Integration Guide: SonicOS and VMware ESXi

May 2019

This document describes how SonicOS NS*v* Series is integrated with VMware ESXi, a bare-metal hypervisor that can be installed on a bare hardware. SonicOS runs on the VMware ESXi infrastructure.

Topics:

- Requirements
- Installing SonicOS NSv on VMware ESXi
- Using the VMware Remote Console to Configure SonicOS NSv

Requirements

- MySonicWall Account
- SonicOS 6.5.0 firmware
- VMware ESXi 5.5 and higher
- Hardware: Intel Penryn (CPU) and higher (2008)

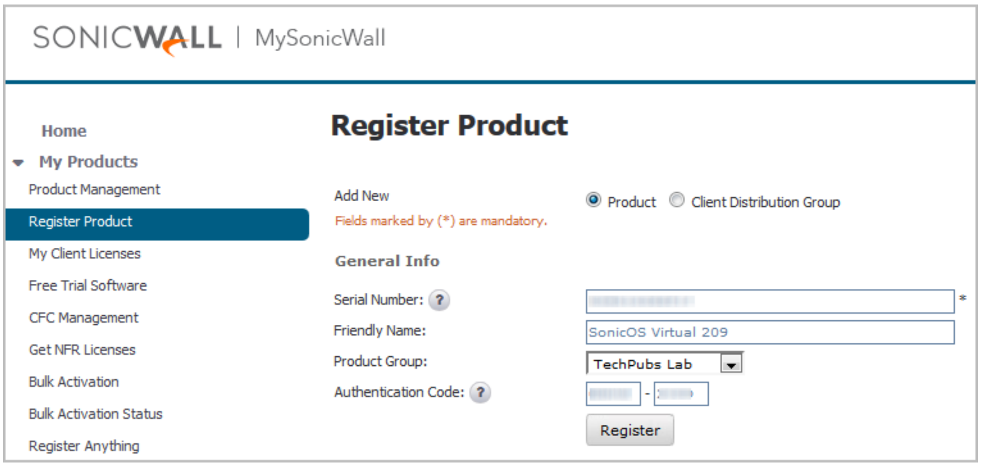
Installing SonicOS NS*v* on VMware ESXi

When you purchase a SonicWall NS*v* from a distributor, you receive a fulfillment email with your serial number and authentication code. Enter this information in MySonicWall when you register and access the OVA file.

Obtaining the OVA from MySonicWall

To register and obtain the OVA file for deployment:

1. In a browser, log into your MySonicWall account.
2. Navigate to **My Products > Register Product**.
3. Fill in the **Serial Number**, **Friendly Name**, **Product Group**, and **Authentication Code** fields, and then click **Register**.



Register Product

Add New ● Product ○ Client Distribution Group

Fields marked by (*) are mandatory.

General Info

Serial Number: ?	[redacted] *
Friendly Name:	SonicOS Virtual 209
Product Group:	TechPubs Lab
Authentication Code: ?	[redacted] - [redacted]

4 The **Registration Code** is displayed. Make a note of it.

You are now given access to the OVA file for your NS*v* model.

5 Download the OVA file and save it to your management computer.

You are now ready to deploy the OVA on your VMware ESXi server. After your NS*v* installation is complete, boot up SonicOS and log in.

Once you have connected and have internet access from the NS*v*, register your NS*v* Series instance using the **Registration Code** to complete the registration process.

Installing the NS*v* appliance

You can install NS*v* by deploying the OVA file to your VMware ESXi server. Each OVA file contains the software components needed. Deploy the OVA file by using the vSphere or vCenter client, which are available with ESXi.

> **NOTE:** VMware ESXi elements must already be in place and the administrator must be familiar with the basics of deploying a virtual appliance on the ESXi server.

> **TIP:** Step 15 has some important information about selecting your networks. Even if you do not need all these step-by-step instructions, be sure to follow the instructions in Step 15 to avoid connectivity issues after the deployment.

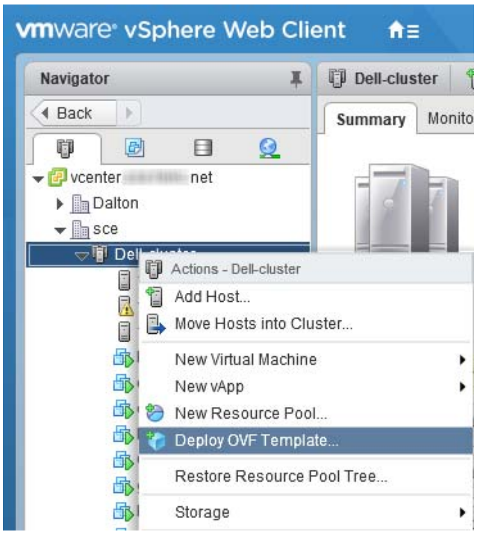
To perform a fresh install of SonicOS NSv Series on VMware ESXi:

