Integration Guide: SonicOS and Microsoft Hyper-V

May 2019

This document describes how SonicOS-based virtual firewalls can be integrated with Microsoft Hyper-V, a native hypervisor supporting the creation of Virtual Machines on x86-64 systems.

Topics:

About Hyper-V

As a native, or bare-metal, hypervisor, Hyper-V runs directly on the host hardware and manages guest operating systems, in this case, SonicOS 6.5. It allows the creation of a private cloud environment with more efficient use of hardware along with improvements in security, disaster recovery, and backup.

SonicOS 6.5 allows the implementation of NS*v* firewalls on second generation Hyper-V versions 5.0 and higher, which became available with Windows Server 2012 RT.

Requirements

Before installing any SonicOS-based NS*v* firewall on Hyper-V:

- Enable Hyper-V 5.0 or higher available on Windows Server (2012 RT, 2016 and 2019).
- Ensure VM resources meet firewall requirements. Refer to *SonicWall NSv Series on Hyper-V Gettting Started Guide* available at: https://www.sonicwall.com/support/technical-documentation/
- Check release notes acompanying the NSv image (***vhd***) from MySonicWall for additional requirements.

Configuring Hyper-V

Before installing SonicOS:

- Enable Hyper-V on Windows Server
- Configure Virtual Switches in Hyper-V

Enable Hyper-V on Windows Server

Before enabling Hyper-V on Windows Server, make sure the Windows software is up-to-date.

For more details on enabling Hyper-V in a Windows Server environment, refer to the instructions at: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server

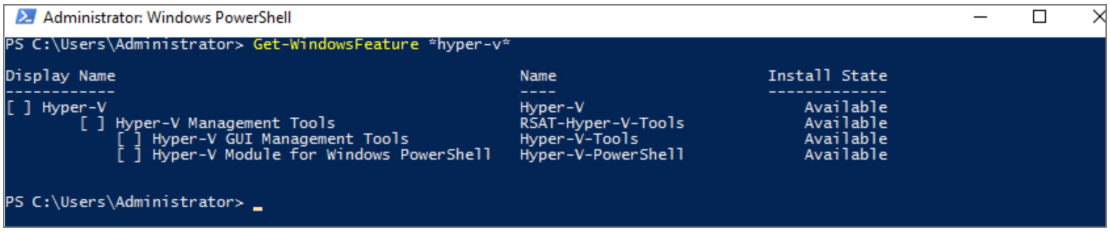
To enable Hyper-V on Windows Server:

1 Start Windows PowerShell as Administrator and run the following command:

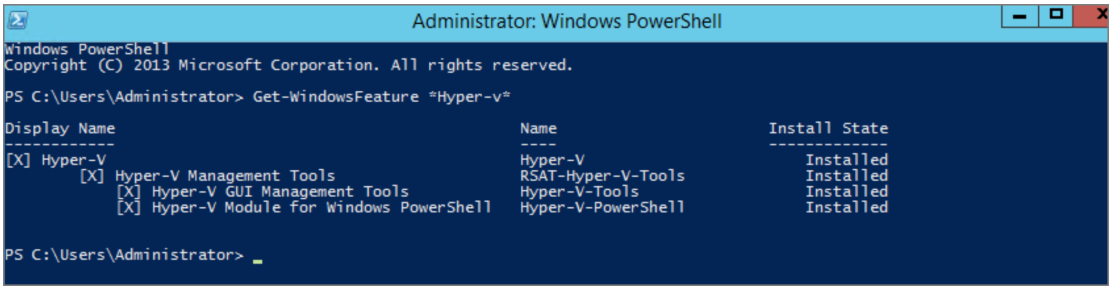
```
Code Block | language = powershell | title = Verify if Hyper-V is installed | linenumbers = true | f...

Get-WindowsFeature *Hyper-v*
```

If Hyper-V is not installed the system shows the installable Hyper-V components:



If Hyper-V is installed the system shows which Hyper-V components are enabled:



2 Install any tools you need and restart the system:

```
Code Block | language = powershell | title = Install Hyper-V | linenumbers = true | firstline = 1.

Install-WindowsFeature -Name HyperV -IncludeManagementTools -restart
```

Configure Virtual Switches in Hyper-V

Microsoft Hyper-V allows you to create three types of virtual switches (vSwitches):

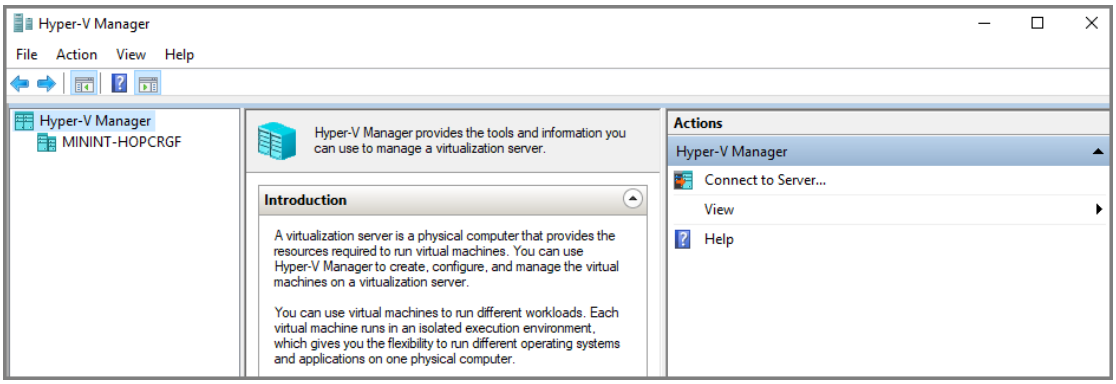
- **External vSwitch** – binds to a physical network adapter and provides the vSwitch access to a physical network.
- **Internal vSwitch** – passes traffic between the virtual machines and the Hyper-V host. This type of vSwitch does not provide connectivity to a physical network.
- **Private vSwitch** – passes traffic between the virtual machines on the Hyper-V host only.

For an NS*v* Series Hyper-V deployment, an ***External vSwitch*** is required to provide connectivity for NS*v* management access and for routing traffic to and from the network devices that the firewall is securing (e.g. LAN or DMZ side devices).

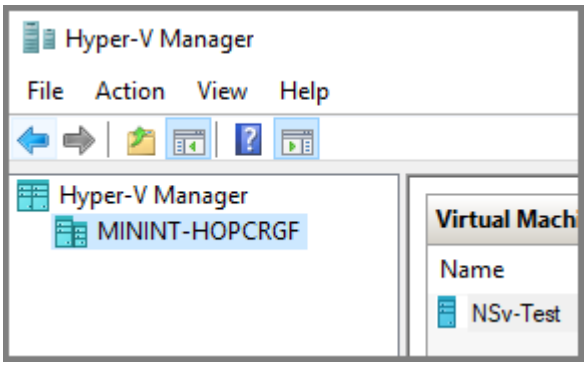
An Internal vSwitch or Private vSwitch is required when the virtual machines that the firewall is securing (e.g. LAN or DMZ side VM) are created in the same Hyper-V server. The difference between an Internal vSwitch and a Private vSwitch is whether to allow traffic between the NS*v* and the Hyper-V host (via Internal vSwitch or, between the NS*v* and other virtual systems running under Hyper-V (via Private VSwitch).

