Manual de configuración del Firewall

Virtual Datacenter en OpenStack IPLAN

Versión: Octubre de 2018
IPLAN | iplan.com.ar | NSS S.A.

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 feature de Firewall (Cortafuegos).

Principales conceptos del Firewall

Firewall VDC en OpenStack IPLAN es una herramienta que permite reforzar la seguridad entre el equipamiento del Cliente que se encuentra en Ringo Datacenter de IPLAN, y el mundo exterior al cual se encuentra conectado por medio de Internet.

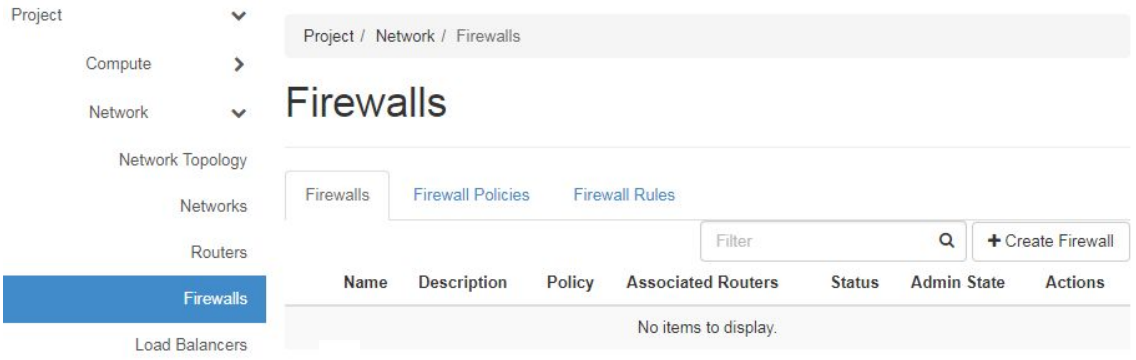
El servicio se habilita como funcionalidad dentro de la misma plataforma web de administración del VDC en OpenStack IPLAN al cual está asociado, por lo que la configuración del servicio está centralizada en la misma plataforma.

Este Firewall se aplica a nivel de router (direccionador) por lo tanto, las reglas impactan para todas las Instancias de Máquinas Virtuales que se encuentren detrás del mismo, aunque también pueden configurarse reglas específicas por IP.

- Posibilidad de sumar al router básico de OpenStack la funcionalidad de firewall.
- Creación de políticas de acceso para el tráfico entrante a la VM del cliente que se encuentre detrás del router.
- Creación de políticas de acceso para el tráfico saliente de la VM del cliente que se encuentre detrás del router.
- Auto gestión de las políticas descriptas en los puntos anteriores sin intervención de Iplan.
- Posibilidad de asociar dichas políticas a cualquier router generado dentro del proyecto del cliente.