1 Download the NS*v* Series OVA file from MySonicWall to a computer with vSphere / vCenter access.

2 Access vSphere or vCenter and log on to your ESXi server.

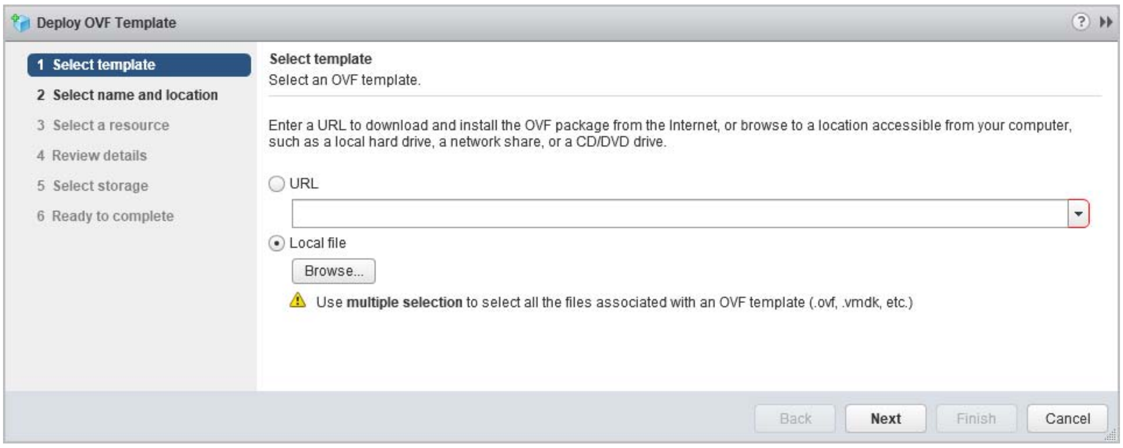
3 Navigate to the location where you want to install the virtual machine, and select the folder.

4 To begin the import process, click **Actions** and select **Deploy OVF Template**.



5 In the **Select template** screen, select **Local file**:

- **Local file** – Click **Browse** and navigate to the NS*v* Series OVA file that you previously downloaded from the provided beta link.



Select template

Select an OVF template.

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

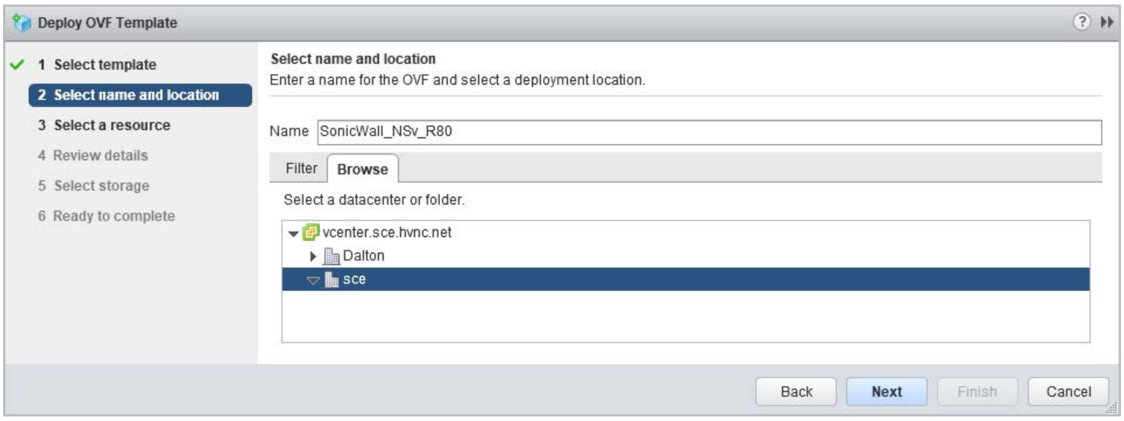
○ URL

● Local file

Use **multiple selection** to select all the files associated with an OVF template (.ovf, .vmdk, etc.)

6 Click **Next**.

7 In the **Select name and location** screen, type a descriptive name for the NS*v* appliance into the **Name** field, and then select the location for it from the ESXi folder structure.



Select name and location

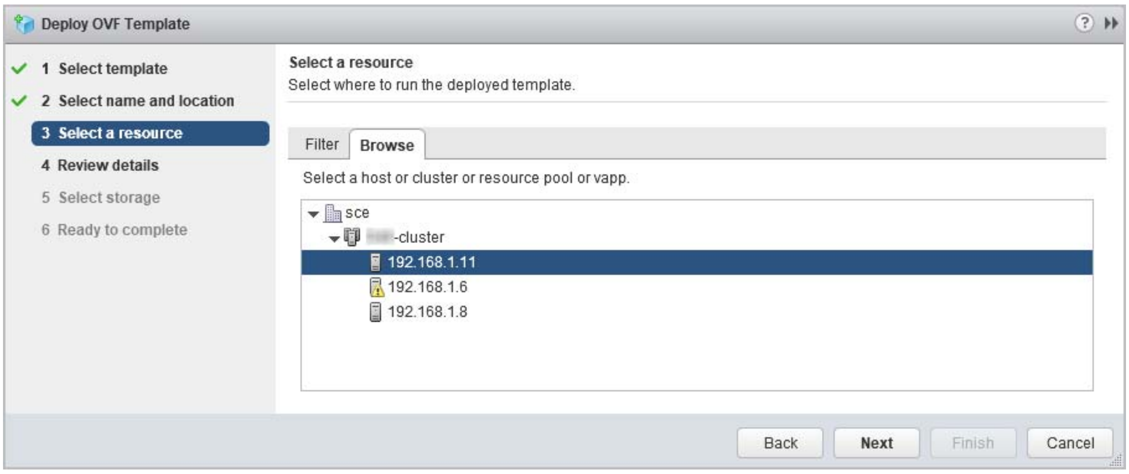
Enter a name for the OVF and select a deployment location.

Name SonicWall_NSv_R80

Select a datacenter or folder.

8 Click **Next**.

9 In the **Select a resource** screen, click **Next** to accept the default resource for the selected folder, or select a different resource and then click **Next**. Wait while the resource is validated. This is the resource pool where you want to deploy the template.



