



Contents

Introducing the NSv Series	. 4
Feature Support Information	. 5
Product Matrix and Requirements	. 7
Backup and Recovery Information	. 8
Exporting and Importing Firewall Configurations	. 9
Github Repository	. 9
Upgrading from SonicOS 6.5	. 9
Upgrading to a Higher Capacity NSv Model	. 10
Creating a MySonicWall Account	. 11
Installing SonicOS on the NSv Series	.13
Supported NSv Models	. 13
Resizing NSv Virtual Machine	. 14
Task List for NSv Instance Setup	. 19
Deploying AWS from Console	. 19
Deploying AWS from Cloud Template	.27
Accessing the SonicWall NSv Web Interface	.34
Forwarding Traffic to your NSv	. 37
Configuring Internet/Public Access Through the NSv	.39
SonicWall NSv Firewall on AWS GovCloud	
Deploying NSv from AWS GovCloud Console	
Creating a Security Policy for Outbound	
Applying Security Services on Policies in NSv for Outbound Traffic	
Deploying Windows 10 from Console	
Creating a Security Policy and NAT Policy for Inbound RDP to the VM	
Troubleshooting Installation Configuration Insufficient Memory Assignment	
PAYG Installation Errors	
Licensing and Registering Your NSv	
Registering the NSv Virtual Machine as BYOL from SonicOS	
Registering the NSv Virtual Machine as PAYG	. 62
SonicOS Management	
Managing SonicOS on the NSv Series	
Using System Diagnostics	.65

Using the Virtual Console and SafeMode	67
Connecting to the Management Console with SSH	67
Navigating the NSv Management Console	6
System Info	'1
Management Network or Network Interfaces	'2
Test Management Network	'3
Diagnostics	'5
NTP Server	'6
Lockdown Mode	'6
System Update	7
Reboot Shutdown	7
About	'8
Logs	'8
Using SafeMode on the NSv	'9
How Management Console Differs in SafeMode	'9
Entering SafeMode	'9
Enabling SafeMode	30
Disabling SafeMode	31
Configuring the Management Network in SafeMode8	31
Using the SafeMode Web Interface	35
Accessing the SafeMode Web Interface	36
Entering/Exiting SafeMode	37
Locking and Unlocking the Management Console8	38
Downloading the SafeMode Logs8	38
Uploading a New Image in SafeMode	9
SonicWall Support9)1
About This Document)2

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.

(i) 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.

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

Feature Support Information

(i) **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.

Functional Category Feature Area Feature **Unified Security Policy** Unified Policy combining Layer 4 to Source/Destination IP/Port/Service Layer 3 Rules 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

FEATURE SUPPORT LIST

Functional Category	Feature Area	Feature
		DoS Profile
	Signature Objects	
		AntiVirus Signature Objec
		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				
	SonicCoreX and SonicOS				
General	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

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

²Memory 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.

- (i) **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.
- 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.
- 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.

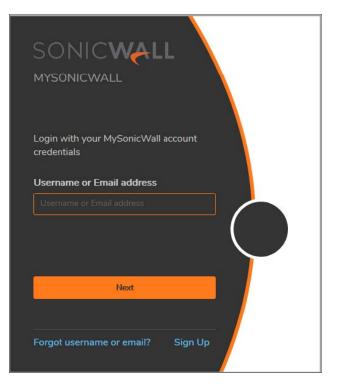
Creating a MySonicWall Account

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.

Installing SonicOS on the NSv Series

Topics:

- Supported NSv Models
- Resizing NSv Virtual Machine
- Task List for NSv Instance Setup
- Deploying AWS from Console
- Deploying AWS from Cloud Template
- Accessing the SonicWall NSv Web Interface
- Forwarding Traffic to your NSv
- Configuring Internet/Public Access Through the NSv
- SonicWall NSv Firewall on AWS GovCloud
- Troubleshooting Installation Configuration

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

2

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		

NEWLY SUPPORTED SIZES (VIRTUAL MACHINE SIZES)

- (i) **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.
- (i) **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.

Contact Us	Support 🕶	English -	My Account -	Sign In	Create an AWS Account

3. Fill in the details for successful sign in.

aws	
Sign in as IAM user	
Account ID (12 digits) or account alias	
1	
IAM user name	
Password	
Remember this account	
Sign in	
Sign in using root user email Forgot password?	

4. Click on EC2.

Con	Console Home Info				
	Recently visited Info				
Ð	EC2				
<u>8</u> -	IAM				

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

aws Services Q Sec
New EC2 Experience X
EC2 Dashboard
EC2 Global View
Events
Tags
Limits
Instances
Instances New
Instance Types
Launch Templates

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

Instances (1/94) Info			C	Connect	Instance state 🔺
Q Search					Stop instance
Name	♥ Instance ID	Instance state V Instan	ce type 🛛 🗸 Status check	Alarm status	Start instance
WAFv WAFv		⊘ Running @Q c5.xla	rge –	No alarms	Reboot instance

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

Instances (90) Info	0		C	Connect	nstance state 🔻	Actions v
Q Search						
Name	Instance state \bigtriangledown	Instance type \bigtriangledown	Status check	Alarm status	Availability Zone	♥ Public IP
WAFv WAFv	⊖ Stopped @Q	c5.xlarge	-	No alarms +	ap-south-1c	-

0	Connect Instance state	Actions Launch insta	ances
ck cks	Alarm status Availability Zone	Connect View details Manage instance state Instance settings Networking	2 F 1
cks	Change shutdown behavior Change instance type Change Nitro Enclaves	Security Image and templates Monitor and troubleshoot	• - 3
:cks :cks	Change credit specification Change resource based naming options Modify instance placement		6 1
	Modify Capacity Reservation settings Edit user data Allow tags in instance metadata	-	
	Manage tags		

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

EC2 > Instances > i-0095fe5aa10bdf030 > Change instance type		
Change instance type Info You can change the instance type only if the current instance type and the instance type that you want a	are compatible.	
Instance ID		
口 (WAFv)		
Current instance type		
c5.xlarge		
Instance type		
c5.xlarge		
c5.xlarge		
c5a.12xlarge		
c5a.16xlarge		
c5a.24xlarge	Cancel	Apply

(i) **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

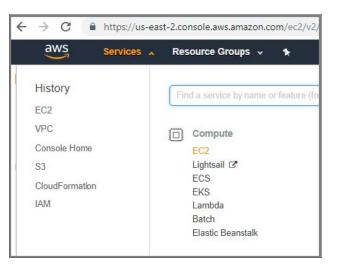
THEN:

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

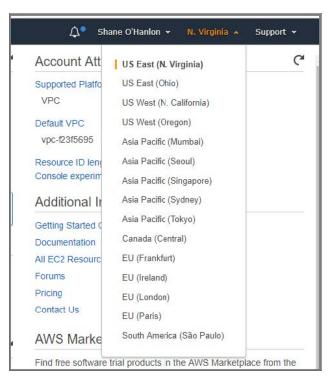
Deploying AWS from Console

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.

INSTANCES	10 Key Pairs	
Instances	0 Placement Groups	
Launch Templates		
Spot Requests	Create Instance	
Reserved Instances	To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2	nstanc
Dedicated Hosts	Launch Instance	
Scheduled Instances		
Capacity Reservations	Note: Your instances will launch in the US East (N. Virginia) region	
IMAGES	Service Health C	Sc
AMIs	Service Status:	USI
Bundle Tasks	US East (N. Virginia):	1

- 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).
 (i) 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	có large	2	4	EBS only	Yes	Up to 10 Gigebit	Yes
1	Compute optimized	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
10	Compute optimized	c6.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
	Compute optimized	c5 4:darge	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.

I. Choose AMI 2. Choose Instance Type	3. Co	nfigure Instanc	e 4. Add Storage	5. Add Tags	6. Co	nfigu	re Security Group
tep 3: Configure Instan			n multiple instances	from the same AMI	, requ	Jest S	Spot instances to ta
Number of instances	(1)	1		Launch into Auto	Scali	ng Gi	roup (j)
Purchasing option	(1)	Request	Spot instances				
Network	1	vpc-0ba966	00ddab58c09 exar	mple	Ŧ	С	Create new VPC
Subnet	1	Line and the second	c2e649082850e4 ≯ esses available	(1WAN us-east-2a	•		Create new subne
Auto-assign Public IP	1	Use subnet	setting (Disable)		¥		
Placement group	1	Add insta	nce to placement gr	oup.			
Capacity Reservation		Open			Ŧ	C	Create new Capa
IAM role	١	None			Ŧ	C	Create new IAM r
CPU options	(1)	Specify C	PU options				
Shutdown behavior	1	Stop			¥		
Enable termination protection	1	Protect a	gainst accidental ter	mination			
Monitoring			loudWatch detailed narges apply.	monitoring			
EBS-optimized instance	(1)	E Launch a	s EBS-optimized ins	tance			
Tenancy	1		in a shared hardwar harges will apply for		v		
Network interfaces (i)							
Device Network Interface	Subnet		Primary IP	Secon	dary	IP ad	ldresses
th0 New network interface 🔻 🛛	subnet-0	72c2e64 🔻	Auto-assign	Add IP			

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.

)evice	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
th0	New network interface •	subnet-072c2e64 ¥	Auto-assign	Add IP	Add IP
th1	New network interface 🔻	subnet-06321bdt •	Auto-assign	Add IP	
0		ddress feature for this in	stance is disabled beca	Ce use you specified multiple network interfaces. P address feature, please specify only the eth0 r	

- 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.

	existing one below. Learn more about Amazon EC2 security groups.			
	©Select an existing security group			
Security group name:	launch-wizard-5			
Description:	launch-wizard-5 created 2018-11-19T18:08:10.944+00:00			
ybe ①	Protocol (j)	Port Range ①	Source ①	Description (j)
SSH V	TCP	22	Custom • 107.154.75.50/32	SSH
Custom ICMP +	Echo Reply *	N/A	Custom • 107.154.75.50/32	e.g. SSH for Admin Desktop
Custom UDP I *	UDP	4500	Custom • 107.154.75.50/32	lpsec-nat-t
Custom UDP I *	UDP	500	Custom v 107.154.75.50/32	ISAKMP
ITTPS T	TCP	443	Custom • 107.154.75.50/32	HTTPS management

- 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.

hey allow btain the	ir consists of a public key that AWS stores, and a w you to connect to your instance securely. For Win e password used to log into your instance. For Linu SSH into your instance.	ndows AMIs, the private key file is required to
lote: The	e selected key pair will be added to the set of keys	authorized for this instance. Learn more
	moving existing key pairs from a public AMI.	
Crea	ate a new key pair	T
	pair name	
Soni	cWall-NSv-example	
		Download Key Pair
	You have to download the private key file (* pe it in a secure and accessible location. You wi again after it's created.	

- I. 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.

	is 👻 Resource Groups 👻 1					
C Dashboard	Create Route Table Delete Ro	ute Table Set As Main Ta	ble			2 0 0
by VPC:	QSearch Route Tables and their	×				\ll \leq 1 to 6 of 6 Route Tables
	Name	* Route Table ID	- Explicitly Assoc	iat+ Main +	VPC ~	
ual Private Cloud	SonicWall NSvRoute Table WA	N rtb-09bba975786ec	1 Subnet	No	vpc-00cc37c92d605f311 NSv VPC	
VPCs		rtb-0826b63bd5613	0 Subnets		vpc-026bc6832afd8be20 existing-vpc	
ets		rtb-0401b47029ba3	0 Subnets		vpc-00cc37c92d605f311 NSv VPC	
e Tables	existing-vpc-rtb-wan	rtb-0ea9f2ede1645	a 1 Subnet	No	vpc-026bc6832afd8be20 existing-vpc	
net Gateways	existing-vpc-rtb-lan	rtb-060a2b8556883	1 Subnet	No	vpc-026bc6832afd8be20 existing-vpc	
ss Only Internet ways	SonicWall NSvRoute Table LAM	tb-053b9ed4te028	d 1 Subnet	No	vpc-00cc37c92d605f311 NSv VPC	
oint Services Gateways	rtb-060a2b85568817fec existing Summary Routes		Route Propagation	Tags		88
ing Connections	Cancel Save View	: All rules				
urity	Destination	Target	Status Propa	gated Remove		
ork ACLs	10.0.0/16	local	Active No			
rity Groups	0.0.0.0/0	eni-08daf802f01eda6f4	No	0		
Connections	Add another route	eni-08daf802f01eda6f4	SonicWall NSv Inter	face LAN		
omer Gateways						
omer Gateways al Private Gateways						

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).

	es 👻 Resource Groups 👻 🐪					gula @ 3798-3630-3831 👻 Mumbai 💌	Support	
	-							
/PC Dashboard	Create Route Table Delete Route	Table Set As Main Table				C	0	0
Q Select a VPC	Q Search Route Tables and their X					<1 to 6 of 6 Rou	te Tables	623
	Name	* Route Table ID -	Explicitly Associal-	Main -	VPC -			
irtual Private Cloud	SonicWall NSvRoute Table WAN	rtb-09bbe975786ec		NO	vpc-00cc37c92d605f311 NSv VPC			
our VPCs	SUBCINE INSTITUTE LEW YOOK	rtb-0826b63bd5613	0 Subnets	Yes	vpc-026bc6832atd8be20 existing-vpc			
ubnets			0 Subnets	Yes	vpc-00cc37c92d605f311 NSV VPC			
oute Tables	existing-vpc-rtb-wan	nts-0ee912ede1645e	1 Subnet	No	vpc-026bc6832ald8be20 existing-vpc			
ternet Gateways	existing-vpc-rtb-lan	rtb-060a2b8556881	1 Subnet	No	vpc-026bc6832atd8be20 existing-vpc			
gress Only Internet ateways	Sonic/Wall NSvRoute Table LAN	ntb-053b9ed4fe028d	1 Subnet	No	vpc-00cc37c92d605f311 NSv VPC			
HCP Options Sets astic IPs								
ndpoints	rtb-0ea9f2ede1645ad25 existing-vpc	-rtb-wan						
indpoint Services AT Gateways	Summary Routes	Subnet Associations Ro	te Propagation	Tags				
eering Connections	Cancel Save			- age				
certify controling to	View: All	rules						
	Destination T	arget	Status Propagate	d Remove				
ecurity			Active No					
ecurity etwork ACLs	10.0.0.0/15							
etwork ACLs	10.0.0.0/16 lo	cai		0				
etwork ACLs ecurity Groups	0.0.0/0)	No	0				
etwork ACLs ecurity Groups PN Connections	0.0.0.0/0 Add another route	al Igw-05753b1d95f01fe97 ex H02dddc5b1fa57cd62 Sonic	No sting-vpc-igw	0				
	0.0.0.0/0 Add another route	gw-05753bid95001097 ex	No sting-vpc-igw	0				

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**.

aws	Services	*	Resourc	e Grou	ips 🗸 🛧					
Dedicated Hosts	• -	Allo	cate new a	ddress	Actions *					
Capacity Reservations		Q	Filter by tag	s and at	tributes or search	by keyw	ord			
IMAGES AMIs			Name		Elastic IP		Allocation ID	*	Instance	
Bundle Tasks					13.58.51.54		eipalloc-all(75-618			Release addresses
					13.58 127.241		elpalloc-traine bell		i-004db3ee9	Associate address
ELASTIC BLOCK STORE					52 14 222 51		eipalloc-miliation		i-0dcf39fe37	
Volumes					12 14 348 195		elpalloc data data		i-02aa41c53	Add/Edit Tags
Snapshots					52 15 153 87		eipalloc memory			
Lifecycle Manager										
E NETWORK & SECURITY										
Security Groups										
Elastic IPs										

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.

