Configuring Firewall Profiles and Policy Objects

This chapter contains the following sections:

Information About Cisco VSG Firewall Policy Objects

This section describes how you can use the Cisco Virtual Network Management Center (VNMC) to configure and manage the firewall policy objects on 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 to configure and manage the Cisco VSG firewall policy objects

Cisco VSG Policy Object Configuration Prerequisites

Cisco VSG policy objects have the following prerequisites:

- You must have the NEXUS_VSG_MSFT_SERVICES_PKG license installed on the Cisco Nexus 1000V Series switch.
- 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 Microsoft Hyper-V and Cisco VNMC Installation Guide*.
- The data IP address and management IP addresses must be configured. To configure the data IP address, see the *Cisco VSG for Microsoft Hyper-V and Cisco VNMC 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 on the VM network Microsoft virtual Switch.
- 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 (control0) 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 Microsoft Hyper-V and Cisco VNMC Installation 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

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
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 permit
```

Cisco Virtual Security Gateway Attributes

This section describes Cisco VSG attributes.

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.

Network Attributes

Table 2: Network Attributes Supported By Cisco VSG

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 **Note** This is a neutral attribute.	net.ip-address
Port **Note** Neutral attribute.	net.port
IP Protocols 9 **Note** Neutral attribute.	net.protocol
EtherType of the frame **Note** Neutral attribute.	net.ethertype

Zone Attributes

Table 3: 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.

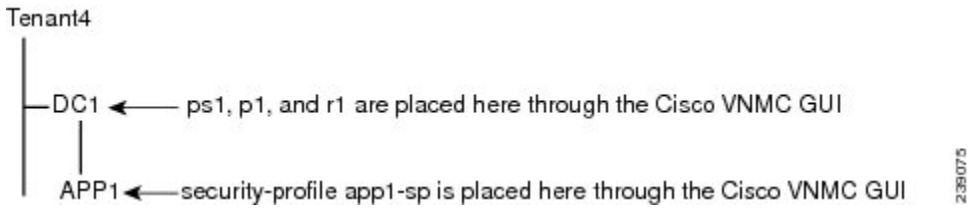
Viewing Security Profiles and Policies on the Cisco VNMC and the Cisco VSG

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.

The following figure shows the Cisco VNMC GUI organization structure.

Figure 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
```

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.

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

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 the "Enabling Global Policy-Engine Logging" section of the *Cisco VSG for Microsoft Hyper-V and Cisco VNMC Installation 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 May 26 15:39:57 2013

version 4.2(1)VSG1(4)
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.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
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 4: 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	32
Maximum rules per Cisco VSG	1024