Deploy OVF Template

✓ 1 Select template
✓ 2 Select name and location
3 Select a resource
4 Review details
5 Select storage
6 Ready to complete

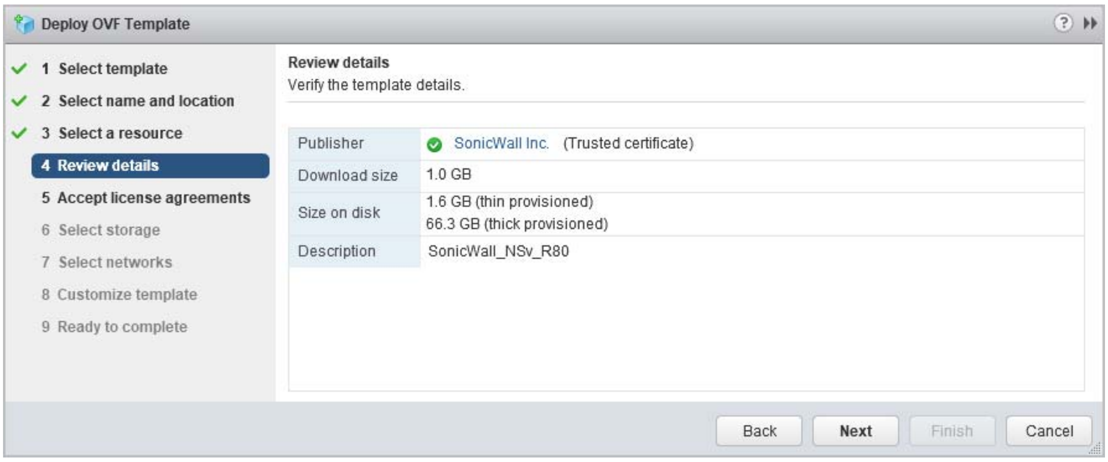
Select a resource
Select where to run the deployed template.

Filter | Browse

Select a host or cluster or resource pool or vapp.

- sce
  - [redacted]-cluster
    - 192.168.1.11
    - 192.168.1.6
    - 192.168.1.8

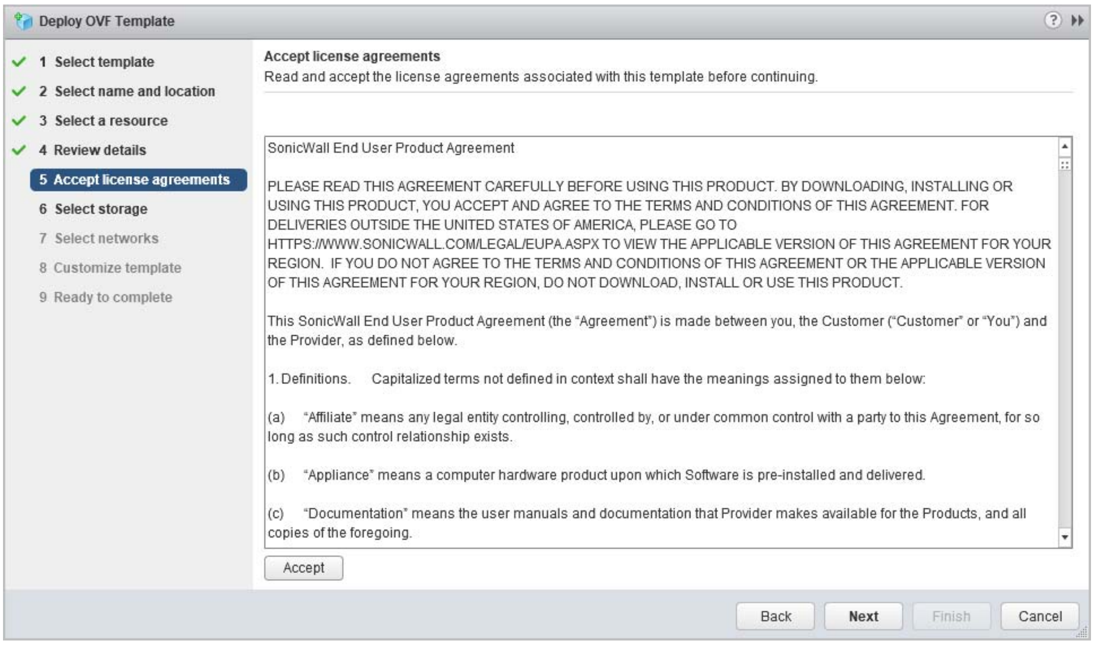
10 In the **Review details** screen, verify the template details and then click **Next**.



Review details
Verify the template details.

Publisher	✓ SonicWall Inc. (Trusted certificate)
Download size	1.0 GB
Size on disk	1.6 GB (thin provisioned) 66.3 GB (thick provisioned)
Description	SonicWall_NSv_R80

11 In the **Accept license agreements** screen, read the agreement, click **Accept** and then click **Next**.



Accept license agreements
Read and accept the license agreements associated with this template before continuing.

SonicWall End User Product Agreement

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THIS PRODUCT. BY DOWNLOADING, INSTALLING OR USING THIS PRODUCT, YOU ACCEPT AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. FOR DELIVERIES OUTSIDE THE UNITED STATES OF AMERICA, PLEASE GO TO HTTPS://WWW.SONICWALL.COM/LEGAL/EUPA.ASPX TO VIEW THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT OR THE APPLICABLE VERSION OF THIS AGREEMENT FOR YOUR REGION, DO NOT DOWNLOAD, INSTALL OR USE THIS PRODUCT.

This SonicWall End User Product Agreement (the "Agreement") is made between you, the Customer ("Customer" or "You") and the Provider, as defined below.

