SonicWall[®] NS_v Series on AWS

Getting Started Guide (BYOL / PAYG)



Contents

Introducing the NSv Series
Feature Support Information
Node Counts Per Platform
Product Matrix and Requirements
Github Repository
Backup and Recovery Information7
Exporting and Importing NSv Configurations
Upgrading to a Higher Capacity NSv Model
Creating a MySonicWall Account
Installing NSv Series on AWS
Supported NSv Series Models on AWS10
Task List for NSv Series AWS Instance Setup11
Deploying NSv from Console
Modify Routing Tables for NSv Access
Deploying AWS from Cloud Template
Change Routing Tables for NSv Access
Accessing the SonicWall NSv Web Interface
Configuring Internet/Public Access Through the NSv
Troubleshooting Installation Configuration
Deployment Options
Deploying the NSv as PAYG
Deploying the NSv as BYOL
De-activating Your NSv
Converting a Free Trial License to Full License
Creating a MySonicWall Account
SonicOS Management
Managing SonicOS on the NSv Series
Using SonicOS on an Unregistered NSv
Using System Diagnostics in SonicOS
Check Network Settings
Upgrading the NSv
Using the Virtual Console and SafeMode48
Connecting to the Management Console with SSH
Navigating the NSv Management Console
System Info
Management Network or Network Interfaces53
Test Management Network
Diagnostics
NTP Server
Lockdown Mode

SonicWall NSv Series AWS Getting Started Guide Contents 2

System Update
Reboot Shutdown
About
Logs
Using the Management Console in SafeMode60
How Management Console Differs in SafeMode
Entering SafeMode
Enabling/Disabling SafeMode61
Configuring the Management Network in SafeMode62
Using the SafeMode Web Interface
Accessing the SafeMode Web Interface
Entering/Exiting SafeMode68
Locking and Unlocking the Management Console69
Downloading the SafeMode Logs69
Uploading a New Image in SafeMode70
SonicWall Support
About This Document

Introducing the NS_v Series

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

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

IMPORTANT: You may choose to operate 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 NSv Series on AWS to start. Separate instructions for different pricing models are given in Deployment Options.

SonicWall NSv on AWS Marketplace

🐲 aws marketplace					Q
Categories 👻 Delivery Methods 👻	Solutions 👻 🛛 AWS IQ 👻	Your Saved List			Partners Sell in AWS Marketplace
	SONICWALL	SonicWall NSv (Firewall/Sec By: SonicWall C Latest Version: 7.0.0-1036 The SonicWall Network Security virtual (NSv) fir generation firewall capabilities such as application > Show more Linux/Unix ******* 1 AWS review 80 Free Trial	wall series brings industry l on control, IPS, TLS/SSL dec	eading next-	Continue to Subscribe Save to List Typical Total Price \$0.655/hr Total pricing en instance for services hosted on c5.large in US East (N. Virgina). View Details
	overview Product Over	Pricing	Usage	Support	Reviews
	SonicWall Network Securit next-generation firewall (h control, real-time monitori threat protection (ATP), VP your AWS environment. NS networking features in Sor patented Reassembly-Free award-winning Capture AT (RTDMI) for advanced thre- Centrally manage all your 1 (CSC) to maintain consister	y virtual (NSv) firewall series brings industry leadii GFW) capabilities such as application intelligence ng, IPS, TLS/SSL decryption and inspection, advan N and network segmentation capabilities to prote virtual frewalls support the same security and icWall physical NGFW appliances including our Deep Packet Inspection (IRFDPI) technology and P sandbox with Real-Time Deep Memory Inspectio at protection. Tirewalls using the SonicWall Capture Security Cen t security policies across cloud and on-premises helps you implement security best practices and	and ced ct n ▶ 0:00 / 2:35	The set of	

The SonicWall[®] Network Security Virtual Series (SonicWall[®] NSv Series) is SonicWall's virtualized next-generation firewall appliance that provides Deep Packet Inspection (DPI) security and segmentation in virtual environments. SonicOS running on the NSv Series offers the feature functionality and security features of a physical appliance, with comparable performance. SonicOS Virtual is a fully featured 64-bit SonicOS powered by SonicCore.

Topics:

- Feature Support Information on page 5
- Node Counts Per Platform on page 6
- Product Matrix and Requirements on page 7
- Github Repository on page 7
- Backup and Recovery Information on page 7
- Exporting and Importing NSv Configurations on page 8
- Upgrading to a Higher Capacity NSv Model on page 8
- Creating a MySonicWall Account on page 8

Feature Support Information

The SonicWall NSv has nearly all the features and functionality of a SonicWall hardware appliance running SonicOS 6.5.4 firmware.

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

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

(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 above. Consequently, DHCP services and VLAN interfaces are not supported on NSv appliances running in AWS.

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

Feature Support List

Network InterfacesOverride MAC AddressNot supportedNetwork InterfacesDHCPv6 Prefix Delegation (PD)Not supportedNetwork InterfacesIPv6 ManagementSupportedNetwork Interfaces6rdNot supportedNetworkPortshield GroupsNot supportedNetwork InterfacesL2 Bridge ModeNot supportedNetwork InterfacesNative BridgeNot supportedNetwork InterfacesWire Mode v4Not supportedNetwork InterfacesWire Mode v4Not supportedNetwork InterfacesPPPENot supportedNetwork InterfacesPPPENot supportedNetwork InterfacesPPOENot supportedNetwork InterfacesPPOENot supportedNetwork InterfacesPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesLap ModeNot supportedNetwork InterfacesTap ModeNot supportedNetwork InterfacesLink AggregationNot supported	
Network InterfacesIPv6 ManagementSupportedNetwork Interfaces6rdNot supportedNetworkPortshield GroupsNot supportedNetwork InterfacesL2 Bridge ModeNot supportedNetwork InterfacesL2 Bridge ModeNot supportedNetwork InterfacesWire BridgeNot supportedNetwork InterfacesWire Mode v4Not supportedNetwork InterfacesWire Mode v6Not supportedNetwork InterfacesPPPOENot supportedNetwork InterfacesPPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesTap ModeNot supported	
Network Interfaces6rdNot supportedNetworkPortshield GroupsNot supportedNetworkInterfacesL2 Bridge ModeNot supportedNetwork InterfacesNative BridgeNot supportedNetwork InterfacesWire Mode v4Not supportedNetwork InterfacesWire Mode v6Not supportedNetwork InterfacesPPPoENot supportedNetwork InterfacesPPTPNot supportedNetwork InterfacesPTPNot supportedNetwork InterfacesTap ModeNot supportedNetwork InterfacesTap ModeNot supported	
NetworkPortshield GroupsNot supportedNetwork InterfacesL2 Bridge ModeNot supportedNetwork InterfacesNative BridgeNot supportedNetwork InterfacesWire Mode v4Not supportedNetwork InterfacesWire Mode v6Not supportedNetwork InterfacesPPPoENot supportedNetwork InterfacesPPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesTap ModeNot supported	
Network InterfacesL2 Bridge ModeNot supportedNetwork InterfacesNative BridgeNot supportedNetwork InterfacesWire Mode v4Not supportedNetwork InterfacesWire Mode v6Not supportedNetwork InterfacesPPPoENot supportedNetwork InterfacesPPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesTap ModeNot supported	
Network InterfacesNative BridgeNot supportedNetwork InterfacesWire Mode v4Not supportedNetwork InterfacesWire Mode v6Not supportedNetwork InterfacesPPPoENot supportedNetwork InterfacesPPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesTap ModeNot supported	
Network InterfacesWire Mode v4Not supportedNetwork InterfacesWire Mode v6Not supportedNetwork InterfacesPPPoENot supportedNetwork InterfacesPPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesTap ModeNot supported	
Network InterfacesWire Mode v6Not supportedNetwork InterfacesPPPoENot supportedNetwork InterfacesPPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesTap ModeNot supported	
Network InterfacesPPPoENot supportedNetwork InterfacesPPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesTap ModeNot supported	
Network InterfacesPPTPNot supportedNetwork InterfacesL2TPNot supportedNetwork InterfacesTap ModeNot supported	
Network Interfaces L2TP Not supported Network Interfaces Tap Mode Not supported	
Network Interfaces Tap Mode Not supported	
· · · ·	
Network Interfaces Link Aggregation Not supported	
Network Interfaces Port Redundancy Not supported	
Network Interfaces IP Unnumbered Not supported	
Network Interfaces VLAN Translation Not supported	
Network Interfaces Users IPv6 Supported	
Network Interfaces DHCP Server Not Supported	
Network Interfaces VLAN Interfaces Not Supported	
Network Interfaces Jumbo Frames Not Supported	
Firewall Settings Global BWM Not Supported	
Firewall Settings QoS Mapping Not Supported	
Firewall Settings Multicast Not Supported	
Switching Not supported	

Feature Support List

Component	Feature	Status
Anti-spam		Not supported
3G/4G Modem		Not supported
Wireless		Not supported
SonicPoints		Not supported
Virtual Assist		Not supported
High Availability	Active/Passive	Not supported
High Availability	Stateful Sync	Not supported
High Availability	Firmware Sync	Not supported
High Availability	Active-Active DPI	Not supported
WAN Acceleration		Not supported
SSL VPN	SSL VPN for IPv6	Supported
VoIP	H.323	Supported
VoIP	SIP	Supported
Diag page	Unsupported Options	Partially supported
External Storage Sup- port		Not supported

Node Counts Per Platform

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

Maximum Node Counts Per Platform

Platform	Maximum Node Count
NSv 10	10
NSv 25	25
NSv 50	50
NSv 100	100
NSv 200 and higher	Unlimited

Node counts are calculated by SonicOS as follows:

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

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

Product Matrix and Requirements

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

Product Models	NSv 10	NSv 25	NSv 50	NSv 100	NSv 200	NSv 400	NSv 800	NSv 1600
Maximum Cores ¹	2	2	2	2	2	4	8	16
Minimum Total Cores	2	2	2	9	2	2	2	2
Management Cores	1	1	1	1	1	1	1	1
Maximum Data Plane Cores	1	1	1	1	1	3	7	15
Minimum Data Plane Cores	1	1	1	1	1	1	1	1
Network Interfaces	2	2	2	2	2	4	8	8
Supported IP/Nodes	10	25	50	100	No limit	No limit	No limit	No limit
Minimum Memory Required	4G	4G	4G	4G	6G	8G	10G	12G
Minimum Hard Disk/Storage	35G	35G	35G	35G	35G	35G	35G	35G

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

Github Repository

SonicWall NSv AWS templates are available in the github repository:

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

Backup and Recovery Information

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

- If the splash screen remains displayed, this can indicate that the disk is corrupted. Please contact SonicWall for assistance.
- If the disk is not recoverable, then the NSv appliance needs to be de-activated. See De-activating Your NSv on page 39 for information.
- If SonicOS does not boot up, you can go into SafeMode and download the log files, upload a new SonicOS image, or take other actions. For information about SafeMode, see Using the Management Console in SafeMode.
- If SonicOS fails three times during the boot process, it will boot into SafeMode. Verify that the minimum required memory is available and allocated based on the NSv model. If it still cannot boot up, download the logs while in SafeMode and contact SonicWall for assistance.

Exporting and Importing NS_v **Configurations**

Moving configuration settings from SonicWall physical appliances to the NSv Series is not supported. However, configuration settings may be moved from one NSv to another. See the *SonicOS 6.5 NSv Series Updates* administration book and the *SonicOS 6.5.4 NSv Series Upgrade Guide* on the Technical Publications portal for more information about exporting and importing configuration settings. Go to

https://www.sonicwall.com/support/technical-documentation/ and select "NSv Series" as the product.

Upgrading to a Higher Capacity NS_v Model

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

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

Creating a MySonicWall Account

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

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

To create a MySonicWall account:

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

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



3 Complete the account information, including email and password.

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

- 4 Enable two-factor authentication if desired.
- 5 If you enabled two-factor authentication, select one of the following authentication methods:
 - Email (one-time passcode) where an email with a one-time passcode is sent each time you log into your MySonicWall account.
 - **Microsoft/Google Authentication App** where you use a Microsoft or Google authenticator application to scan the code provided. If you are unable to scan the code, you can click on a link for a secret code. Once the code is scanned, you need only click on a button.
- 6 Click on **CONTINUE** to go to the **Company** page.
- 7 Complete the company information and click **CONTINUE**.
- 8 On the Your Info page, select whether you want to receive security renewal emails.
- 9 Identify whether you are interested in beta testing new products.
- 10 Click **CONTINUE** to go to the **Extras** page.
- 11 Select whether you want to add additional contacts to be notified for contract renewals.
- 12 If you opted for additional contacts, input the information and click ADD CONTACT.
- 13 Click DONE.
- 14 Check your email for a verification code and enter it in the **Verification Code*** field. If you did not receive a code, contact Customer Support by clicking on the link.

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

Next Steps

- Installing NSv Series on AWS on page 10
- Deployment Options on page 34.

2

Installing NS_v Series on AWS

Topics:

- Supported NSv Series Models on AWS on page 10
- Task List for NSv Series AWS Instance Setup on page 11
- Deploying NSv from Console on page 11
- Modify Routing Tables for NSv Access on page 18
- Change Routing Tables for NSv Access on page 25
- Deploying AWS from Cloud Template on page 20
- Accessing the SonicWall NSv Web Interface on page 26
- Configuring Internet/Public Access Through the NSv
- Troubleshooting Installation Configuration on page 30

Supported NS_v Series Models on AWS

Determine the NSv instance type you will require before starting installation.

NSv Models (Instance Sizes) on AWS

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

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

(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 AWS instance maybe constrained by the AWS VM.

Task List for NS_v Series AWS Instance Setup

- 1 Deploy a new VPC with NSv from the AWS Console
 - Deploying NSv from Console on page 11
 - Change Routing Tables for NSv Access on page 25

OR:

- 1 Deploy NSv to an existing VPC with AWS Cloud Formation Templates
 - Deploying AWS from Cloud Template on page 20
 - Change Routing Tables for NSv Access on page 25

THEN:

- 2 Register the NSv on MySonicWall
 - Creating a MySonicWall Account on page 41

Deploying NS_v from Console

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

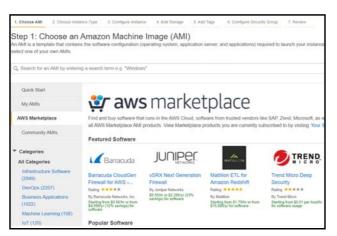
- 1 Log into the AWS Console.
 - a Go to the AWS management console at https://aws.amazon.com.
 - b Log into the AWS management console.
 - c From the Services menu select EC2.

aws Services 🔺		
★ Favorites	All services	
lesource Groups & Tag Editor	Q Find services by names, keywords of	or acronyms.
Recently visited	EC2	ලී Robotics AWS RoboMaker
EC2	Lightsail 🖸	
Console Home	Lambda	③ Customer Enablement
AWS Marketplace Subscriptions	Batch	AWS IQ 🛂
	Elastic Beanstalk	Support
	Serverless Application Repository	Managed Services
	AWS Outposts	Activate for Startups
	EC2 Image Builder	

- 2 Follow these steps to launch the SonicWall NSv:
 - a From the EC2 Dashboard, select Launch Instance.

