

Manual de configuración del Security Group

IPLAN Cloud

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.

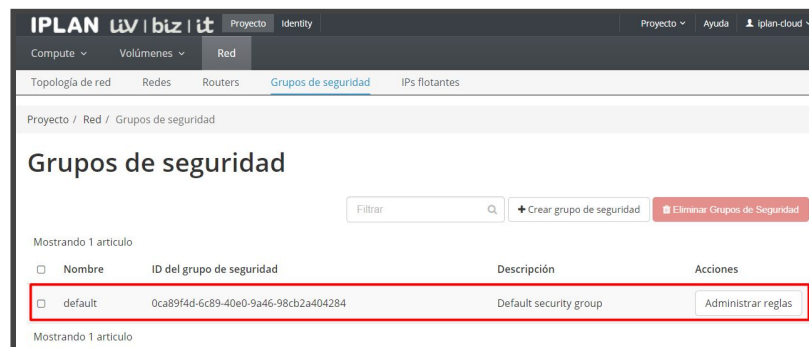
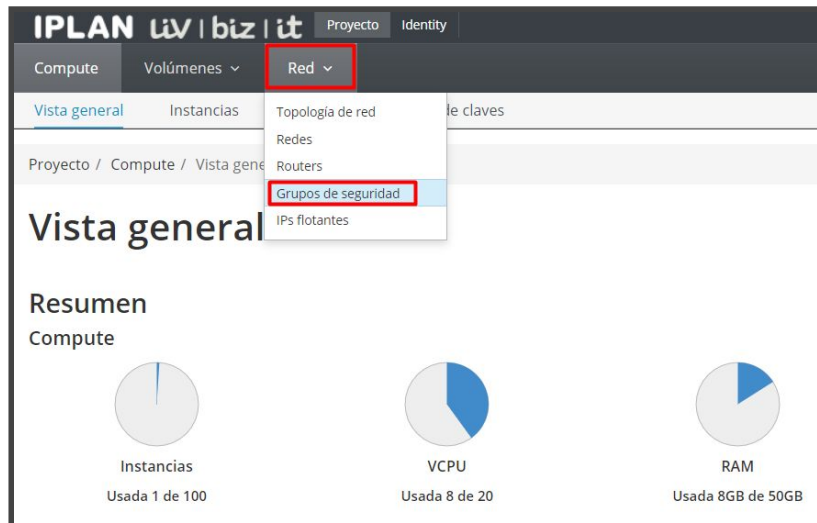
El funcionamiento básico consiste en el Filtrado de puertos.

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".

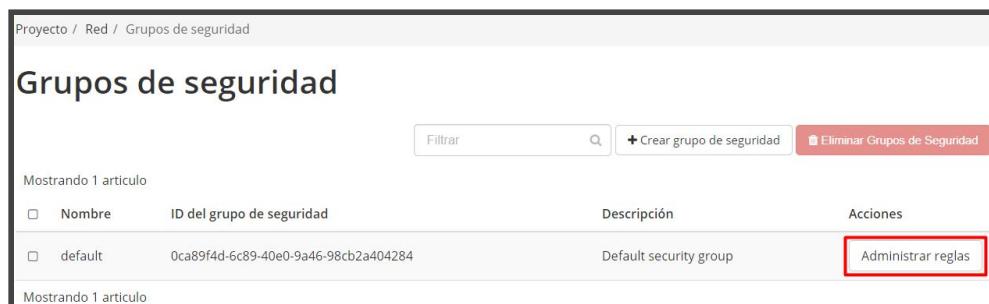


Todos los Clientes tienen configurado por defecto un Security Group denominado “Default”.

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 hacia 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 creamos, 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:

Agregar regla

Regla *
 Regla TCP a medida

Descripción ?
 [Campo de texto]

Dirección
 Entrante

Puerto abierto *
 Puerto

Puerto * ?
 3389

Remoto * ?
 CIDR

CIDR * ?
 0.0.0.0/0

Descripción:
 Las reglas definen el tráfico permitido a las instancias asociadas al grupo de seguridad. Una regla de un grupo de seguridad contiene tres partes principales:
Regla: Puede especificar una plantilla de reglas deseada o usar reglas TCP, UDP e ICMP personalizadas.
Puerto abierto/Rango de puertos Para las reglas de TCP y UDP puede optar por abrir un solo puerto o un rango de ellos. La opción "Rango de puertos" le proporcionará el espacio para especificar tanto el puerto de comienzo como de final del rango. Para las reglas de ICMP por el contrario debe especificar el tipo y código ICMP en los espacios proporcionados.
Remoto: Debe especificar el origen del tráfico a permitir a través de esta regla. Lo puede hacer bien con el formato de un bloque de direcciones IP (CIDR) o especificando un grupo de origen (Grupo de Seguridad). Al seleccionar un grupo de seguridad como origen, se permitirá que cualquier instancia de ese grupo de seguridad pueda acceder a cualquier otra instancia a través de esta regla.

Cancelar Añadir

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".

Proyecto / Compute / Instancias

Instancias

ID de instancia = [] Filtrar [] Lanzar instancia [] Eliminar instancias [] Más acciones []

Mostrando 1 artículo

Nombre de la instancia	Nombre de la imagen	Dirección IP	Sabor	Par de claves	Estado	Zona de Disponibilidad	Tarea	Estado	Age	Acciones
vm-win16-w ebserver	windows-2 016std-64- 0	192.168.0.5	i1.medium- 8vCPU,8GB	-	Apagada	nova	Ninguno	Cerrar	3 días	Iniciar instancia []

Mostrando 1 artículo

- Crear instantánea
- Asociar IP flotante
- Conectar interfaz
- Desconectar interfaz
- Editar instancia

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

Editar instancia

Información * Grupos de seguridad

Añade y elimine grupos de seguridad a esta instancia de la lista de grupos de seguridad disponibles.

Warning: If you change security groups here, the change will be applied to all interfaces of the instance. If you have multiple interfaces on this instance and apply different security groups per port, use "Edit Port Security Groups" action instead.

Todos los grupos de seguridad

win16-webserver

Grupos de seguridad de la instancia

default

Editar instancia

Información * Grupos de seguridad

Añade y elimine grupos de seguridad a esta instancia de la lista de grupos de seguridad disponibles.

Warning: If you change security groups here, the change will be applied to all interfaces of the instance. If you have multiple interfaces on this instance and apply different security groups per port, use "Edit Port Security Groups" action instead.

Todos los grupos de seguridad

default

Grupos de seguridad de la instancia

win16-webserver

*** 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.**