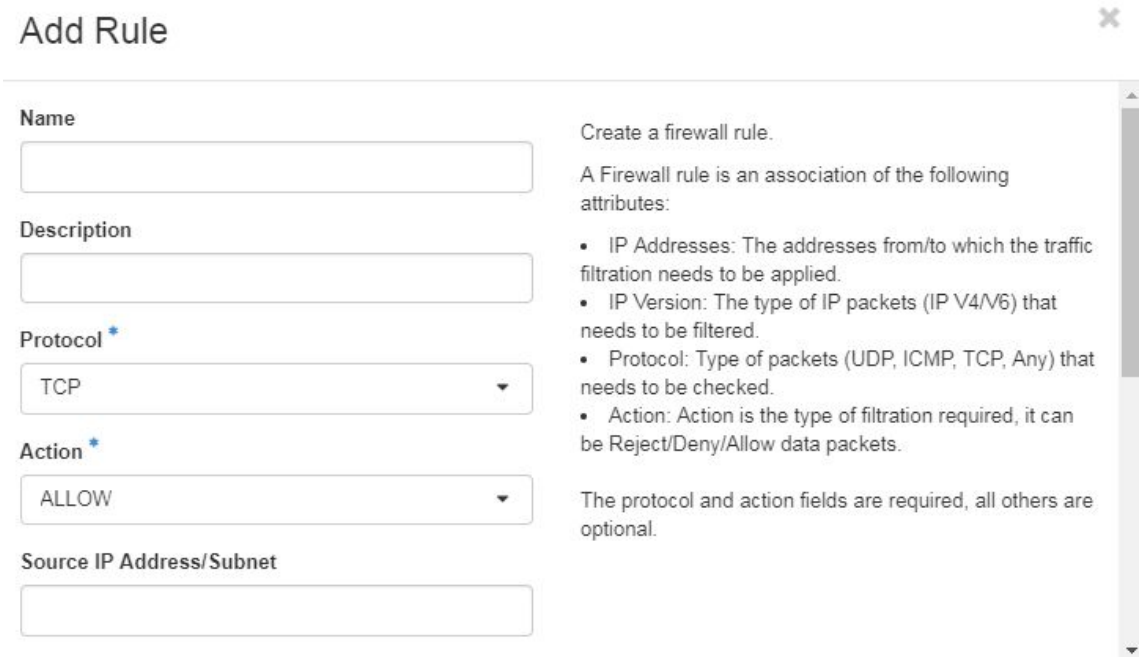
Creación y configuración de un Firewall

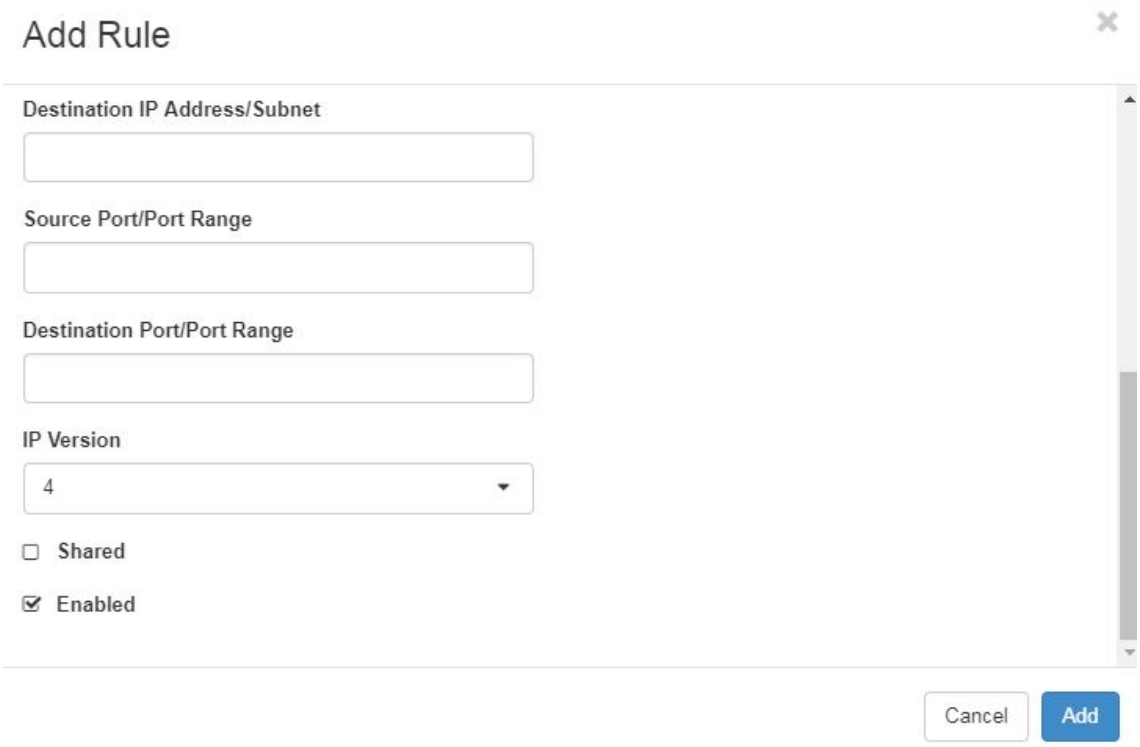
Paso 1.- Una vez que se encuentre dentro de la web de configuración, (seguir los pasos descriptos en el Manual de Usuario) se debe seleccionar dentro del menú desplegable de la izquierda, la opción de "Network" y luego, la opción de "Firewalls"



