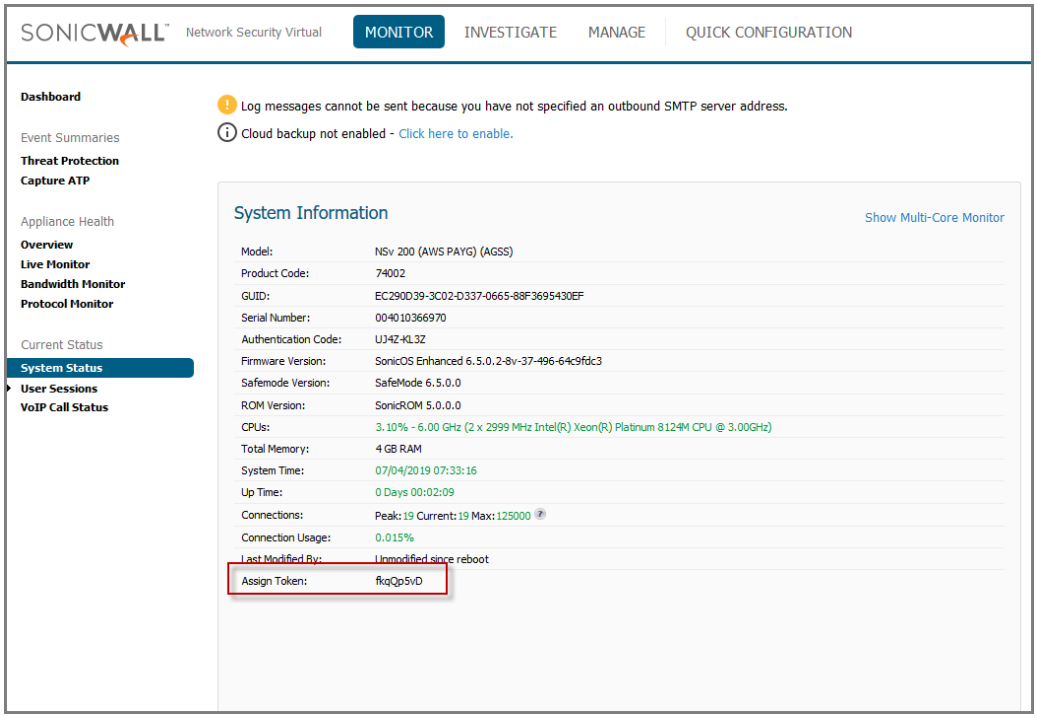
Your SonicWall NSv series firewall is now enabled.

NOTE: To ensure access to SonicWall Technical Support, the procedure, Creating a MySonicWall Account, is recommended. An account at MySonicWall offers advantages:

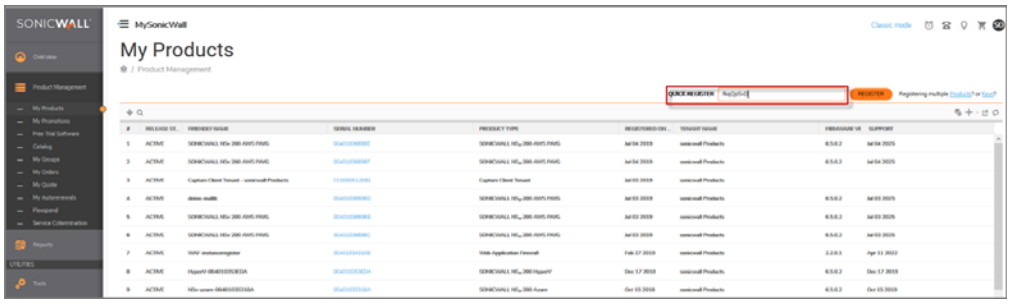
- It allows you send diagnostics from you firewall directly to SonicWall Technical Support.
- It supports easy initiation of support cases online. See:
https://www.sonicwall.com/support/knowledge-base/?sol_id=170814110235888

2 Take the following steps to link your virtual firewall to MySonicWall:

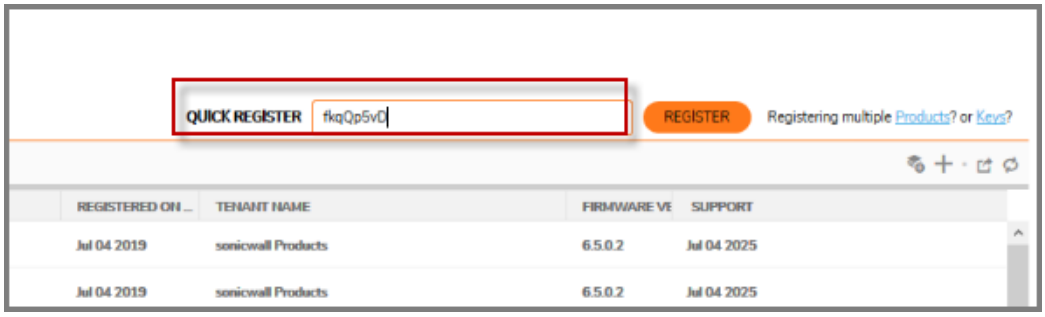
a Login into the NSv (see Step 1), and copy the Assign Token.



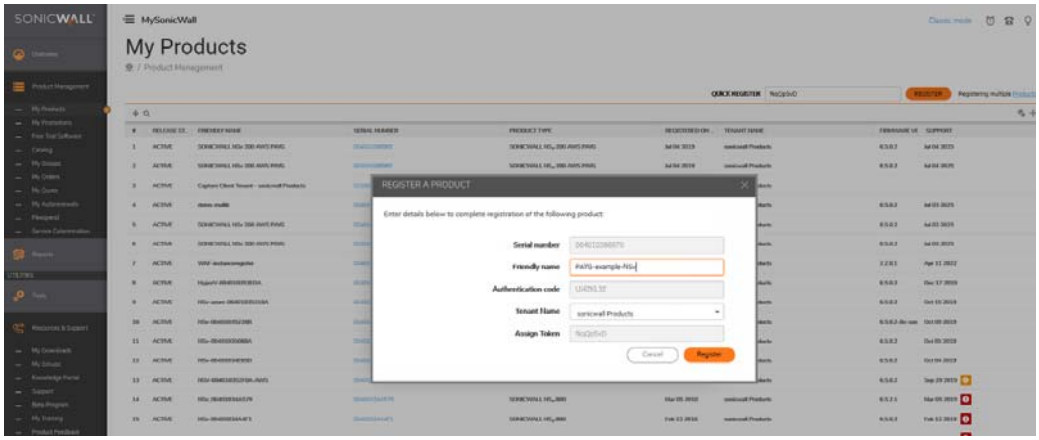
b Login into MySonicWall and go to **My Products**:



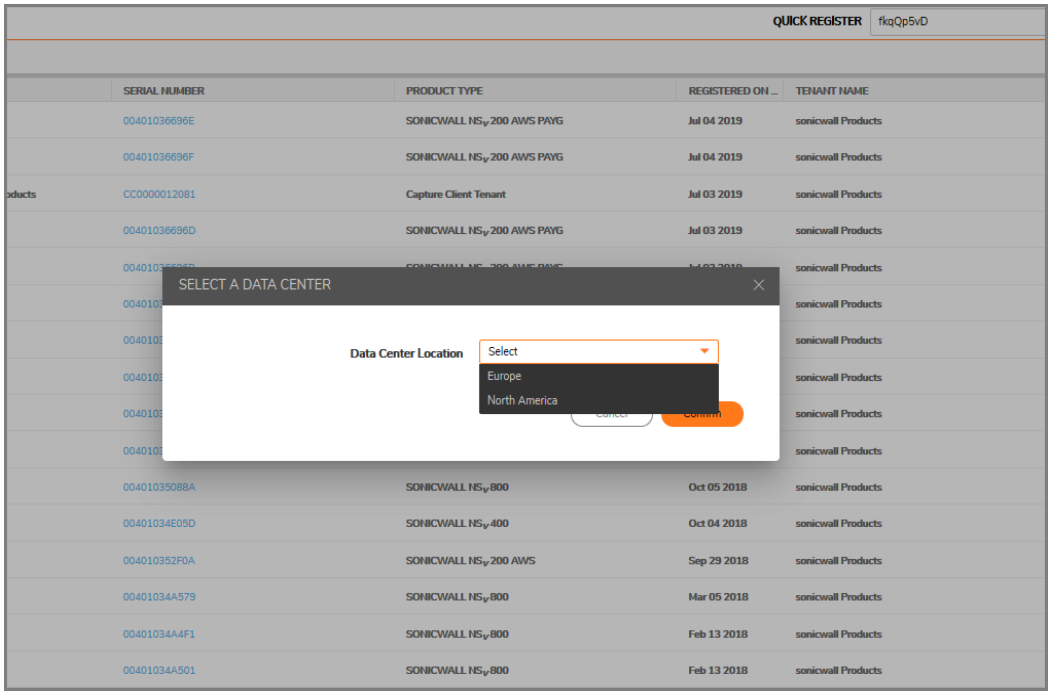
c Enter the Assign Token into the **Quick Register** box, then click on **Register**.



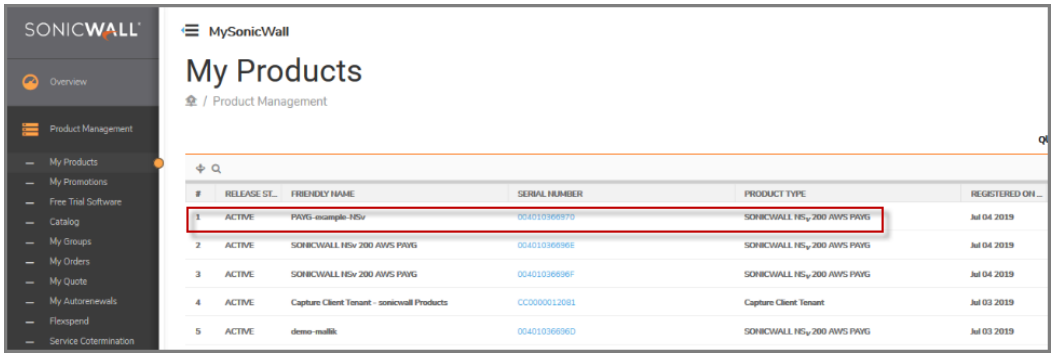
d Enter a friendly name:



e Select a data center:



f Registration is complete. The NS*v* AWS PAYG now appears in My Products on SonicWall:



3 Navigate to **Monitor > System Status** page which reflects licensing of all available features after the deployment process.

