Installing the Cisco VSG

This chapter contains the following sections:

Information About the Cisco VSG

This section describes how to install and complete the basic configuration of the Cisco VSG for Cisco Nexus 1000V Switch

Host and VM Requirements

The Cisco VSG has the following requirements:

- KVM platform with a minimum of 4 GB 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.
  - 2 processors (1 processor is optional.)
  - 2-GB RAM
  - 3 NICs (E1000 type)

- Minimum of 3 GB of SCSI hard disk with LSI Logic Parallel adapter (default)
- Minimum CPU speed of 1 GHz

- There is no dependency on the VM hardware version, so the VM hardware version can be upgraded if required.

Cisco VSG and Supported Cisco Nexus 1000V Series Device Terminology

The following table lists the terminology is used in the Cisco VSG implementation.

Term	Description
Distributed Virtual Switch (DVS)	Logical switch that spans one or more compute nodes. It is controlled by one VSM instance.
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: • Descriptor file (.OVF) • Manifest (.MF) and certificate files (optional)
Open Virtual Machine Format (OVF)	Platform-independent method of packaging and distributing Virtual Machines (VMs).
OpenStack dashboard	Provides administrators and users a graphical interface to access, provision, and automate cloud-based resources.
Virtual Ethernet Module (VEM)/Compute node	Part of the Cisco Nexus 1000V Series switch that switches data traffic. It runs on a KVM host. Up to 64 VEMs are controlled by one VSM.
Virtual Machine (VM)	Virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple VMs 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 with a 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.

Term	Description
Virtual Supervisor Module (VSM)	Control software for the Cisco Nexus 1000V Series distributed virtual device that runs on a virtual machine (VM) and is based on Cisco NX-OS.

Prerequisites for Installing the Cisco VSG Software

The following components must be installed and configured:

- On the Cisco Nexus 1000V Series switch, configure three VLANs, a service VLAN, a management 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 three port profiles for the Cisco VSG: one for the service VLAN, one for management VLAN, and one 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/index.html

Installing the Cisco VSG Software

You can install the Cisco VSG software on a VM by using an open virtual appliance (OVA) file or an QCOW2 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 on OpenStack, on page 3
- Installing the Cisco VSG Software from a QCOW2 File

Installing the Cisco VSG Software on OpenStack

You can install the Cisco VSG software on a VM by using an open virtual appliance (OVA) file or an QCOW2 image file.

Before You Begin

- Specify a name for the new Cisco VSG that is unique within the inventory folder and has up to 80 characters.
- Copy the installation file (.QCOW2 or .ova file) to the OpenStack Controller Node.
- Know the name of the host where the Cisco VSG will be installed in the inventory folder.
- Know the name of the datastore in which the VM files will be stored.
- Know the names of the network port profiles used for the VM.
- Know the Cisco VSG IP address.
- Know the mode in which you will be installing the Cisco VSG:
  - Standalone
  - HA Primary
  - HA Secondary
  - Manual Installation

Procedure

Step 1 Log in to the OpenStack Controller with OpenStack administrator credentials.

Attention If you have QCOW2 installation file, skip Step 2, which converts an OVA installation file to a QCOW2 installation file. The Cisco VSG installation on KVM requires QCOW2 installation file.

Step 2 Convert the OVA file to QCOW2 format using the **qemu-img convert** command. For example:

```
h(openstack_admin)]#qemu-img convert -f vmdk -O qcow2 nexus-1000v.5.2.1.VSG2.1.3.vmdk
nexus-1000v.5.2.1.VSG2.1.3.qcow2
```

Step 3 Create an image file using the **glance image-create** command. For example:

```
h(openstack_admin)]#glance image-create --name "VSG_qcow2" --disk-format=qcow2
--container-format=bare --property architecture=i686 --property hw_vif_model=e1000 --property
 hw_disk_bus='ide' --file nexus-1000v.5.2.1.VSG2.1.3.qcow2
```

Step 4 Display the available network lists using the **neutron net-list** command. For example:

```
h(openstack_admin)]# neutron net-list
+--------------------------------------+----------+-----------------------------------------------------+
| id | name | subnets |
+--------------------------------------+----------+-----------------------------------------------------+
| e4532360-6918-4360-a0ff-5df293e6f4c8 | vlan1452 | 483f9a85-f0f3-4b7d-98cf-ad144ab8d249
14.52.0.0/24 |
| 0ae7059c-4437-4ee4-b2e1-f38560ed00b4 | vlan1455 | 82bbefa3-b676-41ce-aff0-f0858faab088
14.55.0.0/24 |
| 9118659f-84c4-49d3-adb2-e5b0a01b24fc | vlan1454 | 1cc89224-8358-4f7f-961d-3b959db72c7d
14.53.0.0/24 |
| 02227127-69b9-41eb-bae4-9532f6bcb8af | vlan1453 | 351656db-83ba-48cb-bade-78feacfd4879
14.53.0.0/24 |
+--------------------------------------+----------+-----------------------------------------------------+
```

