

Manual de configuración del Security Group Virtual Datacenter en OpenStack IPLAN

**Versión: Septiembre de 2018
IPLAN | iplan.com.ar | NSS S.A.
Reconquista 865 | C1003ABQ | Buenos Aires | Argentina**

Introducción

Virtual Datacenter OpenStack es una aplicación web que permite a sus usuarios crear Máquinas Virtuales (Virtual Machines, VM), definir redes, etc. En definitiva, **administrar el entorno Cloud** facilitado por Virtual Datacenter OpenStack IPLAN.

Con la contratación del servicio de Virtual Datacenter OpenStack IPLAN, se le facilita una URL de acceso a la consola web de administración de OpenStack, un usuario y una password para acceder a su *Proyecto*. Puede ver este *Proyecto*, como su empresa, como su entorno, o como el departamento de su empresa que lidera el proyecto en la nube de su compañía.

Este manual le ofrece la información mínima imprescindible para crear, realizar una configuración correcta y gestionar el featur de Security Group (Grupo de Seguridad).

Principales conceptos del Security Group

El servicio de Security Group es una función que permite reforzar la seguridad entre el equipamiento del Cliente que se encuentra en el Virtual Datacenter OpenStack IPLAN y el mundo exterior al cual se encuentra conectado por medio de Internet.

El componente básico es el Filtrado de puertos.

El Cliente podrá configurar tantos Security Group como crea necesario, cada uno con su grupo de reglas asociadas, y podrá especificar a qué VM (Virtual Machine/ Máquina Virtual) o grupo de VMs asociar los mismos.

La plataforma permite a su vez agregar más de un Security Group a una misma VM o grupo de VMs, aunque esta configuración no se recomienda, ya que si no es correctamente configurado un grupo de reglas de uno de los Security Group, puede entrar en conflicto con el grupo de reglas del otro Security Group.

Creación y configuración de un Security Group

Paso 1.- Una vez que se encuentre dentro de la web de configuración, (seguir los pasos descritos en el Manual de Usuario) se debe seleccionar dentro del menú desplegable de la izquierda, la opción de "Access & Security" y luego, la pestaña de "Security Group"

The screenshot shows the OpenStack web interface. On the left, a sidebar contains a menu with 'Access & Security' highlighted. The main content area is titled 'Access & Security' and has tabs for 'Security Groups', 'Key Pairs', and 'Floating IPs'. Below the tabs, there is a search filter and two buttons: '+ Create Security Group' and 'Delete Security Groups'. A table lists the security groups:

<input type="checkbox"/>	Name	Description	Actions
<input type="checkbox"/>	default	Default security group	Manage Rules
<input type="checkbox"/>	pf		Manage Rules
<input type="checkbox"/>	pruebaregla		Manage Rules

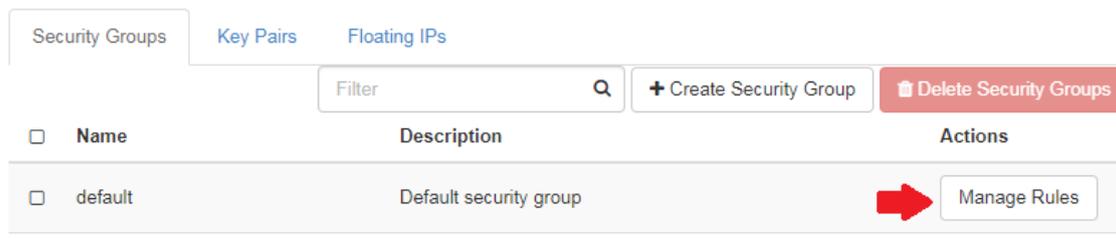
At the bottom of the table, it says 'Displaying 3 items'.

Todos los Clientes tienen configurado por defecto un Security Group denominado "Default".

Como se aclaró en un principio, se pueden generar más de un Security Group, tal como se ve en la imagen, en donde ya hay creados dos Security Group aparte del Default.

Por lo general, sólo se tiene un solo Security Group, por lo que se proceden a configurar todas las reglas en el Security Group Default.

Paso 2.- Para **configurar/modificar las reglas** de un Security Group, se deberá seleccionar la opción de “Manage Rules”.



Una vez seleccionada la opción aparecerá la siguiente pantalla, de la cual pasaremos a explicar cada una de las opciones:

The image shows the AWS IAM console interface for the 'Rules' tab of a Security Group. At the top right, there are two buttons: '+ Add Rule' and 'Delete Rules'. Below is a table with columns: 'Direction', 'Ether Type', 'IP Protocol', 'Port Range', 'Remote IP Prefix', 'Remote Security Group', and 'Actions'. Each row represents a rule, and each row has a 'Delete Rule' button in the 'Actions' column.

