HABILITAR IPTABLES COMO UN SERVICIO

La configuración realizada de IPTABLES solamente permanece mientras el equipo se mantiene encendido, por lo que si queremos que el firewall se mantenga activo una vez se reinicie la máquina pues tendremos que configurar esta configuración como un servicio automático.

Esta es una buena solución al problema comentado, aunque existen otras soluciones como la creación de un script asociado al cron del sistema.

Además de crear este servicio de "iptables", es recomendable dejar habilitado de forma permanente del bit de forward para que la máquina permita el tráfico entre las diferentes interfaces de red.

Los pasos que deben seguirse para conseguir esta configuración final son:

1. *Habilitación permanente del bit de forward.*

Para conseguir dejar este bit habilitado, se tiene que acceder al archivo de configuración llamado "systctl.conf" que se encuentra en el directorio /etc.

En este fichero tenemos que quitar el comentario de la siguiente línea:

net.ipv4.ip_forward=1

Además, si queremos que los cambiamos se apliquen al instante podemos ejecutar el siguiente comando:

sysctl -p /etc/sysctl.conf

Ya tendríamos activa la comunicación entre las interfaces de red.

2. *Guardar las reglas del firewall en un fichero.*

Para guardar las reglas que hemos establecido en el firewall en un fichero podemos hacer uso del comando "iptabes-save" redireccionando el comando a un archivo. Se creará un archivo de configuración de iptables.

iptables-save /etc/iptables/rules.v4 (la carpeta "iptables" debe ser creada anteriormente)

3. *Volcado del fichero de reglas hacia el firewall.*

Una vez creado un archivo de configuración con las reglas del firewall este puede ser volcado en el firewall propio o en cualquier otro equipo mediante el uso del comando "iptables-restore". El uso del comando sería:

iptables-restore ruta-fichero-reglas

iptables-restore /etc/itpables/rules.v4

Este es el modo manual para el volcado de las reglas, pero el objetivo es que se realice de forma automática cuando se inicie el equipo, por lo que crearemos un servicio que vuelca estas reglas y que se iniciará con el sistema.

4. *Crear un servicio del sistema (unidad de systemd).*

El siguiente paso sería la creación de la unidad de systemd para que se inicie con el equipo como un servicio.

El fichero debe guardarse en “/etc/systemd/system/” y lo podríamos llamar “firewall.service”.

La sintaxis de del fichero debe ser:

```
[Unit]
Description=Servicio de firewall
After=systemd-sysctl.service

[Service]
Type=oneshot
RemainAfterExit=yes
ExecStart=/sbin/iptables-restore /etc/iptables/rules.v4
ExecStop=/sbin/iptables-restore /etc/iptables/des_firewall.v4

[Install]
WantedBy=multi-user.target
```

En este fichero podríamos indicar que ocurriría si realizamos un “stop” o un “restart” del servicio. Un ejemplo del “stop” puede ser que se ejecute un “iptables-restore” llamando a un fichero que limpia todas las reglas del firewall.

5. Habilitar el servicio al incio.

Para que este servicio se ejecute de forma automática en cada inicio del equipo tendremos que habilitarlo en “systemctl”. Para ello ejecutamos el comando:

systemctl enable firewall.service

Podemos activar el servicio manualmente:

service firewall start

Ya está todo listo para que el firewall se mantenga siempre activo.

Para desactivar el firewall bastaría con ejecutar el comando:

service firewall stop