New EC2 Experience Tel os what you there	Instances (running) 1
EC2 Dashboard	Elastic IPs 0
Events New	Key pairs 0
Tags	Placement groups 0
Limits	Snapshots 0
 Instances 	Snapshors 0
Instances New	Easily size, configure, and deploy Microsoft SQL Server Always
Instance Types	SQL Server, Learn more
Instance Types Launch Templates	SQL Server, Learn more
a de la construcción de la constru	SQL Server, Learn more
Launch Templates	
Launch Templates Spot Requests	SqL Server, Learn more
Launch Templates Spot Requests Savings Plans	Launch instance
Launch Templates Spot Requests Savings Plans Reserved Instances	
Launch Templates Spot Requests Savings Plans Reserved Instances Dedicated Hosts New	Launch instance To get started, launch an Amazon EC2 Instance, which is a virtual

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

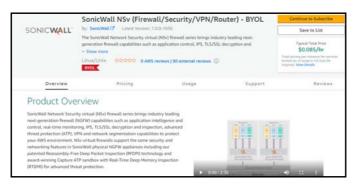


c Click the Select button next to the SonicWall NSv (Firewall/Security/VPN/Router).

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

Q, sonicwall Nsv			×
			Search by Systems Manager parameter
Quick Start (0)			(1 to 2 of 2 Products >)
My AMIs (0)	SONICWALL	SonicWall NSv (Firewall/Security/VPN/Router) - PAYG	Select
AWS Marketplace (2)		************************************	
Community AMIs (4)	Free Trial	Javarneg men an an en en an en an e even pretta samegar de semener e ante unage texe Linux/Unix, Gantos SonicOS 6.5.4.4 64-bit (x80) Amazon Machine Image (AMB) Updated: 11420	
Categories All Categories		The Sonc/Mal Network Security virtual (NSV) frewail series brings industry leading next generation frewail capabilities such as application control, IPS, TLSSSL decypt inspectors, advanced thread protection (ATP), VPN and network segmentation to protect your ANS environment. More into	ion and.
Infrastructure Software (2)	SONICWALL	SonicWall NSv (Firewall/Security/VPN/Router) - BYOL	Select
IoT (2)	DOMERT	***** (0) (7.0.0-1036 Previous versions (By SamcHut	
 Architecture 		LinuxUnia, Gentur SunicOS 7.0.0 (64-bit (eBE) Amazon Machine Image (AMI) Updated: 11/6/20	
064-bit (x86) (2)		The SonicWall Network Security virtual (NSv) treveal series brings industry leading neit-generation freewall capabilities such as application control, IPS, TLS/SSI, decrypt inspection, advanced threat protection (ATP), VPN and network segmentation to protect your AWS environment.	ion and
· Operating System		More info	

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



- e Click Continue to Subscribe and accept the terms and conditions.
- f On the next screen, click **Continue to Configuration**.

SONICWALL SonicWall NSv (Fire BYOL	wall/Securit	y/VPN/Rout	er) -	Continue to Configuration
Thank you for subscribing to this product! You can now o	onfigure your softwa	re.		×
< Product Detail Subscribe				
Subscribe to this software				
You're subscribed to this software. Please see the te configure your software.	rms and pricing de	tails below or click	the button above to	
Terms and Conditions				
SonicWall Offer				
You have subscribed to this software and agreed th and the seller's End User License Agreement (EULA) transaction (including your payment terms) with th applicable, in accordance with the AVX5 Privacy Not Customer AgreementS or other agreement with AVX	C. You agreed the respective seller, ice C. Your use of a	at AWS may share in reseller or underlyin AWS services remain	formation about this og provider, as 15 subject to the AWS	
Product	Effective date	Expiration date	Action	
SonicWall NSv (Firewall/Security/VPN/Router) - BYOL	11/19/2020	N/A	✓ Show Details	

- g On the next screen, select the following based on your requirements:
 - Delivery Method
 - Software Version
 - Region

SONICWALL SonicWall NSv BYOL	(Firewall/Security/VPN/Router) -	Continue to Launch
Product Detail Subscribe <u>Configure</u>		
Configure this software		Pricing information
equired to configure the deployment.	ow you wish to deploy the software, then enter the information	This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.
Delivery Method		Software Pricing
64-bit (x86) Amazon Machine Image (AMI) Software Version	•	SonicWall NSv S0/hr (Firewall/Securit y/VPN/Router) - BYOL
7.0.0-1036 (Nov 06, 2020)	v	BYOL
Select a version		c5 targe
7.0.0-1036 (Nov 06, 2020)		Infrastructure Pricing
6.5.4.4-44v-21-987 (Sep 15, 2020)	ent may alter your final pricing.	EC2: 1 * c5.large Monthly Estimate: \$61.00/month
Ami Id: ami-0a53547243126d7c4		
Product code: 2y77hbheav4o7jahg2c9hpee8		
Release notes (updated November 6, 2020)		

- h Once you have made the selection, click **Continue to Launch**.
- i In the Launch screen, select Launch through EC2 option from the Choose Action drop-down and click Launch.
- j Select the Instance Type corresponding to the SonicWall NSv model you require.

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

NSv Models and AWS Image Types

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

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

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

aws Services - R	esource Groups 🗸 🔸
1. Choose AMI 2. Choose Instance Type	3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. F
Step 3: Configure Instan Configure the instance to suit your require	ce Details ments. You can launch multiple instances from the same AMI, request Spot instances to take a
Number of instances	Launch into Auto Scaling Group ()
Purchasing option	(i) Request Spot instances
Network	(i) vpc-0ba96600ddab58c09 example C Create new VPC
Subnet	(i) [subnet-072c2e649082850e4 X1WAN us-east-2a ▼ Create new subnet 243 IP Addresses available
Auto-assign Public IP	() Use subnet setting (Disable)
Placement group	Add instance to placement group.
Capacity Reservation	Open Open C Create new Capacity
IAM role	(i) None C Create new IAM role
CPU options	(i) Specify CPU options
Shutdown behavior	(i) Stop v
Enable termination protection	 Protect against accidental termination
Monitoring	Image: CloudWatch detailed monitoring Additional charges apply.
EBS-optimized instance	 ✓ Launch as EBS-optimized instance
Tenancy	(i) Shared - Run a shared hardware instance Additional charges will apply for dedicated tenancy.
 Network interfaces (i) 	
Device Network Interface S	Subnet Primary IP Secondary IP addresses
eth0 New network interface •	subnet-072c2e64 Auto-assign Add IP
Add Device	

- I To add additional Elastic Network Interfaces click Add Device. The firewall MUST at minimum have 2 ENI attached. The ENI interfaces MUST be on separate subnets. The eth0 ENI device will be connected to the SonicWall NSv X1 interface that is the public interface. The eth1 ENI device will be connected to the SonicWall NSv X0 interface that is the private interface.
- (i) **NOTE:** If you get a response from the system offering only two interfaces with the same subnet, check all subnets in the VPC with the VPC availability board to ensure that they are in the same availability zone.

▼ Netw	vork interfaces 🛈				
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface v	subnet-072c2e64 V	Auto-assign	Add IP	Add IP
eth1	New network interface v	subnet-06321bdt 🔻	Auto-assign	Add IP	
0		ddress feature for this in	istance is disabled because yo	u specified multiple network interfaces. Public IPs c iss feature, please specify only the eth0 network int	
Add Dev					
	anced Details				

- m Accept the default storage options by clicking the Add Storage button.
- n Click the **Add tags** button. Add metadata to the instance configuration to assist in identifying the SonicWall NSv instance.
- o Click the: **Configure Security Group** button. At minimum, allow SSH and HTTPS from a predefined source.

	#Cruate a new security group Difetect an waterlog security group			
Security group name: Description:	Jaunch witrand 5 Jaunch witrand 5 created 2018-11-19718 08 18 544+08 08			
Ne (j)	Protocol ()	Port Range (3)	Source (j)	Description (j)
UH •)	TCP	22	Custore • 107 154 75 50:32	5.5H
Custom ICMP +	Ectro Rapty •	N/A.	(Custore •) 117 154 75 50/32	a g SSH for Admin Desktop
Custom UDP1 +	UDP	4500	(Custum +) 107.154.75.50/32	ippec natid
Custure UDP1 +	LUDP	500	(Costors •) 107 154 75 50/32	ISAKMP
(TTPS +)	TCP	443	Castars + 107 154 75 50/32	HTTPS management

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

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

Select	an existing key pair or create a new	v key pair ×
they allow obtain the	consists of a public key that AWS stores, and a private you to connect to your instance securely. For Windows A password used to log into your instance. For Linux AMIs, SSH into your instance.	MIs, the private key file is required to
Note: The	selected key pair will be added to the set of keys authoriz	ed for this instance. Learn more
about rem	oving existing key pairs from a public AMI.	
Creat	e a new key pair	¥
Key p	air name	
Sonic	Wall-NSv-example	
		Download Key Pair
	You have to download the private key file (*.pem file) b it in a secure and accessible location. You will not be again after it's created.	

- r Click the Launch Instances button to deploy the SonicWall NSv instance. Deployment will take between 5 to 8 minutes. You can monitor the progress by viewing the instance in the EC2 Dashboard.
- 3 Disable source/destination checking:
 - a Select Network Interfaces from the left menu of the EC2 Dashboard.
 - b For each network interface connected to the new SonicWall NSv instance, disable the source and destination check.

To do this, right click on the network interface and select **Change Source/Dest Check**.

- c Select the **Disabled** checkbox and press **Save**.
- 4 To assign an Elastic IP, follow these steps:
 - a From the EC2 Dashboard left hand menu select Elastic IPs.
 - b Right click on a free Elastic IP and select **Associate**. If no Elastic IPs are available, then click on **Allocate new address**.

aws	Services	•	Resource	Group	isv t⊱					
Dedicated Hosts	• -	Alloo	cate new add	ress	Actions ¥					
Capacity Reservations		Q,	Filter by tags a	ind attri	butes or search I	oy keyw	ord			
IMAGES AMIs			Name	~ E	Elastic IP	*	Allocation ID	Ŧ	Instance	
Bundle Tasks					3.98.91.54		eipalloc-all man		•	Release addresses
ELASTIC BLOCK STORE					(3.58) 1(217 (241) 12.144 (202) 51		eipalloc-		i-004db3ee9 i-0dcf39fe37	Associate address Disassociate address
Volumes				1	2.14.248.156		eipalloc-		i-02aa41c53	Add/Edit Tags
Snapshots				5	2.15.153.97		eipalloc finisement		-	
Lifecycle Manager										
NETWORK & SECURITY										
Security Groups										
Elastic IPs										

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

Addresses > Associate address
Associate address
Select the instance OR network interface to which you want to associate this Elastic IP address (13.58.51.54)
Resource type 0 Instance
Network interface
Network interface eni-06cbb45af81aa1dee 🗸 C
Private IP Select a private IP C
Reassociation 🔲 Allow Elastic IP to be reassociated if already attached 🚯
Warning If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more.
Cancel Associate

- d Click **Associate**. This IP address can now be used to connect to the SonicWall NSv web management interface.
- 5 Connect to the firewall web management interface:
 - a Now that you have associated an Elastic IP to the SonicWall NSv instance you will be able to connect to the web management interface by entering the IP address into your browser.

SONICWALL Network Security Virtual
Username
Password
LOG IN

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

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

Modify Routing Tables for NS_{ν} Access

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

EC2 Dashboard	Launch Instanc	🛛 🤜 Connec	t Actions ~				Z		
Events		and attributes or se					0 K < 1	to 1 of 1 >	
Tags	C Filter by tags	and attributes or se	arch by keyword				e k k i	10 1 01 1 >	21
Reports	Name	- Instance ID	 Instance Type 	e - Availability Zone -	Instance State - Status Checks -	Alarm Status Publ	ic DNS (IPv4)	- IPv4 Pub	blic IP
Limits	SonicWall	ISv i-0c6b32ead	63026d20 c5.large	ap-south-1a	running Ø 2/2 checks	None 🍃		13,232,1	08.24
 INSTANCES 	Concertaint	1000002080	ooozoozo conarge	apoourra	• Torring • 22 Criscos	10000		10.202.1	00.24
Instances									
Launch Templates									
Spot Requests									
Spot Requests Reserved Instances									
Reserved Instances Dedicated Hosts	Instance: 1-0c	ib32ead63026d20	(SonicWall NSv) Elas	itic IP: 13.232.196.249				-	
Reserved Instances Dedicated Hosts	Instance: I-Oct	ib32ead63026d20	(SonicWall NSv) Elas	tic IP: 13.232.198.249					
Reserved Instances Dedicated Hosts IMAGES AMIs	Instance: I-Oct	ib32ead63026d20 Status Checks	(SonicWall NSv) Elas Monitoring Tags	tic IP: 13.232.196.249					
Reserved Instances Dedicated Hosts		Status Checks	Monitoring Tags	tic IP: 13.232.198.249				8	
Reserved Instances Dedicated Hosts IMAGES AMIs				ntic IP: 13.232.198.249	Public DNS (IPv4) IPv4 Public IP				
Reserved Instances Dedicated Hosts IMAGES AMIs Bundle Tasks		Status Checks	Monitoring Tags i-0c6b32ead63026d20	tic IP: 13.232.198.249	Public DNS (IPv4)				
Reserved Instances Dedicated Hosts MAGES AMIs Bundle Tasks © ELASTIC BLOCK STORE		Status Checks Instance ID Instance state	Monitoring Tags I-0c6b32ead63026d20 running	tic IP: 13.232.198.249	Public DNS (IPv4) (IPv4 Public IP		h-1.compute.internal		
Reserved Instances Dedicated Hosts MAGES AMIs Bundle Tasks © ELASTIC BLOCK STORE Volumes		Status Checks Instance ID Instance state Instance type	Monitoring Tags i-0c6b32ead63026d20 running c5.large	tic IP: 13.232.196.249	Public DNS (IPv4) IPv4 Public IP IPv6 IPs	13.232.198.249			
Reserved Instances Dedicated Hosts MAGES AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes Snapshots		Status Checks Instance ID Instance state Instance type Elastic IPs	Monitoring Tags i-0c6b32ead63026d20 running c5.large 13.232.198.249*	pWan-7J2P9ASWNK58.	Public DNS (IPv4) IPv4 Public IP IPv6 IPs Private DNS	13.232.198.249 - ip-192-168-0-4.ap-south			
Reserved Instances Dedicated Hosts MAGES AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager	Description	Status Checks Instance ID Instance state Instance type Elastic IPs Availability zone	Monitoring Tags i-0c6b32ead63026d20 running c5.large 13.232.198.249* ap-south-1a SonicWall-NSV-NSVSecGr	pWan-7J2P9ASWNK58.	Public DNS (IPv4) IIPv4 Public IP IPv6 IPa Private DNS Private IPs	13.232.198.249 - ip-192-168-0-4.ap-south	121		
Reserved Instances Dedicated Hosts Dedicated Hosts AMIs Bundie Tasks ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager NETWORK & SECURITY	Description	Status Checks Instance ID Instance state Instance type Elastic IPs Availability zone Security groups	Monitoring Tags i-0c6b32ead63026d20 running c5.large 13.282.198.249* ap-south-1a SonicWal-NSV-NSVSecGr view inbound rules, view of	pWan-7J2P9ASWNKS8. outbound rules	Public DNS (IPv4) IIPv4 Public IP IIPv6 IPa Privato DNS Privato IPs Secondary private IPs	13.232.198.249 - ip-192-168-0-4.ap-south 192.168.0.4, 192.168.1.1	121		

- 2 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.

