

# Protege Linux aprendiendo a usar un Firewall

Por el mero hecho de estar conectados a Internet podemos estar en peligro. En la red se esconden una gran cantidad de amenazas y piratas informáticos que buscan la menor oportunidad para poder tomar el control de nuestro PC y nuestros datos. Ya sea a través de programas malignos, vulnerabilidades o fallos en la configuración del PC, siempre podemos estar en peligro. Y aunque usemos un sistema operativo seguro, como es el caso de Linux, siempre debemos conocer las medidas de seguridad que nos ofrece para poder tener controlada esta seguridad. Y una de ellas es **UFW**, uno de los Firewall más populares.

Antes de entrar en materia y centrarnos en este elemento tan importante para la seguridad de Linux, veamos de qué hablamos realmente. Es importante saber que en términos generales un firewall es un sistema diseñado para proteger las redes privadas de los accesos no autorizados ni verificados cuando hacemos uso de una conexión a Internet. En este caso nos queremos centrar en aquellos firewalls software, aunque también hay elementos hardware para este tipo de tareas de seguridad.

Esto quiere decir que estos componentes que instalamos en el ordenador se encargan de protegerlo, tanto de forma individual como aquellos que forman parte de una red doméstica. Así estaremos protegidos de primera mano de todos aquellos ataques que provengan de los **sitios web** que visitamos, o de aquellas aplicaciones que hacen uso de determinados puertos de nuestro **router**. Estos elementos software los utilizamos tanto a nivel empresarial como en nuestro hogar a nivel de usuario final.

De manera adicional también se pueden configurar con el fin de impedir el acceso a nuestro equipo por parte de otros usuarios o de determinados sitios web. Estos elementos también son habituales por parte de los padres que quieren establecer una serie de filtros en la **conexión a Internet** para los más pequeños de la casa, por ejemplo.

## ¿Qué es UFW?

Si nos centramos en software de estas características que encontramos en los sistemas Linux, hablaremos de UFW. Este es el acrónimo de «**Uncomplicated Firewall**». Aunque Linux ya tiene otras medidas de control para las conexiones que establecemos aquí, como las iptables, en realidad controlar el cortafuegos a través de ellas es una tarea de lo más complicada. Por ello, Canonical (desarrolladora responsable de Ubuntu) decidió crear un firewall más sencillo de usar para que todos los usuarios puedan **configurar iptables** de forma usando un pequeño número de comandos simples. Y así nació UFW, que es precisamente en el que nos centraremos ahora.

Este es un cortafuegos que es totalmente gratuito, de código abierto y está escrito en Python. Viene por defecto en Ubuntu desde la versión 8.04 LTS, y muchas distros han decidido añadirlo igualmente por defecto debido a su utilidad. Además, si no viene, podemos descargarlo e instalarlo sin problemas desde sus respectivos repositorios.

Esto significa que, si nos convence su utilidad y funcionamiento, además de todas las funciones de seguridad que nos propone, en Ubuntu, igualmente podremos hacer uso de este mismo elemento en otras muchas distribuciones del sistema de código abierto.

# Comandos esenciales para configurar el Firewall de Linux

Es importante tener en cuenta que, aunque venga por defecto en muchas distribuciones, por lo general suele venir desactivado. Esto lo hacen para evitar que los usuarios tengan conflictos de reglas que puedan causar problemas difíciles de identificar al conectarse a Internet o usar determinados programas.

Es por ello que a continuación os vamos a hablar de algunos de los más importantes comandos que podéis ejecutar desde el terminal de Linux para trabajar con este elemento de seguridad. De esta manera podremos realizar algunas tareas básicas de configuración además de comprobar si lo tenemos en funcionamiento en nuestro sistema operativo. En el caso de que no estéis muy cómodos con el uso de estos comandos, más adelante también os mostraremos cómo configurar este firewall a través de una intuitiva interfaz de usuario gráfica.