To create an External vSwitch:

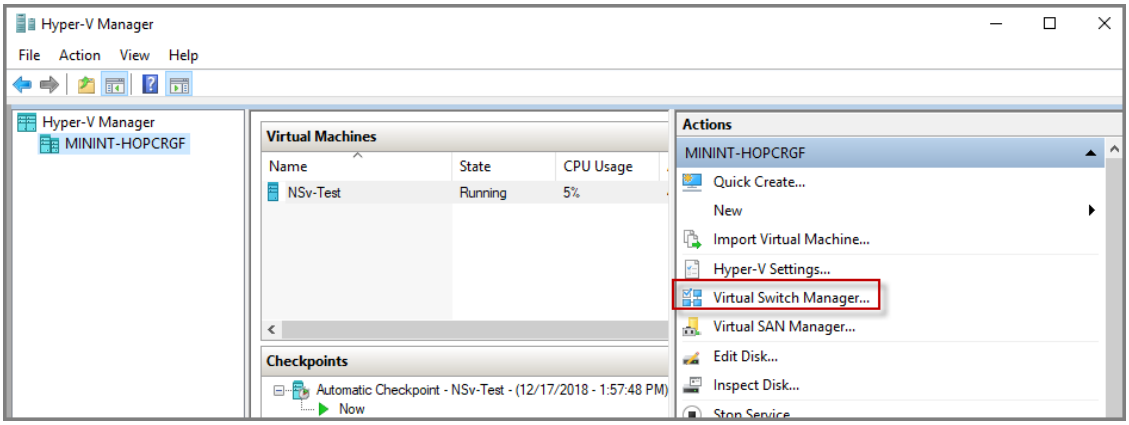
1 Open the **Hyper-V Manager** tool.



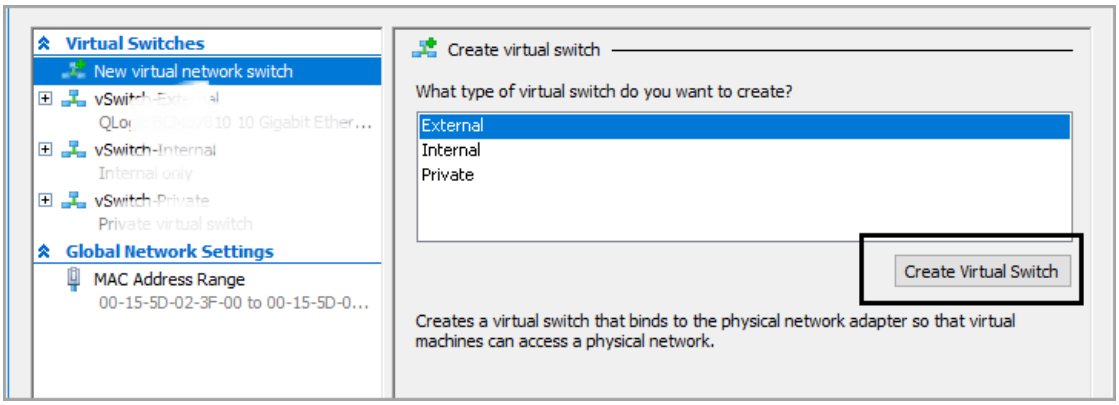
2 To bring up the detailed **Actions** panel, click on the Hyper-V designation in the upper left and then double-click on the name that appears under it.



3 Select **Virtual Switch Manager**.



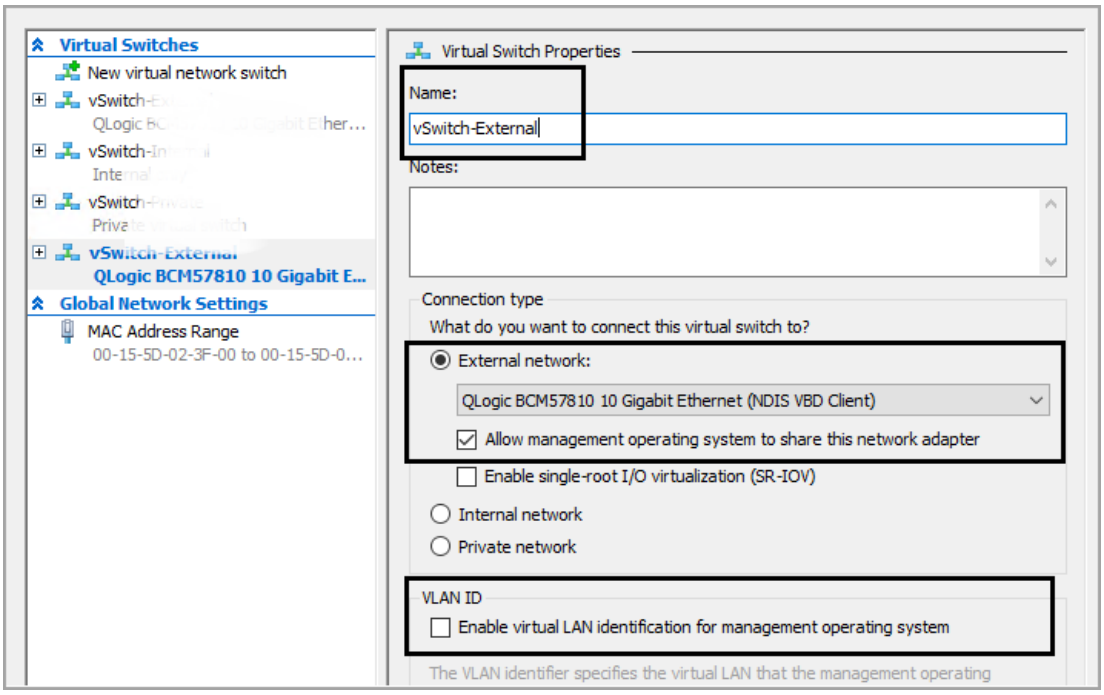
4 Select **External** for the type of virtual switch and then click the **Create Virtual Switch** button.



5 Under **Virtual Switch Properties**, type a descriptive name for the switch into the **Name** field.

6 For **Connection Type**, select **External network** and select the physical network adapter that connects to the external vSwitch from the drop-down list.

7 If you want to use this same physical adapter to manage the Hyper-V host at the same time, select the **Allow management operating system to share this network adapter** check box.



NOTE: If you choose the **Allow management operating system to share this network adapter** option, then specify the VLAN ID that is used for this management traffic. If the VLAN ID is not configured, the management traffic will be untagged.

Always make sure to isolate the Hyper-V management traffic from the NS*v* traffic by using a different VLAN ID.

8 Repeat Step 4 through Step 7 to create more External vSwitches. These can be used to route NS*v* traffic when there are additional physical connections between the Windows Server and the external switch.

If your NS*v* protects virtual machines (LAN or DMZ side VM) located in the same Hyper-V server, perform the next procedure to create an Internal vSwitch or Private vSwitch.