3 CloudFormation Manage X	🗿 Problem loading page 🛛 🔒 S3	Management Console 🗙 🥫	Route Tables V	PC Mane 3	🔞 EC2 Management Conso 🗙 🔓 EC2 Management Conso 🗙 🕴 İcanhazip	.com/	× +	
(←) ← ⊕	① A https://ap-south-1.console.av	is amazon.com/vpc/home?reg	ion=ap-south-1#	routetable	es: 🖾 🗘 🔍 Search		¥ ₩	
aws Services	👻 Resource Groups 👻 🔶				🗘 smađugula (j) 3798-3630-3831	- Mumbai -	Suppor	t Y
VPC Dashboard	Create Route Table Delete Route Tab	le Set As Main Table				C	٥	0
Filter by VPC:	QSearch Route Tables and their X					< 1 to 6 of 6 Ro	ute Tabl	es>>-
Virtual Private Cloud	Name	- Route Table ID - Expl	icitly Associar-	Main -	VPC +			
	SonicWall NSvRoute Table WAN	ntb-09bba975786ec 1 Sul	bnet	No	vpc-00cc37c92d605f311 NSv VPC			-
Your VPCs		rtb-0826b63bd5613 0 Sul	boets	Yes	vpc-026bc6832afd8be20 existing-vpc			
Subnets		ntb-0401b47029ba7 0 Sul	briets	Yes	vpc-00cc37c92d605f311 NSv VPC			
Route Tables	existing-vpc-rtb-wan	rtb-0ea9f2ede1645a 1 Sut	briet	No	vpc-026bc6832afd8be20 existing-vpc			
Internet Gateways	existing-vpc-rtb-lan	nb-060a2b8556881 1 Sul	briet	No	vpc-026bc6832afd8be20 existing-vpc			
Egress Only Internet Gateways	SonicWall NSvRoute Table LAN	rtb-053b9ed4te028d 1 Sut	bnet	No	vpc-80cc37c92d605f311 NSv VPC			
DHCP Options Sets								
Elastic IPs								
Endpoints								
Endpoint Services	rtb-060a2b85568817fec existing-vpc-rtb	lan					-	88
NAT Gateways	Summary Routes Su	onet Associations Route Pro	opagation	Tags				
Peering Connections	Cancel Save							
	View: All rule	s						
Security	Destination Targ	et Statu	s Propagated	Remove				
Network ACLs	10.0.0.0/16 local	Active	No					
Security Groups		08daf802f01eda6f4	No	0				
VPN Connections				_				
	Add another route	-08daf802f01eda6f4 SonicWa	II NSV Interface L	AN .				
Customer Gateways								
Virtual Private Gateways								
VPN Connections								
🗨 Feedback 🔇 Englist	1 (US)				© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights res	served. Privacy Poli	cy Ten	ns of Use

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 ×	: 🔮 Problem loading page 🗙 🤘	53 Management Conso	le × 🧧 Route Tables	VPC Martin X	EC2 Management Consil: X EC2 Management Consil: X Icanhazip.com/	ं	< +	
-) → C @	0 🖨 https://ap-south-1.consol	le.aws.amazon.com/vp	/home/region=ap-south	+1#routetable	s: ···· 🛡 🔂 🔍 Search	3	F 11/	
aws services	Resource Groups 😽 🔸				\Lambda smadugula @ 3798-3630-3831 + →	Mumbal Minist	Support	e.
VPC Dashboard	Create Route Table Delete Route	Table Set As Main	Table			C	٥	0
Filter by VPC:	Q Search Route Tables and their X				· « <11	o 6 of 6 Rout	e Table	is>⇒
Listen Delaste Claud	Name	* Route Table ID	- Explicitly Associat	- Main -	VPC +			
Virtual Private Cloud	SoricWat NSvRoute Table WAN	ntb-09bba975786	en 1 Subnet	No	vpc-00cc37c928605f311 NSv VPC			
Your VPCs		rtti-0826b63bd56	13 0 Subnets	Yes	vpc-026bc6832afd8be20 axisting-vpc			
Subnets		rtb-04010470298	a7 0 Subnets	Yes	vpc-00cc37c92d6056311 NSv VPC			
Route Tables	existing-vpc-ritb-wan	rtts-Dea2H2ede16	Sa 1 Subnet	No	vpc-026bc6B32atd8ba20 existing-vpc			
nternet Gateways	existing-vpc-rtb-ian	rtti-060a2b85568	81 1 Subnet	No	vpc-0280c6832atd8ba20 axisting-vpc			
Egress Only Internet Gateways	Sonic/Wall NSvRoute Table LAN	rtt)-053t99ed41e0	28d 1 Subnet	No	vpc-00cc37c92d905f311 NSV VPC			
DHCP Options Sets								
Elastic IPs								
Endpoints								
Endpoint Services	rtb-0ea9f2ede1645ad25 existing-vp	c-rtb-wan						50
AT Galeways	Summary Routes	Subnet Associations	Route Propagation	Tags				
Peering Connections	Cancel Save							
	View: Al	II rukes						
Security	Destination	Target	Status Propagat	ed Remove				
letwork ACLs	and the second sec	local	Active No					
Security Groups	0.0.0/0	1	NO	0				
PN Connections		kgw-05753b1d95f01fe0	Taninina success					
	Add another route	+02dddc5b1fa57cd62						
ustomer Gateways		The consistence of the	CONTRACTOR					
inual Private Gateways								
PN Connections								
Feedback 😧 Englis	h (US)				© 2008 - 2018. Amazon Web Services. Inc. or its all Miles. All rights reserved.	Privacy Policy	Term	s of Us

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

Deploying AWS from Cloud Template

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

Pre-requisites include:

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

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

Steps:

1 Go to:

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

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

sonicwall-github Upd	ate readme file	Latest commit advacese 24 seconds ago
📾 single-ami	upload launch page and templates first revision	2 minutes ago
README.md	Update readme file	24 seconds ago
III README.md		/
sonicwa	ll-nsv-aws-cf-templates	
SonicWall NSv - A	WS doud formation templates	
https://www.soni	owail.com/	
Deployi	ng	
Marketplac	e deployment	
Find the SonicWa	II NSv product in AWS Marketplace: https://aws.amazon.com/marketp	lace/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 NSv to a new VPC.	
Launch Stack		

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

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

tep 1 specify template	Create stack		
ep 2 secify stack details	Prerequisite - Prepare templ	ate	
ep 3	Prepare template Every stack is based on a template. A templa	te is a JSON or YAML file that contains configuration is	nformation about the AWS resources you want to include in the stack.
onfigure stack options	 Template is ready 	 Use a sample template 	 Create template in Designer
wiew			
	Specify template A template is a JSON or YAML file that descri Template source		
	A template is a JSON or YAML file that descri	3 URL where it will be stored.	Jpload a template file
	A template is a JSON or YAML file that descr Template source Selecting a template generates an Amazon S	3 URL where it will be stored.	Jpload a template file
	A template is a JSON or YAMI, file that descri Template source Selecting a template generates an Amazon 5 O Amazon S3 URL	S URL where it will be stored.	Jpload a template file
	A template is a JSON or VAMI, file that descri Template source Selecting a template generates an Amazon S Amazon S3 URL Amazon S3 URL	S URL where it will be stored.	Jpload a template file

5 Click Next.

ly template	Specify stack details	
: ify stack details	Stack name	
	Stack name	
i gure stack options	SonicWall-NSv	
gene search opposite	Stack name can include letters (A-Z and a-z), numbers (D-9), and dashes (-).	
i W		
	Parameters	
	Parameters are defined in your template and allow you to input custom values when you create or update a stack.	
	Project	
	Project Name	
	This will be in AWS resources tag SonicWall NSv	
	Location	
	Availability Zone Select the AWS Availability Zone	
	instance	
	AMI	
	SonicWall NSV AMI ID	
	Instance Name	
	New KSV Instance Name SonicWall NSV	
	- An institute in Art	
	Instance Type Select the type of instance	
	cs.Large	,
	canage	
	Key Pair	
	Instance Key Pair Name	,
	Allow management (ssh/http://ttps/	

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

- 7 Set the following parameters:
 - Project Name: A name which will be added to the resources tag.
 - Location

Availability Zone: Select the Availability Zone into which NSv is launched.

• Instance

AMI: AMI ID of SonicWall NSv.

Instance Name: A descriptive name for the NSv instance.

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

Key Pair: Select the key pair. This is the key pair available in AWS that can be used to SSH to the SonicWall NSv management console. See:

https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

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

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

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

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

• VPC

VpcId: Select existing VPC to which to deploy NSv.

8 Click Next.

GoudFormation > Stacks > Or	sate chark
Step 1 Specify template	Configure stack options
Sing 2	Tags
Specify stack details	Yoo can specify tago ling-value pairs) to apply to resource in your stack. You can add up to 50 unique tags for each stack. Learn more 😢
Step 3	Key Value Remove
Configure stack options	
Simp 4	Addtag
Review	
	Permissions those as the releasing define how Conditionation can mate, modify, or delete resources in the stack of you don't shows a role. Conditionation can permission
	based in your user instantiali. Learn mere 🕑
	MM role - optional
	Choose the KM role for Cloudformation to use for all operations performed on the stack.
	Advanced options
	You can set additional options for your stack, like notification options and a stack policy. Learn more 💋
	+ Stack salley
	Stark pointy Defines the resources that you want to protect from universe/bonal updates during a stark update.
	Specify alarms for Could'Irmation to monitor when creating and optating the stack. If the operation breaches as alarm threshold, Claudiformation rolls it back. Larm
	Notification options
	Stack creation options
	Carsol Previous Next
	How can set additional options for your stack, like notification options and a stack policy. Learn more (2) • Stack policy infrast the results for your to prace their university of a stack policy. Learn more (2) • Rollback configuration Sumply across for Count from states to prace their university of a stack option. • Notification options • Stack creation options

9 Click Next.

and 1 concilly terreplate	Review SonicWall-NSv		
	Step 1: Specify template		644
ny 3 Secily stack details	Template		
ng) Jerfiger stak splien ne - tenter	Tonycles URL Https://Llawsznawic.com/tex-dh-dox/L exhibing-op.template Statu docretors Genorate Biol.com/templaters Tonyclane to itsplay Mis in an initiang URC Deliverate cost not available		
	Step 2: Specify stack details		. Balt
	Parameters (11)		
	Q, longit provides		Θ
	Key	A Value	
	Acting		
	Availability2one		
	ContropEpAllocations		
	InstanceName	Servictitali NSv	
	instanceType	chiege	
	fayfustiume		
	LantauSubnetil		
	ManagementWhiteliatOdr		
	Maragimentimitiatup		
	ProjectName	SarricHat NSv .	

- 10 Review details and click Create Stack.
- 11 Status changes to **CREATE_COMPLETE**.

Showing 2 stack
C

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

Change Routing Tables for NS_v Access

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

EC2 Dashboard	Launch Instanc	🛛 🤜 Connec	t Actions ~				Z		
Events		and attributes or se					0 K < 1	to 1 of 1 >	
Tags	C Filter by tags	and attributes or se	arch by keyword				e k k i	10 1 01 1 >	21
Reports	Name	- Instance ID	 Instance Type 	e - Availability Zone -	Instance State - Status Checks -	Alarm Status Publ	ic DNS (IPv4)	- IPv4 Pub	blic IP
Limits	SonicWall	ISv i-0c6b32ead	63026d20 c5.large	ap-south-1a	running Ø 2/2 checks	None 🍃		13,232,1	08.24
 INSTANCES 	Concertaint	1000002080	ooozoozo conarge	apoourra	• Torring • 22 Criscos	10000		10.202.1	00.24
Instances									
Launch Templates									
Spot Requests									
Spot Requests Reserved Instances									
Reserved Instances Dedicated Hosts	Instance: 1-0c	ib32ead63026d20	(SonicWall NSv) Elas	itic IP: 13.232.196.249				-	
Reserved Instances Dedicated Hosts	Instance: I-Oct	ib32ead63026d20	(SonicWall NSv) Elas	tic IP: 13.232.198.249					
Reserved Instances Dedicated Hosts IMAGES AMIs	Instance: I-Oct	ib32ead63026d20 Status Checks	(SonicWall NSv) Elas Monitoring Tags	tic IP: 13.232.196.249					
Reserved Instances Dedicated Hosts		Status Checks	Monitoring Tags	tic IP: 13.232.198.249				8	
Reserved Instances Dedicated Hosts IMAGES AMIs				ntic IP: 13.232.198.249	Public DNS (IPv4) IPv4 Public IP				
Reserved Instances Dedicated Hosts IMAGES AMIs Bundle Tasks		Status Checks	Monitoring Tags i-0c6b32ead63026d20	tic IP: 13.232.198.249	Public DNS (IPv4)				
Reserved Instances Dedicated Hosts MAGES AMIs Bundle Tasks ELASTIC BLOCK STORE		Status Checks Instance ID Instance state	Monitoring Tags I-0c6b32ead63026d20 running	tic IP: 13.232.198.249	Public DNS (IPv4) (IPv4 Public IP		h-1.compute.internal		
Reserved Instances Dedicated Hosts MAGES AMIs Bundle Tasks © ELASTIC BLOCK STORE Volumes		Status Checks Instance ID Instance state Instance type	Monitoring Tags i-0c6b32ead63026d20 running c5.large	tic IP: 13.232.196.249	Public DNS (IPv4) IPv4 Public IP IPv6 IPs	13.232.198.249			
Reserved Instances Dedicated Hosts MAGES AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes Snapshots		Status Checks Instance ID Instance state Instance type Elastic IPs	Monitoring Tags i-0c6b32ead63026d20 running c5.large 13.232.198.249*	pWan-7J2P9ASWNK58.	Public DNS (IPv4) IPv4 Public IP IPv6 IPs Private DNS	13.232.198.249 - ip-192-168-0-4.ap-south			
Reserved Instances Dedicated Hosts MAGES AMIs Bundle Tasks ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager	Description	Status Checks Instance ID Instance state Instance type Elastic IPs Availability zone	Monitoring Tags i-0c6b32ead63026d20 running c5.large 13.232.198.249* ap-south-1a SonicWall-NSV-NSVSecGr	pWan-7J2P9ASWNK58.	Public DNS (IPv4) IIPv4 Public IP IPv6 IPa Private DNS Private IPs	13.232.198.249 - ip-192-168-0-4.ap-south	121		
Reserved Instances Dedicated Hosts Dedicated Hosts AMIs Bundie Tasks ELASTIC BLOCK STORE Volumes Snapshots Lifecycle Manager NETWORK & SECURITY	Description	Status Checks Instance ID Instance state Instance type Elastic IPs Availability zone Security groups	Monitoring Tags i-0c6b32ead63026d20 running c5.large 13.282.198.249* ap-south-1a SonicWal-NSV-NSVSecGr view inbound rules, view of	pWan-7J2P9ASWNKS8. outbound rules	Public DNS (IPv4) IIPv4 Public IP IIPv6 IPa Privato DNS Privato IPs Secondary private IPs	13.232.198.249 - ip-192-168-0-4.ap-south 192.168.0.4, 192.168.1.1	121		

- 2 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.

🟮 CloudFormation Manage 🗙	🐠 Problem loading page 🛛 🗙 🧔	3 Management Console X	🥫 Route Tables V	/PC Mane 1	😝 EC2 Management Conso 🗙 🔓 EC2 Management Conso 🗴 🕴 icanhazip.	com/ ×	+	
(←) → 健 @	🛈 🔒 https://ap-south-1.console.	aws.amazon.com/vpc/home	?region-ap-south-1	routetabl	es: 😇 🏠 🔍 Search	7	111	≡
aws Services	👻 Resource Groups 👻 🕏				û smadugula @ 3798-3630-3831	• Mumbhi • S	iupport ·	•
VPC Dashboard Filter by VPC:	Create Route Table Delete Route T	able Set As Main Table				C	0	0
Q Select a VPC	QSearch Route Tables and their X					4 1 to 6 of 6 Route	Tables	2.20
Virtual Private Cloud	Name	Route Table ID	Explicitly Associat -	Main -	VPC ·			
Your VPCs	SonicWall NSvRoute Table WAN	ntb-09bba975786ec	1 Subnet	No	vpc-00cc37c92d605f311 NSv VPC			-
		rtb-0826b63bd5613	0 Subnets	Yes	vpc-026bc6832afd8be20 existing-vpc			
Subnets		rtb-0401b47029ba7	0 Subnets	Yes	vpc-00cc37c92d605f311 NSv VPC			
Route Tables	existing-vpc-rtb-wan	rtb-0ea9f2ede1645a	1 Subnet	No	vpc-026bc6832afd8be20 existing-vpc			
Internet Gateways	existing-vpc-rtb-lan	nb-060a2b8556881	1 Subnet	No	vpc-026bc6832afd9be20 existing-vpc			
Egress Only Internet Gateways	SonicWall NSvRoute Table LAN	ntb-053b9ed4te028d	1 Subnet	No	vpc-00cc37c92d605f311 NSv VPC			
DHCP Options Sets								
Elastic IPs								
Endpoints							_	-
Endpoint Services	rtb-060a2b85568817fec existing-vpc-	rtb-lan						
NAT Gateways	Summary Routes	Subnet Associations Rout	te Propagation	Tags				
Peering Connections	Cancel Save							
	View: All	ules						
Security	Destination Ta	rget	Status Propagated	Remove				
Network ACLs	10.0.0.0/16 loc	al	Active No					
Security Groups		ni-08daf802f01eda6f4	No	0				
VPN Connections		ni-08daf802f01eda6f4 Son	interface listerface I					
Customer Gateways	Add another route	in out to strong out of the strong of the st	icidal internet of	1993				
Virtual Private Gateways								
VPN Connections								
🔍 Feedback 🔇 English	(US)				© 2008 - 2018, Amazon Web Services, Inc. or its affiliates. All rights reser	irved. Privacy Policy	Terms	of Use

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).