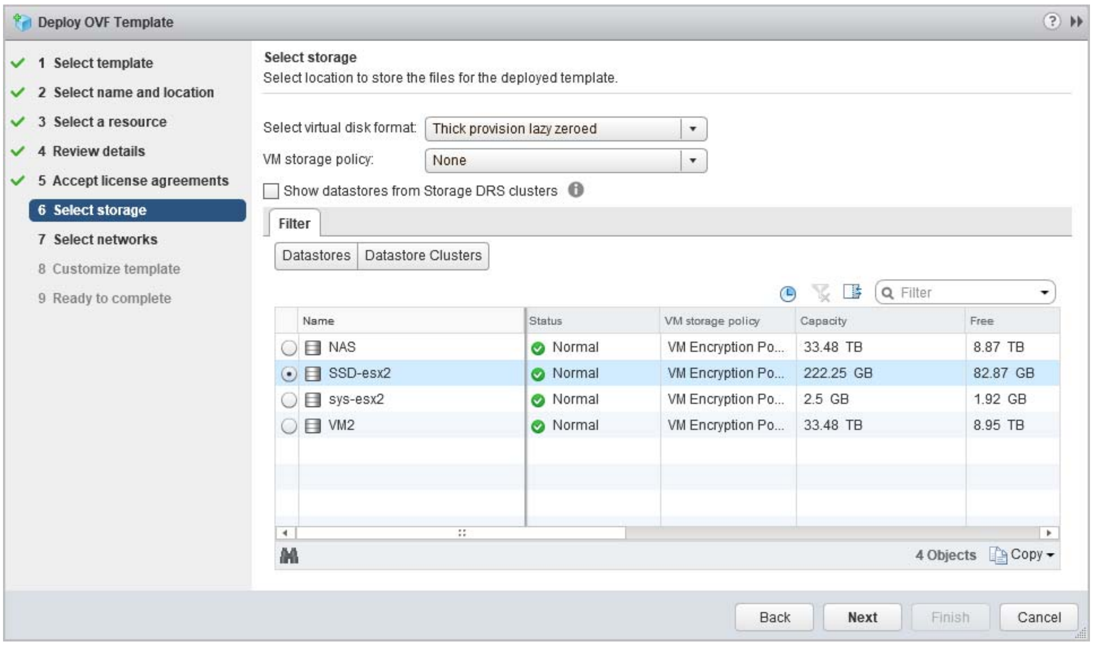
1. Definitions. Capitalized terms not defined in context shall have the meanings assigned to them below:

(a) "Affiliate" means any legal entity controlling, controlled by, or under common control with a party to this Agreement, for so long as such control relationship exists.

(b) "Appliance" means a computer hardware product upon which Software is pre-installed and delivered.

(c) "Documentation" means the user manuals and documentation that Provider makes available for the Products, and all copies of the foregoing.

12 In the **Select storage** screen, first select a datastore from the table. This is the location where you want to store the virtual machine files.



Select storage

Select location to store the files for the deployed template.

Select virtual disk format: Thick provision lazy zeroed

VM storage policy: None

□ Show datastores from Storage DRS clusters

	Name	Status	VM storage policy	Capacity	Free
○	NAS	✓ Normal	VM Encryption Po...	33.48 TB	8.87 TB
●	SSD-esx2	✓ Normal	VM Encryption Po...	222.25 GB	82.87 GB
○	sys-esx2	✓ Normal	VM Encryption Po...	2.5 GB	1.92 GB
○	VM2	✓ Normal	VM Encryption Po...	33.48 TB	8.95 TB

4 Objects

13 In the same screen, select the type of provisioning for the NS*v* appliance disk from the **Select virtual disk format** drop-down list. SonicWall recommends **Thin Provision**, but any selection works.

14 Click **Next**.

15 In the **Select networks** screen, ***first sort the list of interfaces*** by clicking the **Source Network** column heading. Then select the vswitch networks that are mapped to the NS*v* appliance interfaces. The source networks are the NS*v* appliance interfaces (X0, X1, X2, X3, X4, X5, X6, X7), and the destination networks are the vswitch ports of your existing vswitch network configuration. If your vswitch networks are not fully configured, you can further adjust the interface/vswitch port pairs.

NOTE: The ESXi vswitch configuration should have the option for **MAC address changes** enabled for the vswitch ports connected to the NS*v*.

For advanced configurations (DVS), consult the VMware documentation on vswitch configuration.

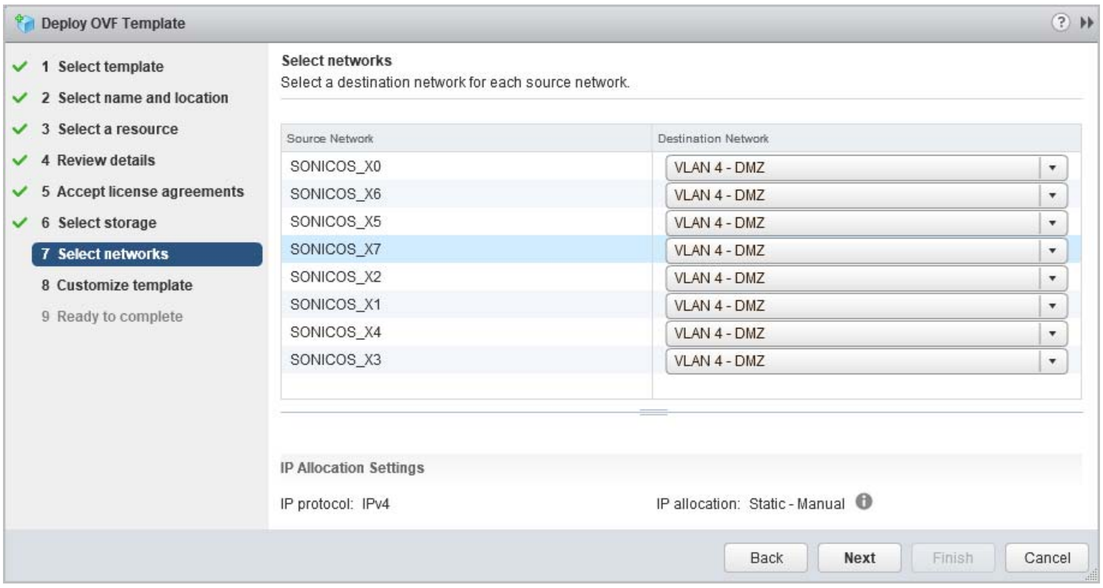
Typically, the NS*v* Series is deployed between your internal network and a network with internet access, and therefore you map the source **X0** to your LAN network (vswitch port), and map the source **X1** to the WAN network (vswitch port) with connectivity to the internet.