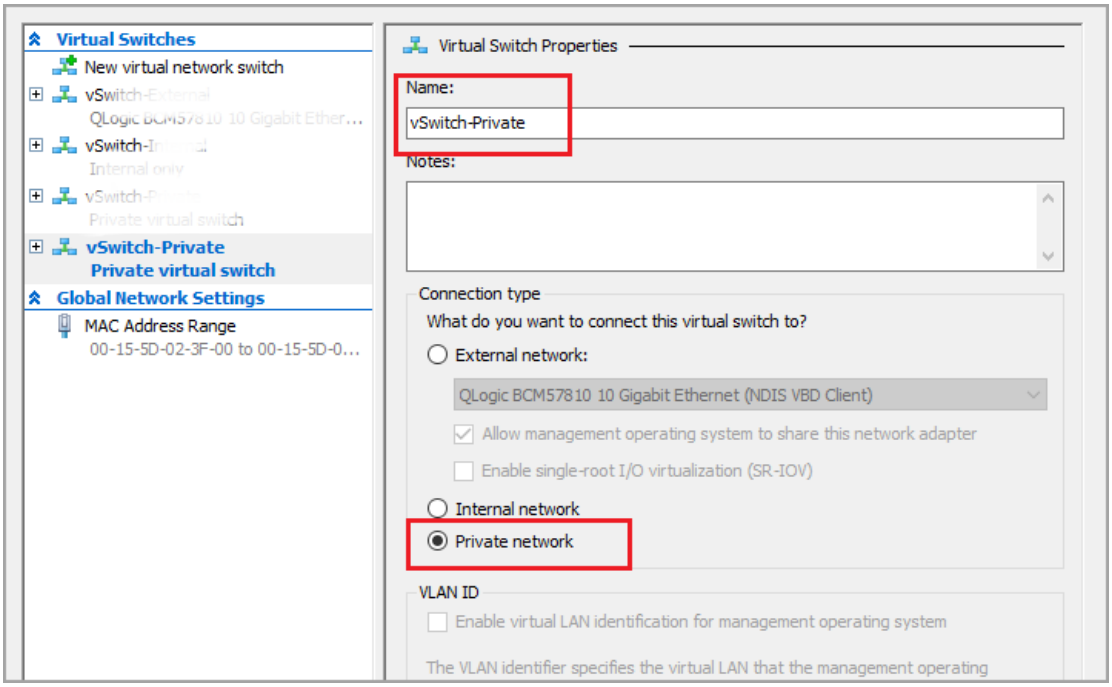
To create an Internal or Private vSwitch:

1 On the **Action** tab of the **Hyper-V Manager** tool, select **Virtual Switch Manager**.

2 Select **Internal** or **Private** for the type of virtual switch and then click the **Create Virtual Switch** button.

3 Under **Virtual Switch Properties**, type a descriptive name for the switch into the **Name** field.

4 For **Connection Type**, select **Internal network** or **Private network**.

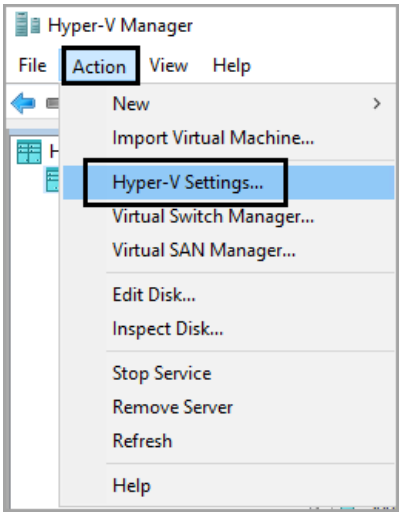


Configuring SonicWall NS$_v$ Firewalls

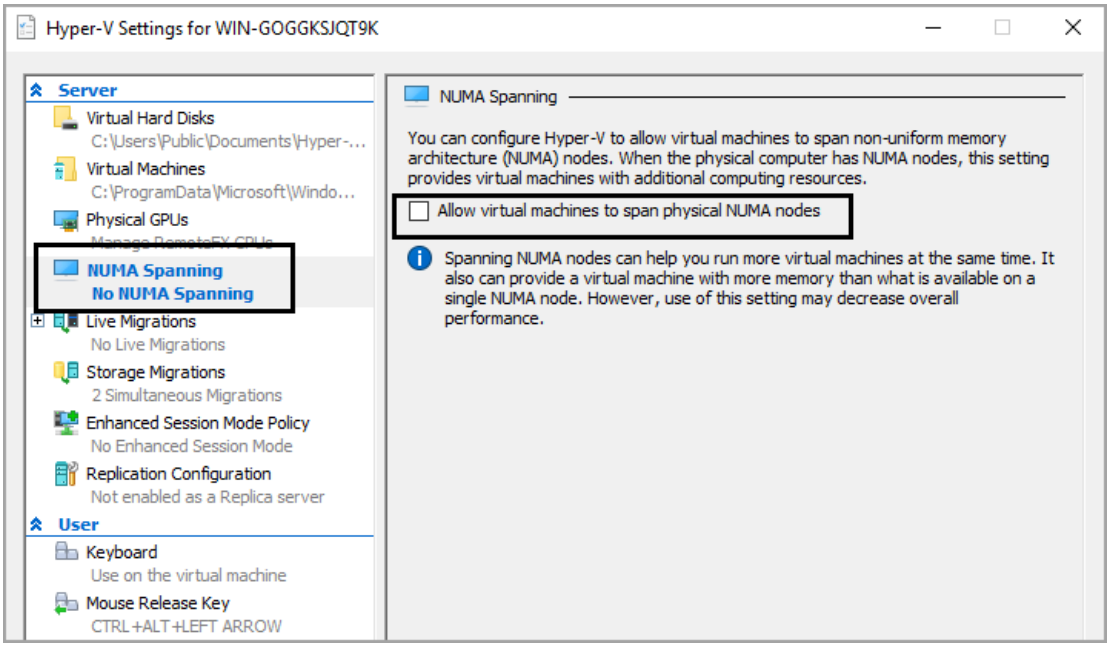
To install NSv on Hyper-V:

1 Download the NS*v* firewall ***vhd*** file to a local folder in the Windows Server system.

2 In the **Hyper-V Manager** window, click **Action** and select **Hyper-V Settings**.

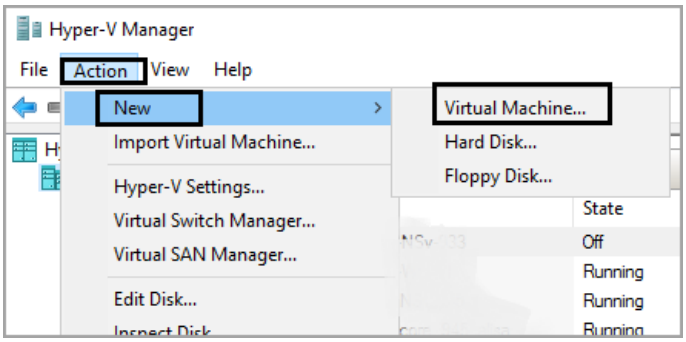


3 Clear the **Allow virtual machines to span physical NUMA nodes** option.



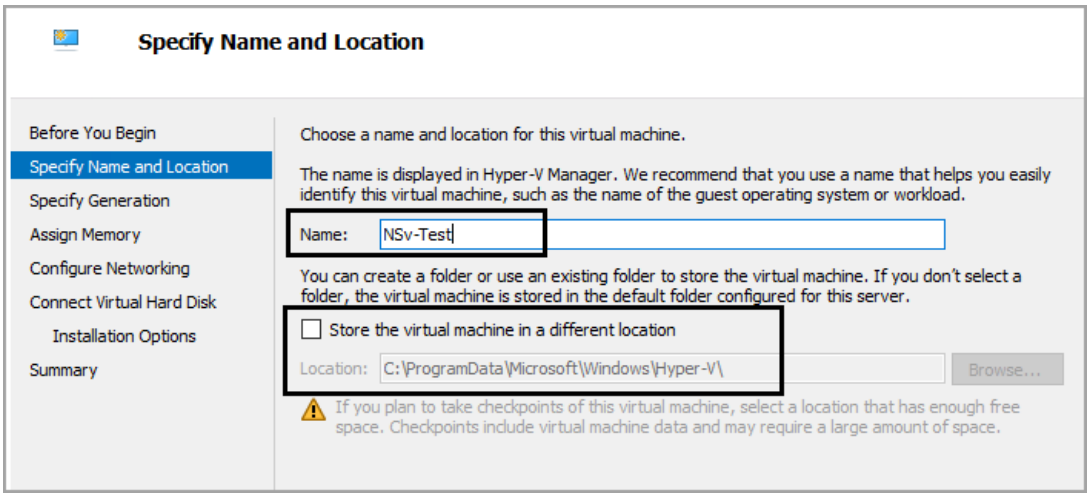
NOTE: After clearing the **Allow virtual machines to span physical NUMA nodes** option, the Hyper-V Virtual Machine Management service must be restarted to apply the change. To restart the service, select **Action > Stop Service**, then select **Action > Start Service** in the Hyper-V Manager.

4 Create a virtual machine by click **Action > New > Virtual Machine**.



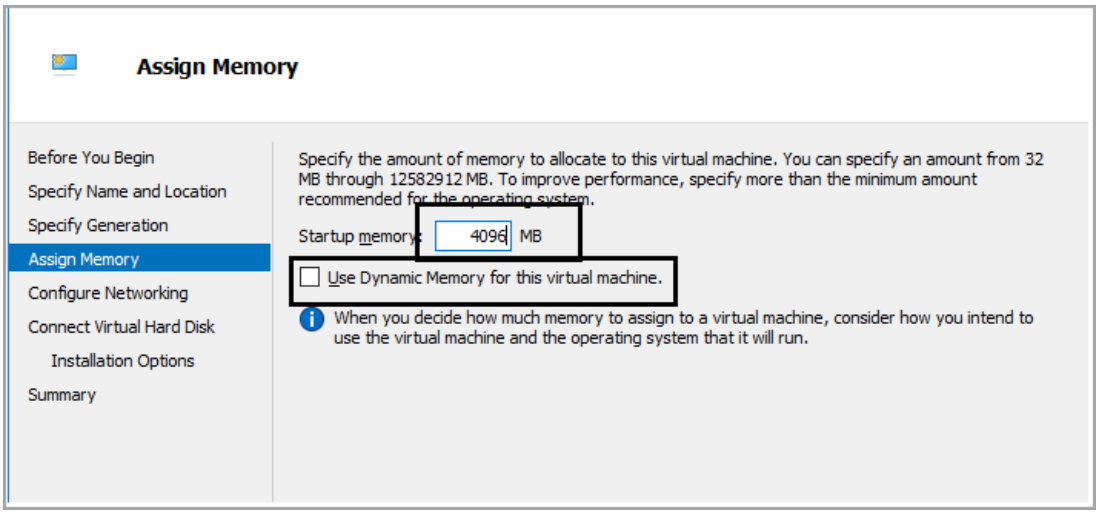
5 Type a descriptive name for the NS*v* VM into the **Name** field.

6 To use a location other than the default location to store VM files, select the **Store the virtual machine in a different location** check box and enter a different location into the **Location** field.



7 In the **Specify Generation** screen, select **Generation 1**. This is the default option and the only version supported.

8 In the **Assign Memory** screen, assign the memory based on the NSv system requirements of your NSv Series Hyper-V model. In general, 4096 MB is the minimum required.

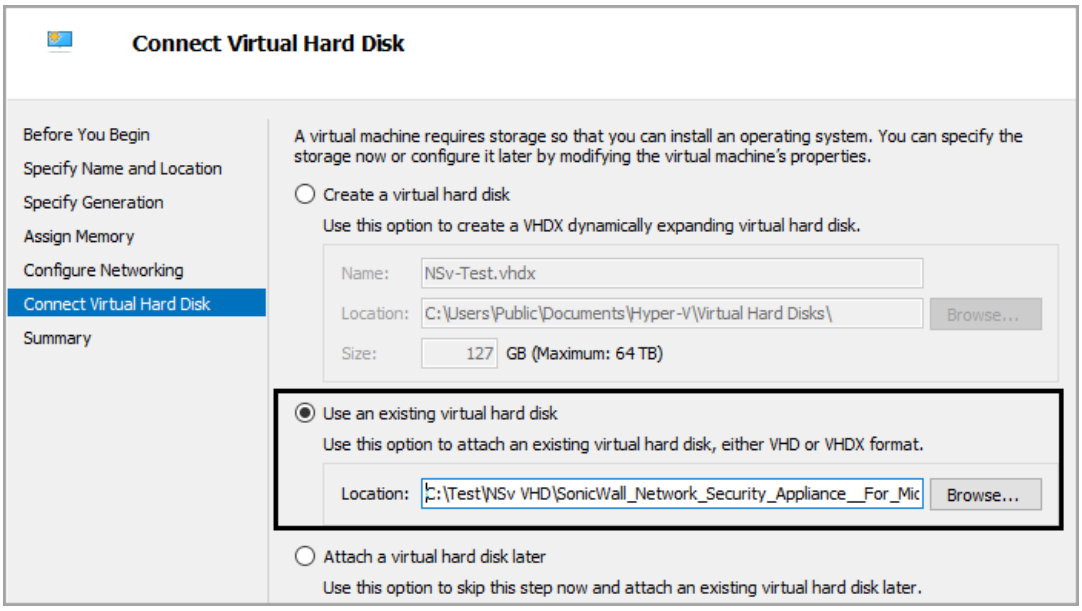


NOTE: Do not select the **Use Dynamic Memory for this virtual machine** option; the NSv Series Hyper-V does not support this function.

