CHAPTER 3

Configuring VSD

This chapter describes how to configure VSD and includes the following topics:

Information About Virtual Service Domain

A virtual service domain (VSD) allows you to classify and separate traffic for network services, such as firewalls, traffic monitoring, and those in support of compliance goals such as Sarbanes Oxley.

Service Virtual Machine

A service VM (SVM) provides the specialized service like firewall, deep packet inspection (application aware networking), or monitoring. Each Service VM has three virtual interfaces:

Interface	Description
Management	A regular interface that manages the SVM Should have Layer 2 or Layer 3 connectivity, depending on its use.
Incoming	Guards the traffic coming into the VSD Any packet coming into the VSD must go through this interface.
Outgoing	Guards the traffic going out of the VSD. Any packet that originates in the VSD and goes out must go through the SVM and out through the outgoing interface.

There is no source MAC learning on these interfaces. Each SVM creates a secure VSD. Interfaces within the VSD are shielded by the SVM.

Port Profiles

A VSD is the collection of interfaces that are guarded by the SVM providing the security service. Any traffic coming into the VSD or going out of the VSD has to go through the SVM.

Traffic that both originates and terminates within the same VSD need not be routed through the SVM as it is considered to be safe.

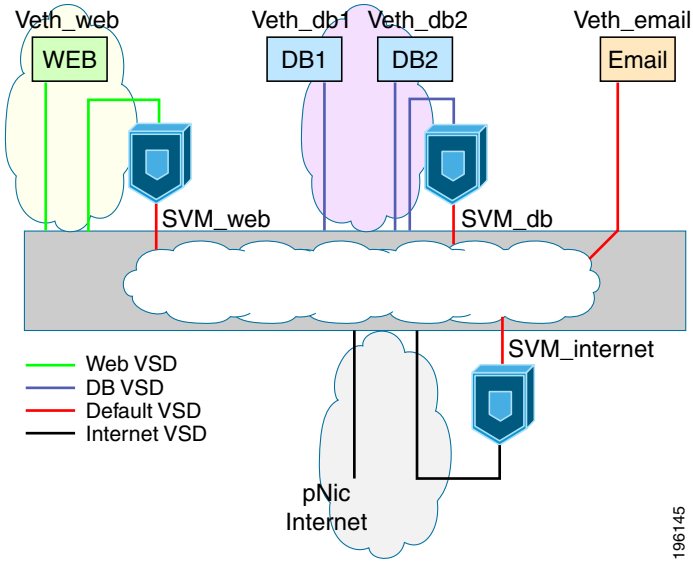
A VSD is formed by creating the following port profiles:

Port Profile	Description
Inside	Traffic originating from a VSD member goes into the service VM (SVM) through the inside port and comes out of the outside port before it is forwarded to its destination.
Outside	Traffic destined for a VSD member goes into the SVM through the outside port and comes out of the inside port before it is forwarded to its destination.
Member	Location for individual inside VMs.

In Figure 3-1, a single VEM takes the place of vswitches; the SVMs define the following VSDs;

VSD	SVM (guard)	Inside Port Profile	Outside Port Profile	Member Port Profile(s)
DB VSD	SVM_db	SVM_db_inside	SVM_db_outside	vEth_db1 vEth_db2
Web VSD	SVM_web	SVM_web_inside	SVM_web_outside	vEth_web
Internet VSD	SVM_Internet	SVM_internet_inside	SVM_internet_outside	
Default		SVM VSD		vEth Email

Figure 3-1 Virtual Service Domain (VSD) Example



Guidelines and Limitations

Virtual Service Domain has the following configuration guidelines and limitations:

- To prevent traffic latency, VSD should only be used for securing traffic.
- Up to 6 VSDs can be configured per host and up to 64 on the VSM.
- Up to 214 interfaces per VSD are supported on a single host, and 2048 interfaces on the VSM.
- Vmotion is not supported for the SVM and should be disabled.
- To avoid network loops following a VSM reload or a network disruption, control and packet VLANS must be disabled in all port profiles of the Service VMs.
- If a port profile without a service port is configured on an SVM, it will flood the network with packets.
- When configuring a port profile on an SVM, first bring the SVM down, This prevents a port-profile that is mistakenly configured without a service port from flooding the network with packets. The SVM can be returned to service after the configuration is complete and verified.
- VShield 4.1 does not support VSD. VSD feature will not function as expected if used with VShield 4.1.

Default Settings

The following table lists the Telnet defaults.

Parameters	Default
service-port default-action	Forward.
switchport trunk allowed vlan	All

Configuring VSD

This section includes the following procedures:

Configuring an Inside or Outside VSD Port Profile

Use this procedure to configure the port-profiles that define the connections going into and out of the SVM.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- You have taken the SVM out of service to prevent any configuration errors from flooding the network. Once the configuration is complete and verified, you can bring the SVM back into service.
- If you do not configure a service-port, the SVM will come up as a regular VM, flooding the network with packets.
- Selected VLAN filtering is not supported in this configuration. The default should be used instead, which allows all VLANs on the port.

