

Cortafuegos UFW

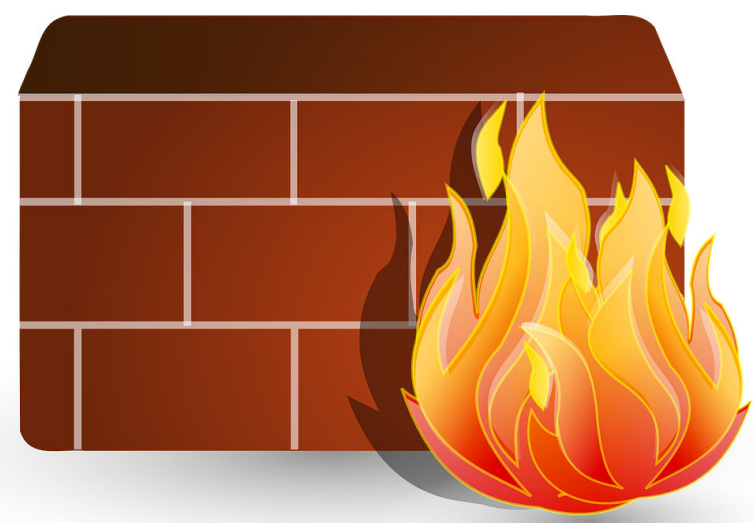
Instalación & Configuración

El cortafuegos UFW (Uncomplicated Firewall)

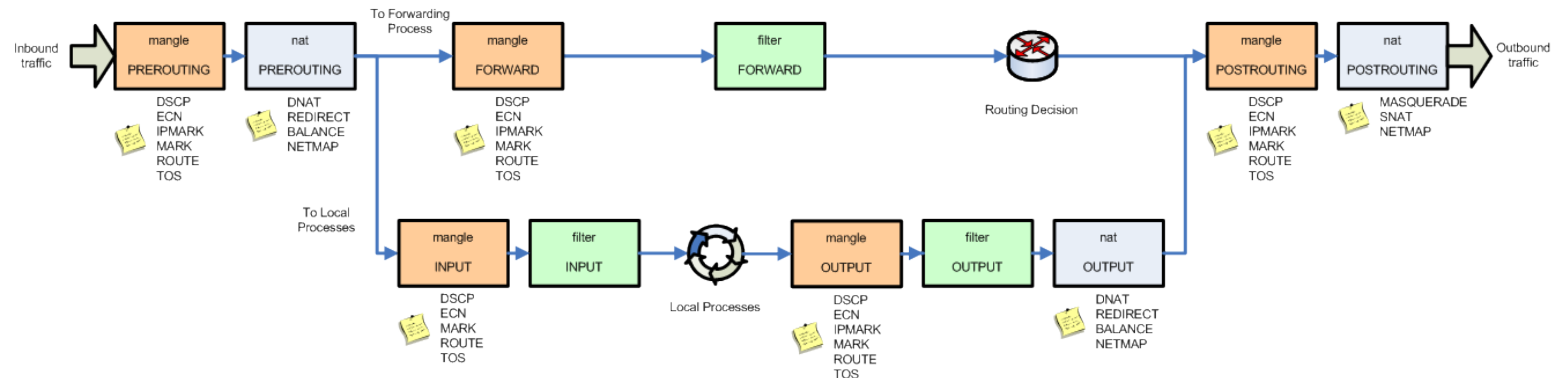
Definición

El Firewall UFW (Uncomplicated Firewall) es una aplicación que simplifica la configuración de reglas en las tablas de firewall nativas de Linux (iptables).

Esta guía proporciona un método sencillo para configurar UFW en un servidor Linux, mejorando la seguridad.

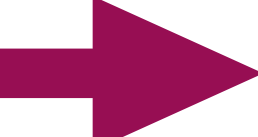


IPTables Chains Order Scheme



Instalación

Utiliza los comandos `sudo apt update` y `sudo apt install ufw` en distribuciones basadas en Debian, como Ubuntu, para instalar UFW.

