3.- Contafuegos en Proxmox

- 3.1.- Firewall gestionado por Proxmox

Licencia Creative Commons BY-NC-SA.

3.1.- Firewall gestionado por Proxmox

> El cortafuegos hay que activarlo a tres niveles

A nivel de Centro de datos

Para activar el cortafuegos a nivel del clúster de servidores, tenemos que activar en la opción Centro de datos - Cortafuego - Opciones:

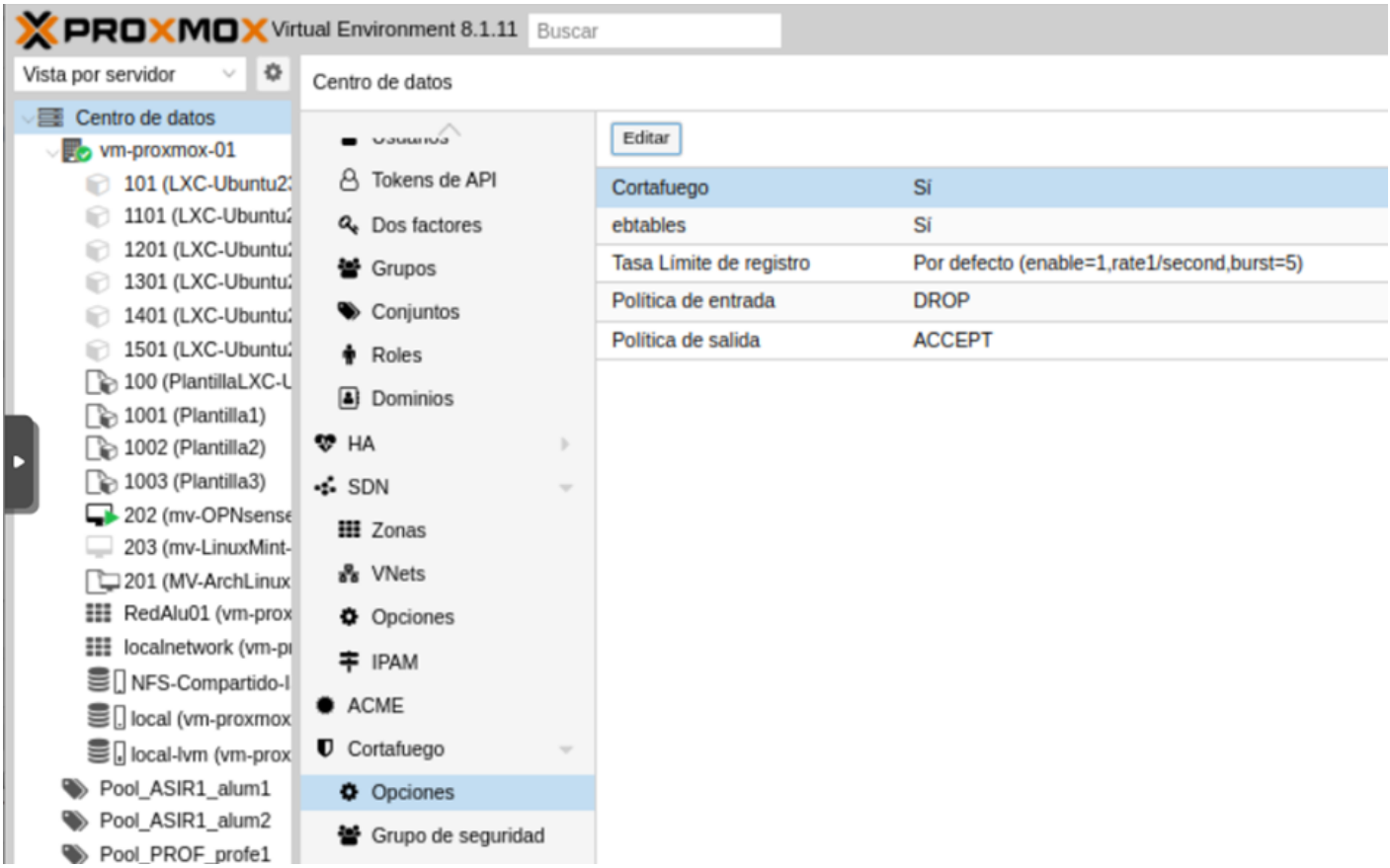


Imagen de elaboración propia: *Activar el firewall a nivel de Centro de Datos* (CC BY-NC-SA)

Aunque no es necesario, para obtener más seguridad en el acceso de los servidores del clúster, podemos cambiar la política para denegar por defecto todo el tráfico de salida, para ello cambiamos la **Políticas de entrada (Output Policy) a DROP**.