9 In the **Configure Networking** screen, since this is the first network interface to be mapped to X0 in the NSv, do one of the following:

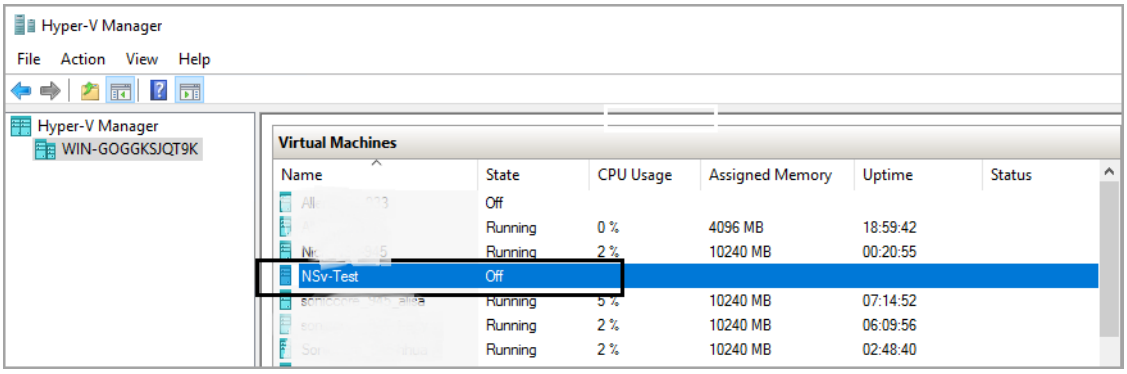
- Select your Private vSwitch if your LAN (X0) side network devices are virtual machines located in the same Hyper-V host.
- Select your External vSwitch if your LAN (X0) side network devices are located external to the Hyper-V host.

10 In the **Connect Virtual Hard Disk** screen, select the **Use an existing virtual hard disk** option and set the **Location** field to the folder where you downloaded the NS*v* ***vhd*** file in Step 1.



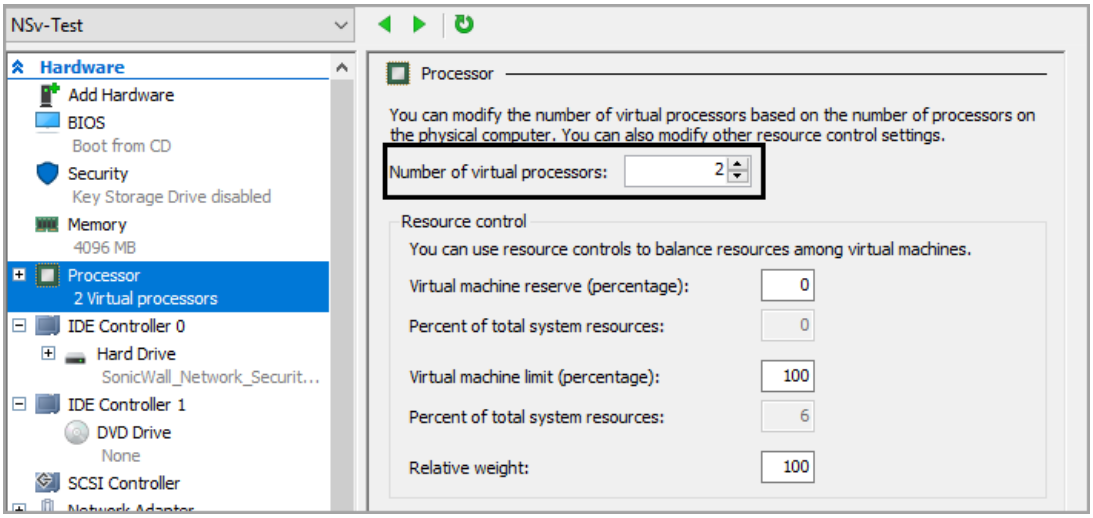
11 Review the summary and click **Finish**.

