Manual de configuración del Security Group

IPLAN Cloud

Versión: Septiembre de 2020
IPLAN | iplan.com.ar | NSS S.A.
Reconquista 865 | C1003ABQ | Buenos Aires | Argentina

CONTENIDO

CONTENIDO **2**

1 - INTRODUCCIÓN **3**

1.1 - PRINCIPALES CONCEPTOS DEL SECURITY GROUP 3

2 - CREACIÓN Y CONFIGURACIÓN DE UN SECURITY GROUP **4**

1 - INTRODUCCIÓN

IPLAN Cloud es una Plataforma que consiste en un conjunto de recursos físicos y lógicos, los cuales basados en la tecnología de virtualización RedHat Openstack, proveen a los Clientes de una infraestructura tecnológica que les permite operar sus aplicaciones de negocio de misión crítica. En definitiva, **administrar el entorno Cloud** facilitado por IPLAN Cloud.

Con la contratación del servicio de IPLAN Cloud, 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 feature de Security Group (Grupo de Seguridad).

1.1 - 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 IPLAN Cloud y el mundo exterior al cual se encuentra conectado por medio de Internet.

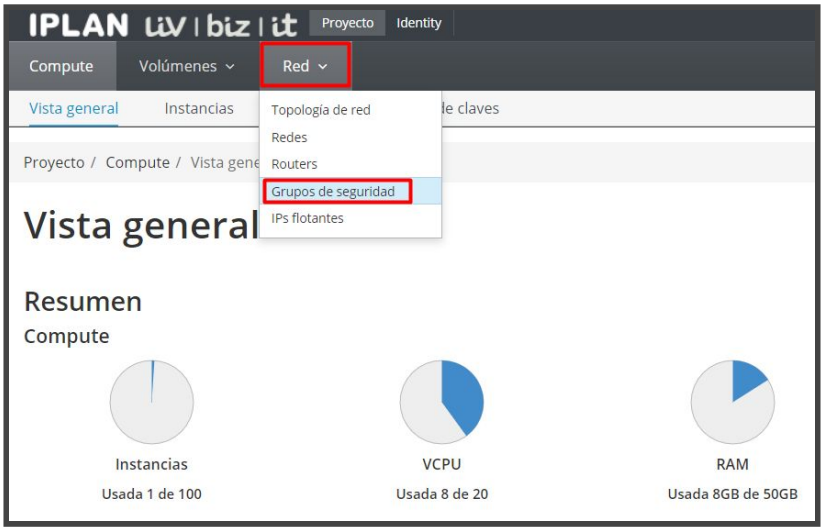
El funcionamiento básico consiste en el Filtrado de puertos.

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 el grupo de reglas de un Security Group, puede entrar en conflicto con las reglas de otro Security Group.

2 - CREACIÓN Y CONFIGURACIÓN DE UN SECURITY GROUP

Paso 1.- Una vez que se encuentre dentro de Plataforma IPLAN Cloud, (seguir los pasos descritos en el “Manual de Usuario IPLAN Cloud” en la sección de Documentación) se debe seleccionar dentro del menú RED la opción "Grupos de seguridad”.

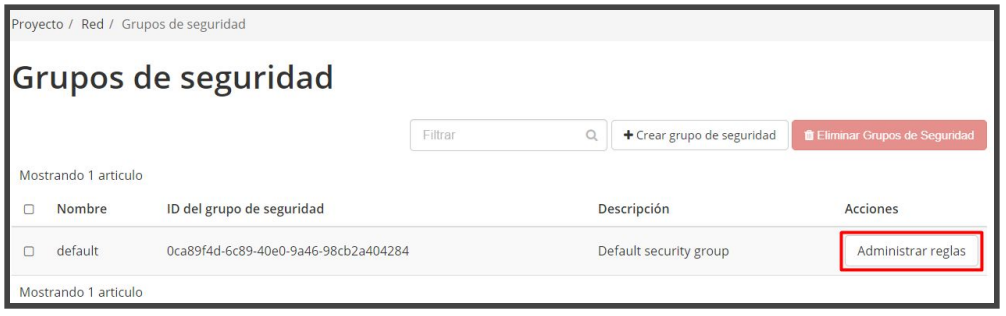


Todos los Clientes tienen configurado por defecto un Security Group denominado “Default”.

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.

Recomendamos crear un Security Group por instancia desplegada a fin de tener un mejor control del tráfico permitido hacía cada instancia.