Licencia Creative Commons BY-NC-SA.

En este nivel también puedes configurar:

- Security Group: Conjuntos de reglas de cortafuegos que posteriormente podemos asignar a un cortafuegos de una máquina.
- Alias: Nos permite nombrar direcciones IP para que sea más sencillo crear las reglas de cortafuegos.
- IPSec: Nos permite crear grupos de IP para facilitar la asignación de reglas de cortafuegos a varias IP.

A nivel de Servidor

En este caso volvemos a activar el cortafuegos eligiendo el nombre del nodo, en mi caso la opción vm-proxmox-01 - Cortafuegos - Opciones.

Al activar el cortafuegos a nivel del servidor, se utilizan las políticas de entrada y salida por defecto que se habían configurado en el nivel de Centro de datos: todo el tráfico (de entrada y de salida bloqueado, pero se mantienen abierto el puerto 8006 (para acceder a la página web) y el 22 (para el acceso por ssh al servidor).

Nivel de máquina/contenedor

Para activar el cortafuegos para una máquina/contenedor nos vamos a la opción Cortafuegos - Opciones del recurso:

Licencia Creative Commons BY-NC-SA.

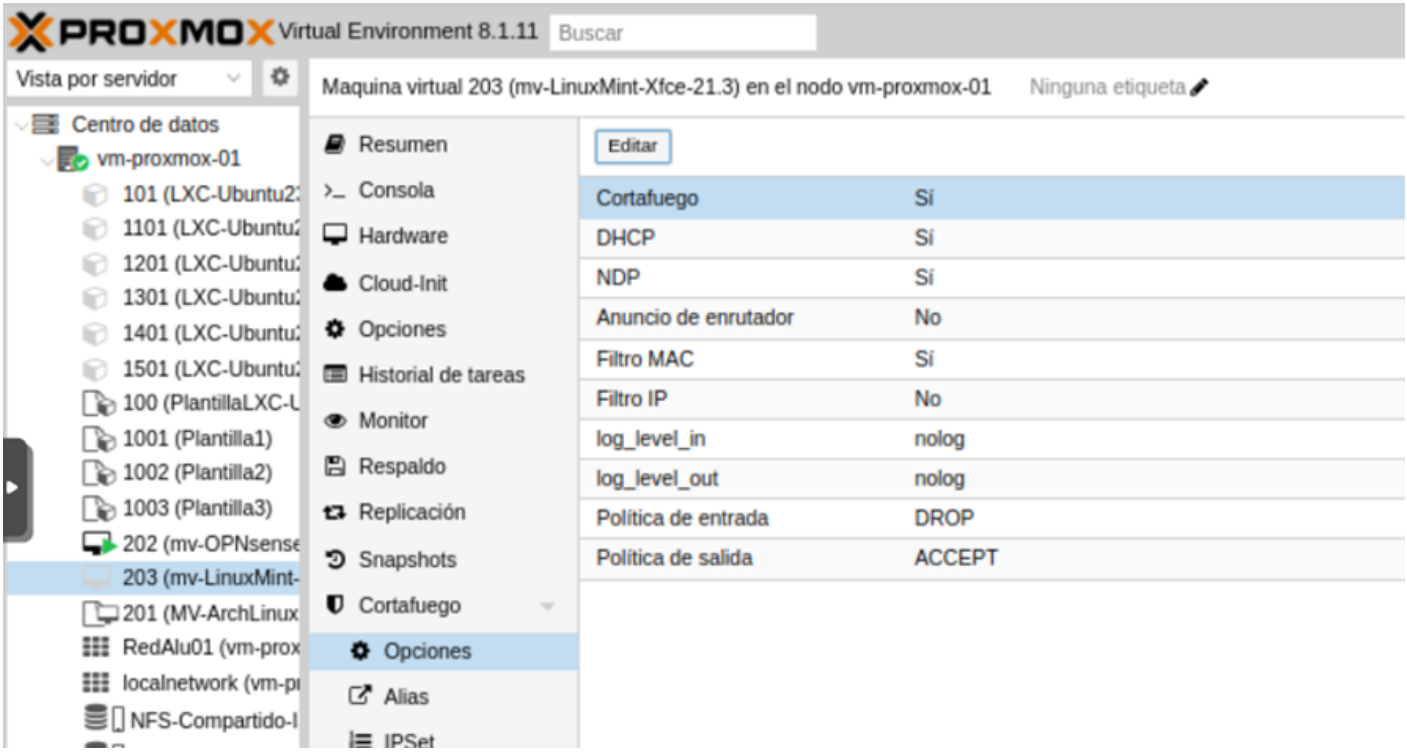


Imagen de elaboración propia: *Activar el cortafuego en una MV* (CC BY-NC-SA)

Tendremos que asegurar en la interfaz de red de la MV que el cortafuegos se encuentra activado:

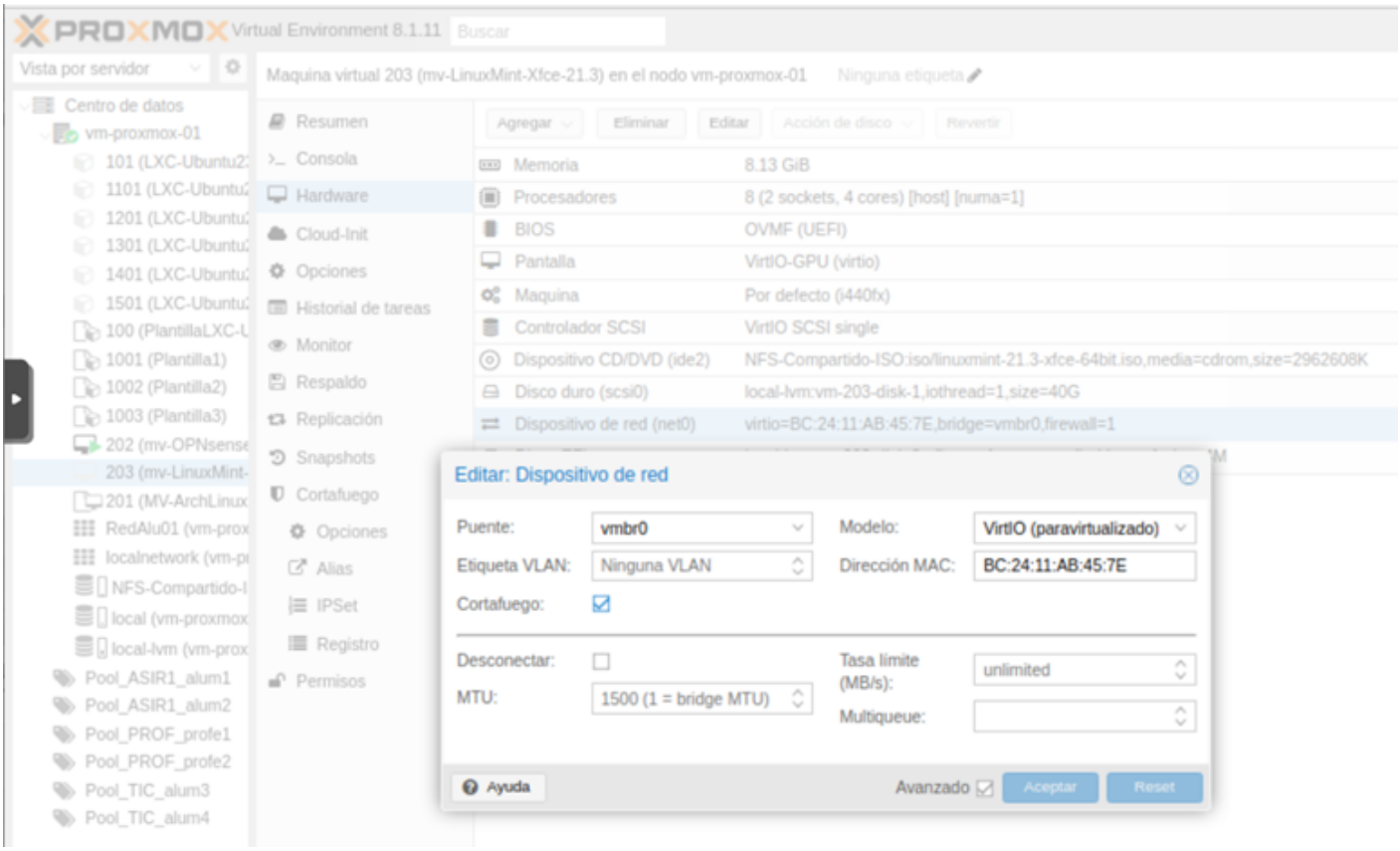


Imagen de elaboración propia: *Activar el cortafuegos en la interfaz de red de la MV* (CC BY-NC-SA)

Licencia Creative Commons BY-NC-SA.

