SonicOS 7

NSv Getting Started Guide

for AWS

SONICWALL®

Contents

1

Introducing the NSv Series

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

The basic configuration information is provided for standard AWS cloud servers and on AWS government cloud servers.

ⓘ **NOTE:** To deploy an NSv running SonicOS 6.5.4.v, refer to Deploying Previous Versions Of NSv On AWS and the NSv 6.5.4 Getting Started Guide.

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

ⓘ **IMPORTANT:** You might 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. Regardless of the pricing model choice, you can go to Installing SonicOS on the NSv Series to start. Separate instructions for different pricing models are given in Licensing and Registering Your NSv.

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

SonicWall® NSv series firewalls support both ***Classic*** mode and ***Policy*** mode. Selection of or changing between ***Classic*** and ***Policy*** modes is supported on NSv series from SonicOS 7.0.1 pnwards. For more information on supported or unsupported feature list refer to the Feature Support Information section and changing between ***Classic*** and ***Policy*** modes is supported on NSv series refer to the *About SonicOS 7 for the TZ, NSa, NSv, and NSsp Series Features Specific to NSv* guide in https://www.sonicwall.com/support/technical-documentation.

Topics:

Feature Support Information

NOTE: The AWS VPC does not support Layer 2 functionality. Therefore, the NSv interface to VPCs is restricted to the layer 3 network level and higher.

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

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

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

FEATURE SUPPORT LIST

Functional Category	Feature Area	Feature
Unified Security Policy	**Unified Policy combining Layer 4 to Layer 3 Rules**	Source/Destination IP/Port/Service
		Application based Control
		CFS/Web Filtering
		Botnet
		Geo-IP/country
		Single Pass Security
		Services enforcement
		Decryption Policy
		DoS Policy
		EndPoint Security Policy
		Rule Diagram
	Profile Based Objects	
		Endpoint Security
		Bandwidth Management
		QoS Marking
		Content Filter
		Intrusion Prevention
		DHCP Option
		AWS VPN
	Action Profiles	
		Security Profile

Functional Category	Feature Area	Feature
		DoS Profile
	Signature Objects	
		AntiVirus Signature Object
		AntiSpyware Signature Object
	Rule Management	
		Cloning
		Shadow rule analysis
		In-cell editing
		Group editing
		Export of Rules
		LiveCounters
	Managing Views	
		Used/unused rules
		Active/inactive rules
		Sections
		Customizable Grid/Layout
		Custom Grouping
TLS 1.3	**Supporting TLS 1.3 with enhanced security**	
SDWAN	**SDWAN Scalability**	
	SDWAN Usability Wizard	
API	**API Driven Management**	
	Full API Support	
Dashboard	**Enhanced Home Page**	
		Actionable Dashboard
		Enhanced Device View
		Top Traffic and User summary
		Insights to threats
		Policy/Object Overview
		Profiles and Signatures Overview
		Zero-Day Attack Origin Analysis

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

Product Matrix and Requirements

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

Product Models	NSv 270	NSv 470	NSv 870
Maximum Cores[1]	2	4	8
Minimum Total Cores	2	4	8
Management Cores	1	1	1
Maximum Data Plane Cores	1	3	7

Product Models	NSv 270	NSv 470	NSv 870
Minimum Data Plane Cores	1	1	1
Network Interfaces	8	10	12
Supported IP/Nodes	Unlimited	Unlimited	Unlimited
Minimum Memory Required [2]	4G	8G	10G
Minimum Hard Disk/Storage	50G	50G	50G

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

MEMORY REQUIREMENTS ON NSV WITH JUMBO FRAMES ENABLED VS DISABLED

NSv Model	Minimum Memory – Jumbo Frames Enabled	Minimum Memory – Jumbo Frames Disabled
NSv 270	6G	4G
NSv 470	10G	8G
NSv 870	14G	10G

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

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

Backup and Recovery Information

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

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Contact SonicWall Technical Support for assistance.
- If the disk is not recoverable, then the NSv virtual machine needs to be deregistered with MySonicWall. Contact technical support for more information.
- If SonicOS does not boot up, you can go into SafeMode and download the log files, upload a new SonicOS image, or take other actions. For more information about SafeMode, see Using SafeMode on the NSv.
- If SonicOS fails three times during the boot process, it boots into SafeMode. Verify that the minimum required memory is available and allocated based on the NSv model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall Technical Support for assistance.

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

Exporting and Importing Firewall Configurations

Moving configuration settings from SonicWall physical appliances to the NSv is not supported. However, configuration settings can be moved from one SonicOS 7 NSv to another or from an NSv running SonicOS 6.5.4.4 to an NSv running SonicOS 7.0.1 or higher (but not SonicOSX).

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

Github Repository

SonicWall NSv templates are available in the Github repository:

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

Upgrading from SonicOS 6.5

- SONICWALL NSV 270 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 470 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 870 SECURE UPGRADE VIRTUAL APPLIANCE ONLY NO ATTACHED SUBSCRIPTION (EXISTING SONICWALL CUSTOMERS ONLY)
- SONICWALL NSV 270 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 470 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)
- SONICWALL NSV 870 SECURE UPGRADE PLUS ESSENTIAL EDITION (2YR, 3YR, or 5YR)

SonicOS 7 NSv supports SWI upgrades from SonicOS 7.0.0 to 7.0.1 in Policy Mode, and fresh deployments of 7.0.0 and 7.0.1. Starting with SonicOS 7.0.1, NSv virtual machines support both Classic Mode (SonicOS) and Policy Mode (SonicOS).

Settings from SonicOS 6.5 NSv installations can be imported into an NSv running 7.0.1 in Classic Mode.

SonicOS 6.5 configuration settings cannot be imported into an NSv running in Policy Mode. In this case, users must manually navigate and configure policies, application rules, and content filtering rules for SonicOS 7 NSv installations. Note that there are console, API, and web management approaches to completing these configurations.

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

1. Purchase a Secure Upgrade license key.
2. Log into MySonicWall and register the Secure Upgrade serial number. Enter a descriptive "friendly" name in the available field, shown here as "SecureUpgrade1."
3. Click **Choose management options**.
4. In the **Secure Upgrade** popup window, select **Register Only** at the top.
5. Select the Trade-In Unit from the list of registered NSv instances. This is the SonicOS 6.5.4.v NSv instance to be upgraded to SonicOS 7.
6. Click **Done** after selecting the Trade-In Unit. The Secure Upgrade serial number is then registered to your MySonicWall account.
7. The action item Secure Upgrade Transfer is added to the To do list at the bottom of the page.

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

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

   ⓘ **NOTE:** If you do not perform the service transfer within 60 days, the transfer is performed automatically.
8. Deploy a new SonicOS 7 NSv instance with the desired model and platform.
9. Register the SonicOS 7 NSv using the **Secure Upgrade** serial number. When prompted to select either Classic mode or Policy mode, select Classic mode. Classic mode supports configuration settings imported from a SonicOS 6.5.4.v NSv.

   Registration initiates a 60-day countdown at the end of which the SonicOS 6.5.4.v NSv is deregistered, completing the Secure Upgrade Transfer.
10. Log into the SonicOS 6.5.4.v NSv and export the configuration settings to a file on your management computer.
11. Using the migration tool (https://migratetool.global.sonicwall.com/), migrate the SonicOS 6 NSv preferences to SonicOS 7 NSv model.
12. Log into SonicOS 7 NSv and import the configuration settings file.

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

Upgrading to a Higher Capacity NSv Model

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

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

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

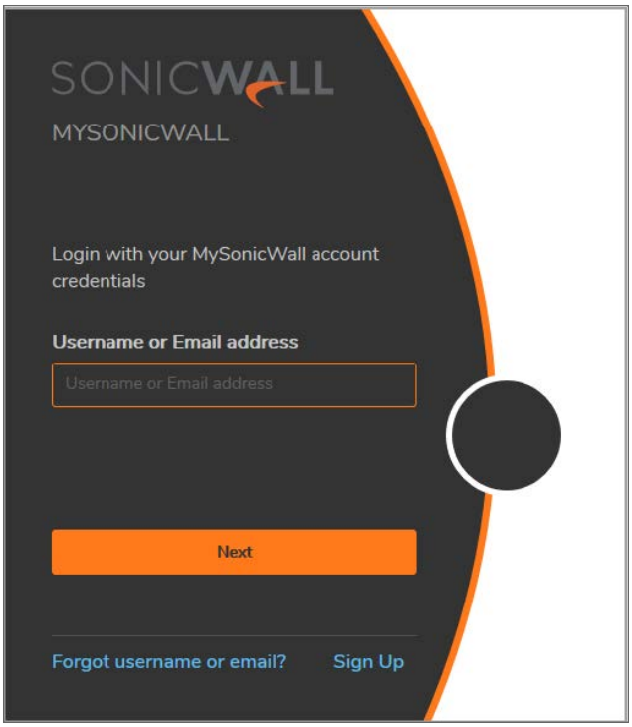
Creating a MySonicWall Account

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

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

To create a MySonicWall account:

1. In your web browser, navigate to https://www.mysonicwall.com.
2. In the login screen, click the **Sign Up** link.



3. Complete the account information, including email and password.
4. Enable two-factor authentication if desired.
5. If you enabled two-factor authentication, select one of the following authentication methods:
   - **Email (one-time passcode)** where an email with a one-time passcode is sent each time you log into your MySonicWall account.

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

6. Click **Continue** to go to the **COMPANY** page.
7. Complete the company information and click **Continue**.
8. On the **YOUR INFO** page, select whether you want to receive security renewal emails.
9. Identify whether you are interested in beta testing of new products.
10. Click **Continue** to go to the **EXTRAS** page.
11. Select whether you want to add additional contacts to be notified for contract renewals.
12. If you opted for additional contacts, input the information and click **Add Contact**.
13. Click **Finish**.
14. Check your email for a verification code and enter it in the **Verification Code** field. If you did not receive a code, contact Customer Support by clicking on the link.
15. Click **Done**. You are returned to the login window so you can login into MySonicWall with your new account.

2

Installing SonicOS on the NSv Series

Topics:

Supported NSv Models

Determine the NSv instance type required before starting installation.

CURRENTLY SUPPORTED AWS SIZE MODELS (VIRTUAL MACHINE SIZES)

SonicWall NSv Model	AWS Instance Type Size	Core Count	Maximum Network Interfaces Count[1]
NSv 270	c5.large	2	3
NSv 470	c5.xlarge	4	4
NSv 870	c5.2xlarge	8	4

NEWLY SUPPORTED SIZES (VIRTUAL MACHINE SIZES)

SonicWall NSv Model	AWS Instance Type Size	Core Count	Maximum Network Interfaces Count
NSv 270	c5n.large	2	3
	c5d.large		
	m5.large		
	m5n.large		
NSv 470	c5n.xlarge	4	4
	c5d.xlarge		
	m5.xlarge		
	m5n.2xlarge		
NSv 870	c5n.2xlarge	8	4
	c5d.2xlarge		
	m5.2xlarge		
	m5n.2xlarge		

NOTE: The maximum number of NICs supported by SonicWall NSv is always eight for all models. But the total number of interfaces in an NSv instance could be constrained by the selected Azure size model.

NOTE: Standard_B server size serves only lab firewall so should be deployed with caution for production networks.

1

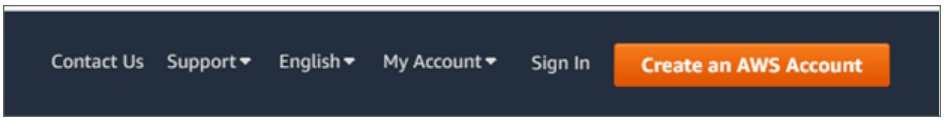
The maximum number of interfaces supported on an NSv instance is defined by the type of AWS virtual machine. For example, if more than two interfaces are required for an NSv 270, then use the NSv options with an AWS virtual machine supporting a higher number of interfaces.

The maximum number of NICs supported by SonicWall NSv is always eight for all models. But the total number of interfaces in an AWS instance maybe constrained by the AWS virtual machine. Do select the instance size accordingly.

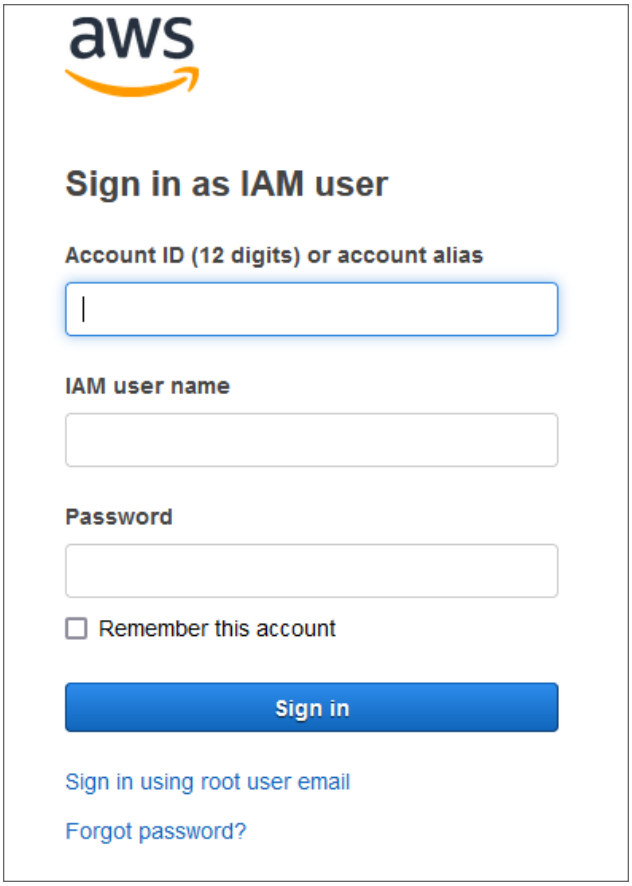
Resizing NSv Virtual Machine

The process of resizing a NSv AWS virtual machine is summarized in the below steps:

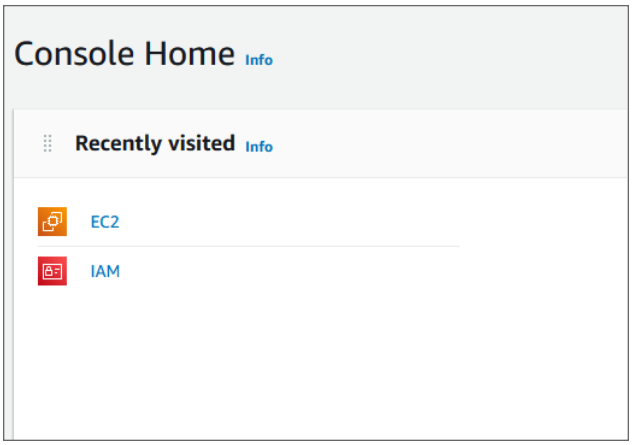
1. Log in to AWS console https://aws.amazon.com/console/ .
2. Click **Sign In** to the console.



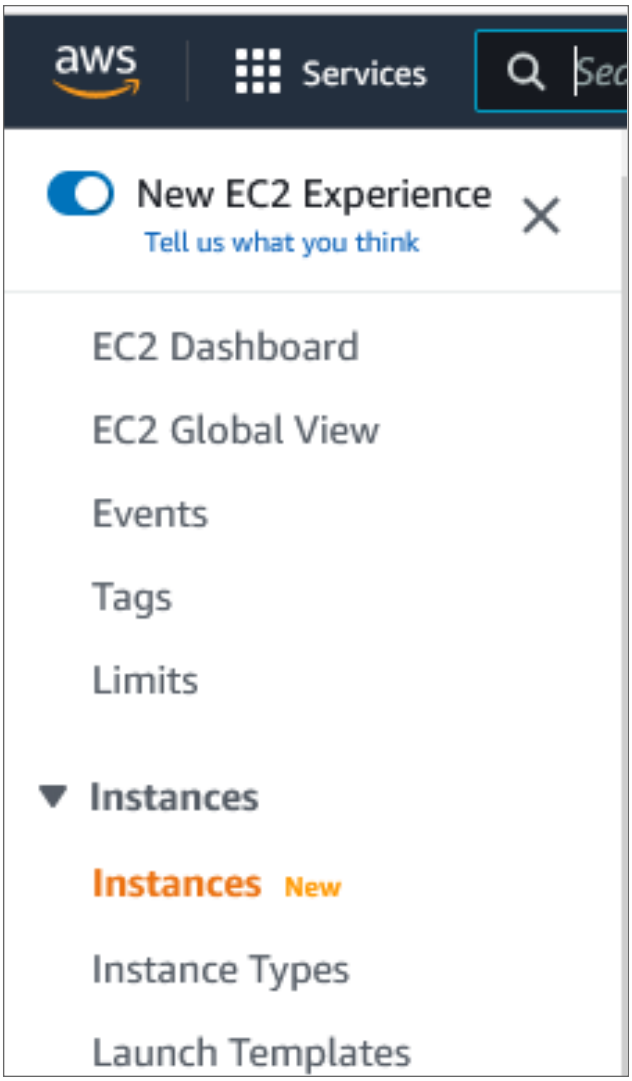
3. Fill in the details for successful sign in.



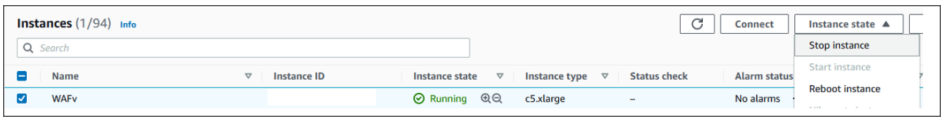
4. Click on **EC2**.



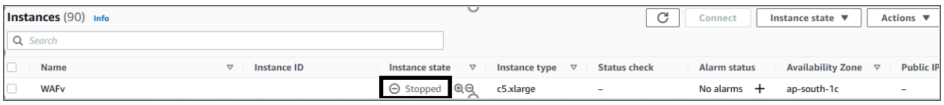
5. Under **Instances**, click on **Instances**. It will display all the running/poweroff instances.

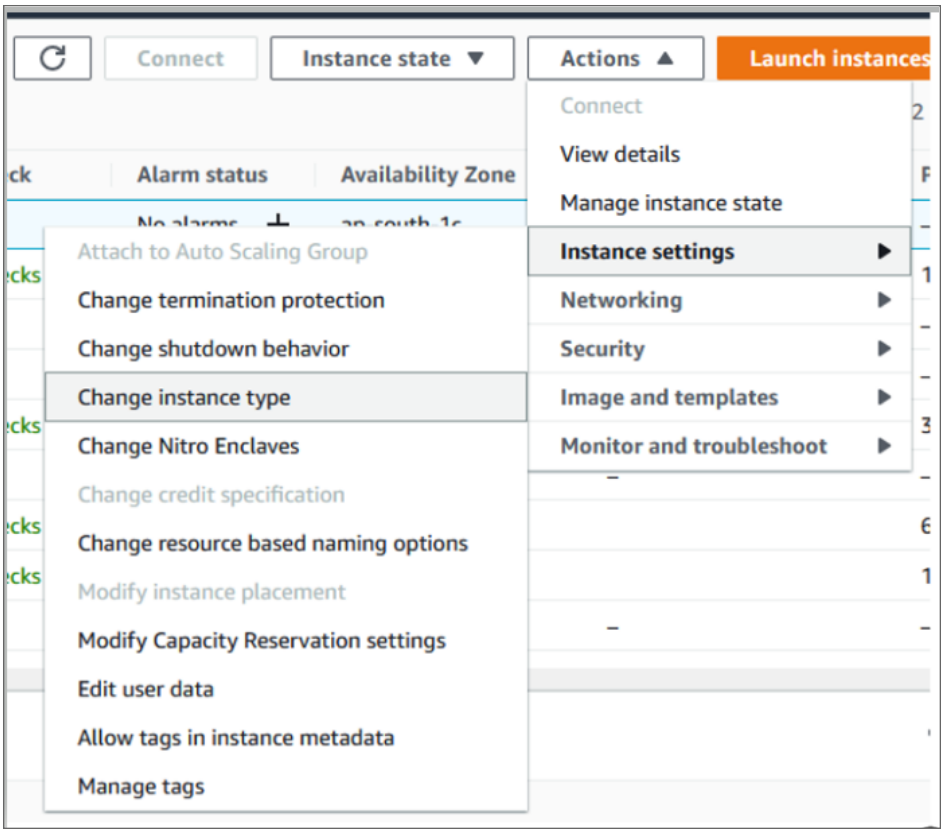


6. Select the instance and then click on **Instance state > Stop instance**.

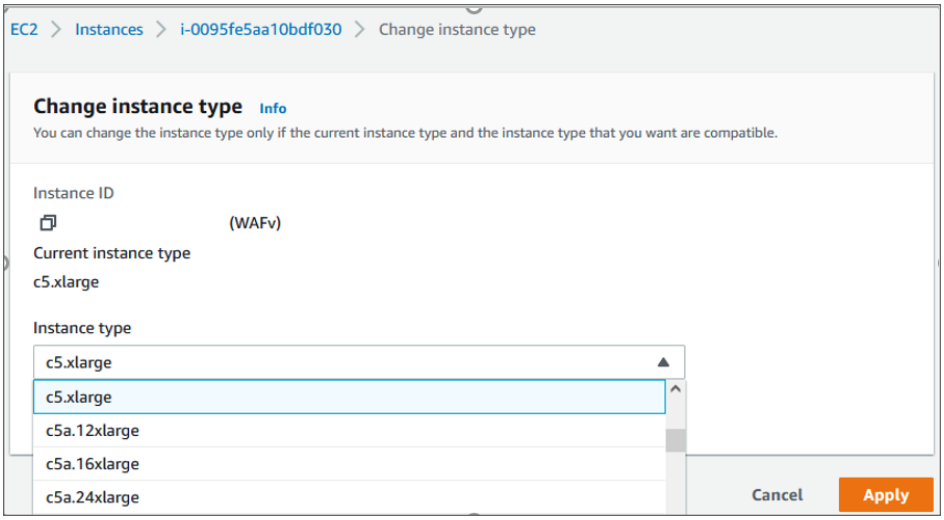


7. After the **Instance state** displays Stopped, click on **Actions > Instance settings > Change instance type**.





8. Select the instance type and click on **Apply**.



ⓘ **NOTE:** Resizing of NSv is only required if user already has an existing NSv running on previous instance sizes. For new deployments, user can select the required instance size from AWS marketplace directly.

Task List for NSv Instance Setup

1. Deploy a new VPC with NSv from the AWS Console
    - Deploying AWS from Console

OR:

1. Deploy NSv to an existing VPC with AWS Cloud Formation Templates
    - Deploying AWS from Cloud Template

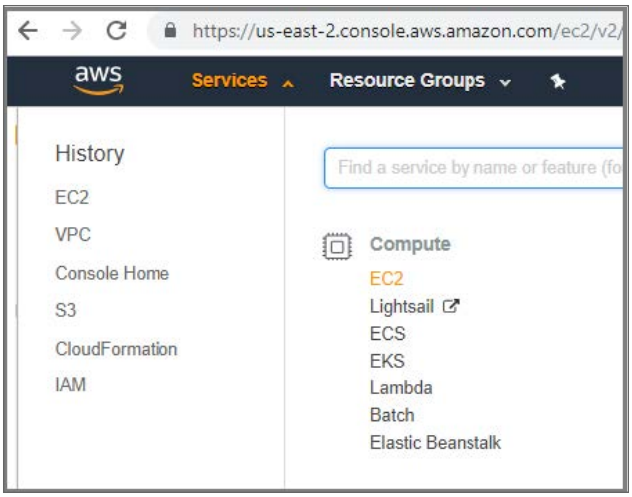
THEN:

2. Register the NSv on MySonicWall
    - Licensing and Registering Your NSv
3. Configure Traffic Forwarding to the NSv
    - Forwarding Traffic to Your NSv

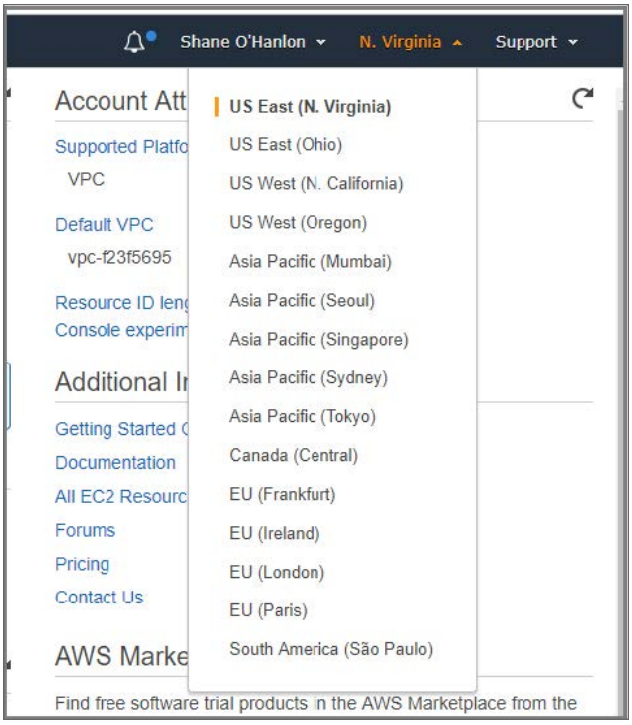
Deploying AWS from Console

To deploy NSv from the 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.



d. Select the AWS region into which you want to deploy.

