Configuring Firewall Profiles and Policy Objects

This chapter contains the following sections:

- Information About Cisco VSG Policy Objects, page 1
- Configuring Service Firewall Logging, page 10
- Verifying the Cisco VSG Configuration, page 10
- Configuration Limits, page 11

Information About Cisco VSG Policy Objects

This section describes how you can use Cisco Prime Network Services Controller (Prime NSC) to configure and manage the firewall policy objects on Cisco VSG.

Note You can configure Cisco VSG only through Cisco PNSC. Currently, we do not support out of band configuration and management of firewall policy objects.

Information About Cisco VSG Policy Objects and Firewall Profiles

Cisco VSG Policy Object Configuration Prerequisites

Cisco VSG policy objects have the following prerequisites:

- You must have the Cisco Nexus 1000V Advanced Edition license installed on the Cisco Nexus 1000V Series switch. Starting with Cisco Nexus 2.1 Release, Cisco VSG license is bundled with Cisco Nexus 1000V Advanced Edition licenses.
- Ensure that you have enough licenses to cover the number of ESX hosts (VEMs) you want to protect.
- Create port profiles for the service and HA interfaces of Cisco VSG on the Virtual Supervisor Module (VSM).

- You have the Cisco VSG software installed and the basic installation completed. For details, see the Cisco VSG for VMware vSphere and Cisco Prime NSC Installation Guide.
- The data IP address and management IP addresses must be configured. To configure the data IP address, see the Cisco VSG for VMware vSphere and Cisco Prime NSC Installation Guide.
- You have the attribute details required for your security policies.
- You are logged in to the Cisco VSG CLI in EXEC mode.

Cisco VSG Configuration Guidelines and Limitations

The Cisco VSG policy objects and firewall policies have the following configuration guidelines and limitations:

- The Management VLAN must be extended to the Cloud and configured as system VLAN.
- The Service VLANs are configured on the uplink ports. (They are not required to be on the system VLAN.)
- Do not configure the same network IP address on the management and data interfaces (data0) of the Cisco VSG.

For any configuration and management tasks, the following requirements must be met:

- The Cisco VSG software must be operating with three network adapters. The network labels are as follows:
  - Service (Eth0) as the port-profile
  - Mgmt (Eth1) as the management VLAN
  - HA (Eth2) as the port-profile
- You have the Cisco VSG VM powered on and the data interface IP address (for data0) and management interface IP address configured.

See the Cisco VSG for VMware vSphere and Cisco Prime NSC Installation and Upgrade Guide, for details about assigning network labels to the network adapters.

Default Settings

Table 1: Default Parameter Settings for Cisco VSG

Parameters	Default
rule policy object	drop

Zones

A zone is a logical group of VMs or hosts. Zones simplify policy writing by allowing users to write policies based on zone attributes using zone names. The zone definitions map the VMs to the zones. The logical group

definition can be based on the attributes associated with a VM or a host, such as VM attributes. Zone definitions can be written as condition-based subnet and endpoint IP addresses.

Because zones can be shared between various rules with different directions, the attributes used in a zone should not have a directional sense and must be neutral.

Zone Example

This example shows how to display a zone in your network:

```
vsg# show running-config zone zone1
zone zone1
cond-match-criteria: match-any
condition 1 net.ip-address eq 1.1.1.1
condition 2 net.port eq 80
```

Object Groups

An object group is a set of conditions relevant to an attribute.

Because the object groups can be shared between various rules with different directions, the attributes used in an object group condition should not have a directional sense and must be neutral. An object group is a secondary policy object that assists in writing firewall rules. A rule condition can refer to an object group by using an operator.

Object Group Example

This example shows how to display the object groups in your network:

```
vsg# show running-config object-group g1
object-group g1 net.port
match 10 in-range protocol 6 port 10 30
match 11 eq protocol 6 port 21 inspect ftp
```

Rules

Firewall rules can consist of multiple conditions and actions. Rules can be defined in a policy as a condition for filtering the traffic. The policy engine uses the policy as a configuration that filters the network traffic that is received on the Cisco VSG. The policy engine uses two types of condition matching models for filtering the network traffic:

- AND Model: A rule is set to matched when all the attributes in a rule match.
- OR model: A rule is set to matched when any one of the attributes in a rule match. The attributes are classified into five different types of columns. The five columns in an OR model are:
  - Source: Attribute to identify source host.
  - Destination: Attribute to identify destination host.
  - Service: Attribute to identify service at the destination host.
  - Ether type: Attribute to identify link level protocol.
  - Source port: Attribute to identify source port.