Puedes comprobar que está correctamente instalado con el comando `sudo ufw help`. Deberías obtener una respuesta similar a esta: 

```
jairo@bravo:~$ sudo ufw help
Usage: ufw COMMAND

Commands:
enable          enables the firewall
disable        disables the firewall
default ARG    set default policy
logging LEVEL  set logging to LEVEL
allow ARGS     add allow rule
deny ARGS     add deny rule
reject ARGS    add reject rule
limit ARGS    add limit rule
delete RULENUM delete RULE
insert NUM RULE insert RULE at NUM
prepend RULE   prepend RULE
route RULE     add route RULE
route delete RULENUM delete route RULE
route insert NUM RULE insert route RULE at NUM
reload         reload firewall
reset         reset firewall
status        show firewall status
status numbered show firewall status as numbered list of RULES
status verbose show verbose firewall status
show ARG      show firewall report
version       display version information

Application profile commands:
app list      list application profiles
app info PROFILE show information on PROFILE
app update PROFILE update PROFILE
app default ARG set default application policy
```

Configuración básica

Comportamiento por defecto

Define el comportamiento por defecto para el tráfico entrante y saliente con los comandos siguientes:

Tipo de tráfico	Comportamiento por defecto	Comando
Entrante	Bloquear todo	<code>ufw default deny incoming</code>
Saliente	Permitir todo	<code>ufw default allow outgoing</code>

Nota: Los comandos deben ejecutarse como administrador: utilizar `su` o `sudo`.

Permitir conexiones SSH

Habilitar las conexiones entrantes para administración via SSH

Si el host se administra a través del protocolo SSH es importante que las conexiones de dicho protocolo se permitan. De lo contrario, el acceso remoto al servidor quedaría bloqueado.

Si al host se accede únicamente de forma local, se puede omitir este paso.

Para permitir las conexiones entrantes de SSH, utiliza el comando `sudo ufw allow ssh`



Reglas de cortafuegos

Permitir, denegar y rechazar tráfico

Para crear reglas del cortafuegos utiliza algunos de los comandos siguientes:

- Para permitir el paso: `ufw allow ...`
- Para denegar el acceso, descartando paquetes: `ufw deny ...`
- Para rechazar el acceso, emitiendo respuesta: `ufw reject ...`

Ejemplo:

```
sudo ufw allow https
```

Nota: Los comandos deben ejecutarse como administrador: utilizar `su` o `sudo`.

Reglas de cortafuegos

Ejemplos

Regla	Comando
Permitir tráfico dirigido al puerto 53	<code>ufw allow 53</code>
Permitir tráfico dirigido al puerto 25 del protocolo TCP	<code>ufw allow 25/tcp</code>
Permitir el tráfico del protocolo SMTP	<code>ufw allow smtp</code>
Permitir tráfico entrante del protocolo HTTP	<code>ufw allow in http</code>
Rechazar el tráfico saliente del protocolo SMTP	<code>ufw reject out smtp</code>
Denegar el tráfico dirigido al host en el puerto 80 de TCP	<code>ufw deny proto tcp to any port 80</code>
Denegar tráfico originado en la red 10.0.0.0/8 dirigido al puerto 25 del host 192.168.0.1	<code>ufw deny proto tcp from 10.0.0.0/8 to 192.168.0.1 port 25</code>

Nota: Los comandos deben ejecutarse como administrador: utilizar `su` o `sudo`.

Ver configuración actual

Consultar el estado del cortafuegos

Con el comando `sudo ufw status verbose` se puede consultar el estado actual del cortafuegos.

```
jairo@bravo:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To Action From
--
22/tcp ALLOW IN Anywhere
443 ALLOW IN Anywhere
3306/tcp ALLOW IN 192.168.1.0/24
161 ALLOW IN Anywhere
22/tcp (v6) ALLOW IN Anywhere (v6)
443 (v6) ALLOW IN Anywhere (v6)
161 (v6) ALLOW IN Anywhere (v6)
```