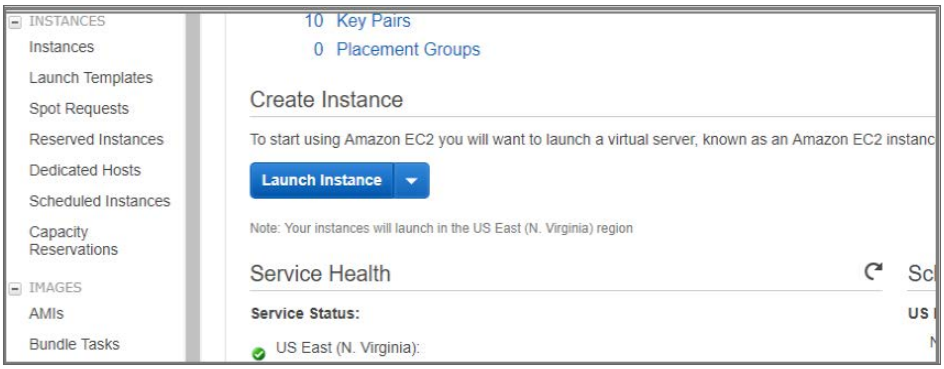


2. Configure a VPC

   The virtual machine can be deployed on a new or existing VPC. Refer to the AWS documentation on how to create a VPC at: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html.

3. Follow these steps to launch the SonicWall NSv:

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



   b. From the menu click **AWS Marketplace** and enter `SonicWall NSv` into the **Search** box.

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

   ⓘ | **NOTE:** This procedure applies to both BYOL and PAYG installations.

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

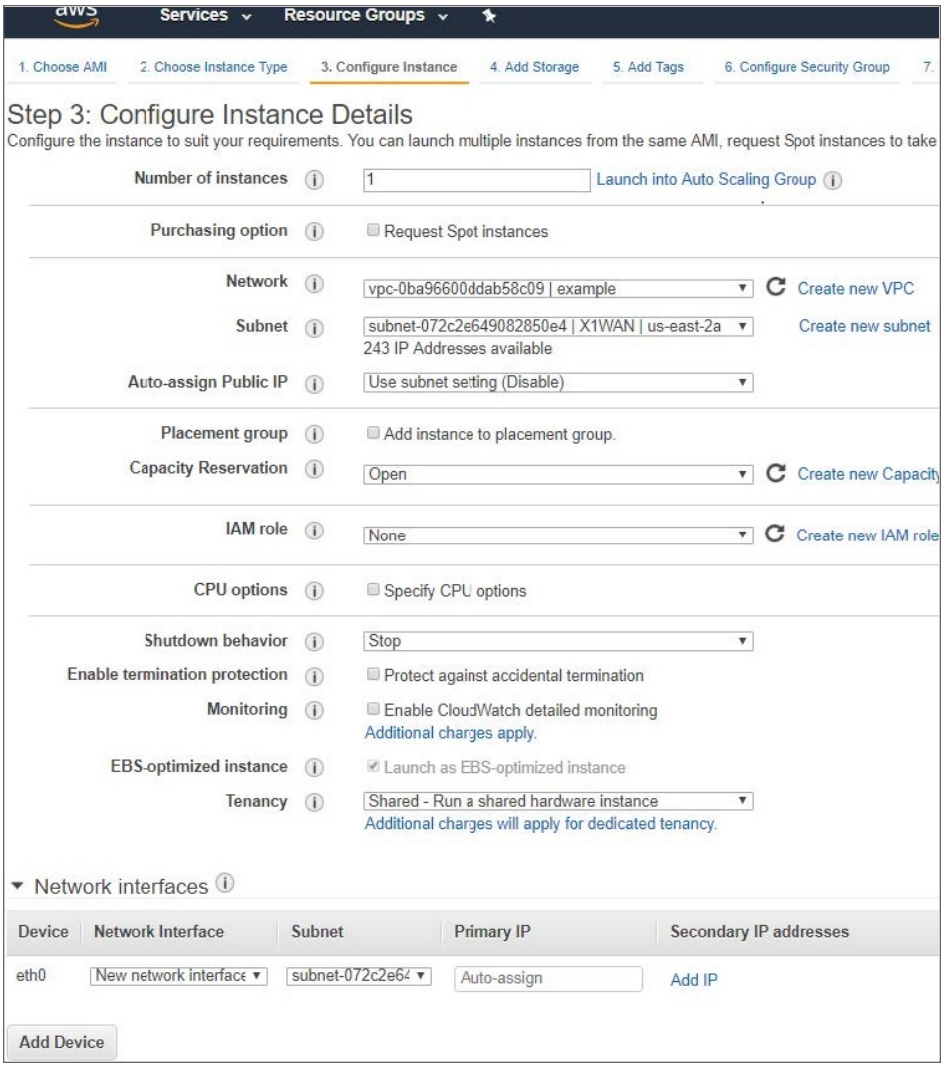
For guidance, refer to Product Matrix and Requirements and Supported NSv Series Models on AWS. Choose instance size from the table displayed:

■	Compute optimized	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
☐	Compute optimized	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
☐	Compute optimized	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
☐	Compute optimized	c5.4xlarge	16	32	EBS only	Yes	Up to 10 Gigabit	Yes

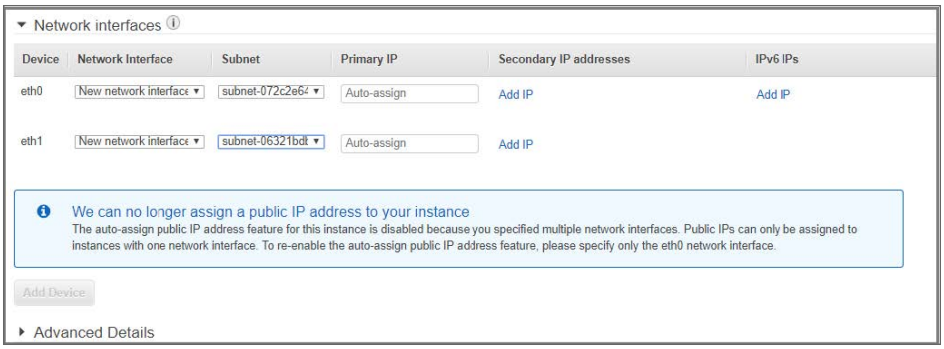
NSV MODELS AND IMAGE TYPES

SonicWall NSv Model	NSv EC2 Instance Type
NSv 270	c5.large
NSv 470	c5.xlarge
NSv 870	c5.2xlarge

e. Click **Configure Instance Details**. From the **Network** drop-down menu select a VPC to deploy the virtual machine on. Select the subnet that is to be the public or WAN interface (X1) of the virtual machine.



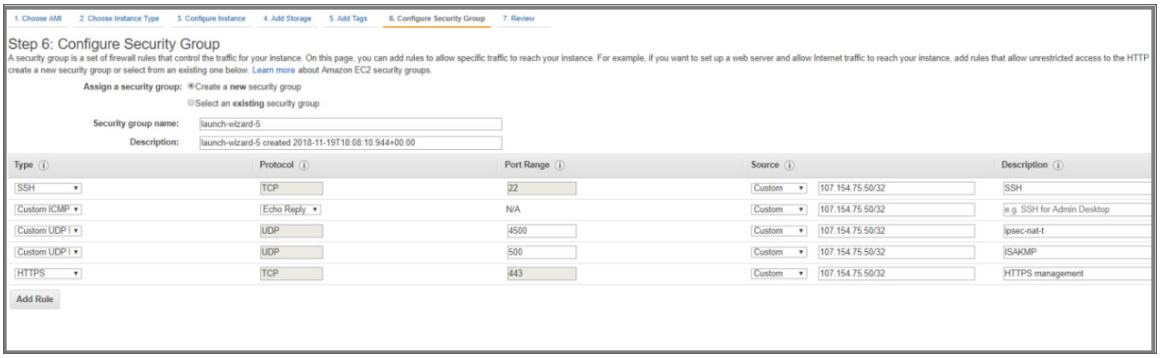
f. To add additional Elastic Network Interfaces click **Add Device**. The virtual machine MUST at minimum have two ENI attached. The ENI interfaces MUST be on separate subnets and both subnets must be in the same ***Availability Zone***. If these subnets are not in the same ***Availability Zone*** you will not see the subnet you have planned to use for ENI *eth1* in the **Subnet** drop-down menu. The *eth0* ENI device is connected to the SonicWall NSv X1 interface that is the public interface. The *eth1* ENI device is connected to the SonicWall NSv X0 interface that is the private interface.



g. Accept the default storage options by clicking **Add Storage**.

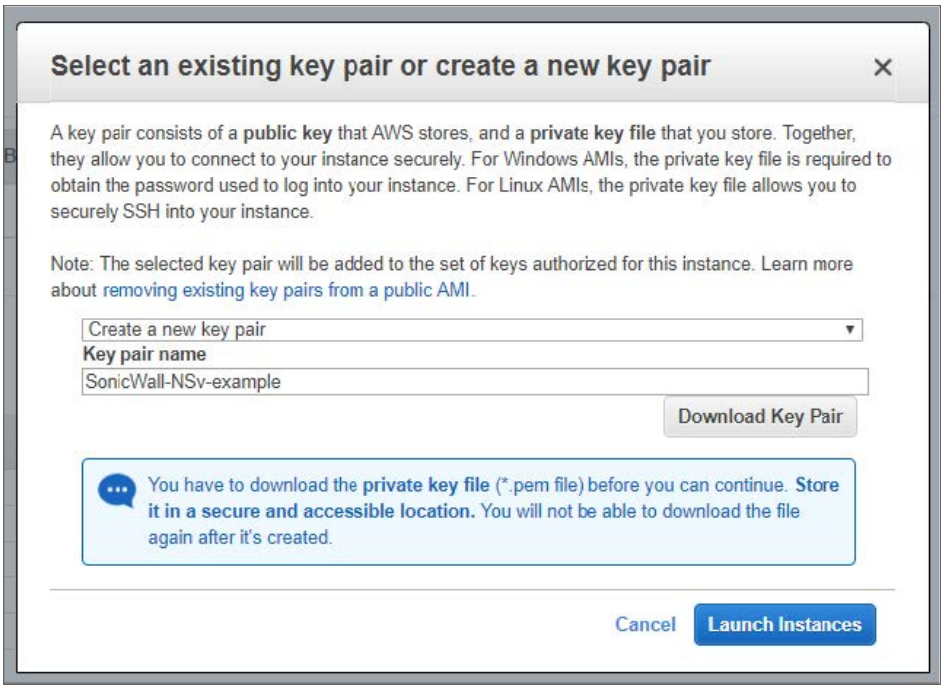
h. Click **Add tags**. Add metadata to the instance configuration to assist in identifying the SonicWall NSv instance.

i. Click **Configure Security Group**. At minimum, allow SSH and HTTPS from a predefined source.



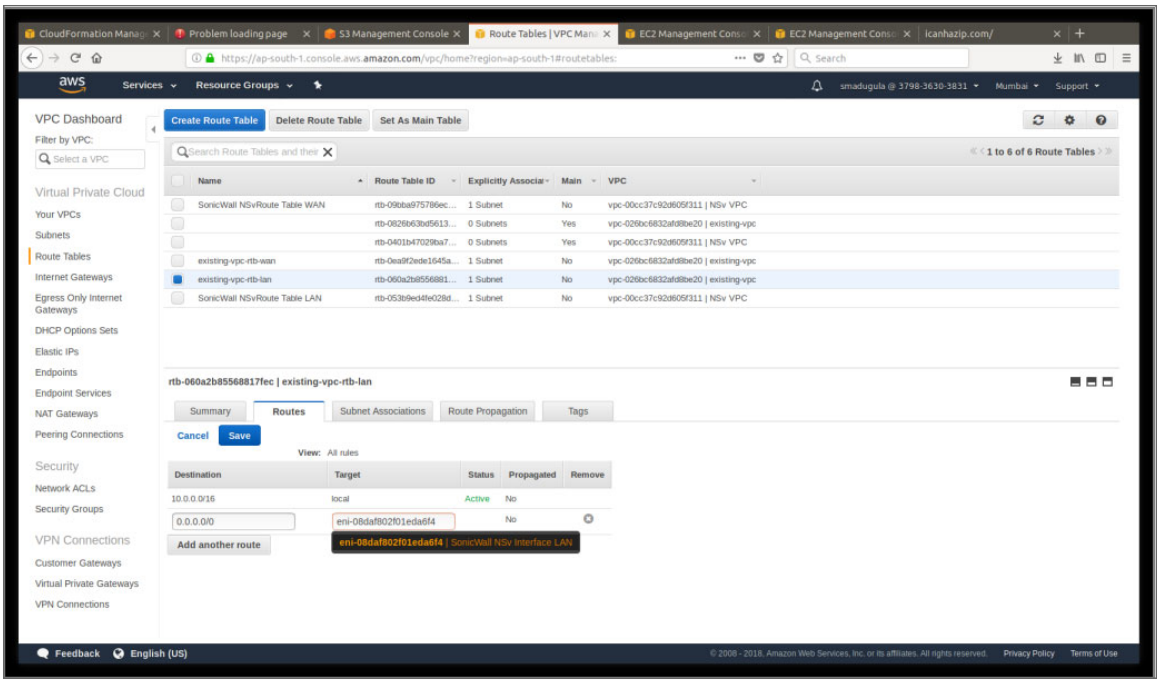
j. Click **Review** and **Launch**. Review the instance details.

k. Click **Launch**. You are prompted to select either **Key-Pair** or **Create a new key pair**. Ensure you have access to the key pair.

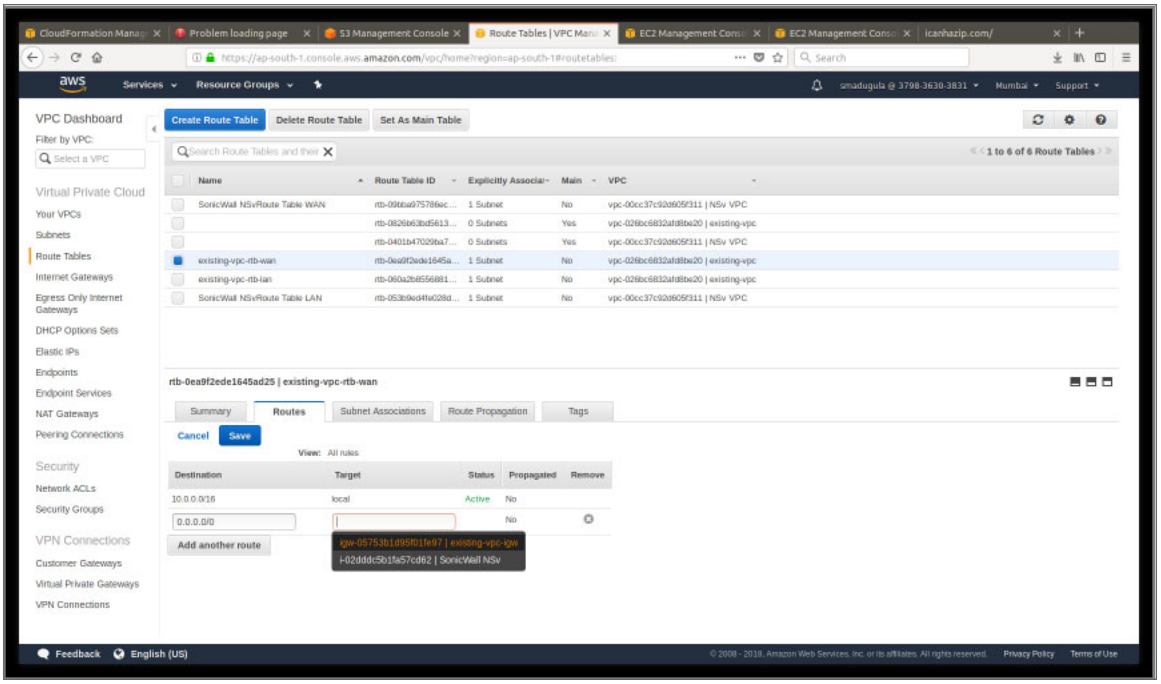


   l. Click **Launch Instances** to deploy the SonicWall NSv instance. Deployment takes between 5 to 8 minutes. You can monitor the progress by viewing the instance in the EC2 Dashboard.

4. Disable source/destination checking:
   a. Select **Network interfaces** on the **Networking** tab.
   b. Choose the interface ID to go to the network interfaces page.
   c. Select **Choose Actions, Networking, Change source/destination check**.
   d. Clear the **Enable** , and click **Save**.
5. Change Routing Tables:
   a. Change your LAN routing table to add a route with **Destination** `0.0.0.0/0` with **Target** to NSv's LAN Interface. This routes all your LAN traffic to the NSv X0 interface.



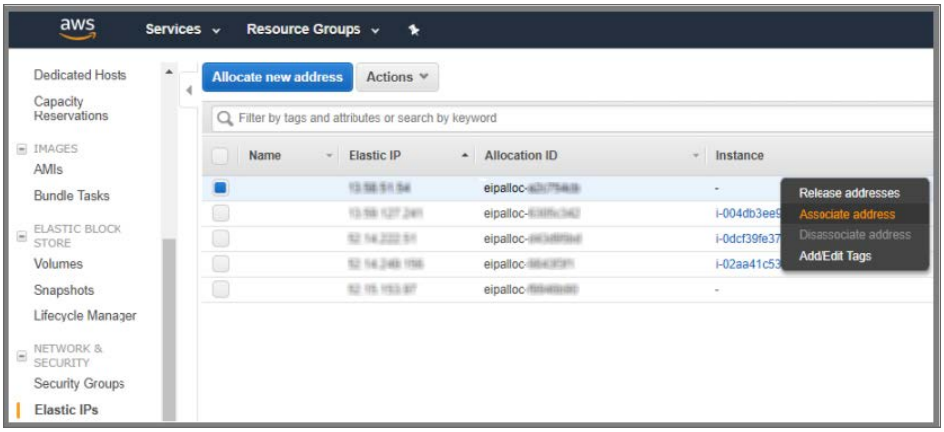
b. Change your WAN routing table to add a route with **Destination** `0.0.0.0/0` with **Target** to your Internet Gateway (igw-xxxxx). This route's NSv WAN traffic to the Internet Gateway (IGW).



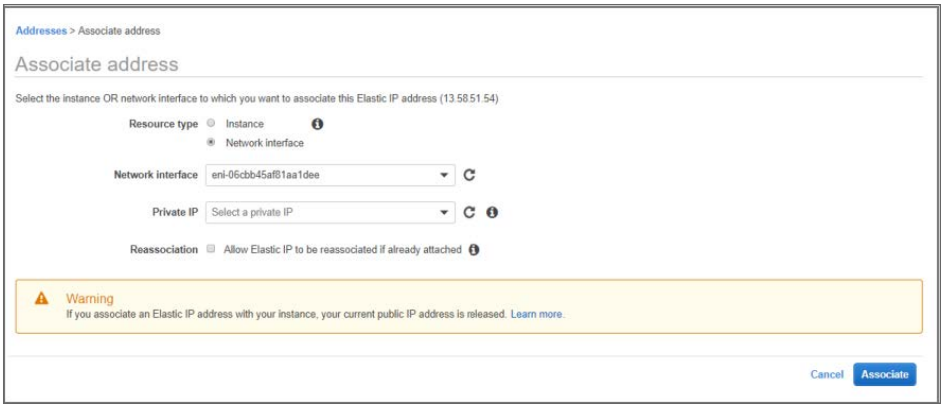
6. To assign an Elastic IP, follow these steps:

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

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



c. Choose the **Resource type** and **Network Interface**. From the **Network Interface** drop-down menu, 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 NSv web management interface.

7. Connect to the virtual machine web management interface:

   a. Now that you have associated an Elastic IP to the SonicWall NSv instance, you are able to connect to the web management interface by entering the IP address into your browser.

b. Enter the username ***admin*** and the password, which is the AWS instance ID of the newly created SonicWall NSv instance such as i-02axxxxxxxxxxxxx given by your SonicWall representative.

After logging in you should proceed to registering your SonicWall NSv virtual machine, see Licensing and Registering Your NSv.

Deploying AWS from Cloud Template

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

Prerequisites include:

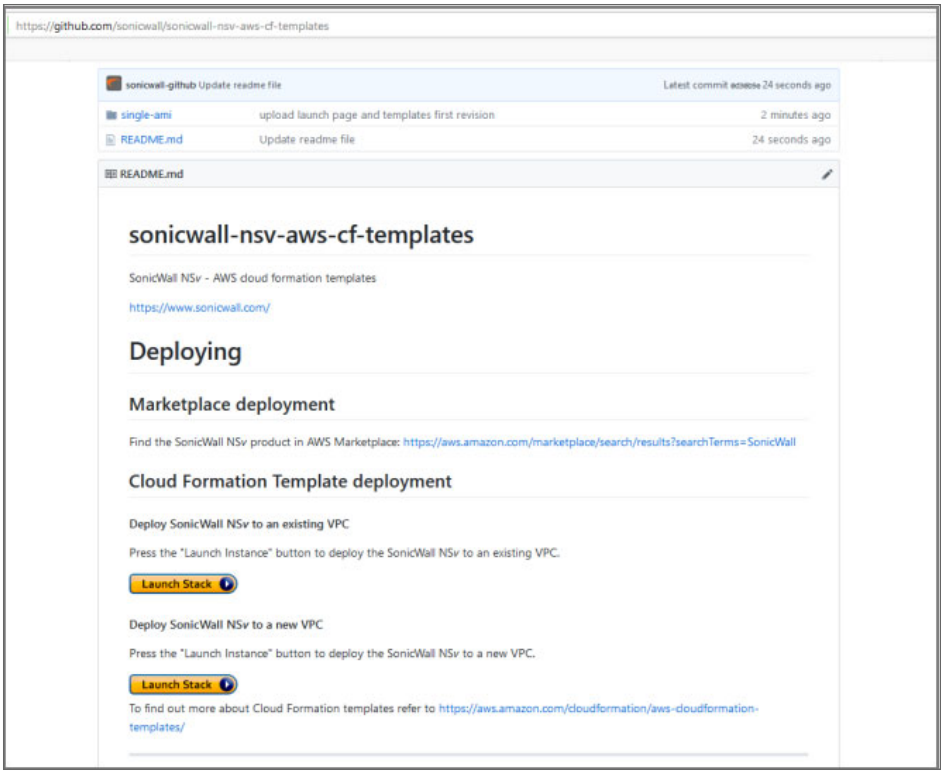
- AMI ID of NSv
- A key pair
- A VPC with:

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.

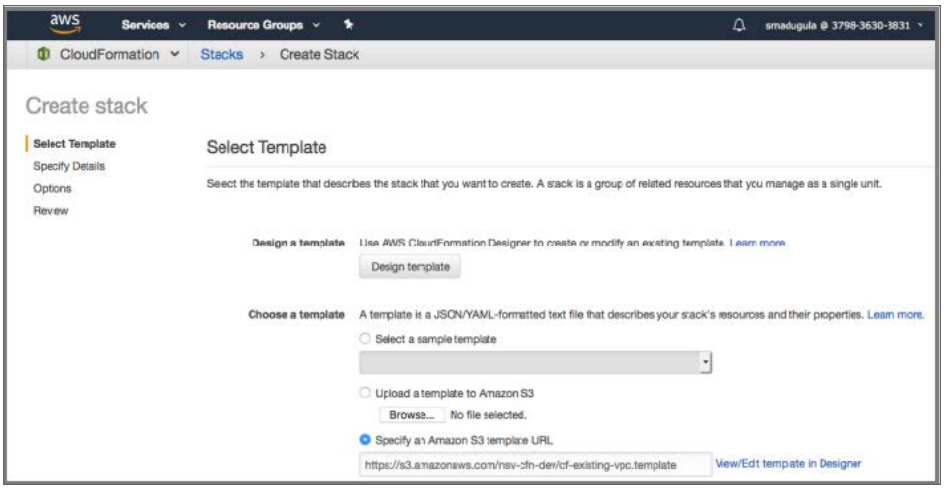
Populate the routing tables after the stack has been deployed successfully.

