Configuración y Análisis de Firewalls en Kali Linux: iptables vs. UFW

Robert Alberto Pertuz Palacio

Laboratorio de ciberseguridad Talentotech 6-7

Talento tech Universidad popular del cesar

06/05/2025

Introducción

La seguridad informática es un aspecto esencial en cualquier sistema de redes, y uno de los mecanismos más importantes de defensa es el firewall. Este actúa como una barrera entre una red confiable y otra no confiable, permitiendo o bloqueando el tráfico según reglas preestablecidas. En sistemas Linux, existen diversas herramientas para la gestión de firewalls. Entre las más conocidas se encuentran iptables y ufw (Uncomplicated Firewall).

iptables ofrece un control detallado sobre las reglas de tráfico, aunque su complejidad puede ser un obstáculo para usuarios novatos. Por otro lado, ufw proporciona una interfaz más sencilla, orientada a usuarios que requieren rapidez y simplicidad. Este informe presenta una comparación técnica entre ambas herramientas mediante su configuración en Kali Linux, una distribución orientada a pruebas de penetración y análisis forense.

Método

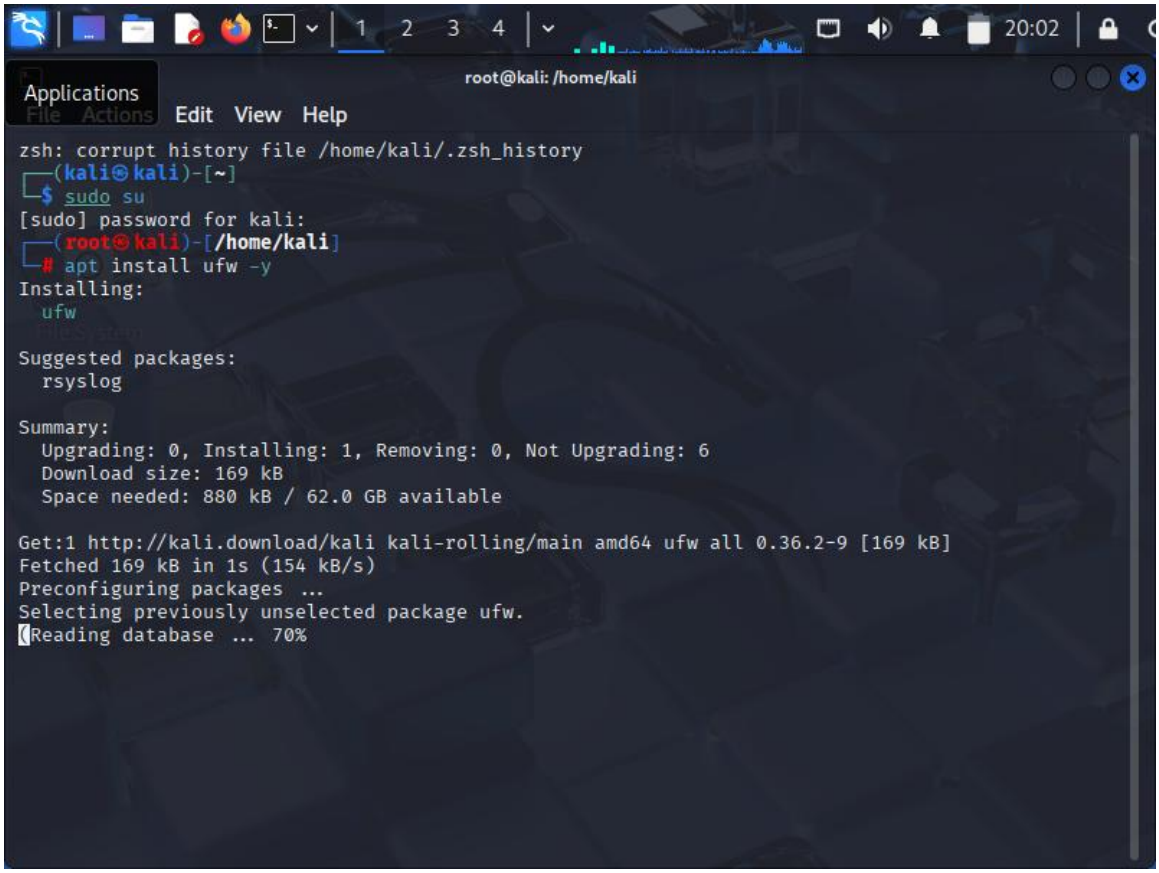
Herramientas Utilizadas:
- Sistema Operativo: Kali Linux (versión actual)
- Firewalls: iptables y ufw
- Terminal Bash