Vemos las políticas por defecto para esta máquina:

- **Políticas de entrada** (Input policy): DROP, es decir se deniega todo el tráfico de entrada (y tenemos que crear reglas de cortafuegos para permitir el tráfico que nos interese).
- **Políticas de salida** (Output Policy): ACCEPT, se acepta todo el tráfico de salida de la máquina (y tenemos que indicar las reglas de cortafuegos para denegar el tráfico que no permitamos).

Si quisiéramos un cortafuegos más restrictivo pondríamos las dos políticas por defecto a DROP, es decir, tanto el tráfico de entrada como el de salida estarían bloqueados, y tendríamos que ir creando reglas de cortafuegos para aceptar el tráfico que deseáramos permitir.

Además, cómo una máquina o contenedor pueden tener más de una interfaz podemos activar o desactivar el cortafuegos para cada interfaz de red. Por defecto, el cortafuegos está activo en cada interfaz de red. Podemos modificar las características del interfaz de red para desactivar el cortafuego.

En resumen, para poder habilitar el cortafuegos para una máquina virtual y/o contenedor, debemos habilitar el cortafuegos tanto a nivel de Centro de datos como a nivel del servidor, finalmente podemos activar o desactivar el cortafuegos para cada una de las interfaces de red de una máquina o contenedor.

Ejemplo de creación de reglas en el cortafuego

Como hemos visto anteriormente, si habilitamos el cortafuegos para una máquina tendrá permitido el tráfico hacia el exterior (Output Policy: ACCEPT) y tendrá denegado el tráfico desde el exterior a la máquina (Input policy: DROP).

Partimos de una máquina que tiene un servidor ssh instalado. Está máquina tendrá conectividad al exterior, pero no tendrá conectividad desde el exterior. Vamos a poner dos ejemplos de reglas:

Regla para denegar que la máquina haga ping al exterior

Todo el tráfico está permitido hacía el exterior, pero vamos a denegar el ping. Para ello debemos crear una regla de salida para denegar el protocolo ICMP, para ello, a nivel de máquina virtual, vamos a añadir una regla al cortafuego, eligiendo la opción Cortafuegos - Añadir:

Licencia Creative Commons BY-NC-SA.

