

Laboratorio 7

Sesión #7 Configuración de un Firewall en un Entorno de Red

Título del Laboratorio: Configuración de un Firewall en un Entorno de Red

Duración: 2 hora

Objetivos del Laboratorio:

1. Implementar Políticas de Filtrado de Tráfico Entrante y Saliente
2. Configurar Reglas de Seguridad para Servicios Específicos
3. Monitorear y Ajustar la Configuración del Firewall

Materiales Necesarios:

1. Utilizar GitHub como repositorio
2. Utilizar Academia Cisco
3. Computador
4. Acceso a internet

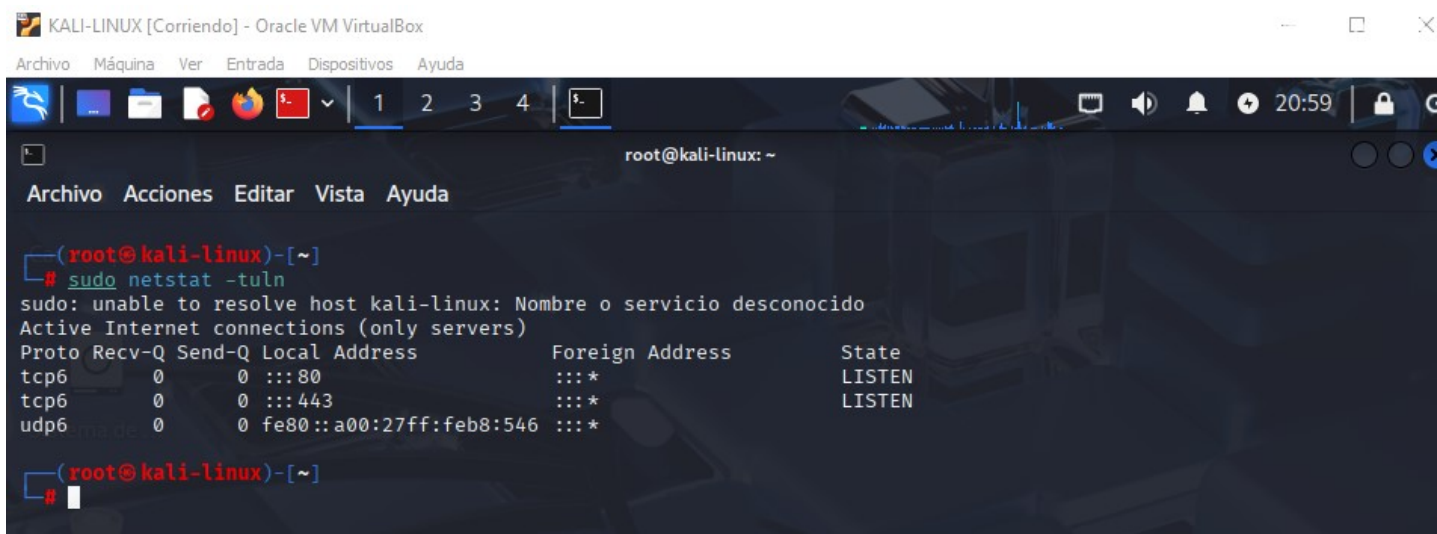
Estructura del Laboratorio:

Parte 1: Introducción al Firewall y Entorno de Configuración

- **Paso 1:** Revisión de la Configuración de Red Actual

R//

Con este comando muestra qué puertos están abiertos y qué servicios están escuchando en esos puertos