Encontraremos 3 solapas para crear los componentes necesarios para segurizar nuestras instancias.
Es importante destacar que el orden a seguir de las solapas es de DERECHA A IZQUIERDA, ya que de no seguir este orden no podremos implementar correctamente el servicio.

Paso 2.- Sabiendo esto, comenzamos por la solapa de Firewall Rules. Aquí iremos agregando de a una, reglas de firewall donde especificaremos que tráfico ingresante dejaremos pasar hacia nuestras instancias.





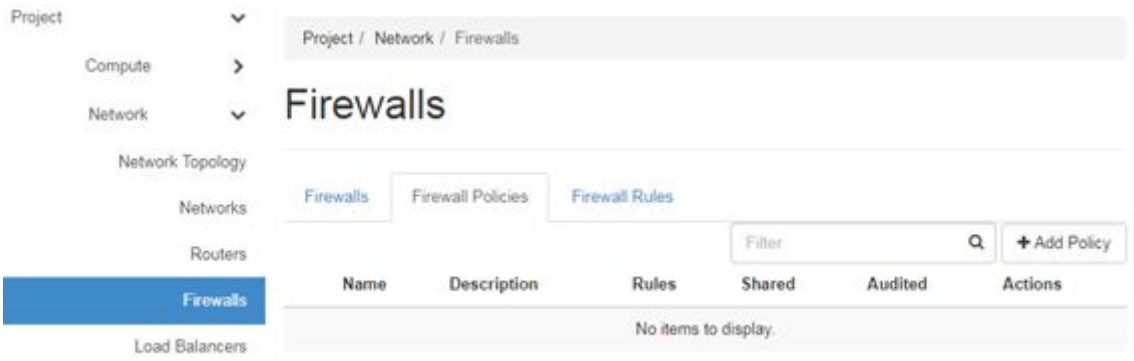
Los valores marcados con un asterisco, son de carácter obligatorio, mientras que el resto son opcionales, la no especificación de los mismos implica el valor más abarcativo y genérico posible.

- **Name**: Un nombre corto referenciando la regla
- **Description**: Una descripción de que tráfico permite
- **Protocol**: Protocolo de transporte, valores posibles: TCP/UDP/ICMP/CUALQUIERA(ANY)
- **Action**: Acción a realizar con el tráfico que cumpla estas condiciones (PERMITIR/DENEGAR/RECHAZAR, la diferencia entre DENY Y REJECT es que este último rechaza implícitamente mandando un mensaje al origen, deny simplemente descarta el tráfico localmente)
- **Source IP Address/Subnet**: IP o Subred de origen. Soporta valores de direcciones ip o redes en formato CIDR (X.X.X.X/X)
- **Destination IP Address/Subnet**: Idem al anterior, pero a que direcciones de destino impacta. En reglas entrantes, serían las ips de nuestras instancias o flotantes.
- **Source Port/Port Range**: Puertos o rangos de puerto de origen
- **Destination Port/Port Range**: Puertos o rangos de puerto de destino. Si es rango, se separa con ":".
- **IP Version**: Tipo de tráfico, IPv4 o IPv6
- **Shared**: Esta regla será visible por el resto de los tenants. No activar.
- **Enabled**: Este tilde habilita la regla, por defecto está activado.