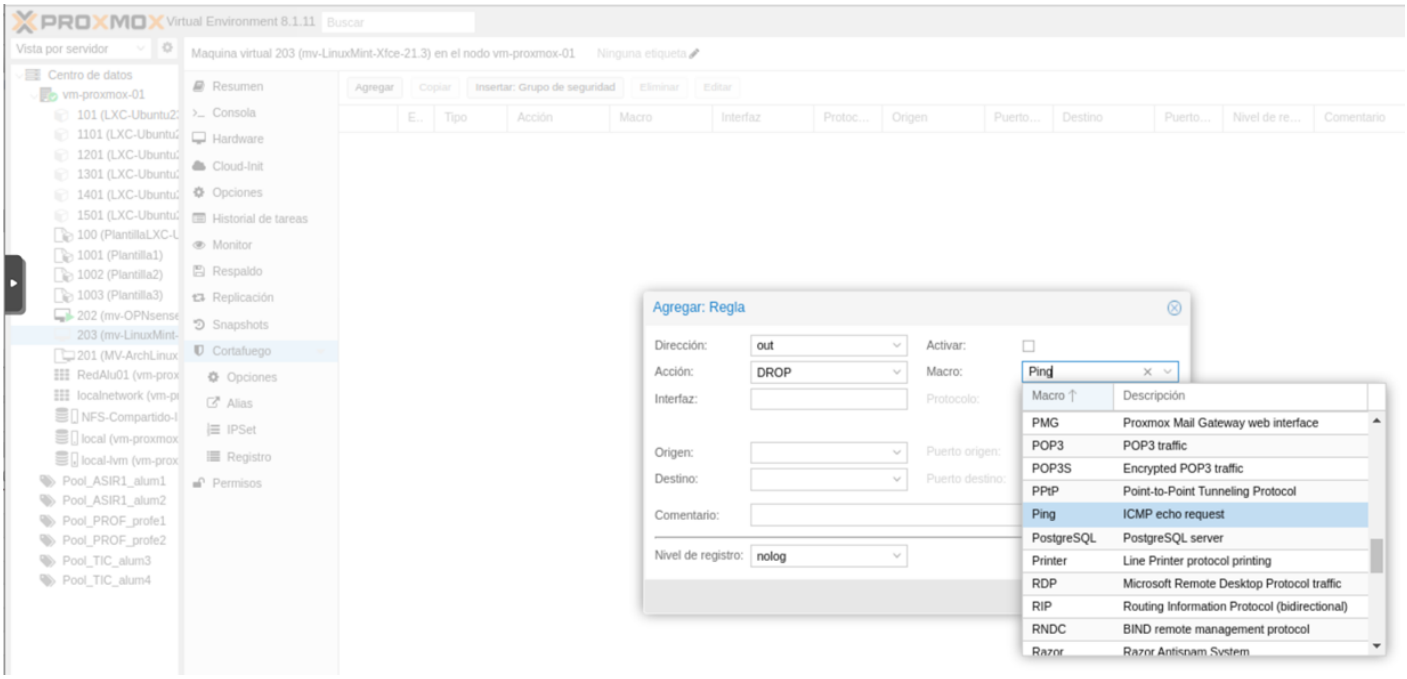


Imagen de elaboración propia· *Regla en el cortafuegos para impedir hacer ping a host fuera de la red local* (CC BY-NC-SA)

> Debemos de activar esta regla para que sea efectiva.

Regla para permitir el acceso por ssh a la máquina

En esta ocasión tenemos que crear una regla que permita (acción ACCEPT) la entrada (dirección in) por el puerto de destino 22 del protocolo TCP. En esta ocasión no vamos a elegir el servicio de la lista de Macro, lo vamos a indicar directamente. Quedaría:

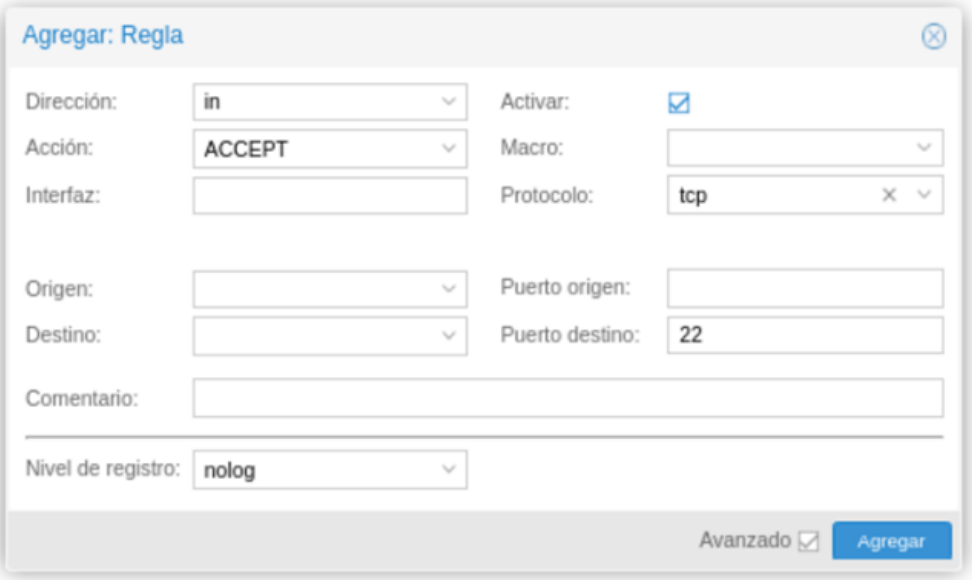


Imagen de elaboración propia· *Permitir el puerto de escucha 22 por TCP en la MV* (CC BY-NC-SA)

Para saber más

- Firewall
- Proxmox VE Firewall

Licencia Creative Commons BY-NC-SA.