Steps:

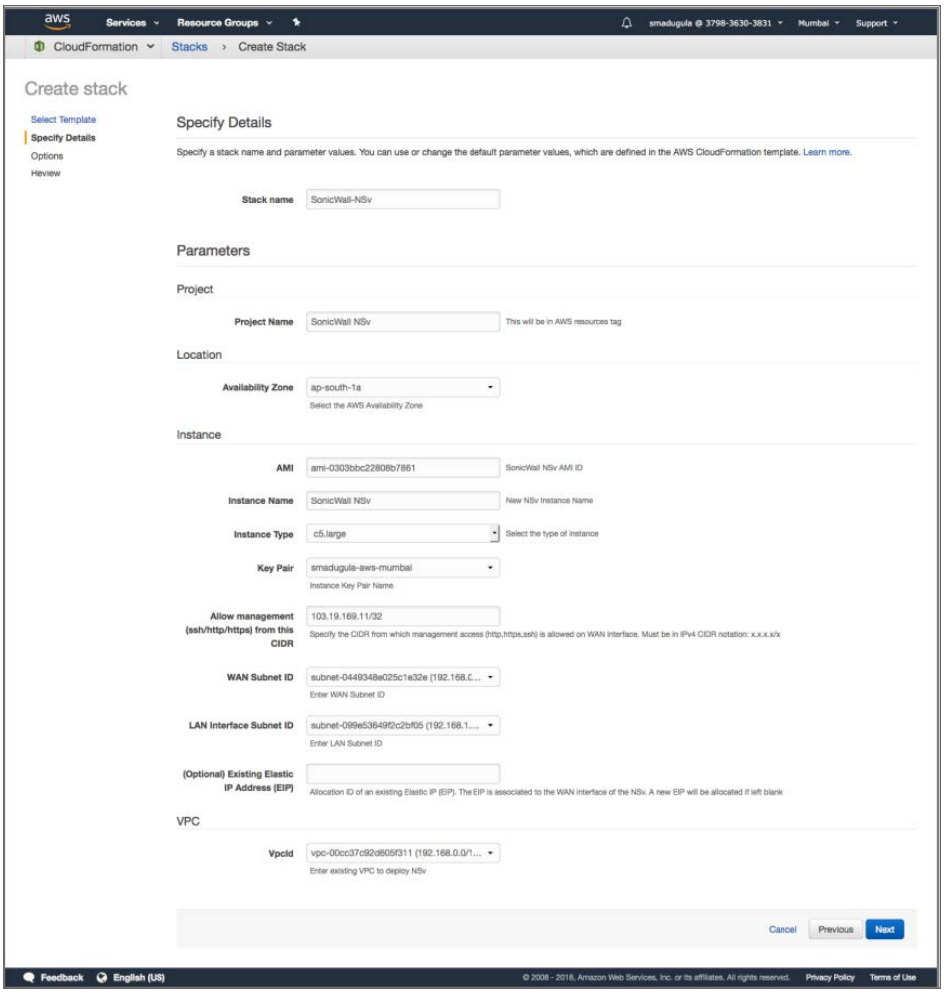
1. Go to: https://github.com/sonicwall/sonicwall-nsv-aws-cf-templates
2. Click **Launch Stack** following the **Deploy SonicWall NSv to an existing VPC**.



3. To select a Region, identify the region into which you wish to deploy NSv.
   ⓘ | **NOTE:** You must copy the AMI to the chosen region and have its ID ready.
4. Click **Launch Stack** under **Deploy NSv in existing VPC**.


aws
Services
Resource Groups
smadugula @ 3798-3630-3831
CloudFormation
Stacks
Create Stack
Create stack
Select Template
Specify Details
Options
Review
Select Template
Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.
Design a template
Design template
Choose a template
A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.
Select a sample template
Upload a template to Amazon S3
Browse...
No file selected.
Specify an Amazon S3 template URL
https://s3.amazonaws.com/nsv-cfn-dev/cf-existing-vpc.template
View/Edit template in Designer

5. Click **Next**.


aws
Services
Resource Groups
smadugula @ 3798-3630-3831
Mumbai
Support
CloudFormation
Stacks
Create Stack
Create stack
Select Template
Specify Details
Options
Review
Specify Details
Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.
Stack name
SonicWall-NSv
Parameters
Project
Project Name
SonicWall NSv
This will be in AWS resources tag
Location
Availability Zone
ap-south-1a
Select the AWS Availability Zone
Instance
AMI
ami-0303bbc22808b7861
SonicWall NSv AMI ID
Instance Name
SonicWall NSv
New NSv Instance Name
Instance Type
c5.large
Select the type of instance
Key Pair
smadugula-aws-mumbai
Instance Key Pair Name
Allow management (ssh/http/https) from this CIDR
103.19.169.11/32
Specify the CIDR from which management access (http,https,ssh) is allowed on WAN interface. Must be in IPv4 CIDR notation: x.x.x.x/x
WAN Subnet ID
subnet-0449348e025c1e32e (192.168.0...
Enter WAN Subnet ID
LAN Interface Subnet ID
subnet-099e53649f2c2bf05 (192.168.1...
Enter LAN Subnet ID
(Optional) Existing Elastic IP Address (EIP)
Allocation ID of an existing Elastic IP (EIP). The EIP is associated to the WAN interface of the NSv. A new EIP will be allocated if left blank
VPC
VpcId
vpc-00cc37c92d605f311 (192.168.0.0/1...
Enter existing VPC to deploy NSv
Cancel
Previous
Next
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

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 that is added to the resources tag.
   - **Location**

   Availability Zone: Select the Availability Zone into which NSv 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.

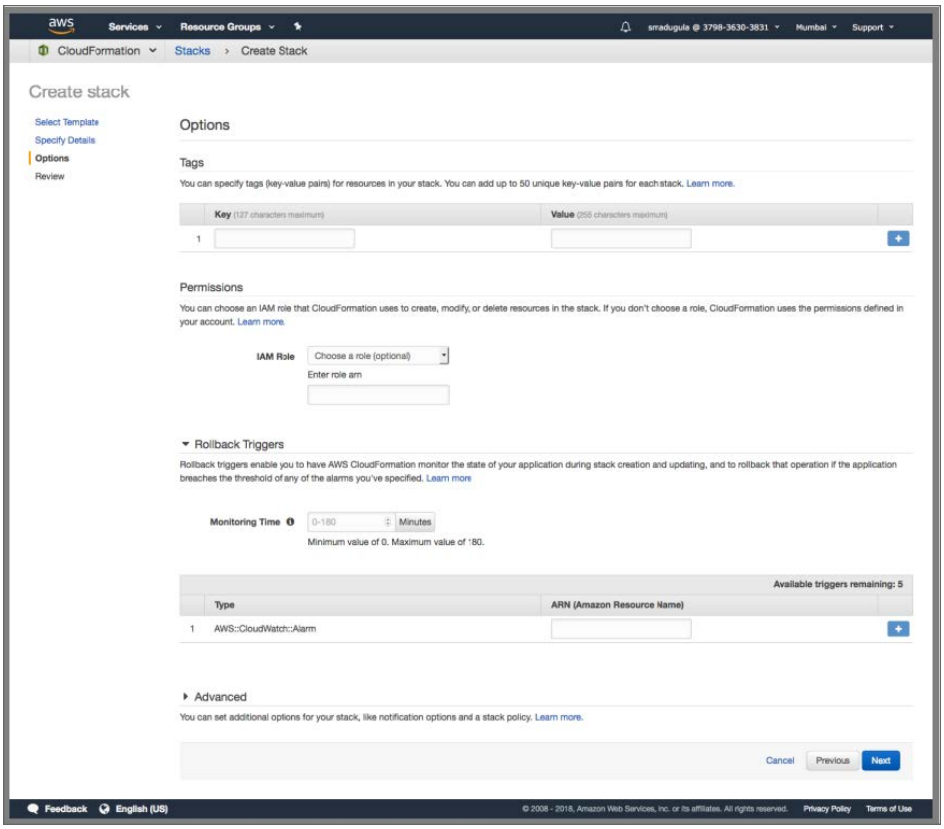
     Allow management (ssh/http/https) from this CIDR: Specify the IP address from which management access is allowed on the WAN interface. Must be in IPv4 CIDR notation `x.x.x.x/x`. Open HTTP, HTTPS, and SSH ports for this address in the Ingress Security Group.

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

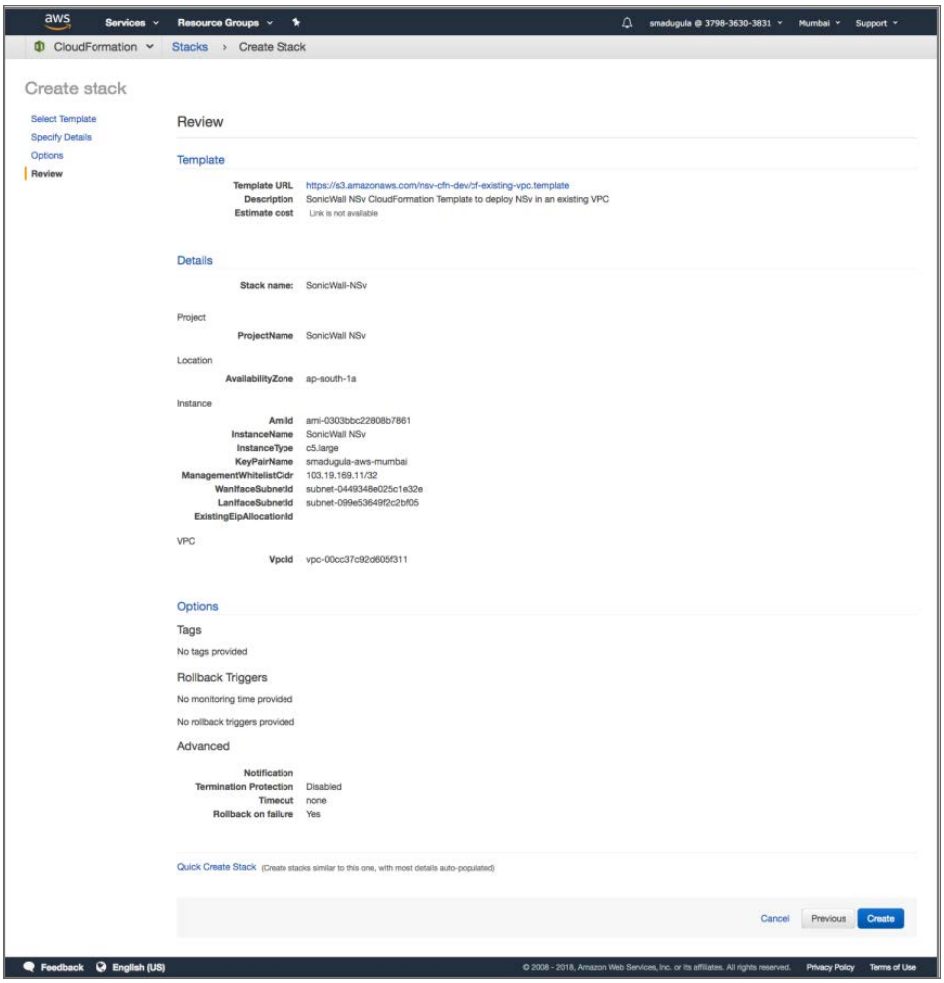
     LAN Interface Subnet ID: Select the subnet id for your LAN interface.

     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 NSv. If this field is left blank, the system allocates a new EIP.
   - **VPC**

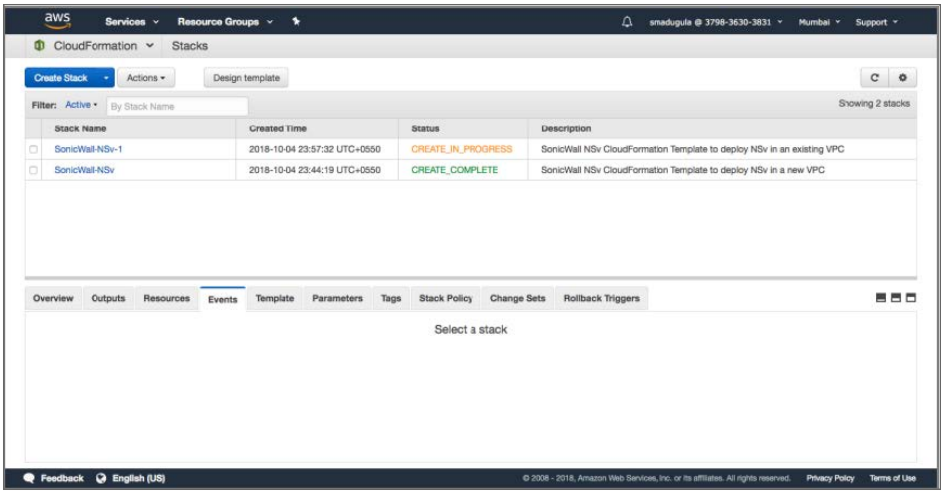
     VpcId: Select existing VPC to which to deploy NSv.
8. Click **Next**.


aws
Services
Resource Groups
smadugula @ 3798-3630-3831
Mumbai
Support
CloudFormation
Stacks
Create Stack
Create stack
Select Template
Specify Details
Options
Review
Options
Tags
You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. Learn more.
Key (127 characters maximum)
Value (256 characters maximum)
Permissions
You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. Learn more.
IAM Role
Choose a role (optional)
Enter role arn
Rollback Triggers
Rollback triggers enable you to have AWS CloudFormation monitor the state of your application during stack creation and updating, and to rollback that operation if the application breaches the threshold of any of the alarms you've specified. Learn more
Monitoring Time
0-180
Minutes
Minimum value of 0. Maximum value of 180.
Available triggers remaining: 5
Type
ARN (Amazon Resource Name)
AWS::CloudWatch::Alarm
Advanced
You can set additional options for your stack, like notification options and a stack policy. Learn more.
Cancel
Previous
Next
Feedback
English (US)
© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy Policy
Terms of Use

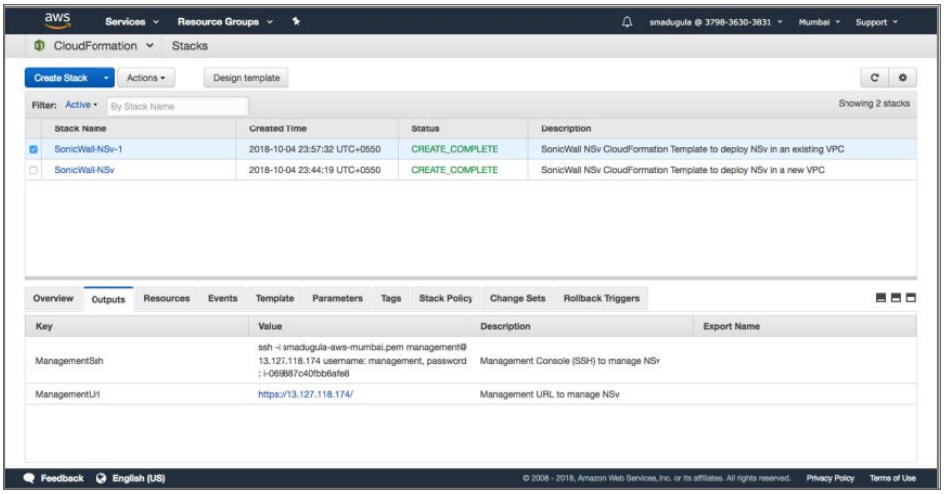
9. Click **Next**.



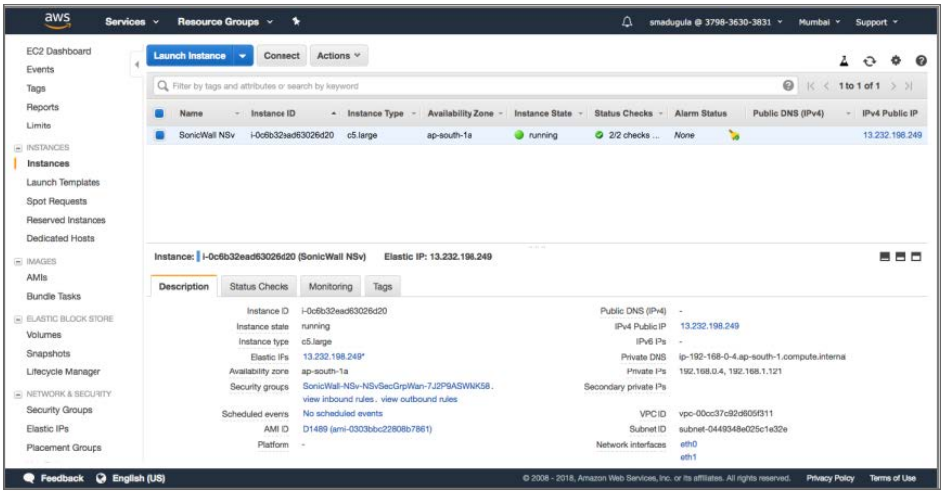
10. Review details and click **Create**.



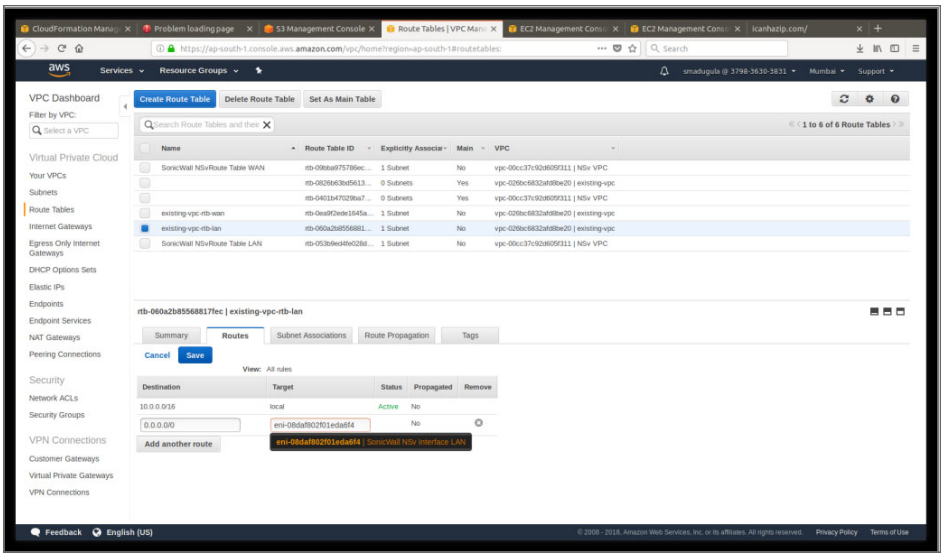
11. Status changes to **CREATE_COMPLETE**.



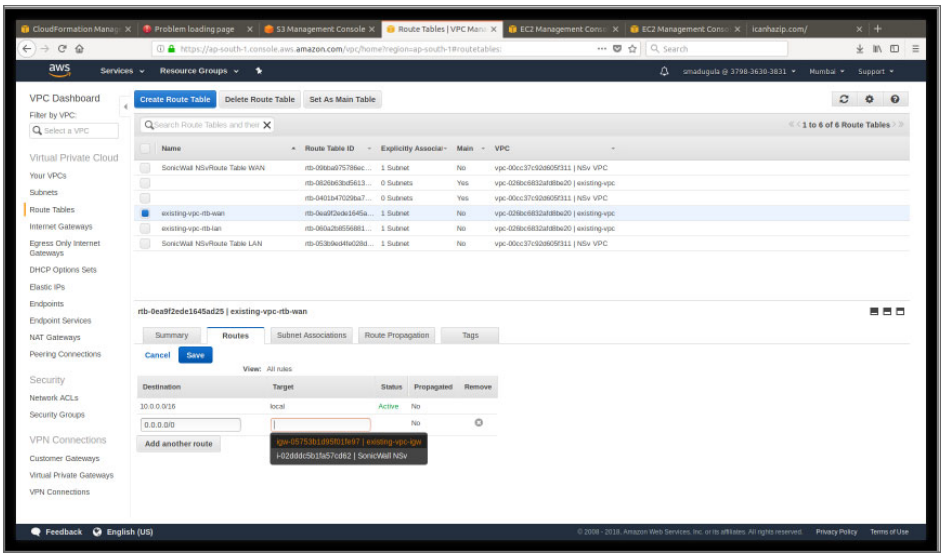
12. When the stack creation is complete (**Status** changes to **CREATE_COMPLETE**). You can get the management and access details in the **Outputs** section.
13. Wait at EC2 Dashboard for **Instance State** — **running**, AND **Status checks** — **2/2 checks passed**.



14. Change Routing Tables:
    a. Change Your LAN routing table to add a route with **Destination** `0.0.0.0/0` with **Target** to NSv's LAN Interface. This routes all your LAN traffic to the NSv 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 NSv WAN traffic to the Internet Gateway (IGW).



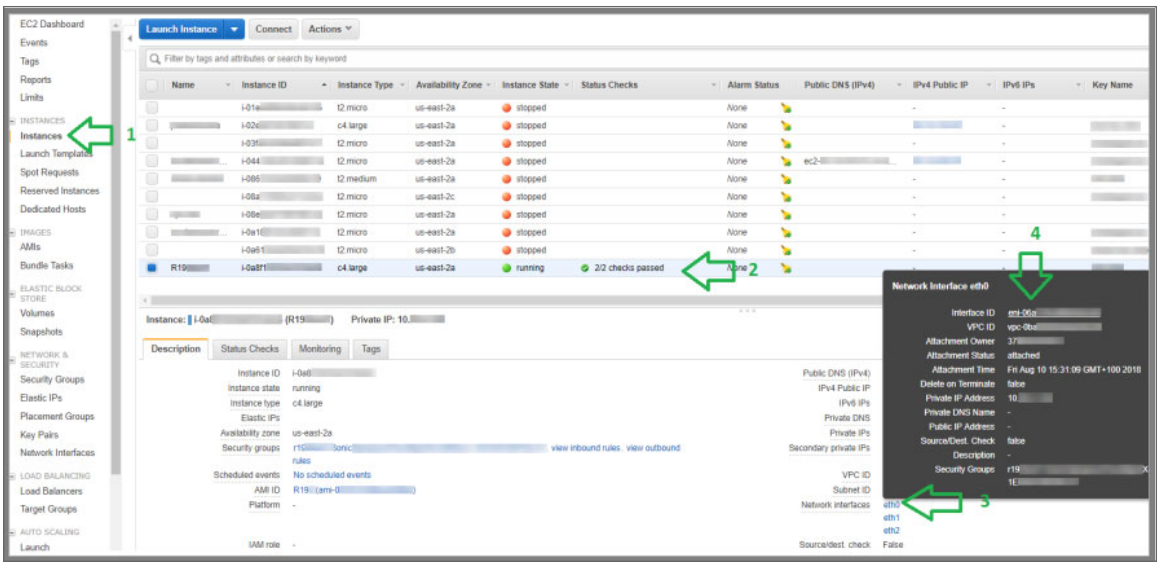
15. Your NSv should now be operational. Next, register your NSv as described in Licensing and Registering Your NSv. The following section details how to set up access to the NSv from the public Internet.

Accessing the SonicWall NSv Web Interface

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

To locate the management ENI:

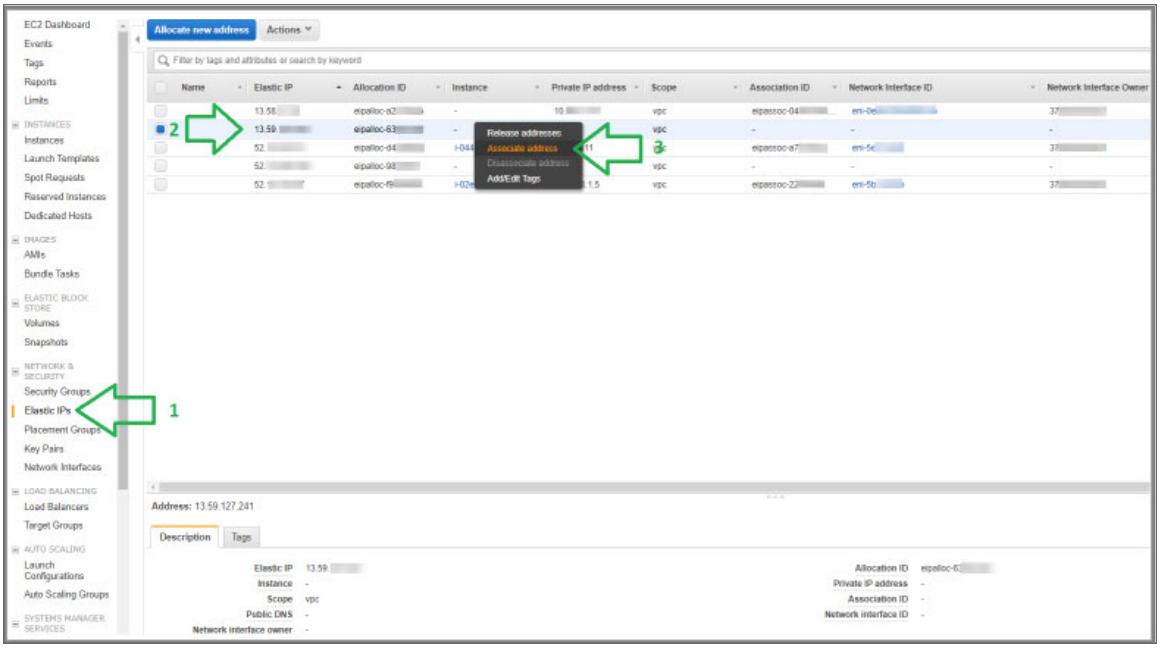
1. In your browser, navigate to **EC2 > Instances**.