Eliminación de reglas

Para eliminar reglas existentes

Se puede eliminar una regla previamente introducida con el comando `ufw delete ...`

```
jairo@bravo:~$ sudo ufw delete allow https
Rule deleted
Rule deleted (v6)
```

Ejemplo: `sudo ufw delete allow https`

Para eliminar reglas existentes (por numeración)

También se puede eliminar una regla indicando su numeración. Para ello, primero consulta las reglas existentes con `ufw status numbered`; luego, elimina la regla con `ufw delete`.

```
jairo@bravo:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 22/tcp    ALLOW IN    Anywhere
[ 2] 3306/tcp   ALLOW IN    192.168.1.0/24
[ 3] 161        ALLOW IN    Anywhere
[ 4] 22/tcp (v6) ALLOW IN    Anywhere (v6)
[ 5] 161 (v6)   ALLOW IN    Anywhere (v6)

jairo@bravo:~$ sudo ufw delete 2
Deleting:
  allow from 192.168.1.0/24 to any port 3306 proto tcp
[Proceed with operation (y/n)? y
Rule deleted
```

Ejemplo: `sudo ufw delete 2`

Inserción de reglas

El orden de las reglas importa, de modo que si quieres añadir una regla para que se procese antes que otras reglas ya existentes, puedes insertarla con el comando `ufw insert ...`

Ejemplo:

```
sudo ufw insert 1 allow https
```

```
jairo@bravo:~$ sudo ufw status numbered
Status: active

    To      Action      From
    --      -
[ 1] 22/tcp   ALLOW IN    Anywhere
[ 2] 161      ALLOW IN    Anywhere
[ 3] 443 (v6) ALLOW IN    Anywhere (v6)
[ 4] 22/tcp (v6) ALLOW IN    Anywhere (v6)
[ 5] 161 (v6) ALLOW IN    Anywhere (v6)

jairo@bravo:~$ sudo ufw insert 1 allow https
Rule inserted
Skipping inserting existing rule (v6)
jairo@bravo:~$ sudo ufw status numbered
Status: active

    To      Action      From
    --      -
[ 1] 443      ALLOW IN    Anywhere
[ 2] 22/tcp   ALLOW IN    Anywhere
[ 3] 161      ALLOW IN    Anywhere
[ 4] 443 (v6) ALLOW IN    Anywhere (v6)
[ 5] 22/tcp (v6) ALLOW IN    Anywhere (v6)
[ 6] 161 (v6) ALLOW IN    Anywhere (v6)
```

Activar/Desactivar cortafuegos

Activación

```
jairo@bravo:~$ sudo ufw enable
[Command may disrupt existing ssh connections. Proceed with operation (y/n)? y
Firewall is active and enabled on system startup
```

```
sudo ufw enable
```

Desactivación

```
jairo@bravo:~$ sudo ufw disable
Firewall stopped and disabled on system startup
```

```
sudo ufw disable
```

Eliminación de todas las reglas

```
sudo ufw reset
```

```
jairo@bravo:~$ sudo ufw reset
Resetting all rules to installed defaults. This may disrupt existing ssh
connections. Proceed with operation (y/n)? y
Backing up 'user.rules' to '/etc/ufw/user.rules.20240328_125506'
Backing up 'before.rules' to '/etc/ufw/before.rules.20240328_125506'
Backing up 'after.rules' to '/etc/ufw/after.rules.20240328_125506'
Backing up 'user6.rules' to '/etc/ufw/user6.rules.20240328_125506'
Backing up 'before6.rules' to '/etc/ufw/before6.rules.20240328_125506'
Backing up 'after6.rules' to '/etc/ufw/after6.rules.20240328_125506'
```

Registros de actividad

Activación

```
sudo ufw logging low
```

Desactivación

```
sudo ufw logging off
```

El registro de actividad se puede consultar con el comando `dmesg -w`, ejecutado como root.

Desinstalación

Para eliminar completamente UFW

Utiliza el comando `sudo apt purge ufw` para eliminar UFW del sistema, dejándolo en el estado previo a la instalación.