Addresses > Associate address				
Associate address				
Select the instance OR network interface to Resource type		tic IP address (13.5	851.54)	
Network interface	eni-06cbb45af81aa1dee	•	C	
Private IP	Select a private IP	•	CO	
Reassociation	Allow Elastic IP to be reassociated	l if already attached	0	
Warning If you associate an Elastic IP as	ddress with your instance, your current	public IP address i	s released. Learn more.	
				Cancel Associate

- 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.

	ONIC	2	
1	vetwork Se	curity Vir	tual
Username			
Password			

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

sonicwall-github Upd	ate readme file	Latest commit adapte 24 seconds ago
🖿 single-ami	upload launch page and templates first revision	2 minutes ago
README.md	Update readme file	24 seconds ago
E README.md		/
sonicwa	ll-nsv-aws-cf-templates	
SonicWall NSv - A	WS doud formation templates	
https://www.soni	owall.com/	
Deployi	ng	
Marketplac	e deployment	
Find the SonicWa	II NSv product in AWS Marketplace: https://aws.amazon.com/marketpla	ace/search/results?searchTerms=SonicWall
Cloud Form	nation Template deployment	
Deploy SonicWa	II NSv to an existing VPC	
Press the "Laund	Instance" button to deploy the SonicWall NS $\!\nu$ to an existing VPC.	
Launch Stack	0	
Deploy SonicWa	II NSv to a new VPC	
Press the "Laund	Instance" button to deploy the SonicWall $\text{NS}\nu$ to a new VPC.	
Launch Stack	0	

- 3. To select a Region, identify the region into which you wish to deploy NSv.
 - (i) **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 ~ 1		۵	smadugula @ 3798-3630-3831
CloudFormation ~	Stacks > Create Stac	×		
Create stack				
Select Template Specify Details	Select Template			
Options Revew	Seect the template that descr	bes the stack that you want to create. A stack is a group of related resou	urces that yo	cu manage as a single unit.
	Design a template	Lise AWS ClaudFormation Designer to create or modify an existing tem Design template	nplate Lean	n more.
	Choose a template	A template is a JSCNVYAML-formatted text file that describes your stat	ck's resourc	es and their properties. Leam mor
		 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/Ed	It tempate in Designer

5. Click Next.

Specify Details Specify Details Specif	eate stack			
book paties have a parameter values. Vou can use or change the default parameter values, which are defined in the AWS Cloud/Foundation template. Lean more. Stack name conception of the State of the S		Specify Details		
Parameters Project Project, Name Sonic/Will NBy Project, Name Sonic/Will NBy Test and Project, Name Sonic/Will NBy Ausliability Zom Sonic/Will NBy Sonic Will NBy The will be in Add Semources tag Instance Sonic/Will NBy Instance Name S	ions	Specify a stack name and para	meter values. You can use or change the default	parameter values, which are defined in the AWS CloudFormation template. Learn more.
Project Project Name Sonic/Mail NSv The with be in AMS resources tog Location Availability Zone ap-outh-1a Description Beter the AMS Availability Zone Instance ami-03030bc/22000b7/861 Mail mi-03030bc/22000b7/861 Instance Name Sonic/Mail NSv Instance Name Sonic/Mail NSv Instance Type Goldrige Instance Type		Stack name	SonicWall-NSv	
Project Name Sonic/Wall N5y The will be in AVIS resources tog Location Instance Instance Instance Sonic/Wall N5y New N5y instance Name Sonic/Wall N5y New N5y instance Name Sonic/Wall N5y Instance Name Sonic/Wall N5y New N5y instance Name Instance Name Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per Iame Instance Stop Per		Parameters		
Location Availability Zone ap-south-1a ap-south-1a benct the XMS Availability Zone Instance AMI ami-00305bc22808b7861 SenictVall NSV New NSV Instance Name Control Name Contro		Project		
Availability Zom ap-studh-11 Better the AVKE Availability Zome Instance Instance Xmm Scinic/Vall XMV Instance Type Childred Instance Type Operational Exact Physics		Project Name	SonicWall NSv	This will be in AWS resources tag
Better the XMS Availability Zone Instance Attile ami-03030bc2202005/7861 Instance Name Sonic/Mail NSv Instance Name Sonic/Mail NSv Instance Type Charge Instance Type Charge <td></td> <td>Location</td> <td></td> <td></td>		Location		
AMI ami-0.0030bcbc22808b7861 SknickNat Nik AAA ID Instance Name ScnicKNall NDv New Kitk instance Name Instance Type C6.large Sketc the type of Instance Key Paar smachulyule-steve-munchal Instance Name Allow management (ssinVhitphttphtp) from this Sketc the UDP from which management access (http./ttpstel) is allowed on WAN interface. Must be in IP-4 ODP notation: x.x.x.kx WAN Subset ID submet-0480348e025c1e325e (192.168.f.,, • Enry LWA Submet ID LAN Interface Subset ID submet-0480348e025c1e325e (192.168.f.,, • Enry LWA Subset ID Uptionall Existing Elseito IP Address (EIP) Address (EIP) VPC Vpc:00027/682e0505111 (192.168.L., •		Availability Zone		
Instance Name Social/Wall Nov New Klov Instance Name Collarge Coll		Instance		
C5.large C5		AMI	ami-0303bbc22808b7861	SonicWall NSv AMI ID
Key Pair immadugula-deve-mumbbal Intance Key Pair Name intance Key Pair Name Allow management (sel/hitp/htp/htp/htp/htp/htp/htp/htp/htp/htp/h		Instance Name	SonicWall NSv	New NSv Instance Name
				Select the type of instance
		Key Pair		
Enter WAN Bubmet ID LAN Interface Submet ID submet-0959e35849f0/c2bb05 (192.168.1, Enter LAN Bubmet ID (Optional) Existing Elastic IP Address (EIP) IP Address (EIP) Address (EIP) Address (EIP) Address (EIP) Address (EIP) Address (EIP) Vpcd Vpcd Vpcd Vpcd Vpcd Vpcd Vpcd Vpcd		(ssh/http/https) from this		, https://shi is allowed on WAN interface, Must be in IPv4 CIDR notation: x.x.x.v/x
Coptional) Existing Elastic IP Address (EIP VPC		WAN Subnet ID		
IP Address (EIP) Alocation ID of an existing Elastic IP (EIP), The EIP is associated to the WAN interface of the NSx. A new EIP will be allocated if left blank VPC Vpcl Vpcl Vpcl Vpcl Vpcl Vpcl Vpcl Vpcl		LAN Interface Subnet ID		
Vpcid vpc-00cc37c82d605f311 (192.168.0.001, •			Allocation ID of an existing Elastic IP (EIP). The EIP is a	associated to the WiAN interface of the NSx. A new EIP will be allocated if left blank
		VPC		
		Vpcld		

- 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

Vpcld: Select existing VPC to which to deploy NSv.

8. Click Next.

CloudFormation	 Stacks > Create Stack 			
Create stack				
Select Template	Options			
Specify Details Options	Tags			
Review		resources in your stack. You can add up	to 50 unique key-value pairs for each stack. Learn more.	
	Key (127 characters maximum)		Value (255 characters maximum)	
	1			
	Permissions			
		rmation uses to create, modify, or delete	resources in the stack. If you don't choose a role, CloudFor	mation uses the permissions defined i
	your account. Learn more.			
		a role (optional)		
	Enter role	am		
	 Rollback Triggers 			
	Rollback triggers enable you to have AWS		ar application during stack creation and updating, and to ro	lback that operation if the application
	breaches the threshold of any of the alarm	s you've specified. Learn more		
	Monitoring Time 0 0-180	‡ Minutes		
		value of 0. Maximum value of 180.		
				Available triggers remaining:
	1 AWS::CloudWatch::Alarm		ARN (Amazon Resource Name)	
	AWSGOUDWARDT.Alenn			
	Advanced			
	You can set additional options for your sta	ick, like notification options and a stack p	olicy. Learn more.	
				Cancel Previous Next

9. Click Next.

aws Services ~	Resource Groups 🗸 🔸			31 ~ Mumbai ~ Support ~
CloudFormation ~	Stacks > Create Stac	<		
120000000000000000000000000000000000000				
Create stack				
Select Template	Review			
Specify Details				
Options Review	Template			
- Contraction		https://s3.amazonaws.com/nsv-cfn-dev/of-existing-vpc.template		
		SonicWall NSv CloudFormation Template to deploy NSv in an existing VPC Unk is not available		
	Details			
	Stack name:	Sonic/Wall-NSv		
	Project ProjectName	Sonic/Wall NSv		
	Location	SAN INSTERN PROF		
	AvailabilityZone	ap-south-1a		
	Instance			
		ami-0303bbc22808b7861		
	InstanceName InstanceType			
	KeyPairName	smadugula-aws-mumbai		
	ManagementWhitelistCidr			
		subnet-0449348e025c1e32e subnet-099e53649f2c2bf05		
	ExistingEipAllocationId			
	VPC			
	Vpcld	vpc-00cc37c92d605f311		
	Options			
	Tags			
	No tags provided			
	Rollback Triggers			
	No monitoring time provided			
	No rollback triggers provided			
	Advanced			
	Notification	Rischief		
	Termination Protection Timecut			
	Rollback on failure			
	Quick Create Stack (Create stac	iss similar to this one, with most details auto-populated)		
				Cancel Previous Create
				Closed
🗬 Feedback 🔇 English (US)		@ 2008 - 2018 Amazon 18	b Services, Inc. or its affiliates. All rights n	eserved. Privacy Policy Terms of Use
reduback by English (US)		10 2006 - 2016, Amazon Ve	to the noos, exercises annuales. All rights r	and room privately rolley terms of Use

10. Review details and click Create.

Cloud	Services		e Groups 🗸 🤸				۵	smadugula @ 3798-363		Mumbai Y	Support	
Create Stac	k - Action	ns -	Design template								C	0
Filter: Acti	By Stack P	Name								Sho	wing 2 st	tacks
Stack	Name		Created Tim	10	Status		Description					
SonicV	Vall-NSv-1		2018-10-04	23:57:32 UTC+05	50 CREATE_IN	PROGRESS	SonicWall NSv CloudFon	nation Template to deple	y NSv in an ex	isting VPC		
SonicV	Vall-NSv		2018-10-04	23:44:19 UTC+05	50 CREATE_CO	MPLETE	RepialAlall MSv ClaudEan	nation Template to depk	y NSv in a nev	VPC		
			2010-10-04									
Overview	Outputs Re	esources E	zents Template	Parameters	Tags Stack Pol						-	=
Overview	Outputs Re	esources Et	_		Tags Stack Pol						=	8
Overview	Outputs Re	esources En	_		Tags Stack Pol	icy Change Set						=

11. Status changes to **CREATE_COMPLETE**.

Actions	s - Desig	n template					C O
e · By Stack N	lame					1	Showing 2 stacks
tame		Created Time	Status	De	scription		
all-NSv-1		2018-10-04 23:57:32 UTC+05	50 CREATE_COM	PLETE So	nicWall NSv CloudFormation Ter	nplate to deploy NSv in an existing VPC)
all-NSv		2018-10-04 23:44:19 UTC+05	50 CREATE_COM	PLETE So	nicWall NSv CloudFormation Ter	plate to deploy NSv in a new VPC	
Outputs Re	sources Events	Template Parameters	Tags Stack Policy	Change Sets	Rollback Triggers		880
Outputs Re	sources Events		Tags Stack Policy		Rollback Triggers	Fxport Name	880
Outputs Re	sources Events	Value		Change Sets Description	Rollback Triggers	Export Name	880
Outputs Re	sources Events		ibai.pem management@	Description	Rollback Triggers	Export Name	
	ame all-NSv-1	ame all-NSv-1	ame Created Time all-NSv-1 2018-10-04 23:57:32 UTC+05	Created Time Status BI-NSv-1 2018-10.04 23:57:32 UTC+0550 CREATE_COM	Created Time Status De BI-NSv-1 2018-10-04 23:57:32 UTC+0550 GREATE_COMPLETE Soc	Created Time Status Description ail H5v-1 2018-10-04 23:57:32 UTC-0550 CREATE_COMPLETE SonicWall N5v CloudFormation Tem	Bit Work Created Time Status Description all NSv-1 2015-10-04 23:57:32 UTG-0550 CREATE_COMPLETE SonicWall NSv CloudFormation Template to deploy NSv in an existing VPC

- 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.