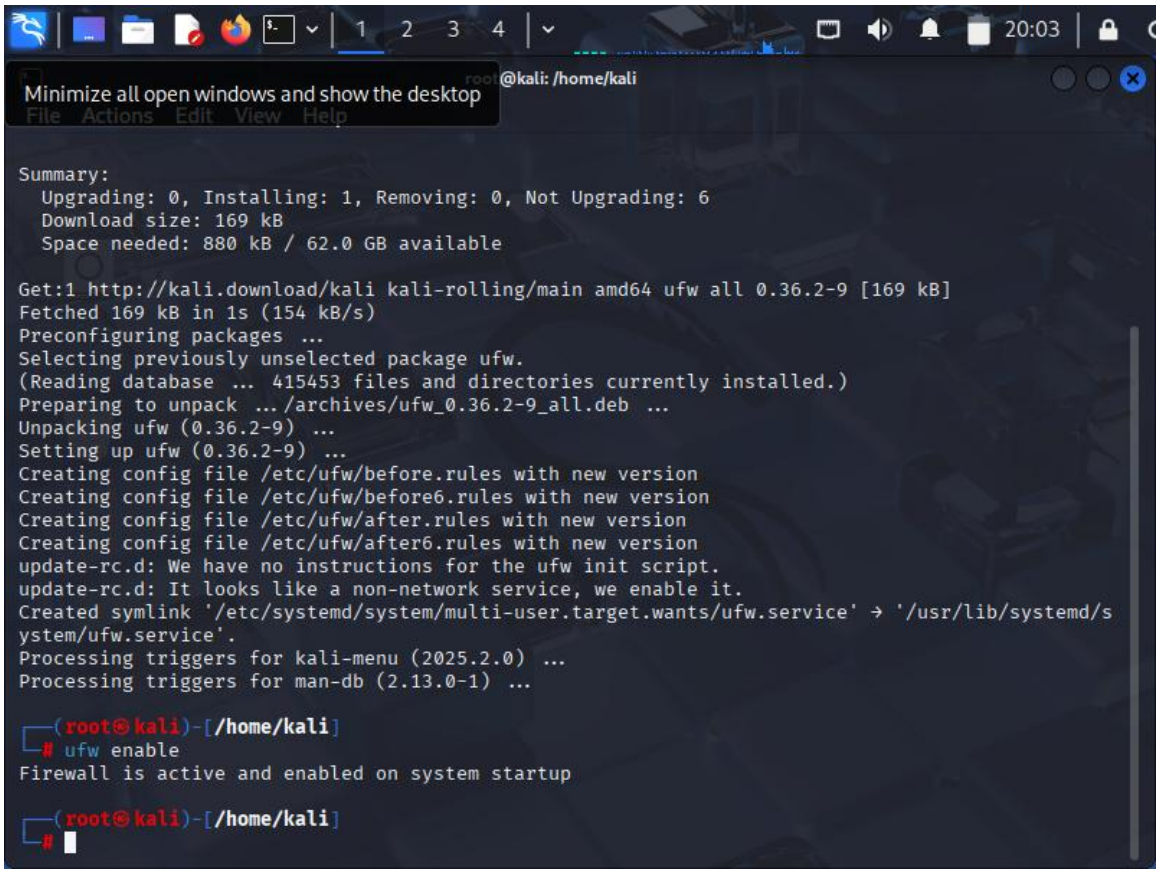
Comandos Ejecutados:

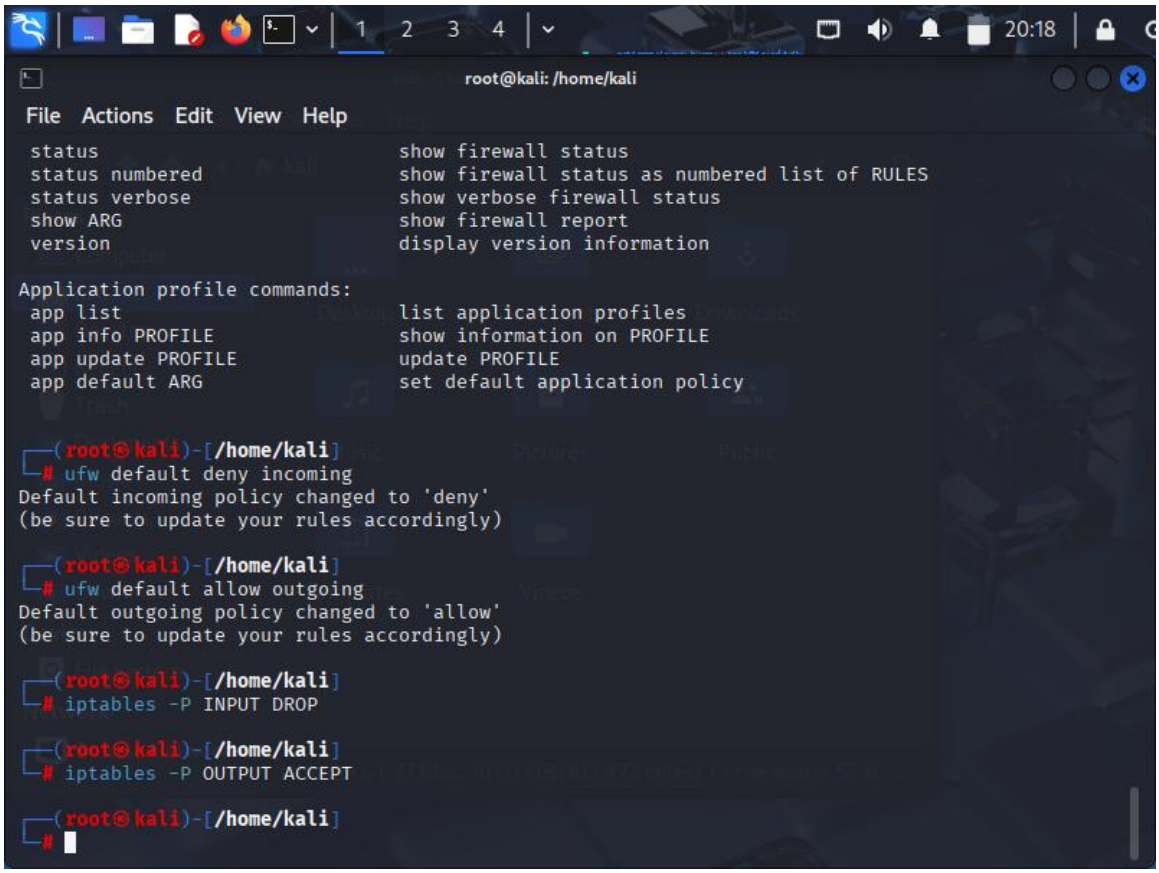
iptables:
sudo iptables -L
sudo iptables -A INPUT -p tcp --dport 22 -j DROP
sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo iptables -D INPUT 1
sudo iptables -F

