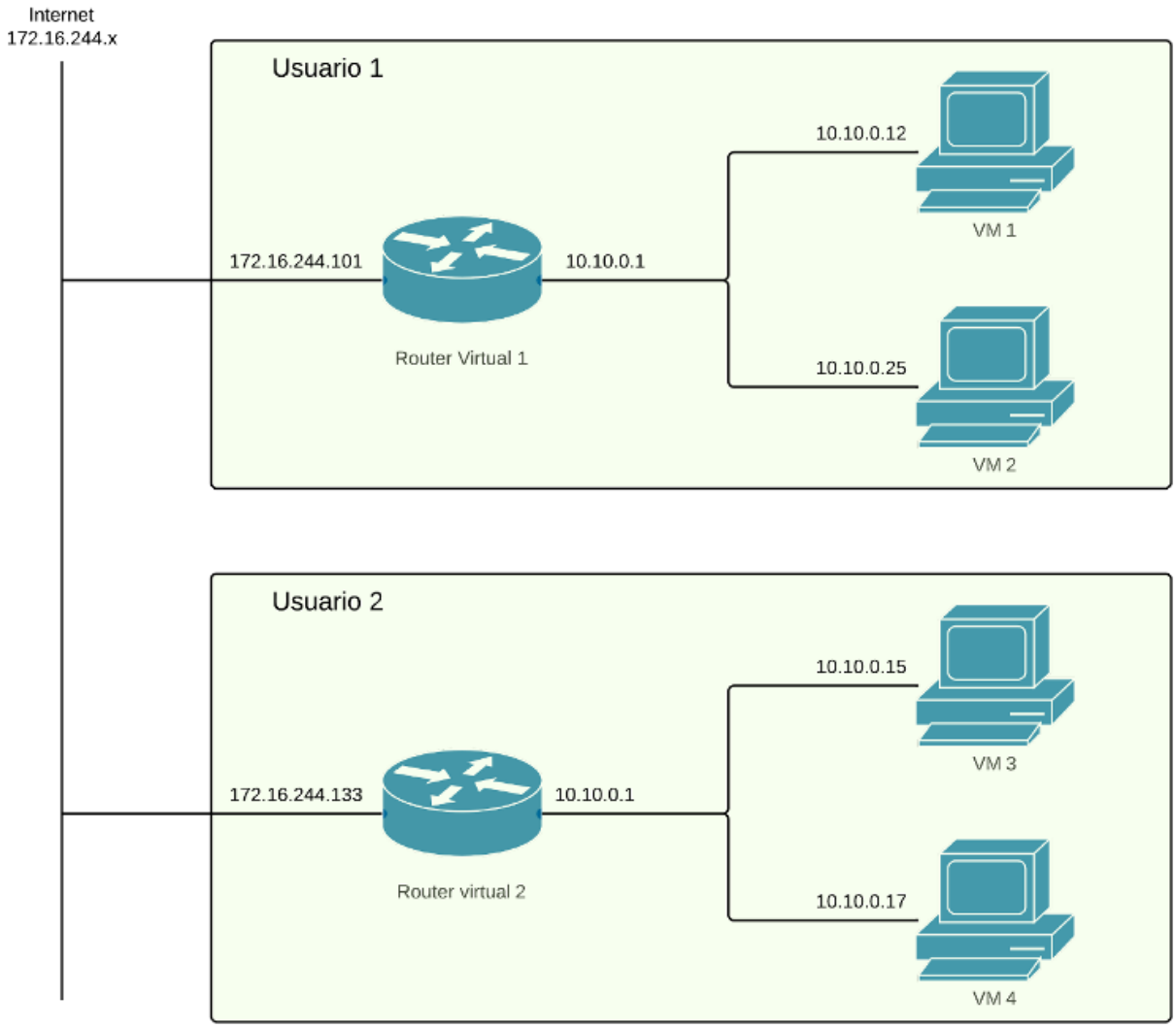
>>Página principal del Cloud

Las redes en Cloudstack

Introducción

Crear una red dentro de Cloudstack provoca la creación de una vlan que aisle la red de este usuario de los demás y la puesta en funcionamiento de un router virtual que realiza la función de puerta de enlace de esta red con el exterior y proporciona los servicios de cortafuegos y nat, todo ello de forma completamente transparente para el usuario.
En el caso del CITIUS, el Cloudstack está configurado de forma que la dirección IP de la interfaz externa del router es accesible desde cualquier otra dirección perteneciente al CITIUS, y está en el rango 172.16.244.0/24. Está es la ip con la que el usuario podrá acceder a cualquiera de las máquinas que haya creado dentro de esta red mediante nat. Si se crean redes adicionales, cada una tendrá una ip diferente.
Todas las máquinas virtuales que se crean reciben su configuración de red de forma dinámica mediante DHCP sin la intervención del usuario.
El router virtual está configurado por defecto para bloquear todas las comunicaciones entre la red externa y la del usuario. Si el usuario quiere abrir puertos en el cortafuegos y/o configurar el nat para que las máquinas puedan comunicarse con el exterior hay que hacerlo desde la interfaz web de la forma que se explica más adelante.

