Universidad Autónoma de Baja California

Facultad de Ciencias Químicas e Ingeniería

GESTIÓN Y SEGURIDAD EN REDES

Meta 4.2

Firewall

Docente: ALVAREZ SALGADO, CARLOS FRANCISCO

Alumno: Gómez Cárdenas, Emmanuel Alberto

Matricula: 01261509

¿Qué tipo de firewall tengo?

Firewall de red:

¿Qué tipo de firewall de red estamos utilizando? Utilizando los comandos “sudo iptables -L” o “sudo ufw status”, podemos darnos cuenta de que nuestro Ubuntu server cuenta con ambos firewalls. En este caso nos enfocaremos en ufw (Uncomplicated Firewall).

¿Cuáles son las reglas de filtrado aplicadas por el firewall? Debido a que nuestro firewall está desactivado no existe ninguna regla de filtrado actualmente activa.

¿Qué protocolos y puertos están siendo monitoreados por firewall? Al igual que la anterior, ninguno actualmente.

¿Cómo se gestiona el firewall? Para gestionar el firewall teneos los comandos básicos “enable”, “disable”, “allow”, “deny”, entre otros, pero si se necesita mas información podemos usar el comando “man ufw”.

¿Qué capacidades de inspección profunda de paquetes tiene el firewall? Al ser una interfaz de firewall simplificada para iptables, ufw no proporciona este tipo de capacidades, sin embargo, puede ser usada con otras herramientas o servicios que agregan este tipo de funcionalidades.

¿Existen funcionalidades de detección y prevención de intrusiones integradas en el firewall? Al igual que la anterior, ufw no incluye funcionalidades integradas, estas pueden ser complementadas con otros servicios y herramientas.

Firewall personal:

¿Qué software de firewall personal estamos utilizando?

¿Cuáles son las reglas de seguridad configuradas en el firewall personal?

¿Se permite el tráfico entrante o saliente por defecto

¿Cuál es el nivel de interacción del usuario con el firewall personal?

¿Qué notificaciones y alertas proporciona el firewall personal?

¿Se pueden establecer excepciones para ciertos programas o servicios?

