Configuring VSD

This chapter contains the following sections:

Information about Virtual Service Domains

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

Service Virtual Machine

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

Interface	Description
Management	A regular interface that manages the SVM. This interface 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 does not need to be routed through the SVM because it is considered to be safe.

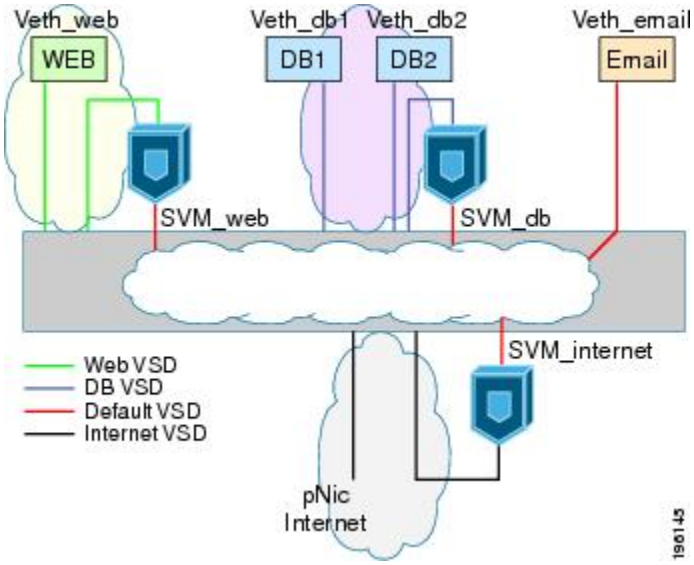
A VSD is formed by creating the following port profiles:

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.

The following diagram shows that a single VEM takes the place of vSwitches. The SVMs define the following VSDs in the diagram.

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 1: Virtual Service Domain Example



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 SVMs, first bring the SVM down, This action 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. The VSD feature will not function as expected if used with VShield 4.1.

Default Settings

Table 1: Telnet Default Settings

Parameters	Default
service-port default-action	Forward

Parameters	Default
switchport trunk allowed vlan	All

Configuring VSD

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. While performing this procedure, keep in mind the following points:

- If you do not configure a service port, the SVM will come up as a regular VM and flood 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.

Before you begin

Before beginning this procedure, be sure you:

- Are logged in to the CLI in EXEC mode.
- 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.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile***name*	Creates a port profile and places you into port profile configuration mode for the named port profile. The name can be up to 80 characters and must be unique for each port profile on the Cisco Nexus 1000V.
Step 3	switch(config-port-profile)# **switchport mode trunk**	Designates that the interfaces are switch trunk ports.
Step 4	switch(config-port-profile)# **switchport trunk allowed vlan***vlanID*	Allows all VLANs on the port.
Step 5	switch(config-port-profile)# **virtual-service-domain** *name*	Adds a VSD name to this port profile.
Step 6	switch(config-port-profile)# **no shutdown**	Administratively enables all ports in the profile.

	Command or Action	Purpose
Step 7	switch(config-port-profile)# **vmware port-group** *pg-name*	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. pg-name—Port group name. If you do not specify a pg-name, 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.

Step 8	switch(config-port-profile)# **service-port** { **inside** | **outside** } [**default-action** { **drop** | **forward** }]
	Example:
	`switch(config-port-profile)# service-port inside default-action forward`
	This example configures an inside VSD that forwards packets if the service port is down.
	Example:
	`switch(config-port-prof)# service-port outside default-action forward`
	This example configures an outside VSD that forwards packets if the service port is down.
		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.
		This command has the following variables:
		• inside—Inside network
		• outside—Outside network
		• default-action — (Optional) Action to be taken if service port is down.
		• drop—drops packets
		• forward: forwards packets
		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.

Step 9	switch(config-port-profile)# **state enabled**	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	(Optional) switch(config-port-profile)# **show virtual-service-domain name**	Displays the configuration for this VSD port profile. Use this to verify that the port profile was configured as expected. name—The name of the VSD.

