CHAPTER 6

Troubleshooting Policy Engine Issues

This chapter describes how to troubleshoot issues that might occur on the policy engine.

This chapter includes the following sections:

Policy Engine Troubleshooting Commands

When there are policy engine issues, use these commands to troubleshoot:

- **show run rule**—Displays all rules configured in the Cisco VSG.
- **show run policy**—Displays all policies configured in the Cisco VSG.
- **show run zone**—Displays all zones configured in the Cisco VSG.
- **show run object-group**—Displays all object-groups configured in the Cisco VSG.
- **show policy-engine stats**—Displays statistics about the rule hits in the Cisco VSG.
- **clear policy-engine stats**—Clears the statistics about the rule hits in the Cisco VSG.

Policy/Rule Not Working as Expected

When policies or rules do not work as expected, do the following:

- Check the show policy-engine statistics and verify that the hits are incrementing by entering the **show policy-engine stats** command. If not, go to the module interactions section to see why hits are not incrementing.
- When policy engine statistics are incrementing, check the rule name that is being hit.
- View the configuration of the rule by entering the **show run rule** *rule-name* command. Verify that the conditions are configured correctly.

Policy/Rule Based on VM Attributes Not Working - But Without VM Attributes Policy/Rule Works

A policy or rule with VM attributes requires additional data for the Cisco VSG to evaluate the policy engine. This data, if not complete, can result in incorrect or not applicable hits in the statistics. When the policy or rule is configured with VM attributes, make sure that you see VM information in the following outputs:

- **show vsg ip-binding**—The output should have the IPs of all the VMs for which the rules will be written in the Cisco VSG.

- **show vsg dvport**—The output should have the port profile and IP information of all the VMs for which rules will be written in the Cisco VSG.

- **show vsg vm**—The output should have VM attribute values (whichever is present in the SCVMM for a given VM) of all the VMs for which rules will be written in the Cisco VSG.

Policy/Rule Configured for Non-Firewalled VMs (port profiles) Not Working

To enable firewall protection for a VM, you must configure the vn-service and org CLI in the port profile at the VSM—this enables access to IP addresses and other network attributes for the VM.

To turn on firewall protection for the server VM (any traffic to or from server VM is protected by the Cisco VSG but not the client VM), write a rule saying that the source with the Source IP address and destination with the Destination VM IP is permitted by doing the following:

- Configure the vn-service and org CLI in the server VM port profile at the VSM.

- Configure the without vn-service and org for the client VM port profile at VSM (no vn-service and no org).

- Write a rule with a source condition source IP that contains the Client VM IP and a destination IP that contain server VM IP, action permit.

Policy Engine Statistics Show Hits as 0 and Traffic Not Reaching the Cisco VSG

Confirm that the buffers in use are not zero by entering the **show ac-driver statistics** command. If zero, check/fix the adapter type.

Microsoft Hyper-V offers the choice between network adapter and legacy network adapter; use the regular network adapter for each interface.