Deploying Security Groups

In a cloud-enabled Data Center, security enforcement is no longer just network-centric (such as network addresses and VLAN attributes). Security has to be enforced specific to application requirements, who the tenant is, and which tier of the application is being protected.

Isolation is the basis for any network security strategy. Isolation has been accomplished in traditional environments through the manual configuration of ACLs or firewall rules on physical devices. In case of VTS enabled overlay networking, tenant isolation and network isolation are enforced by default. Overlay network isolation is achieved by the associated encapsulation mechanism on the VXLAN data plane. If an attack is started by an application workload inside a virtual network, the physical infrastructure of a cloud is completely protected by this isolation.

Segmentation adds security controls to smaller groups of workloads. In an overlay/virtual network, the ACL services are required to be provisioned near the application workloads. ACLs enable to place restrictions on a selective basis to restrict the communication between VMs. The ACLs can be realized on the hardware and software VTEPs.

Security group is a named collection of network access rules that are used to limit the types of traffic that have access to instances. Security rules define access rules within a security group. Security groups consists of security rules on the underlying hardware. They minimize the risk of data leak and protect the datacenter deployments through a proactive stance.

Security Policies are instantiated on VTS Policy plane based on OpenStack Security Groups APIs.

OpenStack Security Group is a named collection of network access rules that are used to limit the types of traffic that have access to instances. When launching an instance, administrator can assign one or more security groups to it. If not assigned, new instances are automatically assigned to the default security group. See OpenStack documentation for more details about OpenStack Security Groups.

The associated rules in each security group control the traffic to instances in the group. Any incoming traffic that is not matched by a rule is denied access by default. Rules can be added to or removed or modified for the default and any other security group. Rules are automatically enforced as soon as it is created or modified.

Admin can modify the rules in a security group to allow access to instances through different ports and protocols. For example, admin can modify rules to allow access to instances through SSH, to ping instances, or to allow UDP traffic; for example, for a DNS server running on an instance by specifying the following parameters for rules:

- **Source of traffic**—Enable traffic to instances from either IP addresses inside the cloud from other group members or from all IP addresses.
- **Protocol**—Choose TCP for SSH, ICMP for pings, or UDP.

- **Destination port on virtual machine**—Define a port range. To open a single port only, enter the same value twice. ICMP does not support ports; instead, you enter values to define the codes and types of ICMP traffic to be allowed.

When the OpenStack security is passed through the VTS ML2 plugin, VTS programs these policies as the ACLs in the underlying forwarding elements.

OpenStack security groups are realized using:

- ACLs on VTFs.
- OVS and Linux IP tables on compute nodes.
- ACLs on TORs for Bare metal and Virtual workloads.

This chapter has the following sections:

Security Group - Feature Scope

Following are the Port types supported in Security Group (SG):

Table 1: Port Types Supported

Port Types	Details
VTF Ports	• No support for remote security group. • All other OpenStack Security Group functionality can be fully realized on VTF Ports.
OVS Ports	Fully Supported
Baremetal Ports and SRIOV Ports	• No support for remote security group. • Reflexive ACLs are not supported. • Security Group Rules applied to traffic ingressing SRIOV port may not get enforced when the traffic is L2 traffic coming from a ToR different from destination ToR. • ACLs on Cisco Nexus 9000 series device cannot block Intra-compute SRIOV traffic. This is device platform issue. • No support for Cisco Nexus 7000 series device.

Table 2: Feature Supported - Detailed Table

Security Group Features	OVS	VPP	SR-IOV on Cisco Nexus 9000	BM on Cisco Nexus 9000
Default SG without Remote SG	Yes	Yes	Yes	Yes
Default SG with Remote SG	Yes	The default SG will be ignored.	The default SG will be ignored.	NA
Custom SG without Remote SG	Yes	Yes	Yes	Yes
Custom SG with Remote SG	Yes	The remote-sg rule will be ignored.	The remote-sg rule will be ignored.	NA
Reflexive Policies	Yes	Yes	No	No
Implicit DHCP allow	Yes	Yes	Yes	Yes
Routed Traffic	Egress/Ingress	Egress/Ingress	Egress/Ingress	Egress/Ingress
Bridged Traffic	Egress/Ingress	Egress/Ingress	• Egress Only for Inter-Compute. • None for Intra Compute (Traffic does not come in TOR).	Egress Only for Inter-Compute

Note

- OpenStack, by default, associates all VMs with their respective Tenant (or Project) 'default' sg. As OpenStack does not support SG for SRIOV Ports, 'default' sg associated with SRIOV ports gets ignored and all traffic will be allowed to passthrough. Same is the case with VTF Ports, as in prior releases VTS did not support SG for VTF ports. From Cisco VTS 2.6.0, the intent of these SGs—'default' or not, will start getting fully realized by Cisco VTS for SRIOV and VTF ports, provided these rules do not contain remote-sg rules. 'remote-sg' rules are not support for non OVS Ports—VTF, SRIOV and Baremetal. If a given SG happens to have a remote-sg rule then please refer to this section for details about expected behavior

  .
- See Cisco VTS syslog for error details.
- For Reflexive policies, reverse ACLs/Security rules need to be configured explicitly. There will not be any error logs.
- Cisco VTS does not allow you to create rules with remote SG.

Important Review the Security Groups feature specific information in the *Limitations and Restrictions* section of the *Cisco VTS Release Notes* before you create or attach security groups.