12 Check the created NS*v* VM in the Hyper-V Manager tool. The VM is ***Off*** by default.

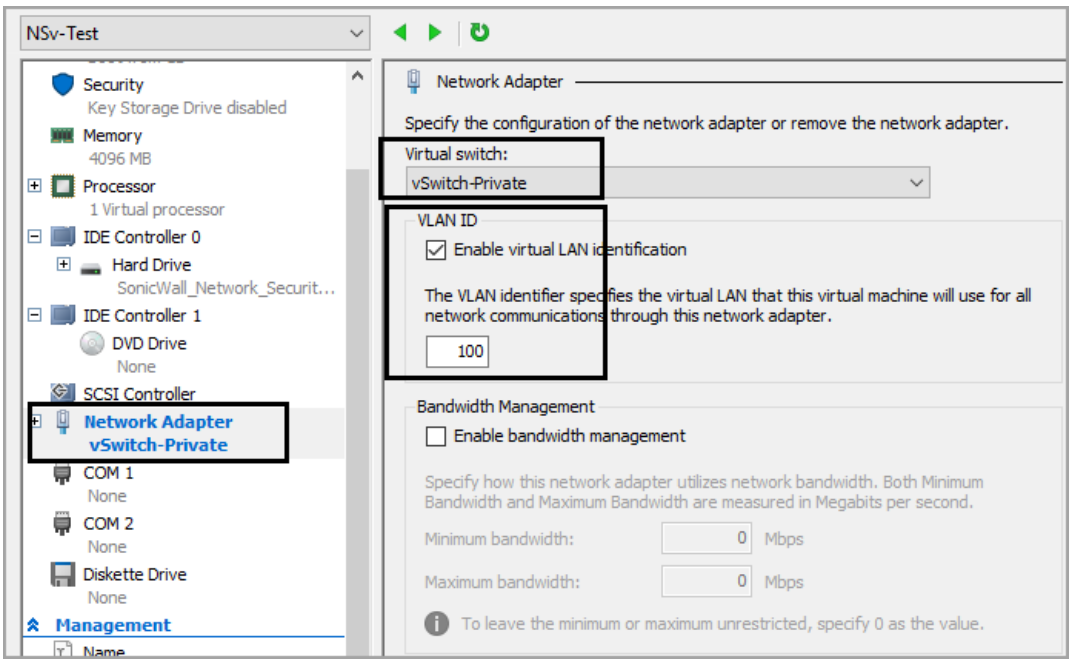


13 Right-click the NS*v* VM and select **Settings** to open the **Edit Settings** page.

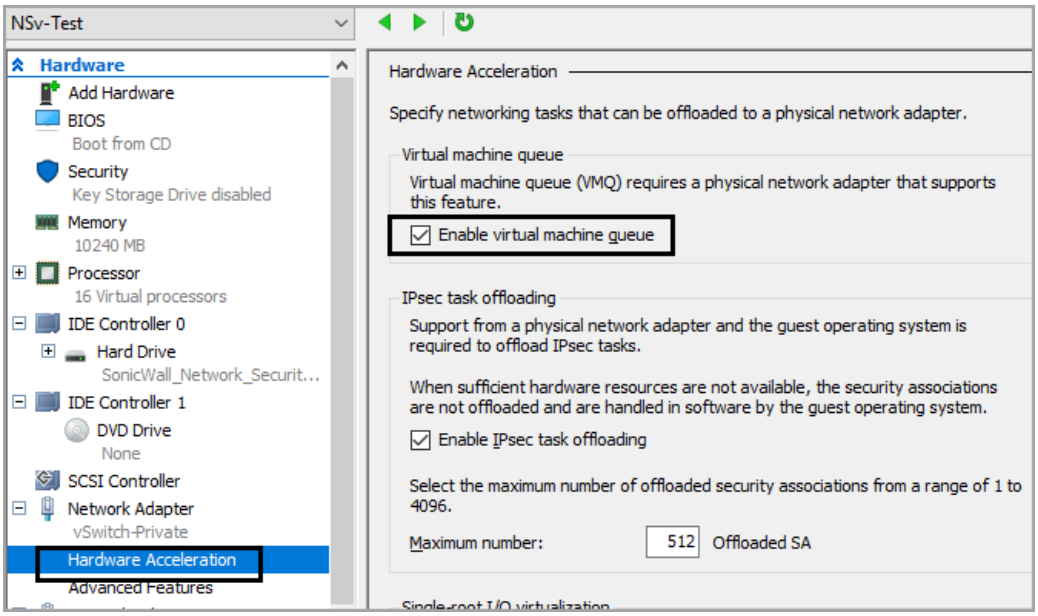
14 Configure the **Number of virtual processors** field based on the NS*v* system requirements of your NS*v* Series Hyper-V model. This is the CPU core number. In general, 2 cores are the minimum required.



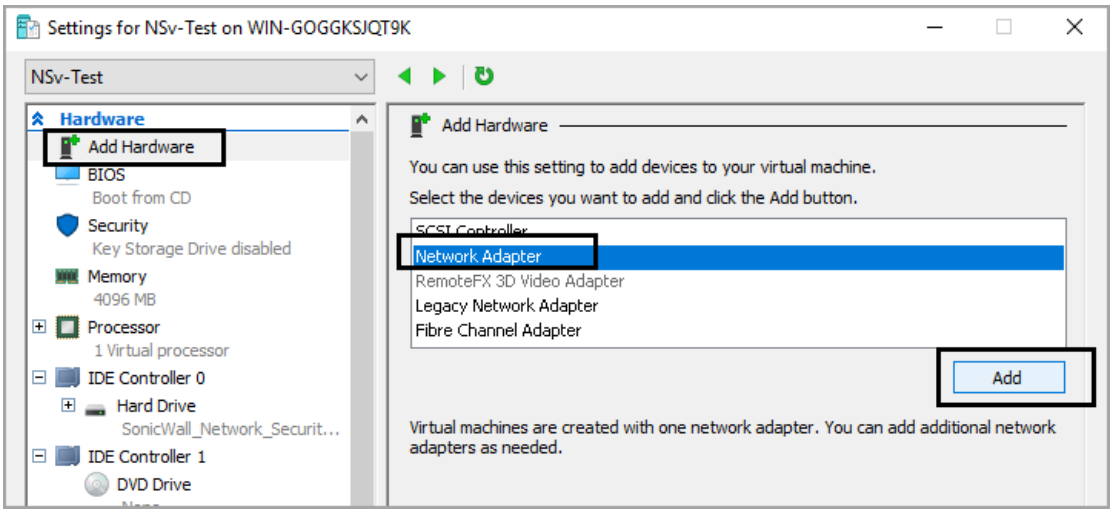
15 Configure the network adapter. The first network adapter is mapped to X0 in the NSv. Configure the vSwitch and VLAN ID which match the network settings in your LAN (X0) side network devices, as configured in Step 9.



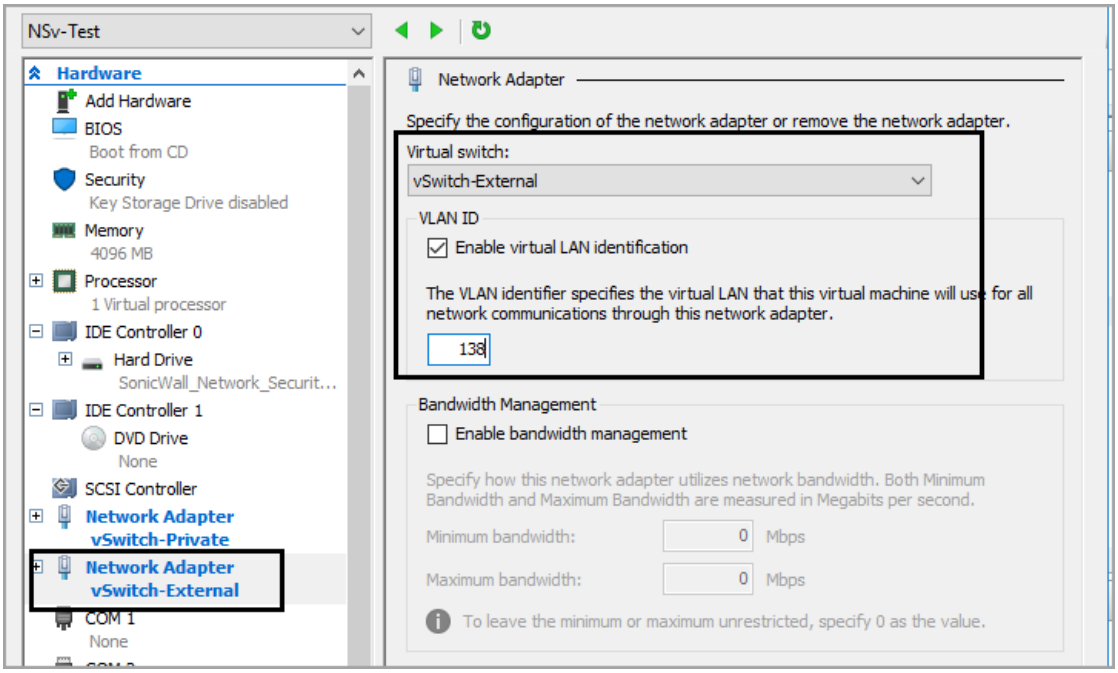
16 Configure the advanced settings of the network adapter. In the **Hardware Acceleration** screen (see below), select the **Enable virtual machine queue** option (enabled by default). This option can improve the NSv firewall performance.



17 To add more network adapters for the NSv, click **Add Hardware** (see below) and select **Network Adapter**, then click **Add**.