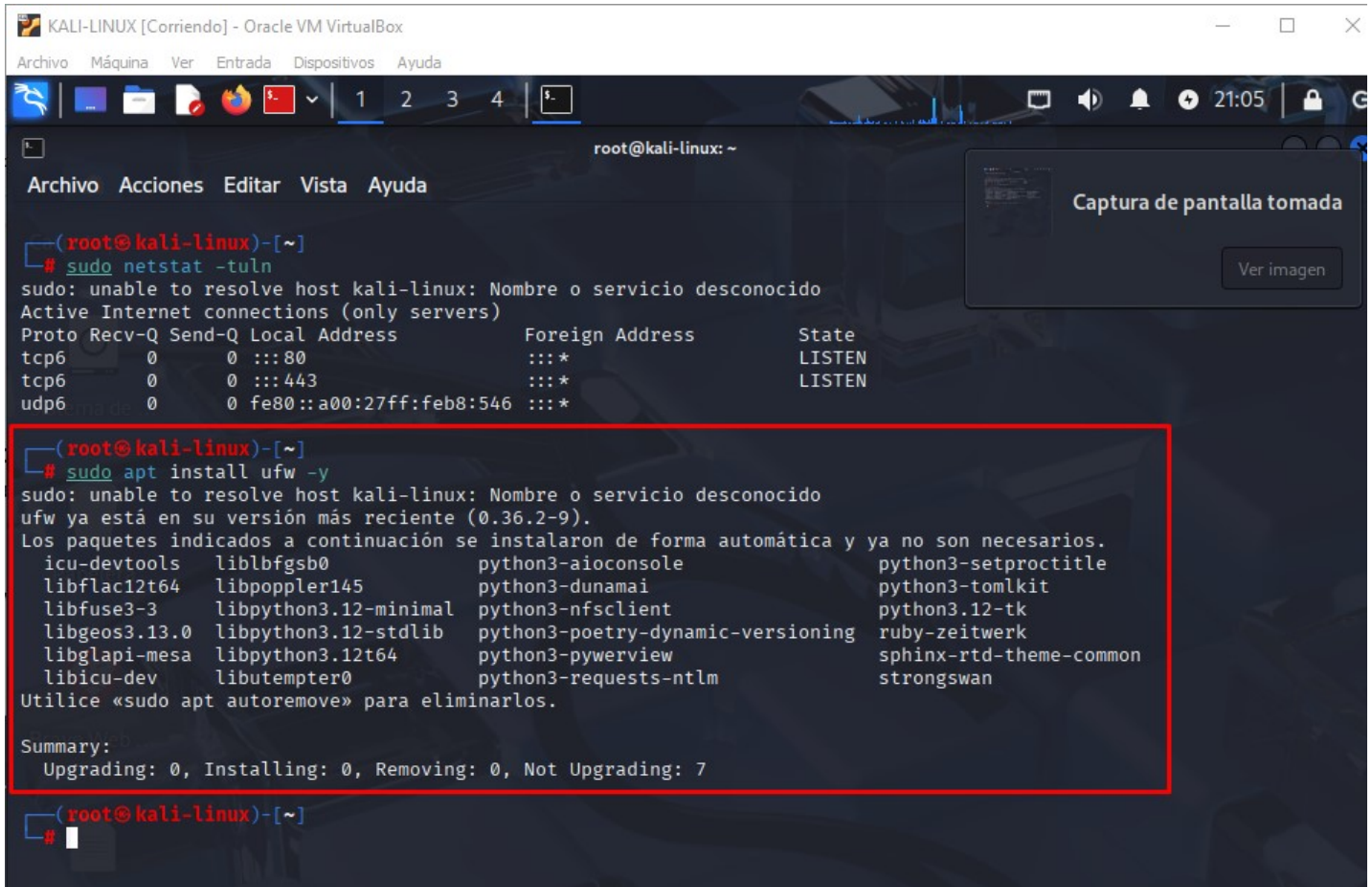


```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali-linux: ~
Archivo Acciones Editar Vista Ayuda
(root@kali-linux)-[~]
# sudo netstat -tuln
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6      0      0 :::80                  :::*                    LISTEN
tcp6      0      0 :::443                  :::*                    LISTEN
udp6      0      0 fe80::a00:27ff:feb8:546 :::*                    LISTEN
(root@kali-linux)-[~]
#
```

- Paso 2: Instalación y Verificación del Firewall

Con los comandos

- **sudo apt install ufw -y**
- **sudo ufw enable**
- **sudo ufw status**



The screenshot shows a terminal window titled 'KALI-LINUX [Corriendo] - Oracle VM VirtualBox'. The user is root. The first command is `sudo netstat -tuln`, which outputs a table of active internet connections. The second command is `sudo apt install ufw -y`, which outputs a message indicating that ufw is already installed and lists several packages that will be removed.

```
(root@kali-linux)-[~]
# sudo netstat -tuln
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp6      0      0 :::80                  :::*                    LISTEN
tcp6      0      0 :::443                  :::*                    LISTEN
udp6      0      0 fe80::a00:27ff:feb8:546 :::*

(root@kali-linux)-[~]
# sudo apt install ufw -y
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
ufw ya está en su versión más reciente (0.36.2-9).
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
icu-devtools      liblbfgsb0        python3-aioconsole  python3-setproctitle
libflac12t64      libpoppler145     python3-dunamai     python3-tomlkit
libfuse3-3        libpython3.12-minimal python3-nfsclient    python3.12-tk
libgeos3.13.0     libpython3.12-stdlib python3-poetry-dynamic-versioning ruby-zeitwerk
libglapi-mesa     libpython3.12t64  python3-pywebview   sphinx-rtd-theme-common
libicu-dev        libutempter0      python3-requests-ntlm strongswan
Utilice «sudo apt autoremove» para eliminarlos.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 7

(root@kali-linux)-[~]
#
```



The screenshot shows a terminal window titled 'KALI-LINUX [Corriendo] - Oracle VM VirtualBox'. The user is root. The command `sudo ufw enable` is executed, resulting in a message that the firewall is active and enabled on system startup.

```
(root@kali-linux)-[~]
# sudo ufw enable
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Firewall is active and enabled on system startup

(root@kali-linux)-[~]
#
```

- Verificación del Firewall

- **sudo ufw status**

```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4 5
root@kali-linux: ~

Archivo Acciones Editar Vista Ayuda

(root@kali-linux)-[~]
# sudo ufw status
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Status: active

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

(root@kali-linux)-[~]
#
```