IMPORTANT: SONICOS_X1 (the default WAN Interface) is set to ***DHCP*** by default, with ***HTTPS management*** enabled for the NS*v* Series, as this configuration eases deployments in virtual/cloud environments.

NOTE: System defaults for the X0 and X1 interfaces are:

- X0 – Default LAN – 192.168.168.168
- X1 – Default WAN – DHCP addressing, with HTTPS and Ping management enabled

NOTE: Configuration settings import from physical firewalls to the NS*v* Series is not supported.



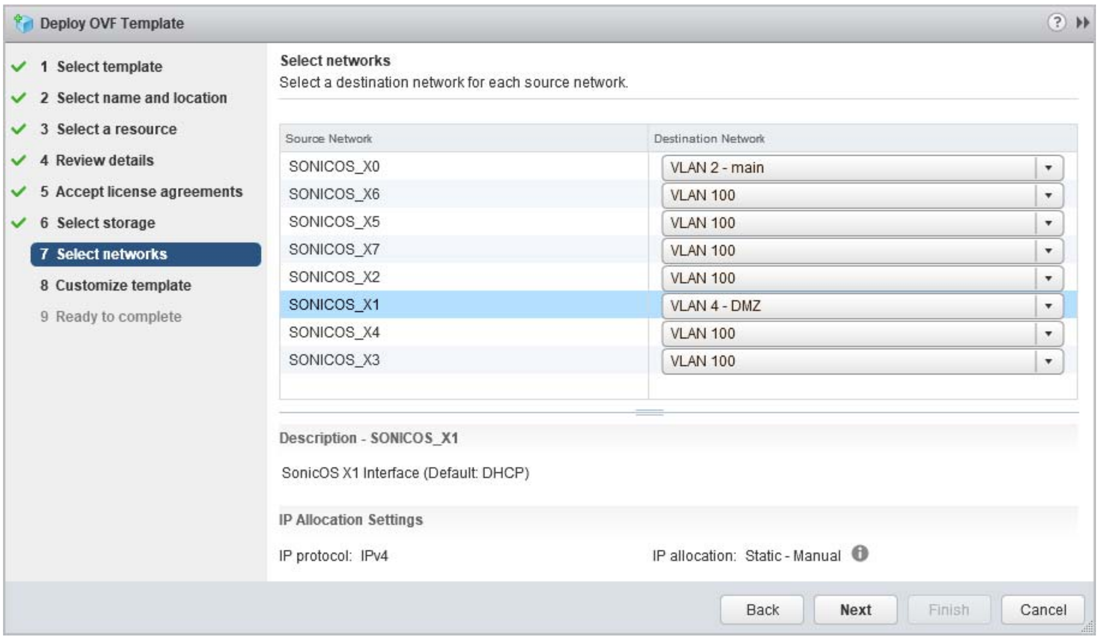
Select networks

Select a destination network for each source network.

Source Network	Destination Network
SONICOS_X0	VLAN 4 - DMZ
SONICOS_X6	VLAN 4 - DMZ
SONICOS_X5	VLAN 4 - DMZ
SONICOS_X7	VLAN 4 - DMZ
SONICOS_X2	VLAN 4 - DMZ
SONICOS_X1	VLAN 4 - DMZ
SONICOS_X4	VLAN 4 - DMZ
SONICOS_X3	VLAN 4 - DMZ

IP Allocation Settings

IP protocol: IPv4   IP allocation: Static - Manual



Select networks

Select a destination network for each source network.

Source Network	Destination Network
SONICOS_X0	VLAN 2 - main
SONICOS_X6	VLAN 100
SONICOS_X5	VLAN 100
SONICOS_X7	VLAN 100
SONICOS_X2	VLAN 100
SONICOS_X1	VLAN 4 - DMZ
SONICOS_X4	VLAN 100
SONICOS_X3	VLAN 100

Description - SONICOS_X1

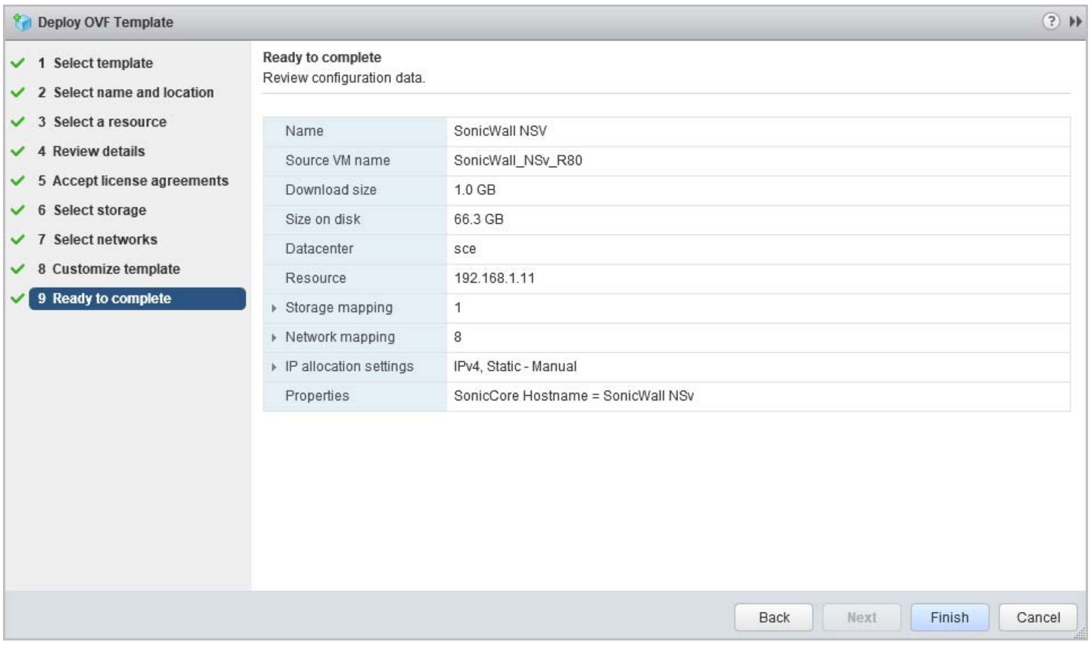
SonicOS X1 Interface (Default: DHCP)