Firewall en server

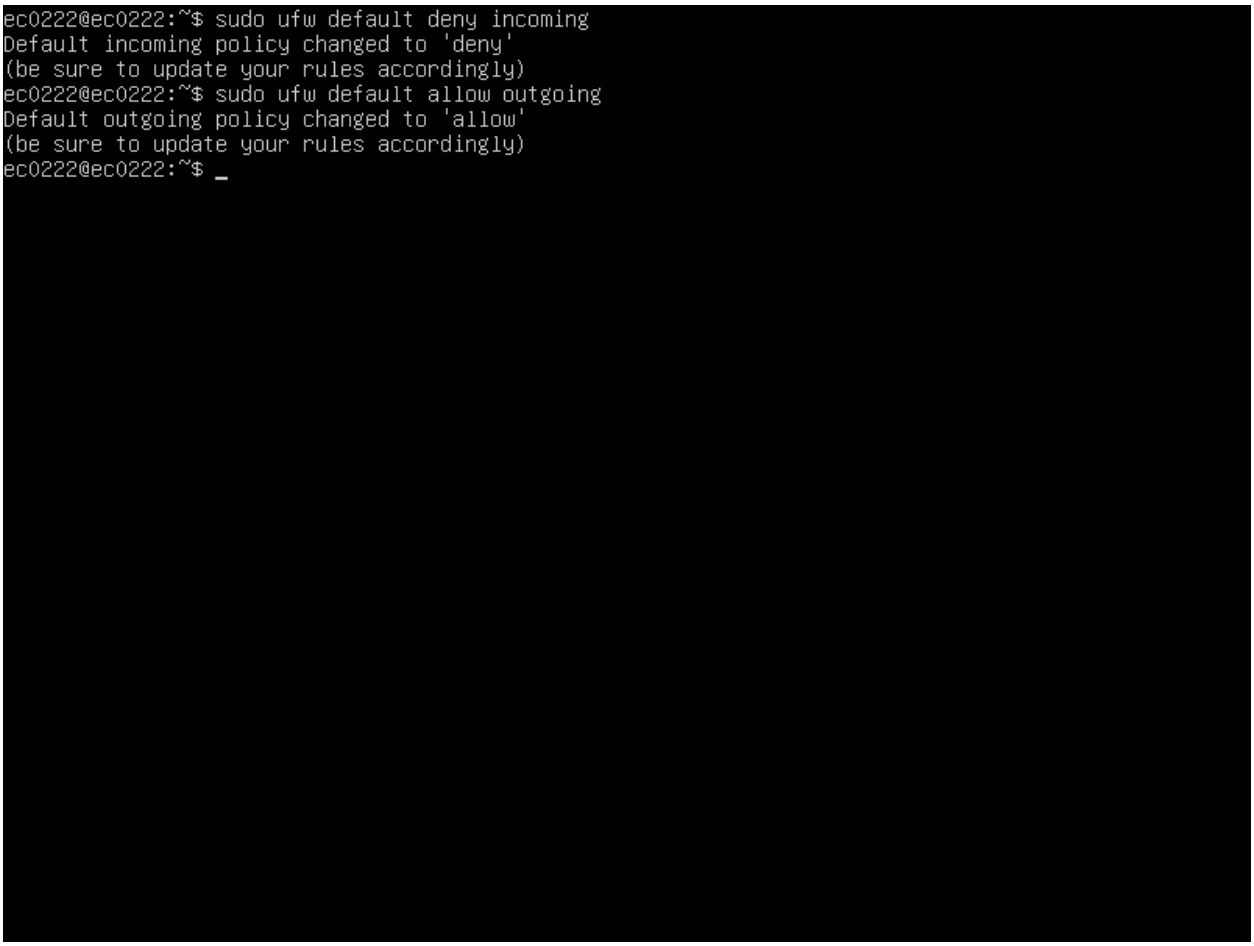
Activar el firewall

1. Establecemos los valores predeterminados de ufw con los siguientes comandos.

---

sudo ufw default deny incoming

sudo ufw default allow outgoing



2. Habilitamos conexiones SSH, HTTP y HTTPS.

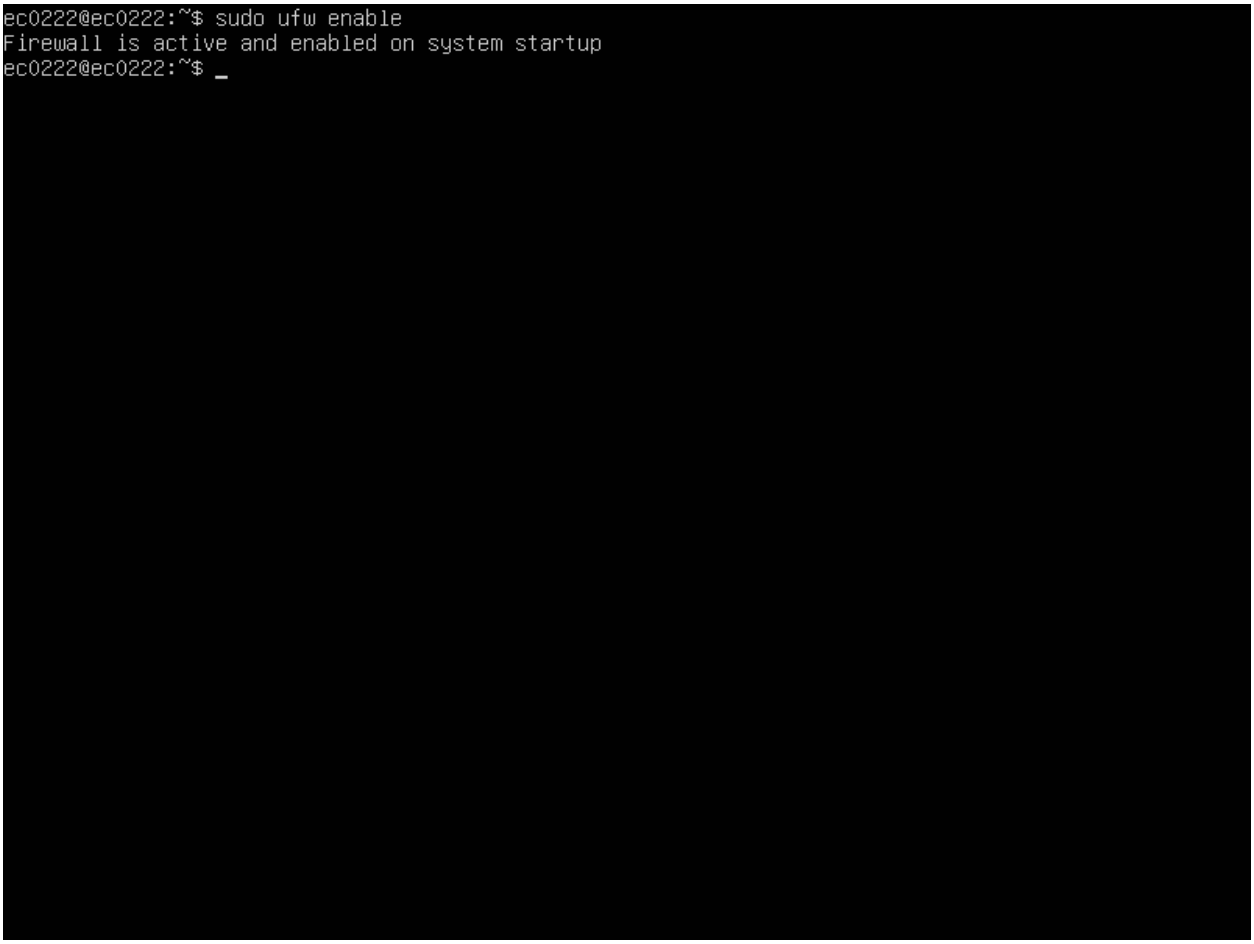
sudo ufw allow ssh

sudo ufw allow http

sudo ufw allow https

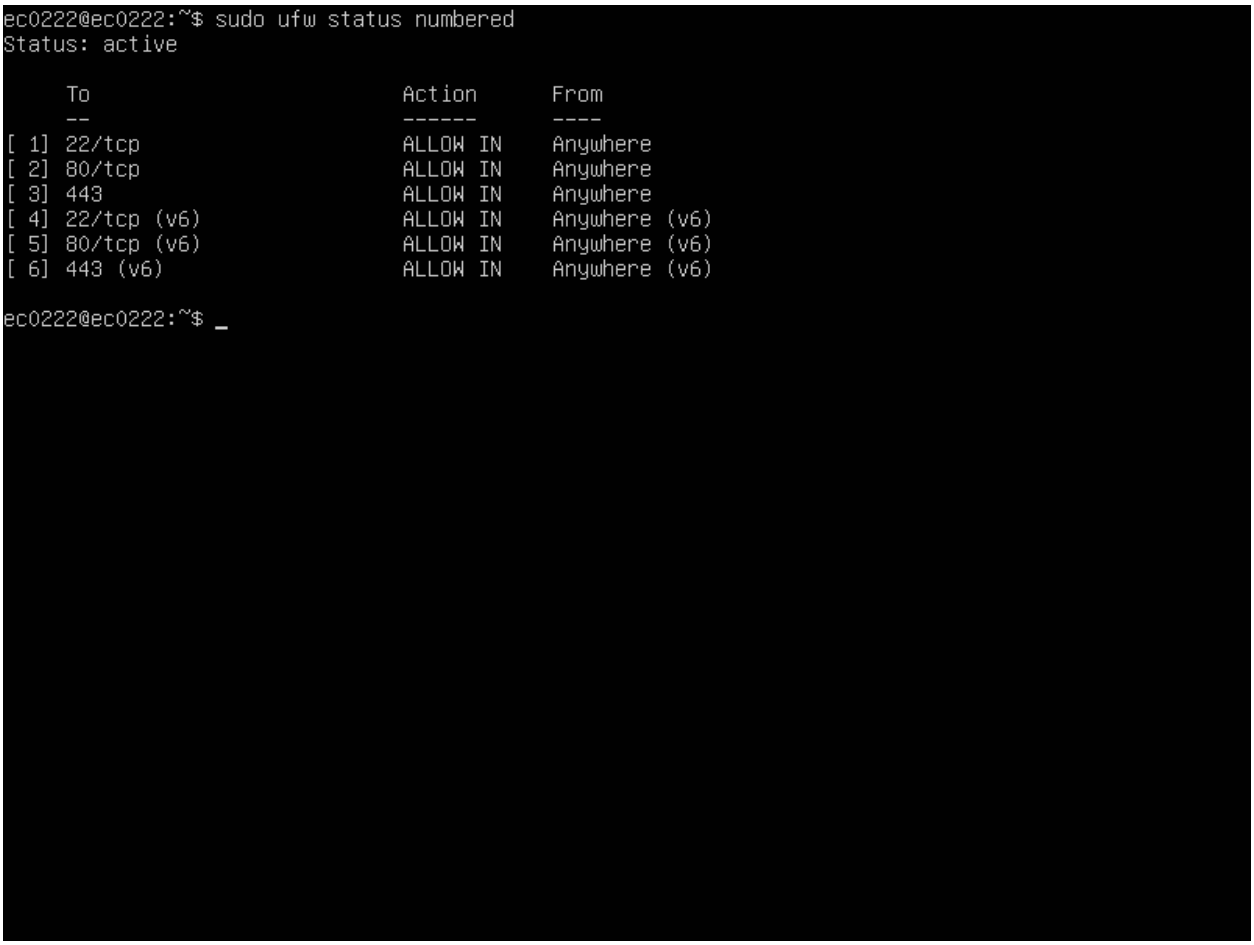
3. Habilitamos UFW.

sudo ufw enable



4. Checar status.

sudo ufw status numbered



5. Permitir tráfico del puerto TCP/80 y sus respuestas, en nuestro caso al usar las opciones por defecto, las conexiones por