Con este comando **Sudo iptables -L**, se puede ver el listado de la tabla de reglas del firewall

```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
1 2 3 4 5
root@kali-linux: ~

Archivo Acciones Editar Vista Ayuda

(root@kali-linux)-[~]
# sudo iptables -L
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
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

Chain ufw-after-input (1 references)
target prot opt source destination
ufw-skip-to-policy-input udp -- anywhere anywhere udp dpt:netbios-ns
ufw-skip-to-policy-input udp -- anywhere anywhere udp dpt:netbios-dgm
ufw-skip-to-policy-input tcp -- anywhere anywhere tcp dpt:netbios-ssn
ufw-skip-to-policy-input tcp -- anywhere anywhere tcp dpt:microsoft-ds
ufw-skip-to-policy-input udp -- anywhere anywhere udp dpt:bootps
ufw-skip-to-policy-input udp -- anywhere anywhere udp dpt:bootpc
ufw-skip-to-policy-input all -- anywhere anywhere ADDRTYPE match dst-type BROADCAST

Chain ufw-after-logging-forward (1 references)
target prot opt source destination
LOG all -- anywhere anywhere limit: avg 3/min burst 10 LOG level warn prefix "[UFW B
LOCK] "

Chain ufw-after-logging-input (1 references)
target prot opt source destination
```

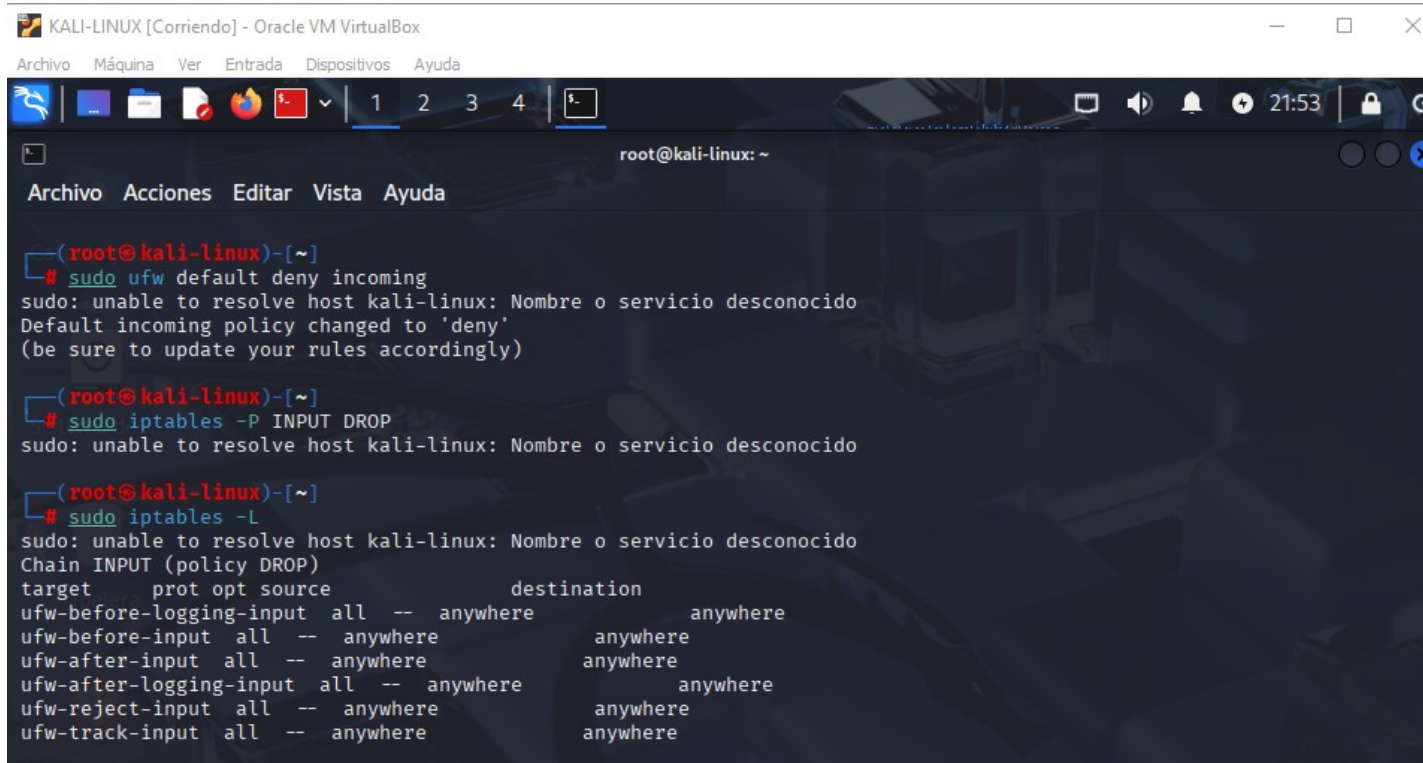

Parte 2: Configuración Básica del Firewall

- Paso 3: Configuración de Políticas por Defecto

R//

Con estos comandos nos ayudaran a configurar las políticas predeterminadas para el tráfico entrante y saliente.

