Cisco Virtual Security Gateway Firewall Profiles and Policy Objects

This chapter describes how to configure the Cisco Virtual Security Gateway (VSG) firewall profiles and policy objects.

This chapter includes the following sections:

Information About Cisco VSG Firewall Policy Objects

Use the Cisco Virtual Network Management Center (VNMC) to do all configuration and management of the Cisco VSG.

Note When the policy-agent (PA) is installed, the command-line interface (CLI) is unavailable for configuring policy-related objects on the Cisco VSG. When the PA is uninstalled (removed), you can again configure the policies (and policy objects) from the CLI; however, we recommend that you use the Cisco VNMC for all configuration and management of the Cisco VSG firewall policy objects.

Cisco VSG Firewall Policy Objects

This section includes the following topics:

Cisco VSG Policy Object Configuration Prerequisites

Cisco VSG policy objects have the following prerequisites:

- You must have the NEXUS_VSG_SERVICES_PKG license installed on the Cisco Nexus 1000V Series switch.
- 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 Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*.
- The data IP address and management IP addresses must 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 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 has the following configuration guidelines and limitations:

- The Management VLAN must be on the VM network vSwitch.
- The HA and 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 Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 Installation and Upgrade Guide*, for details about assigning network labels to the network adapters.

Default Settings

Table 6-1 lists the default setting for the Cisco VSG parameters.

Table 6-1 Default Parameter

Parameters	Default
rule policy object	drop

Zones

A zone is a logical group of virtual machines (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 defined in the vCenter. Zone definitions can be written as condition-based subnet and endpoint IP addresses.

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

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

```
vsg# show running-config zone zone1
zone zone1
   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 that are relevant to an attribute. Because object groups and zones 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.

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

```
vsg# show running-config object-group g1
object-group g1 net.port
  match 1 eq 80
  match 2 eq 443
```

Rules

Firewall rules can consist of multiple conditions and actions. Rules can be defined in a policy as a condition-based subnet or endpoint IP addresses and VM attributes.

Actions are the result of a policy evaluation. You can define and associate one or more of the following actions within a specified rule:

- Permit
- Drop packet
- Log

- Inspection

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

```
vsg# show running-config rule r2
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
```

Policies

Firewall policies bind rules to a given policy, creating a rank among the rules. A policy enforces network traffic on a Cisco VSG and is constructed by using the following set of policy objects:

- Rules
- Conditions
- Actions
- Object-groups
- Zones

A policy is bound to a Cisco VSG 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.

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

```
vsg# show running-config policy p2
policy p2
  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 1 permit
```

Cisco Virtual Security Gateway Attributes

This section describes Cisco Virtual Security Gateway attributes.

This section includes the following topics:

Information About Attribute Name Notations

This section includes the following topics:

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 an object group 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

Cisco VSG attributes are classified into the following classes:

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

Network Attributes

This section describes the VSG network attributes (see Table 6-2).

.

Table 6-2 Network Attributes

Description	Name
Source IP address	src.net.ip-address
Source port	src.net.port
Destination IP address	dst.net.ip-address
Destination port	dst.net.port
IP address[1]	net.ip-address
Port[1]	net.port
IP Protocols 9[1]	net.protocol
EtherType of the Layer 2 mode frame[1]	net.ethertype

1. Neutral attribute

VM Attributes

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

- Virtual infrastructure attributes—These attributes are obtained from the VMware vCenter and are mapped to the names listed in Table 6-3.
- Port profile attributes—These attributes are associated with port profiles.
- Custom attributes—These attributes can be configured under a service profile.

Table 6-3 describes the VM attributes supported.

Table 6-3 VM Attributes

Description	Name
Name of VM	src.vm.name dst.vm.name vm.name[1]
Name of host parent (ESX host)	src.vm.host-name dst.vm.host-name vm.host-name[1]
Full name of OS guest (includes the version)	src.vm.os-fullname dst.vm.os-fullname vm.os-fullname[1]
Name of associated virtual application	src.vm.vapp-name dst.vm.vapp-name vm.vapp-name[1]
Name of associated cluster	src.vm.cluster-name dst.vm.cluster-name vm.cluster.name[1]
Inventory path of the VM	src.vm.inventory-path dst.vm.inventory-path vm.inventory-path[1]
Name of port profile associated with specific vNIC	src.vm.portprofile-name dst.vm.portprofile-name vm.portprofile-name[1]
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[1]

1. Neutral attributes

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:

