



CHAPTER 3

Installing the Cisco Virtual Security Gateway

This chapter describes how to install and complete the basic configuration of the Cisco Virtual Security Gateway (VSG) for Cisco Nexus 1000V Series switch software.

This chapter includes the following sections:

- [Information About the Cisco VSG, page 3-1](#)
- [Prerequisites to Installing Cisco VSG Software, page 3-3](#)
- [Obtaining the Cisco VSG Software, page 3-3](#)
- [Installing the Cisco VSG Software, page 3-3](#)
- [Configuring Initial Settings, page 3-7](#)
- [Verifying the Cisco VSG Configuration, page 3-10](#)
- [Where to Go Next, page 3-11](#)

Information About the Cisco VSG

This section describes the Cisco VSG and includes the following topics:

- [Host and VM Requirements, page 3-1](#)
- [Cisco Virtual Security Gateway and Supported Cisco Nexus 1000V Series Switch Terminology, page 3-2](#)

Host and VM Requirements

The Cisco VSG has the following requirements:

- ESX or ESXi platform running VMware software release 4.1 or 5.0 and requiring a minimum of 4GB physical RAM to host a Cisco VSG VM
- Virtual Machine (VM)
 - 32-bit VM is required and “Other 2.6.x (32-bit) Linux” is a recommended VM type.
 - 1 processor
 - 2-GB RAM
 - 3 NICs (1 of type VMXNET3 and 2 of type E1000)
 - Minimum 3-GB SCSI hard disk with LSI Logic Parallel adapter (default)

[Send document comments to vsg-docfeedback@cisco.com](mailto:vsg-docfeedback@cisco.com)

- CPU speed of 1.5 GHz

Cisco Virtual Security Gateway and Supported Cisco Nexus 1000V Series Switch Terminology

Table 3-1 lists the terminology is used in the Cisco Virtual Security Gateway implementation.

Table 3-1 Cisco Virtual Security Gateway Terminology

Term	Description
Distributed Virtual Switch (DVS)	Logical switch that spans one or more VMware ESX servers. It is controlled by one VSM instance.
ESX/ESXi	Virtualization platform used to create the virtual machines as a set of configuration and disk files that together perform all the functions of a physical machine.
NIC	Network interface card.
Open Virtual Appliance or Application (OVA) file	Package that contains the following files used to describe a virtual machine and saved in a single archive using .TAR packaging: <ul style="list-style-type: none"> • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Open Virtual Machine Format (OVF)	Platform-independent method of packaging and distributing virtual machines.
vCenter Server	Service that acts as a central administrator for VMware ESX/ESXi hosts that are connected on a network. vCenter Server directs actions on the virtual machines and the virtual machine hosts (the ESX/ESXi hosts).
Virtual Ethernet Module (VEM)	Part of the Cisco Nexus 1000V Series switch that switches data traffic. It runs on a VMware ESX host. Up to 64 VEMs are controlled by one VSM. All the VEMs that form a switch domain should be in the same virtual data center as defined by VMware vCenter Server.
Virtual Machine (VM)	Virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same host system concurrently.
vMotion	Practice of migrating virtual machines live from server to server. (The Cisco VSGs cannot be moved by vMotion.)
vPath	Component in the Cisco Nexus 1000V Series switch VEM that directs the appropriate traffic to the Cisco VSG for policy evaluation. It also acts as fast path and can short circuit part of the traffic without sending it to the Cisco VSG.
Virtual Security Gateway (VSG)	Cisco software that secures virtual networks and provides firewall functions in virtual environments using the Cisco Nexus 1000V Series switch by providing network segmentation.
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000V Series distributed virtual switch that runs on a virtual machine (VM) and is based on Cisco NX-OS.
vSphere Client	User interface that enables users to connect remotely to the vCenter Server or ESX/ESXi from any windows PC. The primary interface for creating, managing, and monitoring virtual machines, their resources, and their hosts. It also provides console access to virtual machines.

Send document comments to vsg-docfeedback@cisco.com

Prerequisites to Installing Cisco VSG Software

The Cisco VSG has the following prerequisites:

The following components must be installed and configured:

- On the Cisco Nexus 1000V Series switch, configure two VLANs, a service VLAN, and an HA VLAN on the switch uplink ports. (The VLAN does not need to be the system VLAN.)
- On the Cisco Nexus 1000V Series switch, configure two port profiles for the Cisco VSG: one for the service VLAN and the other for the HA VLAN. (You will be configuring the Cisco VSG IP address on the Cisco VSG so that the Cisco Nexus 1000V Series switch can communicate with it.)

Details about configuring VLANs and port profiles on the Cisco Nexus 1000V Series switch are available in the Cisco Nexus 1000V Series switch documentation.