- `sudo ufw default deny incoming` -> Para UFW
- `sudo iptables -P INPUT DROP` -> Para iptables

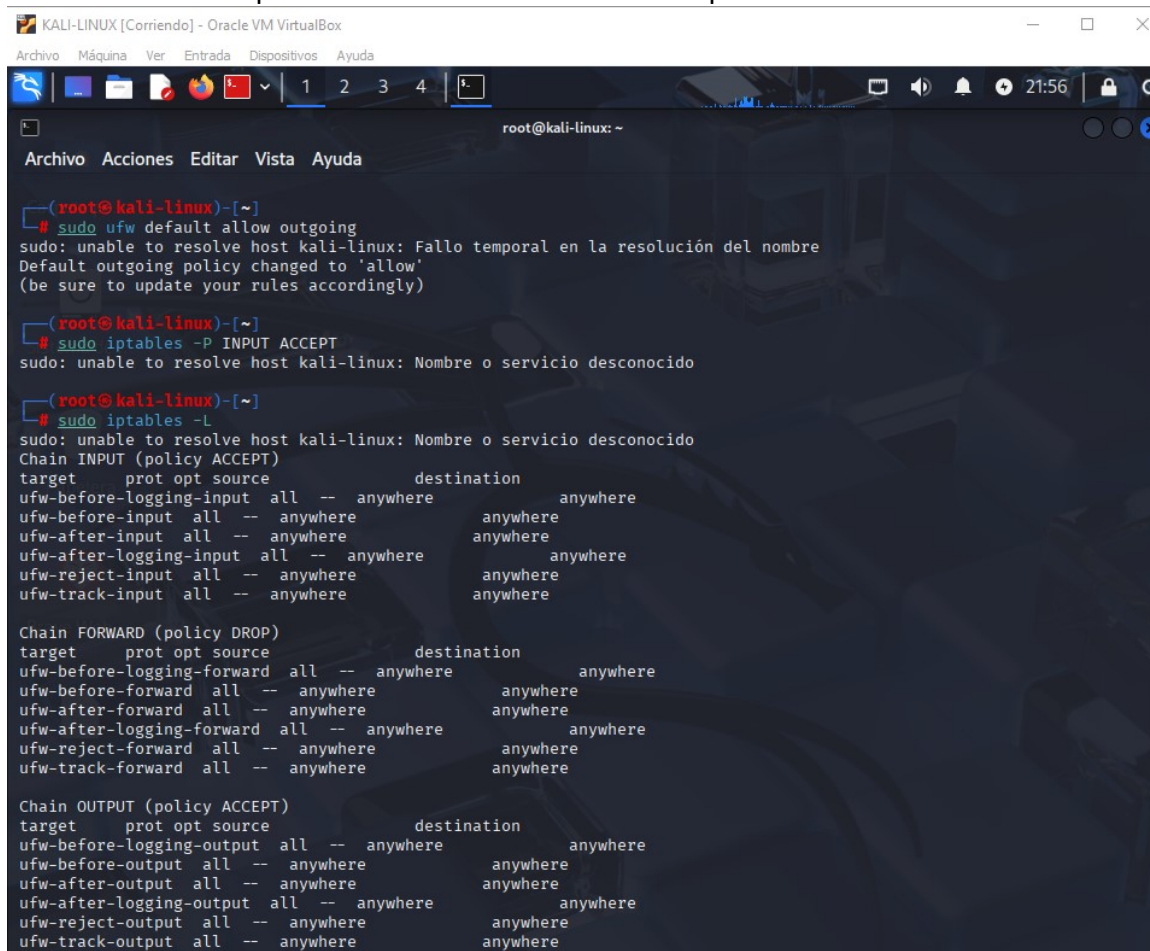


```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali-linux: ~
Archivo Acciones Editar Vista Ayuda
(root@kali-linux)-[~]
# sudo ufw default deny incoming
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)

(root@kali-linux)-[~]
# sudo iptables -P INPUT DROP
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido

(root@kali-linux)-[~]
# sudo iptables -L
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
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
```

- `sudo ufw default allow outgoing` -> Para UFW
- `sudo iptables -P INPUT ACCEPT` -> Para iptables



```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali-linux: ~
Archivo Acciones Editar Vista Ayuda
(root@kali-linux)-[~]
# sudo ufw default allow outgoing
sudo: unable to resolve host kali-linux: Fallo temporal en la resolución del nombre
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

(root@kali-linux)-[~]
# sudo iptables -P INPUT ACCEPT
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido

(root@kali-linux)-[~]
# sudo iptables -L
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Chain INPUT (policy ACCEPT)
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

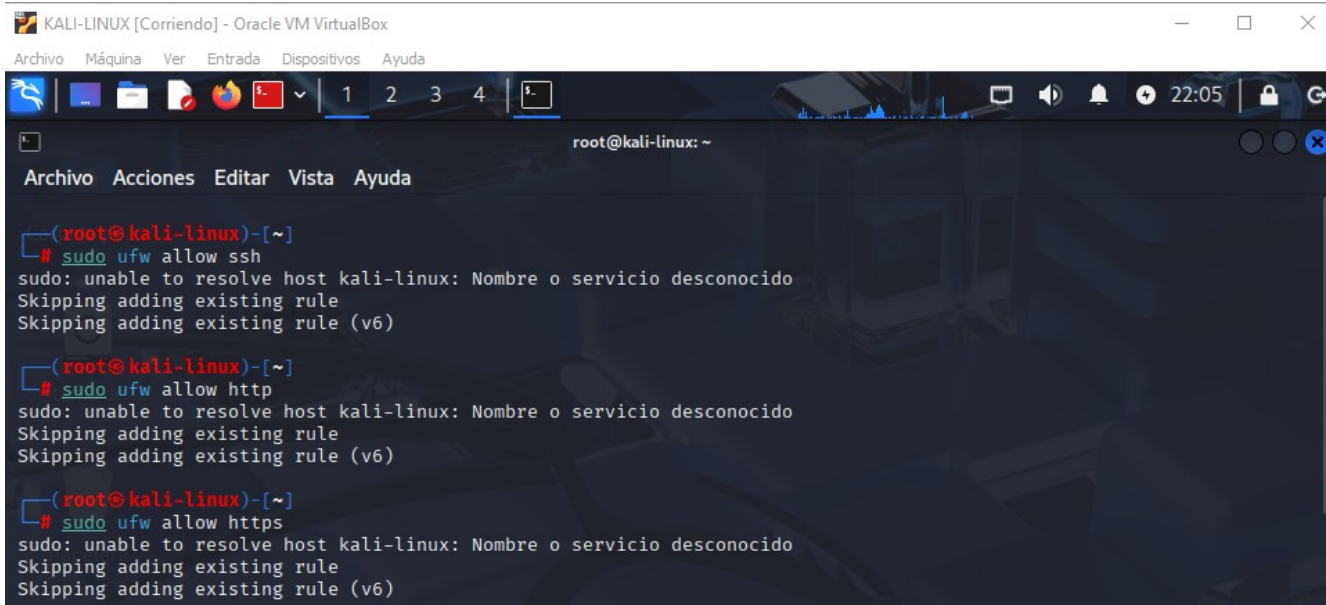
Chain FORWARD (policy DROP)
target prot opt source destination
ufw-before-logging-forward all -- anywhere anywhere
ufw-before-forward all -- anywhere anywhere
ufw-after-forward all -- anywhere anywhere
ufw-after-logging-forward all -- anywhere anywhere
ufw-reject-forward all -- anywhere anywhere
ufw-track-forward 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
```