SUMMARY STEPS

1. **config t**
2. **port-profile** *name*
3. **switchport mode trunk**
4. **switchport trunk allowed vlan** *vlanID*
5. **virtual-service-domain** *name*
6. **no shut**
7. **vmware port-group** *pg-name*
8. **service-port** {**inside** | **outside**} [**default-action** {**drop** | **forward**}]
9. **state enabled**
10. **show virtual-service-domain** *name*
11. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**port-profile** *name*
	
	Example:
	`n1000v(config)# port-profile webserver-inside`
	`n1000v(config-port-profile)#`
		Creates a port profile and places you into Port Profile Configuration mode for the named port profile.
		
		The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.

Step 3	**switchport mode trunk**
	
	Example:
	`n1000v(config-port-profile)# switchport mode trunk`
	`n1000v(config-port-profile)#`
		Designates that the interfaces are switch trunk ports.

Step 4	**switchport trunk allowed vlan** *vlanID*
	
	Example:
	`n1000v(config-port-profile)# switchport trunk allowed vlan all`
	`n1000v(config-port-profile)#`
		Allows all VLANs on the port.

Step 5	**virtual-service-domain** *name*
	
	Example:
	`n1000v(config-port-profile)# virtual-service-domain vsd1-webserver`
	`n1000v(config-port-profile)#`
		Adds a VSD name to this port profile.

Step 6	**no shutdown**
	
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		Administratively enables all ports in the profile.

Step 7	**vmware port-group** *pg-name*
	
	Example:
	`n1000v(config-port-prof)# vmware port-group webservers-inside-protected`
	`n1000v(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. When a vCenter Server connection is established, the port group created in Cisco Nexus 1000V is then distributed to the virtual switch on the vCenter Server.
		
		name: Port group name. If you do not specify a pg-name, then the port group name will be the same as the port profile name. If you want to map the port profile to a different port group name, use the pg-name option followed by the alternate name.

	Command	Purpose
Step 8	**service-port** {**inside** | **outside**} [**default-action** {**drop** | **forward**}]	Configures the interface as either inside or outside and designates (default-action) whether packets should be forwarded or dropped if the service port is down. If you do not specify a default-action, then the **forward** setting is used by default. **Caution** If you do not configure a service-port, the SVM will come up as a regular VM, flooding the network with packets.

	Example:
	`n1000v(config-port-prof)# service-port inside default-action forward`
	`n1000v(config-port-prof)#`
		This example configures an inside VSD that forwards packets if the service port is down.

	Example:
	`n1000v(config-port-prof)# service-port outside default-action forward`
	`n1000v(config-port-prof)#`
		This example configures an outside VSD that forwards packets if the service port is down.

Step 9	**state enabled**
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		Enables the VSD port profile.
		The configuration for this port profile is applied to the assigned ports, and the port group is created in the VMware vSwitch on the vCenter Server.

Step 10	**show virtual-service-domain** *name*
	Example:
	`n1000v(config-port-prof)# show virtual-service-domain vsd1-webserver`
	`Default Action: forward`
	`_____`
	`Interface Type`
	`_____`
	`Vethernet1 Member`
	`Vethernet2 Member`
	`Vethernet3 Member`
	`Vethernet7 Inside`
	`Vethernet8 Outside`
	`n1000v(config-port-prof)#`
		(Optional) Displays the configuration for this VSD port profile. Use this to verify that the port-profile was configured as expected.

Step 11	**copy running-config startup-config**
	Example:
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################] 100%`
	`n1000v(config-port-prof)#`
		(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Configuring a Member VSD Port Profile

Use this procedure to configure the VSD port profile where individual members reside.

BEFORE YOU BEGIN

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

- You are logged in to the CLI in EXEC mode.
- Do not configure a member VSD port profile on an SVM.

  A member VSD port profile does not have a service port, and will flood the network with packets if configured on an SVM.

SUMMARY STEPS

1. **config t**
2. **port-profile** *name*
3. **switchport access vlan** *vlanID*
4. **switchport trunk allowed vlan** *vlanID*
5. **virtual-service-domain** *name*
6. **no shut**
7. **state enabled**
8. **show virtual-service-domain** *name*
9. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 1	**port-profile** *name*
	
	Example:
	`n1000v(config)# port-profile vsd1-member`
	`n1000v(config-port-profile)#`
		Creates a port profile and places you into Port Profile Configuration mode for the named port profile.
		
		The port profile name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.

Step 2	**switchport access vlan** *vlanID*
	
	Example:
	`n1000v(config-port-profile)# switchport access vlan 315`
	`n1000v(config-port-profile)#`
		Assigns a VLAN ID to the access port for this port profile.

	Command	Purpose

Step 3	**virtual-service-domain** *name*
	Example:
	`n1000v(config-port-profile)# virtual-service-domain vsd1-webserver`
	`n1000v(config-port-profile)#`
		Assigns a VSD name to this port profile.

Step 4	**no shutdown**
	Example:
	`n1000v(config-port-prof)# no shutdown`
	`n1000v(config-port-prof)#`
		Administratively enables all ports in the profile.