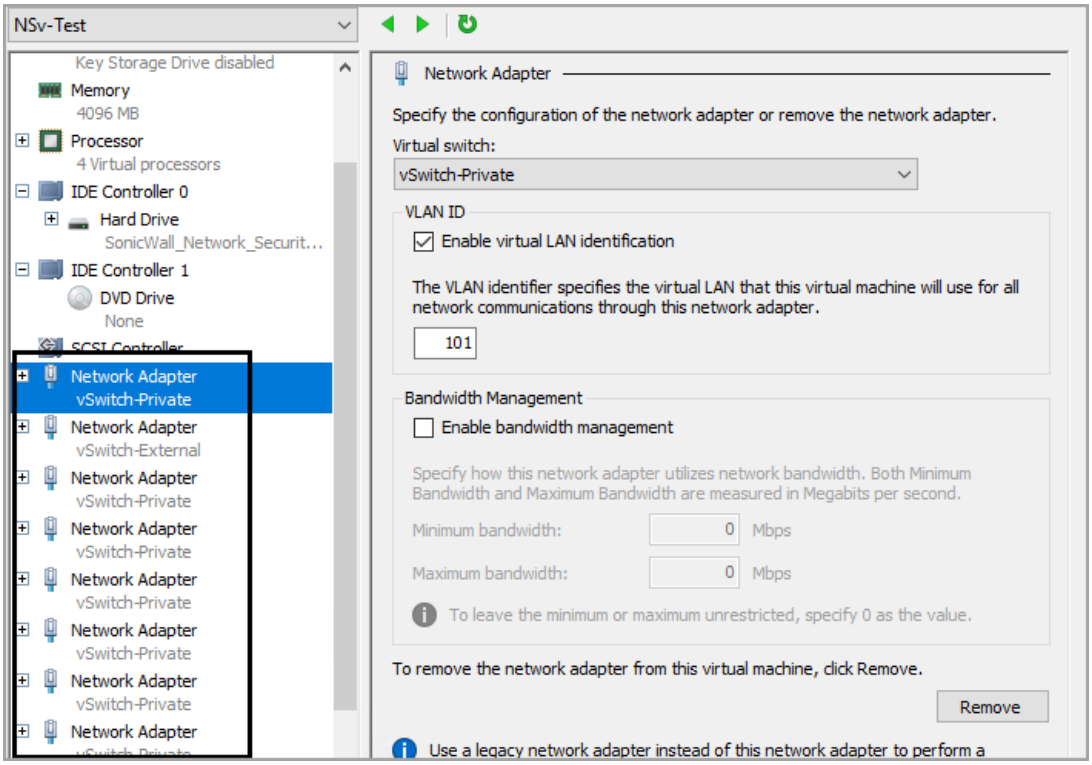


18 Map your second network adapter to X1 (default WAN), which should use an External vSwitch. For the VLAN ID, select **Enable virtual LAN identification** and enter the VLAN ID of the VLAN that connects to the internet via the external switch.



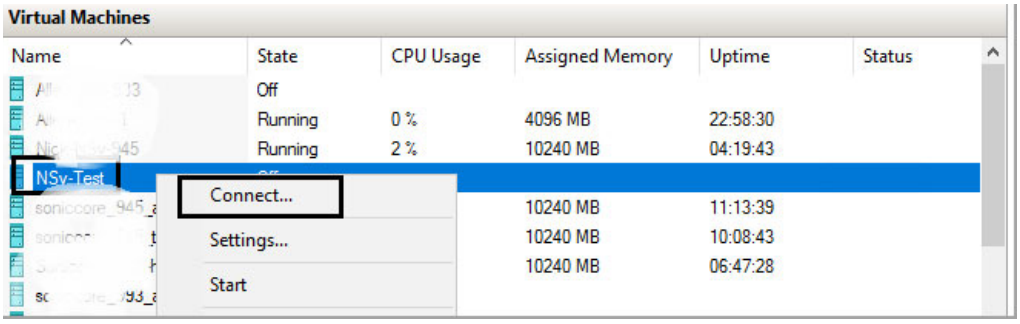
19 Add more network adapters with a mapping sequence from X2-X7 for a maximum of 8 (X0-X7).

NOTE: It is not required to have all eight adapters. SonicOS runs with a minimum of two network adapters configured.



20 Click **OK** when finished adding network adapters.

21 In the Hyper-V Manager tool, right-click your NS*v* and select **Connect** to open the NS*v* console window.



22 Click the **Power On** button to boot up SonicCore and SonicOS.

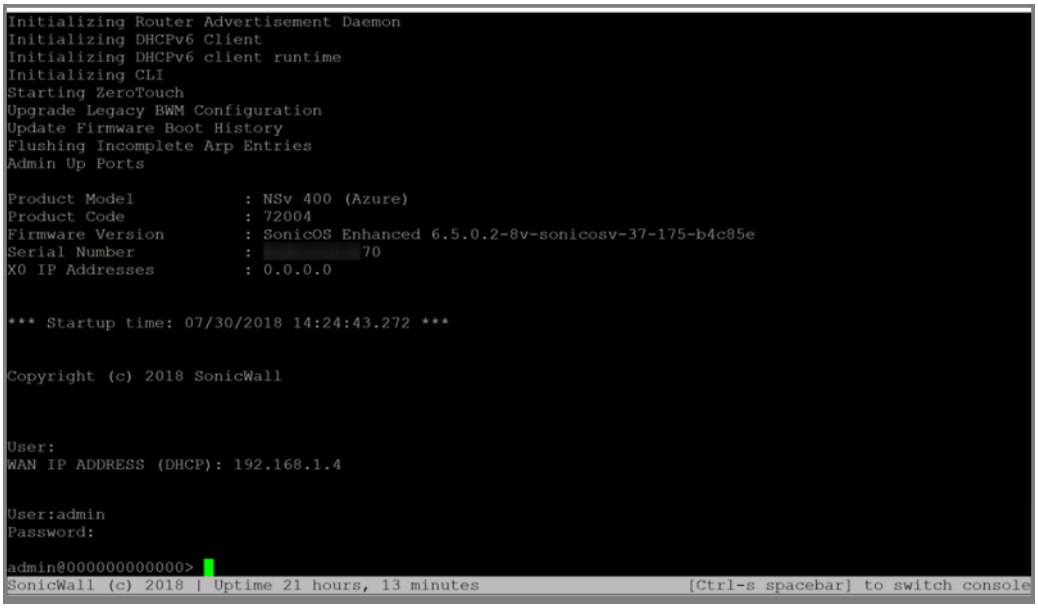
You are now ready to register your NS*v* and proceed with SonicOS management.

Testing Your Integration

Once your NS*v* firewall is running, you can take the following steps to access the Management Console.

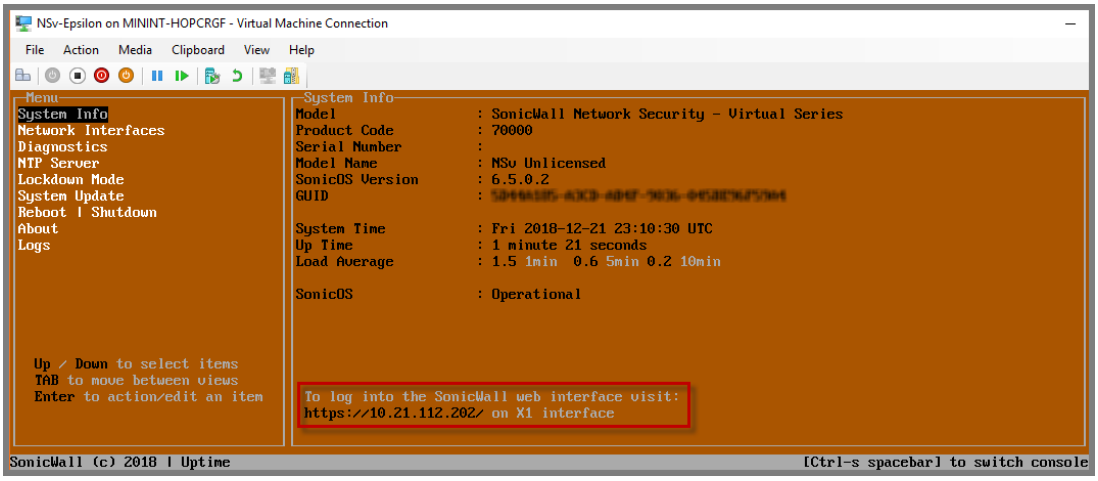
To access the Management Console:

1 Wait for the NS*v* to boot to the command line in the **Hyper-V Virtual Machine Connection** window and then log in as ***admin*** with the password: ***password***.