EC2 Dashboard Events	Launch Instand	Consec	ct Actions ~							4	0	• 6
Tags	Q. Filter by tag	s and attributes or se	earch by keyword						ØK	< 1 to	1 of 1	> >
Reports	Name	- Instance ID	- Inst	tance Type	- Availability Zone -	Instance State -	Status Checks -	Alarm Statu	s Public DNS (IPvi	6) -	IPv4 Pv	ublic IP
Limits	SonicWall	NSv i-0c6b32aa	163026d20 c5.1a	arge	ap-south-1a	🥥 running	2/2 checks	None	6		13.232	198.249
INSTANCES												
Launch Templates												
Spot Requests												
Reserved Instances												
Dedicated Hosts												
m IMAGES	Instance: 1-00	6b32ead63026d20	(SonicWall NSv	 Elastic 	IP: 13.232.198.249						-	
AMIs					IP: 13.232.196.249							80
	Description	Status Checks	Monitoring	7) Elastic	IP: 13.232.196.249							80
AMIs Bundle Tasks		Status Checks Instance D	Monitoring	Tags	IP: 13.232.196.249		Public DNS (IPv4)					
AMIs Bundle Tasks		Status Checks Instance ID Instance state	Monitoring I-0c6b32ead630 running	Tags	IP: 13.232.198.249		IPv4 Public IP	13.232.198	249		-	80
AMIs Bundle Tasks		Status Checks Instance ID Instance state Instance type	Monitoring i-0c6b32ead630 running c5.Jarge	Tags 026d20	IP: 13.232.196.249		IPv4 Public IP IPv6 Ps	13.232.198.		interna		
AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes		Status Checks Instance ID Instance state	Monitoring I-0c6b32ead630 running	Tags 026d20	IP: 13.232.196.249		IPv4 Public IP	13.232.198. - ip-192-168-	249 0-4.ap-south-1.compute. , 192.168.1.121	interna		
AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager		Status Checks Instance ID Instance state Instance type Elastic IFs	Monitoring I-Oc6b32ead630 running c5.large 13.232.198.249 ap-south-1a SonicWall-NSy-	Tags 126d20 NSvSecGrpW	han-7J2P8ASWNK58.		IPv4 Public IP IPv6 Ps Private DNS	13.232.198. - ip-192-168-	0-4.ap-south-1.compute.	interna		
AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager NETWORK & SECURITY		Status Checks Instance ID Instance stale Instance type Elestic IPs Availability zore Security groups	Monitoring i-0c6b32ead630 running c5.Jarge 13.232.198.249 ap-south-1a SonicWall-NSv- view inbound no	Tags 126d20 NSvSecGrpW Jes. view out	han-7J2P8ASWNK58.		IPv4 Public IP IPv6 Ps Private DNS Private IPs Secondary private Ps	13.232.198 - ip-192-168- 192.168.0.4	0-4.ap-south-1.compute. , 192.168.1.121	internal		
AMIs Bundle Tasks ELATIC BLOCK STORE Volumes Snapshots Lifecycle Manager Security Groups		Status Checks Instance ID Instance state Instance type Elestic IPs Availability zone Security groups Scheduled events	Monitoring i-0x6b32ead630 running c5.large 13.232.198.249 ap-south-1a SonicVMI-NSv- view inbound ru No scheduled e	Tags 126d20 NSvSecGrpW des. view outb	lan-7J2P9ASWNK58 . bound nules	5	IPv4 Public IP IPv6 Ps Private DNS Private IPs Secondary private IPs VPCID	13.232.198. - ip-192-168- 192,168.0.4 vpc-00cc37	0-4.ap-south-1.compute. , 192.168.1.121 c92d805f311	internal		
AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager NETWORK & SECURITY		Status Checks Instance ID Instance stale Instance type Elestic IPs Availability zore Security groups	Monitoring i-0c6b32ead630 running c5.Jarge 13.232.198.249 ap-south-1a SonicWall-NSv- view inbound no	Tags 126d20 NSvSecGrpW des. view outb	lan-7J2P9ASWNK58 . bound nules		IPv4 Public IP IPv6 Ps Private DNS Private IPs Secondary private Ps	13.232.198. - ip-192-168- 192,168.0.4 vpc-00cc37	0-4.ap-south-1.compute. , 192.168.1.121	interna		

- 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.

aws service:	s 👻 Resource Groups 👻 🐈				🗘 smad	
		10			20045 - Miller	
PC Dashboard	Create Route Table Delete Rout	e Table Set As Main Ta	ble			2 0
iter by VPC:	QSearch Route Tables and their >					1 to 6 of 6 Route Tables > 3
C DERCLA VPC	Name	Route Table ID	- Explicitly Ase	sociat - Main -	VPC v	
irtual Private Cloud						
our VPCs	SonicWall NSvRoute Table WAN	ntb-09bba975786ec			vpc-00cc37c92d605f311 NSv VPC	
ubnets		ntb-0826b63bd5613			vpc-026bc6832afd8be20 existing-vpc	
oute Tables		rtb-0401b47029ba7			vpc-00cc37c92d605f311 [NSv VPC	
ternet Gateways	existing-vpc-rtb-wan	rtb-Oea9f2ede1645s			vpc-026bc6832afd9be20 existing-vpc	
gress Only Internet	existing-vpc-rtb-lan SonicWall NSvRoute Table LAN	nb-060a2b8556881 nb-053b9ed4te028c			vpc-026bc6832a/d8be20 existing-vpc vpc-00cc37c92d606f311 NSv VPC	
ateways	Sonewai Novhoule Table DAV	10/05209604160280	I outriet	NO	Abconcestentingeneration and abo	
HCP Options Sets						
lastic IPs						
ndpoints						
ndpoint Services	rtb-060a2b85568817fec existing-v	pc-rtb-lan				880
AT Gateways	Summary Routes	Subnet Associations	Route Propagatio	n Tags		
eering Connections	Cancel Save					
	View:	All rules				
iecurity	Destination	Target	Status Pro	pagated Remove		
etwork ACLs	10.0.0/16	local	Active No			
ecurity Groups	0.0.0/0	eni-08dat802f01eda6f4	No	0		
PN Connections		eni-08daf802f01eda6f4				
	Add another route	em-oedaro02101eda614	Serie real (NSV II)	ternice DAN		
ustomer Gateways						
irtual Private Gateways						
PN Connections						

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

CloudFormation Manage X ← → C ^a ☆		S3 Management Console X sole.aws.amazon.com/vpc/hon				EC2 Management Conso: X	icanhazip.com/	× +		=
aws services						\$ smadugula @ 3798	-3630-3831 • Mumbal •			
VPC Dashboard Filter by VPC	Greate Route Table Delete Roo	ute Table Set As Main Table	i -				4	•	0	į.
Q Select a VPC	Q Search Route Tables and their	×					< 1 to 6 of 6 F	toute Tab	les>>	
Virtual Private Cloud	Name	* Route Table ID -	Explicitly Associa	l- Main -	VPC -					
Your VPCs	SonicWall NSvRoute Table WAT	4 ntb-09bba975786ec	1 Subnet	No	vpc-00cc37c92d605f311 NSv VPC					2
Subnets		rtb-0826b63bd5613	0 Subnets	Yes	vpc-026bc6832afd8be20 existing-vpc					
Route Tables		mb-0401b47029ba7	0 Subnets	Yes	vpc-00cc37c92d605f311 NSv VPC					
	existing-vpc-rtb-wan	rtb-0ea9f2ede1645a		No	vpc-026bc6832ald8be20 existing-vpc					
Internet Gateways	existing-vpc-rtb-lan	rtb-060a2b8556881		No	vpc-026bc6832afd8be20 existing-vpc					-
Egress Only Internet Gateways	SonicWall NSvRoute Table LAN	rtb-053b9ed4fe028d	1 Subnet	No	vpc-00cc37c92d605f311 NSv VPC					-
Endpoint Services	rtb-0ea9f2ede1645ad25 existing								80	-
NAT Gateways Peering Connections	Summary Routes	Subnet Associations Ro	te Propagation	Tags						-
Peering Connections		All rules								
Security	Destination	Target	Status Propaga	ated Remove						
	10.0.0.0/16	local	Active No							
Security Groups	0.0.0.0/0	[No	0						
VPN Connections	Add another route	igw-05753b1d95f01fe97 ex	sting-spo-igw							
Customer Gateways		I-02dddc5b1fa57cd62 Sonid								
Virtual Private Gateways										
VPN Connections										
	2224				100 W 100			2.2 2		
🗨 Feedback 🧐 English	(US)				0 2008 - 2018					

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**.

	4									
Tags	Q, Filter by tag	s and attributes or se	arch by keywo	and						
Reports	Name	< Instance ID		Instance Type ·	Availability Zone +	Instance State - Status Checks	- Alarm Statu	s Public DNS (IPv4)	* IPv4 Public IP *	IPv6 IPs - Key Nam
imita		i-01e		t2 micro	us-east-2a	stopped	None	¥.		
ISTANCES		1-02¢		c4 large	us-east-2a	stopped	None	>	and the second second	 Internet
stances	1	1-035		t2 micro	us-east-2a	stopped	None	>		
unch Templates	10 mm	+044		t2 micro	us-east-2a	stopped	None	a ec2-	a and a second se	
ot Requests	() and ()	+0.85	-	t2 medium	us-east-2a	stopped	None	>		
served instances		1-08#		t2 micro	us-east-2c	stopped	None	5		
dicated Hosts	10 mm	1-08e	-	t2 micro	us-east-2a	stopped	None	\$		
uges.	El man	-0a16	-	t2 micro	us-east-2a	stopped	None	S.		- 4
lls	0	i-0e61		t2 micro	us-east-2b	stopped	None	5		
ndle Tasks	R19888			c4 large	us-east-2a	running Ø 2/2 checks passed	Abre 2	<u> </u>		
ASTIC BLOCK							\sim - \sim		Network Interface eth0	マク
DRE										
lumes	Instance: I-0a	JE I	(R19)	Private IP: 10.					Interface ID VPC ID	
apshots									Attachment Owner	
TWORK &	Description	Status Checks	Monitorin	g Tags					Attachment Status	
		Instance ID	i-0a8					Public DNS (IPv4)	Attachment Time	Fri Aug 10 15:31:09 GMT+100
A STATE OF A		Instance state	running					IPv4 Public IP	Delete on Terminate	
curity Groups			out taxaaa					IPv6 IPs	Private IP Address Private DNS Name	10
curity Groups stic IPs		Instance type	Califige							
curity Groups istic IPs icement Groups		Elastic IPs						Private DNS		
culty Groups istic IPs coment Groups y Pairs		Elastic IPs Availability zone	us-east-2a					Private IPs	Public IP Address Source/Dest. Check	- false
suity Groups stic IPs cement Groups Pairs		Elastic IPs Availability zone	us-east-2a r10	onic		view inbound rules, view outbound	£.		Public IP Address	
suity Groups stic IPs cement Groups Pairs work Interfaces		Elastic IPs Availability zone	us-east-2a			view inbound rules. View outbound	£.	Private IPs	Public IP Address Source/Dest. Check	- r19
curity Groups stic IPs cement Groups (Pairs work Interfaces ND BALANCING		Elastic IPs Availability zone Security groups	us-east-2a r19	ad events	0	view inbound rules, view outbound	1	Private IPs Secondary private IPs	Public IP Address Source/Dest. Check Description	
curity Groups etic IPs cement Groups / Pairs work Interfaces NO BALANCING dd Balancers		Elastic IPs Availability zone Security groups Scheduled events	us-east-2a r19 rules No scheduk R19 (ami-1	ad events	0	view inbound rules. view outbound	1	Private IPs Secondary private IPs VPC ID	Public IP Address Source/Dest. Check Description Security Groups	- r19
ECURITY ecurity Groups lastic IPs lacement Groups etwork Interfaces DAD BALANCING DAD BALANCING and Balancers arget Groups UTD SCALING		Elastic IPs Availability zone Security groups Scheduled events AMI ID	us-east-2a r19 rules No scheduk R19 (ami-1	ad events	D	view inbound rules. View outbound		Private IPs Secondary private IPs VPC ID Subnet ID	Public IP Address Source/Dest. Check Description	- r19

- 2. Select the SonicWall NSv instance.
- 3. Select eth0 in the lower pane.
- 4. Copy the Interface ID value into your clipboard (eni-xxxxxxxxxxxxxx). 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**.

EC2 Dashboard	Allocate new ad	dress Actions *								
Events Tags	Q, Filter by tags	and attributes or search by	keyword							
Reports Limits	Name	Elastic IP	- Allocation ID	Instance	- Private IP address	- Scope	- Association ID -	Network Interfac	e ID	Network Interface Ov
A Contract of the second		13.58	eipalioc-a2		10	vpc	elpassoc-04	en-De		37
instances	• 2	13.50	eipalloc-63	- Release	addresses	vpc	-	-		+
Launch Templates		52.	eipalloc-d4		te address	3	eipassoc-a7	en-se-		37
		52	eipalloc-98		ciate address	vpc	14 contraction of the	-		+
Spot Requests		52.1	elpalloc-f9	HOZe Add/Edi	Tags 1.5	VDC	elpassoc-27	eni-5b		37
Reserved Instances Dedicated Hosts										
E INAGES										
AMIs										
Bundle Tasks										
ELASTIC BLOCK										
Volumes										
Snapshots										
B NETWORK &										
Security Groups										
Elastic IPs	1									
Placement Groups										
Key Pairs										
Network Interfaces										
H LOAD BALANCING	1									
Load Balancers	Address: 13.59.1	127.241								
Target Groups										
■ 4JT0 SCALING	Description	Tags								
Launch Configurations		Elastic IP 13.59.							elpelloc-63	
Auto Scaling Groups		Instance -					P	rivate IP address	1	
		Scope vpc Public DNS -						Association ID work interface ID	10	
SYSTEMS MANAGER SERVICES	Network	k interface owner					Net	eors internace ID		

- 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.

hich you want to associate this Elastic IP address (13.59.	
Instance	
ni-06a: • C 🖊 2	
ielect a private IP - C O	
Allow Elastic IP to be reassociated if already attached	
ess with your instance, your current public IP address is released. Learn more.	
d	
e s s	Instance Network interface 1 eni-05a C 2

- 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).

To locate the EIP address, see Step 1.

SONICWELL Network Security Virtual Username admin
Password LOG IN

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.

VPC Dashboard	Create Route Table	Delete Route Table Se					
Filter by VPC:	Q Search Route Tal	the read that he					
Q Select a VPC	G Search Roule Tai						
Virtual Private Cloud	Name	✓ Route Table ID ✓	Explicitly Associal-	Main	- VPC	•	
Your VPCs		rtb-a7	0 Subnets	Yes	vpc-e		
Subnets		rtb-0c	0 Subnets	Yes	vpc-(~
Route Tables	1	rtb-52	0 Subnets	Yes		· Z	1
	- O	rtb-f5	2 Subnets	No	vpc-6	66 vpc	
Internet Gateways		rtb-c7	1 Subnet	Yes	vpc-4	49 -test	2
Egress Only Internet Gateways		rtb-98	1 Subnet	No	vpc-4		2
DHCP Options Sets		rtb-0di	2 Subnets	No	vpc-0)b vpc-shane	
		rtb-a3	0 Subnets	Yes	vpc-6	56 /pc	
Elastic IPs							
Endpoints							
Endpoint Services							
NAT Gateways							
Peering Connections							
Security							
Network ACLs	rtb-0c37d885d0907c8	2f					
Security Groups	Summary	Routes Subnet As	sociations Route I	Propagation	Tags		
VPN Connections	Edit	3					
		View: All rules	v				
Customer Gateways							
Customer Gateways Virtual Private Gateways	Destination	Target	St	tatus Propa	gated		

- 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.

	rtb-0c3 Summary	Subnet Associations	Route Propa	gation	Tags
	Cancel Save	3 View: All rules			
	Destination	Target	Status	Propagated	Remove
~	10.99.0.0/16	local	Active	No	
2	0.0.0/0	eni-090		No	0
-V	Add another route				
	\wedge				
	ז ר				

- 6. For **Destination**, enter 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**.

