ACI Integration Module Support for System Security Group

Revised: October 21, 2021,

New and Changed Information

The table provides an overview of the significant changes to this document.

Feature	Description
Cisco APIC ML2 Plug-in Release 5.2(3)	The document provides details about ACI Integration Module (AIM) support for System Security Group.

Overview

A security group is a collection of network access rules that are used to limit the types of traffic that have access to instances. The associated rules in each security group control the traffic to instances in the group. You can add rules to or remove rules from a security group, and you can modify rules for the default, and any other security group.

System security group (sg) is an operator level security group applicable for the entire OpenStack VMM domain. This operator level / system level security group cannot be overridden by other security groups from the common, and other tenants. Traffic is allowed only if it matches a system security group rule and a normal security group rule. The system security group rules can be fine-tuned further by other security group rules.

ACI Integration Module (AIM) enables the transfer of configuration from the Neutron Database to APIC. The system security group is configured using AIM and the relevant configuration commands are discussed in detail, later in this document.

You can configure the system security group, using the **aimctl** interface.

Note System security group is not configured by default. When system security groups are not configured, the default OpenStack behaviour is enforced, which is, traffic is allowed or denied based on the security groups attached to the OpenStack instances.

Benefits of System Security Group

- The system security group helps you to define a universal rule(s) for your cloud.
- You can create multiple subjects under one system security group. Subjects are used for grouping rules. Different types of rules can be grouped separately using subjects.

Restrictions for System Security Group

- There is only one system security group per VMM Domain.
- System security group rules cannot be overridden by other security group rules. If packets do not match any rules in system security group, then, they will be dropped, even when matching rules are present in other configured security groups.

Configuring a System Security Group

Use this procedure to create and configure a system security group.

Before you begin

From the Undercloud OpenStack node, log in to one of the overcloud controller nodes. To get in to the aim container (for OSP 13), you can use the **docker exec -it ciscoaci_aim bash** command. For OSP 16, use the **podman** command.

Procedure

Step 1 **aimctl manager system-security-group-create**

Creates a system security group.

For more system sg group commands, see System Security Group Commands, on page 3.

Step 2 **aimctl manager system-security-group-subject-create** *subject_name*

Creates a system security group subject.

For more system sg subject commands, see System Security Group Subject Commands, on page 3.

Step 3 **aimctl manager system-security-group-rule-create** *subject_name rule_name* [*--ip_protocol*] [*--direction*] [*--from_port --to_port*] [*--remote_ips*] [*--ethertype*] [*--connection_tracking*]

Creates a system security group rule for a subject with optional parameters.

For more system sg rule commands, and details about the various options for the rule commands, see System Security Group Rule Commands, on page 4.

Configuration Example for System Security Group

The following is an example of a system security group with subject name, *sub1* and rule parameters as defined below.

```
aimctl manager system-security-group-create
aimctl manager system-security-group-subject-create system
aimctl manager system-security-group-rule-create system syn --ip_protocol=tcp --from_port=22 --to_port=22
--ethertype=ipv4 --direction=egress --remote_ips=30.30.30.0/24 —conn_track=normal
```

System Security Group Commands

Commands for managing system security groups:

- To create a system security group— **aimctl manager system-security-group-create**
- To delete a system security group—**aimctl manager system-security-group-delete**
- To display details of a system security group—**aimctl manager system-security-group-show**

System Security Group Subject Commands

Commands for managing subjects of a system security group:

- To create a subject for a system security group— **aimctl manager system-security-group-subject-create** *name*

- To delete a subject for a system security group—**aimctl manager system-security-group-subject-delete** *name*
- To describe a subject for a system security group—**aimctl manager system-security-group-subject-describe**
- To display all the details of a subject for a system security group—**aimctl manager system-security-group-subject-show** *name*

System Security Group Rule Commands

Commands for managing system security group rules:

- To create a system security group rule for a subject—**aimctl manager system-security-group-rule-create** *subject_name rule_name* [*--ip_protocol*] [*--direction*] [*--from_port --to_port*] [*--remote_ips*] [*--ethertype*] [*--connection_tracking*]
- To update a system security group rule for a subject—**aimctl manager system-security-group-rule-update** *subject_name rule_name* [*--ip_protocol*] [*--direction*] [*--from_port --to_port*] [*--remote_ips*] [*--ethertype*] [*--connection_tracking*]
- To delete a system security group rule for a subject— **aimctl manager system-security-group-rule-delete** *subject_name rule_name*
- To display rules in a subject of a system security group— **aimctl manager system-security-group-rule-list**
- To display details of a rule in a subject of a system security group—**aimctl manager system-security-group-rule-show** *subject_name rule_name*

Parameters for system security group rules commands

If system security group rules are not configured, traffic flows according to normal sg rules. When system sg rules are configured, traffic has to match rules from both the security groups (system/normal) to be allowed.