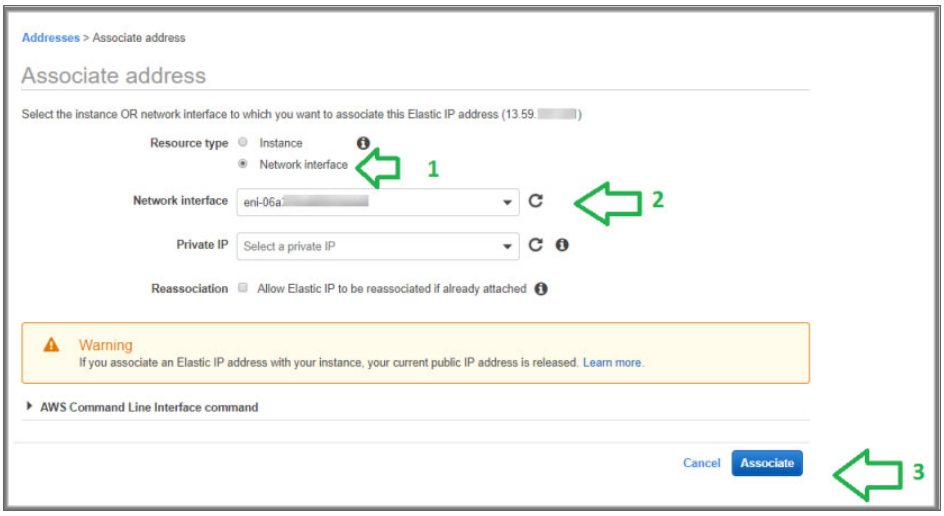
2. Select the SonicWall NSv instance.
3. Select **eth0** in the lower pane.
4. Copy the **Interface ID** value into your clipboard (`eni-xxxxxxxxxxxxxxxxx`). This is the management ENI.
5. Paste the value into a temporary file, so you can refer to it during the next procedure.

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

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



2. Select an IP address that is “free,” or if no addresses are available, click **Allocate new address** 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 displays.



4. For **Resource type**, select **Network interface**.
5. In the **Network interface** drop-down menu, 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 NSv 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.

The SonicWall NSv 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 such as `i-02aaxxxxxxxxxxxx`.

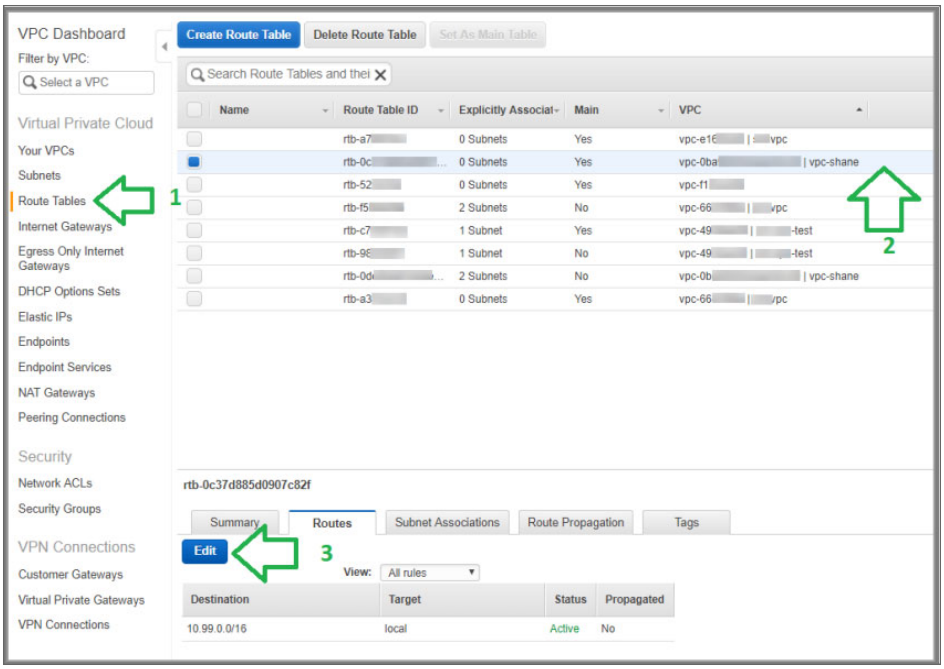
If you have not already registered, register your NSv virtual machine with MySonicWall. See Registering the NSv Appliance as PAYG.

Forwarding Traffic to your NSv

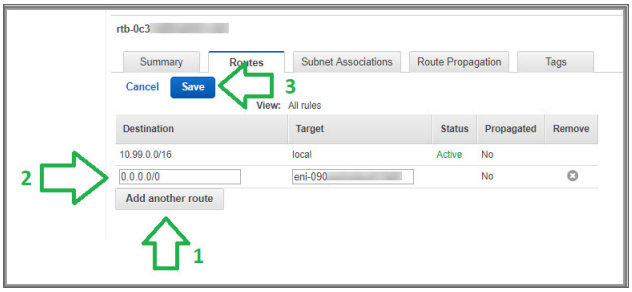
After installing and registering the NSv, the next step is to configure routing of the LAN subnet so that the traffic is forwarded through the NSv.

To configure routing:

1. Navigate to the **VPC Dashboard** and click **Route Tables** in the left navigation pane.



2. Select the row for which the **Main** column displays ***Yes*** and the **VPC** column displays the VPC where the NSv instance is configured.
3. Select the **Routes** tab in the lower pane.
4. Click **Edit**. The lower pane display changes.
5. Click **Add another route**. A new row is displayed in the table.



6. For **Destination**, enter `0.0.0.0/0` to match all traffic.
7. For **Target**, type `eni-` to display a drop-down menu with available ENIs and then select the **eth1** ENI for your NSv.
8. Click **Save**.

Proceed to Configuring Internet/Public Access Through the NSv.

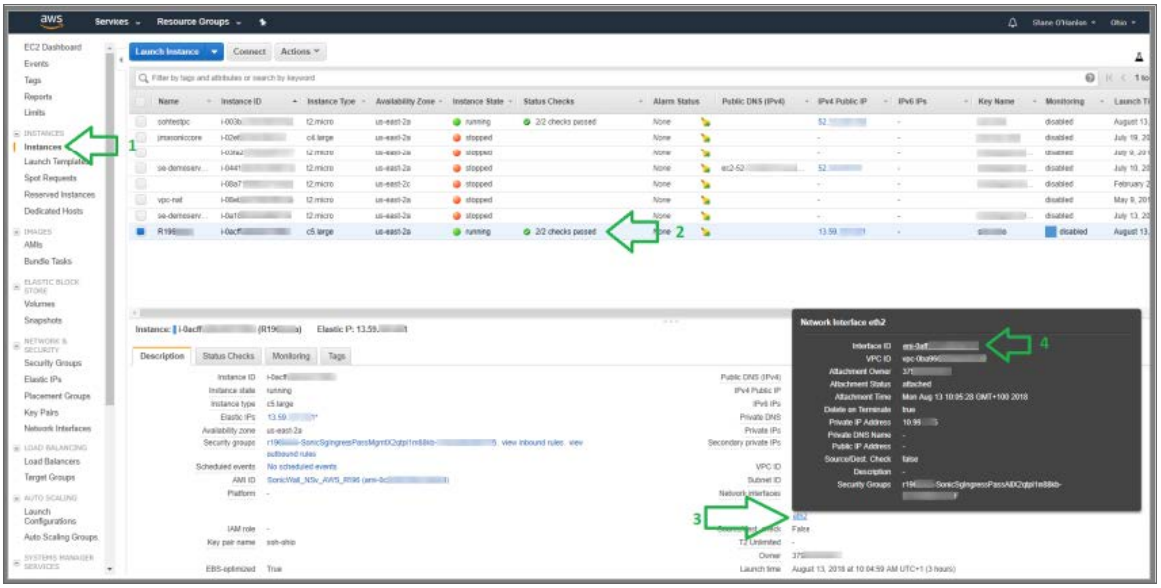
Configuring Internet/Public Access Through the NSv

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 NSv X1 interface, you need to use the Elastic Network Interface (ENI).

To locate the ENI:

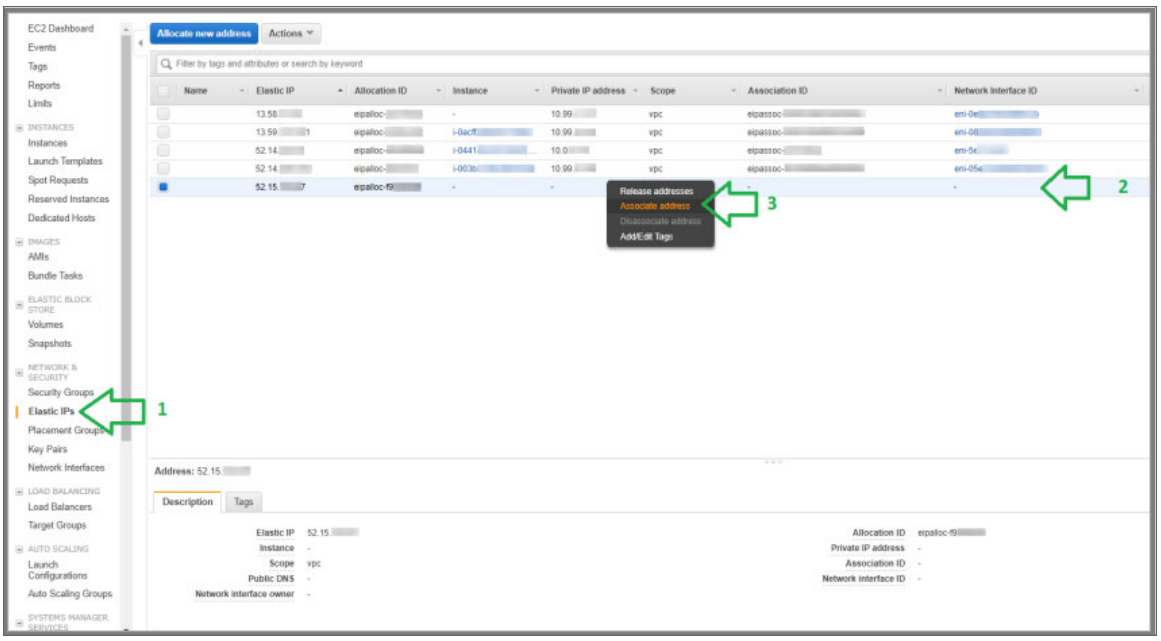
1. In your browser, navigate to **EC2 > Instances**.



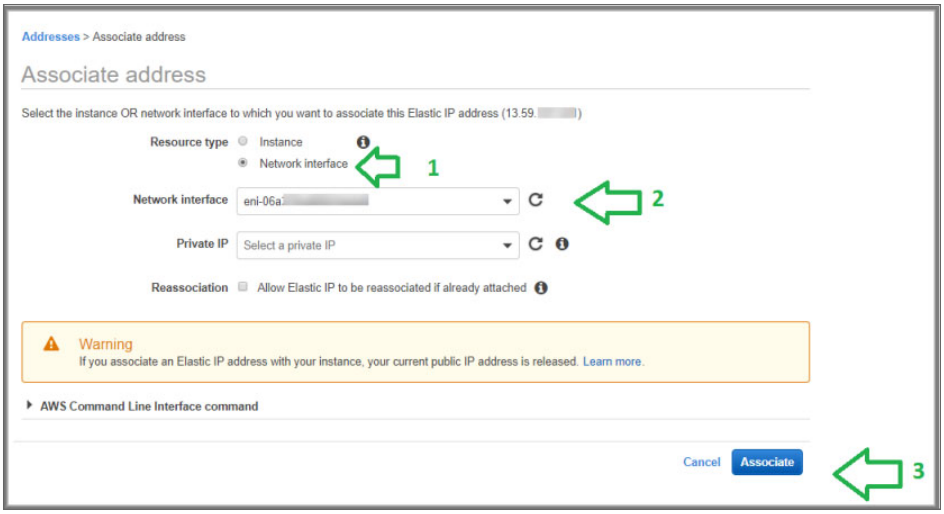
2. In the top pane, select the NSv instance.
3. In the lower pane, click **eth2** to display the **Network Interface eth2** pop-up menu.
4. Copy the **Interface ID** from the pop-up menu. This is the X1 ENI.
5. Paste the value into a temporary file, so you can refer to it during the next procedure.

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

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



2. Select an IP address that is “free,” or if no addresses are available, then click **Allocate new address** 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 displays.



4. For **Resource type**, select **Network interface**.
5. In the **Network interface** drop-down menu, select the ENI of the X1 interface that you located in the

previous procedure.

6. Click **Associate**.

SonicWall NSv Firewall on AWS GovCloud

The AWS Govt Region is an isolated AWS region that meets the regulatory and compliance requirements of the US government agencies and customers.

To secure the workloads that contain all categories of Controlled Unclassified Information (CUI) data and government-oriented, publicly available data in the AWS GovCloud (US) Region, the NSv-Series firewall provides the same robust security features in the standard AWS region cloud servers and on AWS GovCloud servers.

ⓘ **NOTE:** The AWS GovCloud (US) Regions are maintained by U.S. citizens only and provide customers with the ability to access the regions through service endpoints. If you are not deploying from AWS GovCloud, you can skip this section.

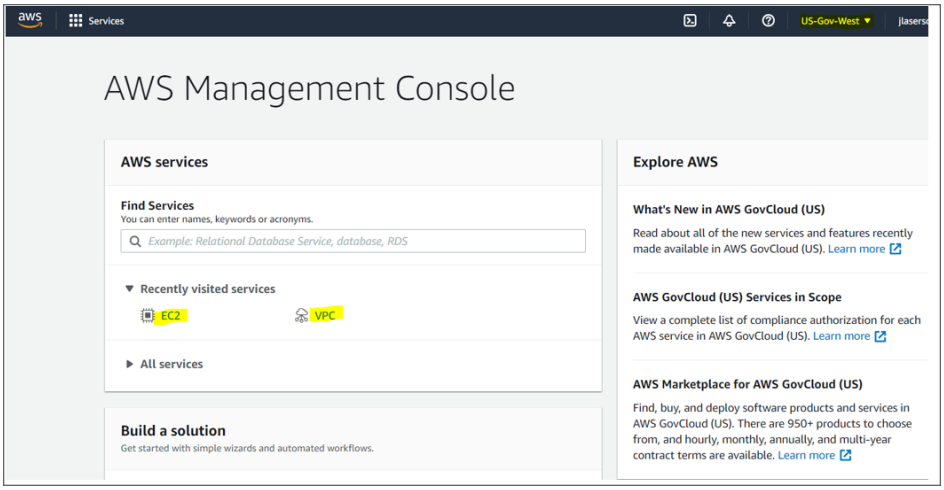
Topics:

Deploying NSv from AWS GovCloud Console

To deploy NSv from the console, follow these steps:

1. Log into the AWS GovCloud 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. Create a VPC

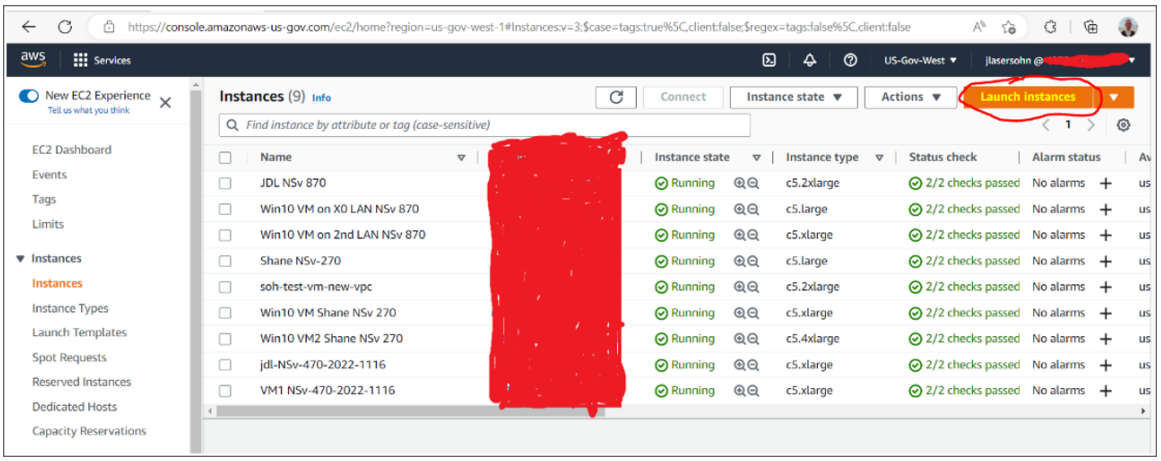
   The virtual machine can be deployed on a new or existing VPC.

3. In the navigation pane, choose **Your VPCs, Create VPC**.

4. Under **Resources to create**, choose **VPC and more**.Refer to the AWS documentation on how to create a VPC at: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html.

5. Follow these steps to launch the SonicWall NSv:

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



   b. From the menu click **AWS Marketplace** and enter `SonicWall NSv` into the **Search** box.

   c. Click **Select** next to the **SonicWall NSv (Firewall/Security/VPM/Router)-BYOL**.

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

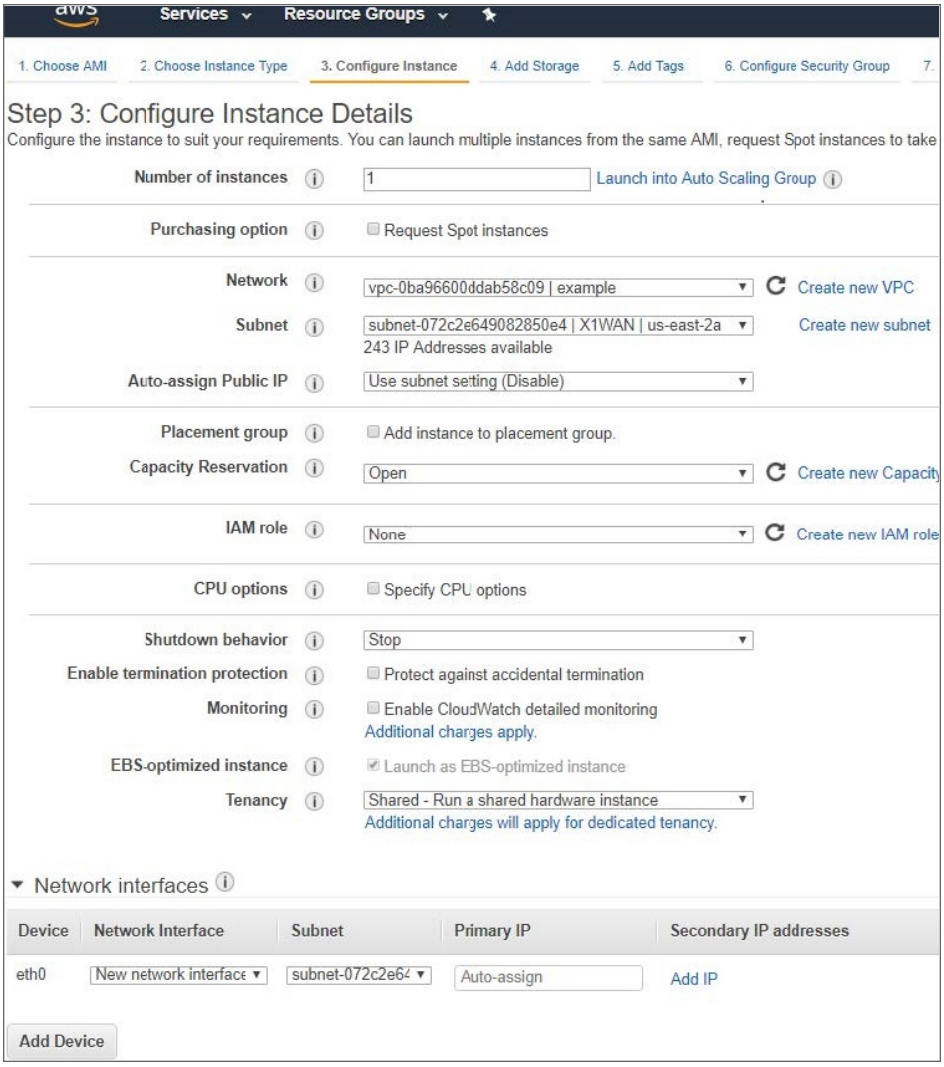
   For guidance, refer to Product Matrix and Requirements and Supported NSv Series Models on AWS. Choose instance size from the table displayed:

■	Compute optimized	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
□	Compute optimized	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
□	Compute optimized	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
□	Compute optimized	c5.4xlarge	16	32	EBS only	Yes	Up to 10 Gigabit	Yes

NSV MODELS AND IMAGE TYPES

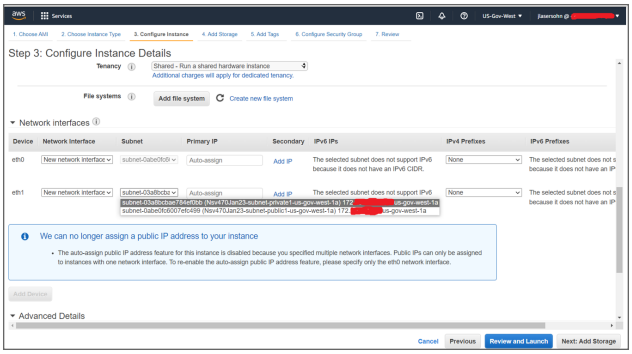
SonicWall NSv Model	NSv EC2 Instance Type
NSv 270	c5.large
NSv 470	c5.xlarge
NSv 870	c5.2xlarge

e. Click **Configure Instance Details**. From the **Network** drop-down menu select a VPC to deploy the virtual machine on. Select the subnet that is to be the public or WAN interface (X1) of the virtual machine.



f. To add additional Elastic Network Interfaces click **Add Device**.

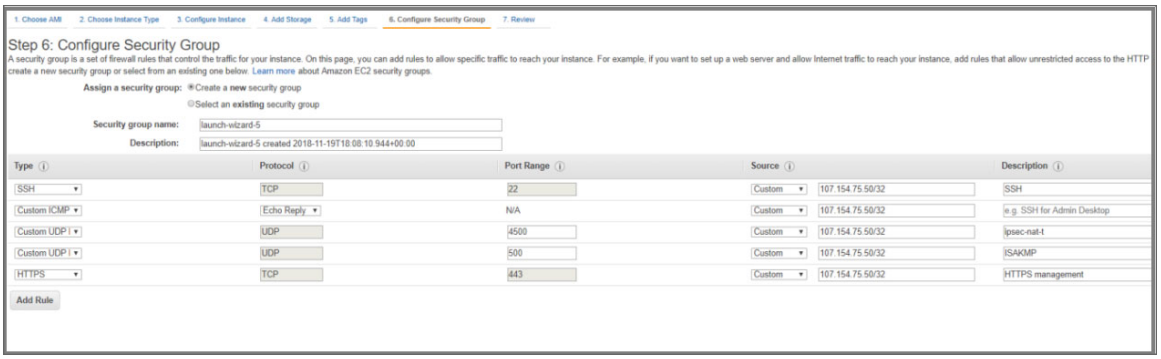
New row appears for ENI *eth1* select the **Subnet** drop-down menu.



g. Accept the default storage options by clicking **Add Storage**.