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



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

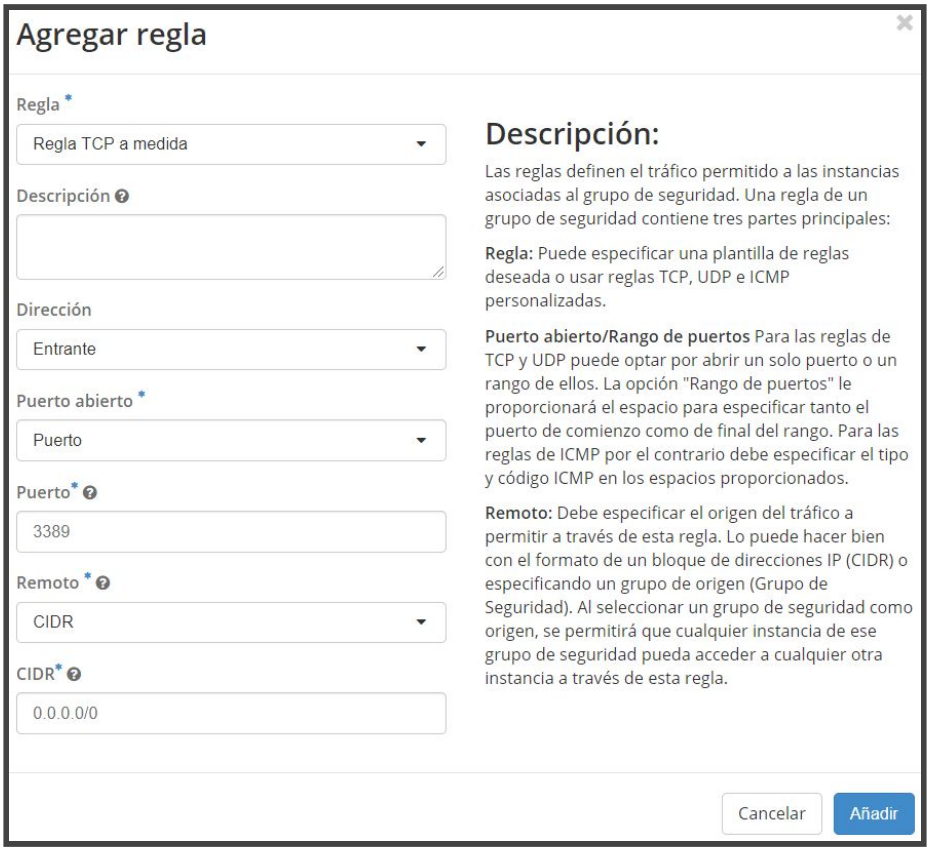
- **Dirección:** Sentido en el que se aplicará la regla, es decir, si la regla será para el tráfico entrante o para el saliente.
- **Tipo Ethernet:** Protocolo a ser aplicada la regla, es decir: IPv4 o IPv6.
- **Protocolo IP:** Tipo de tráfico a ser aplicada la regla, es decir: ICMP, TCP, UDP o any (todos).
- **Rango de Puertos:** Rango de puerto/puertos a ser aplicada la regla.
- **Prefijo de IP Remoto:** Prefijo de IPs en formato CIDR.
- **Grupo de Seguridad Remoto:** Security Group en el que se encuentren las VMs permitidas

Se deberá tener en cuenta que:

1. El tráfico es denegado por defecto y con cada regla que creemos, iremos permitiendo el tráfico deseado.
2. 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 en reemplazo de la anterior.

Paso 3.- Para **agregar una nueva regla** se deberá seleccionar la opción de “Agregar regla”.

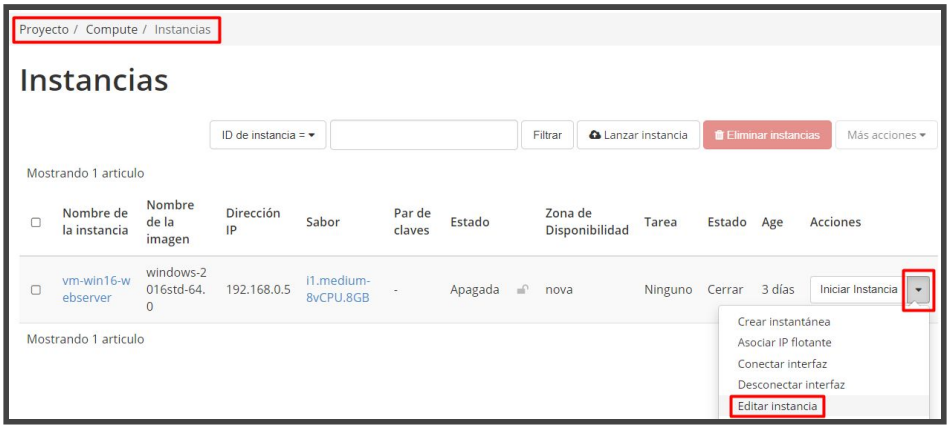
Una vez seleccionada la opción, se presentará la siguiente pantalla en donde se deberá configurar dicha regla:



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

Paso 4.- La asociación de **un Security Group a una VM (virtual machine)** se puede hacer al momento de la creación de la VM (como se puede ver en el Manual de Usuario IPLAN Cloud), o, en su defecto, a una VM ya creada como se explicará a continuación.

Para esto, debemos seleccionar la Instancia deseada y luego, en el menú desplegable de acciones de la misma, seleccionar la opción "Editar Instancia".



Una vez seleccionada la opción, aparecerá la siguiente pantalla en donde deberemos seleccionar “Grupos de Seguridad”.

**** 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.***
Recomendamos crear un Security Group por Máquina Virtual.