Obtaining the Cisco VSG Software

You can obtain the Cisco VSG software files at this URL:

http://www.cisco.com/en/US/products/ps13095/tsd_products_support_series_home.html

Installing the Cisco VSG Software

You can install the Cisco VSG software on a virtual machine (VM) by using an open virtual appliance (OVA) file or an ISO image file from the CD. Depending upon the type of file that you are installing, use one of the installation methods described in the following topics:

- [Installing the Cisco VSG Software from an OVA File, page 3-3](#)
- [Installing the Cisco VSG Software from an ISO File, page 3-6](#)

Installing the Cisco VSG Software from an OVA File

To install the Cisco VSG software from an OVA file, obtain the OVA file and either install it directly from the URL or copy the file to the local disk from where you connect to the vCenter Server.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- A name for the new Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- The name of the host where the Cisco VSG will be installed in the inventory folder.
- The name of the datastore in which the VM files will be stored.
- The names of the network port profiles used for the VM.
- The Cisco VSG IP address.
- Mode in which you will be installing the Cisco VSG:
 - Standalone
 - HA Primary

Send document comments to vsg-docfeedback@cisco.com

- HA Secondary
- Manual Installation

PROCEDURE

-
- Step 1** From the vSphere Client menu, choose the data center where you want to install the OVA file for the Cisco VSG.
- Step 2** Choose **File > Deploy OVF Template**.
The Source dialog box opens.
- Step 3** Click the **Deploy from file** radio button to browse and choose the location of the OVA file on the local disk.
- Step 4** Click **Next**.
The OVF Template Details dialog box opens displaying product information, including the size of the file and the size of the VM disk.
- Step 5** Click **Next**.
The End User License Agreement dialog box opens.
- Step 6** Read the End User License Agreement.
- Step 7** Click **Accept** and then click **Next**.
The Name and Location dialog box opens.
- Step 8** In the Name field, enter a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- Step 9** From the Select a datastore in which to store the VM files pane, choose your datastore and click **Next**.
The Deployment Configuration window opens.
- Step 10** In the Configuration field, you will be presented with four options:
- Standalone
 - HA Primary
 - HA Secondary
 - Manual Installation
- For this example, choose **Standalone** and click **Next**.
The Disk Format dialog box opens.
-
-  **Note** We are using the Standalone installation for this document as an example. If you chose Manual Installation mode, you would choose the default values for the following steps.
-
-  **Note** In Standalone mode, be sure to fill in all the fields indicated below (they will be indicated on the GUI with red type).
-
- Step 11** From the Select a format in which to store the virtual machines virtual disks, click the radio button for the format you choose and click **Next**.

Send document comments to vsg-docfeedback@cisco.com

The Host or Cluster window opens.

Step 12 Choose the host where the Cisco VSG will be installed.

Step 13 Click **Next**.

The Datastore dialog box opens.

Step 14 From the Select a datastore in which to store the VM files pane, choose your datastore.

Step 15 Click **Next**.

The Network Mapping dialog box opens.

Step 16 Click the drop-down arrows for Data (Service), Management, and HA to associate port profiles.

Step 17 Click **Next**.

The Properties dialog boxes opens.

Step 18 Do the following:

- a. In the Cisco VSG HA ID field, enter a unique number between 1 and 4095. This number helps you to identify your Cisco VSG HA pairs.
- b. In the Nexus 1000VSG Administration User Password field, enter your password.
- c. In the Management IP Address field, enter the management address value.
- d. In the Management IP Subnet Mask field, enter the management subnet mask value.
- e. In the Management IP Gateway field, enter the management gateway value.

The Ready to Complete dialog box opens displaying details about your settings.

Step 19 Click **Next**.

Step 20 If the settings are correct, click **Finish**.

The deployment task begins in a dialog box that notifies you when the installation completes successfully.

Step 21 Click **Close**.

You have completed installing the Cisco Virtual Security Gateway software and creating a VM for the Cisco VSG.

Step 22 Power on the Cisco VSG you just created.

Step 23 If you chose the Standalone mode for installation in [Step 10](#), you now see the Cisco VSG login prompt. Log in with your Cisco VSG Administration password.

You may now proceed with configuring the Cisco Virtual Security Gateway. For details, see the *Cisco Virtual Security Gateway for Nexus 1000V Series Switch Fireway Policy Guide, Release 4.2(1)VSG1(3)*.

Step 24 If you chose the manual installation in [Step 10](#), see the “[Configuring Initial Settings](#)” section on page 3-7 to configure the initial settings on the Cisco VSG.

**Note**

If you are installing high availability (HA), you must configure the software on the primary Cisco VSG before installing the software on the secondary Cisco VSG.

Send document comments to vsg-docfeedback@cisco.com

Installing the Cisco VSG Software from an ISO File

You can install the Virtual Security Gateway from an ISO file.