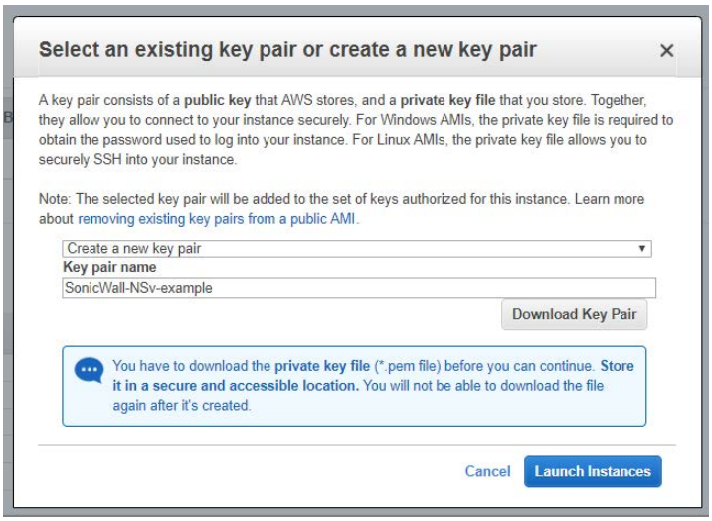
h. Click **Add tags**. Add metadata to the instance configuration to assist in identifying the SonicWall NSv instance.

i. Click **Configure Security Group**. At minimum, allow SSH and HTTPS from a predefined source.



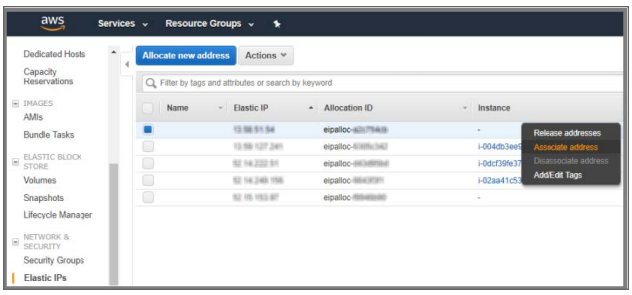
j. Click **Review** and **Launch**. Review the instance details.

k. Click **Launch**. You are prompted to select either **Key-Pair** or **Create a new key pair**. Ensure you have access to the key pair.



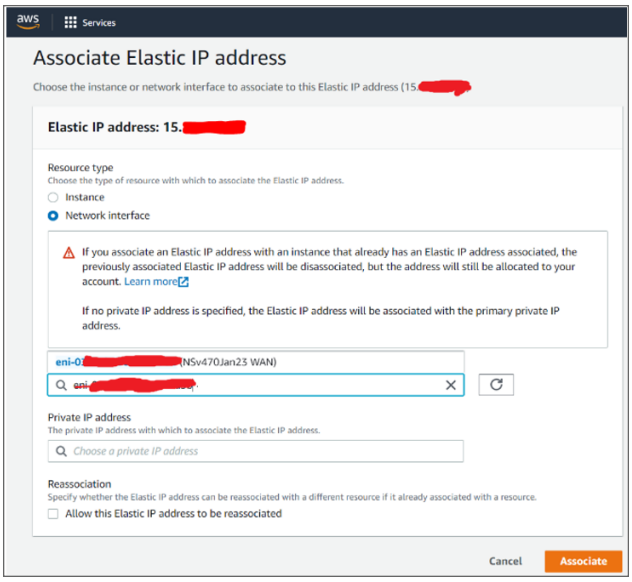
l. Click **Launch Instances** to deploy the SonicWall NSv instance. Deployment takes few minutes. You can monitor the progress by viewing the instance in the EC2 Dashboard.

6. Disable source/destination checking:
   a. Select **Network interfaces** on the **Networking** tab.
   b. Choose the interface ID to go to the network interfaces page.
   c. Select **Choose Actions, Networking, Change source/destination check**.
   d. Clear the **Enable** , and click **Save**.
7. To assign an Elastic IP, follow these steps:
   a. From the EC2 Dashboard left menu select **Elastic IPs**.
   b. Right-click on a free Elastic IP and select **Associate Elastic IPs**. If no Elastic IPs are available, then click **Allocate new address**.



   c. Choose the **Resource type** and **Network Interface**.

      From the **Network Interface** drop-down menu, 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 NSv web management interface.

8. Connect to the virtual machine web management interface:

   a. Now that you have associated an Elastic IP to the SonicWall NSv instance, you are able to connect to the web management interface by entering the IP address into your browser.

   b. Enter the username ***admin*** and the password.

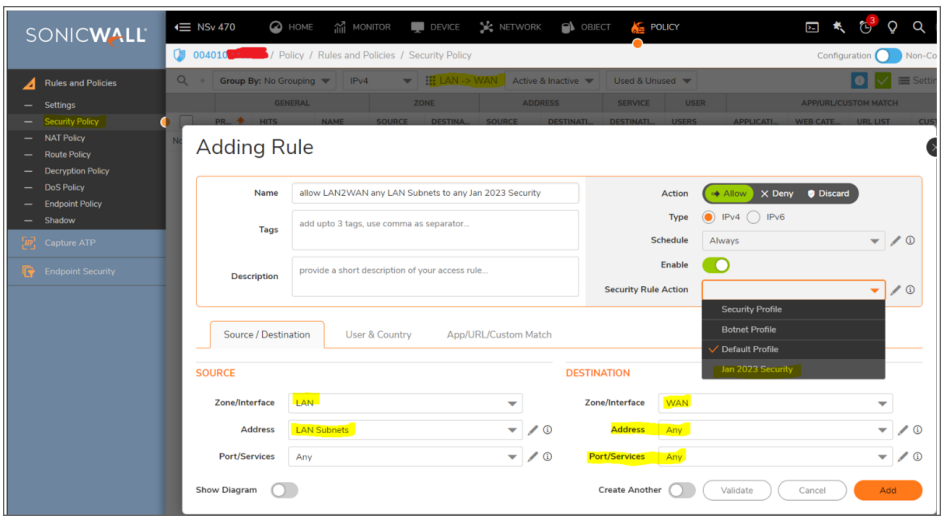
After installing and configuring the network settings for your NSv Series virtual machine, you can log into SonicOS management and register it in your MySonicWall account. See Registering the NSv Virtual Machine as BYOL from SonicOS.

Creating a Security Policy for Outbound

After registering of your SonicWall NSv Series, you can create security policy and apply security services such as SonicWall Gateway Anti-Virus (GAV), Intrusion Prevention, Anti-Spyware Security, Botnet Filtering and Content Filtering.

To configure a Security Policy:

1. Navigate to **Policy > Rules and Policies > Security Policy**.
   The Security Policy page is displayed.
2. Choose LAN to WAN in **Zone Matrix Selector**.
3. From the bottom of the Security Policy table, click **Add**.
   The **Adding Rule** page is displayed.



4. Enter the policy **Name** and any identifying **Tags** you would like to enter to help sort your policies.
5. Enter a **Description** of the policy and its intent.
6. Select an **Action**, whether to **Allow**, **Deny**, or **Discard** access.
7. Specify the IP version in **Type**, **IPv4** or **IPv6**.
8. Set your **Security Policy's Priority**.
9. Specify when the rule is applied by selecting a schedule or Schedule Group from the **Schedule** drop-down menu.
10. Click **Enable** to activate the policy schedule and enable logging.
11. In the **Source/Destination** view, select the **Source** and **Destination** zones, and network address objects, and **Port/Services** for each from the drop-down menus.
    There are no default zones. **Any** is supported for both zone fields.

	Source	Destination
Zone/Interface	LAN	WAN
Address	LAN Subnets (custom subnet)	Any
Port/Services	Any	Any

12. Under **Users**, specify if this rule applies to all users or to an individual user or group in the **Include** drop-down menu. You can exclude users as well using the **Exclude** drop-down menu.

13. Under **GEO Country**, indicate a **(From/To) Country** from the drop-down menu.
14. Click **Save**, and continue with **App/URL/Custom Match** and **Action Profile**.

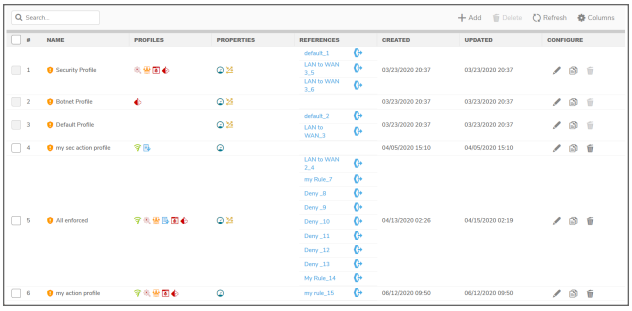
After creating security policy, apply security services. See Applying Security Services on Policies in NSv for Outbound Traffic.

Applying Security Services on Policies in NSv for Outbound Traffic

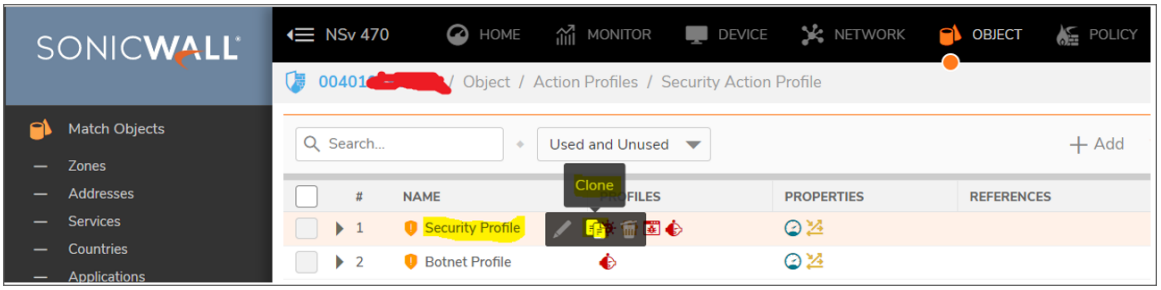
Security Rules define how the Security Rule Action policies react to matching events. You can create a custom Security Rule Action object or select the predefined, default action.

To add the Security Action Profiles:

1. Navigate to **Object > Action Profiles > Security Action Profile**.
   The Security Rule table is displayed.

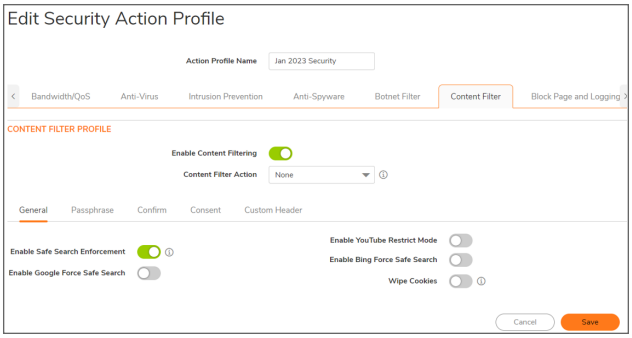


2. Click **+Add** to add security action profile.
   Or
   Hover the mouse over the existing security profile, you can, **Edit**, **Clone**, or **Delete** Security Rule Action policies. You can also configure **Column** elements.



Hover over icons within the columns for additional information about the profile configuration, including

enabled and disabled services, policy properties, referenced or associated policies, and so on.

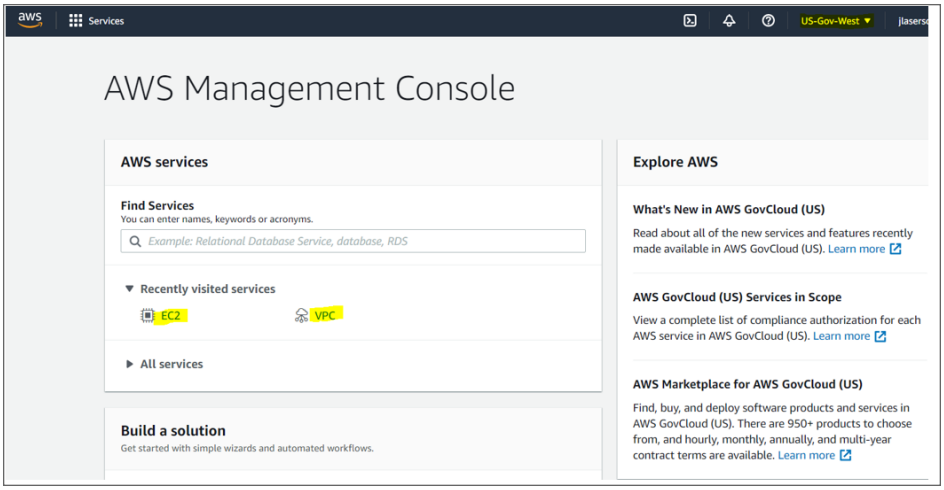


Deploying Windows 10 from Console

Create a Windows 10 Virtual Machine (VM) similar to the NSv on the AWS VPC, and configure the settings to send the Windows 10 VM's outbound traffic to the NSv LAN interface, instead of using the AWS routing infrastructure.

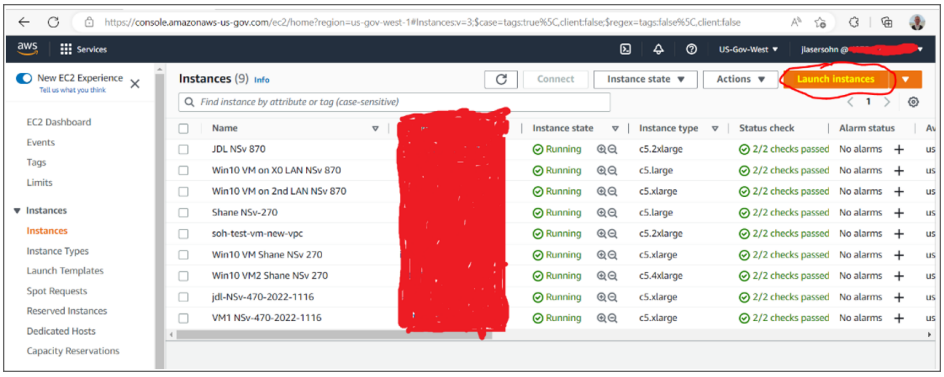
To deploy Windows 10 from the console, follow these steps:

1. Log into the AWS GovCloud 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.



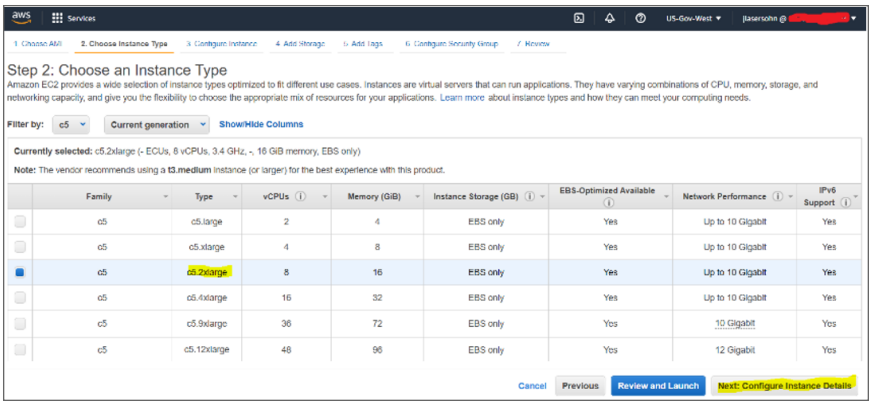
2. Create a VPC
   The virtual machine can be deployed on a new or existing VPC.
3. In the navigation pane, choose **Your VPCs, Create VPC**.

4. Under **Resources to create**, choose **VPC and more**.Refer to the AWS documentation on how to create a VPC at: https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html.
5. Follow these steps to launch the SonicWall NSv:
   a. From the EC2 Dashboard select **Launch Instance**.

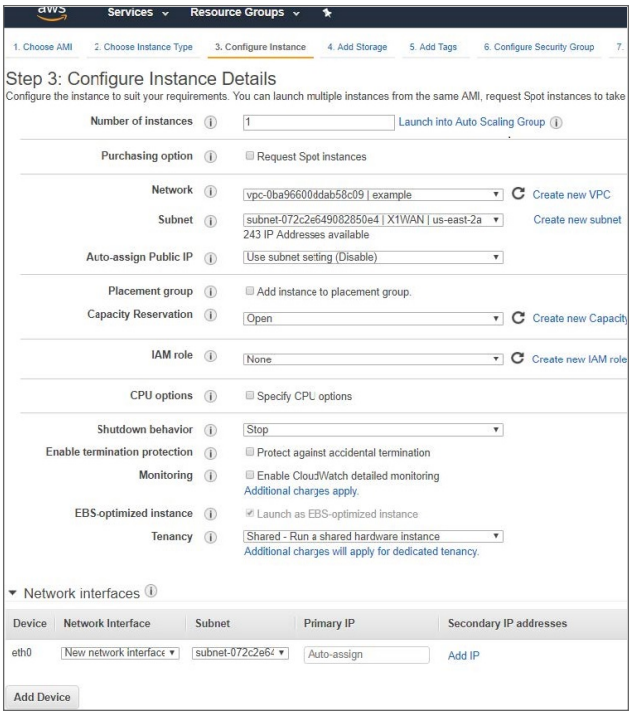


   b. From the menu click **AWS Marketplace** and enter `Windows 10` into the **Search** box.
   c. Select the **Instance Type** and select c5.2xlarge.

      For guidance, refer to Product Matrix and Requirements and Supported NSv Series Models on AWS.



   d. Click **Configure Instance Details**.



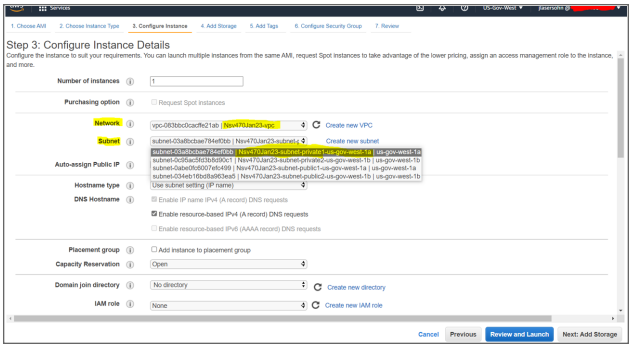
1. From the **Network** drop-down menu select a VPC to deploy the virtual machine on.
2. Select the subnet that is to be the public or WAN interface (X1) of the virtual machine.

e. To add additional Elastic Network Interfaces click **Add Device**.
New row appears for ENI *eth1*.

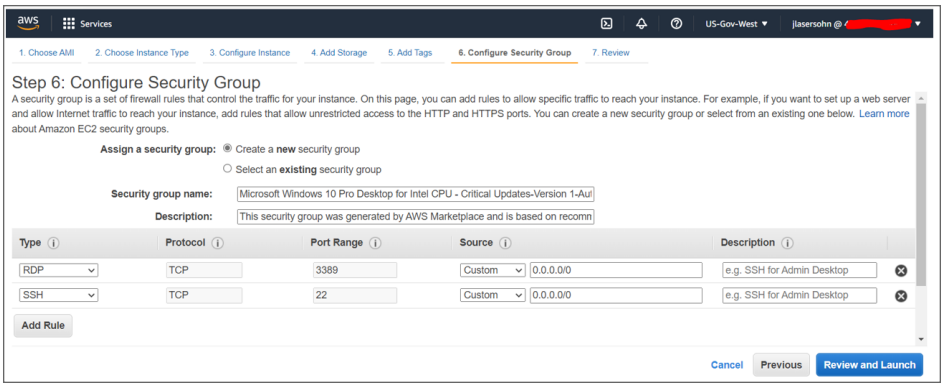
f. Select the **Subnet** drop-down menu.

g. Accept the default storage options by clicking **Add Storage**.

h. Click **Add tags**. Add metadata to the instance configuration to assist in identifying the SonicWall NSv instance.



i. Click **Configure Security Group**. Leave the default settings, which allow SSH & RDP from any source IP, as VM has no public IP.



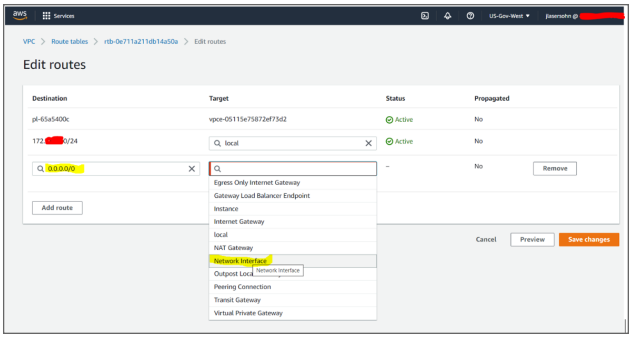
j. Click **Review** and **Launch**. Review the instance details.

k. Click **Launch**. You are prompted to select **Create a new key pair** and choose RSA as **key type**

l. Click **Launch Instances** to deploy the SonicWall NSv instance. Deployment takes few minutes. You can monitor the progress by viewing the instance in the EC2 Dashboard.

6. Change Routing Tables:

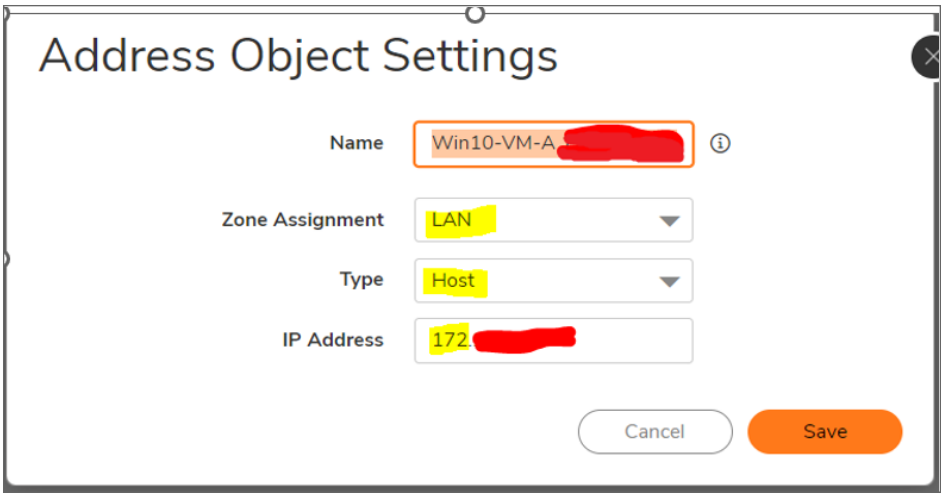
   a. Change your LAN routing table to add a route with **Destination** `0.0.0.0/0` with **Target** to Network Interface. This routes all your outbound traffic to the NSv X0 interface.



Creating a Security Policy and NAT Policy for Inbound RDP to the VM

To add address object for Windows 10 VM:

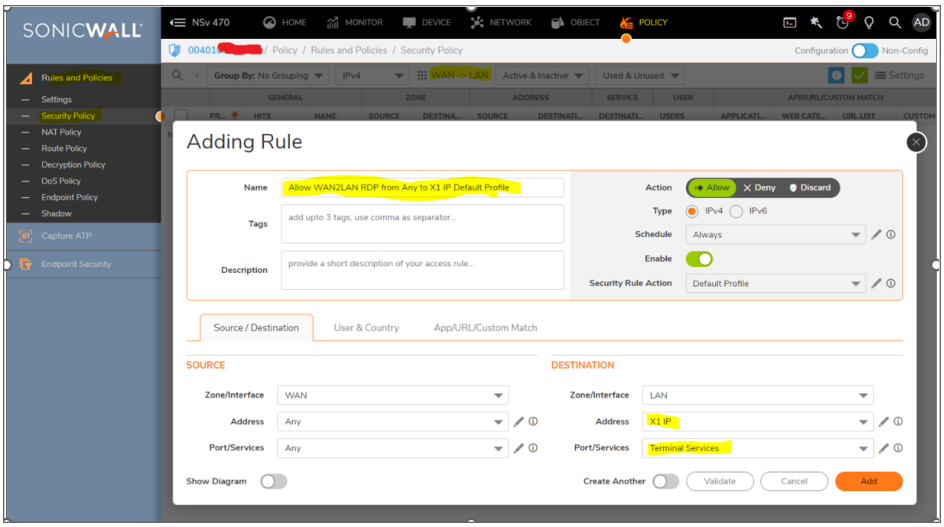
1. Navigate to the **Object > Match Objects > Addresses page** .
2. Click **+Add** at the top of the page.
   The Address Object Settings dialog displays.



3. Enter a friendly description such as `Win10-VM-A 172.x.y.z` for the server's private IP address in the **Name** field.
4. Select the **LAN** to the server from the **Zone Assignment** drop-down menu.
5. Choose **Host** from the **Type** drop-down menu.
6. Enter the `172.x.y.z` IP address in the **IP Address** field.
7. Click **Save**.