```
vsg# show vsg vm

VM uuid          : 421c2a2d-5e7c-3bdb-51e7-f7528163b021
VM attributes :
    name                      : centos5.3_3_vem1_clone
    vapp-name                 : apps
    os-fullname               : red hat enterprise linux 4 (32-bit)
    tools-status              : installed
    host-name                 : 10.193.75.20
    cluster-name              : dc_dm1_clu1
```

Zone Attributes

Table 6-4 lists the zone attributes supported by the Cisco VSG.

Table 6-4 Zone Attributes

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[1]

1. 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-vnm-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-vnm-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
```

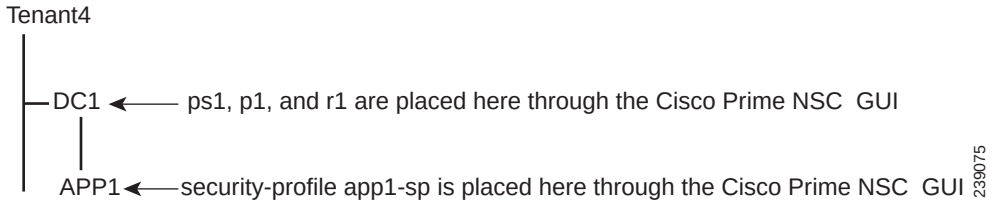
Viewing Security Profiles and Policies on the Cisco VNMC and the Cisco VSG

The Cisco VNMC GUI provides a view of the Cisco VSG security policy objects. The policy objects shown in the Cisco VNMC 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 VNMC 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.

Figure 6-1 shows the Cisco VNMC GUI organization structure.

Figure 6-1 Cisco VNMC 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 VNMC 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 VNMC organizational hierarchy.

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

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

EXAMPLE

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 VNMC.
- The policy p1 is located at root in the organization tree on the Cisco VNMC.
- The rule r1 is placed in the policy p1 on the Cisco VNMC (the Cisco VNMC 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 VNMC.

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 VNMC but are resolved from that location in the Cisco VNMC organization tree.

Configuring Service Firewall Logging

See "Enabling Global Policy-Engine Logging" section of *Cisco Virtual Security Gateway, Release 4.2(1)VSG1(3.1) and Cisco Virtual Network Management Center, Release 1.3 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 2011

version 4.2(1)VSG1(1)
feature telnet
no feature http-server

username admin password 5 $1$CbPcXmpk$l31YumYWiO0X/EY1qYsFB.  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

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.VSG1.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG1.1.bin
bootflash:ukickstart
cli alias name udplug copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-dplug-mzg.VSG1.1.bin
bootflash:dplug
cli alias name uimage copy scp://user@<ip
address>/ws/sjc/baselard_latest/build/images/gdb/nexus-1000v-mzg.VSG1.1.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
vnm-policy-agent
  registration-ip 10.193.73.190
  shared-secret **********
  log-level info

vsg#
```

Configuration Limits

Table 6-5 lists the maximum configuration limits for configuring the Cisco VSG.

Table 6-5 Maximum Configuration Limits

Feature	Maximum Limits
Zones in Cisco VSG	512 counts
Rules per policy	1024 counts
Policy set per Cisco VSG	16 counts
Object Group in Cisco VSG	512
Total number of conditions	16K
Maximum rules per Cisco VSG	1024