BEFORE YOU BEGIN

Before starting the procedure, know or do the following:

- A name for the new Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- The name of the host where the Cisco VSG will be installed in the inventory folder.
- The name of the datastore in which the VM files will be stored.
- The names of the network port profiles used for the VM.
- The Cisco VSG IP address.

PROCEDURE

-
- Step 1** Upload the Cisco Virtual Security Gateway ISO image to the vCenter datastore.
- Step 2** From the data center in the vSphere Client menu, choose your ESX host where you want to install the Cisco Virtual Security Gateway and choose **New Virtual Machine**.
- The Create New Virtual Machine dialog box opens.
- For VM requirements, see the [“Host and VM Requirements” section on page 3-1](#). For detailed information about how to create a VM, see the VMware documentation.
- Step 3** Click the **Custom** radio button to create a VM, and click **Next**.
- The Create New Virtual Machine dialog box opens.
- Step 4** In the Name field, add a name for the Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- Step 5** In the Inventory Location field, choose your data center and click **Next**.
- The Datastore dialog box opens.
- Step 6** From the Select a datastore in which to store the VM files pane, choose your datastore and click **Next**.
- The Virtual Machine Version dialog box opens.
- Step 7** Click the **Virtual Machine Version: Keep the selected virtual machine version**.
- The Guest Operating System dialog box opens.
- Step 8** Click the **Linux** radio button.
- Step 9** In the Version field, from the drop-down list, choose **Other 2.6x Linux (32-bit)** from the drop-down list. Click **Next**.
- The CPUs dialog box opens.
- Step 10** In the Number of virtual processors field, from the drop-down list, choose **1** and click **Next**.
- The Memory dialog box opens.
- Step 11** Choose **2 GB** memory size and click **Next**.
- The Create Network Connectors dialog box opens.
- Step 12** In the How many NICs do you want to connect? field, from the drop-down list, choose **3**.

Send document comments to vsg-docfeedback@cisco.com

- Step 13** In the Network pane, from the drop-down lists, choose **service**, **management**, and **HA** port profiles in that sequence for the NIC 1, NIC 2, and NIC 3. Choose **VMXNET3** for the adapter type for NIC 1. Choose **E1000** for the adapter type for NIC 2 and NIC 3 and click **Next**.
The SCSI Controller dialog box opens.
- Step 14** The radio button for the default SCSI controller is chosen. Click **Next**.
The Select a Disk dialog box opens. The radio button for the default disk is chosen.
- Step 15** Click **Next**.
The Create a Disk dialog box opens. The default virtual disk size and policy is chosen.
- Step 16** Click **Next**.
The Advanced Options dialog box opens. The default options are chosen.
- Step 17** Click **Next**.
The Ready to Complete dialog box opens.
- Step 18** In the Settings for the new virtual machine pane, review your settings.
- Step 19** Check the **Edit the virtual machine before completion** check box and click **Continue**.
A dialog box with device details opens.
- Step 20** From the Hardware pane, choose your **New CD/DVD (adding)**.
- Step 21** Click the **Datastore ISO File** radio button to browse and, from the drop-down list, select your ISO file.
- Step 22** In the Device Status pane, check the **Connect at power on** check box and click **Finish**.
The Summary tab window opens.
- Step 23** In the Recent Tasks pane, wait for the Create virtual machine status to complete.
- Step 24** From the vSphere Client menu, choose your recently installed VM and in the VM pane, click **Power on the virtual machine**.
- Step 25** Click the **Console** tab to view the VM console. Wait for the Install Virtual Firewall and bring up the new image to boot.
See the [“Configuring Initial Settings” section on page 3-7](#) to configure the initial settings on the Cisco VSG.



Note To allocate additional RAM, first power off the VM by right-clicking on the VM icon and then choosing **Power > Power Off** from the popup window. After the VM is powered down, edit the configuration settings on the VM for controlling memory resources.

Configuring Initial Settings

This section describes how to configure initial settings on the Cisco VSG and includes the following topic:

- [Configuring Initial Settings on a Standby Cisco VSG, page 3-9](#)

Send document comments to vsg-docfeedback@cisco.com

When you power on the Cisco VSG for the first time, depending on which mode you used to install your Cisco VSG, you might be prompted to log in to the Cisco VSG to configure initial settings at the console on your vSphere Client.

For details about installing Cisco VSG, see the “Installing the Cisco VSG Software” section on page 3-3.

BEFORE YOU BEGIN

See [Table 3-2](#) to determine if you must configure initial settings as described in this section.