Deploying the NS$_v$ as BYOL

This section presents steps to complete deployment when the NS*v* is setup BYOL, or “Bring Your Own License.”

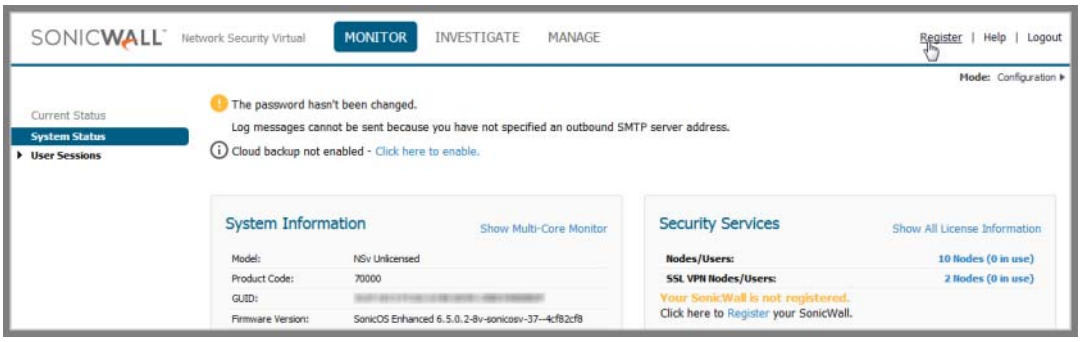
Once you have installed and configured network settings for your NS*v* Series appliance, you can log into SonicOS management and link it in your MySonicWall account. To set up an account, see Creating a MySonicWall Account..

NOTE: System functionality in a BYOL deployment is limited unless the NS*v* is linked to a MySonicWall account. For details refer to Using SonicOS on an Unregistered NSv on page 42.

To link your NSv to MySonicWall:

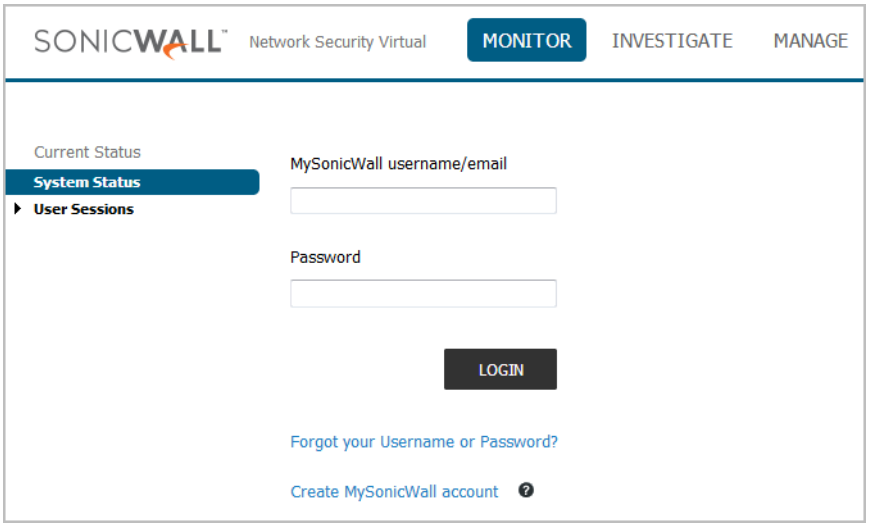
1 Point your browser to your NS*v* WAN or LAN IP address and log in as the administrator (default *admin / password*).

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

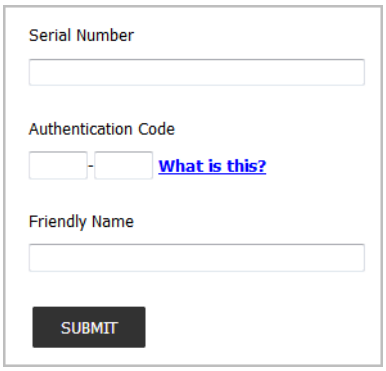


3 Enter your MySonicWall credentials and click **LOGIN** to log into MySonicWall.

> **NOTE:** To create an account, refer to Creating a MySonicWall Account on page 41.



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 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.

Your SonicWall NSv series firewall is now fully enabled.

De-activating Your NS$_v$

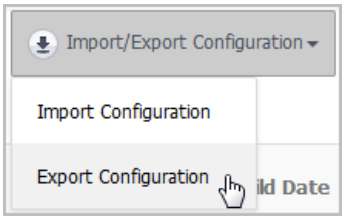
You can de-register your NS*v* directly from the SonicOS management interface. De-activation puts the virtual appliance into a disabled state and deletes the binding between it and MySonicWall. Then you can use the serial number to enable another NS*v* instance. Only one NS*v* instance is allowed per serial number.

To deregister a BYOL 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 deactivating your NS*v*.

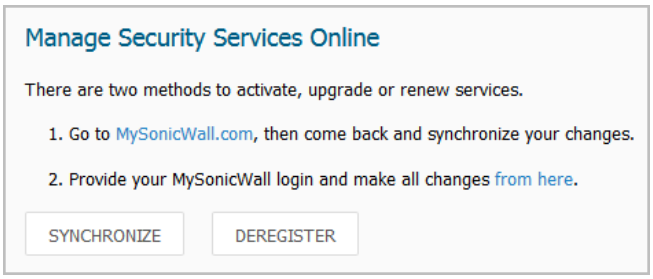


This makes it possible to import the settings to another NS*v* instance.

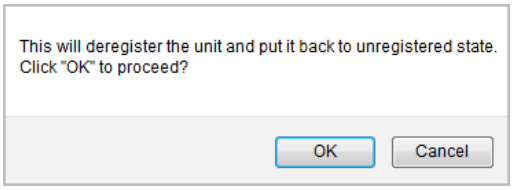
CAUTION: Be sure to export your configuration settings before deactivating your NS*v*. You cannot recover them after deregistration.

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 de-activation is successful, the virtual appliance will return become disabled. 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 de-activation 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 BYOL 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.

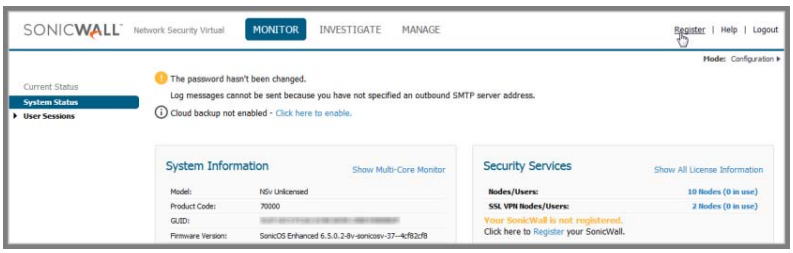
2 Log into SonicOS on your free trial instance.

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

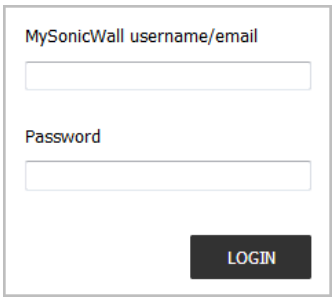
4 Under **Manage Security Services Online**, click the **DEREGISTER** button.

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.

Creating a MySonicWall Account

For **BYOL** users, MySonicWall account is required for product registration to enable full functionality of SonicOS features, and for access to licensed security services.

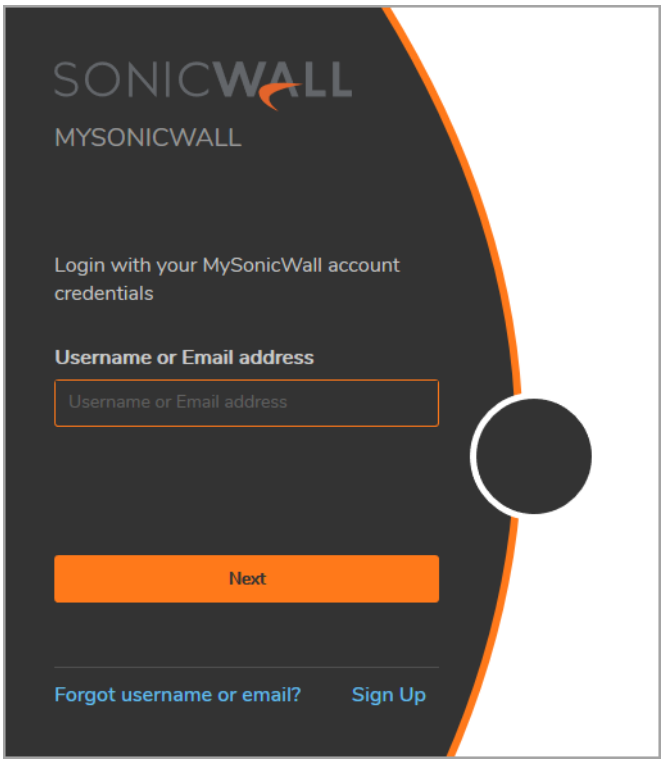
For **PAYG** users, MySonicWall registration ensures connection with, and updates from, SonicWall Technical Support.

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

To create a MySonicWall account:

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

2 In the login screen, click the **Sign Up** link.



3 Complete the account information, including email and password.

4 Follow the prompts to finish creating your account.

5 Click **Finish**.

6 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.

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

For **PAYG** customers, go to Step 2 Take the following steps to link your virtual firewall to MySonicWall: on page 35.