Podemos comprobar fácilmente el estado de este cortafuegos ejecutando:

```
sudo ufw status
```

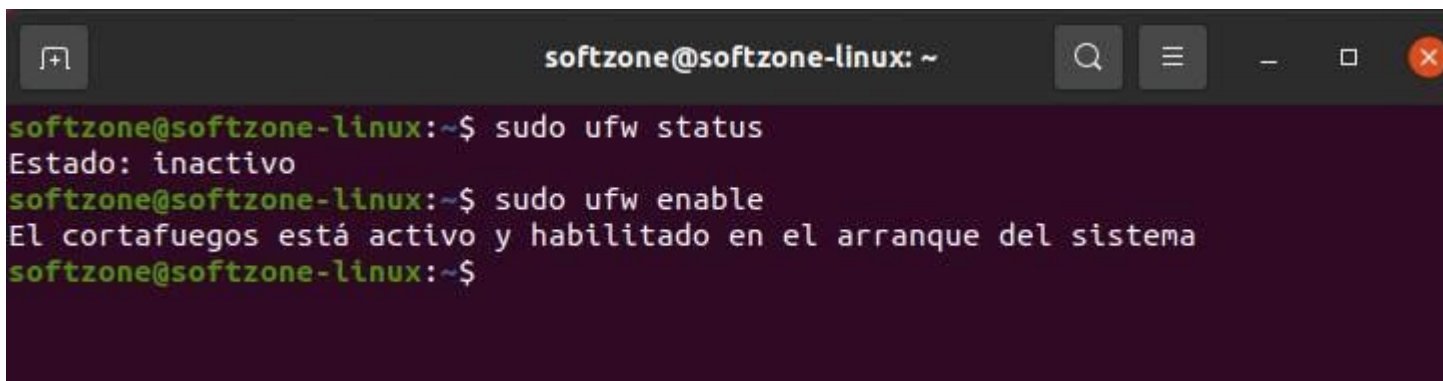
Si está desactivado, podemos activarlo en un momento usando el primero de los siguientes comandos. Y, si está activado y lo queremos desactivar, podemos hacerlo igualmente sin problemas ejecutando el segundo de los siguientes comandos:

**Activar:**

```
sudo ufw enable
```

**Desactivar:**

```
sudo ufw disable
```

A screenshot of a Linux terminal window. The window title is 'softzone@softzone-linux: ~'. The terminal shows the following commands and output: 

```
softzone@softzone-linux:~$ sudo ufw status
Estado: inactivo
softzone@softzone-linux:~$ sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
softzone@softzone-linux:~$
```

Hasta aquí el control básico del cortafuegos que viene por defecto en Linux. Pero por mucho que lo activemos, sin reglas, no servirá de gran cosa. Por lo tanto, una vez activado vamos a ver cómo debemos configurarlo. Y para ello vamos a usar el comando «ufw app». Con él vamos a poder ver los programas que tienen reglas, y los detalles de cada una de estas reglas.

Para ver la **lista de las aplicaciones con reglas**, ejecutaremos el comando de la siguiente manera:

```
sudo ufw app list
```

Y, para ver los detalles de una de las reglas, entonces ejecutaremos lo siguiente:

```
sudo ufw app info nombre_programa
```

```
softzone@softzone-linux: ~  
softzone@softzone-linux:~$ sudo ufw app list  
Aplicaciones disponibles:  
  CUPS  
softzone@softzone-linux:~$ sudo ufw app info CUPS  
Perfil: CUPS  
Título: Common UNIX Printing System server  
Descripción: CUPS is a printing system with support for IPP, samba, lpd,  
and other protocols.  
  
Puerto:  
  631  
softzone@softzone-linux:~$
```

Con el firewall activado ya estaremos un poco protegidos, ya que se bloquearán todas las conexiones del exterior a nuestro PC. Pero ¿qué pasa si necesitamos que un programa pueda conectarse de forma remota al PC? Por ejemplo, los clientes de descarga. ¿O si queremos poder conectarnos nosotros mismos cuando no estemos en casa?

Esto podemos hacerlo principalmente con «ufw allow», seguido del **puerto**, o rango de puertos, y el protocolo deseado. Por ejemplo, podemos ejecutar los siguientes comandos para abrir los puertos del 50000 al 53000 para que los clientes torrent puedan funcionar con normalidad:

```
sudo ufw allow 50000:53000/tcp sudo ufw allow 50000:53000/udp
```

```
softzone@softzone-linux: ~  
softzone@softzone-linux:~$ sudo ufw allow 50000:53000/tcp  
Regla añadida  
Regla añadida (v6)  
softzone@softzone-linux:~$
```

Igualmente, si cambiamos el «allow» por «deny» estaremos cerrando un puerto, o rango de puertos. Esto es útil, por ejemplo, si abrimos un rango de puertos como el que acabamos de ver, pero queremos que alguno entre medias esté cerrado y bloqueado.