	X 🧧 Problem loading page 🛛 🛛	😝 53 Management Conso	le 🗙 🧧 Route	Tables VPC Marrie	× 19 EC2 Management Consol × 19 EC2 Management Consol >	icanhazip.com/ × +
→ C @	🛈 🖨 https://ap-south-1.com	nsole.aws.amazon.com/vpc	/home/region=ap	-south-1#routetal	les: 🖾 🔂 🗌 Q. search	¥ IIV 🖸
aws Service	es 🗸 Resource Groups 🗸 📑				û smadugula ⊗ 37	98-3630-3831 • Mumba • Support •
PC Dashboard	Create Route Table Delete Ro	oute Table Set As Main T	able			2 0 0
Iter by VPC:	QSearch Route Tables and their	×				< 1 to 6 of 6 Route Tables > 3
	Name	 Route Table ID 	- Explicitly As	isociai+ Main +	VPC +	
irtual Private Cloud	SoneWat NSVRoute Table WA	UN mb-0966a0757866	a. 1 Subnet	No	vpc-00cc37c92d605f311 NSv VPC	
ur VPCs		rtb-0826b63bd563	13 0 Subnets	Yes	vpc-026bc6832afd8ba20 existing-vpc	
bnets		mb-0401b47029b	7 0 Subnets	Yes	VDC-00cc:37c82d9055111 NSv VPC	
rute Tables	existing-vpc-rith-wan	rtts-Dea2H2ede164	5a 1 Subnet	No	vpc-026bc6B32atd8be20 existing-vpc	
ernet Gateways-	existing-vpc-ttb-ian	ntb-060a2b855688	11 1 Subnet	NO	vpc-028bc6832afd8be20 existing-vpc	
ress Only Internet Iteways	Sonic/Wall NSvRoute Table LAN	N rtb-053b9ed4fe02	8d 1 Subnet	No	vpc-00cc:37c92d605f311 NSv VPC	
ICP Options Sets						
ISDC IPS						
dooints						
dpoint Services	rtb-0ea9f2ede1645ad25 existing	-vpc-rtb-wan				885
T Galeways	Summary Routes	Subnet Associations	Route Propagati	on Tags		
ring Connections	Cancel Save					
ing connections		c All rukes				
	Destination		1000			
curity	Destination	Target		opagated Remov		
			Active No			
work ACLs	10.0.0/16	local				
work ACLs	10.0.0.016	local	No	0		
work ACLs		local 	No	0		
work ACLs curity Groups IN Connections	0.0.0.0/0	1	No 1 existing-vpc-igw	0		
twork ACLs curity Groups PN Connections stomer Gateways	0.0.0.0/0	l kgw-05759b1d95f01(e07	No 1 existing-vpc-igw	0		
ecurity twork ACLs curity Groups PN Connections stomer Gateways tual Private Gateways N Connections	0.0.0.0/0	l kgw-05759b1d95f01(e07	No 1 existing-vpc-igw	°		
twork ACLs curity Groups PN Connections stomer Gateways tual Private Gateways	0.0.0.0/0	l kgw-05759b1d95f01(e07	No 1 existing-vpc-igw	0		

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

Accessing the SonicWall NS_v Web Interface

To access the SonicWall 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**.

20 E E	O CENTRAL	is and attributes or se	which has been and						
	CL Pritter by the	ps wind attributies or se	ench by keyword						
ots	Name	 Instance ID 	Instance Type	Availability Zone +	Instance State - Status Checks	 Alarm Stat 	tus Public DNS (IPv4)	 IPv4 Public IP 	IPv6-IPs - Key Name
5		i-01e	t2 micro	us-east-2a	stopped	None			
NCES		H026	c4 large	us-east-2a	e stopped	Norse		and the second second	x
	1 0	1-031	12 micro	un-east-2a	stopped	None	2		
Templates	(1) and	i-044	t2.micro	up-east-2a	e stopped	None	1 ec2-		-
equests	() emm	1-005	t2 medium	us-east-2a	e stopped	Norie	>	1.42	
ed Instances		1-08a	12 micro	us-east-2c	e stopped	None	>		
ted Hosts	10 1000	1-08e	12 micra	us-east-2a	sloppet	None	5		
		i-de 10	t2 micro	us-east-2a	Stoped	None	5		- 4
		HOWST	t2 micro	us-east-2b	e stopped	None			
Tasks	819	Hosti	c4 large	us-east-2a	running Ø 2/2 checks passed	Ano 7	5		
es hots	Instance: 1-0	al)	(R19) Private IP: 1	0.111				Interface ID VPC ID	vpc-0ta
	Description	Status Checks	Monitoring Tags					Attachment Owner Attachment Status	37/10 altached
	Treesesterio	L million service and							
ΠΥ	1.000000000000	Instance ID	i-0a0				Public DNS (IPv4)	Attachment Time Delete on Terminate	false
ITY ly Groups	1.000	Instance state	running				IPv4 Public IP		
STOC 8. TTY ty Groups TPs nent Groups	3.00004000							Delete on Terminate Private IP Address Private DNS Name	false
rrγ γ Groups IPs tent Groups	1	Instance state Instance type	running				IPv4 Public IP IPv6 IPs	Delete on Terminale Private IP Address Private DNS Name Public IP Address	faite 10
try ly Groups IPs nent Groups iks	1	Instance state Instance type Elastic IPs	running c4.targe		view inbound rules , view outbound		IPv4 Public IP IPv6 IPs Private DNS	Delete on Terminale Private IP Address Private DNS Name Public IP Address Source/Dest. Check Description	faloe 10 - - faloe -
try ty Groups :IPs nent Groups aks ak Interfaces SALANCTING		Instance state Instance type Elastic IPs Availability zone Security groups Scheduled events	numing c4.large us-east-2a r15iii 2onic nakes No scheduled events		view inbound rules. view outbound		IPv4 Public IP IPv6 IPs Private DNS Private IPs Secondary private IPs VPC ID	Delete on Terminale Private IP Address Private DNS Name Public IP Address Source/Dest. Check	fabe 10 - - fabe -
ITY IV Groups IPs ment Groups aks aks rk Interfaces BALANCING Jalancers		Instance state Instance type Elastic IPs Availability zone Security groups Scheduled events AMI ID	numing c4.large us-east-2s rutis bonic' rutis No scheduled events R19: (um-0		view inbound rules, were outbound		IPv4 Public IP IPv5 IPs Private DNS Private IPs Secondary private IPs VPC ID Subnet ID	Delete on Terminate Private IP Address Private DNS Name Public IP Address SourceDest Check Description Security Groups	fabe 10 - fabe - r19
rry y Groups IPs eant Groups iks ik Interfaces ikunicting ielancers		Instance state Instance type Elastic IPs Availability zone Security groups Scheduled events	numing c4.large us-east-2a r15iii 2onic nakes No scheduled events		view inbound rules. Year outbound		IPv4 Public IP IPv6 IPs Private DNS Private IPs Secondary private IPs VPC ID	Delete on Terminate Phinate IP Address Phinate DNS Name Public IP Address Source/Dest Check Description Security Groups	fabe 10 - fabe - r19
ITY ty Groups IPs]	Instance state Instance type Elastic IPs Availability zone Security groups Scheduled events AMI ID	numing c4.large us-east-2s rutis bonic' rutis No scheduled events R19: (um-0		View inbound rules. View authound		IPv4 Public IP IPv5 IPs Private DNS Private IPs Secondary private IPs VPC ID Subnet ID	Delete on Terminate Private IP Address Private DNS Name Public IP Address SourceDest Check Description Security Groups	10 - fabre - r19

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

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

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

EC2 Dashboard	Allocate new addr	Actions *								
Events Tags	Q. Filter by tags an	d altributes or search b	v kavent							
Reports	Name	 Elestic IP 	- Allocation ED	- Instance	- Private IP address -	Scope	- Association ID -	Network Interfa	ce ID	Network Interface Owner
Limits	N	13.58	epalocia?		10 8	VDC	espannos-04	erti-Dec.		37
# INSTANCES	•2	13.50 10000	eipatioc-63mmm	- Delta	se addresses	Vpc		+		-
Instances		52.	espalac-d4		ima address	3	elpassoc-a7	mite		77
Launch Templates		52	elpahoc-98		in class address	vpc				
Spot Requests		52.	etpalloc-f9	HU2n AddE	dit Tago 1.5	vpc	elpatroc-22	en-to a		37
Reserved Instances Dedicated Hosta										
E INAGES										
AMs.										
Bundle Tasks										
ELASTIC BLOOK										
Volumes										
Snapshots										
Automatic A										
In SECURITY										
Security Groups	-									
Elastic IPs	1									
Placement Groups										
Key Pairs										
Network Interfaces										
E LOAD BALANCING	4									
Load Balancers	Address: 13.59.127	241								
Target Groups	Description	Tago								
⊛ AUTO SCALING										
Launch Configurations			9.					Allocation ID	eipelloc-63	
Auto Scaling Groups		Instance - Scope vpc					4	Association ID		
E SYSTEMS HAMAGER	Network in	Public DNS -					Net	work interface ID		

- 2 Select an IP address that is "free", or if no addresses are available, then click the **Allocate new address** button at the top of the screen.
- 3 Right-click on the address row and select **Associate Address** from the right-click menu. The **Associate address** screen is displayed.

elect the instance OR network interface	to which you want to associate this	Elastic IP address (13.59	1)	
Resource type	 Instance Network interface 	1		
Network interface	eni-06a	• C		
Private IP	Select a private IP	- C 0	0	
Reassociation	Allow Elastic IP to be reasso	clated if already attached 0		
	ddress with your instance, your cu	rrent public IP address is released	f. Learn more.	
AWS Command Line Interface comm	nand			

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

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

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

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

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

r i	SONICMALL	
	Network Security Virtual	
	admin Password	
	LOG IN	

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

Configuring Internet/Public Access Through the NS_v

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

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

To locate the ENI:

