|  |
| --- |
| Intel |
| ISC Security Groups Architecture |
| Draft |

|  |
| --- |
| Arvind Nadendla  9/17/2014 |

Contents

[Introduction 3](#_Toc427934023)

[Basic Attributes of a security group 3](#_Toc427934024)

[Name 3](#_Toc427934025)

[Tenant 3](#_Toc427934026)

[Member Selection 3](#_Toc427934027)

[Selection type 3](#_Toc427934028)

[Overlap 4](#_Toc427934029)

[Between multiple Security Groups 4](#_Toc427934030)

# Introduction

Security group allow you to group a set of entities and apply services on that group. The security group itself can be a static list of entities you want to protect or it can be dynamic where you choose the criteria and we match it against the datacenter environment to determine the entities to protect.

# Basic Attributes of a security group

## Name

The Name of the security group. The name can be modified after the security group is created.

## Tenant

The tenant the security group belongs to. This cannot be modified after the security group is created. We use the tenant as one of the filtering mechanism. You can only add entities which belong to this tenant to this security group.

## Member Selection

The members which can be included in the security group is determined by the tenant (which is not modifiable after the security group is created), the region selection and the type selection.

The region and the type selection can be changed after the security group creation.

All the selections boil down to a set of ports for us to protect. Whatever the selection we dynamically figure out the ports which match that selection criteria and protect them

### Selection type

The selection type can be divided into 4 categories

#### All severs belonging to the tenant

All the servers belonging to this tenant will be included in the security group. All the ports of the Servers are included in this case.

If a new server is created/modified/deleted on behalf of the tenant, we will kick off a sync job which will add/update/remove the server (and ports) from this security group.

#### A static list of Servers

The static list of servers which the user chooses are included in the security group. All ports of the Servers that the user selects will be included in this case.

Any new ports added/deleted to any of the servers, or any of the servers deleted on the list will kick off a sync job which will include/remove the new port in the security group.

#### A static list of Networks

The static list of networks which the user chooses are included in the security group. All ports of the networks that the user selects will be included in this case.

Any new ports added/deleted to any of the Networks on the list will kick off a sync job which will include/remove the new port from the security group.

#### A static list of Servers and Networks – Hybrid model

The user can select a mix of Servers and Network entities. All the Servers and Networks which the user chooses are translated to a list of ports.

Any Servers on the list have a new port added/deleted, the sync job will be kicked off.

Any Networks on the list have new ports added/deleted, the sync job will be kicked off.

## Overlap

Overlap happens when an entity (and its ports) are part of 2 security groups. 

Currently we do not allow this and we are able to explain this to the user in some cases.

### Between multiple Security Groups

|  |  |  |  |
| --- | --- | --- | --- |
| Initial State of Security Group 1 | New Security Group Added | Can be Tested? | Notes |
| Protect All within tenant 1 | All with Tenant 1 | Yes | Adding New security group should not be allowed.  User should be shown a validation message while second group is being added. |
| VM 1 | VM 1 | Yes | Adding new security group is not allowed with the same VM as a member.  User shown a validation message while second group is being added. |
| VM 1 | Network 1 | Yes | For each duplicate port we should get a failed task ‘Validating port with mac 'fa:16:3e:cc:85:58' information’. |
| Network 1 | Network 1 | Yes | Validation error mentioning the network that its part of another security group |
| Network 1 | VM 1 | Yes | Should get an error VM1 part of another security group. Check that one of the ports of the entity is not already protected |