- **Paso 4:** Permitir Tráfico para Servicios Específicos

configura reglas para permitir el tráfico de servicios esenciales, como HTTP/HTTPS para servidores web o SSH para acceso remoto.

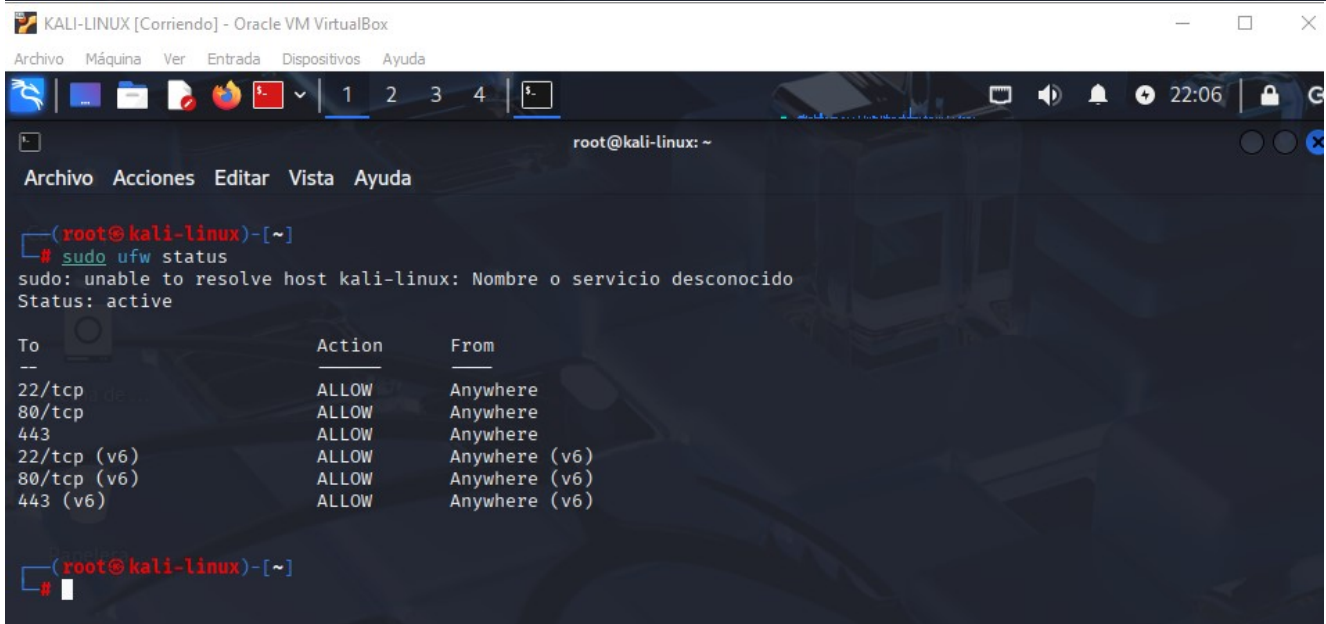
- `sudo ufw allow ssh` -> Para UFW
- `sudo ufw allow http` -> Para UFW
- `sudo ufw allow https` -> Para UFW



```
(root@kali-linux)-[~]
# sudo ufw allow ssh
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Skipping adding existing rule
Skipping adding existing rule (v6)

(root@kali-linux)-[~]
# sudo ufw allow http
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Skipping adding existing rule
Skipping adding existing rule (v6)

(root@kali-linux)-[~]
# sudo ufw allow https
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Skipping adding existing rule
Skipping adding existing rule (v6)
```



```
(root@kali-linux)-[~]
# sudo ufw status
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Status: active

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

(root@kali-linux)-[~]
#
```