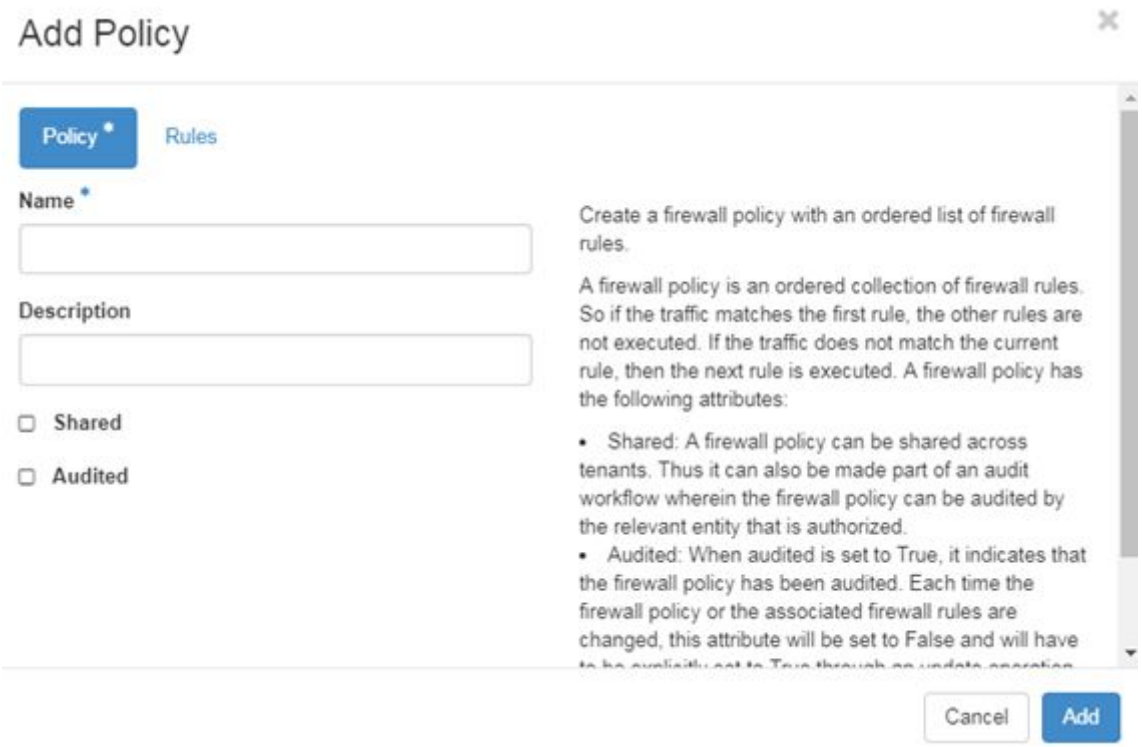
Paso 3.- Creación de una "Firewall Policy"

Una vez que tengamos todas las reglas que necesitamos para permitir el tráfico que deseamos, vamos a la solapa central, y armaremos una policy.

Una firewall policy es un conjunto de reglas de firewall. Luego con esta política ya paquetizada crearemos un firewall virtual para proteger nuestra infraestructura:



Seleccionamos la opción de "Add Policy" para crear una nueva política



- **Shared**: Permite que otros tenants puedan ver y reusar esa política prearmada. No lo utilizaremos.
- **Audited**: Indica que la política está auditada. Cada vez que se modifique automáticamente se destilda y debe ser remarcado en caso de que se requiera auditar cambios en las reglas.

Luego seleccionaremos la solapa de “Rules”

En el botón **Rules**, podremos elegir todas las reglas que hayamos creado, y arrastrarlas al cuadro superior.
En este cuadro definiremos el orden en que serán controladas, como se indicó previamente, es muy importante cargarlas en el orden adecuado a fin de no descartar tráfico válido.

En el ejemplo solo hay creada una regla, pero si hubiera más de una podríamos seleccionar el orden de las mismas.