To add Security policy:

1. Navigate to **Policy > Rules and Policies > Security Policy**.
   The **Security Policy** page is displayed.
2. Choose WAN to LAN in **Zone Matrix Selector**.
3. From the bottom of the Security Policy table, click **Add**.
   The **Adding Rule** page is displayed.



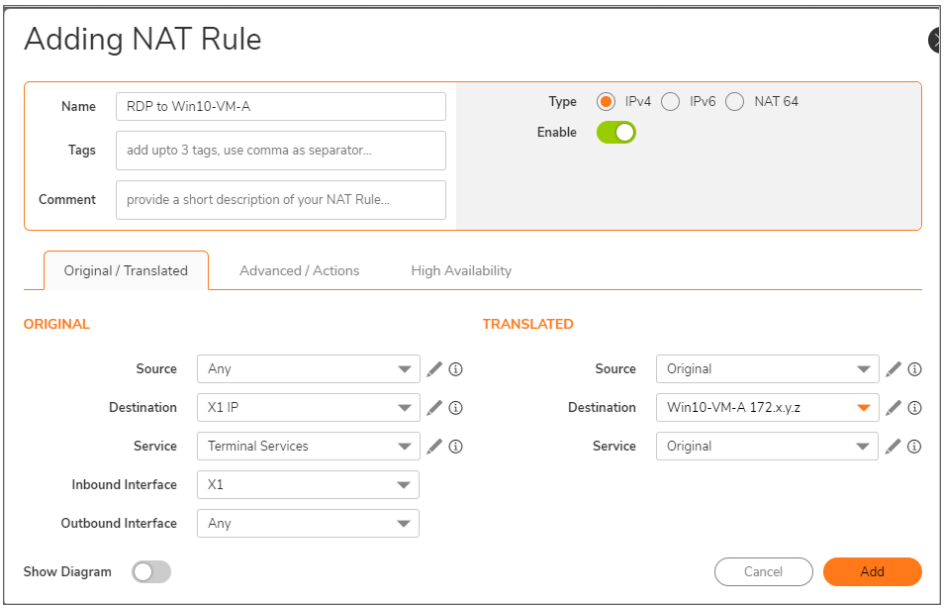
4. Enter the policy **Name** and any identifying **Tags** you would like to enter to help sort your policies.
5. Enter a **Description** of the policy and its intent.
6. Select an **Action**, whether to **Allow**, **Deny**, or **Discard** access.
7. Specify the IP version in **Type**, **IPv4** or **IPv6**.
8. Set your **Security Policy's Priority**.
9. Specify when the rule is applied by selecting a schedule or Schedule Group from the **Schedule** drop-down menu.
10. Click **Enable** to activate the policy schedule and enable logging.
11. In the **Source/Destination** select the following:

	Source	Destination
Zone/Interface	WAN	LAN
Address	Any	X1 IP
Port/Services	Any	Terminal Services

12. Click **Save**.

To add NAT Policy:

1. Navigate to **Policy > Rules and Policies > Security Policy**.
   The **NAT Policy** page is displayed.
2. From the bottom of the Security Policy table, click **Add**.
   The **Adding Rule** page is displayed.



3. Enter the policy **Name** and any identifying **Tags** you would like to enter to help sort your policies.
4. Enter a **Comment** of the policy and its intent.
5. Set your **Original/ Translated**.
   a. Under **Original** select the following:

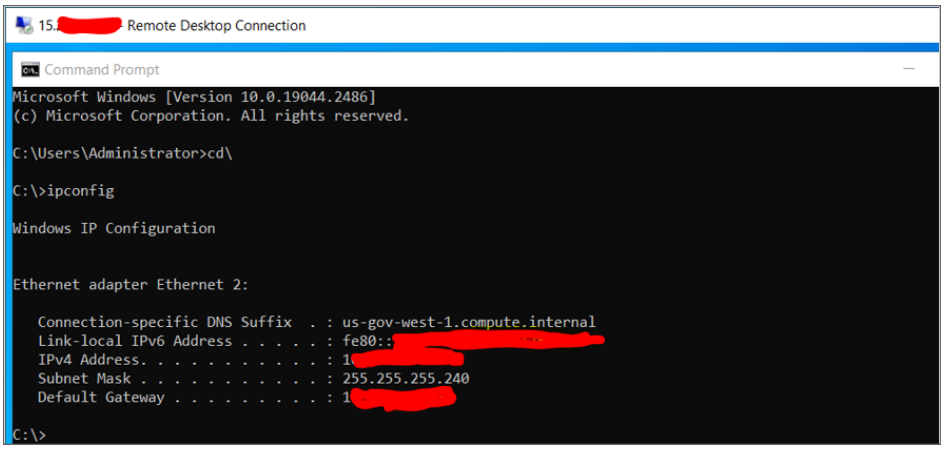
Source	**Any**
Destination	**X1 IP**
Service	**Terminal Services**
Inbound Interface	**X1**
Outbound Interface	**Any**

   b. Under **Translated** select the following:

Source	**Original**
Destination	**Win10-VM-A 172.x.y.z**
Service	**Original**

6. Click **Save**.

In Remote Desktop Connection, run the VM using the same **Elastic public IP** used for logging into the NSv web interface, and the VM can get to the internet through the NSv firewall.



Troubleshooting Installation Configuration

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

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

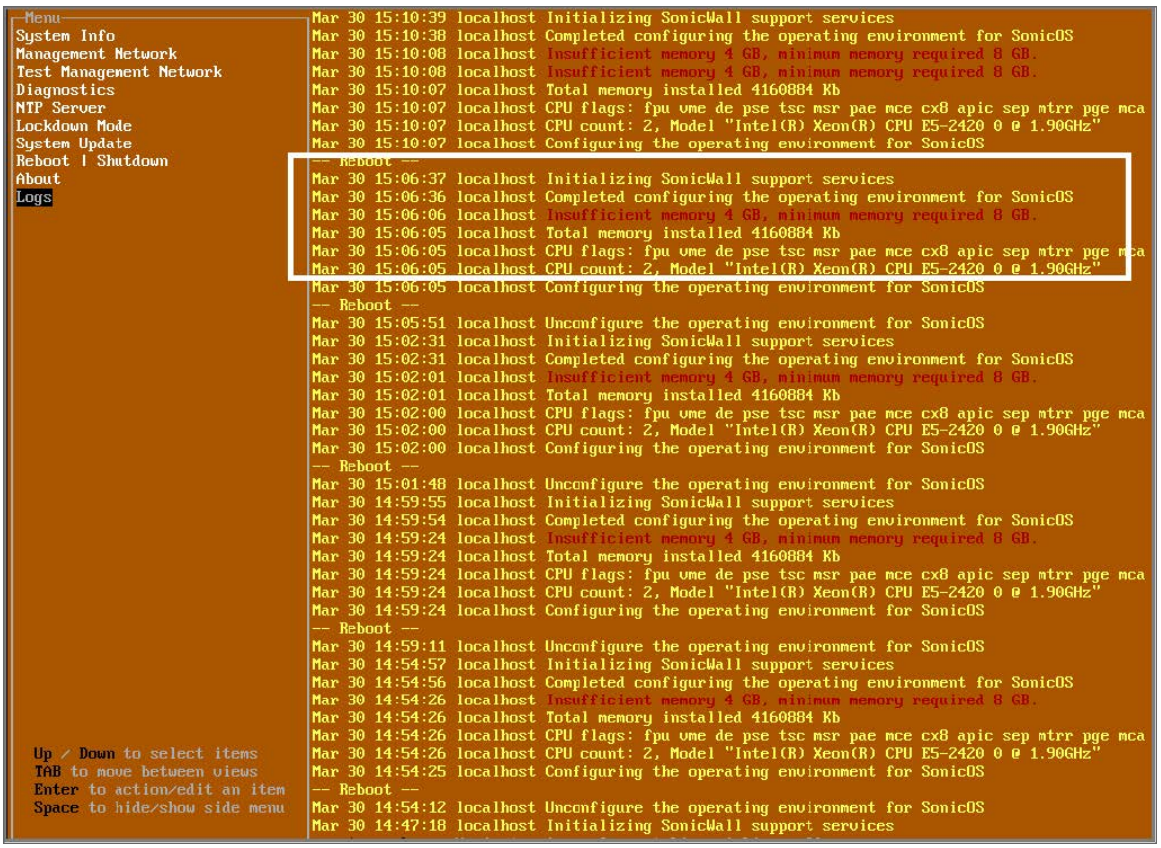
Insufficient Memory Assignment

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

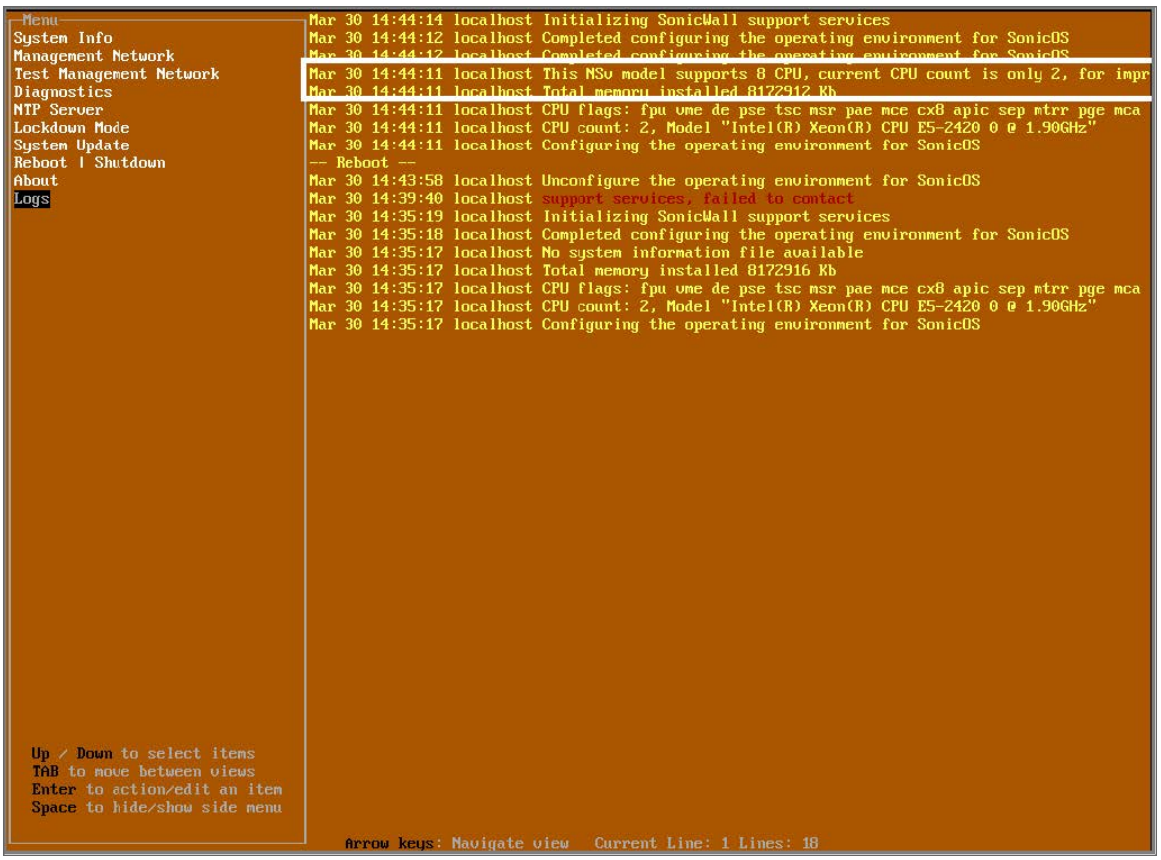
SonicOS boot message:

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

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



Memory might be insufficient without an insufficient memory log entry:



PAYG Installation Errors

Insufficient Interfaces

When less than two network interfaces are assigned to the EC2 instance the following error message appears on the console:

```
*****************************************************************

NSv requires at minimum 2 ENI, power down and add addition ENI

*****************************************************************
```

Unable to Contact Provisioning Service

When the EC2 instance cannot contact the provisioning service, the following error message appears on the console.

```
*****************************************************************************
```

```
Cannot contact provisioning service, check that internet access is provided

*****************************************************************************
```

To resolve this error, check:

- Does the EC2 instance have a public IP (Elastic IP) assigned?
    - If not, is it configured to access the internet by way of an internet gateway?
    - If the virtual machine is not configured to access the internet on initialization, then it is not able to acquire a serial number.
        - After initialization the EC2 instance can be isolated again.
- Check that the security group is not blocking access to internet.
    - If it is, then the customer should enable access temporarily.
    - If they wish to restrict it, then use the IP address associated with `instanceregister.soniccore.cloud.eng.sonicwall.com`.

3

Licensing and Registering Your NSv

You can choose to prepay 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 registration steps differ.

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

The following topics describe how to deploy your NSv using these two approaches: BYOL (Bring Your Own License) and PAYG (Pay As You Go).

Topics:

Registering the NSv Virtual Machine as BYOL from SonicOS

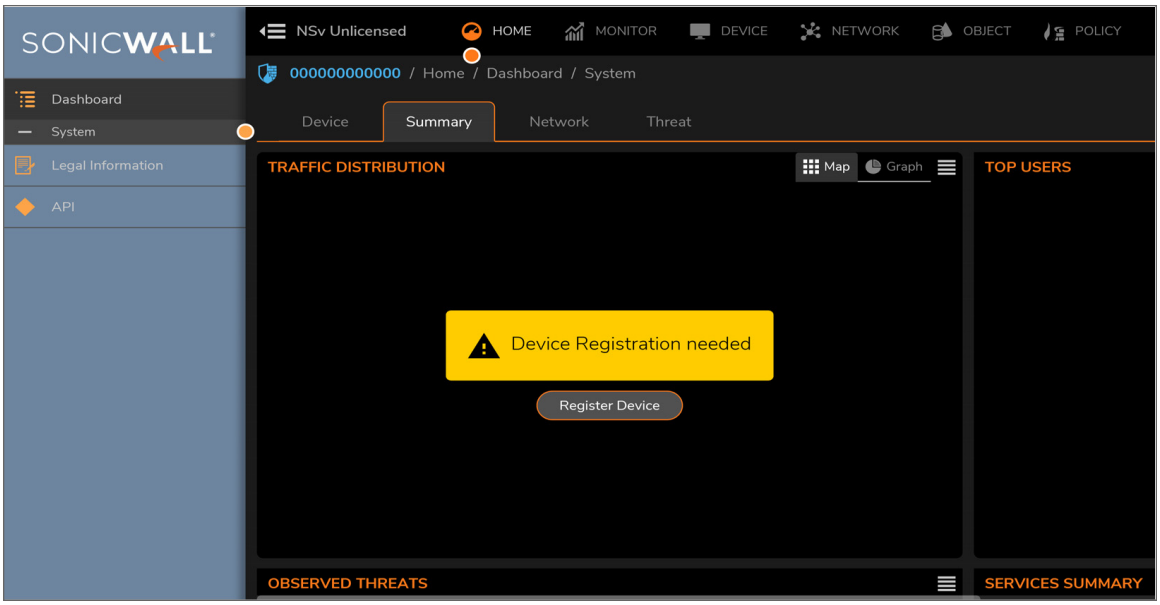
This section describes how to register an NSv when it is being deployed as “Bring Your Own License” (BYOL).

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

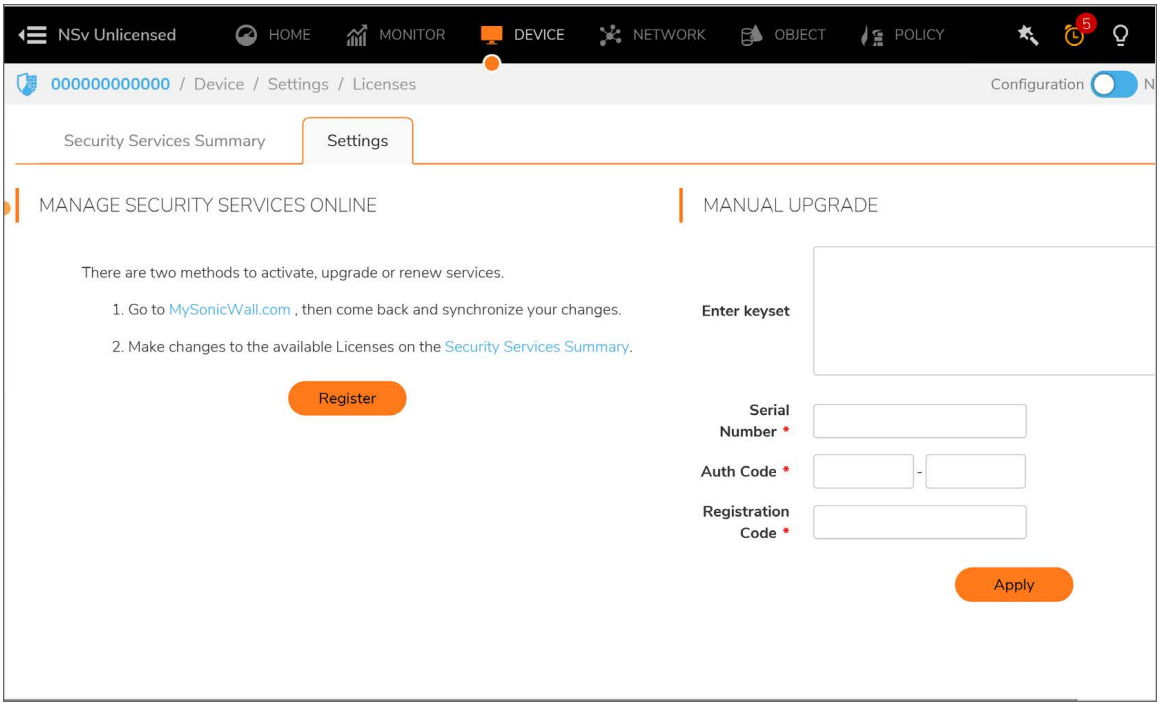
ⓘ **NOTE:** System functionality is extremely limited if registration is not completed. See Using System Diagnostics for more information.

To register your NSv virtual machine:

1. Point your browser to your NSv Series WAN or LAN IP address and log in as the administrator.
2. On the **HOME | Dashboard > System > Summary** page, click **Register Device**.



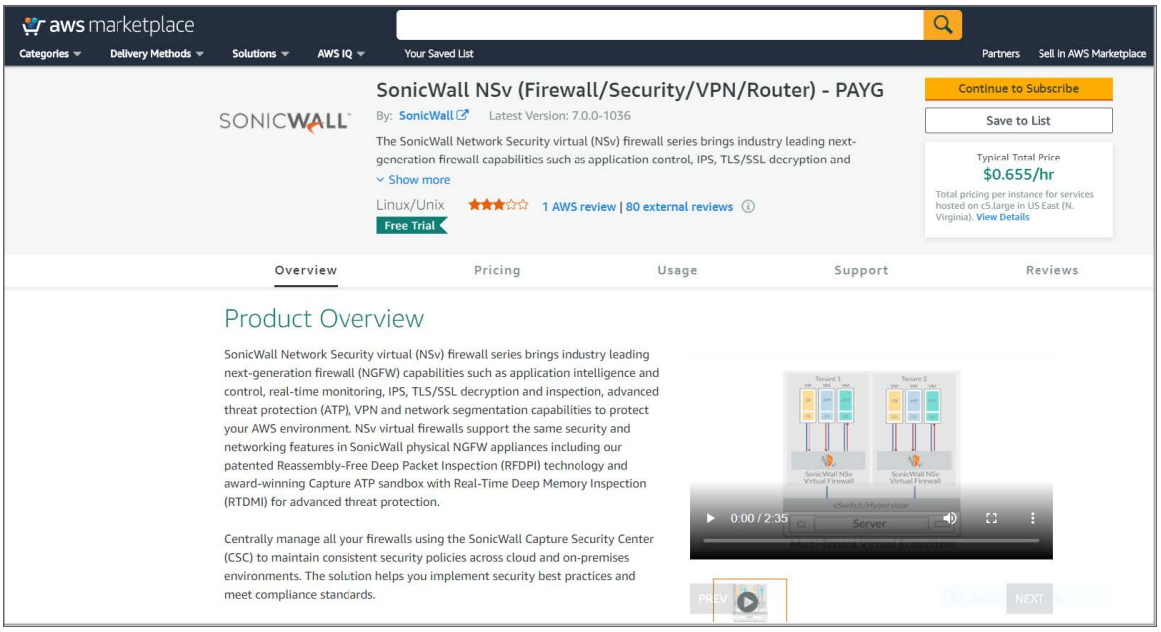
3. At this point you can log into MySonicWall and name the NSv installation while providing the serial number and authorization code to complete registration. Or, if you are unable to reach MySonicWall, use the **Keyset**, **Serial Number**, **Authorization**, and **Registration** codes provided by your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



4. After you are finished, log in to SonicOS and go to **DEVICE | Settings > Licenses** to check that the licensing is complete.

Registering the NSv Virtual Machine as PAYG

This section describes how to register an NSv when it is being deployed as “Pay As You Go” (PAYG). The choice to use PAYG is made as you initiate subscription in the AWS Marketplace.



After you have installed and configured network settings for the NSv as described in Installing SonicOS on the NSv Series, log in to the web management interface. To find the IPv4 address for the web management interface, log into the Management Console as described in Connecting to the Management Console with SSH.

ⓘ **NOTE:** To ensure access to SonicWall Technical Support, creating a MySonicWall account is recommended. You can create an account at https://www.mysonicwall.com/muir/signup. An account at MySonicWall offers advantages:

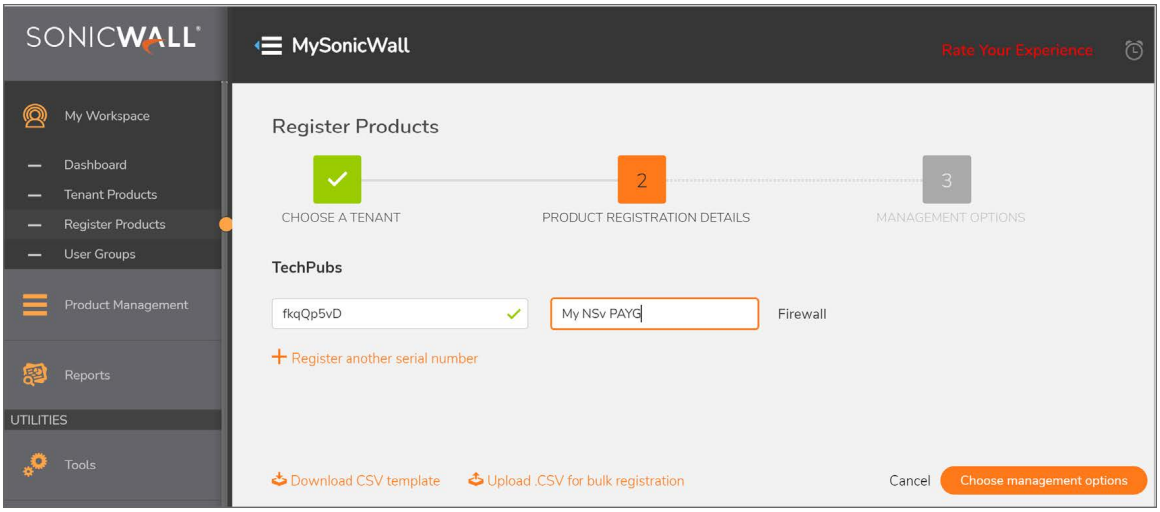
- It allows you send diagnostics from your virtual machine directly to SonicWall Technical Support.
- It supports easy initiation of support cases online. See: https://www.sonicwall.com/support/knowledge-base/?sol_id=170814110235888

To link your NSv Series virtual machine to MySonicWall:

1. Enter the username and password and log into SonicOS on the NSv .

   ⓘ **NOTE:** Ensure to use the new password if you have updated the default password.
2. Navigate to **HOME | Dashboard > System**.
3. On the **Devices** screen, locate the **Assign Token** under the **General** section.
4. Copy the **Assign Token** value into your clipboard. For example, this is a string such as “fkqQp5vD.”
5. Log into MySonicWall at https://www.mysonicwall.com/muir/login.

6. Navigate to **Register Products**, and start by selecting a **Tenant**.
7. Under the tenant name, enter the **Assign Token** value and type in a Friendly Name for the NSv.



8. Click **Choose management options** and make your management selection in the next screen. Select **Cloud** to manage the NSv from SonicWall Network Security Manager (NSM), or select **On-Box** to manage it from the SonicOS web management interface.
9. Click **Done**.
10. In SonicOS, navigate to **DEVICE | Settings > Licenses** to check that licensing is complete.