- `sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT` -> Para iptables
- `sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT` -> Para iptables
- `sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT` -> Para iptables

```

(root@kali-linux)-[~]
# sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido

(root@kali-linux)-[~]
# sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido

(root@kali-linux)-[~]
# sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido

(root@kali-linux)-[~]
# sudo iptables -L
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Chain INPUT (policy ACCEPT)
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     tcp  --  anywhere                anywhere    tcp dpt:https

```

Parte 3: Configuración Avanzada del Firewall

- **Paso 5: Crear Reglas de Filtrado por IP**
R//

Con estos comandos nos ayudaran a configura reglas para permitir o denegar tráfico basado en direcciones IP específicas.

- **para denegar una IP específica:**

- `sudo ufw deny from 192.168.1.100` -> Para UFW
- `sudo iptables -A INPUT -s 192.168.1.100 -j DROP` -> Para iptables

```

(root@kali-linux)-[~]
# sudo ufw deny from 192.168.1.100
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Rule added

(root@kali-linux)-[~]
# sudo iptables -A INPUT -s 192.168.1.100 -j DROP
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido

(root@kali-linux)-[~]
# sudo ufw status
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Status: active

To Action From
--
22/tcp ALLOW Anywhere
80/tcp ALLOW Anywhere
443/tcp ALLOW Anywhere
Anywhere DENY 192.168.1.100
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
443 (v6) ALLOW Anywhere (v6)

(root@kali-linux)-[~]
# sudo iptables -L
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Chain INPUT (policy ACCEPT)
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     tcp  --  anywhere                anywhere    tcp dpt:https
DROP       all  --  192.168.1.100           anywhere

```


- para permitir una IP específica:

- sudo ufw allow from 192.168.1.100 -> Para UFW
- sudo iptables -A INPUT -s 192.168.1.100 -j ACCEPT -> Para iptables

```

KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

root@kali-linux: ~

Archivo Acciones Editar Vista Ayuda

(root@kali-linux)-[~]
# sudo ufw allow from 192.168.1.100
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Rule updated

(root@kali-linux)-[~]
# sudo iptables -A INPUT -s 192.168.1.100 -j ACCEPT
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido

(root@kali-linux)-[~]
# sudo ufw status
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Status: active

To Action From
--
22/tcp ALLOW Anywhere
80/tcp ALLOW Anywhere
443 ALLOW Anywhere
Anywhere ALLOW 192.168.1.100
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
443 (v6) ALLOW Anywhere (v6)

(root@kali-linux)-[~]
# sudo iptables -L
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Chain INPUT (policy ACCEPT)
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 tcp -- anywhere anywhere tcp dpt:https
ACCEPT tcp -- anywhere anywhere tcp dpt:https
DROP all -- 192.168.1.100 anywhere
ACCEPT all -- 192.168.1.100 anywhere
  