Step 5 Display the Cisco policy profile list using the **neutron cisco-policy-profile-list** command. For example:

```
h(openstack_admin)]# neutron cisco-policy-profile-list
+--------------------------------------+-------------+
| id | name |
+--------------------------------------+-------------+
| c64131c5-652b-4ac7-89b2-dfffa1a482a3 | pp3 |
| b95f931d-f09f-4236-90cf-a33df3be4437 | pp4 |
| cf394dae-7665-4b3a-88f0-99cc8517f457 | dummy |
| c336d13c-1e85-4935-9d9f-c073c22fdc08 | default-pp |
+--------------------------------------+-------------+
```

Step 6 Create a port using the **neutron port-create** *net-list_ name —n1kv:profile cisco-policy-profile-list_ID* command. For example:

```
h(openstack_admin)]#neutron port-create vlan1452 --n1kv:profile
c336d13c-1e85-4935-9d9f-c073c22fdc08
Created a new port:
+---------------------+-------------------------------------------------------------------------------------+
| Field | Value |
+---------------------+-------------------------------------------------------------------------------------+
| admin_state_up | True |
| allowed_address_pairs | |
| binding:host_id | |
| binding:profile | {} |
| binding:vif_details | {} |
| binding:vif_type | unbound |
| binding:vnic_type | normal |
| device_id | |
| device_owner | |
| fixed_ips | {"subnet_id": "483f9a85-f0f3-4b7d-98cf-ad144ab8d249", "ip_address": "14.52.0.5"}
 |
| id | 44b424db-55bc-48a0-a7e0-f8dd679b2093 |
| mac_address | fa:16:3e:98:be:05 |
| n1kv:profile | c336d13c-1e85-4935-9d9f-c073c22fdc08 |
| name | |
| network_id | e4532360-6918-4360-a0ff-5df293e6f4c8 |
| security_groups | cb0453c4-9b79-4899-911c-68563853659f |
| status | DOWN |
| tenant_id | 24c4e9637f6f4a0589eca8b129841664 |
+---------------------+-------------------------------------------------------------------------------------+
```

Step 7 Launch the Cisco VSG VM on the Cisco Nexus 1000V using the **nova boot VSG-VM** command. For example:

```
h(openstack_admin)]# nova boot VSG-large-p --flavor VSG-large --image
6bc75d1e-b9e0-49dc-94da-7404f8067e8b --nic port-id=32b8862c-cc9f-4a66-ac8b-6911aeddb114
--nic port-id=bc364ae5-7218-4d56-8758-55f683ae08e1  --nic
port-id=085a0881-8774-4242-9500-7fbb9b91939f
+--------------------------------------+------------------------------------------------+
| Property                             | Value
|
+--------------------------------------+------------------------------------------------+
| OS-DCF:diskConfig                    | MANUAL
|
| OS-EXT-AZ:availability_zone          | nova
|
| OS-EXT-SRV-ATTR:host                 | -
|
| OS-EXT-SRV-ATTR:hypervisor_hostname  | -
```

```
|
| OS-EXT-SRV-ATTR:instance_name        | instance-0000000b
|
| OS-EXT-STS:power_state               | 0
|
| OS-EXT-STS:task_state                | scheduling
|
| OS-EXT-STS:vm_state                  | building
|
| OS-SRV-USG:launched_at               | -
|
| OS-SRV-USG:terminated_at             | -
|
| accessIPv4                           |
|
| accessIPv6                           |
|
| adminPass                            | xyJKcwTH2DbR
|
| config_drive                         |
|
| created                              | 2015-03-27T09:24:44Z
|
| flavor                               | VSG-large (08dfe7b7-f77b-424b-a4aa-6bfd4c53a227)
|
| hostId                               |
|
| id                                   | a8eb1b99-e03e-4acc-9bf3-ab17a01a07fb
|
| image                                | VSG_REL (6bc75d1e-b9e0-49dc-94da-7404f8067e8b)
|
| key_name                             | -
|
| metadata                             | {}
|
| name                                 | VSG-large-p
|
| os-extended-volumes:volumes_attached | []
|
| progress                             | 0
|
| security_groups                      | default
|
| status                               | BUILD
|
| tenant_id                            | 24c4e9637f6f4a0589eca8b129841664
|
| updated                              | 2015-03-27T09:24:44Z
|
| user_id                              | 9476dd26b5ff41bb8152124b3b9f63cb
|
+--------------------------------------+--------------------------------------------------+
[root@macf872eaa3d77e home(openstack_admin)]#
```

Step 8 Open the OpenStack GUI dashboard.

Step 9 Click **Instances**.

Step 10 In the **Instances** pane, note the IP Address of the launched VSG VM instance.

Step 11 In the **OpenStack** Dashboard, locate the newly created VM and choose **More** > **Console** to start the VSG installation procedure.

Step 12 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 to configure the initial settings on the Cisco VSG.

Configuring Initial Settings

This section describes how to configure the initial settings on the Cisco VSG and configure a standby Cisco VSG with its initial settings. For configuring a standby Cisco VSG, see Configuring Initial Settings on a Standby Cisco VSG, on page 9 section.