Un ejemplo de cómo son dos redes de dos usuarios distintos en Cloudstack:



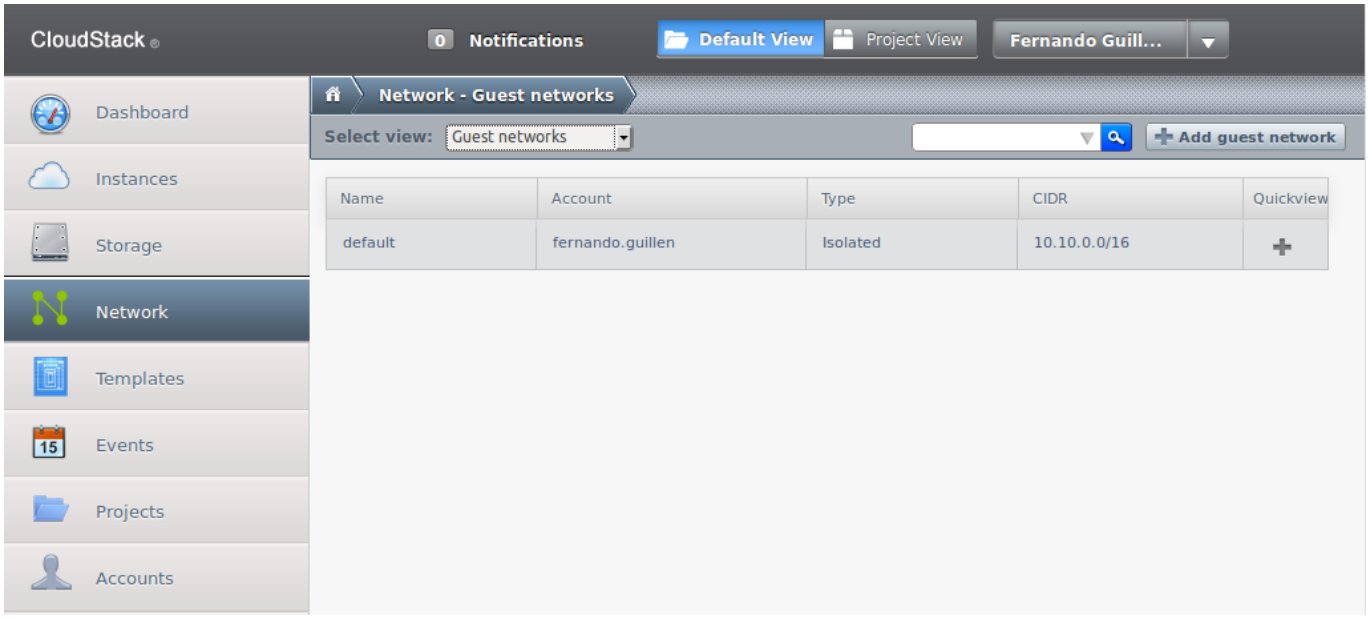
Esquema de dos redes de usuario en CS

Como se puede observar en el esquema, el usuario 1 ha creado una red a la que ha conectado dos máquinas virtuales, VM 1 y 2. Estas dos máquinas se pueden comunicar entre sí porque están en la misma red pero aunque esta red usa el mismo rango que la del usuario 2 están en vlans diferentes por lo que en la práctica están completamente aisladas entre sí. pueden comunicarse con el exterior a través de la puerta de enlace que les ofrece el router virtual 1. Este router tiene dos interfaces, una en la red del usuario (10.10.0.1) y otra en la red del CITIUS (172.16.244.101). El usuario tendría que conectarse a la ip 172.16.244.101 para acceder a cualquier servicio de sus máquinas virtuales. Lo que distingue a qué servicio de qué máquina te conectas al acceder a esa ip es lo que se haya configurado en el nat del router. Por ejemplo, suponiendo que tanto VM1 como VM2 tengan servidores web accesibles en el puerto 80 y que el nat del router 1 tuviera las siguientes reglas:
Puerto 180 → puerto 80 de VM1
Puerto 280 → puerto 80 de VM2
entonces para acceder a ambas webs habría que usar estas direcciones respectivamente:
172.16.244.101:180 y 172.16.244.101:280