IP Allocation Settings

IP protocol: IPv4   IP allocation: Static - Manual

16 Click **Next**.

17 In the **Ready to complete** screen, review the settings and click **Finish** to create the NS*v* appliance. To change a setting, click **Back** to navigate back through the screens to make a change.



Ready to complete
Review configuration data.

Name	SonicWall NSV
Source VM name	SonicWall_NSv_R80
Download size	1.0 GB
Size on disk	66.3 GB
Datacenter	sce
Resource	192.168.1.11
Storage mapping	1
Network mapping	8
IP allocation settings	IPv4, Static - Manual
Properties	SonicCore Hostname = SonicWall NSv

The name of the new NS*v* appliance appears in the left pane of the vSphere or vCenter window when complete.

The next step is to power on your NS*v* virtual firewall in the vSphere or vCenter interface.

Once your NS*v* virtual firewall is powered on, the next step is to register it on MySonicWall.

Using the VMware Remote Console to Configure SonicOS NS*v*

You can use the VMware remote console to set the IP address and network settings of the NS*v* Series interfaces, to change between static and DHCP addressing, and to enable SonicOS management on your NS*v* Series instance.

For example, depending on your network environment, you might need to configure a static IP address on your NS*v* Series X1 WAN interface. If you do so, you need to configure HTTPS management to allow remote management over the WAN.

The NS*v* Series X0 IP address is 192.168.168.168 by default. If your LAN network uses a different IP address range, then you may want to configure your NS*v* Series X0 IP address with an address in your existing LAN network. This will allow you to manage SonicOS from a computer on your LAN.

The *VMware Remote Console* allows you to log into the NS*v* Series console and use the command line interface (CLI) to configure these network settings.

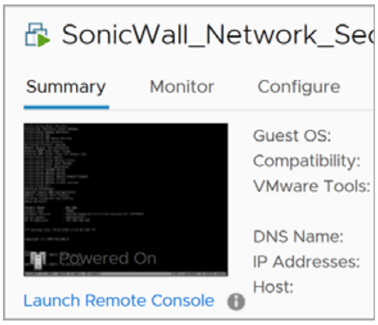
ⓘ **NOTE:** To type within the console window, click your mouse inside the window. To regain control of your mouse, press **Ctrl+Alt**.

To use the console to enable SonicOS management:

1 Log into vSphere or vCenter and select your NS*v* Series instance in the left pane.

2 Do one of the following to open the VMware remote console:

- Click on the image of the console to access the console in browser window.

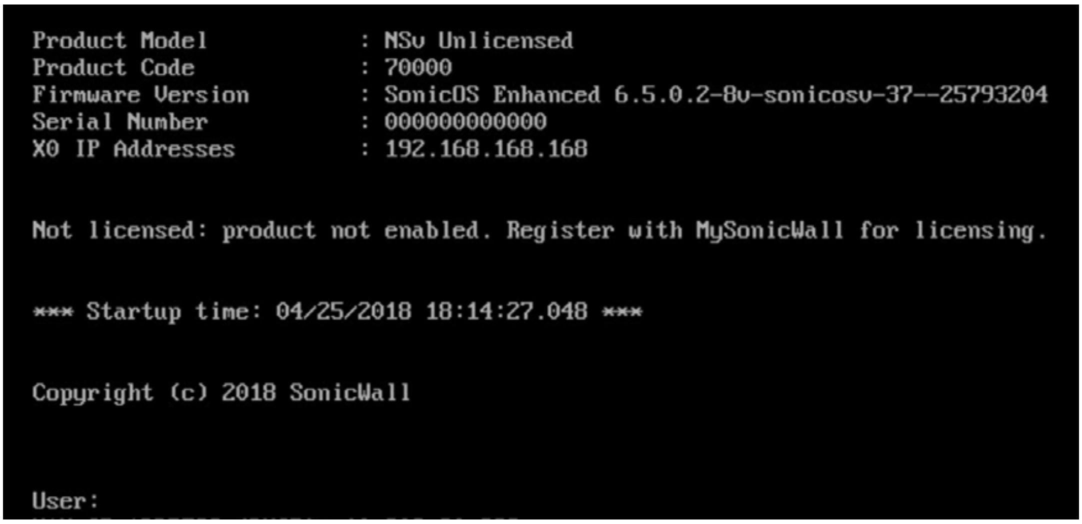


- Click **Launch Remote Console**.
- Click **Actions > Open Remote Console**.

3 Click inside the console window.

> ⓘ **NOTE:** Press **Ctrl+Alt** to regain control of your mouse, or with the browser access method simply move your mouse away from the console area.