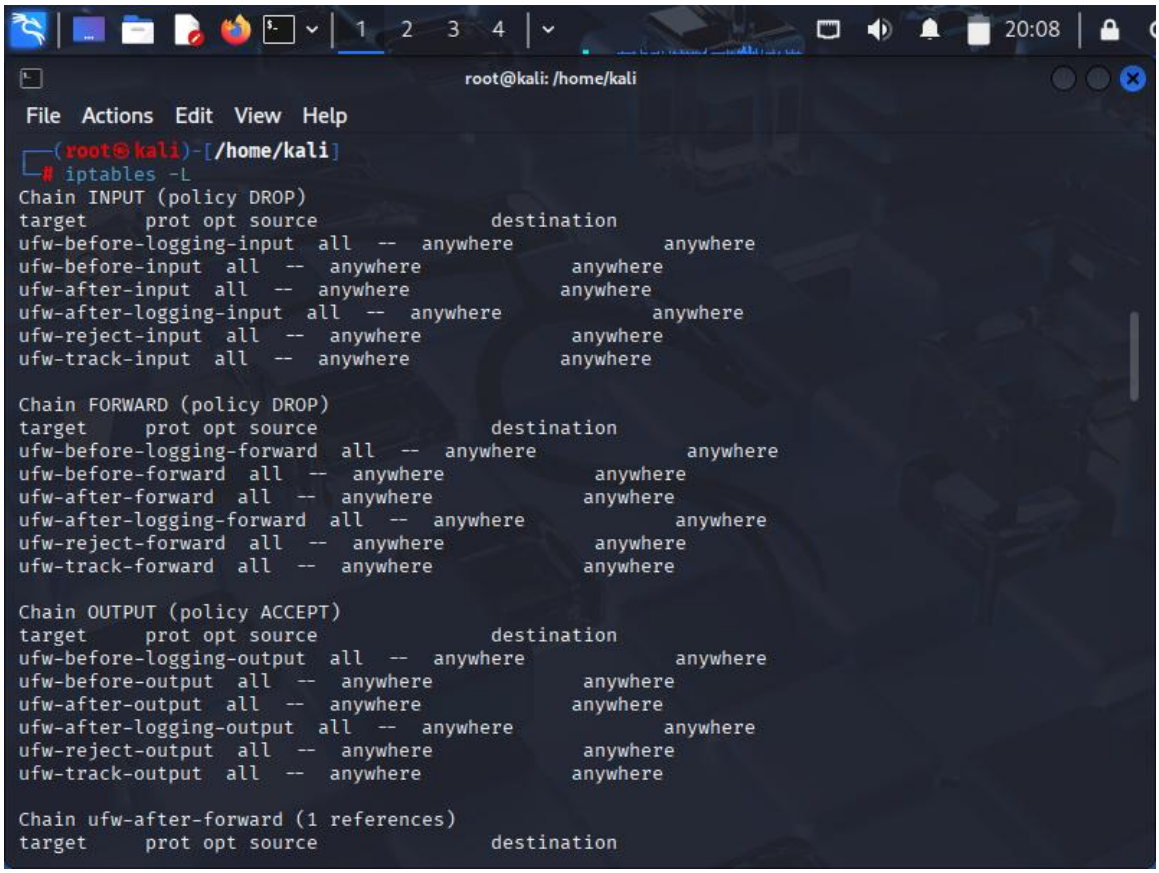
ufw:
sudo ufw status verbose
sudo ufw enable
sudo ufw allow 80/tcp
sudo ufw deny 22/tcp
sudo ufw delete allow 80/tcp
sudo ufw disable