Configuración

La configuración de las redes en Cloudstack se realiza seleccionando “Network” en la columna

izquierda:



Network

Aquí aparecerá una lista de las redes ya creadas; en el caso de la imagen anterior solo hay una de nombre “default”.

Aunque un usuario tenga más de una red, estas se encuentran aisladas entre sí como si fueran de dos usuarios distintos.

Crear nuevas redes

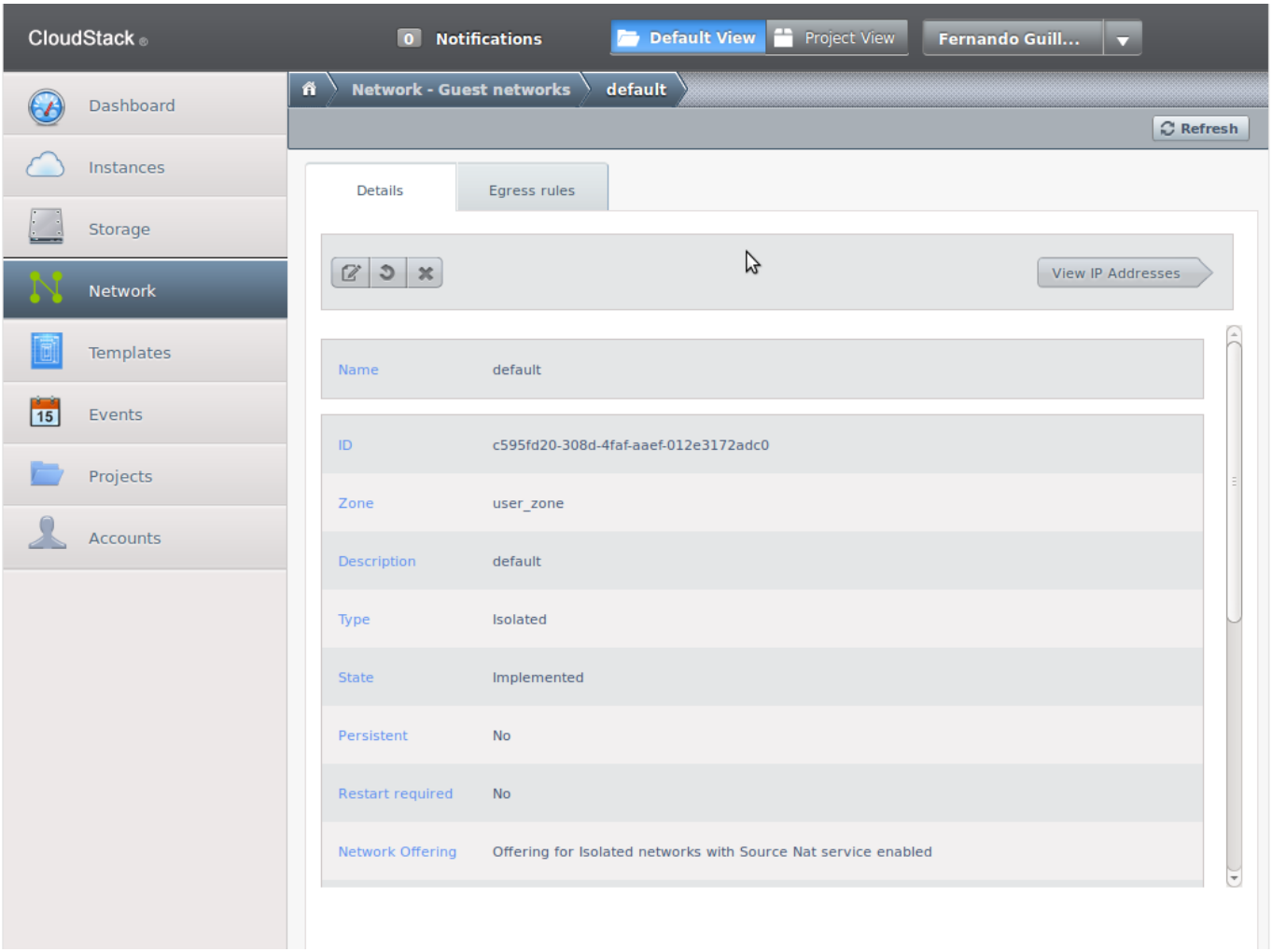
Hay dos maneras de crear nuevas redes, una es automática durante la creación de una VM (la recomendada) y otra es manual seleccionando el botón “Add guest network” en la parte superior derecha.
Esto abrirá una nueva ventana para introducir los datos necesarios:

Crear una nueva red

- Name: el nombre de la red, Cloudstack no lo usa, solo es para la organización del usuario.
- Display text: Una descripción, de nuevo solo de cara al usuario.
- Zone: solo hay una, dejar como está.
- Network offering: solo hay un tipo de red, dejar como está.
- Guest gateway (opcional): por defecto es la 10.10.0.1 pero puede configurarse otra. Es la ip que tendrá el router virtual en su interfaz interna.
- Guest netmask (opcional): máscara de red que se usará en la red.
- Network domain (opcional): puede definirse un nombre de dominio para esta red.

Configurar una red

Seleccionamos una red y aparecerá la siguiente pantalla:

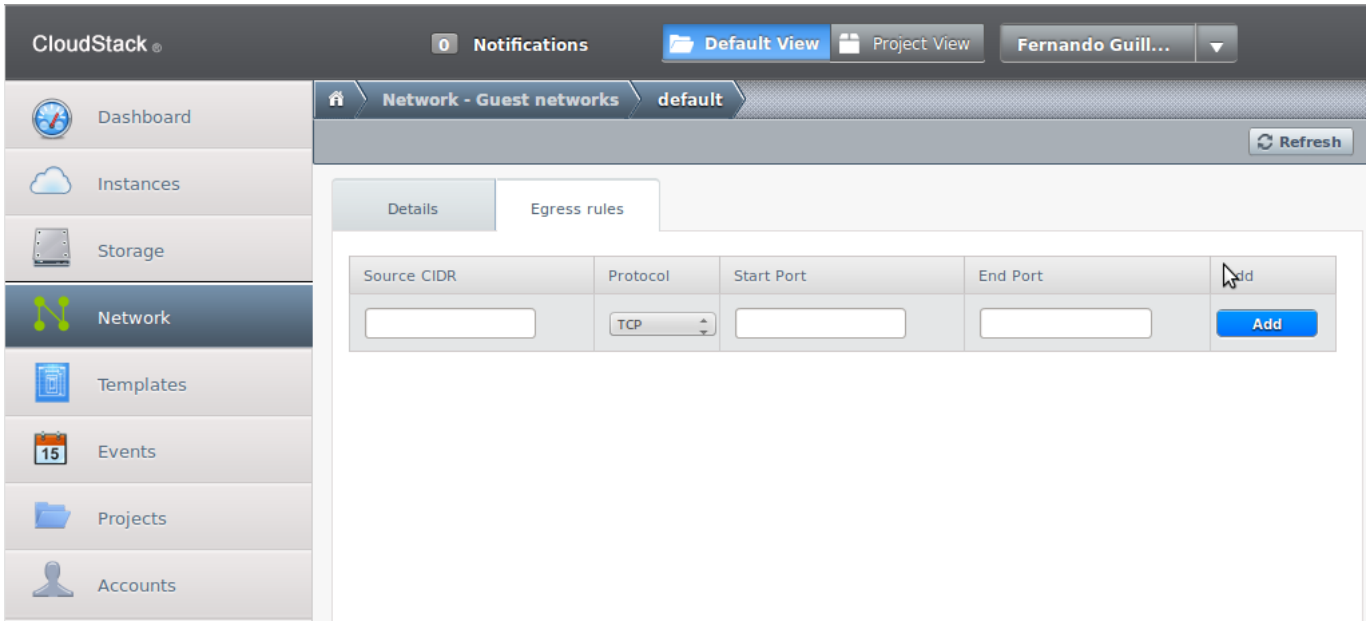


Red “default”

Aquí podemos configurar el tráfico en los dos sentidos: desde la VM hacia el exterior y desde el exterior hacia la VM.