Rule Example

This example shows how to display the rule in your network:

```
vsg# show running-config rule r2
rule r2
cond-match-criteria: match-all
   dst-attributes
     condition 10 dst.zone.name eq z1@r2
   service/protocol-attribute
condition 11 net.service eq protocol 6 port 21 inspect ftp
action permit
```

Policies

A policy enforces network traffic on a Cisco VSG. A key component operating on the Cisco VSG is the policy engine. The policy engine takes the policy as a configuration and executes it when enforced against the network traffic that is received on the Cisco VSG. A policy is constructed by using the following set of policy objects:

- Rules
- Conditions
- Actions
- Objects groups
- Zones

A policy is bound to a Cisco VSG by using a set of indirect associations. The security administrator can configure a security profile and then refer to a policy name within the security profile. The security profile is associated with a port profile that has a reference to a Cisco VSG.

Policy Examples

This example shows how the policy is expressed in the **show running-config** command output:

```
vsg# show running-config policy p2@root/T1
policy p2@root/T1
  rule r2 order 10
```

This example shows how conditions are expressed in the **show running-config** command output:

```
condition 1 dst.net.ip-address eq 2.2.2.2
condition 2 src.net.ip-address eq 1.1.1.1
```

This example shows how an action is expressed in the **show running-config** command output:

```
action permit
```

Cisco Virtual Security Gateway Attributes

This section describes Cisco VSG attributes.

Information About Attribute Name Notations

Directional Attributes

A firewall policy is direction sensitive with regard to incoming or outgoing packets. An attribute in a rule condition requires that you have specified if the attribute is relevant to a source or a destination. The prefixes src., dst., or an attribute name are used to provide the sense of direction.

Neutral Attributes

Because object groups and zones can be shared between various rules with different directions, the attributes used in a zone should not have a directional sense. Attributes without a directional sense (that do not provide a direction prefix such as src. or dst.) are called neutral attributes.

Two rule conditions with different directions can share the same object group definition. A neutral attribute and net.ip-address used in the object group can be associated with the directional attributes, such as src.net.ip-address and dst.net.ip-address, used in the different rules.

Attribute Classes

Attributes are used in configuring policy rules and conditions, or zone definitions. Zones can be defined using VM attributes.

Neutral Attributes

Because object groups and zones can be shared between various rules with different directions, the attributes used in a zone should not have a directional sense. Attributes without a directional sense (that do not provide a direction prefix such as src. or dst.) are called neutral attributes.

Two rule conditions with different directions can share the same object group definition. A neutral attribute and net.ip-address used in the object group can be associated with the directional attributes, such as src.net.ip-address and dst.net.ip-address, used in the different rules.

VM Attributes

The VM attributes are related to the VM infrastructure and include the following classes of VM attributes:

- Virtual infrastructure attributes—These attributes are obtained from the VMware vCenter and are mapped to names.
- Port profile attributes—These attributes are associated with port profiles.
- Custom attributes—These attributes can be configured under a service profile.

The following table describes the VM attributes that are supported by Cisco VSG.

Description	Name
Name of VM	src.vm.name dst.vm.name vm.name **Note** vm.name is a neutral attribute.
Name of VM DNS	dst.vm.os-hostname src.vm.os-hostname **Note** The VM DNS name attribute is available if the VMware tool is installed on the VM and the VM configuration parameter isolation.tools.setinfo.disable is set to False.
Name of host parent (host)	src.vm.host-name dst.vm.host-name vm.host-name **Note** vm.host-name is a neutral attribute.
Full name of OS guest (includes the version)	src.vm.os-fullname dst.vm.os-fullname vm.os-fullname **Note** vm.os-fullname is a neutral attribute.
Name of associated virtual application	src.vm.vapp-name dst.vm.vapp-name vm.vapp-name **Note** vm.vap-name is a neutral attribute.
Name of associated cluster	src.vm.cluster-name dst.vm.cluster-name vm.cluster.name **Note** vm.cluster.name is a neutral attribute.
Inventory path of the VM	src.vm.inventory-path dst.vm.inventory-path vm.inventory-path **Note** vm.inventory-path is a neutral attribute.

Description	Name
Name of port profile associated with specific vNIC	src.vm.portprofile-name dst.vm.portprofile-name vm.portprofile-name **Note** vm.portprofile-name is a neutral attribute.
Custom attributes from security profile of associated port group. **Note** For every unique custom-attribute xxx, the synthesized attribute name is src.vm.custom.xxx or dst.vm.custom.xxx. The policy uses the synthesized attribute name.	src.vm.custom.xxx dst.vm.custom.xxx vm.custom.xxx **Note** vm.custom.xxx is a neutral attribute.

Custom VM attributes are user-defined attributes that can be configured under a service profile.