```

- Paso 6: Configuración de Reglas para Redes Internas y Externas

R//

Con estos comandos nos ayudaran a configuración de Reglas para Redes Internas

- sudo ufw allow from 192.168.1.0/24 -> Para UFW
- sudo iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT -> Para iptables

```

KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

root@kali-linux: ~

Archivo Acciones Editar Vista Ayuda

(root@kali-linux)-[~]
# sudo ufw allow from 192.168.1.0/24
sudo: unable to resolve host kali-linux: Fallo temporal en la resolución del nombre
Rule added

(root@kali-linux)-[~]
# sudo iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT
sudo: unable to resolve host kali-linux: Fallo temporal en la resolución del nombre

(root@kali-linux)-[~]
# sudo ufw status
sudo: unable to resolve host kali-linux: Fallo temporal en la resolución del nombre
Status: active

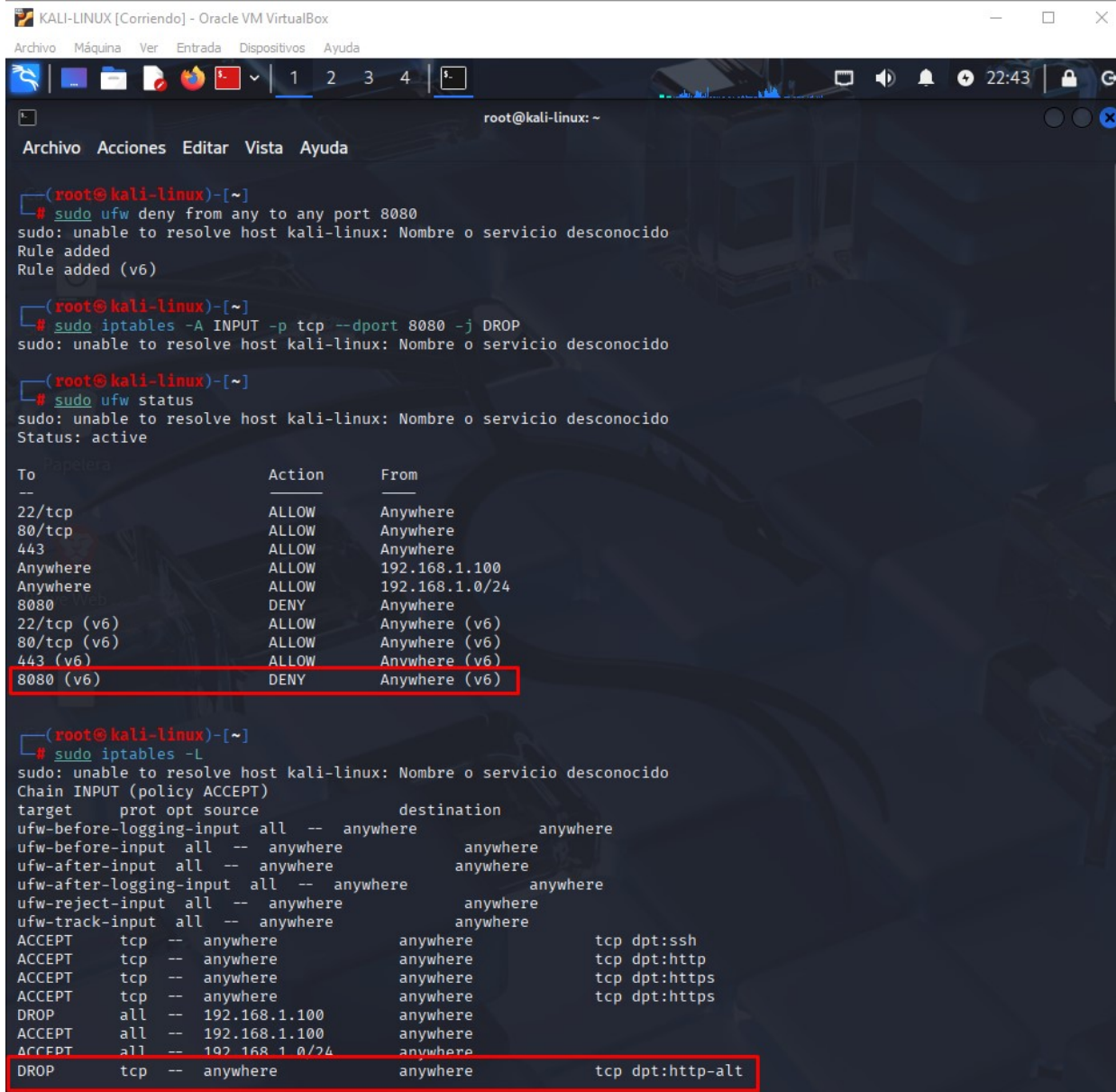
To Action From
--
22/tcp ALLOW Anywhere
80/tcp ALLOW Anywhere
443 ALLOW Anywhere
Anywhere ALLOW 192.168.1.100
Anywhere ALLOW 192.168.1.0/24
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
443 (v6) ALLOW Anywhere (v6)

(root@kali-linux)-[~]
# sudo iptables -L
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Chain INPUT (policy ACCEPT)
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 tcp -- anywhere anywhere tcp dpt:https
ACCEPT tcp -- anywhere anywhere tcp dpt:https
DROP all -- 192.168.1.100 anywhere
ACCEPT all -- 192.168.1.100 anywhere
ACCEPT all -- 192.168.1.0/24 anywhere
  
```

R//

Con estos comandos nos ayudaran a configuración de Reglas para Redes Externas

- `sudo ufw deny from any to any port 8080` -> Para UFW
- `sudo iptables -A INPUT -p tcp --dport 8080 -j DROP` -> Para iptables



```
(root@kali-linux)-[~]
# sudo ufw deny from any to any port 8080
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Rule added
Rule added (v6)

(root@kali-linux)-[~]
# sudo iptables -A INPUT -p tcp --dport 8080 -j DROP
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido

(root@kali-linux)-[~]
# sudo ufw status
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Status: active

To: 22/tcp, 80/tcp, 443, Anywhere, Anywhere, 8080, 22/tcp (v6), 80/tcp (v6), 443 (v6), 8080 (v6)
Action: ALLOW, ALLOW, ALLOW, ALLOW, ALLOW, DENY, ALLOW, ALLOW, ALLOW, DENY
From: Anywhere, Anywhere, Anywhere, 192.168.1.100, 192.168.1.0/24, Anywhere, Anywhere (v6), Anywhere (v6), Anywhere (v6), Anywhere (v6)

(root@kali-linux)-[~]
# sudo iptables -L
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Chain INPUT (policy ACCEPT)
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 tcp -- anywhere anywhere tcp dpt:https
ACCEPT tcp -- anywhere anywhere tcp dpt:https
DROP all -- 192.168.1.100 anywhere
ACCEPT all -- 192.168.1.100 anywhere
ACCEPT all -- 192.168.1.0/24 anywhere
DROP tcp -- anywhere anywhere tcp dpt:http-alt
```