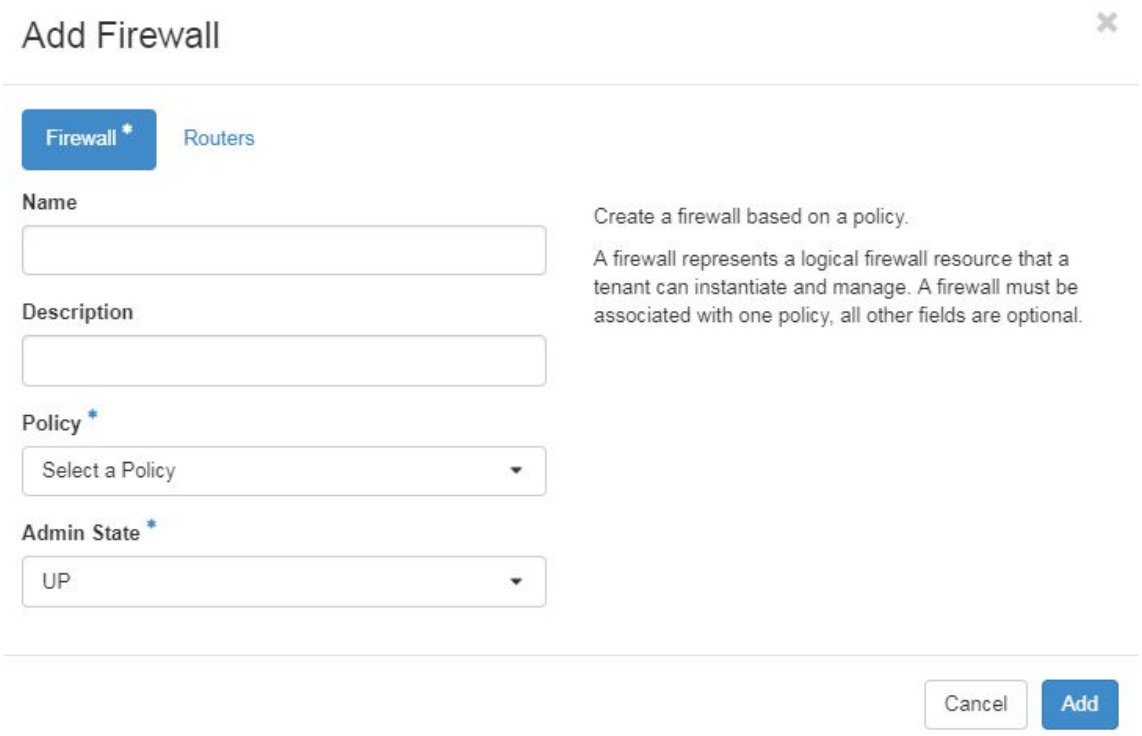
***En las políticas de firewall, es muy importante que respetemos el orden**

- Cada conexión nueva que intente impactar nuestra infraestructura será cotejada, renglón por renglón desde la primera hacia abajo, y si el tráfico coincide con alguna de las reglas, pasa o se descarta en ese renglón y lo que venga debajo no importa.

- Es decir, si permito en el 5to renglón de una policy tráfico http, pero en el renglón 3 tengo una regla que descarta ese tráfico por otro motivo, nunca se concretará la conexión porque nunca se controlará ese tráfico con la regla que nos importa.

Paso 4.- Creación del “Firewall”

Por último, crearemos el firewall en la solapa de la izquierda, y le asociaremos la política que creamos anteriormente, además de asociarlo a el/los router/s de nuestro vdc.



- **Name**: Nombre del Firewall
- **Description**: Deccripción del Firewall
- **Policy**: Selección de la política a utilizar (creada en el paso anterior)
- **Admin State**: Si el mismo estará activo o no

Luego en la solapa de Routers se seleccioná los routers a asociar dicho Firewall