Support for Reflexive ACLs

This feature allows the ACLs configured on VTF Ports to be of reflexive nature. Reflexive ACL takes a packet flow, gets session information, and creates dynamic ACL entry in access-list in reverse direction. This entry gets automatically removed either after the session completes or times out. This dynamic insertion of rules rids the user of the need to explicitly program rules to allow reverse direction traffic.

Prior to this feature support, ingress rules corresponding to each egress rule to allow reverse traffic (and vice versa) had to be explicitly added.

With Reflexive ACLs feature, VTF behavior for Security Groups configured through OpenStack is brought to parity with OVS. For OVS, reflexive is always turned on. If you desire to turn this feature off for VTF ports then set the flag vtf-sg-reflexive-acl-enabled in global-settings to false. This setting applies only to the VTF ports and not OVS.

Creating Security Groups from Cisco VTS GUI

To create security groups in Cisco VTS:

Note These security groups can be attached only to Baremetal Ports from Cisco VTS.

Step 1 Go to **Tenants > Security Groups**. The Tenants / Security Groups window appears.

Step 2 Select **VTS** and **Tenant** as the source from the drop-down list.

Note If you have created a Security Group from OpenStack, it will show under a different source (OpenStack) and it will not show under VTS. You cannot add or edit or delete a Security Group from Cisco VTS after creating it under OpenStack.

Step 3 Click **Add (+)** icon to create a new Security Group. The Tenants / Security Groups / Create New Security Group window appears.

Step 4 Enter the Security Group name. The name requires at least one alphabet or number. Characters "and" are not allowed. The character limit is 255.

Step 5 Select the Tenant from the drop-down list, if you want to change the tenant.

Step 6 In the Description field, enter a description for the Security Group. The character limit is 255.

Step 7 Click **Create**. The Tenants / Security Groups / <new security group name> window appears in which you can see the Security Group details with two default rules that gets added to the new Security Group created.

You may remove the default rules if you wish to. To do this, check the check boxes and click **Delete (x)** icon.

Step 8 Click **Add (+)** icon to create a new rule for the Security Group.

Note Rules you create here cannot be edited. Rules can only be added or removed.

Specify the following Parameters:

- Direction
- IP Protocol
- Port/ Port Range
- IP Protocol Number
- Remote CIDR

Step 9 Click **Save**.

The rules created get saved to the VTS database.

Note You may click on the Security Group name link in the table to review the details.

Attaching Security Group to Baremetal Port

To attach a Security Group to a Baremetal Port:

Before you begin

Create a network before you do a port attach. See Creating a Network using Cisco VTS GUI for details.

Step 1 After you enter the details for attaching a port, click the **Next: Attach Security Groups** button to attach the Security Groups. The Attach Security Group window appears.

Step 2 Specify the Baremetal IPv4 / IPv6 address. You may use CIDR notation.

Step 3 Check the check box corresponding to the Security Groups you want to attach from the Available Security Group(s) table.

Note You can attach different Security Groups from different source by selecting it from **Source** pull down list.

The selected Security Group gets added to the Attached Security Group(s) table. Click the **Expand (>)** icon if you want to expand the Security Groups to view its rules.

Step 4 Click **Review** icon. The Review window appears for you to review the details.

Step 5 Click **Done** icon. The Overlay / Network / Fabric Host Networks / Edit Tenant Network window appears.

Click the link **View / Edit** icon in the Baremetal Ports table if you want to view or edit the Security Group attached.

Step 6 Click **Review** to review the details of the Security Group you have attached.

Step 7 Click **Done** .

Step 8 Click **Save**.

Detaching Security Group from Baremetal Port

To detach a Security Group from a Baremetal Port:

Step 1 Go to Overlay > Network. The Overlay / Network window appears.

Step 2 Click **Fabric Host Networks** tab and select the Network.

Step 3 Click **Edit** button.

Step 4 Click on the **Ports** tab.

You can see both Baremetals Ports and Virtual Machines Ports on the left hand side panel.

Step 5 Click the **View / Edit** link in the Baremetal Ports table. The Review window appears.

Step 6 Click **Edit** on the Attached Security Group(s) pane. The Attach Security Group window appears.

Step 7 Uncheck the check box corresponding to the Security Group you want to detach from the port. The Security Group moves from the Attached Security Group(s) pane to the Available Security Groups pane.

Step 8 Click **Review**. The Review window appears. Make sure that the Security Group you wanted to detach is not listed in the Attached Security Group(s) pane.

Step 9 Click **Done**.

Here you can see the number of the Security Groups that are currently attached, after you have detached the Security Group(s).

Step 10 Click **Save** to save the changes.

Attaching Security Groups to OVS, VTF, and SR-IOV Ports

Attaching Security Groups to OVS, VTF, and SR-IOV ports .

Procedure

	Command or Action	Purpose
Step 1	To attch Security Groups from OpenStack to OVS, VTF, and SR-IOV, see the OpenStack Horizon documentation for details.	**Note** Ensure that you do not select any remote-sg rules while you attach security groups to VTF and SR-IOV ports.

Detaching Security Groups from OVS, VTF, and SR-IOV Ports

Procedure

	Command or Action	Purpose
Step 1	Detach Security Groups from OVS, VTF, and SR-IOV from OpenStack. For more information, see the OpenStack Horizon documentation.	

Security Group - Examples

This section provides examples of Security Group use cases.

Creating Security Group to Restrict Access to a Given Application

Associating SRIOV port with Security Group