EC2 Dashboard		Resource Gr	roups - 1e											4	State O'Harlan +	Ohio -
Events		inch Instance	Connect	Actio	vis ¥											
Taga	Q	Filter by legs and	attribules or sear	rich by key	yiard.										0	Re
Reports		Name	instance ID		Isstance Type -	Availability Zone -	Instance State -	Status Checks	- A	Uarm Status	Public DNS (IPv4)	· IPv4 Public IP	 IPv6 IPs 	- Key Name	- Monitoring	- Laure
Limits		softestoc	i-003b	-	t2/micro	10-00120	a synthing	2/2 checks pussed	N	Vore	-	52			disabled	Augus
NSTANCES		interoniccore	H02wr.		of large	un-east-2n	e stopped		Ň	Vorw	S				divabled.	July 1
netances	1		1-03ra2		12/11/20	10-6892-28	💓 stopped			VOTW				and the second second	theme	Juty S
eartch Templates		se demosery	1-0441		t2.micro	10-885128	stopped			Vorie	ar2.62	52		CONTRACTOR OF A	disabled.	July 1
pot Requests			H08a7		t2.micro	un-eest-2c	stopped			Vone:				Contraction of the	disabled.	Febru
leserved instances		vpo-ruit	HODel		12 micró	in-east-2n	beqqdh 🤤		Ň	Vore					disabled	May 1
iedicated Hosts		se-denteserv	H0w10	-	t2.micro	10-4451-29	Dequit 🤤		1 .	Vone			-	Contraction of the	disabled	July 1
AGES		R199	HOact	-	c5 large	up-east-2a	a running	@ 32 checks passed		2++ 2		13.59.		and the second	eisabied	Augus
LASTIC BLOCK																
/skimes	1410											Read and the second second				
inapshots	Ins	tancs: 1-0acffil	18	(19. a	Elestic P: 13.	52. 1						Network Interface othic				
		100 C 100 C										NARWORK FIREFULD CALL				
ETWORK IL														_ ~		
ECURITY	De	escription	tatus Checks	Monitor	ing Tags							Interface VPC	iD eni-def	- 🗘		
ecurity Groups	De	escription S		Monitor	ing Tags						Public DNS (IPv4)	Intertace VPC Atlactment Over	10 eni-Set 10 vpc (ha956) 14 3/1	_ (
iculary iculty Groups iastic IPs	Đ		Instance ID								Public DNS ((Pv4) IPv4 Public IP	Intertace VPC Attachment Own Attachment Stat	10 em-Set 10 epc/ba996 14 3/1 14 attached	_<		
ecularity acuity Groups lastic IPs lacement Groups	D		Instance ID Instance state Instance type	Hoseffill running c5 large							IPv4 Public IP IPv8 IPs	Intertace VPC Atlactment Over	10 em-Sat 10 epc/ba990 nar 3/1 na attached na Man Aug 13-10	95 28 OMT+100 2018		
ecularity acuelty Groups lastic IPs lacement Groups by Pairs	De		Instance ID Instance state Instance type Elastic IPs	Hoseffill running c5 targe 13.59							IPv4 Public IP IPv8 IPs Private DNS	Interface VPC Atlactorent Over Atlactorent Stat Atlactorent Te	10 eni-Saft 10 upc Obu990 10 stacked 11 Man Aug 13 10 14 bus	at 28 GWT+100 2018		
ecusery acuity Groups action Pa accenent Groups by Pairs abuork Interfaces	D		Instance ID Instance state Instance type Elastic IPs valiability zone	Hösettill running et5 targe 13 59 us-east 23				- Phone of Index - stars -			IPv4 Public IP IPv8 IPs Private DNS Private IPs	Interface VPC Attactment Out Attactment Stat Datate en terreter Provate DHD har Provate DHD har	10 em-Sat 10 ep-Ohu996 ar 3/1 ar affacted he Man Aug 13 10 de tue s 10.95 5	# 23 GMT+100 2018		
cusory curity Groups astic IPs scenert Groups by Pairs doork Interfaces w/D mico/cinic	D		Instance ID Instance state estance type Elastic IPs valiability zone ecurity groups	Hösettill running et5 targe 13 59 us-east 23	Sonc Spingres Pass	MgmDQstp11n5Bke-	3. viev	information view			IPv4 Public IP IPv8 IPs Private DNS	Interface VPC Atlachment Own Atlachment Stat Datate an Terman Private IP Addre Private DNS Nat Patric IP Addre Patric IP Addre	10 em-Sat 10 epc (huy96) 10 apc (huy96) 11 at 10 at 1	= <		
CLUSTY Acuity Groups astic IPs accement Groups by Pairs dwork Interfaces AD BALANCING ad Balancers	D	A	Instance ID Instance state estance type Elastic IPs valiability zone ecurity groups reduced overits	+Dect tutning c5.targe t3.50 us-each2s r190 suthound No sched	son: Sgingres Pars uas ded events			inbound rules, view			IPv4 Public IP IPv8 IPs Private DNS Private IPs	Interface VPC Attactment Out Attactment Stat Datate en terreter Provate DHD har Provate DHD har	10 emi-Saff 10 epi-Obu996 ari 37 ari attached ne Man Aug 13 10 an true os 10.95 5 - ck Date	= <		
ECURITY acturity Groups laceneerd Groups ey Pairs etwork Interfaces JAD BALANCING pad Balancers	D	A	Instance ID Instance state Instance type Elastic IPs valiability zone ecurity groups reduked oversts AMI ID	Hoect running c5 large t3 50 as each 20 r190 softward No schedt Soric/Wall	son: Sgingres Pars uas ded events	Mgr6X2dpi1n88ke-		l bound rules, view			IPv4 Public IP IPv3 IPs Private DMS Private IPs Secondary private IPs VPC ID Dubnet ID	Interface VFC Attactment Own Attachment Ter Matterner Ter Dielete an Termes Pinute (P Adte Pinute (P Adte Pinute (P Adte Source/Dest Che Descripti	ID emi-3af ID epic Obu995 as albached In Main Aug 13 10 In Lue s 10.95 is 10.95 is - s - ot laise an -	95 28 GWT+100 2018	4 x1#3840-	
ECURITY iaccelly Groups alastic IPs facement Groups (sy Pairs ialastock Interfecens CAD INLANCING oad Balancers inget Groups V/TO ISCALING	D	A	Instance ID Instance state estance type Elastic IPs valiability zone ecurity groups reduced overits	Hoect running c5 large t3 50 as each 20 r190 softward No schedt Soric/Wall	son: Sgingres Pars uas ded events			i bound rules, vev			IPv4 Public IP IPv8 IPs Private DNS Private IPs Secondary private IPs VPC ID	Interface VFC Attactment Own Attachment Ter Matterner Ter Dielete an Termes Pinute (P Adte Pinute (P Adte Pinute (P Adte Source/Dest Che Descripti	ID emi-3af ID epic Obu995 as albached In Main Aug 13 10 In Lue s 10.95 is 10.95 is - s - ot laise an -		4 sta3se	
ECURITY acurity (Insups lastic IPs loscenert Groups ay Pairs letwork Interfaces DAD RELAYCING DAD RELAYCING DAD RELAYCING DAD RELAYCING DATO SCALDIG DATO	D	A	Instance ID Instance state Instance type Elastic IPs valiability zone ecurity groups reduked oversts AMI ID	Hoect running c5 large t3 50 as each 20 r190 softward No schedt Soric/Wall	son: Sgingres Pars uas ded events			inbound rules were			IPv4 Public IP IPv3 IPs Private DMS Private IPs Secondary private IPs VPC ID Dubnet ID	Interface VFC Attactment Own Attachment Ter Matterner Ter Dielete an Termes Pinute (P Adte Pinute (P Adte Pinute (P Adte Source/Dest Che Descripti	ID emi-3af ID epic Obu995 as albached In Main Aug 13 10 In Lue s 10.95 is 10.95 is - s - ot laise an -		4	
Accusity Groups Security Groups Security Groups Macement Groups (sy Pairs Security Content Security Security Security Security Security Security Security Se	D	A So	Instance ID Instance state Instance state Eastic Ps valiability zone ecurity groups reduked overts AMI ID Platform IAM role	Hoeff turning c5 large t3 50 us east 20 r190 schoord No school Sonic/Wall	son: Sgingres Pars uas ded events			i inbound rules. Kew		3	IPVE PLACE IP IPVE IPS Private IPS Private IPS Private IPS Secondary private IPS VPC ID Submet ID Network Instators	Interface VFC Attactment Own Attachment Ter Matterner Ter Dielete an Termes Pinute (P Adte Pinute (P Adte Pinute (P Adte Source/Dest Che Descripti	ID emi-3af ID epic Obu995 as albached In Main Aug 13 10 In Lue s 10.95 is 10.95 is - s - ot laise an -		4 stu38e	
ELEVIORE & ELEVIORE & ELISIETY Sociality Orisigne Elisade Dra Macoment Occupie Gry Palts Unito Instantismo (Instantismo Instantismo Instantismo Configurations Auto: Scalause Juanch Configurations Auto: Scalause Juanch Configurations Auto: Scalause Juanch Configurations	D	A So	Instance ID Instance state Instance state Instance type Erastic Ps usitability zone lecarity groups reduked overts AMI ID Plattern	Hoeff turning c5 large t3 50 us east 20 r190 schoord No school Sonic/Wall	son: Sgingres Pars uas ded events			i inbound njies, view		3	IPVE PLace IP IPVE IPS PRIvate IPS Private IPS Secondary private IPS VPC ID Dubnet ID Network referance T Unimited	Idention VPC Attachment Dat Attachment Dat Attachment Tat Delete an Termes Private IP Adde Private IP Adde Security Grou Security Grou	ID emi-3af ID epic Obu995 as albached In Main Aug 13 10 In Lue s 10.95 is 10.95 is - s - ot laise an -		4	

- 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**.

gs	Q, Filter by lags an	nd attributes or search by i	keyword						
sports	Name	- Elastic IP	Allocation ID	- Instance -	Private IP address -	Scope -	Association ID	- Network Interface ID	
nits		13.58	eipalloc-		10.99	vрс	elpassoc-	eni-della della	
STANCES		13.59 1	eipalloc-	i-0acff	10.99	vpc	elpassoc-	eni-08	
stances		52.14	eipafloc-	H0441	10.0	vpc	elpassoc-	eni-5e	
unch Templates		52.14	eipelloc-	H0036	10.99	vpc	eipassoc-	eni-05e	_
ot Requests eserved Instances		52.15. 7	eipalioc-f9		· Relea	se addresses 🖊	-	· · · · · · · · · · · · · · · · · · ·	
						sala address <	3		
licated Hosts						sociale address			
GES					Addle	dit Tags			
5									
dle Tasks									
STIC BLOCK RE									
mes									
pshots									
WORK IL									
urity Groups	11111								
stic IPs	1								
stic IPs	1								
tic IPs ement Groups	1								
tic IPs ement Groups Pairs	1								
stic IPs sement Groups Pairs work Interfaces	Address: 52.15	-							
etic IPs coment Groups Pairs work Interfaces D BALANCING		Tags							
stic IPs coment Groups Pairs work Interfaces D BALANCING d Balancers		Tags							
etic IPs comment Groups Pairs work Interfaces D BALANCING d Balancers get Groups		Tags Elastic IP 52.15					Allocation ID	eipalise 19	
etic IPs comment Groups Pairs work Interfaces D BALANICING d Balancers yeit Groups O SCALING		Tags Elastic IP 52.15 Instance -					Allocation ID Private IP address	eipatoc-9	
stic IPs coment Groups Pairs work Interfaces D BALANCING d Balancers yet Groups		Tags Elastic IP 52.15					Allocation ID Private IP address Association ID		

- 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.

Associate address	which you want to associate this Elastic IP address (13.59.	
Resource type	Instance Network interface 1	
Network interface	eni-06a - C 🔁 2	
Private IP	Select a private IP C O	
Reassociation	Allow Elastic IP to be reassociated if already attached	
Warning If you associate an Elastic IP a AWS Command Line Interface comm	dress with your instance, your current public IP address is released. Learn more.	

- 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.

(i) **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
- Creating a Security Policy for Outbound
- Applying Security Services on Policies in NSv for Outbound Traffic
- Deploying Windows 10 from Console
- · Creating a Security Policy and NAT Policy for Inbound RDP to the VM

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.

aws 🏭	ervices	▶ � ⑦ US-Gov-West ▼ jlaserso
	AWS Management Console	
	AWS services	Explore AWS
	Find Services You can enter names, keywords or acronyms. Q. Example: Relational Database Service, database, RDS	What's New in AWS GovCloud (US) Read about all of the new services and features recently made available in AWS GovCloud (US). Learn more
	▼ Recently visited services	AWS GovCloud (US) Services in Scope View a complete list of compliance authorization for each AWS service in AWS GovCloud (US), Learn more [2]
	► All services	AWS Marketplace for AWS GovCloud (US)
	Build a solution Get started with simple wizards and automated workflows.	Find, buy, and deploy software products and services in AWS GovCloud (US). There are 950+ products to choose from, and hourly, monthly, annulty, and multi-year contract terms are available. Learn more

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.