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

aws servic	ces ⊮ Re	esource Groups	~ %										4	Shane O'Hanlon *	Ohio *
EC2 Dashboard	Launch	Instance 💌	Connect Act	tions *											
Tags	Q, File	er by tags and attrib	des or search by k	nyword										0	К. С.
Reports		ame - In	stance ID	Instance Type -	Availability Zone -	Instance State ~	Status Checks	~ AJ	Jarm Status	Public DNS (IPv4)	 IPv4 Public IP 	IPv6 IPs	- Key Name	- Monitoring	- Laun
	50	ohtestpc H0	036	t2.micro	us-east-2a	running	2/2 checks passed	N	one	>	52.		1000	disabled	Augur
STANCES	1 I II	sasoniccore i-0	214	o&large	us-east-2a	stopped		N	one	2				disabled	July
istances	-	i-0	3642	t2.micro	us-east-2a	stopped		No	bre	>			1000	disabled	July 1
runch Templates	50	e-demoserv i-0	441	t2.micro	us-east-2a	stopped		N	one	ec2-52-	52			. disabled	July
ot Requests		HO	667	t2.micro	us-east-2c	stopped		N	one	>			1000	disabled	Febr
eserved instances	VP	so-nat i-0	Ord	12.micro	us-east-2a	stopped		N	one	>				disabled	May
edicated Hosts	50	-demoserv i-0	a16	t2.micro	us-east-2a	stopped		A 10	one	>				. disabled	July
AGES	R1	196 i i i	ocf.	c5.large	us-east-2a	running	Ø 2/2 checks passed		210 2		13.59 1		2000	disabled	Augu
lis															
ORE															
LASTIC BLOCK TORE Islumes inapshots	< Instance	i: i-Oacff	(R19:	a) Elastic IP: 13	.59. 1			_			Network Interface eth2		~		
rore slumes napshots ETWORK & SCURITY	Instance	-			.59. 1			_			Intertace ID		_	4	
ORE slumes sepshots ETWORK & cultury scurity Groups		ption Status	Checks Monit	oring Tags	.59							vpc 0ba996	_	4	
ORE Aumes appshots ETWORK & ECURTY ACURTY ACURTY ACURTS AUTORNAL ACURTS	Instance	iption Status Inst	Checks Monit		.59. 1					Public DNS (IPv4)	Intertace ID VPC ID	vpc-0ba996 371	_	4	
ORE Aumes apshots TWORK & CURTY curfty Groups astic IPs acement Groups	Instance	iption Status I Inst Instan	Checks Monit ance ID i-Dectil ce state running	oring Tags	<u>.59. 1</u>					Public DNS ((Pv4) (Pv4 Public IP (Pv4 Ps	Interface ID VPC ID Attachment Owner Attachment Status Attachment Time	vpc 0ba999 3/1 attached Mon Aug 13 10	0.05.28 GMT+100 2018	4	
ORE fumes apshots TWORK 6. CLIRITY curity Groups table IPa sceneet Groups y Pales	Instance	iption Status I Insta Instan	Checks Monit	oring Tags	<u>39. 1</u>					IPv4 Public IP	Interface ID VPC ID Attachment Owna Attachment Status Attachment Time Delete on Terminale	vpc 0ba996 371 alfached Mon Aug 13 10 Inw	0 05 28 GMT+109 2018	4	
COLE Aumes appshots EnviOKK & CLURETY ACUITY Stoups astic IPs acement Groups by Pales	Instance	iption Status I Insta Instan	Checks Monit ance ID Headfi ce state running roe type c5 large satic IPs 13 50	oring Tags	.59. 1					IPv4 Public IP IPv6 IPs	Interface ID VPC ID Attachment Owner Attachment Status Attachment Time	vpc-0ba995 371 alfached Mon Aug 13 10 Inae 10.95 5	0105.28 GMT+100 2018	4	
rone slumes nepshots Erwörks & custry Groups lastic IPs lastic IPs lascement Groups by Pairs etwark Interfaces	Instance	iption Status I Inst Instan Instan Instan Eli Availabi	Checks Monit ance ID i-Decti ce state running roe type c5 large istic IPs 13.59. ity zone us-east groups r190	oring Tags 7' 2a SonicSgingressPac	.59. 1	5. vie	n inbound rules, view			IPv4 Public IP IPv6 IPs Private DNS	Intertaco IC VPC IC Attachment Status Attachment Status Datete on Terminate Private IP Address	vpc 0bu996 371 attached Mon Aug 13 10 Irun 10.99 5	01528 CMT+100 2018	4	
IONE interest interfaces into BALANCING	Instance	iption Status Instan Instan Instan Ex Availabi Security	Checks Moniti anos ID i-Dectfil ce state state type c5 large state IPs 13.50 IV zone groups r190 ccbout	aring Tags Tags 2a 		5. viev	n Inbound rules. Hew			IPv4 Public IP IPv6 IPs Private DNS Private IPs Secondary private IPs	Intertacin IIO VPC-IIO Attachment Sonie Attachment Taine Deletie as Terminale Prindie IP Address Prindie DHS Name Preide IP Address Source/Dest. Check	vpc 0ba996 371 attached Mon Aug 13 10 true 10.99 5 - - 5 5	0.05528 GMT+100 2018	4	
CONE skarnes skarnes skarnes ETWORK & ETWORK & ETWORK & scarnert Groups association py Paks stowark Interfaces shor PauLancing and Balancers	Instance	iption Status Instan Instan Instan Ex Availabi Security	Checks Monitoria Monitoria Monitoria Checks Monitoria Monitoria Monitoria Monitoria Monitoria Monitoria Monitoria Monitoria Calendaria Monitoria M	Tags Tags T [*] Za Sonic9gingressPac dukes eduled events			ribbund rules, view			IPv4 Public IP IPv6 IPs Private DNS Private IPs	Interface ID VPC ID Attachmert Owne Attachmert Statu Attachmert Time Delete en Termanal Pinde IP Address Pinde IP Address Source/Des LP Address Source/Des LP Address Description	vpc 00a995 371 attached Mon Aug 13 10 true 10.99 5 - 5 faise -		4	
ONE Annes Annes EnvOHX & CLURTY CLURTY Associated Second able Second Sec	Instance	iption Status I Instan Instan Instan Ex Availabi Security Scheduler	Checks Monitoria Monitoria Monitoria Checks Monitoria Monitoria Monitoria Monitoria Monitoria Monitoria Monitoria Monitoria Calendaria Monitoria M	Tags Tags T [*] Za Sonic9gingressPac dukes eduled events	sMgn024p1m88ia-		r indourd rules. Hew			IPv4 Public IP IPv6 IPs Private DNS Private IPs Secondary private IPs VPC ID	Interface ID VPC ID Attachmert Owne Attachmert Statu Attachmert Time Delete en Termanal Pinde IP Address Pinde IP Address Source/Des LP Address Source/Des LP Address Description	vpc 00a995 371 attached Mon Aug 13 10 true 10.99 5 - 5 faise -	00528 CMT+100 2018	4 ptrability	
ICONE SAMPARES CONTRACTORS CON	Instance	iption Status I Instan Instan Instan Ex Availabi Security Scheduler	Checks Monit ance ID i-Decfi costate satisfies 13.50 ly zone us-east rigit groups rigit events No sch- AMI ID Senich	Tags Tags T [*] Za Sonic9gingressPac dukes eduled events	sMgn024p1m88ia-		nitoond rubes, view			IPv4 Public IP IPv5 IPs Private DNS Private IPs Secondary private IPs VPC ID Submit ID	Interface ID VPC ID Attachmert Owne Attachmert Statu Attachmert Time Delete en Termanal Pinde IP Address Pinde IP Address Source/Des LP Address Source/Des LP Address Description	vpc 00a995 371 attached Mon Aug 13 10 true 10.99 5 - 5 faise -		4 stn380-	
IONE SAMMENTS AND	Instance	ption Status I Inst Instan Instan Bi Availubi Security Scheduler	Checks Monit ance ID i-Decti custate custate static IPs 13.50 ity zone groups r100 custoan events No sch AMI ID SenicW Pattern -	Tags Tags T [*] Za Sonic9gingressPac dukes eduled events	sMgn024p1m88ia-		nitiound rules, view			PA4 Public IP IPA5 IP5 Private DNS Private IP5 Secondary private IP5 VPC ID Submit ID Network phortacos	Interface IC VPC IC Adlachment Come Atlachment States Adlachment States Adlachment States Private IP Address Private IP Address Security Group: Security Group:	vpc 00a995 371 attached Mon Aug 13 10 true 10.99 5 - 5 faise -		4 stn386-	
TORE	Instance	Status I Insta Insta Avaitabi Secunty	Checks Monit ance ID i-Decfi costate satisfies 13.50 ly zone us-east rigit groups rigit events No sch- AMI ID Senich	Tags Tags T SancGgingrosPas drukes duked events ed_NSV_AVAS_R196 (sMgn024p1m88ia-		e Hourd rules. Here			PA4 Public IP IPA5 IP5 Private DNS Private IP5 Secondary private IP5 VPC ID Submit ID Network phortacos	Interface ID VPC ID Attachmert Owne Attachmert Statu Attachmert Time Delete en Termanal Pinde IP Address Pinde IP Address Source/Des LP Address Source/Des LP Address Description	vpc 00a995 371 attached Mon Aug 13 10 true 10.99 5 - 5 faise -		4 sins86	
TONE Vikamas kapshots Envotice 6. Ecustry Exactly Groups lacement Groups gr Pats Heavent Interfaces OAD BILANCOM Gal Bilancers arget Groups TO SCALING Galphatanes	Instance	Status I Insta Insta Avaitabi Secunty	Checks Monit anno ID -Oschi ce state state ci large stic IPs 13.50 us-east r100 schour events No schour events Sonow Nationer - AM role -	Tags Tags T SancGgingrosPas drukes duked events ed_NSV_AVAS_R196 (sMgn024p1m88ia-		nitioand rules, view		3	Pr4 Public IP IPv5 IPs Private IPs Private IPs Secondary private IPs Secondary private IPs Network pre-tase Network pre-tase T-Cutember	Interface IC VPC IC Adlachment Come Atlachment States Adlachment States Adlachment States Private IP Address Private IP Address Security Group: Security Group:	vpc 00a995 371 attached Mon Aug 13 10 true 10.99 5 - 5 faise -		4	

- 2 In the top pane, select the NSv instance.
- 3 In the lower pane, click on **eth0** to display the **Network Interface eth0** popup.
- 4 Copy the Interface ID from the popup. This is the X1 ENI.
- 5 Paste the value into a temporary file, so you can refer to it during the next procedure.

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

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

EC2 Dashboard	Rocate new address Actions *	
Events Tags	Q. Filter by lags and altributes or search by keyword	
Reports	Name - Elastic IP - Allocation ID - Instance - Private IP address - Scope - Association ID - Network Interfa	ce 10 ~
Làmha	13.56 epaloc - 10.99 vpc eipatoc emile	
■ INSTANCES		
Instances	52.14 epatoc +0441 10.0 vpc eparatoc enide	
Launch Templates	52 14 epetoc 10.00 10.00 vpc eigestoc enid5e	- 1
Spot Requests	52.15.17 epalloc-19 · · · Release addresses	7 2
Reserved Instances Dedicated Hosts	Attracture address	~
⊕ THAGES	AddEdR Top	
AMIs		
Bundle Tasks		
B BLASTIC BLOCK		
Volumes		
Snapshots		
B SECURITY		
Security Groups		
Elastic IPs		
Placement Group		
Key Pairs		
Network Interfaces	ddress: 52 15	
B LOAD BALANCING		
Load Balancers	Description Tags	
Target Groups	Elestic IP 52.15 Allocation ID exator 9	
@ AUTO SCALING	Ensue * 2010 Anocation to Espace *	
Launch	Scope vpc Association ID -	
Configurations	Public DNS - Network interface ID -	
Auto Scaling Groups	Network interface owner -	
SYSTEMS MANAGER		

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

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

elect the instance OR network interface	which you want to associate this Elastic IP address (13.59.		
Resource type	Instance Network interface		
Network interface	eni-06a C 2	(
Private IP	Select a private IP C		
Reassociation	Allow Elastic IP to be reassociated if already attached		
Warning If you associate an Elastic IP a	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 list, select the ENI of the X1 interface that you located in the previous procedure.
- 6 Click Associate.

Troubleshooting Installation Configuration

If the NSv fails to come up, follow the instruction in Navigating the NSv Management Console on page 50 to go to the NSv Management Console window or the SonicOS CLI window. Check the boot messages:

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

Insufficient Memory Assignment

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

SonicOS boot message:

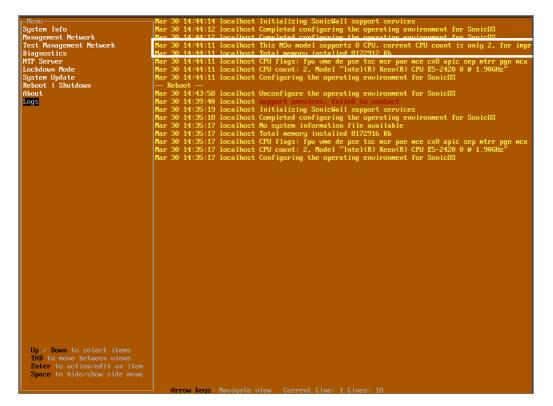
Insufficient memory 4 GB, minimum memory required 10 GB for NSv model: "NSv 800 Beta" Power off the Network Security virtual appliance and assign 10 GB to this virtual appliance.

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

-Menu-	¬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 15:10:07 localhost Total memory installed 4160884 Kb
NTP Server	Mar 30 15:10:07 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
Lockdown Mode	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 Configuring the operating environment for SonicDS
Reboot Shutdown	Reboot
About	Mar 30 15:06:37 localhost Initializing SonicWall support services
Logs	Mar 30 15:06:36 localhost Completed configuring the operating environment for SonicOS
	Mar 30 15:06:06 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
	Mar 30 15:06:05 localhost Total memory installed 4160884 Kb
	Mar 30 15:06:05 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
	Mar 30 15:06:05 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
	Mar 30 15:06:05 localhost Configuring the operating environment for SonicOS
	Reboot
	Mar 30 15:05:51 localhost Unconfigure the operating environment for SonicOS
	Mar 30 15:02:31 localhost Initializing SonicWall support services
	Mar 30 15:02:31 localhost Completed configuring the operating environment for SonicOS
	Mar 30 15:02:01 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
	Mar 30 15:02:01 localhost Total memory installed 4160884 Kb
	Mar 30 15:02:00 localhost CPU flags: fpu 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 Insufficient memory 4 GB, minimum memory required 8 GB.
	Mar 30 14:59:24 localhost Total memory installed 4160884 Kb
	Mar 30 14:59:24 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
	Mar 30 14:59:24 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
	Mar 30 14:59:24 localhost Configuring the operating environment for SonicOS
	Reboot
	Mar 30 14:59:11 localhost Unconfigure the operating environment for SonicOS
	Mar 30 14:54:57 localhost Initializing SonicWall support services
	Mar 30 14:54:56 localhost Completed configuring the operating environment for SonicOS
	Mar 30 14:54:26 localhost Insufficient memory 4 GB, minimum memory required 8 GB.
	Mar 30 14:54:26 localhost Total memory installed 4160884 Kb
	Mar 30 14:54:26 localhost CPU flags: fpu une de pse tse 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
	Mar 30 14:47:18 localhost Initializing SonicWall support services

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

Memory may be insufficient without a insufficient memory log entry:



Incompatible CPU

If the CPU does not support AES instructions the following message will appear:

CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz is not supported by SonicWall Network Security Virtual CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does not support the Advanced Encryption Standard(AES) instructions

Refer to Getting Started Guide and install the SonicWall Network Virtual on a supported platform

The message can also be seen in the logs provided by the management console:

Menu	אר 30 16:56:01 localhost Initializing SonicWall support services
System Info	Mar 30 16:56:00 localhost Completed configuring the operating environment for SonicOS
Management Network	Mar 30 16:56:00 localhost This NSu model supports 8 CPU, current CPU count is only 2, for impr
Test Management Network	Mar 30 16:56:00 localhost Total memory installed 8099184 Kb
Diagnostics	Mar 30 16:55:15 localhost CPU model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does not support
NTP Server	Mar 30 16:55:15 localhost CPU model Intel(R) Xeom(R) CPU E5-2420 0 @ 1.90GHz does not support
Lockdown Mode	Mar 30 16:55:15 localhost CPU flags: fou ume de use tsc msr pae mce cx8 apic sep mtrr pge mca
System Update	Mar 30 16:55:15 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Reboot Shutdown	Mar 30 16:55:15 localhost Configuring the operating environment for SonicOS
About	Reboot
Logs	Mar 30 16:55:01 localhost Unconfigure the operating environment for SonicOS
	Mar 30 16:50:29 localhost Initializing SonicWall support services Mar 30 15:20:32 localhost This NSv model supports 8 CPU, current CPU count is only 2, for impr
	Mar 30 15:20:32 localhost Total memory installed 8099184 Kb
Up / Down to select items	Mar 30 15:20:32 localhost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca
TAB to move between views	Mar 30 15:20:32 localhost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz"
Enter to action/edit an item	Mar 30 15:20:31 localhost Configuring the operating environment for SonicOS
Space to hide/show side menu	Reboot
	Mar 30 15:10:39 localhost Initializing SonicWall support services

If the CPU does not support SSE 4.1 or 4.2 instructions the following message will appear:

CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz is not supported by SonicWall Network Security Virtual CPU Model Intel(R) Xeon(R) CPU E5-2420 0 @ 1.90GHz does support SSE 4.1 or 4.2 instructions

Refer to Getting Started Guide and install the SonicWall Network Virtual on a supported platform

Incorrect CPU Configuration

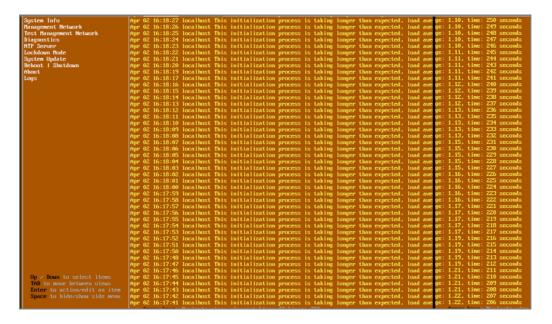
All cores must be on the same socket. Customer needs to change the CPU configuration in settings.

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

Insufficient Resources at Time of Configuration

If the infrastructure where the NSv is being installed has poor performance the following message may appear at time of installation:

If the above message occurs during initialization, more information is available in the logs:



Deployment Options

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

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

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

Topics:

- Deploying the NSv as PAYG
- Deploying the NSv as BYOL

Deploying the NS_v as PAYG

This section presents the steps to complete deployment of a PAYG or "Pay as you go" NSv instance.

SONICWALL	By: SonicWall The SonicWall No	Latest Version: 6.5.0.2-8v atwork Security virtual (NSv all capabilities such as appl	37-496) firewall series brings		Continue to Subscribe Save to List Typical Total Price \$0.655/hr Total pricing per instance for services heated on CLarge in US Sate (M. Virginia), View Details
next-generation firewall control, real-time monito threat protection (ATP), V your AWS environment. I networking features in S patented Reassembly-Fir award-winning Capture A (RTDMI) for advanced the (RTDMI) for advanced the Centrally manage all you (CSC) to maintain consist environments. The solution meet compliance standar Note: SonicWall supports including models from O Barracuda Networks, Che Citrix Systems, Hewlett P	rity virtual (NSv) fire (NGFW) capabilities ring, IPS, TLS/SSL d (IPA and network see (Sv virtual firewalis) (Sv v	Pricing wall series brings industry such as application intellige ecryption and inspection, a gmentation capabilities to support the same security a FW appliances including or suction (RFDPI) technology a al-Time Deep Memory insp al-Time Deep Memory insp sonicWall Capture Security across cloud and on-premi ent security best practices in center and cloud solution to Networks, Sophos, Wab you, McAfae, Huawei, Forcer swan, pfSense, Vyatta, plu 1/2, AES 256/128, SHA1, 1	Ince and Hightham of the section of	Support shights Vext-generation security for p and resources; Gain complete anvironment for threat preven iccurity zoning and ensure app bolicies Defend against zero-day vulne capture ATP; Prevent any servi firtual ecosystem; Gain central with single-pane-of-glass man ncrease agility and scalability mpact; improve security gover sist management Use Casse: Internet gateway for protection; Lateral protection to-Site VPH deployment; Secu- access; Multi-cloud secure com	visibility into your virtual tion; Implement proper arapriate placement of rabilities with SonicWall loc disruption in the lized control and visibility agement via the CSC; without performance mance, compliance and or ingress/egress traffic of east-west traffic; Site- re end-to-end remote

To complete deployment:

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

Your SonicWall NSv series firewall is now enabled.