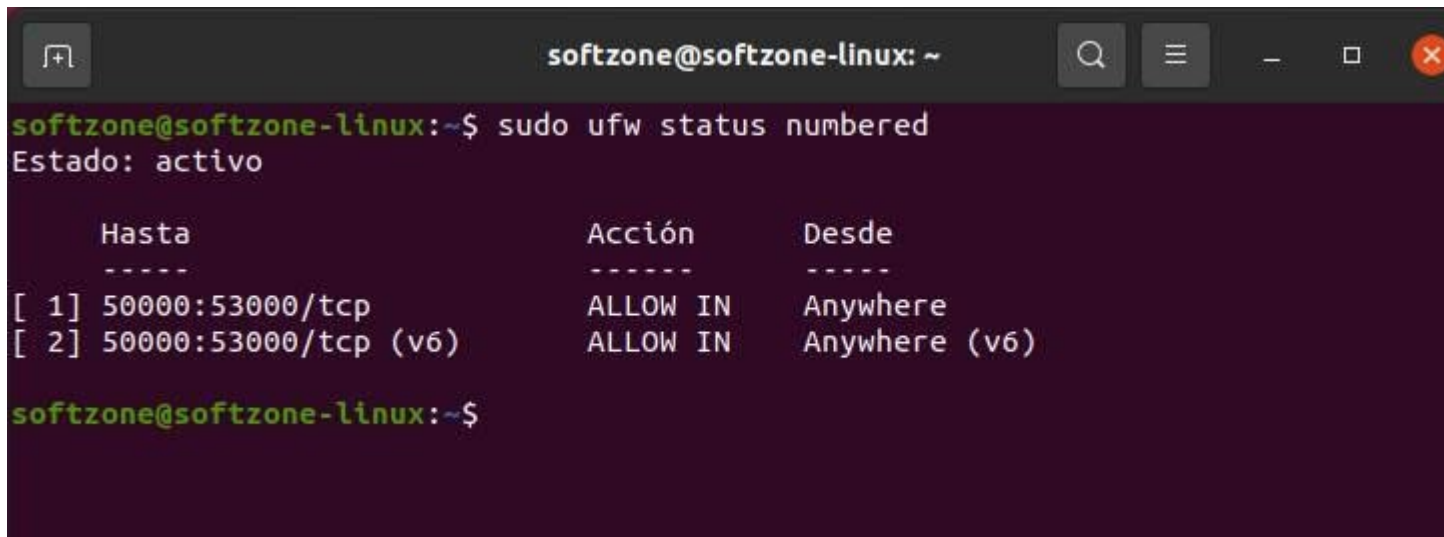
También podemos crear reglas que se apliquen dentro de la red LAN para que otros PCs de la misma puedan conectarse a nuestro ordenador. Por ejemplo:

```
sudo ufw allow from 192.168.1.100/24 to any port 8080
```

En este ejemplo estamos permitiendo a un PC con IP 192.168.1.100 dentro de una subred 24 pueda conectarse a nuestro Linux a través del puerto 8080. Igualmente, podemos denegar la conexión cambiando el «allow» por «deny» en el comando.

Podemos **ver una lista completa con todas las reglas** e instrucciones que tenemos creadas en nuestro cortafuegos usando este comando:

```
sudo ufw status numbered
```

A terminal window titled 'softzone@softzone-linux: ~' with search, menu, and window control icons in the title bar. The prompt is 'softzone@softzone-linux:~\$'. The command 'sudo ufw status numbered' has been executed, showing 'Estado: activo' and a table of rules. The table has three columns: 'Hasta', 'Acción', and 'Desde'. Rule 1 allows TCP traffic from anywhere on port 50000 to 53000. Rule 2 allows TCP (v6) traffic from anywhere on port 50000 to 53000. The prompt returns to 'softzone@softzone-linux:~\$'.

Si queremos eliminar cualquiera de ellas, podemos hacerlo de forma muy sencilla ejecutando la siguiente instrucción (cambiando «numero» por el número que nos aparecerá):

```
sudo ufw delete numero
```

Y, por último, si queremos resetear por completo el cortafuegos, podemos hacerlo de forma sencilla deteniéndolo como ya hemos visto antes y ejecutando:

```
sudo ufw reset
```

Con esto, se borrarán todas las reglas y toda la configuración volverá a sus valores de fábrica.

## GUFW: configurar el cortafuegos de Linux en modo gráfico

Como hemos podido ver, usar UFW no es para nada complicado, y nos brinda toda la protección y seguridad que podemos necesitar. Sin embargo, si se pueden simplificar aún más las cosas, ¿por qué no hacerlo?