Configurar el tráfico desde la VM hacia el exterior

Por defecto el cortafuegos de la red impide cualquier tipo de comunicación entre la VM y el exterior. Para cambiar eso hay que acceder a la pestaña “Egress rules”:



Ahi aparecerá una lista con las reglas existentes y una línea en blanco para añadir nuevas. Hay una negación implicita, lo que quiere decir que cualquier tráfico que no sea explicitamente permitido por una regla es denegado. La regla más sencilla que se puede añadir que permita todo el tráfico desde la VM hacia el exterior es la siguiente:

Source CIDR	0.0.0.0/0
Protocol	All

La CIDR 0.0.0.0/0 indica todos los orígenes y el protocolo All indica todos los puertos.

Si se quieren poner reglas menos permisivas se pone en el campo “Source CIDR” la ip de la red o del host desde el que se quiere permitir el tráfico y en “Protocol”,“Start Port” y “Destination Port” el protocolo y los puertos que se permiten.

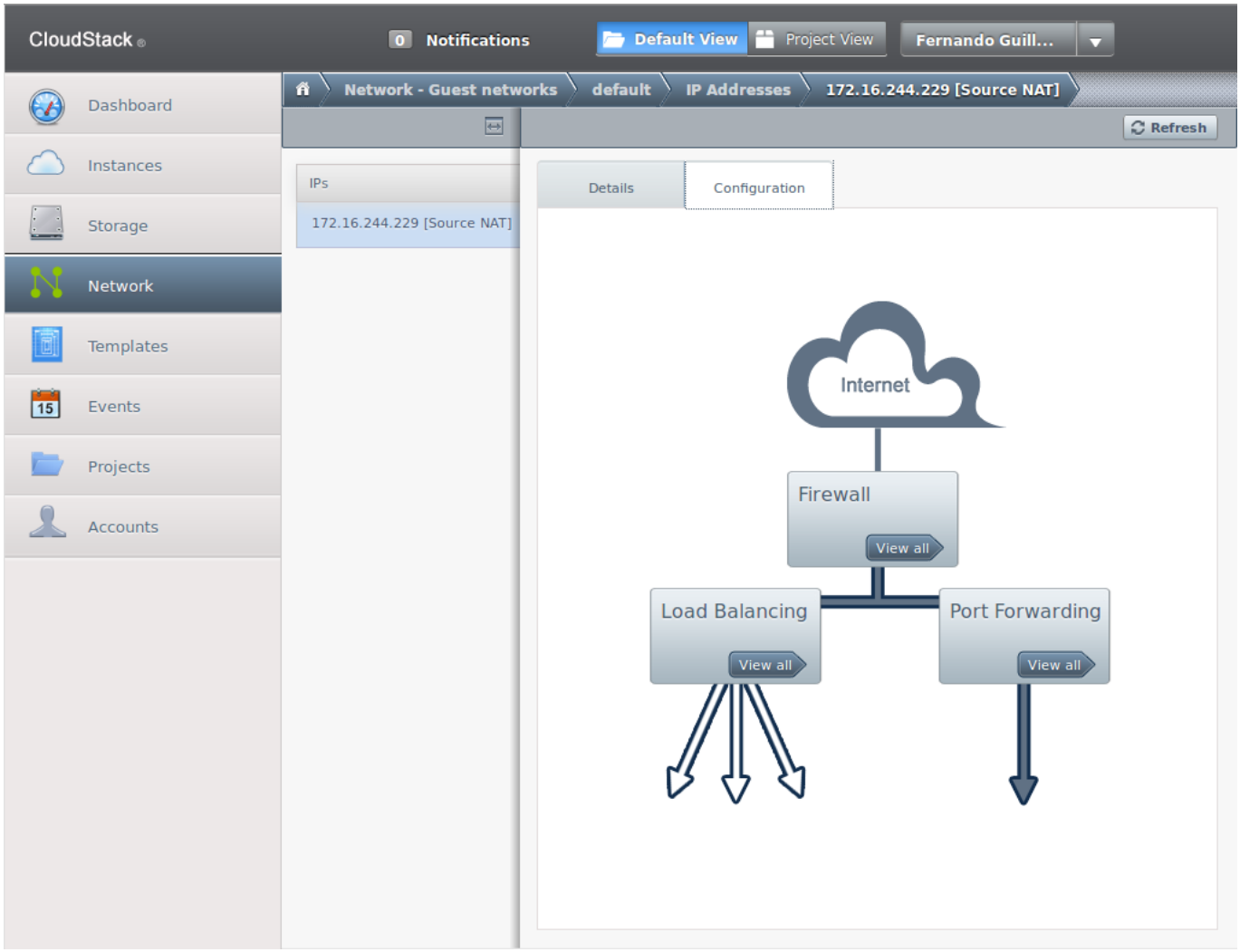
Una vez una regla está creada el botón de “Add” se sustituye por una cruz para poder borrarla.