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

- It allows you send diagnostics from you firewall directly to SonicWall Technical Support.
- It supports easy initiation of support cases online. See:
 - https://www.sonicwall.com/support/knowledge-base/?sol_id=170814110235888
- 2 Take the following steps to link your virtual firewall to MySonicWall:
 - a Login into the NS ν (see Step 1), and copy the Assign Token.

SONIC	Network Security Virtual	MONITOR INVESTIGATE MANAGE QUICK CONFIGURA	TION
Dashboard	Log messages canno	be sent because you have not specified an outbound SMTP server address.	
Event Summaries	 Cloud backup not ena 	bled - Click here to enable.	
Threat Protection			
Capture ATP			
Appliance Health	System Informa	tion	Show Multi-Core Monitor
Overview	Model:	NSv 200 (AWS PAYG) (AGSS)	
Live Monitor	Product Code:	74002	
Bandwidth Monitor	GUID:	EC290D39-3C02-D337-0665-88F3695430EF	
Protocol Monitor	Serial Number:	004010366970	
Current Status	Authentication Code:	UJ4Z-KL3Z	
System Status	Firmware Version:	SonicOS Enhanced 6.5.0.2-8v-37-496-64c9fdc3	
User Sessions	Safemode Version:	SafeMode 6.5.0.0	
VoIP Call Status	ROM Version:	SonicROM 5.0.0.0	
	CPUs:	3.10% - 6.00 GHz (2 x 2999 MHz Intel(R) Xeon(R) Platinum 8124M CPU @ 3.00GHz)	
	Total Memory:	4 GB RAM	
	System Time:	07/04/2019 07:33:16	
	Up Time:	0 Days 00:02:09	
	Connections:	Peak: 19 Current: 19 Max: 125000 🕐	
	Connection Usage:	0.015%	
	Last Modified By:	Unmodified since reboot	
	Assign Token:	fkgQp5vD	

b Login into MySonicWall and go to My Products:

	Μ		ducts						Classic mode 🔯 🕇	8 0 m (
 Polut Margenert Mr Poluth 	\$ /	Product Man	agement			(QUACK REGISTER [NyOyf-C]		ECENTER Registering multip	s + · c c
 My Promotions 		HELEANS CF.	PRENERY MARK	VIEW MARKET	PRODUCT TVP	INCOMEND ON	TERMAN NAME	FEMALE V	Saman	
 Free Trial Software Catalog 	1	ACIM	50R8CW/NLL NS+ 200 AN75 PM/5	00400000000	SOMECHINAL INST 200 ANYS PRIMS	Art 04 2019	senicual Protects	6502	M-04 2025	_
 My Groups 	2	ACINE	SCHRCHARLE HER 200 ARES PAIRS	00400000007	SCHRONINUL INS., 300 ABYS PHINS	Jul 04 2019	senioreal Products	4542	M-04 2025	
My Orders My Outle		ACTIVE	Cipture Clear Tanant - sonicisal Products	00000012000	Capitaro Client Tenant	Arr/10 2015	series all Products			
My Automoreals		ACTM	dame-mails	00401000000	SCHRONINAL INS., 200-2025 PROS	Art 03 2019	seriosal Protects	6502	M 10 2025	
Perspend Service Cotermination	5	ACIME	SCHIECHARLE NEW 200 ANYS PAUS	004000000088	SCHRONALLINE, 300 AMS PRIME	Art13 2019	surveyal Products	6502	M-03-2025	
		ACINE	SCHIECHAREL NEW 200 ANYS PHONE	00400000000	SCHECKING, HE, 300 ANYS PROFE	Art 03 2009	sanicural Products	6502	M-02-2025	
Seports	7	ACINE	10V autocomptor	004030343309	Web Application Firewall	Feb 27 2019	sanicoull Products	2283	Apr 33 2022	
15		ACIME	HyperV-064010053EDA	004090953EDA	SONICHINAL INS., 200 Physiol/	Dec 17 2018	serieval Protects	6502	Dec 17 2013	
D Task		ACINE	HSv anere 0040103338A	00401003184	SCHRCHINUL INS, 200 Asset	Oct 15 2018	senicoul Probats	6562	Oct 15 2019	

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



d Enter a friendly name:

SONICWALL		4ySonicWa	a								Cum main (0 12 9
😧 taraan		y Pro	oducts				o	CIRCK HEGGENTH	No(ph/0		Approving working frequency
- Nyfretett	141	à. T									6.4
- Ny Version - Tex Lat (Alexa)		HOLIDHE ER.	(MORY NAM	127846	100000 PRODUCT (WE		eacure or .	TENNATIANA		TREAMING OF	SPIOIT
- Doing	. 1	ACIME	SCHICKHEL HON 300 ANTS PROF.	in a second	1014C304L115_030	ANSPAS A	4 (H 3113	sand and Posts		65.63	M-04 3023
- Hy2mm		ACTION	STREETWICH HIGH STREAMING MINUTE	-	STRENGLE IN., 190	ANTERNAL A		control Prater	•	4583	Note that the second
 Helpines Helpines 	- 3	ACTIVE	Capture Oliver Tenant - send, and Photosic		REGISTER A PRODUCT			- 25	<i>i</i> .		
- Ny Automatik	- 14	ACTIV	nen rall	-				-		6583	winters.
- Peoperal - Server Coloreration		ACENT	SCHRONNEL HOU DOE ANTO PAND	-	Exter details below to complete impistration of the follows	ng product		**	-	85.63	64.03.3698
And the standard st			Interesting ten and everyteen	-	Serial mandeer	004010396879		1 8	•	8343	1400.00%
	×.	ACTA	WW astancespite	-	Friendly name	PAYO-example-NS-		i -		1283	Aut 31 2022
Littles.		actor	Harry Managements	-	Authentication code	Q4513r		1		8563	flue 17.000
P		ACTIVE	Mir anet MillSUBJURA	-				. 8		6587	Get 13:2018
· · ·	38	ACTION	10%-48-0000752308	and the second	Senant Name	seriewal Products				\$503-bross	Navies asian
	- 15	ACTIVE	INTE- OD-OD DOLONDA	2002	Assign Token	10205-0		1	2	4582	Dei 80 3929
 Hybridit Hybridit 		ACTIVE	HS- 48-8887943300	-		Cevel	Angel	-		1552	10x1104.0002
- Kennedig Facual	10	ACINE	HEAR ADDRESS OF DAL ANYS	-				-		4543	3ag 23 2023
- Separa - Beschapen		ACTIM	His membranty	-	ALCON NEWSFILL INC.		for 15 JULU	united Posts		8575	Nar 61. 2011
- Malaning - Malaning	0	ACTIN		-	uners unerstand of the second		100 ED 2010	named Product	*		Tel: 53 2019

e Select a data center:

				QL	JICK REGISTER fkqQp5vD
	SERIAL NUMBER	PRODUCT TYP	Έ	REGISTERED ON	TENANT NAME
	00401036696E	SONICWALL	IS _V 200 AWS PAYG	Jul 04 2019	sonicwall Products
	00401036696F	SONICWALL	IS _V 200 AWS PAYG	Jul 04 2019	sonicwall Products
oducts	CC0000012081	Capture Client	Tenant	Jul 03 2019	sonicwall Products
	00401036696D	SONICWALL	IS _V 200 AWS PAYG	Jul 03 2019	sonicwall Products
	004010355050 SELECT A DATA CENTER	CONICIMALLA	C 200 AMC DAVC	×	sonicwall Products
	0040103			^	sonicwall Products
	0040103 Da	ata Center Location	Select	•	sonicwall Products
	0040103		Europe		sonicwall Products
	0040103		North America		sonicwall Products
	0040103				sonicwall Products
	00401035088A	SONICWALL	IS _V 800	Oct 05 2018	sonicwall Products
	00401034E05D	SONICWALL	IS _V 400	Oct 04 2018	sonicwall Products
	004010352F0A	SONICWALL	IS _V 200 AWS	Sep 29 2018	sonicwall Products
	00401034A579	SONICWALL	IS _V 800	Mar 05 2018	sonicwall Products
	00401034A4F1	SONICWALL	IS _V 800	Feb 13 2018	sonicwall Products
	00401034A501	SONICWALL	IS _V 800	Feb 13 2018	sonicwall Products

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

SONICWALL'	MySonicW My Pro Product Mai	oducts			94
- My Products	φQ				
 My Promotions 					
 Free Trial Software 	# RELEASE ST.	FRIENDLY NAME	SERIAL NUMBER	PRODUCT TYPE	REGISTERED ON
- Catalog	1 ACTIVE	PAYG-example-NSv	004010366970	SONICWALL NS _V 200 AWS PAYS	Jul 04 2019
 My Groups 	2 ACTIVE	SONICWALL NSV 200 AWS PAYG	00401036696E	SONICWALL NS _V 200 AWS PAYS	Jul 04 2019
 My Orders 	3 ACTIVE	SONICWALLINSV 200 AWS PAVG	00401036696F		Jul 04 2019
 My Quote 	3 ALTIVE	SUNIC WALL NSV 200 AVVS PARG	00401030030+	SONICWALL NS _V 200 AWS PAYG	Jul 04 2019
 My Autorenewals 	4 ACTIVE	Capture Client Tenant - sonicwall Products	CC0000012081	Capture Client Tenant	Jul 03 2019
Flexspend Service Cotermination	5 ACTIVE	demo-mallik	00401036696D	SONICWALL NS _V 200 AWS PAYS	Jul 03 2019

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

Deploying the NS_v as BYOL

This section presents steps to complete deployment when the NSv is setup BYOL, or "Bring Your Own License."

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

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

To link your NSv to MySonicWall:

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

SONIC WALL	Network Security Virtual	MONITOR INVESTIGATE MANAGE		Register Help Logout
				Mode: Configuration >
Current Status System Status		not be sent because you have not specified an outbound	SMTP server address.	
 User Sessions 	(i) Cloud backup not	enabled - Click here to enable.		
	System Inform	show Multi-Core Monitor	Security Services	Show All License Information
	Model:	NSv Unlicensed	Nodes/Users:	10 Nodes (0 in use)
	Product Code:	70000	SSL VPN Nodes/Users:	2 Nodes (0 in use)
	GUID:	AND RECEIPTING AND AND AND READING	Your SonicWall is not registered.	
	Firmware Version:	SonicOS Enhanced 6.5.0.2-8v-sonicosv-374cf82cf8	Click here to Register your SonicWall.	

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

NOTE: To create an accou	nt, refer to Creating a MySonic\	Nall Account on page 41.
--------------------------	----------------------------------	--------------------------

SONIC WALL " Ne	twork Security Virtual	MONITOR	INVESTIGATE	MANAGE
Current Status System Status User Sessions	MySonicWall username Password	e/email		
	Forgot your Username Create MySonicWall ac	_		

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

Serial Number
Authentication Code
Friendly Name
SUBMIT

- 5 Type a descriptive name for the NSv into the **Friendly Name** field.
- 6 Click SUBMIT.
- 7 The licensing server acquires the necessary information from the NSv Series appliance and your MySonicWall account.
- 8 Acknowledge the completion notification by clicking **CONTINUE**.

SonicOS automatically restarts and then displays the login page.

9 Log into SonicOS.

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

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

Your SonicWall NSv series firewall is now fully enabled.

De-activating Your NS_v

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

To deregister a BYOL NSv:

- 1 Log into the SonicOS management interface on your NSv virtual appliance.
- 2 Navigate to the Updates | Setting page in the MANAGE view.
- 3 Select **Export Configuration** from the **Import/Export Configuration** drop-down list to export your current configuration settings before deactivating your NSv.

 ● Import/Export Configuration 		
Import Configuration		
Export Configuration 👆 ild Date		

This makes it possible to import the settings to another NSv instance.

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

- 4 Navigate to the Updates | Licenses page in the MANAGE view.
- 5 Under Manage Security Services Online, click the DEREGISTER button.

Manage Security Services Online				
There are two methods to activate, upgrade or renew services.				
1. Go to MySonicWall.com, then come back and synchronize your changes.				
2. Provide your MySonicWall login and make all changes from here.				
SYNCHRONIZE	DEREGISTER			

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

This will deregister the unit and put in Click "OK" to proceed?	t back to unregistered state.
	OK Cancel

If de-activation is successful, the virtual appliance will return become disabled. You can see the **Register** link in the top banner of SonicOS and the message "Your SonicWall is not registered" on the **MONITOR** | **System > Status** page.

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

Converting a Free Trial License to Full License

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

To convert your free trial to a production version:

- 1 Purchase a SonicWall NSv license from a distributor. You will receive a fulfillment email with the new serial number and authentication code.
- 2 Log into SonicOS on your free trial instance.
- 3 Navigate to the **Updates | Licenses** page in the **MANAGE** view.
- 4 Under Manage Security Services Online, click the DEREGISTER button.
- 5 Click **OK** in the confirmation dialog. The virtual firewall returns to the unregistered state.
- 6 Click the **Register** link in the top banner or on the **MONITOR | System > Status** page.

SONICWALL	Network Security Virtual	MONITOR INVESTIGATE MANAGE		Register Help Logout
Current Status System Status) User Sessions		I't been changed. ot be sent because you have not specified an outbound SM nabled - Click here to enable.	TTP server address.	Mode: Configuration ►
	System Inform	ation Show Multi-Core Monitor	Security Services	Show All License Information 10 Nodes (0 in use)
	Product Code:	70000	SSL VPN Nodes/Users:	2 Nodes (0 in use)
	GUID:	101101-01-01-02-010000-000-000-000000000	Your SonicWall is not registered.	
	Firmware Version:	SonicOS Enhanced 6.5.0.2-8v-sonicosv-374cf82cf8	Click here to Register your SonicWall.	

7 Enter your MySonicWall credentials and then click LOGIN.

MySonicWall use	rname/email
Password	
	LOGIN

- 8 Enter the **Serial Number** and **Authentication Code** you received after purchasing your NSv Series instance.
- 9 Click SUBMIT.
- 10 The licensing server acquires the necessary information from the NSv Series appliance and your MySonicWall account. If asked, you can specify a **Friendly Name** or **Product Group** for the NSv Series appliance.
- 11 Acknowledge the registration completion notification by clicking **CONTINUE**.

SonicOS automatically restarts and then displays the login page.

12 Log into SonicOS.

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

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

Creating a MySonicWall Account

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

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

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

To create a MySonicWall account:

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

SONIC WALL mysonicwall	
Login with your MySonicWall account credentials Username or Email address	
Next	
Forgot username or email? Sign Up	
rongot username of ernam? Sign op	

- 3 Complete the account information, including email and password.
- 4 Follow the prompts to finish creating your account.
- 5 Click Finish.
- 6 Check your email for a verification code and enter it in the **Verification Code** field. If you did not receive a code, contact Customer Support by clicking on the link.
- 7 Click **Done**. You are returned to the login window so you can log into MySonicWall with your new account.

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

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

SonicOS Management

Topics:

- Managing SonicOS on the NSv Series on page 42
- Using SonicOS on an Unregistered NSv on page 42
- Using System Diagnostics in SonicOS on page 45

Managing SonicOS on the NS_v Series

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

The X0 interface is the default LAN interface. By default, the X0 interface has HTTPS management and DHCP enabled. So the X0 IP address is acquired from the AWS provided DHCP server in the X0 subnet. After deployment, you can reconfigure the IP address to an address in your network.