For **BYOL** customers, go to To link your NS***v to MySonicWall:*** on page 37.

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. By default, the X0 interface has HTTPS management and DHCP enabled. So the X0 IP address is acquired from the AWS provided DHCP server in the X0 subnet. 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.

   You can access the DHCP-assigned IP address of the X0 LAN interface of your NS*v* through your AWS instance for SonicOS management.

2. Enter the administrator credentials (default *admin / instance-ID*) 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 Uploading a New Image in SafeMode on page 70.

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 NS***v*** 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: Check Network Settings Ipv6 Check Network Settings Connections Monitor Multi-Core Monitor Core Monitor Link Monitor Packet Size Monitor DNS Name Lookup Find Network Path Ping Core 0 Process Monitor Real-time Black List Lookup Reverse Name Resolution Connection Limit TopX TraceRoute PMTU Discovery Web Server Monitor User Monitor See Using System Diagnostics in SonicOS on page 45 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:

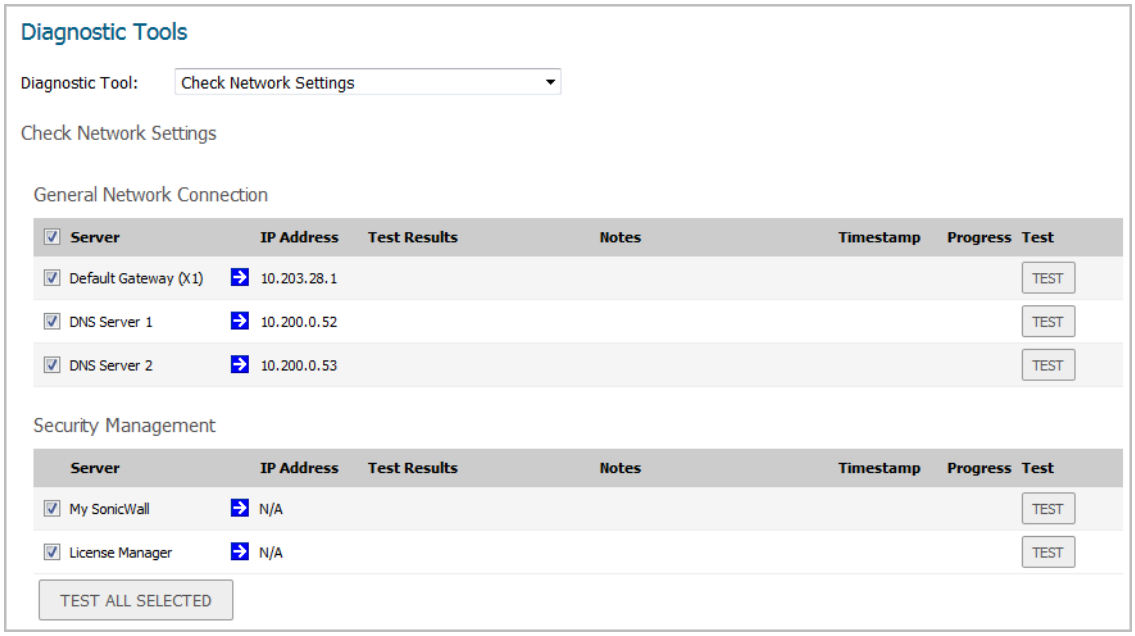
Button	Function
ACCEPT	Saves any changes you made to the diagnostic support report or diagnostic tool.
CANCEL	Cancels any changes you initially made to the diagnostic support report or diagnostic tool.
REFRESH	Refreshes the data being displayed in the **Diagnostic Tools** section.

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 **IP Address** field of the failed item to jump to the configuration page to investigate the root cause.

Upgrading the NS*v*

There are two ways to install the latest upgrade file (SWI) for your NSv:

- In the firewall GUI, navigate to **MANAGE | Firmware Management & Backup > Upload Firmware.**
- Use the Management Console in SafeMode. See Uploading a New Image in SafeMode.

The SWI file will be available via mysonicwall or from Technical Support.

For more information, see the *SonicOS 6.5 NSv Series Upgrade Guide*.

5

Using the Virtual Console and SafeMode

This chapter discusses two software interfaces supporting NS*v*:

- the NS*v* Management Console
- the NS*v* SafeMode web interface

> **NOTE:** For information on using the SonicOS CLI and NS*v* management console to troubleshoot the installation, see Troubleshooting Installation Configuration on page 30.

Topics:

Connecting to the Management Console with SSH

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

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

Logging in via SSH is only possible through the certificate file configured during the NS*v* deployment.

To connect from Linux, refer to the AWS documentation on how to connect to the SonicWall NS*v* EC2 instance:

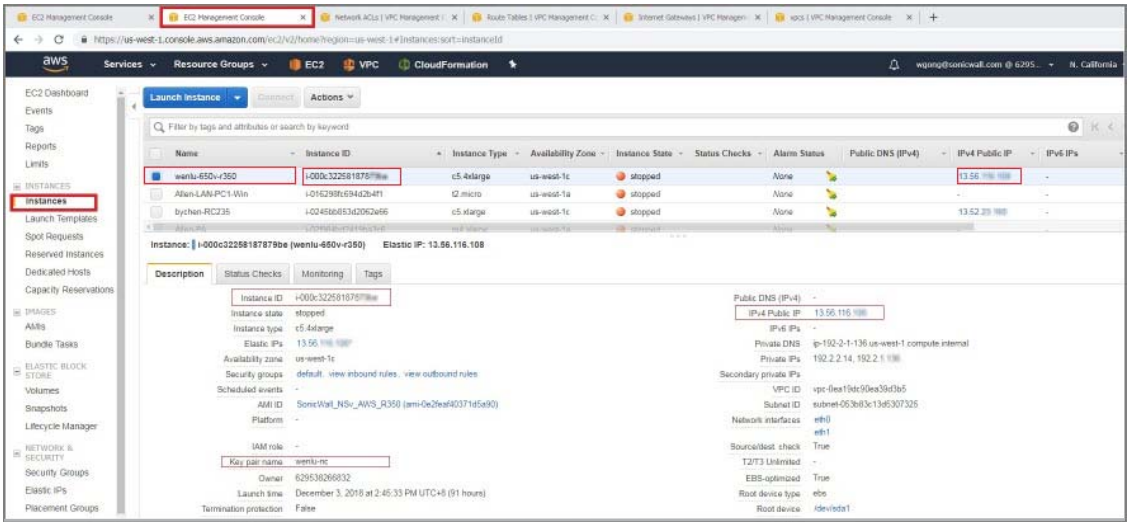
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstancesLinux.html

To connect from Windows, refer to AWS documentation:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

To connect to the management console from the command line:

1. Survey the AWS documentation referenced above.
2. Navigate to the AWS EC2 Management Console and view the **Instances** page for your NSv.



3 Copy and paste the Instance ID and IPv4 address into a temporary file.

4 Refer to the instructions in the AWS documentation referenced above.

5 When ready to connect using the ssh command from Linux or with Putty from Windows, use ***management*** as the SSH username.

For example, from Linux:

```
ssh -i /path/my-key-pair.pem management@ec2-198-51-100-1.compute-1.amazonaws.com
```

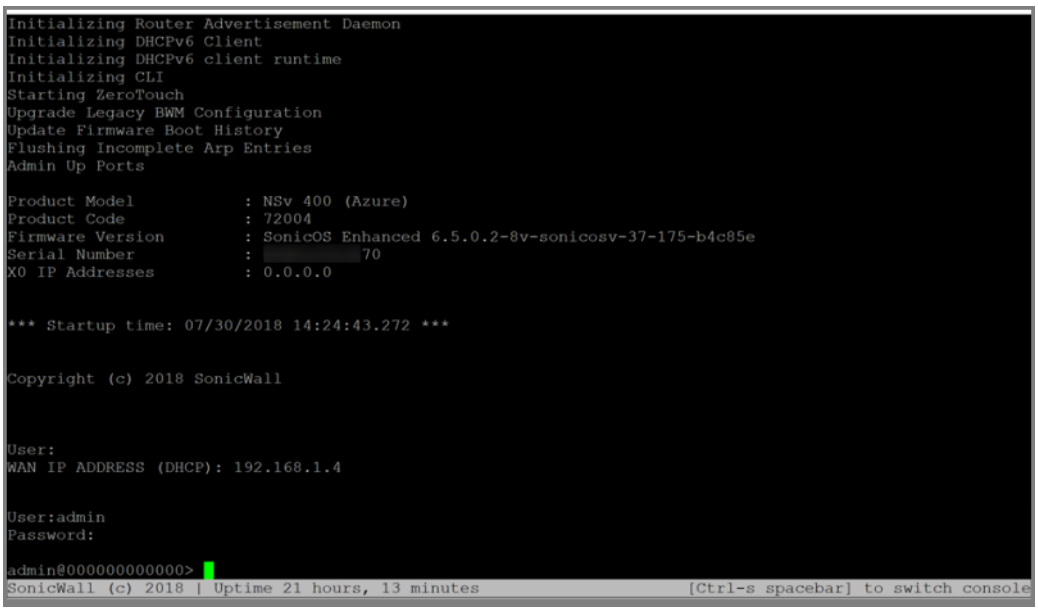
From Windows, with PuTTY: in the Host Name box, enter management@<public_dns_name>.

6 The .pem (on Linux) or .ppk (on Windows) file created from the key pair for your AWS NSv instance is used to authenticate the SSH session, as explained in the AWS documentation.

The orange NSv Management Console displays.

NOTE: The address to log into the web interface is given in the lower right of the display.

You can switch to the black SonicOS 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* where password is the Instance ID).