4

SonicOS Management

Topics:

Managing SonicOS on the NSv Series

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

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

To log into SonicOS for management of the NSv:

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

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

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

2. Enter the administrator credentials.

   Your default password must be changed at first time while logging in after upgrade. Create a password that meets the security requirements. A password should have at least one uppercase letter, one lowercase letter, one number, and one special character. For example, MyP@ssw0rd.

a. In the **Old Password** text box, enter your default password.

b. In the **New Password** text box, enter your new password.

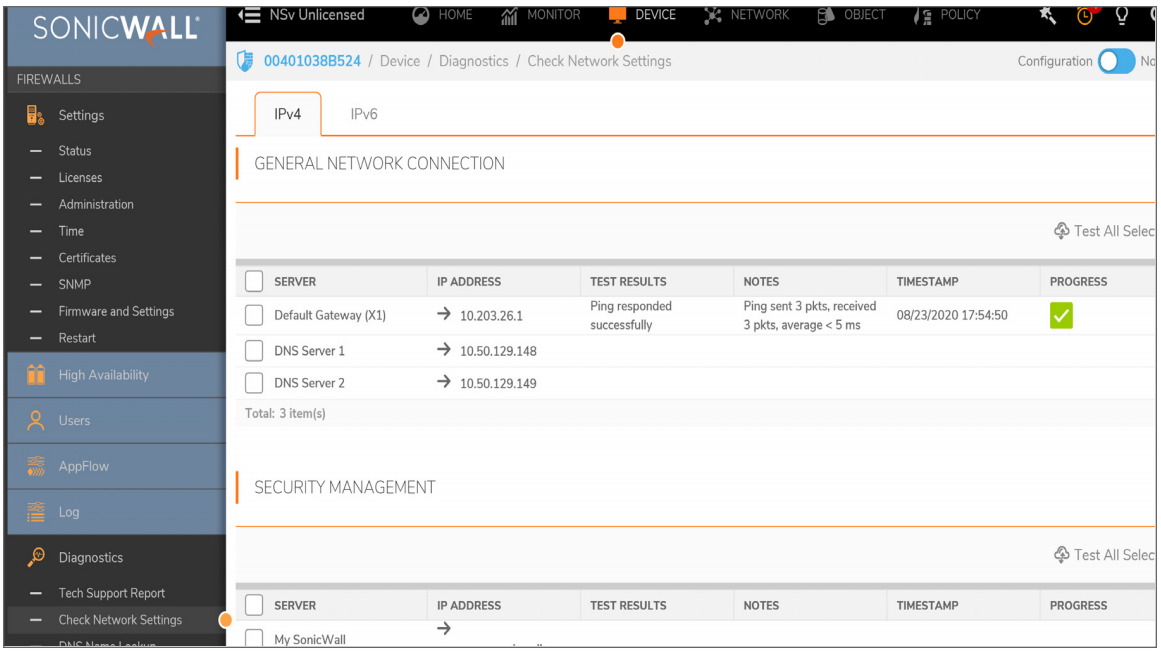
c. In the **Confirm Password** text box, re-enter the new password.

3. Click **Change Password**.

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

Using System Diagnostics

Check Network Settings, at **DEVICE | Diagnostics > Check Network Settings**. is a diagnostic tool that automatically checks the network connectivity and service availability of several predefined functional areas of the NSv Series, returns the results, and attempts to describe the causes if any exceptions are detected. This tool helps you locate the problem area when users encounter a network problem.



Specifically, Check Network Settings automatically tests the following functions:

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

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

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

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

5

Using the Virtual Console and SafeMode

Topics:

Connecting to the Management Console with SSH

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

Logging in by way of SSH is only possible through the certificate file configured during the NSv deployment.

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

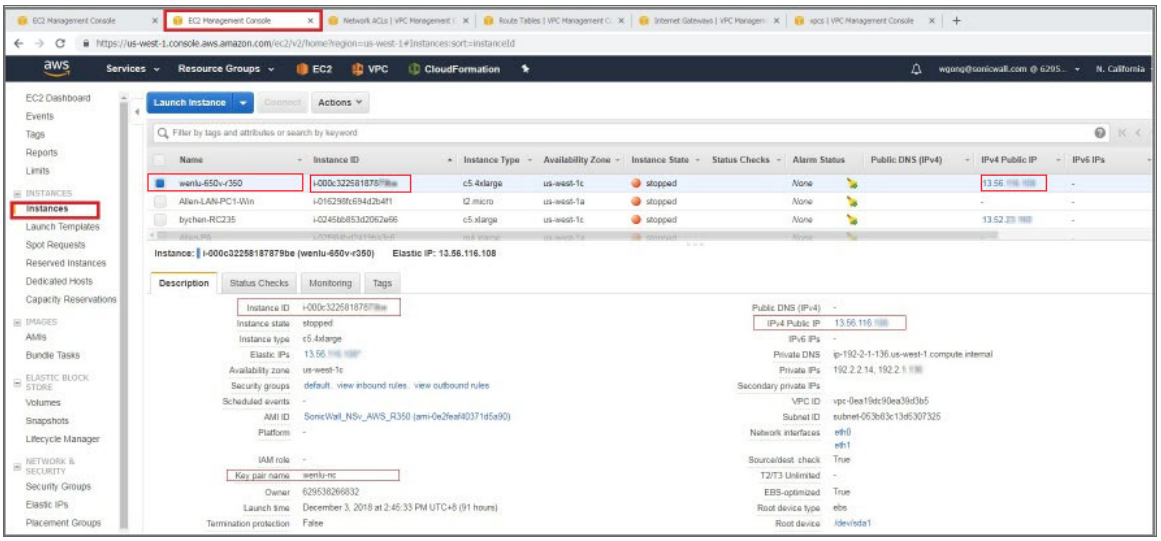
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstancesLinux.html