Packets matching the normal security group rule have to first match with the system security group rule. Traffic is dropped, if it does not match any rule(s) in the system security group even if a matching rule is present in a normal security group. Therefore, it is crucial to design normal security group rules in alignment with system security group rule.

This section explains how to identify whether a normal security group rule aligns with the system security group rule(s). Details for parameters of a system security group rule:

- Remote IPs: If a rule defined in the normal sg contains remote IPs that aligns with remote IPs defined in the system sg rule keeping all other options of the rule same, then, the normal sg rule is called aligned. Consider a system sg rule with tuple (ip_protocoI: ICMP, direction: egress, port_range: any, remote_ips: 30.30.0.0/16, ethertype: ipv4, conn_track: reflexive):
  - A normal sg rule represented by tuple (ICMP, egress, any, 30.30.30.0/24, ipv4,reflexive). Since 30.30.30.0/24 aligns with 30.30.0.0/16, normal sg rule aligns with system sg rule.
  - A normal sg rule represented by tuple (ICMP, egress, any, 30.40.30.0/24, ipv4, reflexive). Since 30.40.30.0/24 doesn't aligns with 30.30.0.0/16, normal sg rule does not align with system sg rule.
- IP protocol: *IP protocol* has to be same in the system sg rule and normal sg rule for them to be aligned, given all other options are aligned. Consider a system sg rule with tuple (TCP, ingress, 22, 40.40.0.0/16, ipv4, reflexive).
  - A normal sg rule with tuple (TCP, ingress, 22, 40.40.40.0/16, ipv4,reflexive): aligns with the system sg rule.
  - A normal sg rule with tuple (UDP, ingress, 22, 40.40.40.0/16, ipv4, reflexive): does not align with the given system sg rule.

- Direction: *Direction* (egress/ingress) has to be same in the system sg rule and normal sg rule for them to be aligned, given all other options are aligned. Consider a system sg rule with tuple (TCP, ingress, 22, 40.40.0.0/16, ipv4,reflexive).
    - A normal sg rule with tuple (TCP, ingress, 22, 40.40.40.0/16, ipv4,reflexive): aligns with the system sg rule.
    - A normal sg rule with tuple (TCP, egress, 22, 40.40.40.0/16, ipv4,reflexive): does not align with given system sg rule.
- Port range: *Port range* defined in a normal sg rule should lie within the port range defined in the system sg rule, given all other options are aligned. Consider a system sg rule with tuple (TCP, ingress, 30-40, 12.12.0.0/16, ipv4,reflexive).
    - A normal sg rule with tuple (TCP, ingress, 34, 12.12.12.0/24, ipv4,reflexive) aligns with the system sg rule.
    - A normal sg rule with tuple(TCP, ingress, 22, 12.12.12.0/24, ipv4,reflexive) does not align with the system sg rule.
- Connection tracking: *Conn_track* option defined in normal sg rule should be same as conn_track option defined in system sg rule given all other options are aligned. Either both should use reflexive rules for a traffic or both should not. Consider a system sg rule with tuple (TCP, ingress, 30-40, 12.12.0.0/16,ipv4, reflexive).
    - A normal sg rule with tuple (TCP, ingress, 30-40, 12.12.12.0/24, ipv4,reflexive) aligns with the system sg rule.
    - A normal sg rule with tuple(TCP, ingress, 30-40, 12.12.12.0/24, ipv4,normal) does not aligns with the system sg rule.
- Ethertype: Rules in system sg and normal sg need to have same ethertype value to be aligned, given all other options are aligned. Examples for *Ethertype* are, ipv4, ipv6, arp, etc.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA 95134-1706
USA

Asia Pacific Headquarters
CiscoSystems(USA)Pte.Ltd.
Singapore

Europe Headquarters
CiscoSystemsInternationalBV
Amsterdam,TheNetherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.