Services							Σ	\$ Ø	US-Gov-West 🔻 jlasersol	nn @	
New EC2 Experience	Insta	ances (9) Info	[C Connect Instance state ▼ Actions ▼ Launch instances							
reit us what you think	QI	ind instance by attribute or tag (case	e-sensitive)						\sim	< 1 >	6
EC2 Dashboard		Name	▼			Instance state	. ▼	Instance type		Alarm statu	JS
Events		JDL NSv 870				Running	QQ	c5.2xlarge	⊘ 2/2 checks passed	No alarms	+
Tags		Win10 VM on X0 LAN NSv 870				⊘ Running	ଭ୍ର୍	c5.large	Ø 2/2 checks passed	No alarms	+
Limits		Win10 VM on 2nd LAN NSv 870	10			Running	θQ	c5.xlarge	Ø 2/2 checks passed	No alarms	+
Instances		Shane NSv-270	1			Running	QQ	c5.large	Ø 2/2 checks passed	No alarms	+
Instances		soh-test-vm-new-vpc				⊘ Running	QQ	c5.2xlarge	⊘ 2/2 checks passed	No alarms	+
Instance Types		Win10 VM Shane NSv 270				⊘ Running	QQ	c5.xlarge	Ø 2/2 checks passed	No alarms	+
Launch Templates		Win10 VM2 Shane NSv 270	1.1			⊘ Running	QQ	c5.4xlarge	Ø 2/2 checks passed	No alarms	+
Spot Requests		jdl-NSv-470-2022-1116	1			Running	ΦQ	c5.xlarge	Ø 2/2 checks passed	No alarms	+
Reserved Instances		VM1 NSv-470-2022-1116	1.1			⊘ Running	QQ	c5.xlarge	⊘ 2/2 checks passed	No alarms	+
Dedicated Hosts	4		-								

- b. From the menu click AWS Marketplace and enter <code>SonicWall NSv</code> 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	ත් large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
0	Compute optimized	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
10	Compute optimized	c6.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
8	Compute optimized	c5.4xlarga	16	32	EBS anly	Yes	Up to 10 Gigabit	Yes

NSV MODELS AND IMAGE TYPES

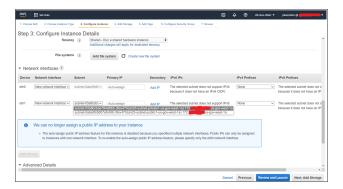
SonicWall NSv Model	NSv EC2 Instance Type	
NSv 270	c5.large	
NSv 470	c5.xlarge	
NSv 870	c5.2xlarge	

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.

Choose AMI 2. Choose Instance Type	3. Co	nfigure Instance	4. Add Storage	5. Add Tags	6. Co	nfigur	e Security Group 7.
tep 3: Configure Instan			tiple instances	from the same Al	MI, requ	iest S	Spot instances to take
Number of instances		1		Launch into Aut	o Scalir	ng Gr	oup 🕕
Purchasing option		Request Spot	instances				
Network	1	vpc-0ba96600dd	lab58c09 exar	nple	v	C	Create new VPC
Subnet	(1)	subnet-072c2e6 243 IP Addresses		2a 🔻		Create new subnet	
Auto-assign Public IP		Use subnet setti			Ŧ		
Placement group	(1)	Add instance t	o placement gr	oup.			
Capacity Reservation		Open			Ŧ	C	Create new Capaci
IAM role	1	None			Ŧ	C	Create new IAM rol
CPU options	(1)	Specify CPU o	ptions				
Shutdown behavior	()	Stop			•		
Enable termination protection	()	Protect agains	t accidental terr	nination			
Monitoring		Enable Cloud Additional charge		nonitoring			
EBS-optimized instance	1	Launch as EB	S-optimized ins	ance			
Tenancy	1	Shared - Run a s Additional charge	and a second		▼ y.		
Network interfaces (i)							
Device Network Interface	Subnet	Prin	nary IP	Seco	ndary	IP ad	dresses
th0 New network interface •	subnet-0	72c2e64 V Aut	o-assign	Add I	P		

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.

ate a new security group or select from an exist	trol the traffic for your instance. On this page, you can add rules to allow sting one below. Learn more about Amazon EC2 security groups.	specific traffic to reach your instance. For example, it	f you want to set up a web server and allow Internet traffic to reach your in	stance, add rules that allow unrestricted access to the HTT
	Create a new security group			
	Select an existing security group			
Security group name: Description:	launch-wizard-5 launch-wizard-5 created 2018-11-19T18:08:10.944+00:00			
(ype ()	Protocol ()	Port Range (j)	Source ①	Description ①
SSH V	TCP	22	Custom • 107.154.75.50/32	SSH
Custom ICMP *	Echo Reply V	N/A	Custom • 107.154.75.50/32	e.g. SSH for Admin Desktop
Custom UDP •	UDP	4500	Custom • 107.154.75.50/32	lpsec-nat-t
Custom UDP I *	UDP	500	Custom • 107.154.75.50/32	ISAKMP
HTTPS T	TCP	443	Custom • 107.154.75.50/32	HTTPS management
Add Rule				

- 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.

ey allow otain the ecurely S	you to connect to your instance securely. password used to log into your instance. I SH into your instance.	, and a private key file that you store. Together, For Windows AMIs, the private key file is required to For Linux AMIs, the private key file allows you to
	selected key pair will be added to the set oving existing key pairs from a public AMI	of keys authorized for this instance. Learn more
	e a new key pair	Ŧ
	air name	
Sonic\	Wall-NSv-example	
		Download Key Pair
		ile (*.pem file) before you can continue. Store

- I. 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**.

		_		_						
Dedicated Hosts	- * - I	Allo	cate new a	ddress	Actions ¥					
Capacity Reservations		Q,	Filter by tag	s and a	ttributes or search i	by keyv	vord			
AMIs			Name		Elastic IP		Allocation ID	*	Instance	
Bundle Tasks					13.56.51.54		eipalloc-all/75-all			Release addresses
					13.58 127.241		elpalloc-traine and		i-004db3ee5	
ELASTIC BLOCK STORE					52 14 222 51		eipalloc-miliaterina		i-0dcf39fe37	
Volumes					12 14 348 156		elpalloc della stati		i-02aa41c53	Add/Edit Tags
Snapshots					82 15 153 87		eipalloc miserando			
Lifecycle Manager	11									
NETWORK & SECURITY										
Security Groups										

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.

/5 Hitl Services		
Associate Elastic IP address		
Choose the instance or network interface to associate to this Elastic IP address (15.	•	
Elastic IP address: 15.		
Resource type Choose the type of resource with which to associate the Elastic IP address. Instance Network interface		
▲ If you associate an Elastic IP address with an instance that already has an Elastic IP previously associated Elastic IP address will be disassociated, but the address will st account. Learn more[2] If no private IP address is specified, the Elastic IP address will be associated with the address.	ill be allocated	l to your
eni-02 (NSv470Jan23 WAN) Q eni-	C	
Private IP address The private IP address with which to associate the Elastic IP address.		
Q Choose a private IP address		
Reassociation Specify whether the Elastic IP address can be reassociated with a different resource if it already associated Allow this Elastic IP address to be reassociated	I with a resource.	

- 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.

Network Security Virtual Username Password	ity Virtual
Password	
Password	

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:

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

SONICWALL	€ NSv 470 		OR 💻 DEVICE	🔆 NETWORK	🗊 овјест 🔏	POLICY			🥵 🔉 વ
	🔰 004010	olicy / Rules and Poli	cies / Security Policy		•			Configura	ition 🔵 Non-Co
Rules and Policies	Q + Group By: No Gr	ouping 🔻 IPv4	▼ ::: LAN ->	WAN Active & Ina	ctive 🔻 🛛 Used &	Unused 🔻			🚺 🔽 🚍 Settir
— Settings	GEN	IERAL	ZONE	ADDRESS	SERVIC	E US	ER	APP/URL/CUST	ГОМ МАТСН
Security Policy NAT Policy	PR 🔶 HITS	NAME	SOURCE DESTINA.	SOURCE DE	STINATI DESTINA	TI USERS	APPLICATI	WEB CATE	URL LIST CUS
Route Policy	Adding R	ule							0
DoS Policy Endpoint Policy	Name	allow LAN2WAN an	ny LAN Subnets to any J	an 2023 Security		Action	Allow X Deny	/ 🥥 Discard	
- Shadow	Tags	add upto 3 tags, use	e comma as separator			Туре	IPv4 O IPv6		
Capture ATP	Tags					Schedule	Always		- / O
	Description	provide a short desc	cription of your access ru	Je		Enable			
	Description				Security F	Rule Action			- / 0
							Security Profile		
	Source / Destin	ation User & (Country App/L	JRL/Custom Match			Botnet Profile		
							 Default Profile Jan 2023 Security 		
	SOURCE				DESTINATION		Jan 2023 Security		
	Zone/Interface	LAN		-	Zone/Interface	WAN			-
	Address	LAN Subnets		▼ 🖊 🛈	Address	Any			~ / ()
	Port/Services	Any		~ / ()	Port/Service:	Any			v / ()
	Show Diagram				Create And	ther	Validate	Cancel	Add

- 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** dropdown 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** dropdown 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.

Q Sear	ch						🕂 Add 🍵 Delete	🔾 Refresh	🚯 Column
	NAME	PROFILES	PROPERTIES	REFERENCES		CREATED	UPDATED	CONFIGU	RE
				default_1	C+				
1	Security Profile	a 😁 🖬 🌒	© 14	LAN to WAN 3.5	0+	03/23/2020 20:37	03/23/2020 20:37	16	1
				LAN to WAN 3_6	0+				
2	😌 Botnet Profile	•	@ 24			03/23/2020 20:37	03/23/2020 20:37	/ 6	1
				default_2	C+				
3	Orfault Profile		© 24	LAN to WAN_3	0+	03/23/2020 20:37	03/23/2020 20:37	/ 6	1
- 4	my sec action profile	9 💀	٢			04/05/2020 15:10	04/05/2020 15:10	/ 6	6
				LAN to WAN 2_4	0+				
				my Rule_7	0+				
				Deny_8	0+				
				Deny_9	0+				
5	All enforced	🐬 🔍 🔮 📑 🖬 🌒	@ <u>24</u>	Deny_10	0+	04/13/2020 02:26	04/15/2020 02:19	/ 6	1
				Deny_11 C+					
				Deny_12	C+				
				Deny_13	C+				
				My Rule_14	C+				
6	my action profile	💎 🔍 😬 🖬 🌢	Q	my rule_15	C+	06/12/2020 09:50	05/12/2020 09:50	16	1

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.

SONICWALL	🗲 NSv 470 🕜 Home 🏦 Monitor 💻 Devic	ce 🔀 network 🦰 object 🔏 policy
	😺 00401 Object / Action Profiles / Security Acti	ion Profile
Aatch Objects	Q. Search + Used and Unused V	+ Add
— Zones		
— Addresses	# NAME FILES	PROPERTIES REFERENCES
— Services	📄 🕨 1 🛛 🔍 Security Profile	© <u>2</u> 4
 Countries Applications 	► 2 ● Botnet Profile	© 14

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.

Edi	t Security	Action	Profile				
			Action Profile Name	Jan 2023 Security			
< 1	Bandwidth/QoS	Anti-Virus	Intrusion Prevention	Anti-Spyware	Botnet Filter	Content Filter	Block Page and Logging
CONTR	ENT FILTER PROFILE						
CONT	ENT FILTER FROFILE			_			
		I.	inable Content Filtering				
			Content Filter Action	None	· (i)		
				m Header			
Gen	eral Passphrase	Confirm	Consent Custo	m Header			
		-		Enable You	Tube Restrict Mode		
	Safe Search Enforcem			Enable Bing	g Force Safe Search		
Enable	Google Force Safe Sea	arch			Wipe Cookies	0	
						\subset	Cancel Save

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.

aws its services	
AWS Management Console	
AWS services	Explore AWS
Find Services You can enter names, keywords or acronyms. Q. Example: Relational Database Service, database, RDS	What's New in AWS GovCloud (US) Read about all of the new services and features recently made available in AWS GovCloud (US). Learn more 🔀
	AWS GovCloud (US) Services in Scope View a complete list of compliance authorization for each AWS service in AWS GovCloud (US). Learn more [2]
► All services	AWS Marketplace for AWS GovCloud (US)
Build a solution Get started with simple wizards and automated workflows.	Find, buy, and deploy software products and services in AWS GovCloud (US). There are 950+ products to choose from, and hourly, monthly, annually, and multi-year contract terms are available. Learn more 2

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.

Services						D.	\$ Ø	US-Gov-West 🔻 jlasersoh	n @	
New EC2 Experience	Însta	nces (9) Info		C	Connect	Insta	nce state 🔻	Actions V Launch	instances)•
	Q, F	ind instance by attribute or tag (case	-sensitive)					\sim	< 1 >	
C2 Dashboard		Name	▼		Instance state	v	Instance type	▼ Status check	Alarm statu	IS
vents		JDL NSv 870			⊘ Running	QQ	c5.2xlarge	⊘ 2/2 checks passed	No alarms	+
ags		Win10 VM on X0 LAN NSv 870		=	⊘ Running	θQ	c5.large	⊘ 2/2 checks passed	No alarms	+
imits		Win10 VM on 2nd LAN NSv 870			⊘ Running	θQ	c5.xlarge	⊘ 2/2 checks passed	No alarms	+
istances		Shane NSv-270	-		⊘ Running	ΘQ	c5.large	⊘ 2/2 checks passed	No alarms	+
istances		soh-test-vm-new-vpc		1	⊘ Running	QQ	c5.2xlarge	⊘ 2/2 checks passed	No alarms	+
nstance Types		Win10 VM Shane NSv 270			⊘ Running	QQ	c5.xlarge	⊘ 2/2 checks passed	No alarms	+
aunch Templates	0	Win10 VM2 Shane NSv 270			⊘ Running	QQ	c5.4xlarge	⊘ 2/2 checks passed	No alarms	+
pot Requests		jdl-NSv-470-2022-1116	1		⊘ Running	QQ	c5.xlarge	Ø 2/2 checks passed	No alarms	+
eserved Instances		VM1 NSv-470-2022-1116			Running	ΘQ	c5.xlarge		No alarms	+

- 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.

Choose A	41/1 2. Choose Instance Type	3 Contigure Insta	nce 4 Add Storage	5 Add Lags 6 Co	infigure Security Group 7. Review			
azon EC vorking ar by:		instance types opti- bility to choose the ition	appropriate mix of reso	urces for your application	irtual servers that can run applica ms. Learn more about instance t			p, and
ote: The	e vendor recommends using a t Family ~	3.medium Instance	e (or larger) for the best	experience with this pro-	Instance Storage (GB) () ~	EBS-Optimized Available	Network Performance () *	IPv6 Support (
	c 5	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
	05	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
	00							
)	c5	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes
		c5.2xlarge	8	16 32	EBS only EBS only	Yes Yes	Up to 10 Gigabit	Yes Yes
	c5							

d. Click Configure Instance Details.