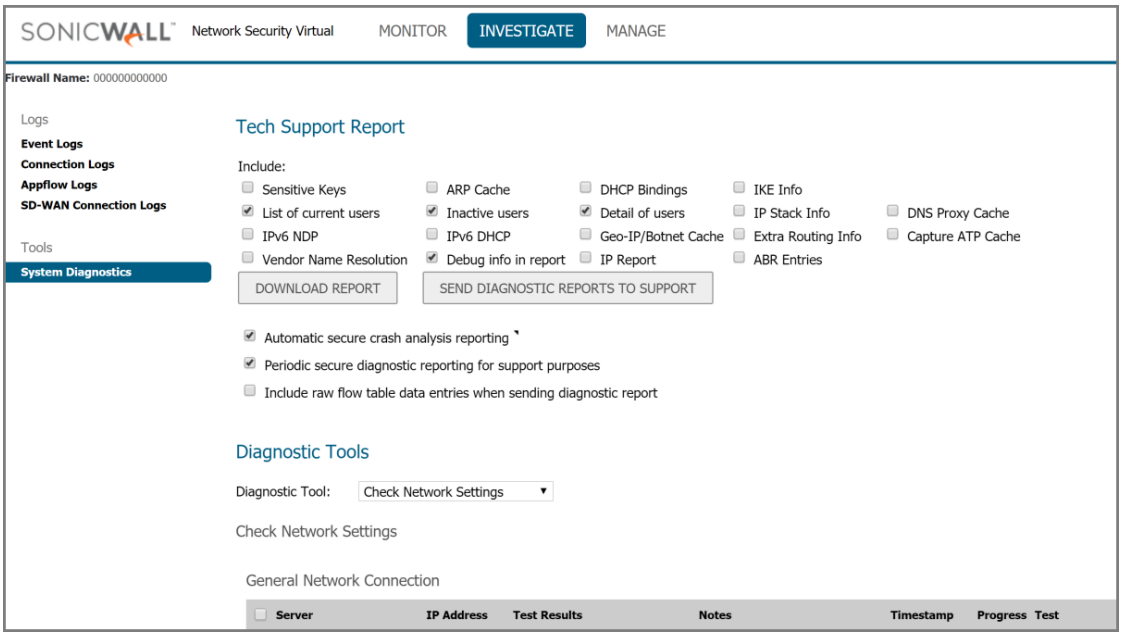


2 Press **Ctrl+s** and then press the **spacebar** to toggle between the SSH virtual console or Hyper-V Virtual Machine Connection console and the NS*v* management console. That is, press the **Ctrl** key and '**s**' key together, then release and press the **spacebar**.

3 Once the Management Console appears, note the X1 web interface address as shown below:



4 Enter this IP address into a browser to get to the NSv management interface. Then navigate to The **Tools | System Diagnostics** page on the **INVESTIGATE** view:



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. This to helps 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:

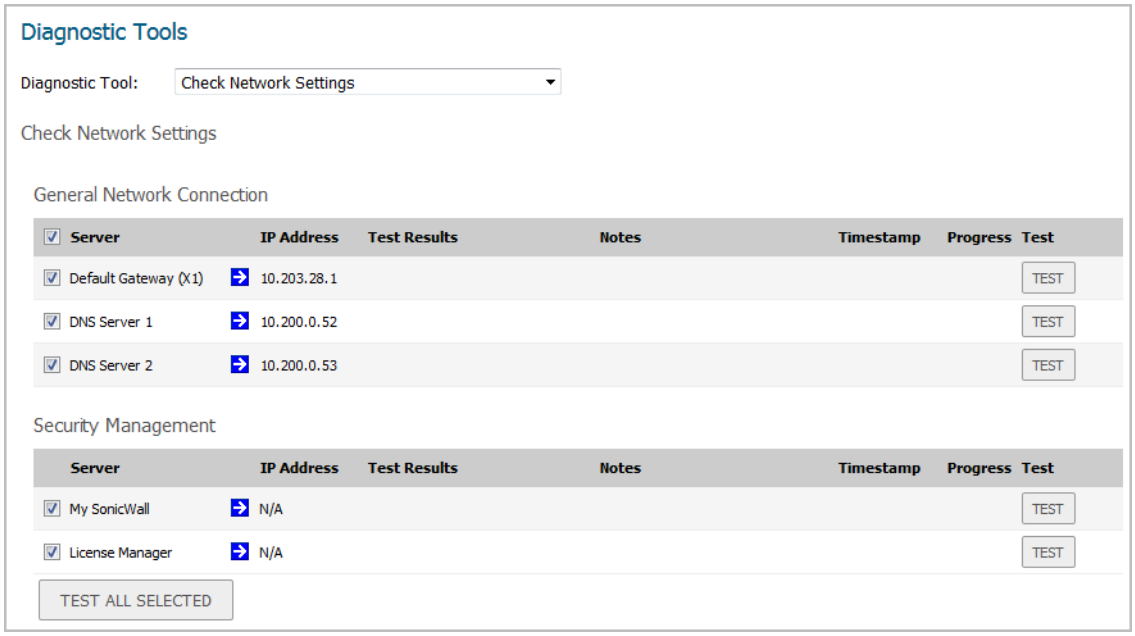
Button	Function
ACCEPT	Saves any changes you made to the diagnostic support report or diagnostic tool.
CANCEL	Cancels any changes you initially made to the diagnostic support report or diagnostic tool.
REFRESH	Refreshes the data being displayed in the **Diagnostic Tools** section.

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 (look for NS*v* documentation at https://www.sonicwall.com/support/technical-documentation/) for complete information about the available diagnostic tools.

Check Network Settings



Check Network Settings is a diagnostic tool that automatically checks the network connectivity and service availability of several pre-defined functional areas of the NS*v* Series Hyper-V. This diagnostic tool returns the results, and attempts to describe the causes of any detected exceptions. 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 Filtering test), a corresponding Network Monitor Policy appears on the **Tools | Network Probes** page, with a special diagnostic tool policy name in the form:

```
diagTestPolicyAuto_<IP_address/Domain_name>_0
```

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

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

To test multiple items at the same time, select the **Server** checkbox at the top of the table to choose 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.

References

At the SonicWall technical documentation portal (https://www.sonicwall.com/support/technical-documentation/), enter **NSv series** as the product and enter your model number. A link to the Getting Started Guide appears:

- ***SonicWall NSv Series on Hyper-V Getting Started Guide***

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: 5/29/19