el puerto TCP/80 ya están permitidas (como puede ser observado en la imagen anterior), pero para activar se utiliza el siguiente comando.

sudo ufw allow 80/tcp

6. Permitir el Puerto 22 solo a mi equipo real (la maquina host).

sudo ufw allow from 192.168.1.64 to any port 22 proto tcp

sudo ufw deny 22

7. Permitir a los servicios solo conectarse a la maquina huésped asegurándose que los cambios se apliquen cada reinicio del sistema.

sudo ufw allow from 192.168.1.64 to any

sudo ufw deny from any

```
ec0222@ec0222:~$ sudo ufw status
Status: active

To                         Action      From
--                         ------      ----
22/tcp                     ALLOW       Anywhere
80/tcp                     ALLOW       Anywhere
443                        ALLOW       Anywhere
22/tcp                     ALLOW       192.168.1.64
22                         DENY        Anywhere
Anywhere                   ALLOW       192.168.1.64
Anywhere                   DENY        Anywhere
22/tcp (v6)                ALLOW       Anywhere (v6)
80/tcp (v6)                ALLOW       Anywhere (v6)
443 (v6)                   ALLOW       Anywhere (v6)
22 (v6)                    DENY        Anywhere (v6)
Anywhere (v6)              DENY        Anywhere (v6)

ec0222@ec0222:~$
```