Step 3: Configure Insta	nce D	otails					
Configure the instance to suit your requ			h multiple instances	from the same AM	Al, requ	lest S	Spot instances to t
Number of instance	s ()	1		Launch into Aut	o Scali	ng Gi	roup (i)
Purchasing option	n (j)	Request	Spot instances				
Netwo	k 🕕	vpc-0ba96	600ddab58c09 exa	mple	Ŧ	С	Create new VPC
Subn	et 🕕		c2e649082850e4) resses available	K1WAN us-east-3	2a 🔻		Create new subr
Auto-assign Public I	Р 🕕	Use subne	t setting (Disable)		Ţ		
Placement grou	p 🕕	Add insta	ance to placement g	oup.			
Capacity Reservation	n 🕕	Open			¥	C	Create new Cap
IAM ro	e 🕕	None			Ŧ	C	Create new IAM
CPU option	s (j)	Specify (CPU options				
Shutdown behavio	or (j)	Stop			Ŧ		
Enable termination protection	n (j)	Protect a	gainst accidental ter	mination			
Monitorin	g 🕕		NoudWatch detailed harges apply.	monitoring			
EBS-optimized instance	e (j)	E Launch a	as EBS-optimized ins	stance			
Tenano	y 🕕		un a shared hardwa harges will apply for		v y.		
 Network interfaces ① 							
Device Network Interface	Subnet		Primary IP	Seco	ndary	IP ad	dresses
eth0 New network interface *	subnet-0	72c2e64 🔻	Auto-assign	Add	P		

- 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.

ton 2. Con	figure Instan	οο Γ	lotaila										
				ultiple instances	from the same A	MI, requ	est Sj	pot instances to take advantag	e of the lo	ver pricing, ass	gn an access manag	ement role to the in	stance,
N	umber of instances	۲	1										
	Purchasing option	۲	C Request Sp	ot instances									
	Network	١	vpc-083bbc0c	acffe21ab New	170Jan23-vpc	4	С	Create new VPC					
	Subnet				Nav470Jan23-au			Create new subnet					
Au	to-assign Public IP	۲	subnet-0c95a subnet-0abe0	c5fd3b8d90c1 fc6007efc499	Nsv470Jan23-si Nsv470Jan23-si	ubmet-pri binet-pub	valie2 slic1-i	Eusgov-west-to us-gov-west- sus-gov-west-to us-gov-west- us-gov-west-to us-gov-west- sus-gov-west-to us-gov-west-	t-1b -1a				
	Hostname type	(1)		ting (IP name)	NSWI70Janza-	ubnet-pi	UDEC2	ous-gov-west-to us-gov-wes	8-10				
	DNS Hostname	(1)	E Enable IP n	ame IPv4 (A reci	ord) DNS request	8							
			Enable reso	urce-based IPv4	(A record) DNS	requests							
			Enable reso	urce-based IPv6	(AAAA record) [NS requ	iests						
	Placement group	۲	Add instance	e to placement g	roup								
Ca	pacity Reservation	۲	Open			4							
Do	main join directory	۲	No directory			+	с	Create new directory					
	IAM role	æ	None			a	α	Create new IAM role					

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

Choose AMI 2.	Choose Instance Type 3. Co	nfigure Instance 4. Add Storage 5. A	dd Tags 6. Configure Security Group 7. Review	
ecurity group is a	ffic to reach your instance, ac	ol the traffic for your instance. On this pa		ch your instance. For example, if you want to set up a web server security group or select from an existing one below. Learn more
A	ssign a security group: @	Create a new security group		
	C	Select an existing security group		
	Security group name:	Microsoft Windows 10 Pro Desktop fo	r Intel CPU - Critical Updates-Version 1-Aul	
	Description:	This security group was generated by	AWS Marketplace and is based on recomn	
	Protocol (i)	Port Range (i)	Source (j)	Description (i)
ype (i)	Protocol ()			
	TCP	3389	Custom v 0.0.0/0	e.g. SSH for Admin Desktop
ype (i) RDP v SSH v		3389	Custom ▼ 0.0.0.0/0 Custom ▼ 0.0.0.0/0	e.g. SSH for Admin Desktop &

- 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
- I. 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.

dit routes						
Destination		Target		Status	Propagated	
pl-65a5400c		vpce-05115e75872ef73d2		⊘ Active	No	
172.0000/24		Q, local	×	⊘ Active	No	
Q 000.0/0	×	٩		-	No	Remove
		Egress Only Internet Gateway				
		Gateway Load Balancer Endpoint				
Add route		Instance				
		Internet Gateway				
		local			Cancel	Preview Save chang
		NAT Gateway				
		Network Interface				
		Outpost Loca Network Interface Peering Connection				

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 .
- Click +Add at the top of the page. The Address Object Settings dialog displays.

Address Object	Settings
Name	Win10-VM-A
Zone Assignment	
Туре	Host
IP Address	172
	Cancel

- 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:

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

	🔰 00401 🦛 / F	Policy / Rules and P	olicies / Security Policy						Configuration (Non-C
Rules and Policies	Q + Group By: No C	Brouping 🔻 IPv4	▼ WAN->1	AN Active 8	& Inactive 🔻	Used & Un	used 🔻			🔳 Setti
Settings	G	ENERAL	ZONE	ADD	RESS	SERVICE		R	APP/URL/CUSTOM M	АТСН
Security Policy	PR 🔶 HITS	NAME	SOURCE DESTINA	SOURCE	DESTINATL	DESTINATI	USERS	APPLICATI	WEB CATE URL L	IST C
NAT Policy Route Policy Decryption Policy	Adding R	ule								(
DoS Policy Endpoint Policy	Name	Allow WAN2LAN	RDP from Any to X1 IP Defa	ult Profile			Action	+ Allow X Deny	Oiscard	
Shadow		add upto 3 tags, u	se comma as separator				Туре	IPv4 O IPv6		
Capture ATP	Tags					Sc	hedule	Always		/ 0
		provide a short de	scription of your access rule				Enable			
	Description					Security Rule	Action	Default Profile		10
	Source / Destin SOURCE Zone/Interface	User &	: Country App/URL	/Custom Matc	DESTIN	NATION ne/Interface	LAN			-
	Address	Any		- / (D	Address	X1 IP			/ 0
	Port/Services	Any		- / (D Po	ort/Services	Terminal	Services		/ 0
	Show Diagram					Create Another		Validate	Cancel	Add

- 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** dropdown 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:

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

Adding	g NAT	Rule						
Name	RDP to Wir	10-VM-A			Type 🦲 IPv4	IPv6 O NAT 64		
Tags	add upto 3	tags, use comma as separat	or		Enable 🗾			
Comment	provide a sł	nort description of your NAT	Rule					
RIGINAL	Source	Any	•	TR/	ANSLATED	Original	•	/
l	Destination	X1 IP		()	Destination	Win10-VM-A 172.x.y.z		/ (
	Service	Terminal Services	•	/ (ì	Service	Original	•	
Inbour	nd Interface	X1	•					
Outbour	nd Interface	Any	•					
how Diagram						Cancel	Add	

- 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:

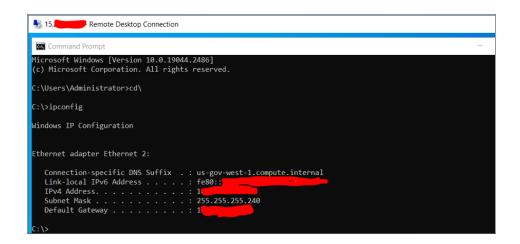
Source	Any
Destination	X1 IP
Service	Terminal Services
Inbound Interface	X1
Outbound Interface	Any

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:

(i) | 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.

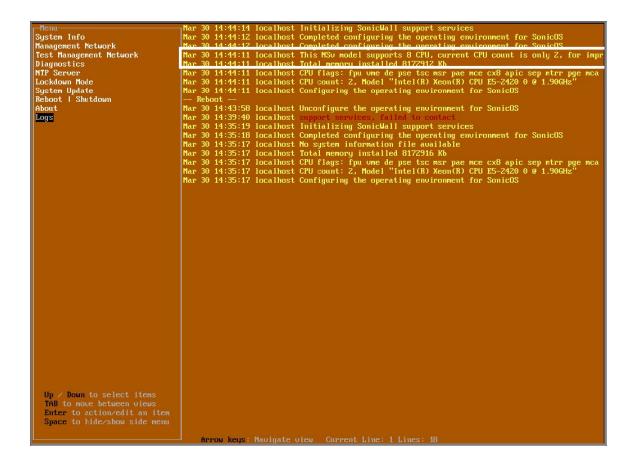
SonicOS boot message:

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.

- Menu-	→Mar 30 15:10:39 localhost Initializing SonicWall support services
Sustem Info	Mar 30 15:10:38 localhost Completed configuring the operating environment for SonicOS
Management Network	Mar 30 15:10:08 localhost insufficient memory 4 GB, minimum memory required 8 GB.
Test Management Network	Mar 30 15:10:08 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
Diagnostics	Mar 30 15:10:00 localhost Total memory installed 4160884 Kb
NTP Server	
Lockdown Mode	Mar 30 15:10:07 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtr pge mca Mar 30 15:10:07 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
System Update	Mar 30 15:10:07 localhost Cru count: 2, nodel inter(n) Acon(n) Cru E3-2420 0 @ 1.506n2
Reboot Shutdown	Har 30 15:10:07 localhost configuring the operating environment for sonicos
About	Mar 30 15:06:37 localhost Initializing SomicWall support services
	Mar 30 15:06:36 localhost Completed configuring the operating environment for SonicOS
Logs	Mar 30 15:06:06 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
	Mar 30 15:06:05 localhost Total memory installed 4160884 Kb
	Mar 30 15:06:05 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtr pge mca Mar 30 15:06:05 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
	Mar 30 15:06:05 localhost Configuring the operating environment for SonicOS
	- Reboot
	Mar 30 15:05:51 localhost Unconfigure the operating environment for SonicOS
	Mar 30 15:02:31 localhost Initializing SonicWall support services
	Mar 30 15:02:31 localhost Completed configuring the operating environment for SonicOS
	Mar 30 15:02:01 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
	Mar 30 15:02:01 localhost Total memory installed 4160884 Kb
	Mar 30 15:02:00 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
	Mar 30 15:02:00 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz" Mar 30 15:02:00 localhost Configuring the operating environment for SonicOS
	- Reboot
	Mar 30 15:01:48 localhost Unconfigure the operating environment for SonicOS
	Mar 30 14:59:55 localhost Initializing SonicWall support services
	Mar 30 14:59:54 localhost Completed configuring the operating environment for SonicOS
	Mar 30 14:59:24 localhost Completed configuring the operating environment for solicos
	Mar 30 14:59:24 localhost Total memory installed 4160884 Kb
	Mar 30 14:59:24 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtr pge mca Mar 30 14:59:24 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
	Mar 30 14:55:24 localhost Cru count: 2, nodel Inter(k) Keon(k) Cru E5-2420 0 @ 1.506Hz
	- Reboot
	Mar 30 14:59:11 localhost Unconfigure the operating environment for SonicOS
	Mar 30 14:54:57 localhost Initializing SonicWall support services
	Mar 30 14:54:56 localhost Completed configuring the operating environment for SonicOS Mar 30 14:54:26 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
	Mar 30 14:54:26 localhost Total memory installed 4160884 Kb
	Mar 30 14:54:26 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Up / Down to select items	Mar 30 14:54:26 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
TAB to move between views	Mar 30 14:54:25 localhost Configuring the operating environment for SonicOS
Enter to action/edit an item	- Reboot
Space to hide/show side menu	Mar 30 14:54:12 localhost Unconfigure the operating environment for SonicOS
opace to infuershow state menu	Mar 30 14:47:18 localhost Initializing SonicWall support services
	har so in the local lost initializing sonicwall support services

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:

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.

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.

(i) **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 Appliance as BYOL from SonicOS
- Registering the NSv Appliance as PAYG

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

SONICWALL		DBJECT I S POLICY
	🕒 🕞 0000000000000000000000000000000000	
Dashboard		
— System	Device Summary Network Threat	
Legal Information	TRAFFIC DISTRIBUTION	TOP USERS
	Device Registration needed	
	Register Device	
	OBSERVED THREATS	SERVICES SUMMARY

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.

	etwork 🔂 object / 👷 policy 🛛 💐 🔂	2
000000000000 / Device / Settings / Licenses	Configuration 🔵	N
Security Services Summary Settings		
MANAGE SECURITY SERVICES ONLINE	MANUAL UPGRADE	
There are two methods to activate, upgrade or renew services. 1. Go to MySonicWall.com , then come back and synchronize your changes. 2. Make changes to the available Licenses on the Security Services Summary.	Enter keyset	
Register	Serial Number * Auth Code * Registration Code *	
	Apply	

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.

👯 aws r	marketplace					Q				
Categories 🕶	Delivery Methods 🔻	Solutions 👻 🛛 AWS IQ 👻	Your Saved List			Partners Sell in AWS Marketplace				
		SONICWALL	The second second second second second	sonicWall NSv (Firewall/Security/VPN/Router) - PAYG						Continue to Subscribe Save to List
			The SonicWall Network Security virtu generation firewall capabilities such a Show more Linux/Unix 1 AWS Free Trial			Typical Total Price \$0.655/hr Total pricing per instance for services hosted on cSlarge in US East (N. Virginio), Wew Details				
		Overview	Pricing	Usage	Support	Reviews				
		next-generation firewall (t control, real-time monitor threat protection (ATP), Vf your AWS environment. N' networking features in So patented Reassembly-Free award-winning Capture A1 (RTDMI) for advanced three Centrally manage all your (CSC) to maintain consiste	ty virtual (NSv) firewall series brings inc (SFW) capabilities such as application i ing, IPS, TLS/SSL decryption and inspec PN and network segmentation capabilit Sv virtual firewalls support the same se inclwall physical NGFW appliances inclu 2 Deep Packet Inspection (RFDPI) techni (P sandbox with Real-Time Deep Memo at protection. firewalls using the SonicWall Capture S firewalls using the SonicWall Capture S in security policies across cloud and on in helps you implement security best pr	ntelligence and tition, advanced les to protect uruity and ding our slogy and ny Inspection our 0.00 / 2.3 ecurity Center - premises	Vinit 1 with the second					

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.