To log into SonicOS for management of the NSv:

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

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

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

2 Enter the administrator credentials (default *admin / instance-ID*) and press Enter.

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

NOTE: To upgrade your release of NSv, either use the management interface as described in SonicOS 6.5 for NSv Series Updates documentation available on the SonicWall portal, or use the SafeMode web interface as described in Uploading a New Image in SafeMode on page 70.

Using SonicOS on an Unregistered NS_v

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

4

Top Level View	Page Group	Page Within Group	Description	
MONITOR	System Status	n/a	System information, Node license, Alerts, Network interface settings	
	User Sessions	SSL-VPN Sessions	User sessions connected via SSL VPN	
		Active Users	Active user session information; Logout button for users	
		Active Guest Users	Active guest user session informatio Logout button for guest users	
		User Monitor	Graph of logged in users over time for client logins and web based logins	
NVESTIGATE	Event Logs	n/a	Log event table, dynamically updated filterable, searchable, one-click detai	
	Connection Logs	n/a	Connection log, source/destinations, protocols, bytes transferred, filterable searchable, flush option	
	Appflow Logs	n/a	Requires App Visualization license, which requires registration	
	System Diagnostics	n/a	TSR access and Diagnostic tools:	
			Check Network Settings	
			Ipv6 Check Network Settings	
			Connections Monitor	
			Multi-Core Monitor	
			Core Monitor	
			Link Monitor	
			Packet Size Monitor	
			DNS Name Lookup	
			Find Network Path	
			Ping	
			Core 0 Process Monitor	
			Real-time Black List Lookup	
			Reverse Name Resolution	
			Connection Limit TopX	
			TraceRoute	
			PMTU Discovery	
			Web Server Monitor	
			User Monitor	
			See Using System Diagnostics in SonicOS on page 45 for information.	
MANAGE	Licenses	n/a	Node license information, MySonicWall access, Manual Upgrad	
	Settings	n/a	Firmware versions, Local Backup, Settings import/export, Settings options to send to SonicWall Supp	
	Restart	n/a	Restarts the virtual firewall after confirmation	

Available SonicOS Pages on Unregistered NSv

43

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

Available SonicOS Pages on Unregistered NSv

Using System Diagnostics in SonicOS

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

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

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

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

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

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

Check Network Settings

Diagnostic Too	ols					
iagnostic Tool:	Check	Network Settings		•		
heck Network Se	ettings					
General Network	k Conne	ction				
Server		IP Address	Test Results	Notes	Timestamp	Progress Test
Default Gatewa	iy (X1)	→ 10.203.28.1				TEST
DNS Server 1		→ 10.200.0.52				TEST
DNS Server 2		▶ 10.200.0.53				TEST
Security Manage	ement					
Server		IP Address	Test Results	Notes	Timestamp	Progress Test
V SonicWall		N/A				TEST
License Manage	er	N/A				TEST
TEST ALL SEL	ECTED]				

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

Specifically, Check Network Settings automatically tests the following functions:

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

The return data consists of two parts:

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

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

diagTestPolicyAuto_<IP_address/Domain_name>_0

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

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

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

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

Upgrading the NS_V

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

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

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

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

5

Using the Virtual Console and SafeMode

This chapter discusses two software interfaces supporting NSv:

- the NSv Management Console
- the NSv SafeMode web interface
 - **NOTE:** For information on using the SonicOS CLI and NSv management console to troubleshoot the installation, see Troubleshooting Installation Configuration on page 30.

Topics:

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

Connecting to the Management Console with SSH

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

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

Logging in via SSH is only possible through the certificate file configured during the 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 above.
- 2 Navigate to the AWS EC2 Management Console and view the Instances page for your NSv.

aws Service	is 🗸 Resource Groups 🗸	1 EC2 9 VPC	CloudFormation *						A wgong@sonicwall.com 0 i	i295 + N. Cal
2 Dashboard	Launch Instance + Court	Actions ¥	21. Constant (1997)							
9	Q. Filter by tags and attributes or	search by keyword								0
onts	Name	- Instance ID	* Instance Type +	Availability Zone ~	Instance State +	Status Checks +	Alarm Stat	es Public DN	S (IPv4) + IPv4 Public IP	+ IPv6 IPs
115	weniu-650v-r350	1-000c322581878****	c5.4xlarge	us-west-1c	stopped		None	5	13.56 110 100	1 .
TANCES	Alan-LAN-PC1-Win	i-016293ft/694d2b4f1	t2 micro	us-west-1a	estopped		Nane	>		1
lances	bythen-RC235	1-0245bb853d2062a66	c5.xlarge	us-west-1c	e stopped		None		13 52 20 100	
ch Templates Requests	A Dian the	ADMARK THE STOR			and company		Alim			
city Reservations	Instance II	D i-000c3225818757784				Public D	45 (IPv4)			
SES	Instance stat							13.56.116.100		
	Instance typ	a c5.4starge				2	IPv6 IPs			
the Tasks	Elastic IP	a 13.56 mil 100				Pro	ate DNS	p-192-2-1-136 us-we	est-1 compute internal	
TTC BLOCK	Availability 2019	a us-west-1c				P	rivate IPs	192.2.2.14, 192.2.1	36	
	Security group	a default, view inbound rules, vi	ew outbound rules			Secondary p				
E	Scheduled event							pc-flea19dc9Dea39		
50.51		SoneWall NSv AWS R350 (a)	mi-Oe2fear/40371d5a90)					subnet-063b83c13d6	307326	
mes	AMU					Network		eth0 eth1		
mes shots	AM110 Platform									
RE mes pshots ycle Manager WORX &	Platform					Source/de		True		
mes oshots ycle Manager WORX & RUTY	Platform	le - a wenlu-nc								
mes pshots ycle Manager WORX & werty unty Groups	Platton IAM rol	la - a wentu-nc ar 629538266832				T2/T3	st check	True		
mes oshots ycle Manager WORX & RUTY	Platten LAM rol Keir pair nam	la - a wentu-nc ar 629538266832	l UTC+8 (91 hours)			T2/T3 EBS-	st sheck Unlimited	frue Frue		

- 3 Copy and paste the Instance ID and IPv4 address into a temporary file.
- 4 Refer to the instructions in the AWS documentation referenced above.
- 5 When ready to connect using the ssh command from Linux or with Putty from Windows, use *management* as the SSH username.

For example, from Linux:

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

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

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

-Menu-		
System Info	Model	: SonicWall Networ
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	 ACTIVATION AND ADDRESS OF ADDRE
About		

System Time Up Time Load Average

SonicOS

The orange NSv Management Console displays.

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

onicWall (c) 2018 | Uptime 20 hours, 1 minute

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

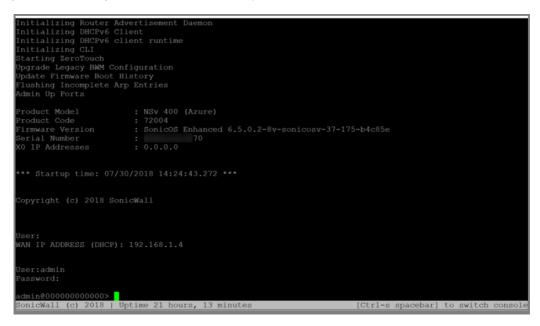
[Ctrl-s spacebar] to switch consol

k Security - Virtual Serie

: Tue 2018-07-31 17:26:57 UTC : 20 hours 2 minutes 50 seconds : 0.3 1min 0.4 5min 0.5 10min

: Operational

To log into the SonicWall web interface visit: https://192.16 / on X1 interface You can switch to the black SonicOS console window by pressing **Ctrl+s** and then the **spacebar**. If you are prompted to log in at the **User** prompt, enter the SonicOS administrator credentials (default: *admin / password* where password is the Instance ID).



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

Navigating the NS_v Management Console

The NSv management console provides options for viewing and changing system and network settings, running diagnostics, rebooting SonicOS, and other functions. To connect to the NSv Management Console, see Connecting to the Management Console with SSH.

To navigate and use the management console:

1 Press **Ctrl+s** and then press the **spacebar** to toggle between the SSH virtual console or VMware remote console and the NSv Management Console. That is, press the **Ctrl** key and 's' key together, then release and press the **spacebar**. The NSv management console has an orange background.

NTP Server Lockdown Mode System Update Reboot Shutdown About Logs	SonicOS Version GUID Systen Time Up Time CPU Load SonicOS	: Tue 2018-03-27 20:58:06 UTC : 41 minutes 35 seconds		
Up / Down to select items TAB to move between views Enter to action/edit an item	To log into the SonicWall web interface visit: https://192.168.			

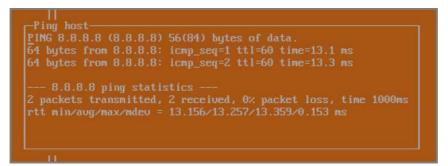
50

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



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

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



Some dialogs are for input:



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

The 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

r-Menu	I System Info			
System Info	Model	: SonicWall Network Security - Virtual Series		
Management Network	Product Code	: 70000		
Test Management Network	Serial Number			
Diagnostics	Model Name	: NSv Unlicensed Beta		
NTP Server	SonicOS Version	: 6.5.0.0		
Lockdown Mode	GUID			
System Update				
Reboot Shutdown	System Time	: Tue 2018-03-27 20:58:06 UTC		
About	Up Time	: 41 minutes 35 seconds		
Logs	CPU Load	: 1.1 1min 1.1 5min 1.0 10min		
	SonicOS	: Operational		
Up / Down to select items TAB to move between views Enter to action/edit an item	To log into the SonicWall web interface visit: https://192.168.			
SonicWall (c) 2018 Uptime 41 min	nutes	[Ctrl-s spacebar] to switch console		

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

- **Model** This is the model of the NSv appliance.
- **Product code** This is the product code of the NSv appliance.
- Serial Number The serial number for the appliance; this is a number unique to every NSv instance deployed. This number can be used to identify the NSv appliance on MySonicWall.
- Model Name This is the model name of the NSv appliance.
- **SonicOS Version** This is the currently running SonicOS version of the NSv appliance.
- **GUID** Every NSv instance has a GUID which is displayed here.
- **System Time** This is the current system time on the NSv appliance.
- Up Time This is the total time that the NSv appliance has been running.
- Average Load This shows the average CPU load for the last 1 minute, 5 minutes and 10 minutes. You can change the Average load time durations to view the CPU load over longer or shorter time periods.
- SonicOS This presents the current state of the SonicOS service on the 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

-Menu-	Network Interfaces	
System Info	Network interface	X1
Network Interfaces		
Diagnostics	IPv4 Address	192.168.1.4
NTP Server	Netmask	255.255.255.0
Lockdown Mode	Mac address	00:00:100:100:100:100
System Update	IPv6 Address	fe80::20d:3aff:fe37:d01d
	Gateway	192.168.1.1
About	DNS 1	8.8.8.8
Logs	DNS 2	8.8.4.4
Up / Down to select items TAB to move between views Enter to action/edit an item	To log into the SonicWall w https://192.168.1.4/ on X1	
onicWall (c) 2018 Uptime 22 hou	urs, 3 minutes	[Ctrl-s spacebar] to switch consol

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

Test Management Network

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

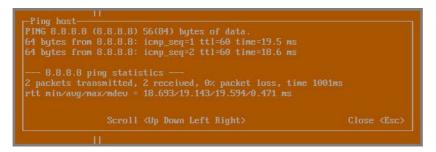
Menu System Info Management Network Test Management Network Diagnostics NTP Server Lockdown Mode	-Test Management Network- Ping E Ping Nslookup E Nslookup	1
System Update Reboot Shutdown About Logs	-Enter IP address	
	192.168.8.1_ Confirm <enter> Cancel <esc></esc></enter>	
Up / Down to select items TAB to move between views Enter to action/edit an item SonicWall (c) 2018 Uptime 3 minu	tes [Ctrl-s spacebar] to switch (concole

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

To use Ping:

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

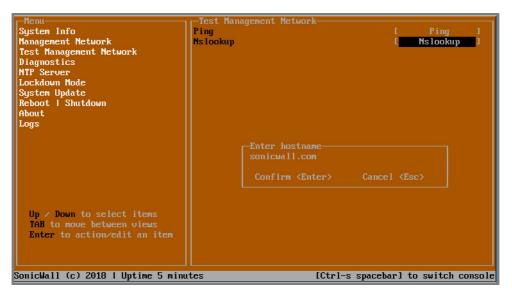
The ping output is displayed in the **Ping host** dialog.



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

To use Nslookup:

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



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

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



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

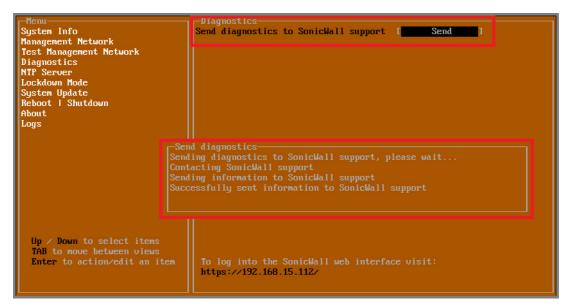
Diagnostics



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

NOTE: Your NSv appliance must have internet access to send the diagnostics report to SonicWall Support.

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



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

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

Common reasons for the report failing to send include:

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

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

NTP Server

Sync with ntp server	E Perform sync 1
Current time	Fri 2018-01-26 23:16:52 UTC
Network time enabled	
NTP synchronized	
	Network time enabled

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 appliance's NTP client to perform a sync with the configured NTP server(s).
- **Current time** The current time on the NSv appliance.

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

Lockdown Mode



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

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

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

Temporary Lockdown Mode

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

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

System Update

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

-Menu-		
System Info	System Update	[Start Update]
Network Interfaces	bybeem opdace	[btare opdate]
Diagnostics		
NTP Server		
Lockdown Mode		
System Update		
Reboot Shutdown		
About		
Logs		
	-Begin System Update?	
	Yes	
	No	
	Confirm <enter> Cancel <esc></esc></enter>	
Un (Davin the select items		
Up / Down to select items		
TAB to move between views		
Enter to action/edit an item	To log into the SonicWall web inte	
	https://192.168.1.4/ on X1 interfa	ce
SonicWall (c) 2018 Uptime 22 h	ours, 21 minutes [(Ctrl-s spacebar] to switch console

Reboot | Shutdown



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

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

- **Reboot SonicWall** Restarts the NSv Series virtual appliance with current configuration settings.
- Shutdown SonicWall Powers off the NSv Series virtual appliance.
- **Boot with factory default settings** Restarts the NSv Series virtual appliance using factory default settings. All configuration settings will be erased.
- **Boot SonicWall into debug** Restarts the NSv Series virtual appliance into debug mode. Normally this operation is performed under the guidance of SonicWall Technical Support.
- **Boot SonicWall into safemode** Puts the NSv Series virtual appliance into SafeMode. For more information, see Using the Management Console in SafeMode on page 60.

About

r Menu	About	
System Info	SonicWall SonicCo	re
Management Network	Version	
Test Management Network	Build name	6.5.0-288+SonicCore-SonicOsV-6.5-Daily
Diagnostics		
NTP Server		
Lockdown Mode		
Reboot Shutdown		
About		

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

Logs

The **Logs** screen displays log events for the NSv appliance.