Este cortafuegos se puede configurar mediante los comandos que acabamos de ver en el paso anterior, y también a través de una interfaz gráfica muy sencilla y cómoda que simplifica mucho más las cosas. Hablamos de **GUFW**. Esta interfaz la podemos instalar fácilmente desde los repositorios de las distros (generalmente no viene por defecto) y nos va a permitir controlar por completo el cortafuegos sin aprendernos ningún comando.



Desde su ventana principal vamos a poder activar y desactivar el cortafuegos, así como crear varios perfiles en función del uso que vayamos a dar del PC. Podemos aplicar reglas generales para «permitir» o «bloquear» el tráfico entrando o saliente, o crear reglas mucho más específicas.



Para crear una regla, no tenemos más que ir al apartado «Reglas», hacer clic en el botón «+» y configurar la regla que queremos añadir al programa. Podemos elegir la política que queremos que tenga, la dirección a la que queremos aplicarla, la categoría y la aplicación a la que queremos que se aplique. Tenemos también opciones para una creación simple, y otras para una configuración más avanzada de la misma.

## Añadir una regla al cortafuegos



Preconfigurada

Simple

Avanzada

Política:	Permitir	▼
Dirección:	Entrante	▼
Categoría	Todos	▼
Subcategoría	Todos	▼
Aplicación:	0 A.D.	▼
<input type="text" value="Filtro de aplicaciones"/>  		

Cerrar

Añadir

## Añadir una regla al cortafuegos



Preconfigurada

Simple

Avanzada

Nombre:	Descripción de regla			
Insertar:	0	-	+	
Política:	Permitir			▼
Dirección:	Entrante			▼
Interfaz:	Todas las interfaces			▼
Registro:	No registrar			▼
Protocolo:	Ambos			▼
Desde:	IP			Puerto
A:	IP			Puerto

Cerrar

Añadir



## Añadir una regla al cortafuegos



Preconfigurada

Simple

Avanzada

Política:	Permitir	▼
Dirección:	Entrante	▼
Categoría	Todos	▼
Subcategoría	Todos	▼
Aplicación:	0 A.D.	▼
<input type="text" value="Filtro de aplicaciones"/>  		

Cerrar

Añadir

## Añadir una regla al cortafuegos



Preconfigurada

Simple

Avanzada

Nombre:	Descripción de regla			
Insertar:	0	-	+	
Política:	Permitir			▼
Dirección:	Entrante			▼
Interfaz:	Todas las interfaces			▼
Registro:	No registrar			▼
Protocolo:	Ambos			▼
Desde:	IP			Puerto
A:	IP			Puerto

Cerrar

Añadir



Una vez rellenados los datos de la regla, hacemos clic sobre «Añadir» y esta se añadirá y aplicará al cortafuegos. En caso de querer eliminarla, o modificarla, podemos hacerlo igualmente desde el apartado de teclas de GUFW.

Para tener el máximo control sobre las reglas de las que os hablamos, tenemos la posibilidad de configurarlas en el firewall en base a los estados que os describimos a continuación. Hay que saber que podremos configurar estas para los puertos TCP, UDP, o para ambos. Estos son los posibles estados que podremos establecer aquí,

- Permitir: se permite el tráfico entrante para un determinado puerto en el firewall.
- Denegar: bloqueamos el tráfico entrante para el puerto al que hacemos referencia.
- Rechazar: se rechaza el tráfico entrante para un puerto, aunque siempre se informa de esta acción al sistema que solicita la conexión.
- Limitar: sirve para limitar el intento de conexiones denegadas anteriormente. Esto quiere decir que, si una IP intenta iniciar seis o más conexiones en los últimos 30 segundos, se denegará el acceso.

Al mismo tiempo aquí podremos crear diferentes perfiles de uso para poner en marcha dependiendo de dónde nos encontremos. Asimismo, hay que tener en consideración que estos perfiles que vayamos creando podremos importarlos y exportarlos en Linux para no tener que repetir el proceso cada vez.

Antes de terminar os diremos que en el caso de que no nos termine de convencer el funcionamiento de este elemento de seguridad en Linux, tenemos algunas otras interesantes alternativas entre las que elegir para descartar Gufw.

Igualmente, estas las podremos descargar e instalar desde su correspondiente **repositorio** en nuestra distribución de Linux. De entre las alternativas hoy más conocidas nos podemos encontrar con Guarddog, **Netfilter** o Firestarter.