Table 3-2 Configure Initial Settings Based on Cisco Virtual Security Gateway Installation Method

Your Cisco Virtual Security Gateway Software Installation Method	Do You Proceed with “Configuring Initial Settings”?
Installing an OVA file and choosing Manually Configure Nexus 1000VSG in the configuration field during installation.	Yes. Proceed with configuring initial settings described in this section.
Installing an OVA file and choosing any of the options other than the manual method in the configuration field during installation.	No. You have already configured the initial settings during the OVA file installation.
Installing an ISO file.	Yes. Proceed with configuring initial settings described in this section.

PROCEDURE

Step 1 At the Console tab on your VM after the Cisco VSG software image boots, create the admin password.

```
Enter the password for "admin":<password>
```



Note

This password is required for further access for Cisco VSG administrators.

Step 2 Confirm the admin password.

Step 3 Enter the HA role of the Cisco VSG.

```
Enter HA role[standalone/primary/secondary]:primary
```

Step 4 Enter an ID number for the HA pair.

```
Enter the ha id(1-4095): 25
```



Note

The HA ID uniquely identifies the two Cisco VSGs in an HA pair. If you are configuring Cisco VSGs in an HA pair, make sure that the ID number you enter is identical to the other Cisco VSG in the pair.

Step 5 Enter the basic system configuration setup dialog.

This example shows how to configure a basic system configuration setup dialog:

```
Would you like to enter the basic configuration dialog (yes/no):yes
```

Send document comments to vsg-docfeedback@cisco.com

```

Create another login account(yes/no)[n]:n

Configure read-only SNMP community string (yes/no)[n]:n

Enter the Virtual Security Gateway (VSG) name:VSG-demo

Continue with Out-of-band (mgmt0) management configuration? (yes/no)[y]:y

Mgmt IPv4 address:10.10.10.11

Mgmt IPv4 netmask:255.255.255.0

Configure the default gateway? (yes/no)[y]:y

IPv4 address of the default gateway:10.10.10.1

Configure the DNS IPv4 address? (yes/no)[no]:no

Enable the telnet service? (yes/no)[y]:n

Configure the ntp server? (yes/no) [n]:n

The following configuration will be applied:
  Interface mgmt0
  ip address 10.10.10.11 255.255.255.0
  no shutdown
  interface data0
  ip address 215.1.1.1 255.255.0
  vrf context management
  ip route 0.0.0.0/10.10.11.1
  no telnet server enable
  ssh key rsa 768 force
  ssh server enable
  no feature http-server
  ha-pair id 25

Would you like to edit the configuration? (yes/no)[n]:n

Use this configuration and save it? (yes/no)[y]:y
[#####] 100%

```

Step 6 Enter the administrator login.

```
User Access Verification
VSG login: <admin>
```

Step 7 Enter the password.

```
Password: <password>
```

You are now at the Cisco VSG node.

Configuring Initial Settings on a Standby Cisco VSG

You can add a standby Cisco VSG by logging in to the Cisco VSG you have identified as secondary and using the following procedure to configure a standby Cisco VSG with its initial settings.

Send document comments to vsg-docfeedback@cisco.com

PROCEDURE

Step 1 At the Console tab on your VM after the Cisco VSG software image boots, enter the admin password.

Enter the password for "admin":<password>

Step 2 Confirm the admin password.

Step 3 Enter an ID number for the HA pair.

Enter the ha-pair id(1-4095): **25**



Note

The HA ID uniquely identifies the two Cisco VSGs in an HA pair. If you are configuring Cisco VSGs in an HA pair, make sure that the ID number you provide is identical to the other Cisco VSG in the pair.

Step 4 Enter the HA role of the Cisco VSG.

Enter HA role[standalone/primary/secondary]: **secondary**

Step 5 Enter the administrator login.

User Access Verification
VSG login: <admin>

Step 6 Enter the password.

Password: <password>

You are now at the Cisco VSG node.

Verifying the Cisco VSG Configuration

To display the Cisco VSG configuration, perform one of the tasks:

Command	Purpose
show interface brief	Displays brief status and interface information
show vsg	Displays the Cisco VSG and system-related information

This example shows how to verify the Cisco VSG configurations.

vsg# **show interface brief**

```
-----
Port      VRF      Status IP Address      Speed  MTU
-----
mgmt0    --      up      10.193.77.217   1000   1500
-----

Port      VRF      Status IP Address      Speed  MTU
-----
data0    --      up      172.168.1.1     1000   1500
-----
```

vsg# show vsg

Send document comments to vsg-docfeedback@cisco.com

```
Model: VSG
HA ID: 3437
VSG Software Version: 4.2(1)VSG1(1) build [4.2(1)VSG1(0.399)]
VNMC IP: 10.193.75.73

vsg#
```

Where to Go Next

After installing and completing the initial configuration of the Cisco VSG, you can configure firewall policies on the Cisco VSG through the Cisco VNMC.

Send document comments to vsg-docfeedback@cisco.com