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 previously.
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 previously.
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
   ```

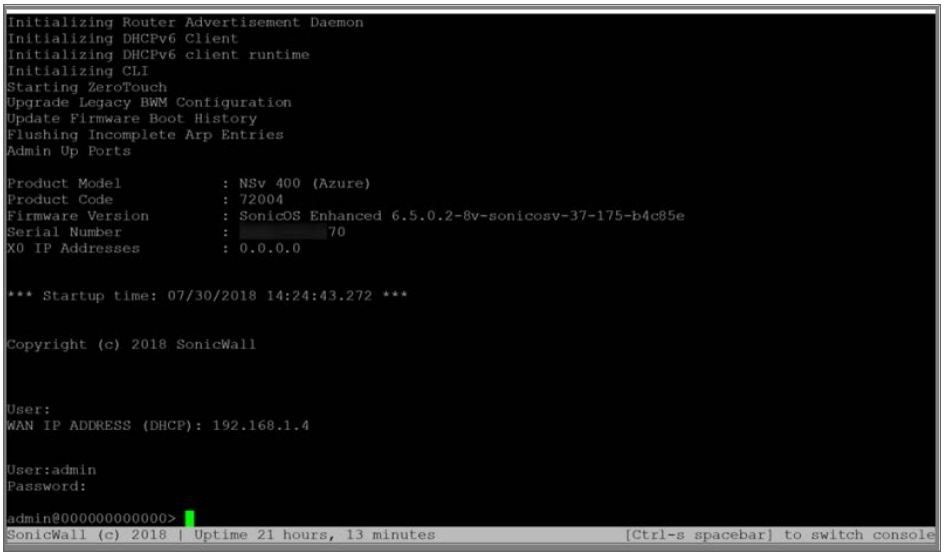
   From Windows, with PuTTY: in the Host Name box, enter `management@<public_dns_name>`.
6. The `.pem` (on Linux) or `.ppk` (on Windows) file created from the key pair for your NSv instance is used to authenticate the SSH session, as explained in the AWS documentation.

   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 CLI window by pressing **Ctrl+s** and then the **spacebar**. If you are prompted to log in at the **User** prompt,

7. Enter the SonicOS administrator credentials (default: ***admin / password*** where password is the Instance ID given by your SonicWall representative).



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

Navigating the NSv Management Console

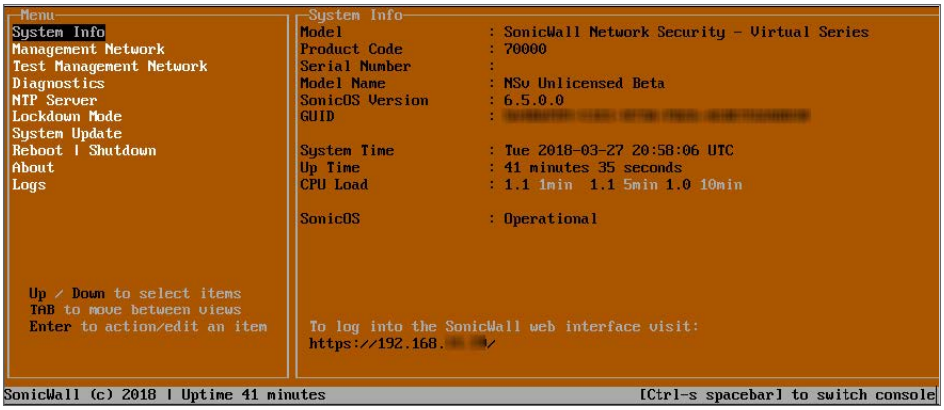
The NSv management console provides options for viewing and changing system and network settings, running diagnostics, rebooting SonicOS, and other functions.

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.

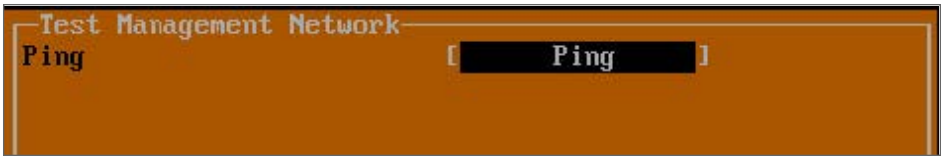
To navigate and use the management console:

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

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

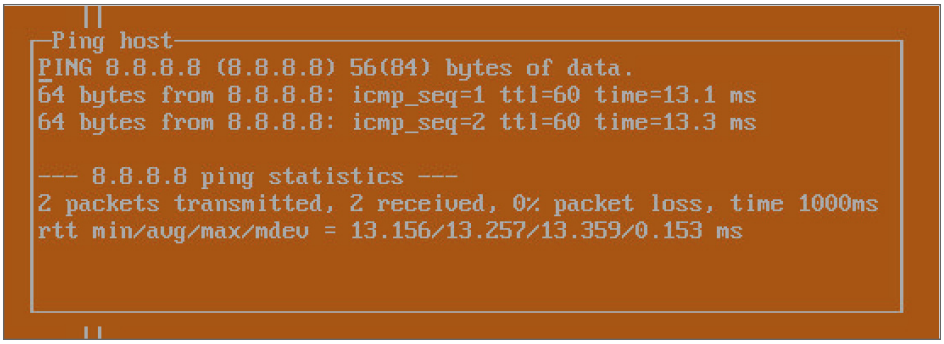


2. The main menu is displayed in the side menu (left pane). Use the up/down arrow keys to move the focus between menu items. As the focus shifts, the right pane displays the options and information for that menu item. The currently selected item is highlighted in black.
3. Press the **Tab** key to move the focus from side menu to the main view (right pane), or vice versa.
4. In the main view, use the up/down arrow keys to move the focus between options. Items shown inside square brackets denote actionable items.



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

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



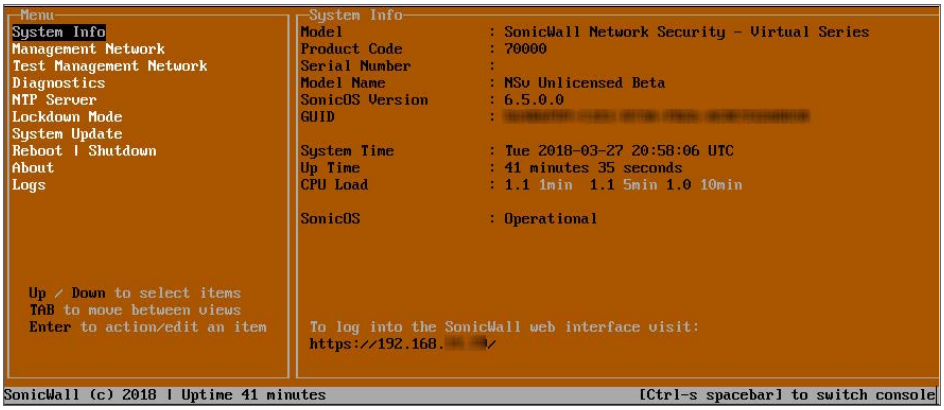
Some dialogs are for input:

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

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

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

System Info



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

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

Management Network or Network Interfaces

NETWORK INTERFACES SCREEN

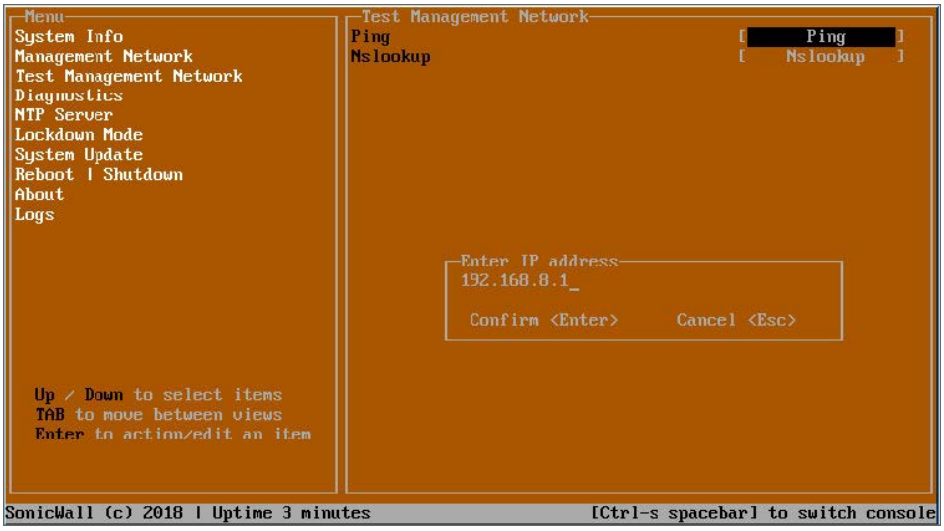
In this screen, the network settings are read-only except when the management console is in SafeMode. In SafeMode, you can configure these settings.

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

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

Test Management Network

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

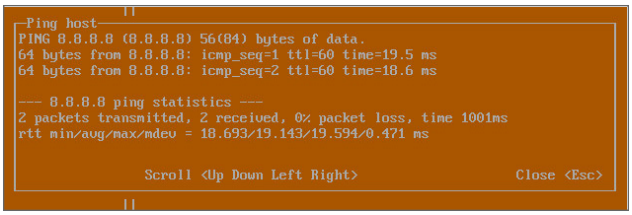


The **Test Management Network** screen provides the **Ping** and **Nslookup** tools to test connectivity between the management interface and the local network. **Ping** is used to test whether hosts in the network are reachable. **Nslookup** is available for sending DNS queries from the NSv virtual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

To use Ping:

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

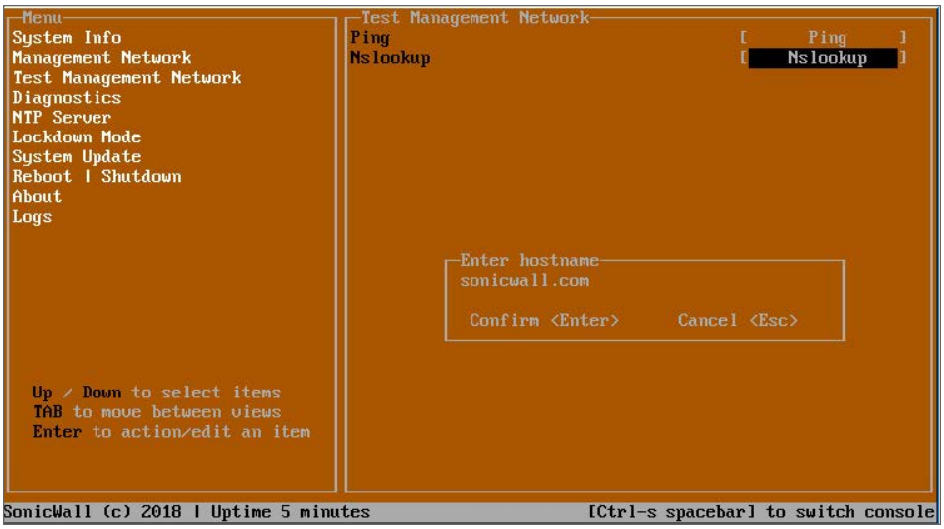
   The ping output is displayed in the **Ping host** dialog.



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.

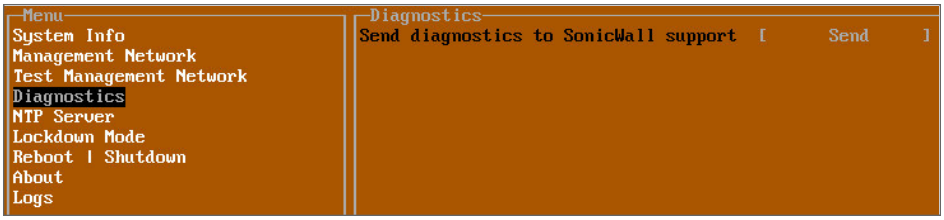


3. Navigate into the dialog, press **Backspace** to clear the current value, and then type in the hostname that you want to look up with a DNS query.
4. Press **Enter**.

   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.

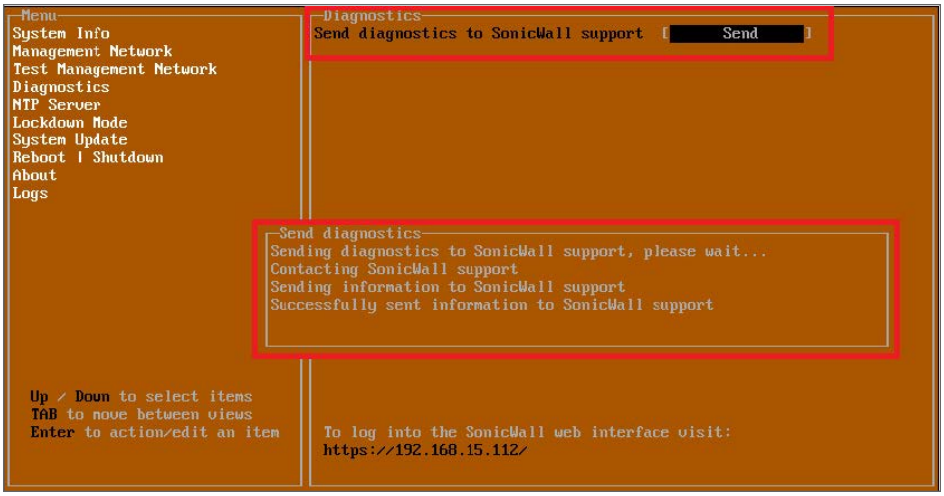
Diagnostics



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 virtual machine must have internet access to send the diagnostics report to SonicWall Support.

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



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

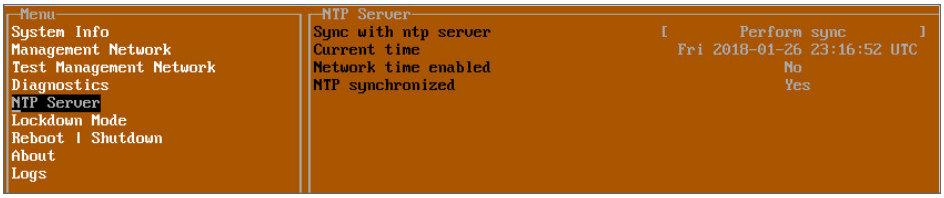
Any errors during the Send process are displayed in the **Send diagnostics** dialog box.

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

Lockdown Mode

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

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

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

Temporary Lockdown Mode

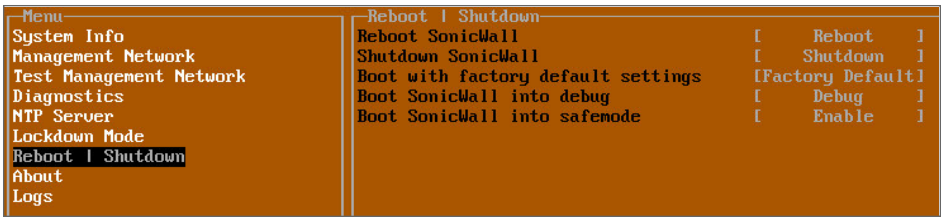
A temporary lockdown mode can be enabled and disabled in SonicOS on the **MANAGE | Appliance > Base Settings** page. You can enable lockdown mode by clearing the **Enable management console** checkbox under the **Advanced Management** section, and can disable lockdown mode by selecting the checkbox.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

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

System Update

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

Reboot | Shutdown

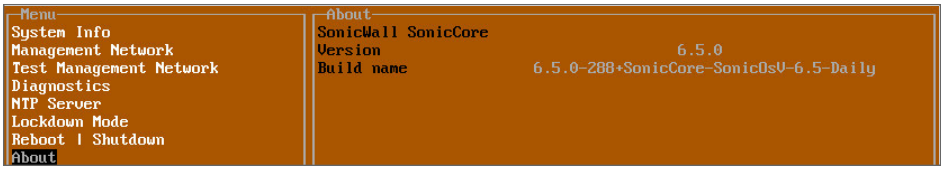


The **Reboot | Shutdown** screen provides functions for rebooting the NSv virtual machine, enabling debug mode, and enabling SafeMode. To perform an action, position the focus and then press **Enter** to select the desired action. Select **Yes** in the confirmation dialog, then press **Enter** again.

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

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

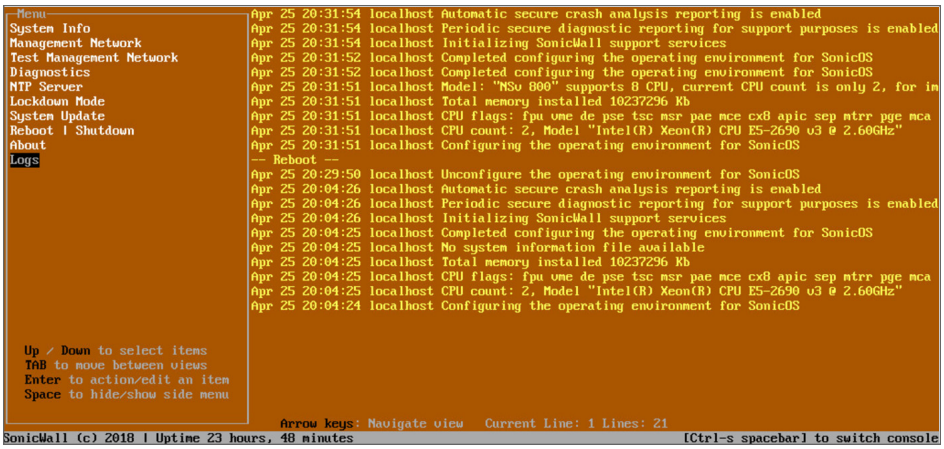
About



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

Logs

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



Using SafeMode on the NSv

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

Topics:

How Management Console Differs in SafeMode

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

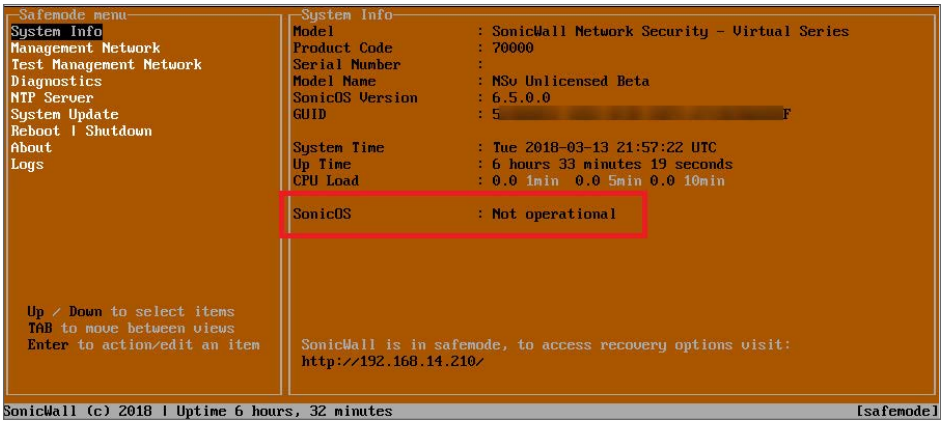
- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

  ⓘ | **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 Installing a New SonicOS Version in SafeMode for more information.

Topics:

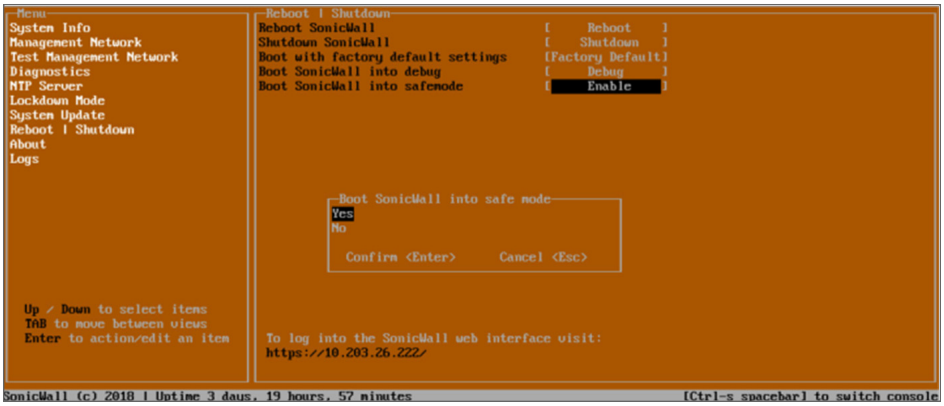
- Enabling SafeMode
- Disabling SafeMode
- Configuring the Management Network in SafeMode

Enabling SafeMode

SafeMode can be enabled from the management console.

To enable SafeMode:

1. Access the NSv management console as described in one of:
   - For NSv, see: Connecting to the Console with SSH
2. In the console, select the **Reboot | Shutdown** option and then press **Enter**.
3. Navigate down to the **Boot SonicWall into safemode** option to highlight **Enable**, and then press **Enter**.



4. Select **Yes** in the confirmation dialog.
5. Press **Enter**.

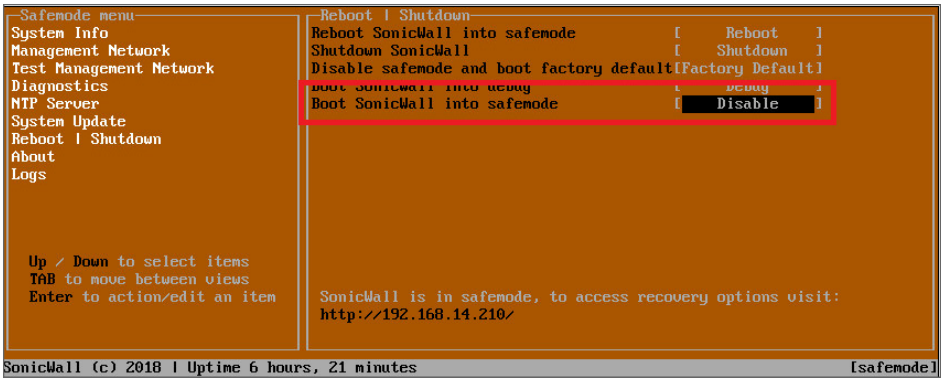
   The NSv immediately reboots and comes back up in SafeMode.

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

Disabling SafeMode

To disable SafeMode:

1. In the SafeMode menu in the NSv management console, select the **Reboot | Shutdown** option and press **Enter**.
2. In the **Reboot | Shutdown** screen, navigate down to the **Boot SonicWall into safemode** option to highlight **Disable**, and then press **Enter**.



3. Select **Yes** in the confirmation dialog.
4. Press **Enter**.

   The NSv immediately reboots and boots up in normal mode.

Configuring the Management Network in SafeMode

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

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

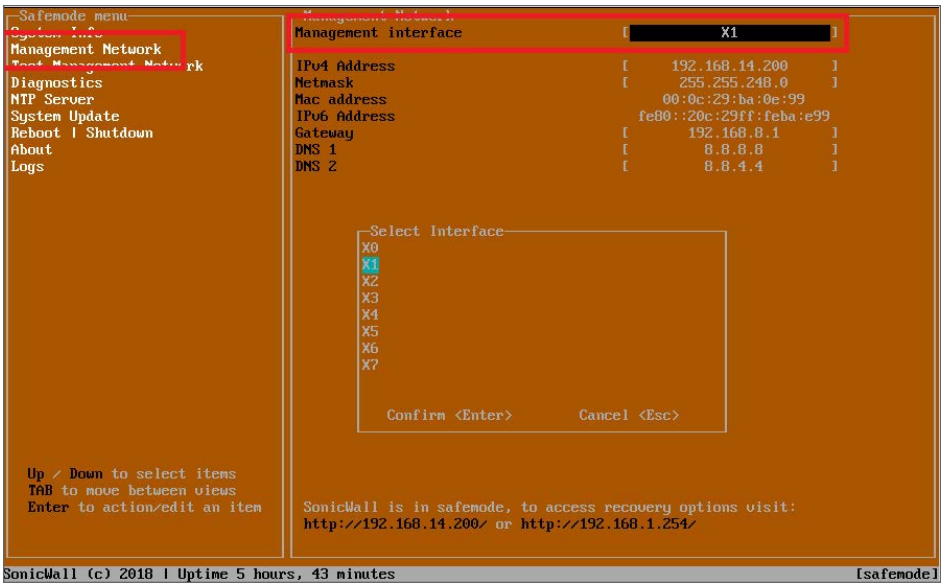
Changes made to interfaces in SafeMode are ***not*** persistent between reboots.

Topics:

- Configuring Interface Settings
- Disabling an Interface

Configuring Interface Settings

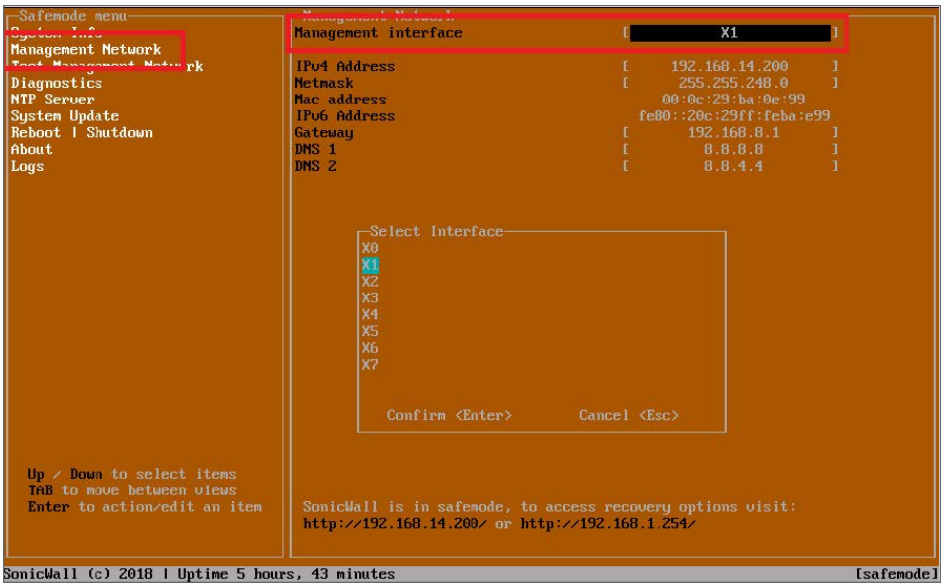
In SafeMode, the **Management Network** screen includes editable and actionable items that are read-only when the management console is in normal mode.



To edit an interface:

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

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



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

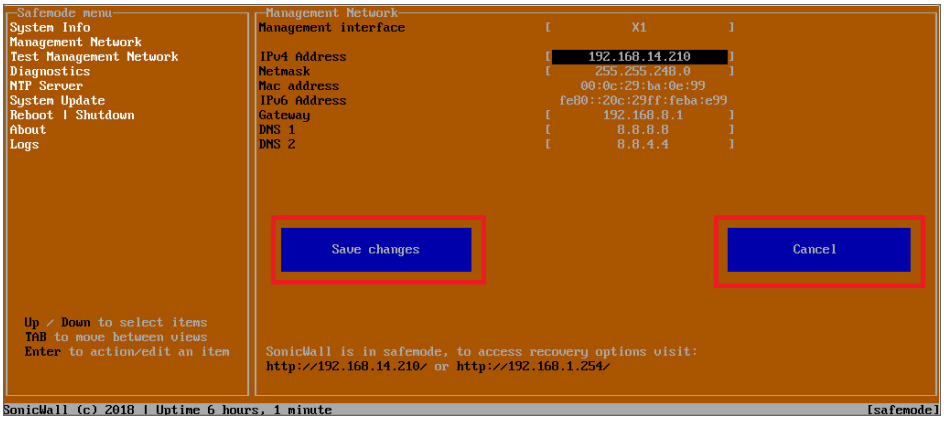
   The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed on the screen above the interface selection dialog.

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

   The on-screen dialog displays the current IP address.

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

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



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

Do one of the following:

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

Disabling an Interface

You can disable an interface while in SafeMode.

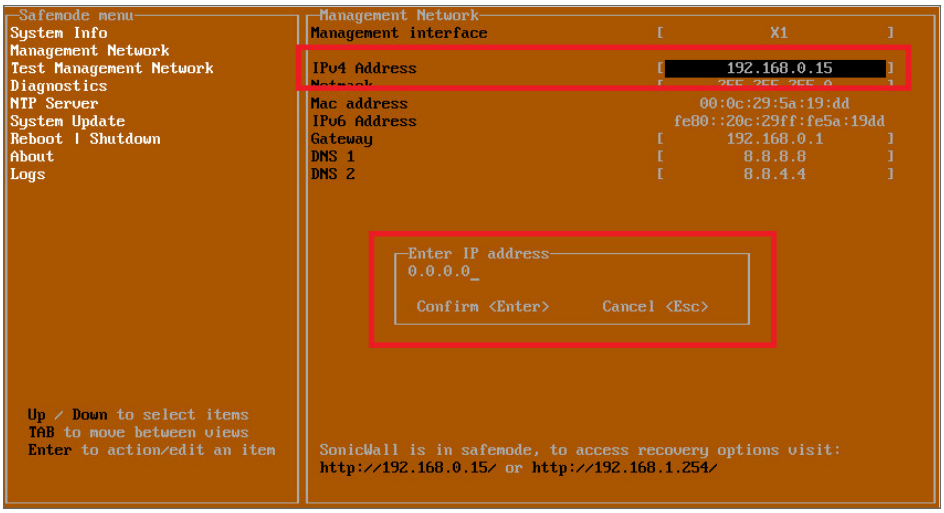
To disable an interface:

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

   The **Select Interface** list appears, displaying all of the interfaces available on the NSv.
3. Select the interface you wish to edit and press **Enter**.

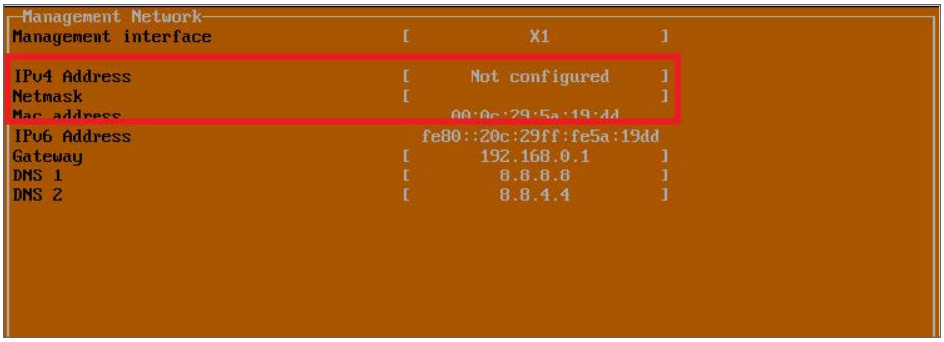
   The IPv4 and IPv6 addresses, Netmask, MAC address, Gateway, and DNS settings are displayed previously on the interface selection dialog.
4. Select **IPv4 Address** and press **Enter**.

   The onscreen dialog displays the current IP address.
5. Navigate into the dialog and change the IP address to `0.0.0.0`, then press **Enter**.



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

The interface is disabled.



Using the SafeMode Web Interface

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

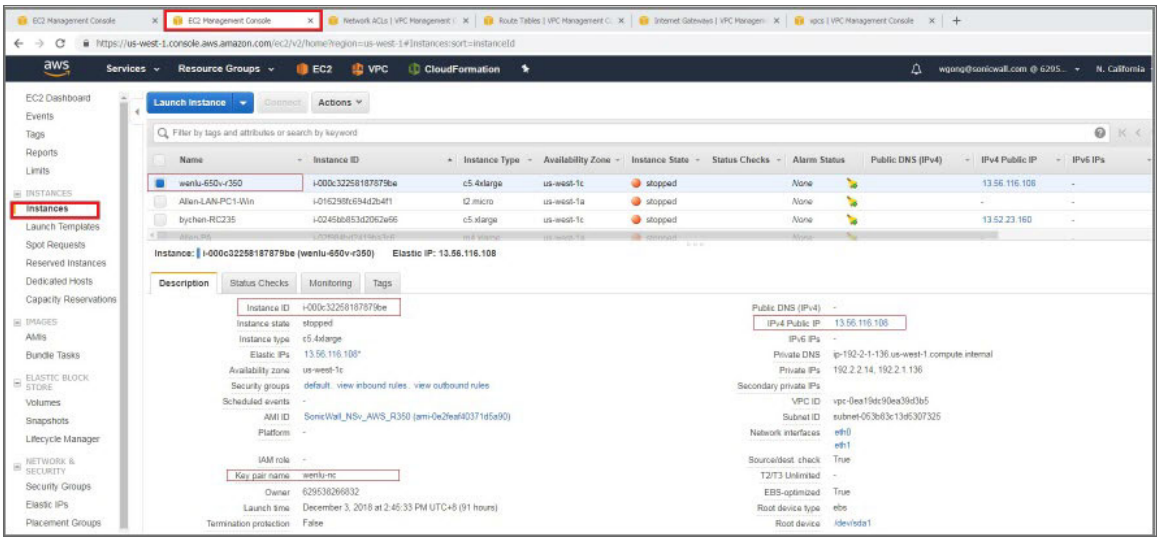
Topics:

- 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.

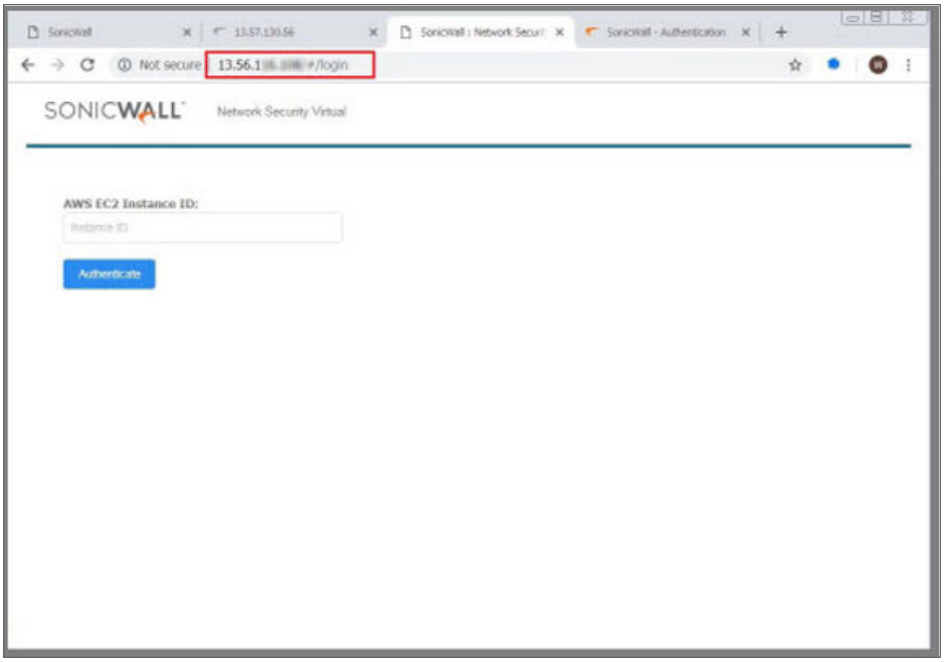


2. In the **Instances** page, locate the public IP address assigned to the NSv and the Instance ID for your NSv. You can access the SafeMode web interface at the public IP address of the NSv, and you must authenticate to gain access.

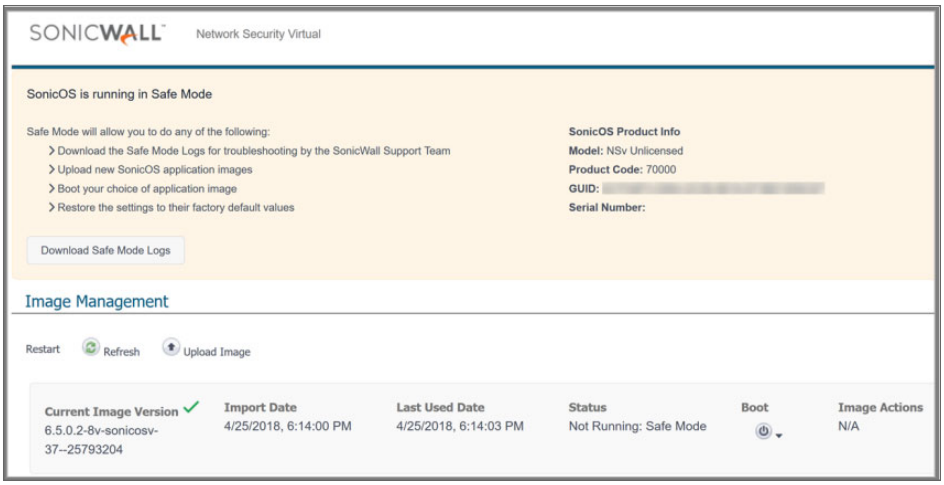
   ⓘ | **NOTE:** In SafeMode, the web management interface is only available by way of **http** (not https).

   The web interface address is also given on the management console screen as shown in the following image.

3. Go into the management console and boot into SafeMode. See **Entering SafeMode** under Using SafeMode on the NSv.
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.



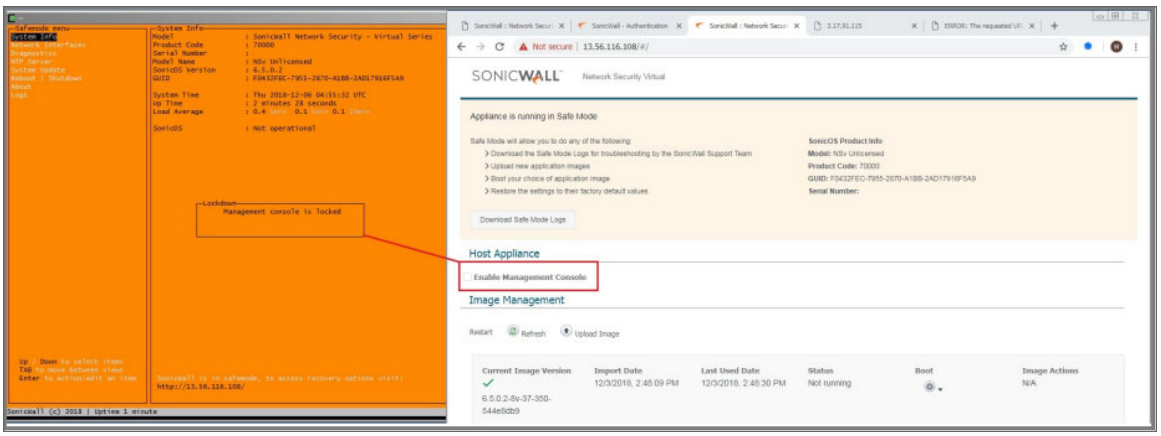
Entering/Exiting SafeMode

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 SafeMode and Disabling SafeMode).

Locking and Unlocking the Management Console

From the management web interface, the management console can be locked an unlocked as shown in the following image.



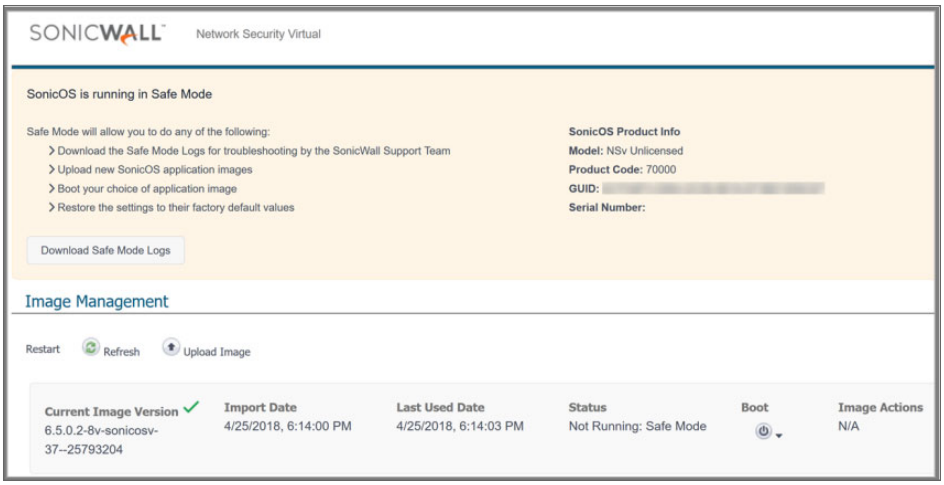
Downloading the SafeMode Logs

You can download logs of SafeMode activity.

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

Uploading a New Image in SafeMode

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

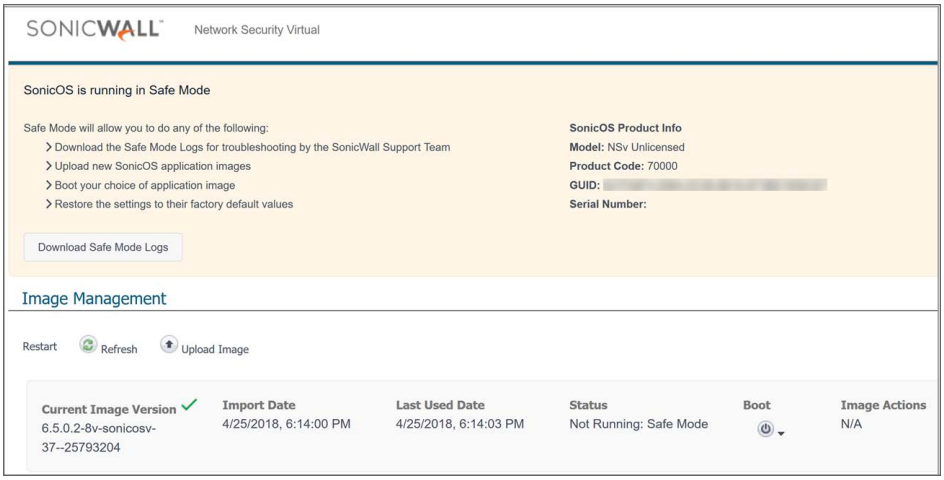
For additional information on uploading a new image, refer to: https://www.sonicwall.com/support/knowledge-base/?sol_id=180404172741874

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

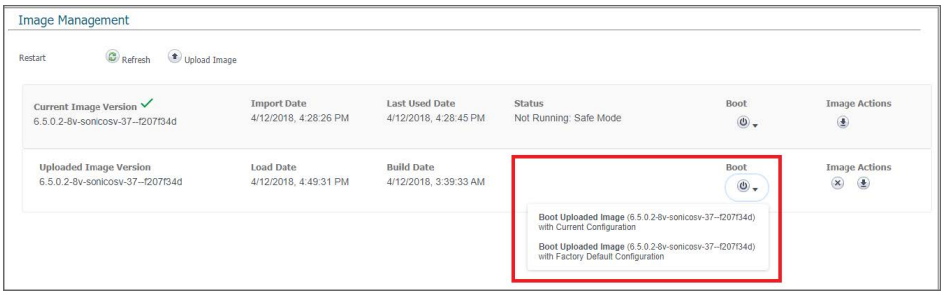
ⓘ | **NOTE:** In SafeMode, the web management interface is only available by way of **http** (not **https**).

To install a new SonicOS from SafeMode:

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



2. In the row with the uploaded image file, click **Boot** and select one of the following:
   - **Boot Uploaded Image with Current Configuration**
   - **Boot Uploaded Image with Factory Default Configuration**



The NSv virtual machine reboots with the new image.

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 https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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

About This Document

SonicOS NSv Getting Started Guide for the AWS Series
Updated - March 2023
Software Version - 7
232-005462-00 Rev F

End User Product Agreement

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

Open Source Code

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

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