4 Log in using the administrator credentials.

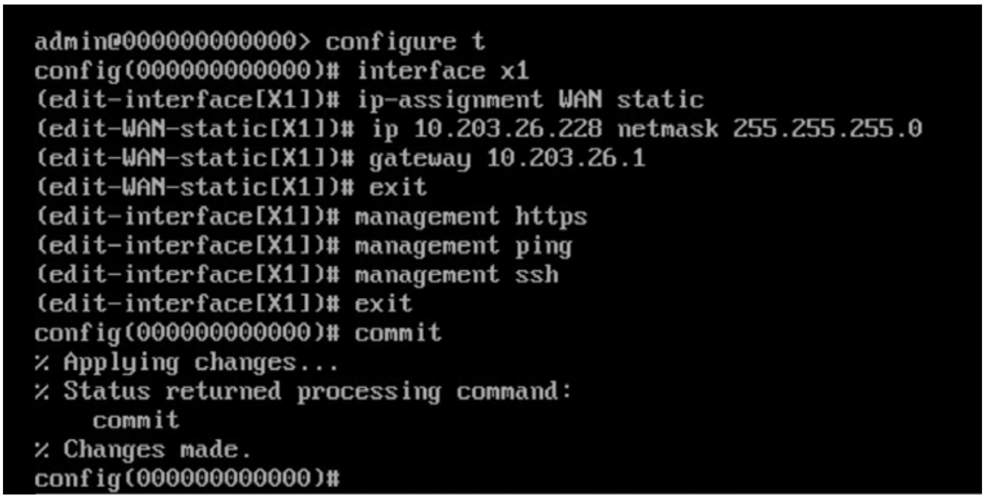


```
Product Model              : NSv Unlicensed
Product Code               : 70000
Firmware Version           : SonicOS Enhanced 6.5.0.2-8v-sonicosv-37--25793204
Serial Number              : 000000000000
X0 IP Addresses            : 192.168.168.168

Not licensed: product not enabled. Register with MySonicWall for licensing.

*** Startup time: 04/25/2018 18:14:27.048 ***

Copyright (c) 2018 SonicWall


User:
```

5 To use a static IP address for the WAN, type the following sequence of commands to enable a static IP and management access on the X1 WAN interface. The command prompt will change as you enter or exit different command levels. This command sequence shown below uses example IP address settings in the 10.203.26.0 network, which should be replaced with the correct settings for your environment.

```
configure t
interface x1
ip-assignment WAN static
ip 10.203.26.228 netmask 255.255.255.0
gateway 10.203.26.1
exit
management https
management ping
management ssh
exit
commit
```

After entering `commit`, the console displays `Applying changes` and other status information, then displays the `config` prompt. Type `exit` to return to the `admin` command level and prompt.

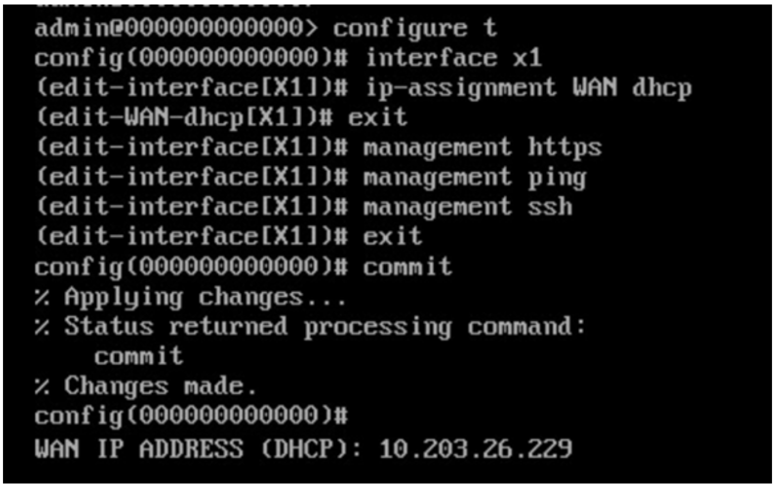


```
admin@000000000000> configure t
config(000000000000)# interface x1
(edit-interface[X1])# ip-assignment WAN static
(edit-WAN-static[X1])# ip 10.203.26.228 netmask 255.255.255.0
(edit-WAN-static[X1])# gateway 10.203.26.1
(edit-WAN-static[X1])# exit
(edit-interface[X1])# management https
(edit-interface[X1])# management ping
(edit-interface[X1])# management ssh
(edit-interface[X1])# exit
config(000000000000)# commit
% Applying changes...
% Status returned processing command:
    commit
% Changes made.
config(000000000000)#
```

6 To return to DHCP for the WAN address, type the following sequence of commands to enable DHCP and management access on the X1 WAN interface. The command prompt will change as you enter or exit different command levels.