This example shows how to verify the VM attributes on a Cisco VSG:

```
firewall(config)# show vsg vm
VM uuid          : 852a1ff3-149d-4c75-adfa-c75e0d583d37
VM attributes :
  name                        : vm
  os-fullname               : windows server 2012 r2 datacenter
  os-hostname             : vm


Zone(s) :
```

Zone Attributes

Table 2: Zone Attributes Supported by Cisco VSG

Description	Name
Zone name. This is a multi-valued attribute and can belong to multiple zones at the same time.	src.zone.name dst.zone.name zone.name **Note** zone.name is a neutral attribute.

Security Profiles

The security profile defines custom attributes that can be used to write policies. All the VMs tagged with a given port profile inherit the firewall policies and custom attributes defined in the security profile associated with that port profile. Each custom attribute is configured as a name value pair such as state = CA.

This example shows how to verify the security profile on a Cisco VSG:

```
vsg_d3338(config-nsc-policy-agent)# show vsg security-profile table
--------------------------------------------------------------------------------
Security-Profile Name VNSP ID Policy Name
--------------------------------------------------------------------------------
default@root 1 default@root
sp10@root/tenant_d3338 9 ps9@root/tenant_d3338
sp9@root/tenant_d3338 10 ps9@root/tenant_d3338
sp2@root/tenant_d3338 11 ps1@root/tenant_d3338
sp1@root/tenant_d3338 12 ps1@root/tenant_d3338
```

This example shows how to verify the security profile on a Cisco VSG:

```
vsg_d3338(config-nsc-policy-agent)# show vsg security-profile
VNSP : sp10@root/tenant_d3338
VNSP id : 9
Policy Name : ps9@root/tenant_d3338
Policy id : 3
Custom attributes :
  vnsporg : root/tenant_d3338
VNSP : default@root
VNSP id : 1
Policy Name : default@root
Policy id : 1
Custom attributes :
  vnsporg : root
VNSP : sp1@root/tenant_d3338
VNSP id : 12
Policy Name : ps1@root/tenant_d3338
Policy id : 2
Custom attributes :
  vnsporg : root/tenant_d3338
location : losangeles
color9 : test9
color8 : test8
color7 : test7
color6 : test6
color5 : test5
color4 : test4
color3 : test3
color2 : test2
color13 : test13
color12 : test12
color11 : test11
color10 : test10
color1 : test1
color : red
VNSP : sp2@root/tenant_d3338
VNSP id : 11
Policy Name : ps1@root/tenant_d3338
Policy id : 2
Custom attributes :
  vnsporg : root/tenant_d3338
  location : sanjose
  color : blue
VNSP : sp9@root/tenant_d3338
VNSP id : 10
Policy Name : ps9@root/tenant_d3338
Policy id : 3
Custom attributes :
  vnsporg : root/tenant_d3338
```

Viewing Security Profiles and Policies on the Cisco Prime NSC and the Cisco VSG

The Cisco Prime NSC GUI provides a view of the Cisco VSG security policy objects. The policy objects shown in the Cisco Prime NSC GUI are not necessarily shown in the same organizational path location as they appear in the Cisco VSG CLI when you enter the **show running-config** command.

For example, in the Cisco Prime NSC GUI, if the virtual data center DC1 is under the tenant and the application APP1 is under DC1, the vnsp app1-sp in the APP1 level is pointing to the policy set ps1 at the DC level.

The following figure shows the Cisco Prime NSC GUI organization structure.

Figure 1: Cisco Prime NSC Organizational Hierarchy for a Tenant, Data Center, and Application

```
security-profile app1-sp@root/tenant4/DC1/APP1
policy ps1@root/tenant4/DC1/APP1
custom-attribute loc "sunnyvale"
custom-attribute vnsporg "root/tenant4/dc1/app1"
```

The output of the **show running-config** command shows that the policy set and its objects are resolved from the APP1 level where the security profile is defined. The actual location of the objects in the Cisco Prime NSC GUI is at the DC1 level.

```
policy ps1@root/tenant4/DC1/APP1
rule p1/r1@root/tenant4/DC1/APP1 order 101
```

The policy object DNs that are shown in the Cisco VSG **show running-config** command output are shown with a DN relative to where they are resolved from. The policy object DNs are not where the actual policy objects are in the Cisco Prime NSC organizational hierarchy.

However, security profiles are shown with the DN where the actual security profile is created on the Cisco Prime NSC organizational hierarchy.

Policy objects are resolved upwards from where the security profile is located in the Cisco Prime NSC organizational hierarchy.

In the following example, the Cisco VSG is configured with the following specifications:

- The security profile (VNSP) sp1 has policy-set ps1 in which there is a policy p1 that includes a rule, r1.
- The policy-set ps1 is located at root in the organization tree on the Cisco Prime NSC.
- The policy p1 is located at root in the organization tree on the Cisco Prime NSC.
- The rule r1 is placed in the policy p1 on the Cisco Prime NSC (the Cisco Prime NSC does not allow you to create a rule object in and of itself).
- The security profile sp1 is placed in tenant_d3337/dc1 on the Cisco Prime NSC.