- (i) 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/knowledgebase/?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.

SC	DNIC WALL	<≡ MySonicWall		Ö
8	My Workspace Dashboard	Register Products	_	
-	Tenant Products		3	
-	Register Products	CHOOSE A TENANT PRODUCT REGISTRATION DETAILS		
-	User Groups	TechPubs		
Ξ		fkqQp5vD V My NSv PAYG Firewall		
(2)		+ Register another serial number		
UTILITI	ES			
, 0	Tools	CSV for bulk registration	Cancel Choose management opti	ons

- 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.

SonicOS Management

4

Topics:

- Managing SonicOS on the NSv Series
- Using System Diagnostics

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.

SonicOS 7 Getting Started Guide for AWS SonicOS Management

SONICWALL*							
Your default password must be changed at first time login Please enter a new password:							
Old Password							
New Password							
Confirm New Password							
	Cancel Change Password						

- 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.

S	onic wall '		🖌 HOME 🎢 MONI		💥 NETWORK 😭 OBJECT	POLICY	🗶 💽 Ö (
FIREW	/ALLS	00401038B524 / Devic	e / Diagnostics / Chec	k Network Settings			Configuration ONC	
	Settings IPv4 IPv6							
	Status GENERAL NETWORK CONNECTION Licenses							
-	Administration Time Certificates						🕸 Test All Selec	
_	SNMP	SERVER	IP ADDRESS	TEST RESULTS	NOTES	TIMESTAMP	PROGRESS	
-	Firmware and Settings	Default Gateway (X1)	→ 10.203.26.1	Ping responded successfully	Ping sent 3 pkts, received 3 pkts, average < 5 ms	08/23/2020 17:54:50	Image: A start of the start	
_	Restart	DNS Server 1	→ 10.50.129.148					
		DNS Server 2	→ 10.50.129.149					
ዾ		Total: 3 item(s)						
***		SECURITY MANAGEME	NT					
, ⊕	Diagnostics						🕼 Test All Selec	
-	Tech Support Report Check Network Settings	SERVER	IP ADDRESS	TEST RESULTS	NOTES	TIMESTAMP	PROGRESS	
-	DNC Name Leekup	My SonicWall	→ 					

Specifically, Check Network Settings automatically tests the following functions:

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

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

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

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

Using the Virtual Console and SafeMode

Topics:

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

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.

5

aws Servi	ices - Resource (Groups 🗸	EC2 🔱 VPC 🗯	CloudFormation 🕈				🗘 wqonqi	@sonicwall.com @ 629	15 + N. Ca
2 Dashboard ·	Launch Instance	Gonnec	Actions ¥							
Q6	Q, Filter by tags a	ind attributes or sea	arch by keyword							0
eports mits	Name		- Instance ID	* Instance Type -	Availability Zone +	Instance State + Status Checks +	Alarm Statu	as Public DNS (IPv4) -	- IPv4 Public IP	- IPv6 IPs
Children and Chi	wenlu-650v-r	350	H00Dc322581878	c5.4xlarge	us-west-1c	🥚 stopped	Nane	>	13.56.094.904	-
stances	Allen-LAN-PO	D1-Win	i-016298fc694d2b4f1	12 micro	us-west-1a	🥥 stopped	None	2	13	84 - C
unch Templates	bychen-RC23	35	i-0245bb853d2062e66	c5.xlarge	us-west-1c	stopped	None	>	13.52.23 (90)	S
of Requests	< Alion Ph		LADRABUTZ (14hs3rf)	mé visco:	111.0002.73	Stropped	More-	No. 1		
ticated Hosts bacity Reservations	Description	Status Checks	Monitoring Tags							
barità incocrationa		1	1000-20200028200-							
			i-000c322581876				NS (IPv4) -			
IGE5		Instance state	+000c322581875			1P14		3.56.116.11		
iges Is		Instance state Instance type	stopped			IPr4	Public IP 1 IPv6 IPs ·		internal	
iges Is Idle Tasks		Instance state Instance type	stopped c5.4xtarge 13.56 million			IPv4	Public IP 1 IPv6 IPs - vate DNS ip	3.66.116.118	internal	
iges Is Idle Tasks		Instance state Instance type Elastic IPs Availability zone	stopped c5.4xtarge 13.56 million	iew outbound rules		IPv4	Public IP 1 IPv6 IPs - vate DNS ip rivate IPs 1 rivate IPs	13.56,110,110,100,000,000,000,000,000,000,00	nternal	
iges Is Idle Tasks STEC BLOCK JRE		Instance state Instance type Elastic IPs Availability zone Security groups cheduled events	stopped c5.4xlange 13.56 us-west-1c default, view inbound rules.			Prin Prin Secondary p	Public IP 1 IPv6 IPs - vate DNS ip rivate IPs 1 rivate IPs VPC ID w	13.66.116.116 >192.2-1-136.us-west-1.compute i 92.2.2.14, 192.2.1.116 pc-Dea19dc9Dea39d3b5	nternal	
GES Is Idle Tasks STIC BLOCK IRE		Instance state Instance type Elastic IPs Availability zone Security groups icheduled events AMI ID	stopped c5.4xlange 13.56 us-weat-1c default, view inbound rules. SomcWat_NSv_AWS_R350			Pin Pin Secondary p	Public IP 1 IPv6 IPs - vate DNS ip rivate IPs 1 rivate IPs VPC ID vi Subnet ID s	13.56.116.000 = 192-2-1-136.us-west-1.compute i 92.2.2.14, 192.2.1.100 pc-Des19dc9Des39d3b5 ubnet-053b83c13d5307325	ntemal	
kges Is Indie Tasiks STTC BLOCK JRE Umes apshots		Instance state Instance type Elastic IPs Availability zone Security groups cheduled events	stopped c5.4xlange 13.56 us-weat-1c default, view inbound rules. SomcWat_NSv_AWS_R350			Prin Prin Secondary p	Public IP 1 IPv6 IPs - vate DNS (p rivate IPs 1 IVv6 IPs VPC ID v Subnet ID p riterfaces (c	13.66.116.116 >192.2-1-136.us-west-1.compute i 92.2.2.14, 192.2.1.116 pc-Dea19dc9Dea39d3b5	nterral	
ides lis stitle Tasks stitle BLOCK ske umes apshots scycle Manager		Instance state Instance type Elastic IPs Availability zone Security groups cheduled events AMI ID Platform IAM role	stopped c5.4stange 13.56 us-weet-1c default, view inbound rules. SomeWatLNSy_AWS_R350			(Pud Pin Pin Secondary Pin Secondary Pin Source/M	Public IP 1 IPv6 IPs - vate DNS ip rivate IPs 1 rivate IPs VPC ID v Subnet ID p mienfaces c est check T	13.66.116. >-192-2-1-136.us-west-1.compute i 92.2.2.14, 192.2.1 pc-0es19dc90es39d3b5 ubmet-053b83c13d5307325 sh0	ntemal	
KGES Is Istic BLOCK JRE umes cycle Manager IVIORX: B. UNITY		Instance state Instance type Elastic IPs Availability zone Security groups cheduled events AMI ID Platform IAM role Key pair name	stopped c5.4/arage 13.56 usweesh1r default, view inbound rules, - SoncWalt_NSv_AWS_R350 - sentu-nc			IP-4 Pin P Secondary p Secondary p Secondary Sourcebits T2/73	Public IP 1 IP\6 IPs - vate DNS ip rivate IPs 1 ivate IPs VPC ID iv Subnet ID is interfaces in est check T Unlimited -	13 55 110 ->192-2-1-136 us-west-1 compute i 92 2.2 14, 192.2 1 pc-0es1(94c90es3)633b5 utenet/65803c13d5307325 def1 rue	nternal	
kiges reservations kiges dele Tasks strice BLOCK SRE apphots spychie Manager (WORK & UNITY WORK & UNITY Groups etc. IPS		Instance state Instance type Elastic IPs Availability zone Security groups chedioled events AMI ID Platform IAMI role Key pair name Owner	stopped c5.4stange 13.56 us-weet-1c default, view inbound rules. SomeWatLNSy_AWS_R350	ami-Qe2feaf4037145a90)		IP-4 Pin Pic Secondary p Sourcebbs Sourcebbs Sourcebbs 2073 2073 2073	Public IP 1 IPv6 IPs - vate DNS ip rivate IPs 1 invate IPs VPC ID v Subnet ID p interfaces c est check T	3 56 116 -1922-1-136 us-west-1 compute i 92 2 2 14, 192 2 1 pc-0ea156c50ea30d305 ubere/053e03a13d5307525 dr0 dr1 tue tue	nternal	