	Command or Action	Purpose
Step 11	(Optional) switch(config-port-profile)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

```
switch# config terminal
switch(config)# port-profile webserver-inside
switch(config-port-profile)# switchport mode trunk
switch(config-port-profile)# switchport trunk allowed vlan all
switch(config-port-profile)# virtual-service-domain vsd1-webserver
switch(config-port-prof)# no shutdown
switch(config-port-prof)# vmware port-group webservers-inside-protected
switch(config-port-prof)# service-port inside default-action forward
switch(config-port-prof)# state enabled
switch(config-port-prof)# show virtual-service-domain vsd1-webserver
Default Action: forward

_____________________________
Interface        Type

_____________________________
Vethernet1       Member
Vethernet2       Member
Vethernet3       Member
Vethernet7       Inside
Vethernet8       Outside
switch(config-port-prof)# copy running-config startup-config
[########################################] 100%
```

Configuring a Member VSD Port Profile

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

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.

Before you begin

Before beginning this procedure, you must be logged in to the CLI in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	switch# **configure terminal**	Enters global configuration mode.
Step 2	switch(config)# **port-profile** *name*	Creates a port profile and places you in 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.

	Command or Action	Purpose
Step 3	switch(config-port-profile)# **switchport access vlan** *vlanID*	Assigns a VLAN ID to the access port for this port profile. VLAN ID—The VLAN identification number. The range of valid values is 1 to 3967.
Step 4	switch(config-port-profile)# **virtual-service-domain** *name*	Created and names a VSD for this port profile
Step 5	switch(config-port-prof)# **no shutdown**	Administratively enables all ports in the profile.
Step 6	switch(config-port-prof)# **state enabled**	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 7	(Optional) switch(config-port-prof)# **show virtual-service-domain** *name*	Displays the configuration for this VSD port profile. Use this to verify that the port-profile was configured as expected
Step 8	(Optional) switch(config-port-prof)# **copy running-config startup-config**	Copies the running configuration to the startup configuration.

Example

```
switch# configure terminal
switch(config)# port-profile vsd1-member
n1000v(config-port-profile)# switchport access vlan 315
n1000v(config-port-profile)# virtual-service-domain vsd1-webserver
n1000v(config-port-prof)# no shutdown
n1000v(config-port-prof)# state enabled
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)# copy running-config startup-config
[########################################] 100%


n1000v# config t
n1000v(config)# port-profile vsd1_member
n1000v(config-port-profile)# vmware port-group
n1000v(config-port-profile)# switchport access vlan 315
n1000v(config-port-profile)# virtual-service-domain vsd1
n1000v(config-port-profile)# no shutdown
  state enabled
n1000v(config-port-profile)# port-profile svm_vsd1_in
n1000v(config-port-profile)# vmware port-group
```

```
n1000v(config-port-profile)# switchport mode trunk
n1000v(config-port-profile)# switchport trunk allowed vlan 310-319
n1000v(config-port-profile)# virtual-service-domain vsd1
n1000v(config-port-profile)# service-port inside default-action drop
n1000v(config-port-profile)# no shutdown
  state enabled
n1000v(config-port-profile)# port-profile svm_vsd1_out
n1000v(config-port-profile)# vmware port-group
n1000v(config-port-profile)# switchport mode trunk
n1000v(config-port-profile)# switchport trunk allowed vlan 310-319
n1000v(config-port-profile)# virtual-service-domain vsd1
n1000v(config-port-profile)# service-port outside default-action drop
n1000v(config-port-profile)# no shutdown
```

Verifying the Configuration

Use one of the following commands to verify the configuration:

Command	Purpose
show virtual-service-domain name *vsd-name*	Displays a specific VSD configuration.
show virtual-service-domain brief	Displays a summary of all VSD configurations.
show virtual-service-domain interface	Displays the interface configuration for all VSDs.
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.
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.

Example: show virtual-service-domain name vsd_name

```
switch# show virtual-service-domain name vsd1
Default Action: drop

_____________________________
Interface        Type

_____________________________
Vethernet1       Member
Vethernet2       Member
Vethernet3       Member
Vethernet6       Member
Vethernet7       Inside
Vethernet8       Outside

switch#
```

Example: show virtual-service-domain brief

```
switch# 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
switch#
```

Example: show virtual-service-domain interface

```
switch# show 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
switch#
```

Example: module module_number execute vemcmd show vsd

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

module module_number execute vemcmd show vsd ports

```
switch# 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
switch#
```

Configuration Examples for VSD

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
```

Feature History for VSD

This table includes only the updates for those releases that have resulted in additions or changes to the feature.

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