CHAPTER 3

Configuring the Cisco Virtual Security Gateway

This chapter describes how to configure the Cisco Virtual Security Gateway (VSG) for the Cisco Nexus 1000V Series switch and the Cisco Nexus 1010 Virtual Services Appliance.

This chapter includes the following sections:

For additional details about the Cisco Nexus 1000V Series switch port profiles, see the *Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(5.1)*.

Configuring the Port Profile on the VSM for a Cisco VSG in the Layer 2 Mode

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide.*
- You must have the NEXUS_VSG_SERVICES_PKG license installed on the switch. Ensure that you have enough licenses to cover the number of Virtual Ethernet Modules (VEMs) you want to protect.
- The data IP address and management IP addresses should be configured. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.
- You have completed creating the Cisco VSG port profiles for the service and high-availability (HA) interface. see the“Cisco VSG Configuration Guidelines and Limitations” section on page 6-2
- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**
2. **port-profile** *port-profile-name*
3. **org** *org-name*
4. **vn-service ip-address** *ip-address* **vlan** *vlan-id* [**fail** {**open** | **close**}] [**security-profile** *security-profile-name*]
5. (Optional) **copy running-config startup-config**
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure`**
	Example:
	`n1000v# configure`
	`n1000v(config)#`
		Places you in global configuration mode.

Step 2	**`port-profile`** *`port-profile-name`*
	Example:
	`n1000v(config-port-prof)# port-profile host-profile`
	`n1000v(config-port-prof)#`
		Enters the port profile configuration mode for the named port profile. If the port profile does not exist, it is created using the following characteristics:
		port-profile-name—The port profile name can be up to 80 alphanumeric characters and must be unique for each port profile on the Cisco VSG.

Step 3	**`org`** *`org-name`*
	Example:
	`n1000v(config-port-prof)# org root/Tenant-A`
	`n1000v(config-port-prof)#`
		Designates an organization name for the Cisco VSG port profile.

Step 4	**`vn-service ip-address`** *`ip-address`* **`vlan`** *`vlan-id`* [**`fail`** {**`open`** | **`close`**}] [**`security-profile`** *`security-profile-name`*]
	Example:
	`n1000v(config-port-prof)# vn-service ip 100.1.1.100 vlan 1000 profile vnsp-1`
	`n1000v(config-port-prof)#`
		Configures the IP address, VLAN ID, and profile for the Cisco VSG, and optionally allows a fail-safe configuration.
		Note The IP address must match the data interface (data0) IP address on the Cisco VSG.
		Note If you do not pick a security profile name, the default name is assumed. The security profile name must match the security profile created on the Cisco VSG.

Step 5	**`copy running-config startup-config`**
	Example:
	`n1000v(config-port-prof)# copy running-config startup-config`
	`n1000v(config-port-prof)#`
		(Optional) Saves configuration changes.

Step 6	**`exit`**
	Example:
	`n1000v(config-port-prof)# exit`
	`n1000v(config)#`
		Exits the configuration mode and returns you to the global configuration mode.

Configuring the Port Profile on the VSM for a Cisco VSG in the Layer 3 Mode

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.
- You must have the NEXUS_VSG_SERVICES_PKG license installed on the switch. Ensure that you have enough licenses to cover the number of Virtual Ethernet Modules (VEMs) you want to protect.
- You have configured the data IP and management IP addresses. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide.*
- When VEM communicates with the Cisco VSG in the Layer 3 mode, an additional header with 94 bytes is added to the original packet. You must have set the MTU to a minimum of 1594 bytes to accommodate this extra header for any network interface through which the traffic passes between the Cisco Nexus 1000V and the Cisco VSG. These interfaces can include the uplink port profile, the proxy ARP router, a virtual switch or other interfaces.
- If jumbo frames are enabled in the network, you must have set the MTU of the client and server VMs to at least 94 bytes smaller than the uplink port profile MTU. For example, if the uplink port profile MTU is set to 9000 bytes, the MTU of the VMs must be 8906 bytes or less.
- You have completed creating the Cisco VSG port profiles for the service and high-availability (HA) interface. For details, see the "Cisco VSG Configuration Guidelines and Limitations" section on page 6-2.
- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**
2. **port-profile** *port-profile-name*
3. **org** *org-name*
4. **vn-service ip-address** *ip-address* **l3-mode** [**fail** {**open** | **close**}] [**security-profile** *security-profile-name*]
5. (Optional) **copy running-config startup-config**
6. **exit**