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 of your OpenStack dashboard. For details about installing Cisco VSG, see Installing the Cisco VSG Software, on page 3.

Before You Begin

The following table determines if you must configure the initial settings as described in this section.

Your Cisco Virtual Security Gateway Software Installation Method	Do You Need to Proceed with "Configuring Initial Settings"?
Installing an OVA file and choosing Manually Configure Nexus 1000 VSG 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 QCOW2 file.	Yes. Proceed with configuring initial settings described in this section.

Procedure

Step 1 Navigate to the **Console** tab in the VM.

Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.

Step 2 At the `Enter the password for "admin"` prompt, enter the password for the admin account and press **Enter**.

Step 3 At the prompt, confirm the admin password and press **Enter**.

Step 4 At the `Enter HA role[standalone/primary/secondary]` prompt, enter the HA role you want to use and press **Enter**.
This can be one of the following:

- standalone
- primary
- secondary

Step 5 At the `Enter the ha id(1-4095)` prompt, enter the HA ID for the pair and press **Enter**.

Note If you entered secondary in the earlier step, the HA ID for this system must be the same as the HA ID for the primary system.

Step 6 If you want to perform basic system configuration, at the `Would you like to enter the basic configuration dialog (yes/no)` prompt, enter **yes** and press **Enter**, then complete the following steps.

a) At the `Create another login account (yes/no)[n]` prompt, do one of the following:

- To create a second login account, enter **yes** and press **Enter**.
- Press **Enter**.

b) (Optional) At the `Configure read-only SNMP community string (yes/no)[n]` prompt, do one of the following:

- To create an SNMP community string, enter **yes** and press **Enter**.
- Press **Enter**.

c) At the `Enter the Virtual Security Gateway (VSG) name` prompt, enter **VSG-demo** and press **Enter**.

Step 7 At the `Continue with Out-of-band (mgmt0) management configuration? (yes/no)[y]:` prompt, enter **yes** and press **Enter**.

Step 8 At the `Mgmt IPv4 address:` prompt, enter **10.10.10.11** and press **Enter**.

Step 9 At the `Mgmt IPv4 netmask` prompt, enter **255.255.255.0** and press **Enter**.

Step 10 At the `Configure the default gateway? (yes/no)[y]` prompt, enter **yes** and press **Enter**.

Step 11 At the `Configure the DNS IPv4 address? (yes/no)[n]:` prompt, enter **no** and press **Enter**.

Step 12 At the `Enable the telnet service? (yes/no)[y]:` prompt, enter **no**.

Step 13 At the `Configure the ntp server? (yes/no)[n]` prompt, enter **no** and press **Enter**.

Step 14 At the `Continue with Policy Agent Configuration? (yes/no)[y]` prompt, enter **yes** and press **Enter**.

a) At the `vnmc IPv4 address:` prompt, enter the registration IPv4 address and press **Enter**.
b) At the `Policy agent shared secret string:` prompt, enter a secret string and press **Enter**.
c) At the `Policy agent image name[vnmc-vsgpa.2.1.3.bin]:` prompt, press **Enter**.

The following configuration will be applied:

```
hostname vsg
nsc-policy-agent
    registration-ip 16.0.9.7
    shared-secret  ******
    policy-agent-name bootflash:/vnmc-vsgpa.2.1.3.bin
no telnet server enable
ssh key rsa 2048 force
ssh server enable
feature http-server
ha-pair id 1
```

Step 15 At the `Would you like to edit the configuration? (yes/no)[n]` prompt, enter **n**and press **Enter**.

Step 16 At the `Use this configuration and save it? (yes/no)[y]:` prompt, enter **y** and press **Enter**.

Step 17 At the `VSG login` prompt, enter the name of the admin account you want to use and press **Enter**.
The default account name is `admin`.

Step 18 At the `Password` prompt, enter the name of the password for the admin account and press **Enter**.
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.

Procedure

Step 1 Navigate to the **Console** tab in the VM.
Cisco Nexus 1000V Series switch opens the **Console** window and boots the Cisco VSG software.

Step 2 At the `Enter the password for "admin"` prompt, enter the password for the admin account and press **Enter**.

Step 3 At the prompt, confirm the admin password and press **Enter**.

Step 4 At the `Enter HA role[standalone/primary/secondary]` prompt, enter the secondary HA role and press **Enter**.

Step 5 At the `Enter the ha id(1-4095)` prompt, enter **25** for the HA pair id and press **Enter**.

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 6 At the `VSG login` prompt, enter the name of the admin account you want to use and press **Enter**.
The default account name is `admin`.

Step 7 At the `Password` prompt, enter the name of the password for the admin account and press **Enter**.
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

vsg# show vsg
Model: VSG
HA ID: 111
VSG software version: 5.2(1)VSG2(1.3) build [5.2(1)VSG2(1.3)]
NSC IP: 14.52.0.9
NSC PA version: 2.1(2a)-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 PNSC.