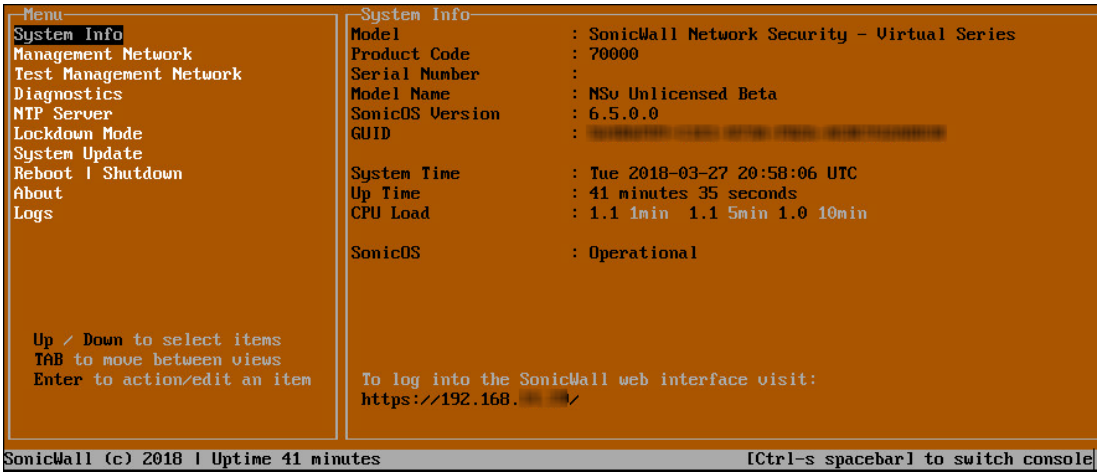
See Navigating the NSv Management Console for information about the options in the NSv management console.

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. To connect to the NSv Management Console, see Connecting to the Management Console with SSH.

To navigate and use the management console:

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



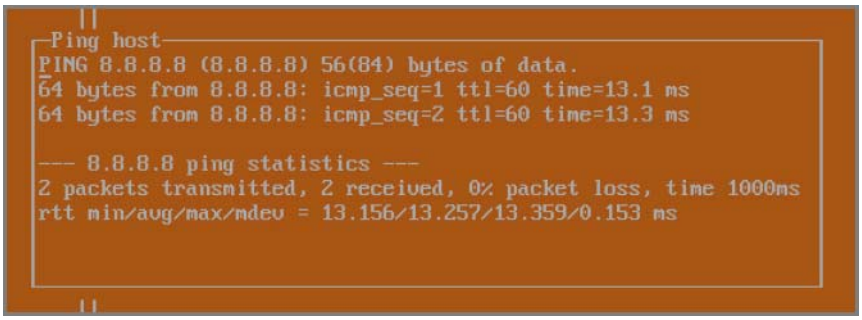
2 The main menu is displayed in the side menu (left pane). Use the up/down arrow keys to move the focus between menu items. As the focus shifts, the right pane displays the options and information for that menu item. The currently selected item is highlighted in black.

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:



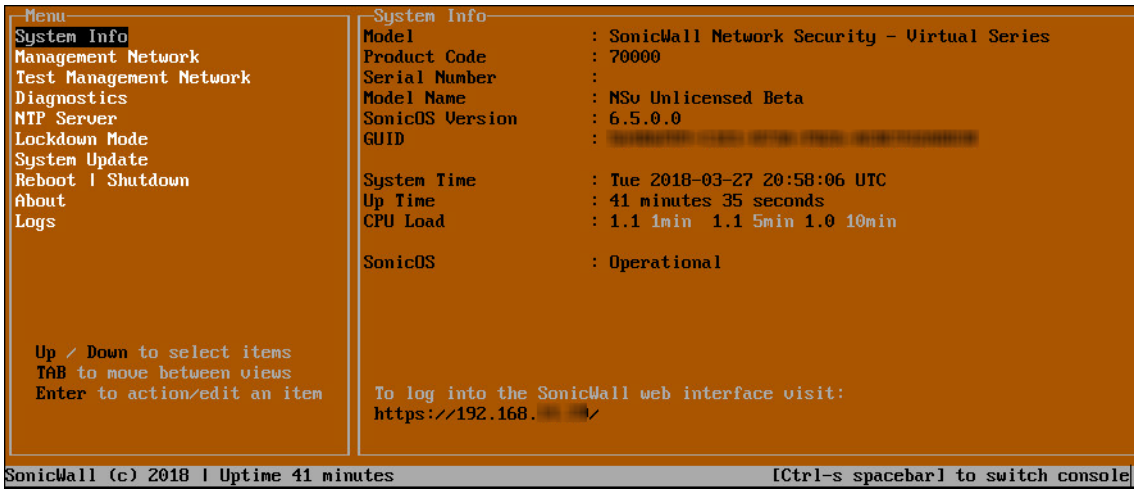
Some dialogs are for input:

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

System Info



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

- **Model** – This is the model of the 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

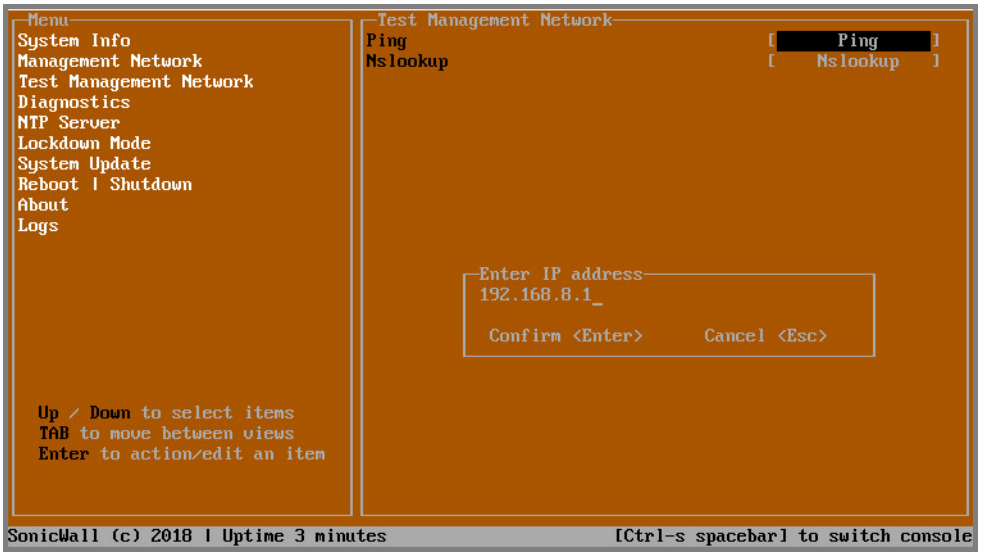
Network Interfaces screen

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 AWS. In an AWS 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:

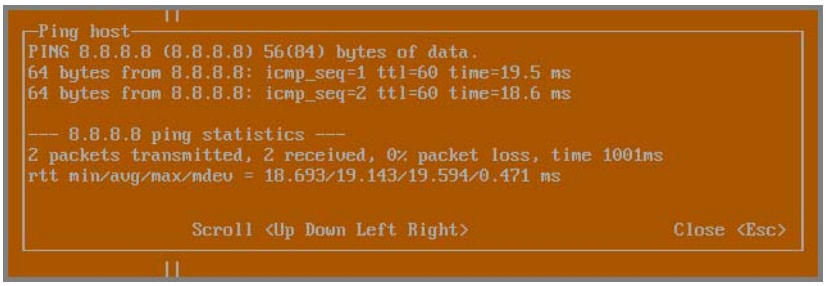
1 Select **Test Management Network** in the Menu and press **Tab** to move the focus into the **Test Management Network** screen.

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.

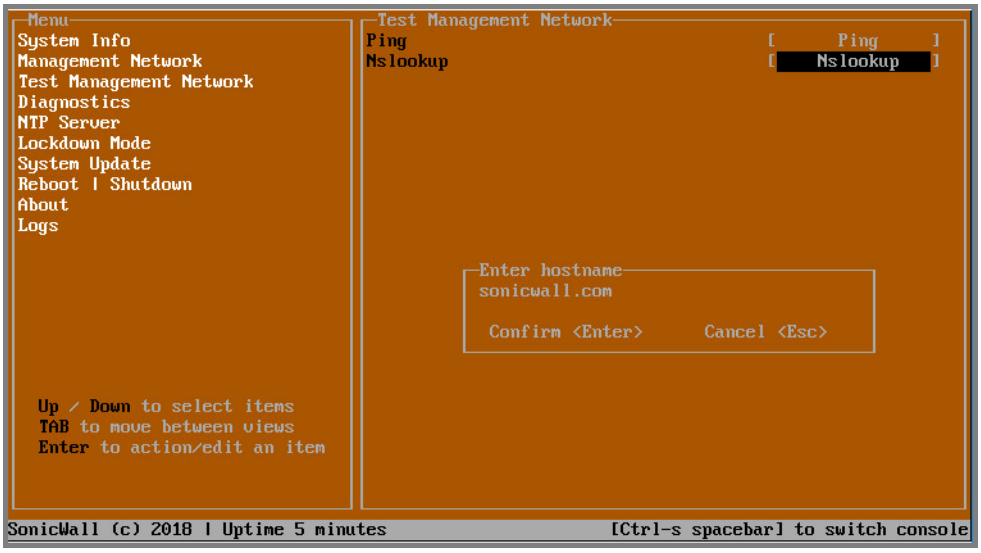


5 Press the **Esc** key to close the dialog.

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.



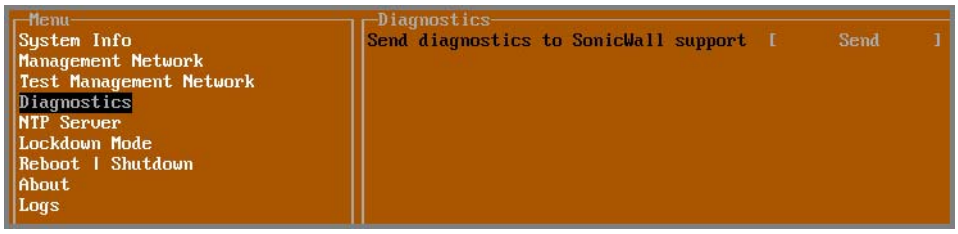
3 Navigate into the dialog, press **Backspace** to clear the current value, and then type in the hostname that you want to look up with a DNS query.