DETAILED STEPS

	Command	Purpose
Step 1	**configure** **Example:** n1000v# configure n1000v(config)#	Places you in global configuration mode.
Step 2	**port-profile** *port-profile-name* **Example:** n1000v(config-port-prof)# port-profile host-profile n1000v(config-port-prof)#	Enters the port profile configuration mode for the named port profile. If the port profile does not exist, it is created using the following characteristics: *port-profile-name*—The port profile name can be up to 80 alphanumeric characters and must be unique for each port profile on the Cisco VSG.
Step 3	**org** *org-name* **Example:** n1000v(config-port-prof)# org root/Tenant-A n1000v(config-port-prof)#	Designates an organization name for the Cisco VSG port profile.
Step 4	**vn-service ip-address** *ip-address* **l3-mode** [**fail** {**open** | **close**}] [**security-profile** *security-profile-name*] **Example:** n1000v(config-port-prof)# vn-service ip 100.1.1.100 l3-mode profile vnsp-1 n1000v(config-port-prof)#	Configures the IP address, Layer 3 mode, and port profile for the Cisco VSG, and optionally allows a fail-safe configuration. **Note** The IP address must match the data interface (data0) IP address on the Cisco VSG. **Note** If you do not pick a security profile name, the default name is assumed. The security profile name must match the security profile created on the Cisco VSG.
Step 5	**copy running-config startup-config** **Example:** n1000v(config-port-prof)# copy running-config startup-config n1000v(config-port-prof)#	(Optional) Saves configuration changes.
Step 6	**exit** **Example:** n1000v(config-port-prof)# exit n1000v(config)#	Exits the configuration mode and returns you to the global configuration mode.

Configuring vmknics for the Layer 3 Mode VSG Encapsulation

You can configure vmknics for a Cisco VSG in the Layer 3 mode encapsulation by running the following procedure.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- Identify a VLAN to be used for transporting the Cisco VSG in the Layer 3 mode-encapsulated traffic. Ensure that VLAN is configured on the uplink port profile for all VEMs on which the Cisco VSG in Layer 3 mode can be configured.

SUMMARY STEPS

1. **configure terminal**
2. **port-profile** *profilename*
3. **vmware port-group** *name*
4. **switchport mode access**
5. **switchport access vlan** ***id***
6. **capability l3-vn-service**
7. **no shutdown**
8. **state enabled**
9. **(**Optional**) show port-profile name** *profilename*
10. **(**Optional**) copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure terminal`**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	**`port-profile`** *`profilename`*
	Example:
	`switch(config)# port-profile vmknic-pp`
	`switch(config-port-prof)`
		Enters port profile configuration mode for the named port profile. If the port profile does not already exist, it is created using the following characteristics:
		• *profilename*—The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
		Note If a port profile is configured as an Ethernet type, it cannot be used to configure VMware virtual ports.

Step 3	**`vmware port-group`** *`name`*
	Example:
	`switch(config-port-prof)# vmware`
	`port-group`
	`switch(config-port-prof)#`
		Designates the port profile as a VMware port group.
		The port profile is mapped to a VMware port group of the same name unless you specify a name. When you connect the VSM to vCenter Server, the port group is distributed to the virtual switch on the vCenter Server.

Step 4	**`switchport mode access`**
	Example:
	`switch(config-port-prof)# switchport mode`
	`access`
	`switch(config-port-prof)#`
		Designates the interfaces as switch access ports (the default).

	Command	Purpose

Step 5	**`switchport access vlan`** *`id`*
	`Example:`
	`switch(config-port-prof)# switchport access vlan 100`
	`switch(config-port-prof)`
		Assigns a VLAN ID to this port profile.

Step 6	**`capability l3-vn-service`**
	`Example:`
	`switch(config-port-prof)# capability l3-vn-service`
	`switch(config-port-prof)`
		Assigns the capability **l3-vn-service** to the port profile to ensure that the interfaces that inherit this port profile are used as sources for the Cisco VSG in Layer 3 mode encapsulated traffic.

Step 7	**`no shutdown`**
	`Example:`
	`switch(config-port-prof)# no shutdown`
	`switch(config-port-prof)`
		Administratively enables all ports in the profile.

Step 8	**`state enabled`**
	`Example:`
	`switch(config-port-prof)# state enabled`
	`switch(config-port-prof)`
		Sets the operational state of a port profile.

Step 9	**`show port-profile name`** *`profilename`*
	`Example:`
	`switch# show port-profile vmknic-pp`
		(Optional) Displays the port profile configuration.

Step 10	**`copy running-config startup-config`**
	`Example:`
	`switch# copy running-config startup-config`
		(Optional) Copies the running configuration to the startup configuration.