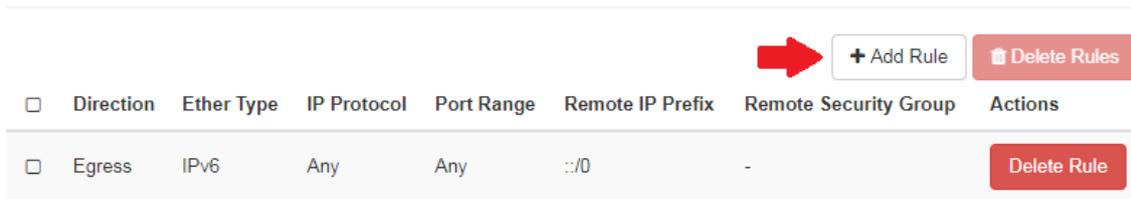
Direction	Ether Type	IP Protocol	Port Range	Remote IP Prefix	Remote Security Group	Actions
Egress	IPv6	Any	Any	::/0	-	Delete Rule
Ingress	IPv4	Any	Any	-	default	Delete Rule
Egress	IPv4	Any	Any	0.0.0.0/0	-	Delete Rule
Ingress	IPv6	Any	Any	-	default	Delete Rule
Ingress	IPv4	ICMP	Any	0.0.0.0/0	-	Delete Rule
Ingress	IPv4	TCP	22 (SSH)	0.0.0.0/0	-	Delete Rule
Ingress	IPv4	TCP	54321	0.0.0.0/0	-	Delete Rule

Disolavina 7 items

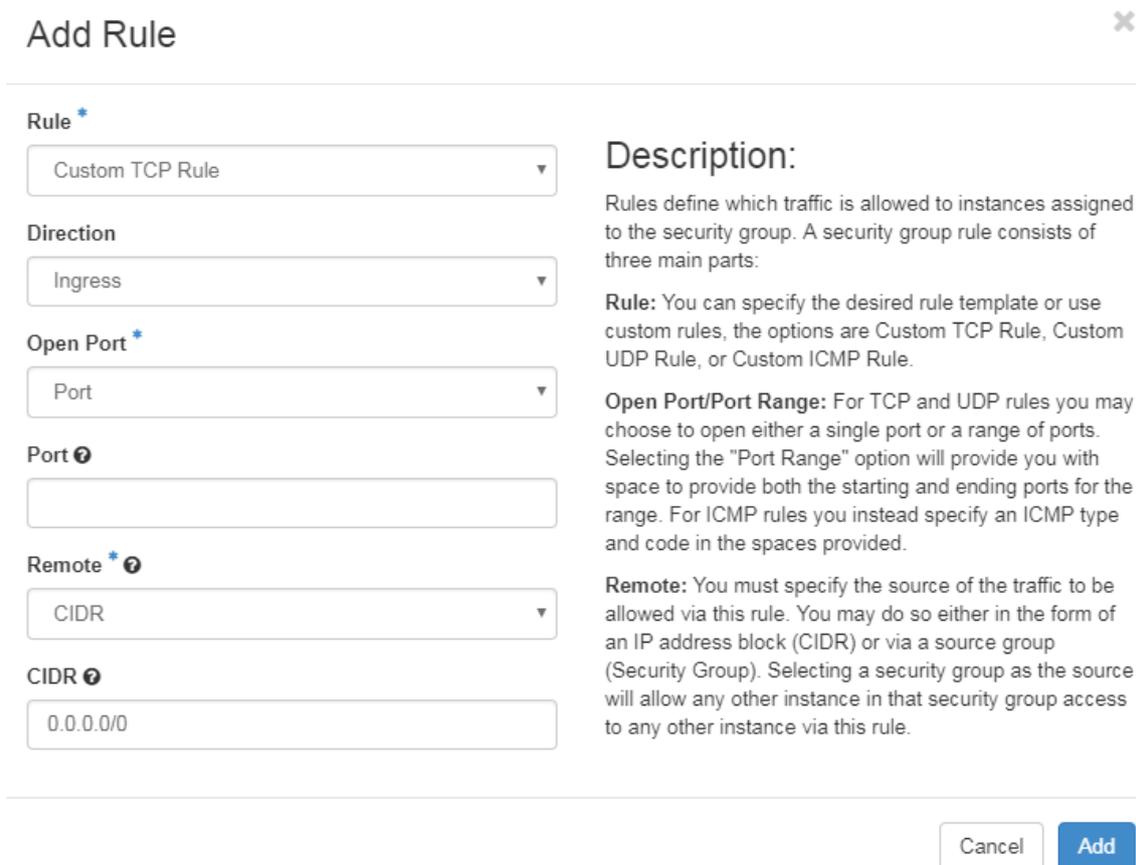
- **Direction:** Sentido en el que se aplicará la regla, es decir, si la regla será para el tráfico entrante o para el saliente.
- **Ether Type:** Protocolo a ser aplicada la regla, es decir: IPv4 o IPv6.
- **IP Protocol:** Tipo de tráfico a ser aplicada la regla, es decir: ICMP, TCP, UDP o any (todos).
- **Port Range:** Rango de puerto/puertos a ser aplicada la regla.
* Más allá que la plataforma indica el puerto 22 como SSH en las imágenes de IPLAN, este servicio ha sido cambiado por seguridad al puerto 54321.
- **Remote IP Prefix:** Prefijo de IPs en formato CIDR.
- **Remote Security Group:** Security Group en el que se encuentren las VMs permitidas o denegadas