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.

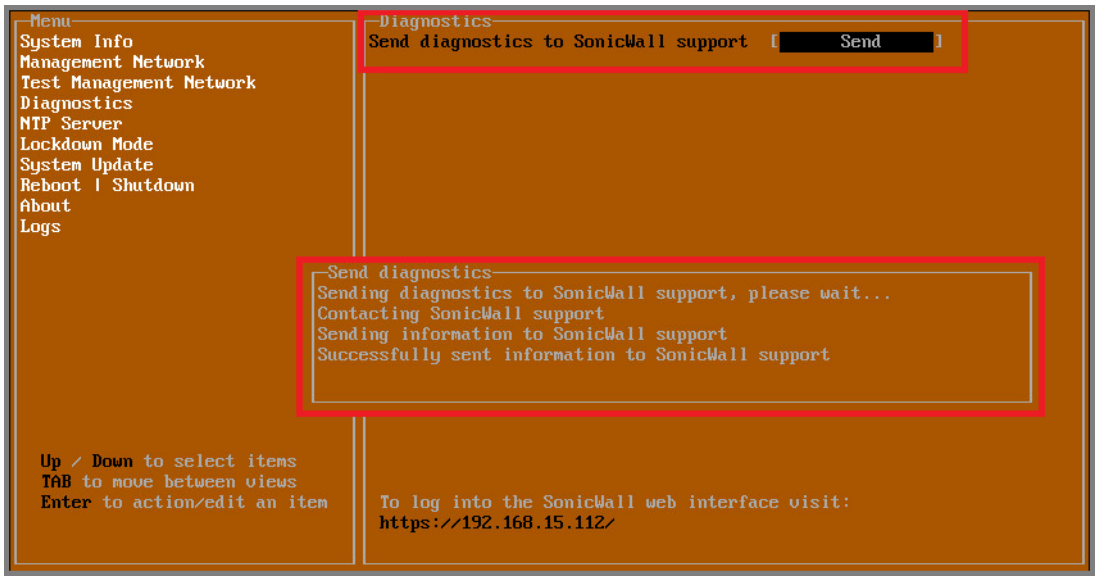
Diagnostics



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

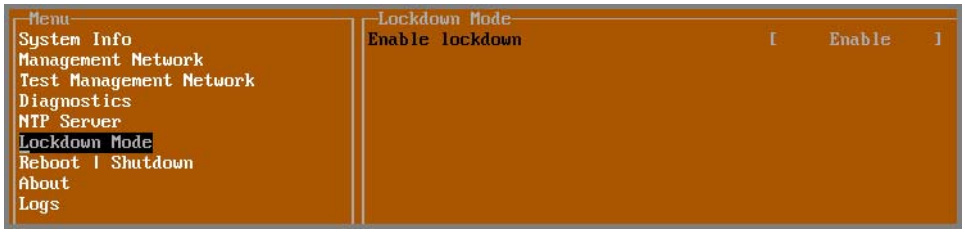
In the **NTP Server** screen, you can synchronize with an NTP server. For complete NTP Server configuration options, log into the SonicOS management interface and navigate to the **MANAGE | Appliance > System Time** page.

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.**

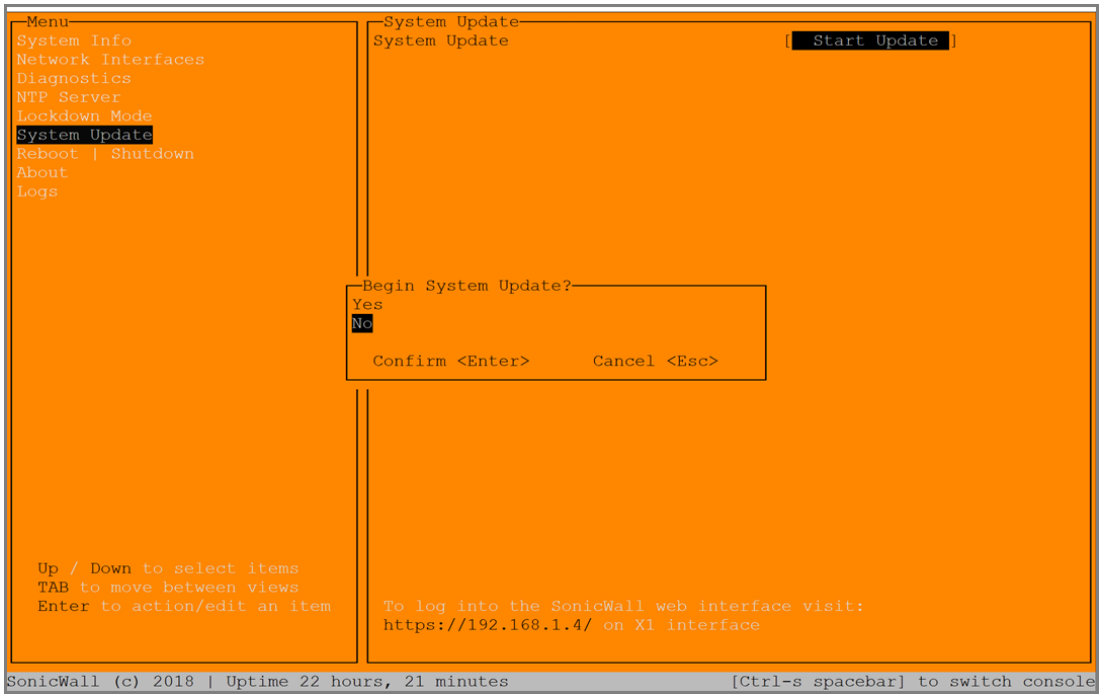
Temporary Lockdown Mode

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 AWS.



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:

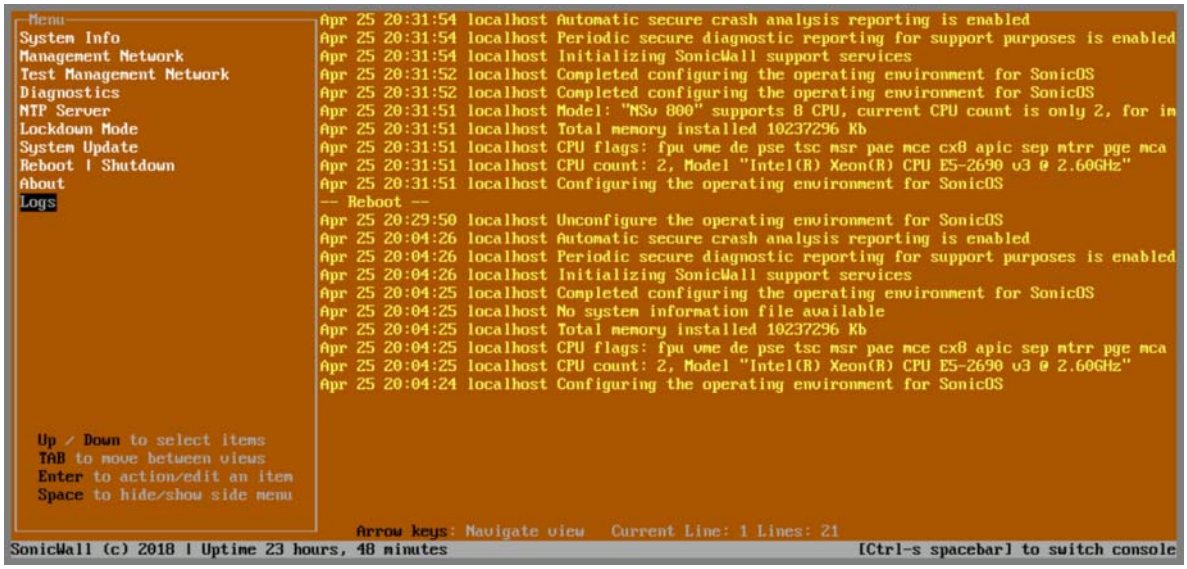
- **Reboot SonicWall** – Restarts the NS*v* Series virtual appliance with current configuration settings.
- **Shutdown SonicWall** – Powers off the NS*v* Series virtual appliance.
- **Boot with factory default settings** – Restarts the NS*v* Series virtual appliance using factory default settings. All 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 the Management Console in SafeMode on page 60.

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 the Management Console in SafeMode

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

Topics:

How Management Console Differs in SafeMode

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

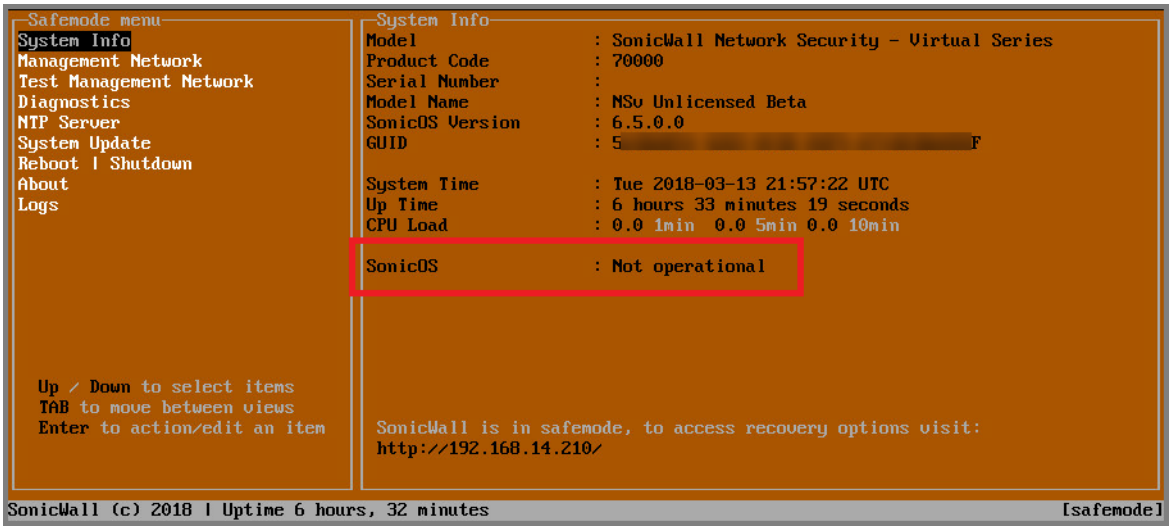
- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

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

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

Entering SafeMode

After booting into SafeMode, the management console always starts with the **System Info** screen.