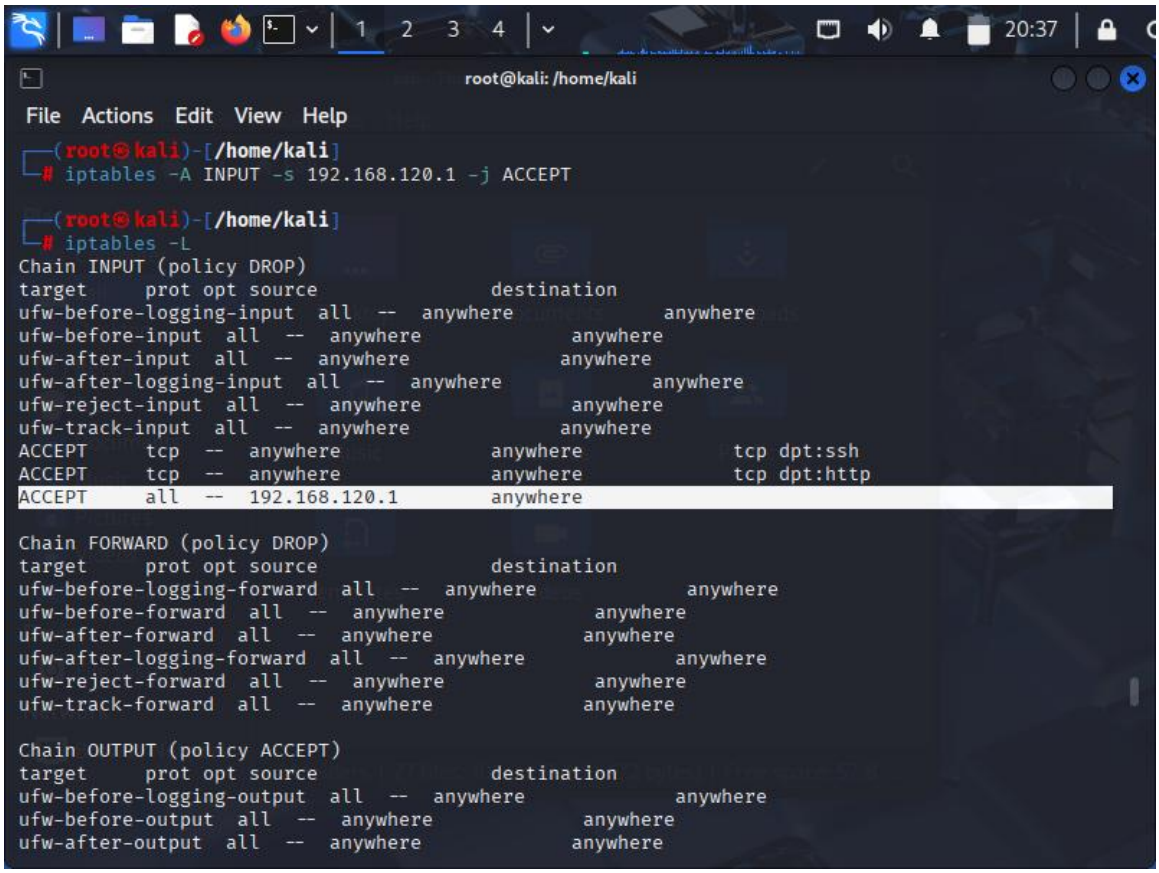
Resultados

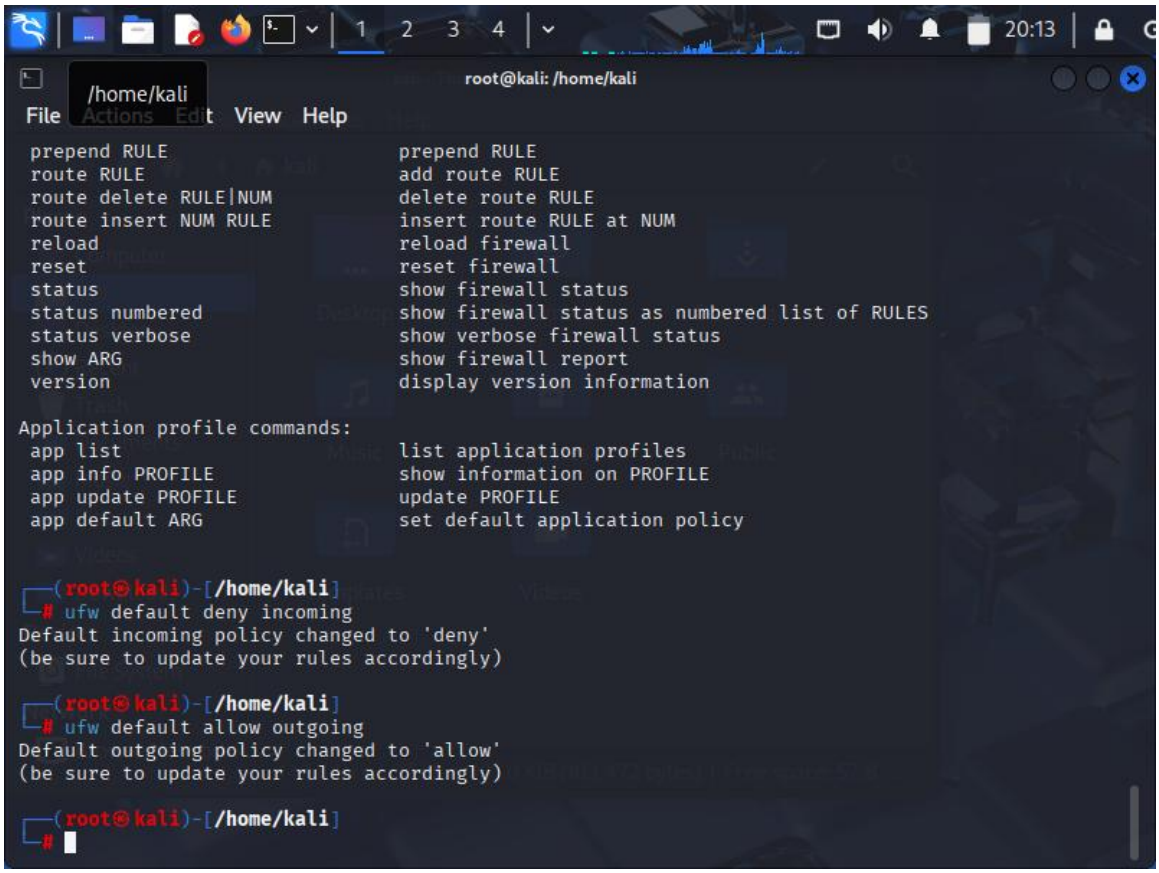

1 2 3 4
20:02
root@kali: /home/kali
Applications
Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
apt install ufw -y
Installing:
ufw
Suggested packages:
rsyslog
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 6
Download size: 169 kB
Space needed: 880 kB / 62.0 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (154 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 70%


1 2 3 4
20:03
Minimize all open windows and show the desktop
@kali: /home/kali
File Actions Edit View Help
Summary:
Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 6
Download size: 169 kB
Space needed: 880 kB / 62.0 GB available
Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169 kB]
Fetched 169 kB in 1s (154 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 415453 files and directories currently installed.)
Preparing to unpack .../archives/ufw_0.36.2-9_all.deb ...
Unpacking ufw (0.36.2-9) ...
Setting up ufw (0.36.2-9) ...
Creating config file /etc/ufw/before.rules with new version
Creating config file /etc/ufw/before6.rules with new version
Creating config file /etc/ufw/after.rules with new version
Creating config file /etc/ufw/after6.rules with new version
update-rc.d: We have no instructions for the ufw init script.
update-rc.d: It looks like a non-network service, we enable it.
Created symlink '/etc/systemd/system/multi-user.target.wants/ufw.service' → '/usr/lib/systemd/system/ufw.service'.
Processing triggers for kali-menu (2025.2.0) ...
Processing triggers for man-db (2.13.0-1) ...
┌──(root㉿kali)-[/home/kali]
└─# ufw enable
Firewall is active and enabled on system startup
┌──(root㉿kali)-[/home/kali]
└─#


1 2 3 4
20:18
root@kali: /home/kali
File Actions Edit View Help
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
┌──(root㉿kali)-[/home/kali]
└─# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
┌──(root㉿kali)-[/home/kali]
└─# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
┌──(root㉿kali)-[/home/kali]
└─# iptables -P INPUT DROP
┌──(root㉿kali)-[/home/kali]
└─# iptables -P OUTPUT ACCEPT
┌──(root㉿kali)-[/home/kali]
└─#