Henu System Info Management Network Test Management Network Diagnostics NTP Server Lockdoum Mode System Update Reboot I Shutdown About Logs	Apr 25 20:31:54 local Apr 25 20:31:52 local Apr 25 20:31:52 local Apr 25 20:31:52 local Apr 25 20:31:51 local Apr 25 20:04:26 local Apr 25 20:04:26 local Apr 25 20:04:26 local Apr 25 20:04:25 local Apr 25 20:04:25 local Apr 25 20:04:25	Nost Automatic secure crash analysis reporting is enabled Nost Periodic secure diagnostic reporting for support purposes is enabled Nost Initializing Sonickall support services Nost Completed configuring the operating environment for SonicOS Nost Completed configuring the operating environment for SonicOS Nost Model: "NSU 000" supports 8 CPU, current CPU count is only 2, for in Nost Total memory installed 10237296 Kb Nost CPU flags: fpu une de pse tsc msr pae mce cx0 apic sep mtrr pge mca Nost CPU count: 2, Model "Intel(R) Xeon(R) CPU E5-2690 u3 0 2.60GHz" Nost Configure the operating environment for SonicOS Nost Unconfigure the operating environment for SonicOS Nost Automatic secure diagnostic reporting for support purposes is enabled Nost Congleted configuring the operating environment for SonicOS Nost Automatic secure diagnostic reporting for support purposes is enabled Nost Congleted configuring the operating environment for SonicOS Nost Automatic secure diagnostic reporting for support purposes is enabled Nost Congleted configuring the operating environment for SonicOS Nost Automatic secure diagnostic reporting for support purposes is enabled Nost Congleted configuring the operating environment for SonicOS Nost No system information file available Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flags: fpu ume de pse tsc msr pae mce cx8 apic sep mtrr pge mca Nost CPU flag
Up / Down to select items TAB to move between views Enter to action/edit an item Space to hide/show side menu SonicWall (c) 2018 Uptime 23 ho	Arrow keys: Mavig	nte view - Current Line: 1 Lines: 21 [Ctrl-s spacebar] to switch console

Using the Management Console in SafeMode

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

Topics:

- How Management Console Differs in SafeMode
- Entering SafeMode
- Enabling/Disabling SafeMode
- Configuring the Management Network in 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.

Safemode menu System Info Management Network Test Management Network Diagnostics NTF Server System Update Reboot I Shutdown About Logs	SonicOS Version GUID System Time	: SonicWall Network Security - Virtual Series : 70000 : NSU Unlicensed Beta : 6.5.0.0 : 5 : Tue 2018-03-13 21:57:22 UTC : 6 hours 33 minutes 19 seconds : 0.0 1min 0.0 5min 0.0 10min : Not operational	
Up / Down to select items TAB to move between views Enter to action/edit an item SonicWall (c) 2018 Uptime 6 how	http://192.168.14	Afemode, to access recovery options visit: 210/	[safemode]

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

Enabling/Disabling SafeMode

Topics:

- Enabling SafeMode
- Disabling SafeMode

Enabling SafeMode

SafeMode can be enabled from the management console.

To enable SafeMode:

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



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

The NSv immediately reboots and comes back up in SafeMode.

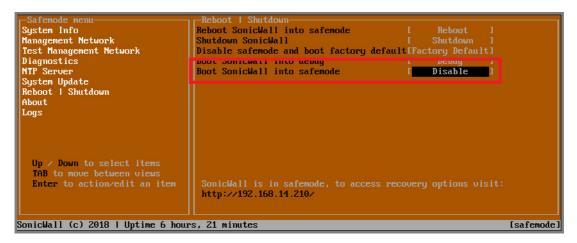
(i) NOTE: In SafeMode, the web interface is served from an HTTP server. The HTTPS server is not started in SafeMode.

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**.



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

The NSv immediately reboots and boots up in normal mode.

Configuring the Management Network in SafeMode

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



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

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

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

Topics:

- Configuring Interface Settings
- Disabling an Interface

Configuring Interface Settings

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

() №	OTE: In	SafeMode,	the X0	will b	e set by	DHCP.
-------------	---------	-----------	--------	--------	----------	-------

-Safemode menu	M COLORA CONTRACTOR CONTRACTOR		
	Management interface	[X1]	
Management Network			
Toot Management Noter rk	IPv4 Address	[192.168.14.200]	
Diagnostics	Netmask	[255.255.248.0]	
NTP Server	Mac address	00:0c:29:ba:0e:99	
System Update Reboot Shutdown	IPu6 Address Gateway	fe80::20c:29ff:feba:e99 [192.168.8.1]	
About	DNS 1		
Logs	DNS 2	[8.8.4.4]	
	-Select Interface		
	XZ		
	X3		
	X4		
	X5		
	X6 X7		
	Confirm <enter></enter>	Cancel <esc></esc>	
Up ∕ Down to select items			
TAB to move between views			
Enter to action/edit an item	SonicWall is in safemode, to a		
	http://192.168.14.200/ or http	://192.168.1.254/	
SonicWall (c) 2018 Uptime 5 hour	s, 43 minutes		[safemode]

To edit an interface:

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

-Safemode menu				
Ogoton Tito	Management interface	E	X1	1
Management Network		T 100	10.00	
Toot Management Notice rk	IPu4 Address		168.14.200	1
Diagnostics NTP Server	Netmask Mac address		.255.248.0 :29:ba:0e:99	1
System Update	IPu6 Address		:29ff:feba:e9	9
Reboot I Shutdown	Gateway		2.168.8.1	_]
About	DNS 1			1
Logs	DNS 2			1
Up / Down to select items TAB to move between views Enter to action/edit an item SonicWall (c) 2018 Uptime 5 hour	Select Interface X0 X2 X3 X4 X5 X6 X7 Confirm <enter> SonicWall is in safemode, to acc http://192.168.14.200/ or http:/</enter>		ions visit:	[safenode]

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

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

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

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

The on-screen dialog displays the current IP address.

- 4 Navigate into the dialog and make the desired changes, then press **Enter** to close the dialog or press **Esc** to cancel and close the dialog.
- 5 Two new buttons appear on the screen after you make changes to an interface setting: **Save changes** and **Cancel**. You can use the **Tab** key to navigate to these buttons.

Safenode nenu System Info Managenent Network Test Managenent Network Diagmostics NTP Server System Update	Hanagement Network Management interface IPv4 Address Netmask Mac address IPv6 Address	[X1 [192.168.14.210 [255.255.248.0 00:00:29:ba:00:99 fe80:29:20:29ff;feba:e9	1 1 1 9
Reboot I Shutdown About Logs	Gateway DMS 1 DMS 2		
	Save changes		Cance 1
Up / Down to select items TAB to move between views Enter to action/edit an item	SonicWall is in safemode, to http://192.168.14.210/ or h	p access recovery options visit: ttp://192.168.1.254∕	
SonicWall (c) 2018 Uptime 6 hou	rs, 1 minute		Isafemod



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 on the screen above the interface selection dialog.

4 Select IPv4 Address and press Enter.

The on-screen dialog displays the current IP address.

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

Safemode menu	Management Network-	
System Info	Management interface	T X1]
Management Network Test Management Network Diagnostics	IPu4 Address	[192.168.0.15]
NTP Server System Update Reboot I Shutdown About Logs	Mac address IPu6 Address Gateway DMS 1 DNS 2	00:0c:29:5a:19:dd fe80::20c:29ff:fe5a:19dd [192.168.0.1] [8.8.8.8] [8.8.4.4]
	Enter IP address 0.0.0_ Confirm <enter> Cance</enter>	l (Esc)
Up / Down to select items TAB to move between views Enter to action/edit an item	SonicWall is in safemode, to access re http://192.168.0.15/ or http://192.166	

The Save changes button is displayed.

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

65

The interface is disabled.

Management Network- Management interface	X1	
IPu4 Address Netmask Mar. address	Not configured	
IPu6 Address Gateway DNS 1 DNS 2	fe80::20c:29ff:fe5a:19d 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 which provides image upgrade and log download functions. You can also lock or unlock the NSv management console from the SafeMode web interface.

Topics:

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

Accessing the SafeMode Web Interface

To access the SafeMode web interface:

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

		Contraction of the contraction of the	a manuel reduction and	st-1#Instances:sort=instanceId							
aws Service	es - Resourc	e Groups 👻 🛛	EC2 🥵 VPC	CloudFormation 🔸					Δ.	qong@sonicwall.com @ 6	195 + N. Califor
EC2 Dashboard	Launch Instan	ce 👻 Connec	Actions ¥								
Tags	Q, Filter by tag	s and attributes or sea	rch by keyword								ØK
Reports	Name		Instance ID	* Instance Type -	Availability Zone -	Instance State ~	Status Checks -	Alarm Stat	us Public DNS (IPv4)	+ IPv4 Public IP	✓ IPv6 IPs
S	weniu-650	N-r350	H000c32258187875	ibe c5.4xlarge	us-west-1c	stopped		None	2	13.56.116.108	1.7
INSTANCES	Allen-LAN	PC1-Win	1-016298fc694d2b4	f1 t2.micro	us-west-1a	🥥 stopped		Nane	2		
Launch Templates	bychen-R	C235	i-0245bb853d2062g	a56 c.5.xlarga	us-west-1c	stopped		None	>	13.52.23.160	<u></u>
Spot Requests	4 Man.Ph		1071984bvt7419ha3	cfi mé viaros	1127-022-10	e stonned		Albert	-	1.00	
Reserved Instances Dedicated Hosts	Description	Status Checks	Monitoring Tag	Elastic IP: 13.56.116.108							
Capacity Reservations		Instance ID	i-000c32258187879be				Public D	VS (IPv4)			
MAGES		Instance state	stopped				IP/4	Public IP	13.56.116.108		
AMIS		Instance type	c5.4xlarge					IPv6 IPs			
lundle Tasks			13.56.116.108*						p-192-2-1-136.us-west-1.com	apute internal	
LASTIC BLOCK		Availability zone							192.2.2.14, 192.2.1.136		
			default, view inbound	rules, view outbound rules			Secondary p		vpc-Dea19dc9Dea39d3b5		
/olumes		Scheduled events	Constitute NO. AIRIS	R350 (ami-0e2feaf40371d5a90)					vpc-Dea19dc9Dea39d365 subnet-063b83c13d5307325		
Snapshots		Platform		_H000 (allF062/68/4007 (008/60)					eth0		
.flecycle Manager		T INFORM					Transmission, I		eth1		
NETWORK &		LAM role	-				Source/de	st check	True		
SECURITY Security Groups		Key pair name	wenlu-nc				т2/т3	Unlimited			
		Owner	629538266832				EBS-	optimized	True		
Elastic IPs Placement Groups		Launch time	December 3, 2018 at 2	2:45:33 PM UTC+8 (91 hours)			Root de	vice type	ebs		

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

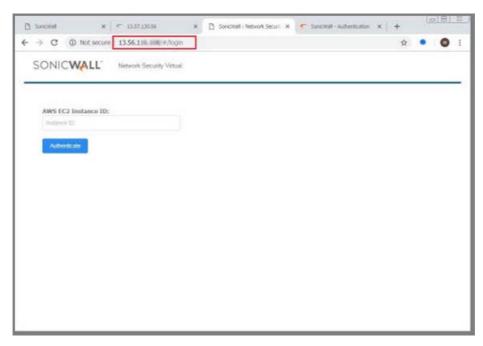
You can access the SafeMode web interface at the public IP address of the NSv, and you must authenticate to gain access.

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

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

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		: NSv 400 (Azure)
System Update	SonicOS Version	
Reboot Shutdown	GUID	A THE OWNER WATCH TO AND THE ADDRESS OF THE OWNER OWNE
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
	boud morage	
	SonicOS	: Operational
		· operationar
Up / Down to select items		
TAB to move between views		
Enter to action/edit an item	To log into the So	nicWall web interface visit:
	https://192.16	
SonicWall (c) 2018 Uptime 20 hou	urs, 1 minute	[Ctrl-s spacebar] to switch console

- 3 Go into the management console and boot into SafeMode. See Entering SafeMode
- 4 In a web browser, navigate to *http://<NSv public IP address>*, using the applicable IP address. The SafeMode authentication screen displays.



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

SONICWALL Ne SonicOS is running in Safe Mode	twork Security Virtual				
Safe Mode will allow you to do any of t > Download the Safe Mode Logs f > Upload new SonicOS application > Boot your choice of application i > Restore the settings to their factor Download Safe Mode Logs	or troubleshooting by the SonicWa n images mage	all 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- 3725793204	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 Action N/A

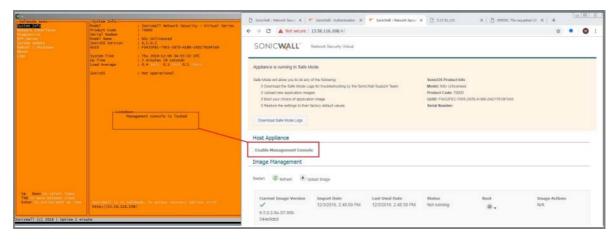
Entering/Exiting SafeMode

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/Disabling SafeMode).

Locking and Unlocking the Management Console

From the management web interface, the management console can be locked an unlocked as shown below. This locking and unlocking has the same effect as Locking and Unlocking the Management Console.



Downloading the SafeMode Logs

You can download logs of SafeMode activity.

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

To download logs from SafeMode:

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

SONICWALL No	twork Security Virtual				
SonicOS is running in Safe Mode					
Safe Mode will allow you to do any of t > Download the Safe Mode Logs I > Upload new SonicOS application > Boot your choice of application i > Restore the settings to their fact	for troubleshooting by the SonicWa n images mage	all Support Team	SonicOS Product Info Model: NSv Unlicensed Product Code: 70000 GUID: Serial Number:		
Download Safe Mode Logs 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 Action N/A

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

Uploading a New Image in SafeMode

SWI files are used to upgrade SonicOS.

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

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

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

To install a new SonicOS from SafeMode:

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

Safe Mode will allow you to do any of the following: SonicOS Product Info > Download the Safe Mode Logs for troubleshooting by the SonicWall Support Team Model: NSv Unlicensed > Upload new SonicOS application images Product Code: 70000 > Boot your choice of application image GUID: > Restore the settings to their factory default values Serial Number: Download Safe Mode Logs	SonicOS is running in Safe Mode					
> Upload new SonicOS application images Product Code: 70000 > Boot your choice of application image GUID: > Restore the settings to their factory default values Serial Number:	Safe Mode will allow you to do any of t	he following:		SonicOS Product Info		
> Boot your choice of application image GUID: > Restore the settings to their factory default values Serial Number:	> Download the Safe Mode Logs f	or troubleshooting by the SonicWa	all Support Team	Model: NSv Unlicensed		
> Restore the settings to their factory default values Serial Number: Download Safe Mode Logs	> Upload new SonicOS application	n images		Product Code: 70000		
Download Safe Mode Logs	> Boot your choice of application in	mage		GUID:	the second second	
	mage Management estart @ Refresh		Last line d Parts	Challers		
Current Image Version ✓ Import Date Last Used Date Status Boot Image Activity 6.5.0.2-8v-sonicosv- 4/25/2018, 6:14:00 PM 4/25/2018, 6:14:03 PM Not Running: Safe Mode 0	image Management Restart @ Refresh ③ Uploa	Import Date	Last Used Date	Status Not Running: Sofa Mode	Boot	Image Acti

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

art 🔞 Refresh 🛈 Upload	Image				
Current Image Version 🗸 6.5.0.2-8v-sonicosv-37f207f34d	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-37t207t34d	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- with Current Configuration Boot Uploaded Image (6.5.0.2-8v-s with Factory Default Configuration		

The NSv 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 MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

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

About This Document

Legend

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

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

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

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

Copyright © 2020 SonicWall Inc. All rights reserved.

SonicWall is a trademark or registered trademark of SonicWall Inc. and/or its affiliates in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners

The information in this document is provided in connection with SonicWall Inc. 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 SonicWall 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 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. SonicWall Inc. 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 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 SonicWall Inc. Attn: Jennifer Anderson 1033 McCarthy Blvd Milpitas, CA 95035