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

Enabling/Disabling SafeMode

Topics:

- Enabling SafeMode
- Disabling SafeMode

Enabling SafeMode

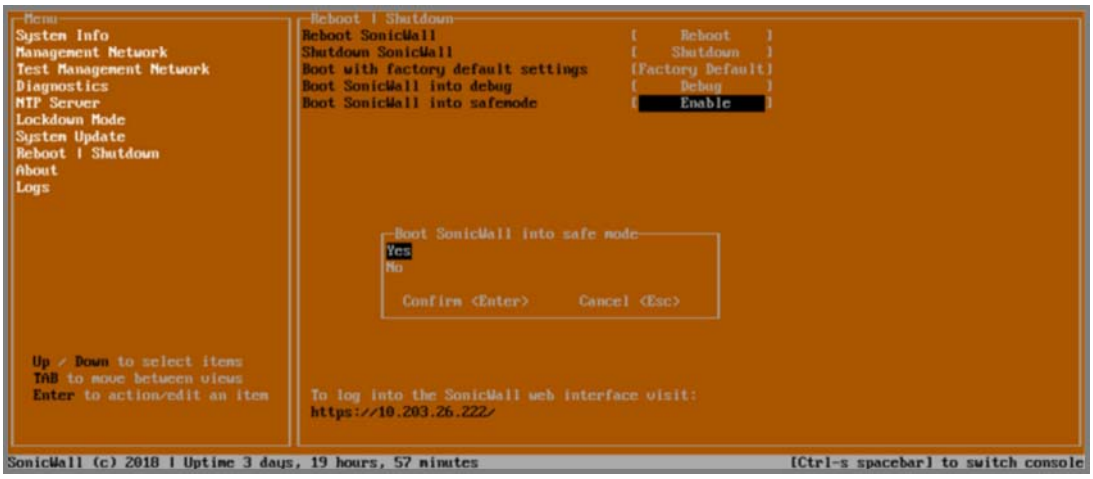
SafeMode can be enabled from the management console.

To enable SafeMode:

1 Access the NSv management console as described in Connecting to the Management Console with SSH.

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

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



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

5 Press **Enter**.

The NSv immediately reboots and comes back up in SafeMode.

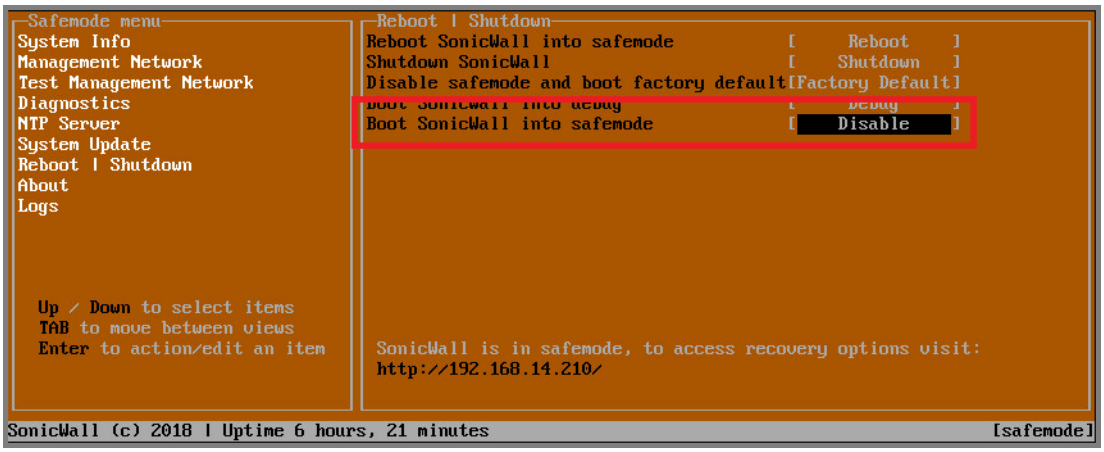
NOTE: In SafeMode, the web interface is served from an HTTP server. The HTTPS server is not started in SafeMode.

Disabling SafeMode

To disable SafeMode:

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

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



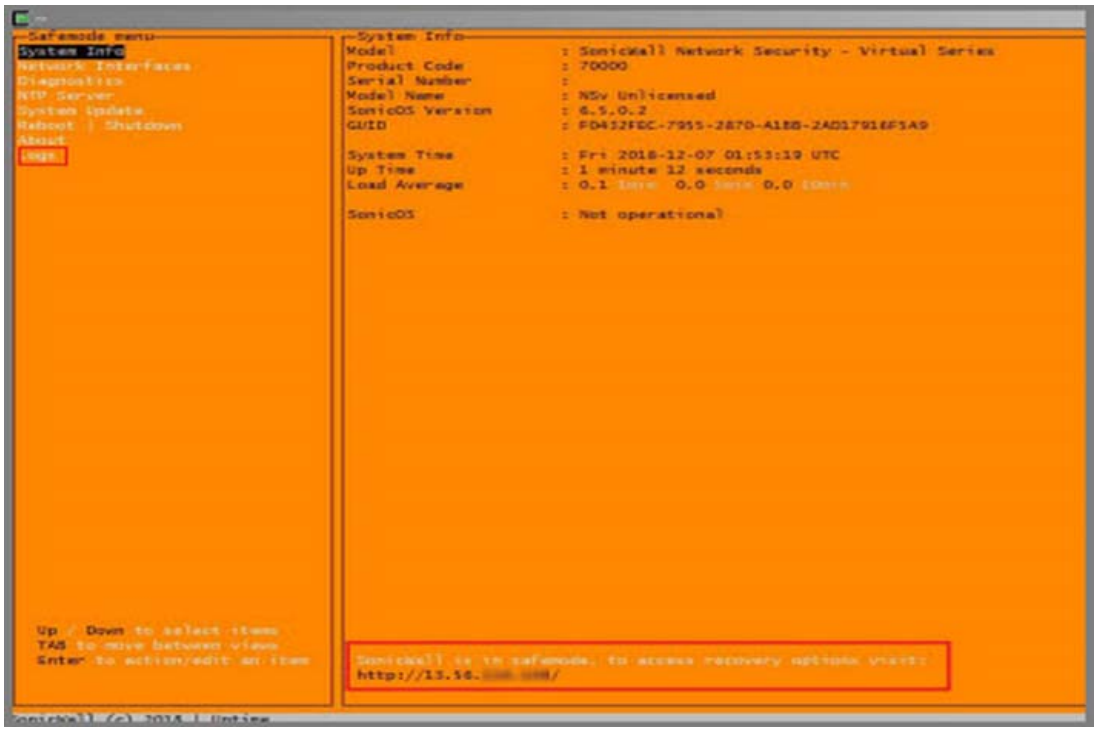
3 Select **Yes** in the confirmation dialog.

4 Press **Enter**.

The NSv immediately reboots and boots up in normal mode.

Configuring the Management Network in SafeMode

Refer to Enabling/Disabling SafeMode to get into SafeMode. Once access is authenticated you will have access to the management console in SafeMode.



[

When the Management Console is in SafeMode, the **Management Network** screen in the NS*v* management console provides features to configure the NS*v* appliance interfaces:

- **Management Interface** – This is the currently selected interface. This defaults to X1. Use this to select any of the NS*v* appliance interfaces.
- **IPv4 Address** – The current IPv4 address currently assigned to the Management Interface.
- **Netmask** – The current Netmask assigned to the Management Interface.
- **Mac Address** – The MAC address of the Management Interface.
- **IPv6 Address** – The currently assigned IPv6 address of the Management Interface.
- **Gateway** – The current Default Gateway currently in use by the NS*v* appliance.
- **DNS** – A list of the current DNS servers currently being used by the NS*v* appliance.

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

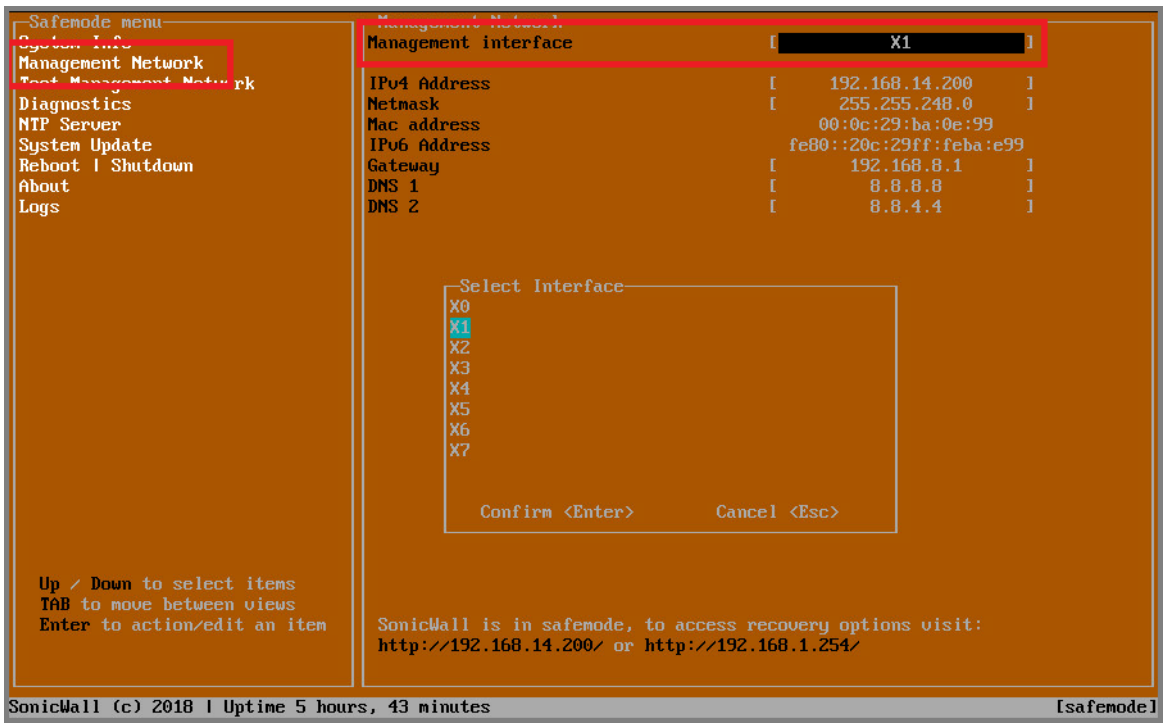
Topics:

- Configuring Interface Settings
- Disabling an Interface

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.