1 2 3 4
20:08
root@kali: /home/kali
File Actions Edit View Help
(root㉿kali)-[/home/kali]
iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ufw-before-logging-input all -- anywhere anywhere
ufw-before-input all -- anywhere anywhere
ufw-after-input all -- anywhere anywhere
ufw-after-logging-input all -- anywhere anywhere
ufw-reject-input all -- anywhere anywhere
ufw-track-input all -- anywhere anywhere
Chain FORWARD (policy DROP)
target prot opt source destination
ufw-before-logging-forward all -- anywhere anywhere
ufw-before-forward all -- anywhere anywhere
ufw-after-forward all -- anywhere anywhere
ufw-after-logging-forward all -- anywhere anywhere
ufw-reject-forward all -- anywhere anywhere
ufw-track-forward all -- anywhere anywhere
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ufw-before-logging-output all -- anywhere anywhere
ufw-before-output all -- anywhere anywhere
ufw-after-output all -- anywhere anywhere
ufw-after-logging-output all -- anywhere anywhere
ufw-reject-output all -- anywhere anywhere
ufw-track-output all -- anywhere anywhere
Chain ufw-after-forward (1 references)
target prot opt source destination


1 2 3 4
20:37
root@kali: /home/kali
File Actions Edit View Help
┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -s 192.168.120.1 -j ACCEPT
┌──(root㉿kali)-[/home/kali]
└─# iptables -L
Chain INPUT (policy DROP)
target prot opt source destination
ufw-before-logging-input all -- anywhere anywhere
ufw-before-input all -- anywhere anywhere
ufw-after-input all -- anywhere anywhere
ufw-after-logging-input all -- anywhere anywhere
ufw-reject-input all -- anywhere anywhere
ufw-track-input all -- anywhere anywhere
ACCEPT tcp -- anywhere anywhere tcp dpt:ssh
ACCEPT tcp -- anywhere anywhere tcp dpt:http
ACCEPT all -- 192.168.120.1 anywhere
Chain FORWARD (policy DROP)
target prot opt source destination
ufw-before-logging-forward all -- anywhere anywhere
ufw-before-forward all -- anywhere anywhere
ufw-after-forward all -- anywhere anywhere
ufw-after-logging-forward all -- anywhere anywhere
ufw-reject-forward all -- anywhere anywhere
ufw-track-forward all -- anywhere anywhere
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
ufw-before-logging-output all -- anywhere anywhere
ufw-before-output all -- anywhere anywhere
ufw-after-output all -- anywhere anywhere



Discusión

El análisis comparativo mostró que iptables es una herramienta poderosa, ideal para administradores de sistemas avanzados que requieren reglas personalizadas y detalladas. Sin embargo, su complejidad implica una mayor posibilidad de errores en la configuración, especialmente en ambientes dinámicos.

Por el contrario, ufw está diseñada para facilitar la gestión de reglas en entornos donde se requiere una configuración rápida y segura, sin necesidad de profundos conocimientos técnicos. Esto lo hace apropiado para estaciones de trabajo personales o servidores con necesidades básicas de filtrado.

Un aspecto relevante fue la persistencia: iptables no guarda las reglas tras reiniciar el sistema sin herramientas adicionales como iptables-persistent, mientras que ufw mantiene su configuración sin intervención adicional.

Conclusión

En entornos donde se prioriza el control granular y se cuenta con personal capacitado, iptables es la opción preferible. Para configuraciones más simples o cuando el tiempo es un factor crítico, ufw ofrece una alternativa eficaz y sencilla. En ambos casos, es fundamental probar las reglas cuidadosamente para evitar bloqueos no deseados.

Recomendación: Para usuarios principiantes o entornos de desarrollo, usar ufw. Para servidores en producción con políticas estrictas, preferir iptables acompañado de documentación adecuada.

Referencias

Netfilter Project. (s.f.). iptables - administration tool for IPv4 packet filtering and NAT. Recuperado de https://linux.die.net/man/8/iptables
Ubuntu Documentation. (s.f.). Uncomplicated Firewall (UFW). Recuperado de https://help.ubuntu.com/community/UFW
Nemeth, E., Snyder, G., Hein, T. R., Whaley, B., & Mackin, D. (2017). Unix and Linux System Administration Handbook (5th ed.). Pearson Education.

Criterio	iptables	UFW		
Complejidad	Alta	Baja		
Flexibilidad	Muy alta	Moderada		
Persistencia	No persistente por defecto	Persistente automáticamente		
Nivel de control	Avanzado	Básico a intermedio		
Curva de aprendizaje	Pronunciada	Suave		