All Cisco VSGs in the tenant_d3337 have the following **show running-config** command output (this configuration is replicated to all Cisco VSGs in the leaf path):

```
security-profile sp1@root/tenant_d3337/dc1
policy ps1@root/tenant_d3337/dc1
custom-attribute vnsporg "root/tenant_d3337/dc1"
policy p1@root/tenant_d3337/dc1
rule p1/r1@root/tenant_d3337/dc1 order 101
```

Note The policy objects above do not actually exist at the DC1 level of the organization tree on the Cisco Prime NSC but are resolved from that location in the Cisco Prime NSC organization tree.

Configuring Service Firewall Logging

See the "Enabling Global Policy-Engine Logging" section of the *Cisco VSG for VMware vSphere and Cisco Prime NSC Installation and Upgrade Guide*.

Verifying the Cisco VSG Configuration

To display the Cisco VSG configuration, use the **show running-config** command.

```
vsg# show running-config

!Command: show running-config
!Time: Wed Jan 26 15:39:57 2014

version 5.2(1)VSG2(1.2)
feature telnet
no feature http-server

username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na. role network-operator
username admin password 5 $1$CbPcXmpk$l31YumYWiO0X/EY1qYsFB. role network-admin
username vsnbetauser password 5 $1$mr/jBgON$hoJsM9ACdPHRWPM3KpI6/1 role network-admin

banner motd #Nexus VSN#

ssh key rsa 2048
ip domain-lookup
ip domain-lookup
hostname vsg
snmp-server user admin auth md5 0x0b4894684d52823092c7a7c0b87a853d priv
0x0b4894684d52823092c7a7c0b87a853d localizedkey engineID 128:0:0:9:
3:0:0:0:0:0:0
snmp-server user vsnbetauser auth md5 0x272e8099cab7365fd1649d351b953884 priv
0x272e8099cab7365fd1649d351b953884 localizedkey engineID 128:
0:0:9:3:0:0:0:0:0:0

vrf context management
  ip route 0.0.0.0/0 10.193.72.1
vlan 1
port-channel load-balance ethernet source-mac
port-profile default max-ports 32

vdc vsg id 1
limit-resource vlan minimum 16 maximum 2049
limit-resource monitor-session minimum 0 maximum 2
limit-resource vrf minimum 16 maximum 8192
limit-resource port-channel minimum 0 maximum 768
limit-resource u4route-mem minimum 32 maximum 32
limit-resource u6route-mem minimum 16 maximum 16
```

```
limit-resource m4route-mem minimum 58 maximum 58
limit-resource m6route-mem minimum 8 maximum 8
interface mgmt0
  ip address 10.193.73.185/21
interface data0
cli alias name ukickstart copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-kickstart-mzg.VSG2.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG2.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG2.1.bin
bootflash:dplug
cli alias name uimage copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-mzg.VSG2.1.bin
bootflash:user_bin
line console
boot kickstart bootflash:/ukickstart sup-1
boot system bootflash:/user_bin sup-1
boot kickstart bootflash:/ukickstart sup-2
boot system bootflash:/user_bin sup-2
mgmt-policy TCP permit protocol tcp
  ha-pair id 25
security-profile profile1
  policy p2
security-profile profile2
  policy p1
custom-attribute state "texas"
object-group g1 net.port
  match 1 eq 80
  match 2 eq 443
zone zone1
  condition 1 net.ip-address eq 1.1.1.1
  condition 2 net.port eq 80
  condition 2 net.port eq 80
rule r2
  condition 1 dst.net.ip-address eq 2.2.2.2
  condition 2 src.net.ip-address eq 1.1.1.1
  condition 3 src.net.port eq 100
  condition 4 dst.net.port eq 80
  condition 5 net.protocol eq 6
  action 1 permit
rule r5
  condition 1 net.ethertype eq 0x800
  action 1 inspect ftp
rule r6
rule r7
policy p2
  rule r2 order 10
policy p1
  rule r2 order 10

service firewall logging enable
nsc-policy-agent
 registration-ip 10.193.73.190
 shared-secret **********
 log-level info
vsg#
```

Configuration Limits

Table 3: Maximum Configuration Limits for Configuring the Cisco VSG

Feature	Maximum Limit
Zones in Cisco VSG	512

Feature	Maximum Limit
Rules per policy	1024
Policy set per Cisco VSG	16
Object Group in Cisco VSG	512
Total number of conditions	16k
Maximum rules per Cisco VSG	1024