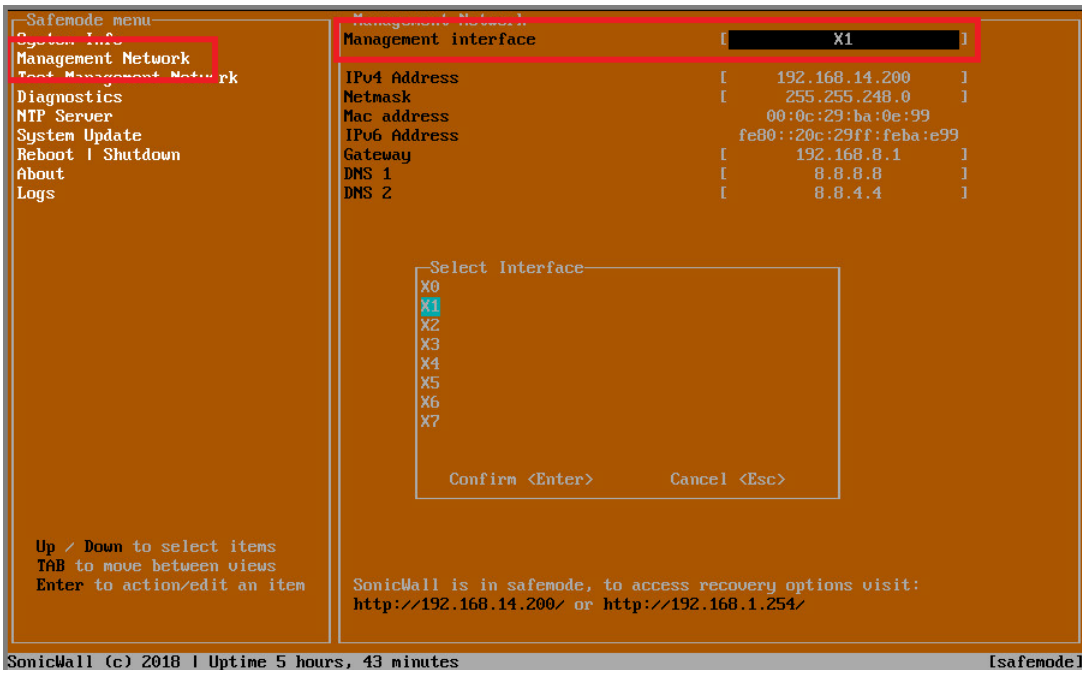
NOTE: In SafeMode, the X0 will be set by DHCP.



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**.

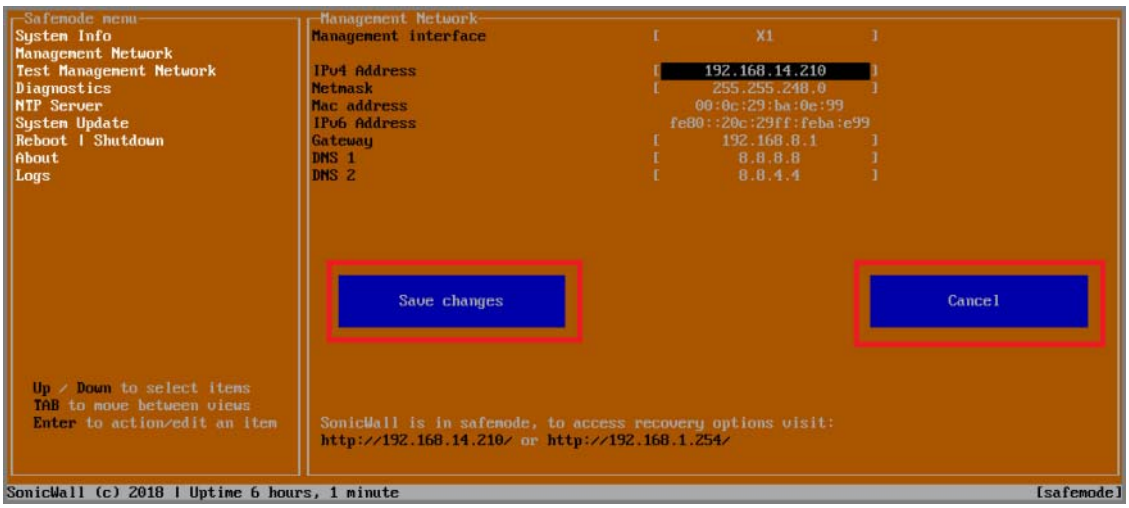
The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

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*.

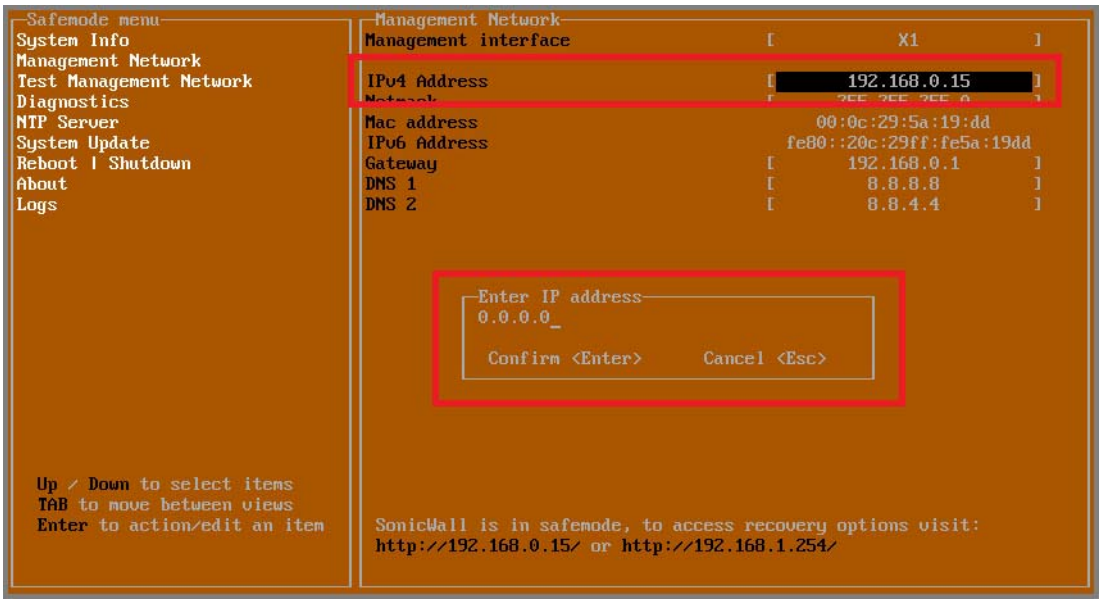
3 Select the interface you wish to edit and press **Enter**.

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.

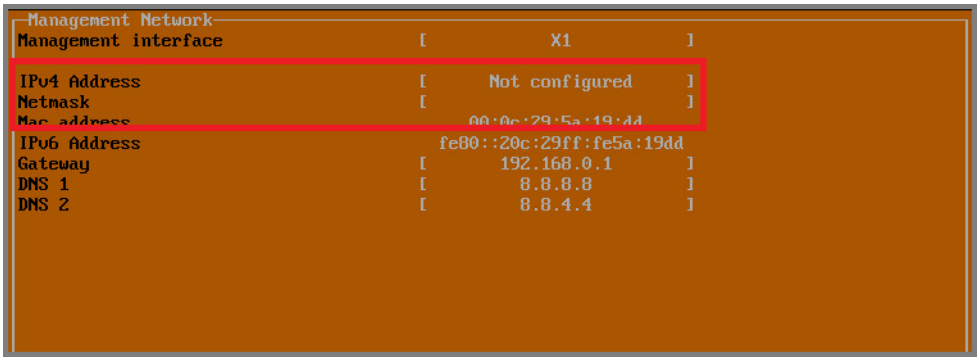
5 Navigate into the dialog and change the IP address to **0.0.0.0**, then press **Enter**.



The **Save changes** button is displayed.

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

The interface is disabled.