Configuring the Cisco VSG with the vsn type Command

The Cisco VSG is a virtual service node (VSN). To configure the VSN for Cisco VSG functionality, use the **vsn type vsg global** command to enter the global configuration mode for the Cisco VSG.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.
- You must have the NEXUS_VSG_SERVICES_PKG license installed on the switch. Ensure that you have enough licenses to cover the number of VEMs that you want to protect.
- You must configure the data IP address and management IP addresses. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.
- You have completed creating the Cisco VSG port profiles for the service and HA interface.
- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**
2. **vsn type vsg global**

DETAILED STEPS

	Command	Purpose

Step 1	**configure**
	Example:
	`vsm# configure`
	`vsm(config)#`
		Places you in global configuration mode.

Step 2	**vsn type vsg global**
	Example:
	`vsm(config)# vsn type vsg global`
	`vsm(config-vsn)#`
		Enters VSN configuration mode.

Configuring TCP State-Checks for All Cisco VSG VSNs in a vPath

Although the TCP state-checks for Cisco VSGs on a vPath feature is enabled by default, there may be times when you want to disable this feature, such as when you do not want the information generated by this feature to hide other information in which you are specifically interested.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You have the Cisco VSG software installed and the basic installation completed. For details, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.
- You must have the NEXUS_VSG_SERVICES_PKG license installed on the switch. Ensure that you have enough licenses to cover the number of VEMs that you want to protect.
- You must configure the data IP address and management IP addresses. To configure the data IP address, see the *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide.*
- You have completed creating the Cisco VSG port profiles for the service and HA interface.
- You are logged in to the switch CLI in EXEC mode.

SUMMARY STEPS

1. **configure**
2. **vsn type vsg global**
3. **tcp state-checks**
4. **no tcp state-checks**
5. **exit**
6. **exit**

DETAILED STEPS

	Command	Purpose

Step 1	**`configure`**
	
	`Example:`
	`vsm# configure`
	`vsm(config)#`
		Places you in global configuration mode.

Step 2	**`vsn type vsg global`**
	
	`Example:`
	`vsm(config)# vsn type vsg global`
	`vsm(config-vsn)#`
		Enters VSN configuration mode.

Step 3	**`tcp state-checks`**
	
	`Example:`
	`vsm(config-vsn)# tcp state-checks`
	`vsm(config-vsn)#`
		Enables TCP state checks for all Cisco VSG VSNs in the vPath. (This is the default status.)

Step 4	**`no tcp state-checks`**
	
	`Example:`
	`vsm(config-vsn)# no tcp state-checks`
	`vsm(config-vsn)#`
		Disables the TCP state-checks feature.

Step 5	**`exit`**
	
	`Example:`
	`vsm(config-vsn)# exit`
	`vsm(config)#`
		Exits the VSN configuration mode and returns you to the global configuration mode.

Step 6	**`exit`**
	
	`Example:`
	`vsm(config)# exit`
	`vsm#`
		Exits the global configuration mode and returns you to EXEC mode.

Verifying the Cisco VSG Configuration

To display information related to a Cisco VSG, perform one of the following tasks on the switch CLI:

Show Commands

Command	Purpose
show license usage **Example:** `vsm# show license usage`	Displays a table with the Cisco VSG license usage information for the Cisco Nexus 1000V Series switch.
show license usage NEXUS_VSG_SERVICES_PKG **Example:** `vsm# show license usage NEXUS_VSG_SERVICES_PKG`	Displays the usage information for the license package NEXUS_VSG_SERVICES_PKG.

show vsn {**statistics** | **brief** | {**detail** [{{**vlan** *vlan-num* [**ip** *ip-addr*]} | **module** *module-num*}]}}
Example:
`vsm# show vsn statistics detail vlan 1`
	Displays information about the configuration, MAC address, state of associated Cisco VSG and Virtual Ethernet Module (VEM), Veths to which Cisco VSGs are bound, and Virtual Service Node (VSN) statistics for all VEM modules associated with Cisco VSGs.

For detailed information about the fields in the output from these commands, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(5.1)*.

vPath Ping Command for the Layer 2 Mode

To verify various connections and reachable attributes of the Cisco VSG VSN, you can use the vPath **ping** command.