- 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
```

 $\label{eq:product} From Windows, with PuTTY: in the Host Name box, enter {\tt management@<public_dns_name>}.$

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.

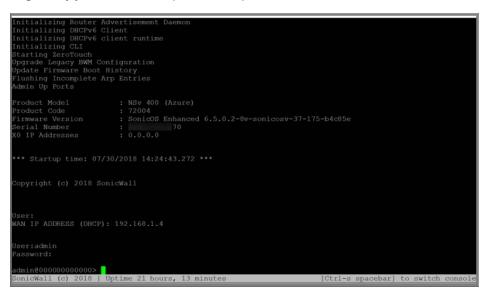
The orange NSv Management Console displays.

Menu	-System Info-	
System Info	Model	: SonicWall Network Security - Virtual Series
Network Interfaces		
Diagnostics	Product Code	: 72004
NTP Server	Serial Number	: 0 70
Lockdown Mode	Model Name	: NSV 400 (Azure)
System Update	SonicOS Version	: 6.5.0.2
Reboot Shutdown	GUID	· A CONTRACTOR OF A CONTRACTOR
About		
Logs	System Time	: Tue 2018-07-31 17:26:57 UTC
		: 20 hours 2 minutes 50 seconds
		: 0.3 1min 0.4 5min 0.5 10min
	hoad Average	· 0.5 thirth 0.4 bhirth 0.5 romain
	SonicOS	: Operational
	5011005	. operacionar
and the second second second		
Up / Down to select items		
TAB to move between views	and a second second second second second	COMPANY AND COMPANY AND
Enter to action/edit an item		lcWall web interface visit:
	https://192.16	/ on X1 interface
SonicWall (c) 2018 Uptime 20 hou	irs. 1 minute	[Ctrl-s spacebar] to switch console

(i) **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

System Info Management Network Test Management Network Diagnostics NIP Server Lockdown Mode System Update Reboot I Shutdown About Logs	Model Product Code Serial Number Model Name SonicOS Version GUID System Time Up Time CPU Load	: SonicWall Network Security - Virtual Series : 70000 : : NSU Unlicensed Beta : 6.5.0.0 : : Tue 2018-03-27 20:58:06 UTC : 41 minutes 35 seconds : 1.1 Imin 1.1 Smin 1.0 10min
Up / Down to select items TAB to move between views Enter to action/edit an item SonicWall (c) 2018 Uptime 41 mi	https://192.168.	: Operational micWall web interface visit: // [Ctrl-s spacebar] to switch consol

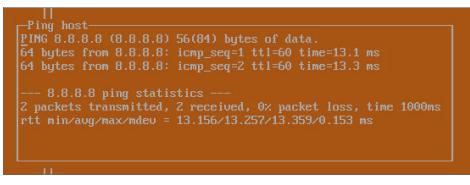
and press the **spacebar**. The NSv management console has an orange background.

- 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.

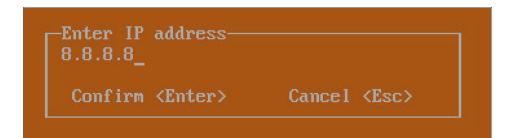
r	-Test	Management	Network-				
	Ping	Management		E	Ping	1	

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:



 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.

r-Menu	-Test Management Network	
System Info	Ping	[Ping]
Management Network	Nslookup	[Nslookup]
Test Management Network		
Diaynustics		
NTP Server		
Lockdown Mode		
System Update		
Reboot Shutdown		
About		
Logs		
1775 3 700		
	Enter IP address	
	192.168.8.1_	
	Confirm <enter></enter>	Cancel <esc></esc>
Up / Down to select items		
TAB to move between views		
Enter to action/edit an item		
THE REPORT OF THE PROPERTY OF		
SonicWall (c) 2018 Uptime 3 minu	tes [Ctrl-:	s spacebar] to switch console

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

To use Ping:

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

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



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

To use Nslookup:

- 1. Select **Test Management Network** in the Menu and press **Tab** to move the focus into the **Test Management Network** screen.
- 2. Select Nslookup to highlight it and press Enter to display the Enter hostname dialog.

- Menu	-Test Management Network	
System Info	Ping	[Ping]
Management Network	Nslookup	[Nslookup]
Test Management Network		
Diagnostics		
NTP Server		
Lockdown Mode		
System Update		
Reboot I Shutdown		
About		
Logs		
LUgs		
	Enter hostname	
	sonicwall.com	
		The second s
	Confirm <enter></enter>	Cancel <esc></esc>
the second second second		
Up / Down to select items TAB to move between views		
Enter to action/edit an item		
SonicWall (c) 2018 Uptime 5 minu	tes [Ctrl-s	s spacebar] to switch console

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

The Nslookup query results are displayed in an information dialog. You can scroll up and down within the dialog by using the up/down arrow keys.



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

Diagnostics

- Menu	Dia	gnostics——					
System Info	Send	diagnostics	to	SonicWall	support		
Management Network							
Test Management Network							
Diagnostics							
NTP Server							
Lockdown Mode							
Reboot Shutdown							
About							
Logs							
and the second sec							

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.

(i) **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

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

NTP Server

r-Menu-	-NTP Server-	
System Info	Sync with ntp server	
Management Network	Current time	
Test Management Network	Network time enabled	
Diagnostics	NTP synchronized	
NTP Server		
Lockdown Mode		
Reboot Shutdown		
About		
Logs		

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

The NTP Server screen displays the following information:

- Sync with NTP server This button forces the NSv 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.

▲ 40 PuTTY		-		×
-Menu- System Inio Network Interfaces Diagnostics NTP Serve: Lockdown Mode System Update Reboot Shutdown About Logs	-System Update	h		
	Begin System Update? Yes ℃ Confirm <enter> Cancel <esc></esc></enter>			
Up / Down to select items TAB to move between views Enter to action/edit an item SonicWall (c) 2018 Uptime 22	To log into the SonicWall web interface visit: https://192.168.1.4/ on Xl interface pours, 21 minutes [Ctrl-s spacebar] to	quit	The core	ole

Reboot | Shutdown

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

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.

Menu	Apr 25 20:31:54 localho	st Automatic secure crash analysis reporting is enabled
System Info	Apr 25 20:31:54 localho	st Periodic secure diagnostic reporting for support purposes is enable
Management Network	Apr 25 20:31:54 localho	st Initializing SonicWall support services
Test Management Network	Apr 25 20:31:52 localho	st Completed configuring the operating environment for SonicOS
Diagnostics	Apr 25 20:31:52 localho	st Completed configuring the operating environment for SonicOS
NTP Server	Apr 25 20:31:51 localho	st Model: "NSv 800" supports 8 CPU, current CPU count is only 2, for i
Lockdown Mode	Apr 25 20:31:51 localho	st Total memory installed 10237296 Kb
System Update	Apr 25 20:31:51 localho	st CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Reboot Shutdown	Apr 25 20:31:51 localho	st CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz"
About	Apr 25 20:31:51 localho	st Configuring the operating environment for SonicOS
Logs	Reboot	
	Apr 25 20:29:50 localho	st Unconfigure the operating environment for SonicOS
	Apr 25 20:04:26 localho	st Automatic secure crash analysis reporting is enabled
	Apr 25 20:04:26 localho	st Periodic secure diagnostic reporting for support purposes is enable
	Apr 25 20:04:26 localho	st Initializing SonicWall support services
	Apr 25 20:04:25 localho	st Completed configuring the operating environment for SonicOS
	Apr 25 20:04:25 localho	st No system information file available
	Apr 25 20:04:25 localho	st Total memory installed 10237296 Kb
	Apr 25 20:04:25 localho	st CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
	Apr 25 20:04:25 localho	st CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz"
	Apr 25 20:04:24 localho	st Configuring the operating environment for SonicOS
Up / Down to select items		
TAB to move between views		
Enter to action/edit an item		
Space to hide/show side menu		
	Arrow keys: Navigat	e view Current Line: 1 Lines: 21
micWall (c) 2018 Untime 23 ho		[Ctrl-s spacebar] to switch conso]

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
- Entering SafeMode

How Management Console Differs in SafeMode

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

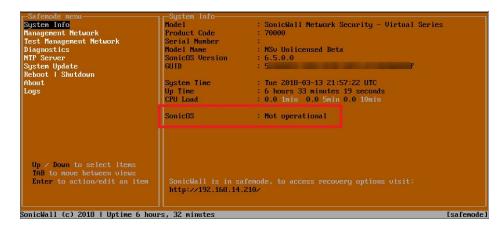
- Configurable interfaces
- Configurable default gateway
- Configurable DNS servers

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

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

Entering SafeMode

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



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

r Menu	-Reboot Shutdown-	
System Info	Reboot SonicWall	[Reboot 1
Management Network	Shutdown SonicWall	[Shutdown]
Test Management Network	Boot with factory default settings	[Factory Default]
Diagnostics	Boot SonicWall into debug	[Debug]
NTP Server	Boot SonicWall into safenode	Enable 1
Lockdown Mode	boot Sourcearr into Sarchoac	LINDIC
System Update		
Reboot I Shutdown		
About		
Logs		
		10
	Yes	
		l <esc></esc>
Up / Down to select items		
TAB to move between views		
Enter to action/edit an item	To log into the SonicWall web interfa	an utnitt
circle to action/calt an item	https://10.203.26.222/	ue visit.
	neeps .// 10.203.20.222/	
SomicHall (c) 2010 Untime 2 days	19 house 52 minutes	[Ctal_s spacebar] to suitch consols
SonicWall (c) 2018 Uptime 3 days	, 19 hours, 57 minutes	[Ctrl-s spacebar] to switch console

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

The NSv immediately reboots and comes back up in SafeMode.

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

Disabling SafeMode

To disable SafeMode:

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

-Safenode menu- System Info Management Network Test Management Network Diagnostics NTP Server	Reboot Shutdown Reboot SonicWall into safemode Shutdown SonicWall Disable safemode and boot factory de puot contewall into safemode	[Reboot] [Shutdown] fault[Factory Default] [PCong J [Disable]	
System Update Reboot Shutdown About Logs			
Up / Down to select items TAB to move between views Enter to action/edit an item	SonicWall is in safemode, to access http://192.168.14.210/		
onicWall (c) 2018 Uptime 6 hou	rs, 21 minutes		[safemod

- 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.

-Safemode menu			
Ogeton Info	Management interface	[X1]	
Management Network			
Toot Management Noter rk	IPv4 Address		
Diagnostics	Netmask		
NTP Server	Mac address		
System Update	IPu6 Address		
Reboot Shutdown	Gateway		
About	DNS 1		
Logs	DNS 2		
Up ∕ Down to select items TAB to move between views Enter to action∕edit an item	Select Interface X0 X1 X2 X3 X4 X5 X6 X7 Confirm (Enter) SonicWall is in safemode, to a http://192.168.14.200/ or http	access recovery options visit: ://192.168.1.254/	
SonicWall (c) 2018 Uptime 5 hou	rs, 43 minutes	Esafe	emode

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.

-Safemode menu	- M / M / T			
	Management interface	1	X1	1
Management Network				
Toot Management Noter rk	IPv4 Address		192.168.14.200	
Diagnostics	Netmask			
NTP Server	Mac address			
System Update	IPu6 Address	fe8		
Reboot Shutdown	Gateway			
About	DNS 1			
Logs	DNS 2			
	XZ X3 X4 X5 X6 X7 Confirm <enter></enter>			
Up / Down to select items TAB to nove between views Enter to action/edit an item	SonicWall is in safemode, to http:///192.168.14.200/ or htt			
onicWall (c) 2018 Uptime 5 hou	rs, 43 minutes			[safem

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 $\ensuremath{\text{IPv4}}$ Address on the screen and press $\ensuremath{\text{Enter.}}$

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.

-Safemode menu			
System Info	Management interface		
Management Network			
Test Management Network	IPu4 Address	[192.168.14.210	1
Diagnostics	Netmask	[255.255.248.0	1
NTP Server	Mac address		
System Update	IPu6 Address		
Reboot I Shutdown	Gateway		
About	DNS 1		
Logs	DNS 2		
	Save changes		Cancel
Up / Down to select items TAB to move between views Enter to action/edit an item	SonicWall is in safemode, to a http://192.168.14.210/ or http		
SonicWall (c) 2018 Uptime 6 hour	rs, 1 minute		[safemode]

(i) **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.

-Safemode menu	-Management Network-			
System Info	Management interface		X1	
Management Network				
Test Management Network	IPu4 Address	T	192.168.0.15	1
Diagnostics	Notrook	- P	PEE PEE PEE A	
NTP Server	Mac address		0:0c:29:5a:19:dd	
	IPu6 Address		::20c:29ff:fe5a:	
System Update				
Reboot Shutdown	Gateway			
About	DNS 1			
Logs	DNS 2			
Up / Down to select items TAB to move between views Enter to action/edit an item	SonicWall is in safemode, to a http://192.168.0.15/ or http:/			

Save changes displays.

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

The interface is disabled.

-Management Network	X1	
IPu4 Address Netmask Mar. address	Not configured	
IPo6 Address Gateway DNS 1 DNS 2	e80::20c:29ff:fe5a: 192.168.0.1 8.8.8.8 8.8.4.4	

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.

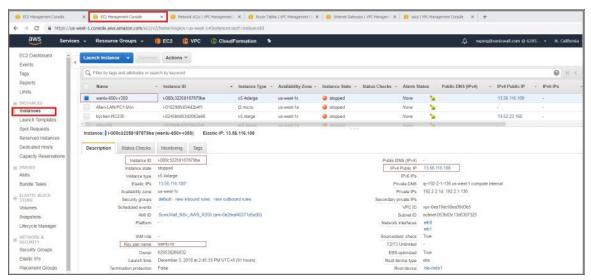
Topics:

- 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.



 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.

Menu	System Info-	
System Info	Mode 1	: SonicWall Network Security - Virtual Series
Network Interfaces		
Diagnostics	Product Code	: 72004
NTP Server		: 0
Lockdown Mode	Model Name	: NSV 400 (Azure)
System Update	SonicOS Version	: 6.5.0.2
Reboot Shutdown	GUID	A STATE OF A DESCRIPTION OF A DESCRIPTIO
About		
Logs	System Time	: Tue 2018-07-31 17:26:57 UTC
	Up Time	: 20 hours 2 minutes 50 seconds
	Load Average	
	SonicOS	: Operational
and the second second		
Up / Down to select items		
TAB to move between views		No. of Control of Cont
Enter to action/edit an item		onicWall web interface visit:
	nttps://192.16	/ on X1 interface
and the second se		
SonicWall (c) 2018 Uptime 20 ho	ura 1 minuto	[Ctrl-s spacebar] to switch console
BOILTEWAIT TEL 2010 ODLIME 20 NO	ars, r minute	ICUIT-S SDACeDAIT to SWITCH CONSOLE

- 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.

🗅 Soviewali 🗙 k k 🗧 🕫 13.57.201.56	×	Soricital Network Security X	 Sociolal - Authentication 	× +			-
← → C (() Not secure 13.56.1 # 100 #/log	ín			\$	•	0	1
SONICWALL Network Security Virtu	al						_
AWS EC2 Instance ID:							
Redarce ID							
Authenticate							
	_					_	_

- 5. In the AWS EC2 Instance ID field, enter the Instance ID for the NSv.
- 6. Click Authenticate. The SafeMode web interface displays.

SONICWALL NO	twork Security Virtual				
SonicOS is running in Safe Mode Safe Mode will allow you to do any of > Download the Safe Mode Logs > Upload new SonicOS applicatio > Boot your choice of application > Restore the settings to their fact Download Safe Mode Logs	he following: for troubleshooting by the SonicWa n images mage	ill Support Team	SonicOS Product Info Model: NSv Unliconsed Product Code: 70000 GUID: Serial Number:		
Image Management Restart Refresh Uploa Current Image Version 6.5.0.2-8v-sonicosv- 37-25793204	d Image Import Date 4/25/2018, 6:14:00 PM	Last Used Date 4/25/2018, 6:14:03 PM	Status Not Running: Safe Mode	Boot () •	Image Actions N/A

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.

C - - Saferede neru - System Cité - Server & Enterfaces - Diagneset co	Product Code	: Sonickall Hetwirk Security - Virtual Series 70000	D Second Hence Sec: X € Second - Achemican X € Second - Indexed Securit X D 11/31.115 X D 00000; The reparad (0, X + € → O ▲ Not Secure 13.56.116.106.04/	÷	© :
AUF Server System Uniste Refort Distibut About	Model Name SonictS Version GUID System Time	1 NSV Unlicensed 1 6-5-0-2 F EMIJSEC-7955-2870-A188-2A017914F549 1 The 2018-12-06 04-55132 UTC	SONICWALL [®] Network Security Virtual		
	Up Time Load Average SoulcOS	i 2 divinites 24 seconds 2 d.4 int 0.3 line 0.3 line i Not operational	Applance is numing in Safe Mode Safe Void any visit to dury of the bitmany Safe Mode will allow you to dury of the bitmany Safe Mode Mode Safe Control Product Infle Docenses the Safe Note Control Product Control National Inner Scottantin mapse		
	Lockdtwo	agement console is locked	Souri par criterie of application image Gauge instances of application image Gauge instances Another Souri fault instances Souri fault instances Deverticed Bah Nodel Loge		
			Host Appliance Catable Management Console		-
			Image Management Rester D Retron S Upload Image		
Up / Dewn 10 solect items TAB to move between view Enter in action/with an item Somickell (c) 2018 Uptime 1 min	http://13.36.116.10	mende, to access recovery options visit: 6/	Current Image Version Import Date Link Used Date Status Boot Image Av v 12/3/2016, 2:46.09 PM 12/3/2016, 2:46.30 PM Not running Image Av Not 6.50.2.8V-37.500- Status Status Not Not Not	tions	

Downloading the SafeMode Logs

You can download logs of SafeMode activity.

(i) **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:

SONICWALL Ne	twork Security Virtual				
SonicOS is running in Safe Mode Safe Mode will allow you to do any of t > Download the Safe Mode Logs > Upload new SonicOS applicatio > Boot your choice of application > Restore the settings to their fact Download Safe Mode Logs	the following: for troubleshooting by the SonicWa n images mage	ill Support Team	SonicOS Product Info Model: NSv Unliconsed Product Code: 70000 GUID: Serial Number:		
Image Management Restart Refresh Uploa	d Image				
Current Image Version ✓ 6.5.0.2-8v-sonicosv- 3725793204	Import Date 4/25/2018, 6:14:00 PM	Last Used Date 4/25/2018, 6:14:03 PM	Status Not Running: Safe Mode	Boot	Image Actions N/A

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

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.

(i) **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.

SONICWALL	twork Security Virtual				
SonicOS is running in Safe Mode Safe Mode will allow you to do any of t > Download the Safe Mode Logs > Upload new SonicOS application > Boot your choice of application > Restore the settings to their fact Download Safe Mode Logs	he following: for troubleshooting by the SonicWa n images mage	III Support Team	SonicOS Product Info Model: NSv Unlicensed Product Code: 70000 GUID: Serial Number:		
Image Management Restart © Refresh • Uploa Current Image Version ✓ 6.5.0.2-8v-sonicosv- 37-25793204	d Image Import Date 4/25/2018, 6:14:00 PM	Last Used Date 4/25/2018, 6:14:03 PM	Status Not Running: Safe Mode	Boot () v	Image Actions N/A

- 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

art 🕲 Refresh 🕑 Upload 1	Image				
urrent Image Version 🗸 .5.0.2-8v-sonicosv-37-f207f34d	Import Date 4/12/2018, 4:28:26 PM	Last Used Date 4/12/2018, 4:28:45 PM	Status Not Running: Safe Mode	Boot	Image Actions
Uploaded Image Version 6.5.0.2-8v-sonicosv-37f207f34d	Load Date 4/12/2018, 4:49:31 PM	Build Date 4/12/2018, 3:39:33 AM		Boot () +	Image Actions
			Boot Uploaded Image (6.5.0.2-8v-s with Current Configuration Boot Uploaded Image (6.5.0.2-8v-s with Factory Default Configuration	~	

The NSv virtual machine reboots with the new image.

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.

SonicOS 7 Getting Started Guide for AWS 91 SonicWall Support

6

About This Document

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

Copyright © 2023 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/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