Se deberá tener en cuenta que las reglas no podrán modificarse ya que la plataforma sólo permite agregar o borrar las mismas, por lo que, en caso de necesitar modificar una regla, se deberá eliminar y crear una nueva regla en reemplazo de la anterior.

Paso 3.- Para agregar una nueva regla se deberá seleccionar la opción de “+Add Rule”.



Una vez seleccionada la opción, se presentará la siguiente pantalla en donde se deberá configurar dicha regla:



Rule *

Custom TCP Rule

Direction

Ingress

Open Port *

Port

Port ?

Remote * ?

CIDR

CIDR ?

0.0.0.0/0

Description:

Rules define which traffic is allowed to instances assigned to the security group. A security group rule consists of three main parts:

Rule: You can specify the desired rule template or use custom rules, the options are Custom TCP Rule, Custom UDP Rule, or Custom ICMP Rule.

Open Port/Port Range: For TCP and UDP rules you may choose to open either a single port or a range of ports. Selecting the "Port Range" option will provide you with space to provide both the starting and ending ports for the range. For ICMP rules you instead specify an ICMP type and code in the spaces provided.

Remote: You must specify the source of the traffic to be allowed via this rule. You may do so either in the form of an IP address block (CIDR) or via a source group (Security Group). Selecting a security group as the source will allow any other instance in that security group access to any other instance via this rule.

Cancel Add

Como se ve en la imagen, sólo es posible definir un tipo de acceso remoto, ya sea por CIDR o por VMs pertenecientes a un determinado Security Group.

** Recordar que los puertos de acceso remoto en las imágenes de IPLAN han sido cambiados por seguridad al puerto 54321 (SSH/ RDP).*

Paso 4.- Para asociar un Security Group a una VM se puede hacer al momento de la creación de la VM (como se puede ver en el Manual de Usuario) o, en su defecto, a una VM ya creada como se explicará a continuación.

Para esto, debemos seleccionar la VM a ser asociada y luego, en el menú desplegable de acciones de la misma, seleccionar la opción "Edit Security Group".

Project / Compute / Instances / linux-redhat6-64

linux-redhat6-64

Create Snapshot

- Associate Floating IP
- Attach Interface
- Detach Interface
- Edit Instance
- Attach Volume
- Detach Volume
- Update Metadata
- Edit Security Groups
- Console
- ...

Overview	
Name	linux-redhat6-64
ID	22b59d52-4838-4c4e-97ce-200862bf3ed8
Status	Active
Availability Zone	nova
Created	Aug. 21, 2018, 4:23 p.m.
Time Since Created	4 weeks

Specs

Una vez seleccionada la opción, aparecerá la siguiente pantalla en donde podremos elegir qué Security Group asociar.

Edit Instance

Information * Security Groups

Add and remove security groups to this instance from the list of available security groups.

All Security Groups	Instance Security Groups
pft +	default -
pruebaregla +	

Cancel Save

* Recuerde que la plataforma permite a su vez agregar más de un Security Group a una misma VM o grupo de VMs aunque esta configuración no se recomienda, ya que si no es correctamente configurado un grupo de reglas de uno de los Security Group puede entrar en conflicto con el grupo de reglas del otro Security Group.