Configurar el tráfico desde el exterior hacia la VM

Al crear una red se inician dos servicios: cortafuegos y source nat. El cortafuegos por defecto no permite ningún tráfico entrante en la red, por lo que habrá que configurar reglas explicitas para cada puerto que queramos abierto en la red. El source nat hay que configurarlo para que cuando haya tráfico entrante en la red, este sea redirigido a la máquina virtual que nosotros queramos.
Para llegar hasta la pantalla de configuración hay que seleccionar el nombre de la red de entre la lista, pulsar el botón “View ip addresses” y ahí seleccionar la dirección ip de la red.

Camino hasta la configuración del cortafuegos y el nat.

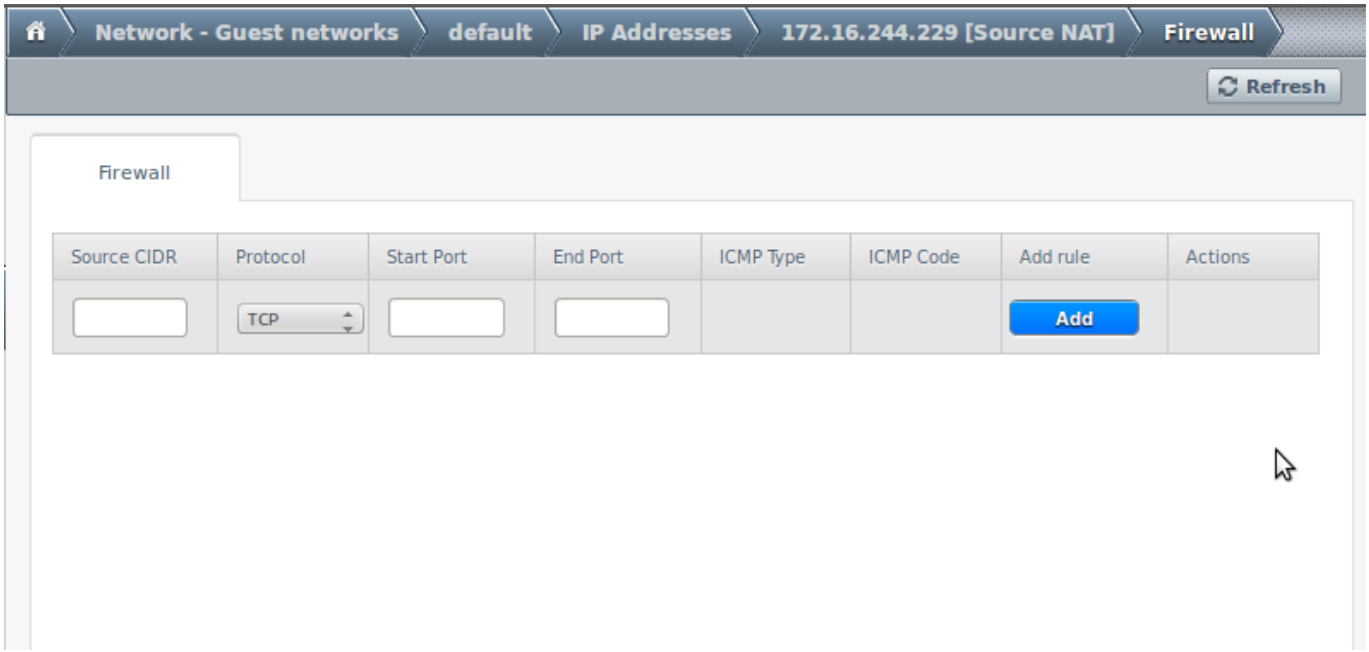
Ahí hay que pinchar en la pestaña “Configuration”, con lo que llegaremos a esta pantalla:



Pantalla de configuración de cortafuegos y nat.