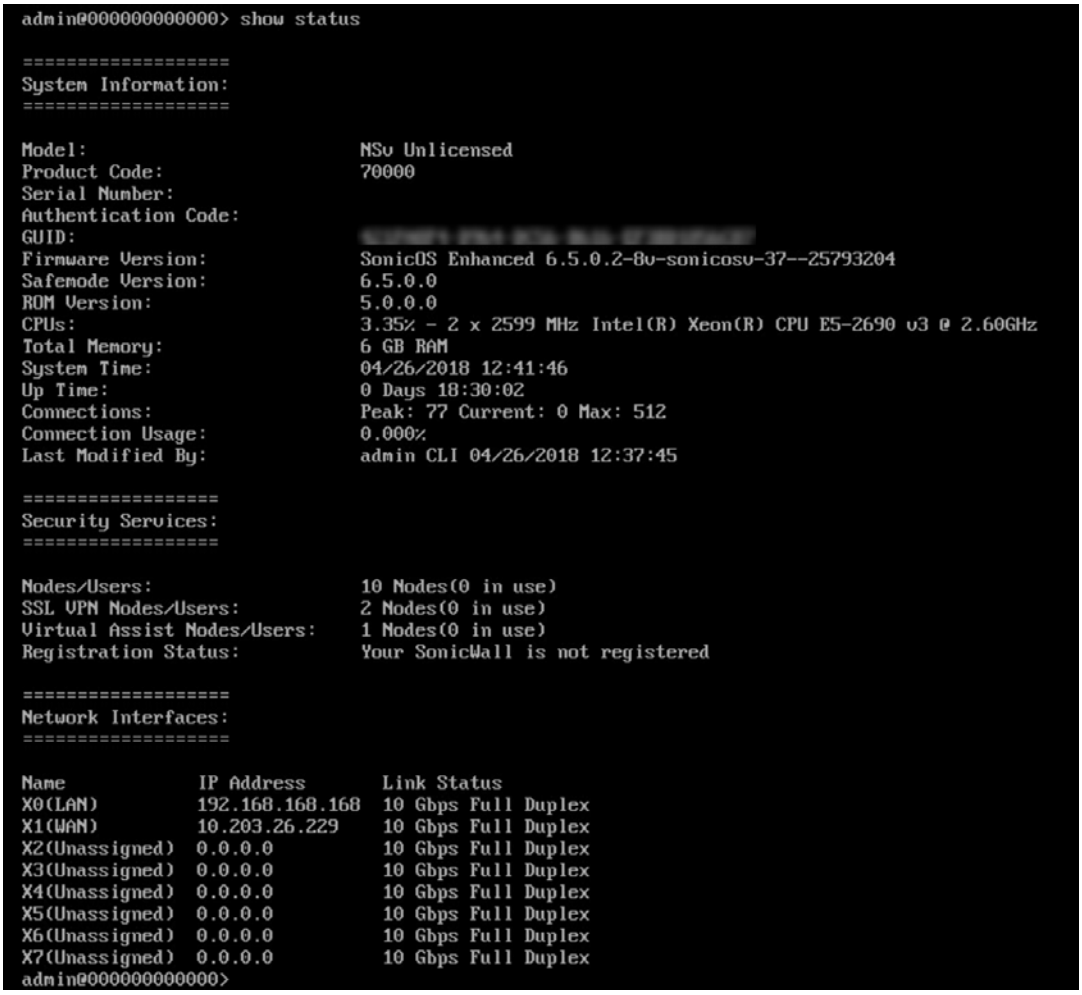
```
configure t
interface x1
ip-assignment WAN dhcp
exit
management https
management ping
management ssh
exit
commit
```

After entering `commit`, the console displays `Applying changes` and other status information, then displays the `config` prompt. After a few seconds, the assigned DHCP address is displayed. You can access the SonicOS web management interface at that address.



```
admin@000000000000> configure t
config(000000000000)# interface x1
(edit-interface[X1])# ip-assignment WAN dhcp
(edit-WAN-dhcp[X1])# exit
(edit-interface[X1])# management https
(edit-interface[X1])# management ping
(edit-interface[X1])# management ssh
(edit-interface[X1])# exit
config(000000000000)# commit
% Applying changes...
% Status returned processing command:
    commit
% Changes made.
config(000000000000)#
WAN IP ADDRESS (DHCP): 10.203.26.229
```

7 You can use the `show status` command at the `admin` prompt to view the assigned IP address for the X1 (WAN) interface and other information.



```
admin@000000000000> show status

===================
System Information:
===================

Model:                         NSv Unlicensed
Product Code:                  70000
Serial Number:
Authentication Code:
GUID:                          [redacted]
Firmware Version:              SonicOS Enhanced 6.5.0.2-8v-sonicosv-37--25793204
Safemode Version:              6.5.0.0
ROM Version:                   5.0.0.0
CPUs:                          3.35% - 2 x 2599 MHz Intel(R) Xeon(R) CPU E5-2690 v3 @ 2.60GHz
Total Memory:                  6 GB RAM
System Time:                   04/26/2018 12:41:46
Up Time:                       0 Days 18:30:02
Connections:                   Peak: 77 Current: 0 Max: 512
Connection Usage:              0.000%
Last Modified By:              admin CLI 04/26/2018 12:37:45

==================
Security Services:
==================

Nodes/Users:                   10 Nodes(0 in use)
SSL VPN Nodes/Users:           2 Nodes(0 in use)
Virtual Assist Nodes/Users:    1 Nodes(0 in use)
Registration Status:           Your SonicWall is not registered

===================
Network Interfaces:
===================

Name            IP Address       Link Status
X0(LAN)         192.168.168.168  10 Gbps Full Duplex
X1(WAN)         10.203.26.229    10 Gbps Full Duplex
X2(Unassigned)  0.0.0.0          10 Gbps Full Duplex
X3(Unassigned)  0.0.0.0          10 Gbps Full Duplex
X4(Unassigned)  0.0.0.0          10 Gbps Full Duplex
X5(Unassigned)  0.0.0.0          10 Gbps Full Duplex
X6(Unassigned)  0.0.0.0          10 Gbps Full Duplex
X7(Unassigned)  0.0.0.0          10 Gbps Full Duplex
admin@000000000000>
```

8 To change the X0 LAN static IP address, use the following commands:

ⓘ **NOTE:** SonicOS HTTPS management is enabled by default on the X0 interface.

For a static IP address in an example 10.10.10.0/24 LAN network, enter:

```
configure t
interface x0
ip 10.10.10.100 netmask 255.255.255.0
exit
exit
commit
```

9 When IP address configuration and management settings are complete, type `restart` to reboot NS*v* Series with the new settings.

ⓘ **NOTE:** Press **Ctrl+Alt** to regain control of your mouse.

After configuring an IP address and enabling management, you can log into SonicOS on your NS*v* Series instance from a browser, or ping the virtual appliance from a command window or other application.

Legend

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

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

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

Last updated: 5/9/19