Step 5	**state enabled**
	Example:
	`n1000v(config-port-prof)# state enabled`
	`n1000v(config-port-prof)#`
		Enables the VSD port profile.
		The configuration for this port profile is applied to the assigned ports, and the port group is created in the VMware vSwitch on the vCenter Server.

Step 6	**show virtual-service-domain** *name*
	Example:
	`n1000v(config-port-prof)# show virtual-service-domain vsd1-webserver`
	`Default Action: forward`
	`_____`
	`Interface Type`
	`_____`
	`Vethernet1 Member`
	`Vethernet2 Member`
	`Vethernet3 Member`
	`Vethernet6 Member`
	`Vethernet7 Inside`
	`Vethernet8 Outside`
	`n1000v(config-port-prof)#`
		(Optional) Displays the configuration for this VSD port profile. Use this to verify that the port-profile was configured as expected.

Step 7	**copy running-config startup-config**
	Example:
	`n1000v(config-port-prof)# copy running-config startup-config`
	`[########################################] 100%`
	`n1000v(config-port-prof)#`
		(Optional) Saves the running configuration persistently through reboots and restarts by copying it to the startup configuration.

Verifying the Configuration

To display the VSD configuration, use the following commands:

Command	Purpose
show virtual-service-domain name *vsd-name*	Displays a specific VSD configuration. See Example 3-1 on page 3-9.
show virtual-service-domain brief	Displays a summary of all VSD configurations. See Example 3-2 on page 3-9.

Command	Purpose
show virtual-service-domain interface	Displays the interface configuration for all VSDs. See Example 3-3 on page 3-9.
module vem *module_number* **execute vemcmd show vsd**	Displays the VEM VSD configuration by sending the command to the VEM from the remote Cisco Nexus 1000V. See Example 3-4 on page 3-10.
module vem *module_number* **execute vemcmd show vsd ports**	Displays the VEM VSD ports configuration by sending the command to the VEM from the remote Cisco Nexus 1000V. See Example 3-5 on page 3-10.

For detailed information about command output for these commands, see the *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*.

***Example 3-1 show virtual-service-domain name** vsd_name*

```
n1000v## show virtual-service-domain name vsd1
Default Action: drop
_____________________________
Interface         Type
_____________________________
Vethernet1        Member
Vethernet2        Member
Vethernet3        Member
Vethernet6        Member
Vethernet7        Inside
Vethernet8        Outside

n1000v#
```

Example 3-2 show virtual-service-domain brief

```
n1000v# show virtual-service-domain brief
Name   vsd-id    default action    in-ports   out-ports   mem-ports    Modules with
                                                                      VSD Enabled
zone    1         forward           1          1           2            4
n1000v#
```

Example 3-3 show virtual-service-domain interface

```
n1000v# sho virtual-service-domain interface
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
Name             Interface             Type      Status
_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
vsd1             Vethernet1            Member    Active
vsd1             Vethernet2            Member    Active
vsd1             Vethernet3            Member    Active
vsd1             Vethernet6            Member    Active
vsd1             Vethernet7            Inside    Active
vsd1             Vethernet8            Outside   Active
vsd2             Vethernet9            Inside    Active
vsd2             Vethernet10           Outside   Active
```

Example 3-4 module** module_number **execute vemcmd show vsd

```
n1000v# module vem 4 execute vemcmd show vsd
ID Def_Act ILTL OLTL NMLTL State Member LTLs
1 FRWD 51 50 1 ENA 49
n1000v#
```

Example 3-5 module** module_number **execute vemcmd show vsd ports

```
n1000v# module vem 4 execute vemcmd show vsd ports
LTL IfIndex VSD_ID VSD_PORT_TYPE
49 1c000010 1 REGULAR
50 1c000040 1 OUTSIDE
51 1c000030 1 INSIDE
n1000v#
```

Configuration Example

The following example shows how to configure VSD.

```
port-profile vsd1_member
  vmware port-group
  switchport access vlan 315
  virtual-service-domain vsd1
  no shutdown
  state enabled
port-profile svm_vsd1_in
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 310-319
  virtual-service-domain vsd1
  service-port inside default-action drop
  no shutdown
  state enabled
port-profile svm_vsd1_out
  vmware port-group
  switchport mode trunk
  switchport trunk allowed vlan 310-319
  virtual-service-domain vsd1
  service-port outside default-action drop
  no shutdown
```

Additional References

For additional information related to VSD configuration, see the following:

- Related Documents, page 3-11
- Standards, page 3-11

Related Documents

Related Topic	Document Title
Port Profiles	*Cisco Nexus 1000V Port Profile Configuration Guide, Release 4.2(1)SV1(4a)*
CLI	*Cisco Nexus 1000V Getting Started Guide, Release 4.2(1)SV1(4a)* *Cisco Nexus 1000V Command Reference, Release 4.2(1)SV1(4)*

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History

This section provides the VSD release history.

Feature Name	Releases	Feature Information
VSD	4.0(4)SV1(2)	This feature was introduced.