En el botón “Firewall” abrimos la pantalla de configuración del cortafuegos y en el botón “Port Forwarding” la de configuración del nat.

Configurar el cortafuegos

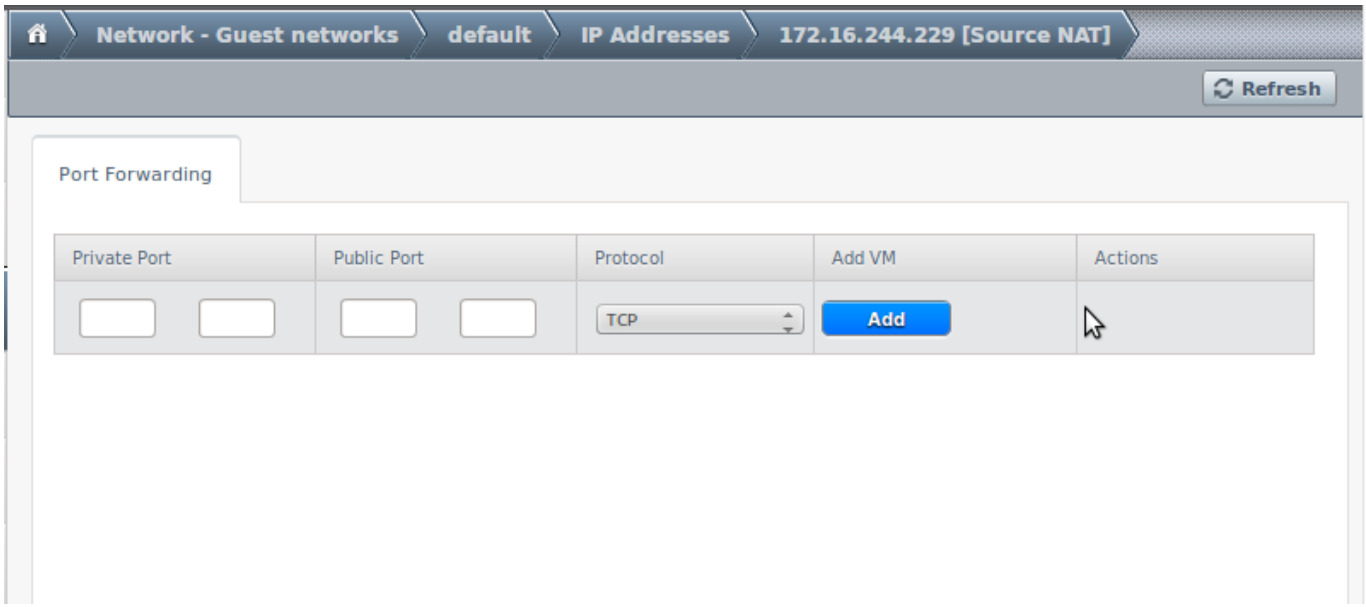


Configuración del cortafuegos

Aqui podemos abrir rangos de puertos de modo que sean accesibles desde la red externa:

- Source CIDR: define para qué direcciones de origen estará permitido el tráfico de esta regla. Se puede poner una red, un host o 0.0.0.0/0 para indicar cualquiera.
- Protocol: TCP, UDP o ICMP.
- Start y End Ports (solo para TCP y UDP): definen el rango de puertos en el que se permitirá el paso. Para especificar un único puerto poner el mismo número en ambos.
- ICMP Type y ICMP Code (solo para ICMP): definen el tipo de mensaje ICMP que se permitirá.
- Add rule: botón que añade la regla a la lista. Una vez añadida es sustituido por un botón para borrarla.

Configurar el nat



Configuración de la redirección de puertos (NAT).

Aqui redirigimos el tráfico que llega a la interfaz externa del router hacia una máquina virtual concreta en función del puerto de destino:

- Private port: puerto de la máquina virtual al que queremos que se conecte.
- Public port: puerto del router virtual que usaremos para conectarnos a la máquina virtual.
- Protocol: especifica si el puerto es TCP o UDP.
- Add VM: aquí se selecciona la máquina virtual a la que irá dirigida la conexión.

El puerto público de la redirección tiene que estar abierto en el cortafuegos.