Using the SafeMode Web Interface

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

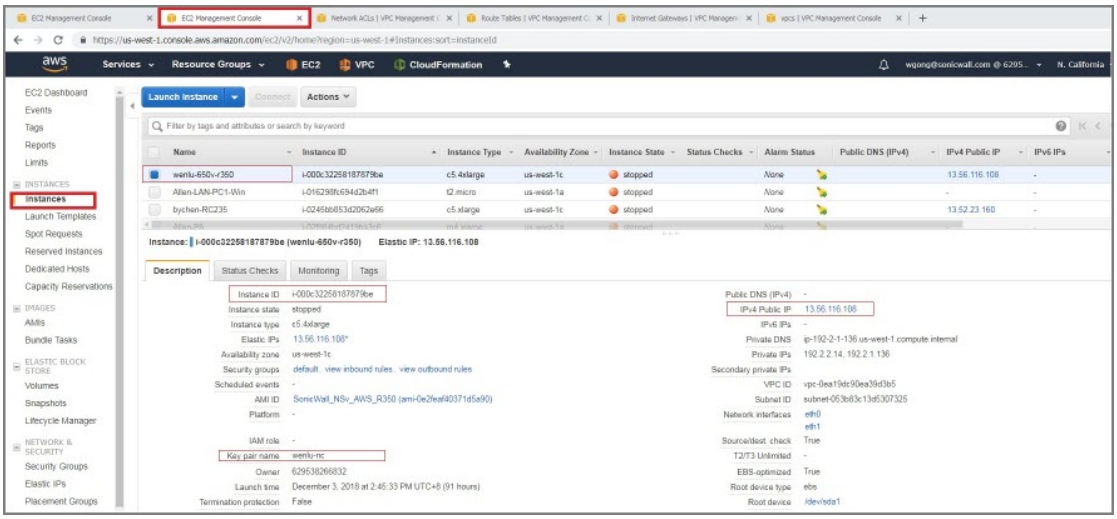
Topics:

- Accessing the SafeMode Web Interface
- Entering/Exiting SafeMode
- Locking and Unlocking the Management Console
- Downloading the SafeMode Logs
- Uploading a New Image in SafeMode

Accessing the SafeMode Web Interface

To access the SafeMode web interface:

1 Navigate to the AWS E2C Management Console page and view the **Instances** page for your NSv.

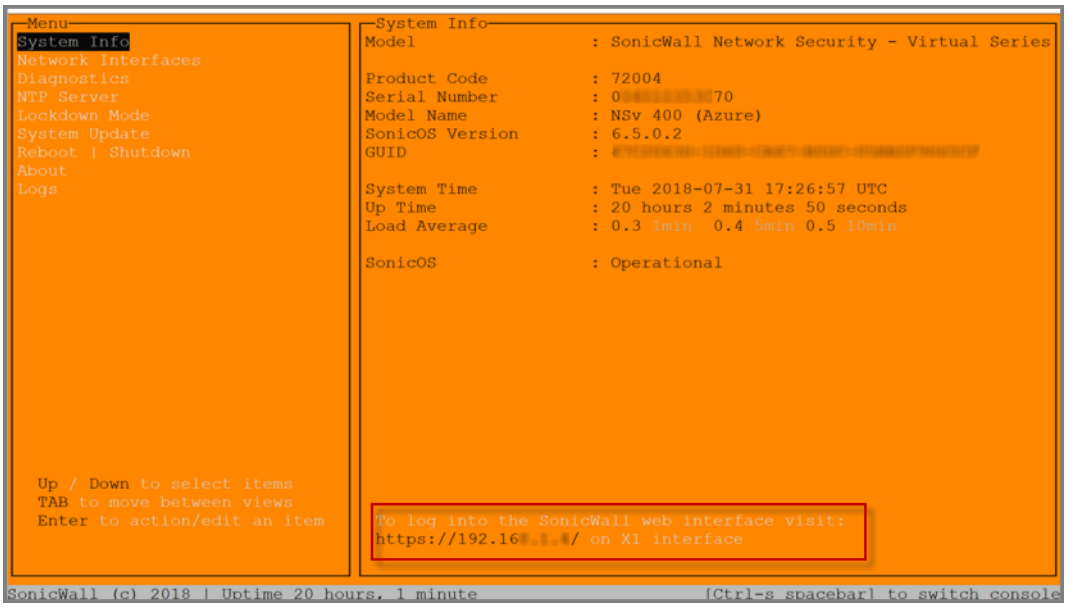


2 In the **Instances** page, locate the public IP address assigned to the NSv and the Instance ID for your NSv.

You can access the SafeMode web interface at the public IP address of the NSv, and you must authenticate to gain access.

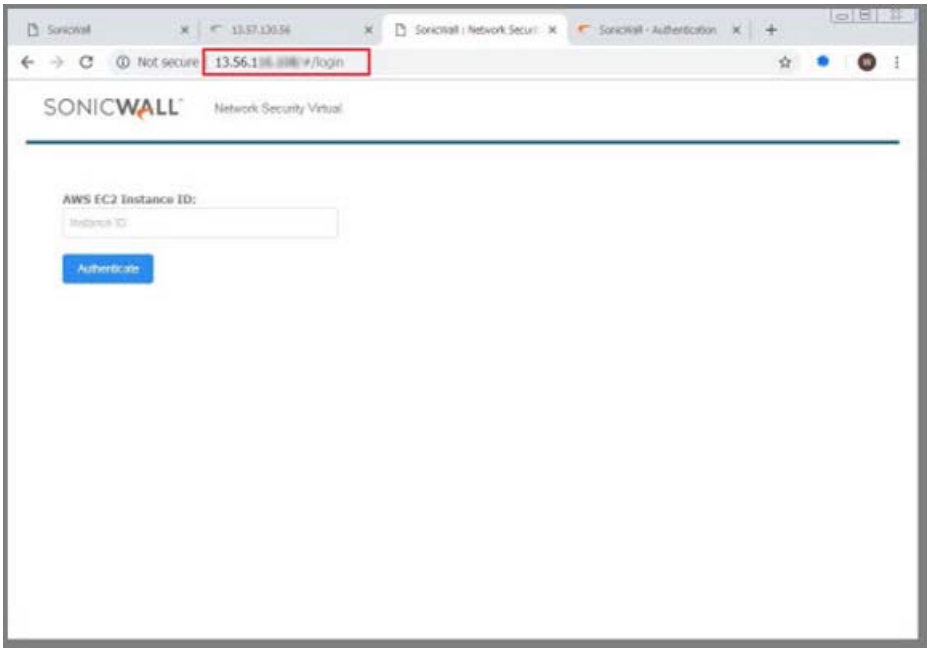
NOTE: In SafeMode, the web management interface is only available via **http** (not **https**).

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



3 Go into the management console and boot into SafeMode. See Entering SafeMode

4 In a web browser, navigate to ***http://<NSv public IP address>***, using the applicable IP address. The SafeMode authentication screen displays.



5 In the **AWS EC2 Instance ID** field, enter the Instance ID for the NSv.

6 Click **Authenticate.** The SafeMode web interface displays.

Entering/Exiting SafeMode

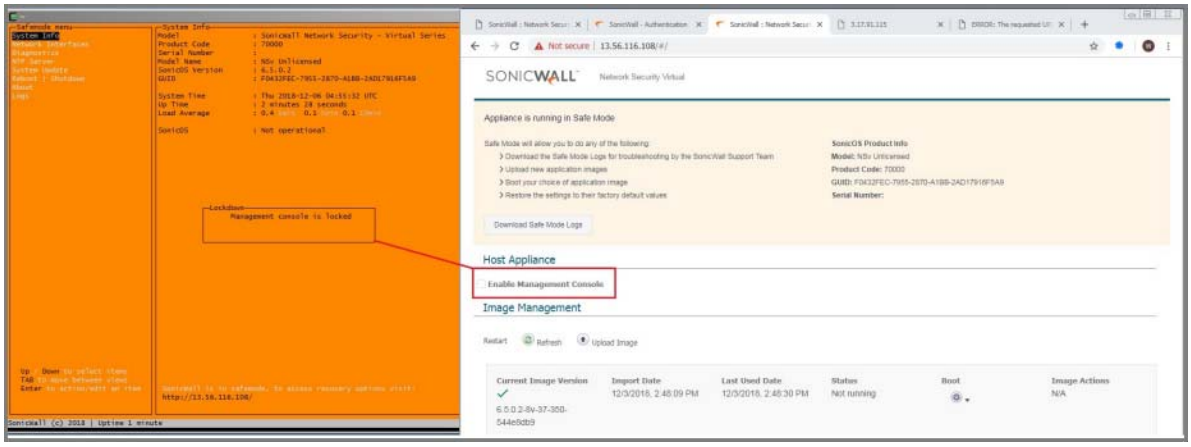
Enter SafeMode as described in Accessing the SafeMode Web Interface.

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

Locking and Unlocking the Management Console

From the management web interface, the management console can be locked an unlocked as shown below.

This locking and unlocking has the same effect as Locking and Unlocking the Management Console.



Downloading the SafeMode Logs

You can download logs of SafeMode activity.

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

To download logs from SafeMode:

1 Access the web interface in SafeMode as described. The SafeMode web management interface displays:

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

Uploading a New Image in SafeMode

SWI files are used to upgrade SonicOS.

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

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

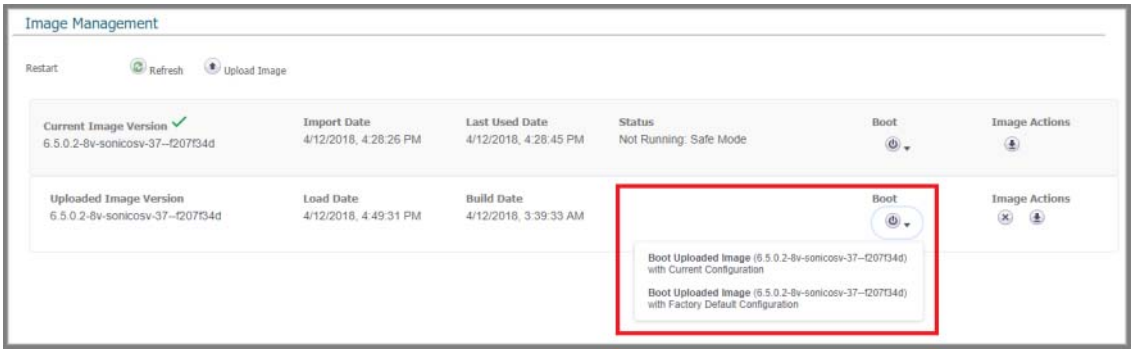
NOTE: In SafeMode, the web management interface is only available via **http** (not **https**).

To install a new SonicOS from SafeMode:

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

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

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



The NS*v* reboots with the new image.

6

SonicWall Support

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

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

The Support Portal enables you to:

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

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

About This Document

Legend

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

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

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

NSv Series on AWS Getting Started Guide
Updated - December 2020
Software version - 6.5.4
232-004956-00 Rev E