The vPath **ping** command for Layer 2 mode has the following syntax:

ping vsn {**all** | {**ip** *ip-addr* [**vlan** *vlan-num*]}} **src-module** {**all** | **vpath-all** | *module-num*} [**timeout** *secs*] [**count** {*count* | **unlimited**}]

Examples

The following example shows how to see the VSN connections and if they are reachable:

```
VSM-1# ping vsn all src-module all
ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=0 timeout=1-sec
  module(usec)   :  3(156)  5(160)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=0 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=1 timeout=1-sec
  module(usec)   :  3(230)  5(151)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=1 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=2 timeout=1-sec
  module(usec)   :  3(239)  5(131)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=2 timeout=1-sec
```

```
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=3 timeout=1-sec
  module(usec)   :  3(248)  5(153)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=3 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)

ping vsn 106.1.1.1 vlan 54 from module 3 5, seq=4 timeout=1-sec
  module(usec)   :  3(259)  5(126)
ping vsn 110.1.1.1 vlan 54 from module 3 5, seq=4 timeout=1-sec
  module(failed) :  3(VSN ARP not resolved)  5(VSN ARP not resolved)
```

This example shows how VSN ping options are displayed:

```
VSM-1# ping vsn ?
  all   All VSNs associated to VMs
  ip    IP Address
  vlan  VLAN Number
```

This example shows how VSN ping options are displayed for all source modules:

```
VSM-1# ping vsn all src-module ?
  <3-66>     Module number
  all        All modules in VSM
  vpath-all  All modules having VMs associated to VSNs
```

This example shows how to set up a ping for all source modules from a specified IP address:

```
VSM-1# ping vsn ip 10.1.1.60 src-module all
ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=0 timeout=1-sec
  module(usec)   :  4(301)  5(236)
  module(failed) :  7(VSN ARP not resolved)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=1 timeout=1-sec
  module(usec)   :  4(241)  5(138)  7(270)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=2 timeout=1-sec
  module(usec)   :  4(230)  5(155)  7(256)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=3 timeout=1-sec
  module(usec)   :  4(250)  5(154)  7(284)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=4 timeout=1-sec
  module(usec)   :  4(231)  5(170)  7(193)
```

This example shows to set up a ping for all Vpath source modules for a specified IP address:

```
VSM-1# ping vsn ip 10.1.1.60 src-module vpath-all
ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=0 timeout=1-sec
  module(usec)   :  4(223)  5(247)

ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=1 timeout=1-sec
  module(usec)   :  4(206)  5(167)

ping vsn 10.1.1.60 vlan 501 from module 4 5, seq=2 timeout=1-sec
  module(usec)   :  4(241)  5(169)
```

This example shows how to set up a ping for all source modules of a specified IP address with a time-out and a count:

```
VSM-1# ping vsn ip 10.1.1.60 src-module all timeout 2 count 3
ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=0 timeout=2-sec
  module(usec)   :  4(444)  5(238)  7(394)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=1 timeout=2-sec
```

```
  module(usec)   :  4(259)  5(154)  7(225)

ping vsn 10.1.1.60 vlan 501 from module 4 5 7, seq=2 timeout=2-sec
  module(usec)   :  4(227)  5(184)  7(216)
```

vPath Ping Command for the Layer 3 Mode

Examples

```
vsm# ping vsn ip 10.1.1.40 src-module vpath-all
ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(698) 11(701) 12(826)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(461) 11(573) 12(714)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(447) 11(569) 12(598)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(334) 11(702) 12(559)

ping vsn 10.1.1.40 vlan 0 from module 9 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(387) 11(558) 12(597)

vsm#


vsm# ping vsn all src-module all
ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(508)
  module(failed) : 10(VSN ARP not resolved) 11(VSN ARP not resolved)
                   12(VSN ARP not resolved)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=0 timeout=1-sec
  module(usec)   :  9(974) 11(987) 12(1007)
  module(failed) : 10(VSN ARP not resolved)

ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(277) 10(436) 11(270) 12(399)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=1 timeout=1-sec
  module(usec)   :  9(376) 10(606) 11(468) 12(622)

ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(272) 10(389) 11(318) 12(357)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=2 timeout=1-sec
  module(usec)   :  9(428) 10(632) 11(586) 12(594)

ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(284) 10(426) 11(331) 12(387)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=3 timeout=1-sec
  module(usec)   :  9(414) 10(663) 11(644) 12(698)

ping vsn 10.1.1.44 vlan 501 from module 9 10 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(278) 10(479) 11(334) 12(469)
ping vsn 10.1.1.40 vlan 0 from module 9 10 11 12, seq=4 timeout=1-sec
  module(usec)   :  9(397) 10(613) 11(560) 12(593)

vsm#
```

Where to Go Next

After you have completed configuring the Cisco VSG port profile on the switch for protection, proceed to assign port profiles to your VMs for Cisco VSG firewall protection on the vCenter.