Parte 4: Monitoreo y Ajustes del Firewall

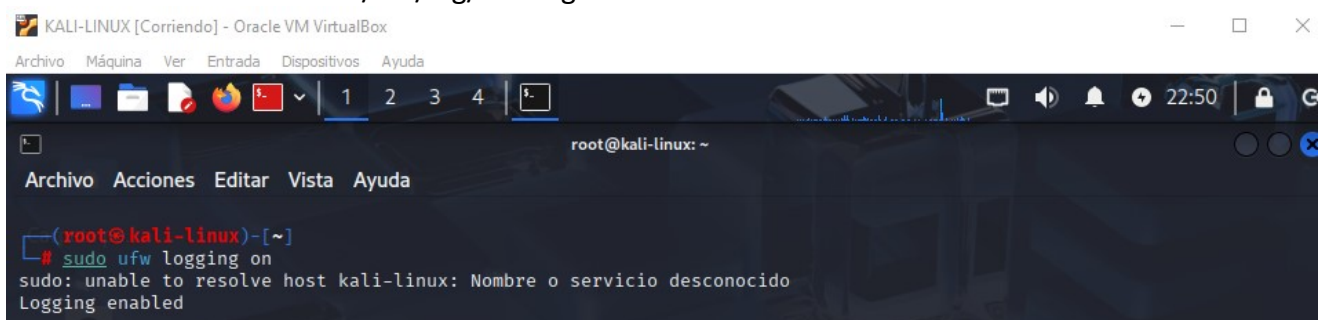
- **Paso 7: Monitoreo de Logs del Firewall**

R//

Con estos comandos nos ayuda Habilitar el registro de los intentos de acceso denegados y revisar los logs.

Para UFW:

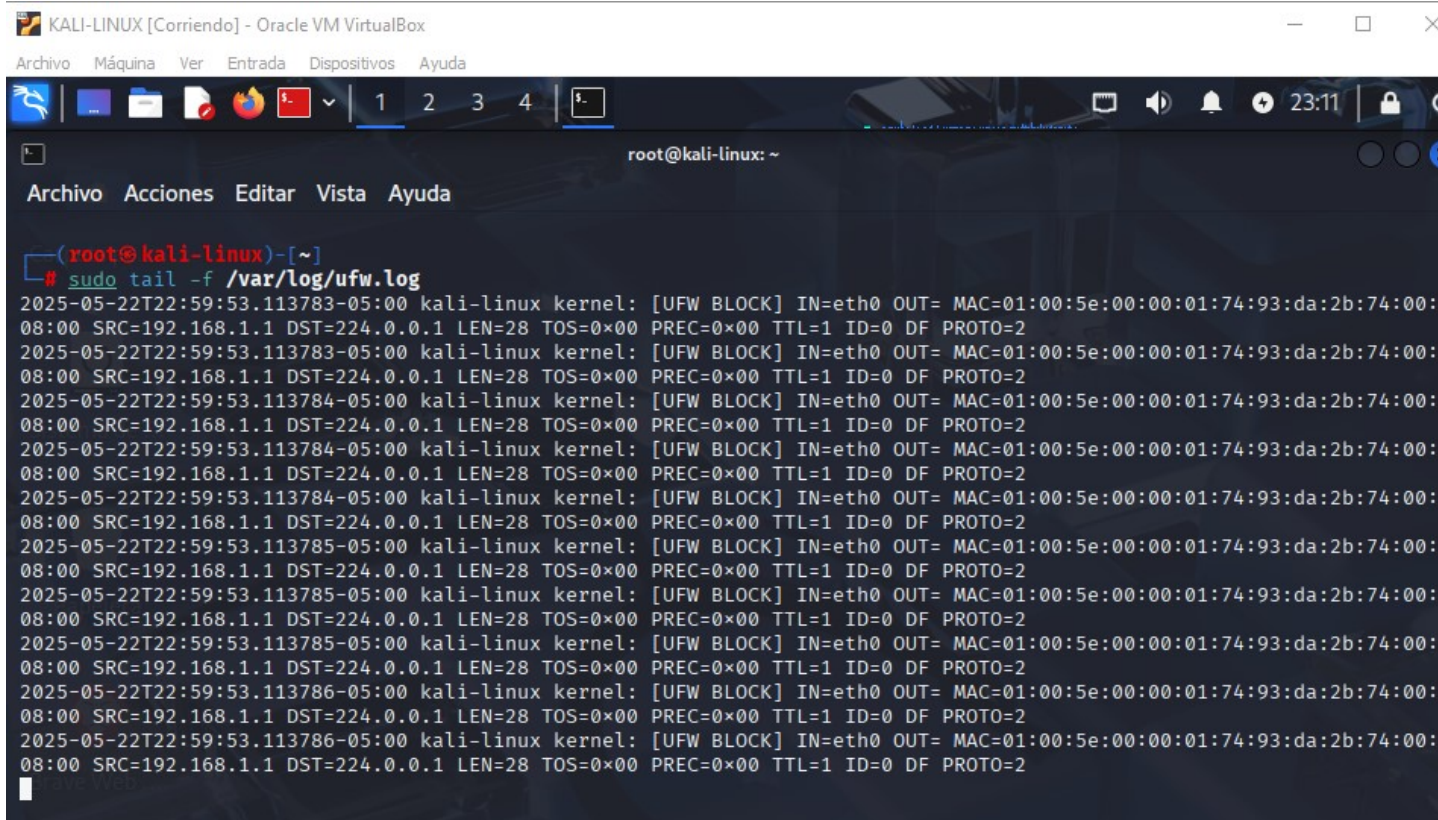
- `sudo ufw logging on`
- `sudo tail -f /var/log/ufw.log`



```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

root@kali-linux: ~

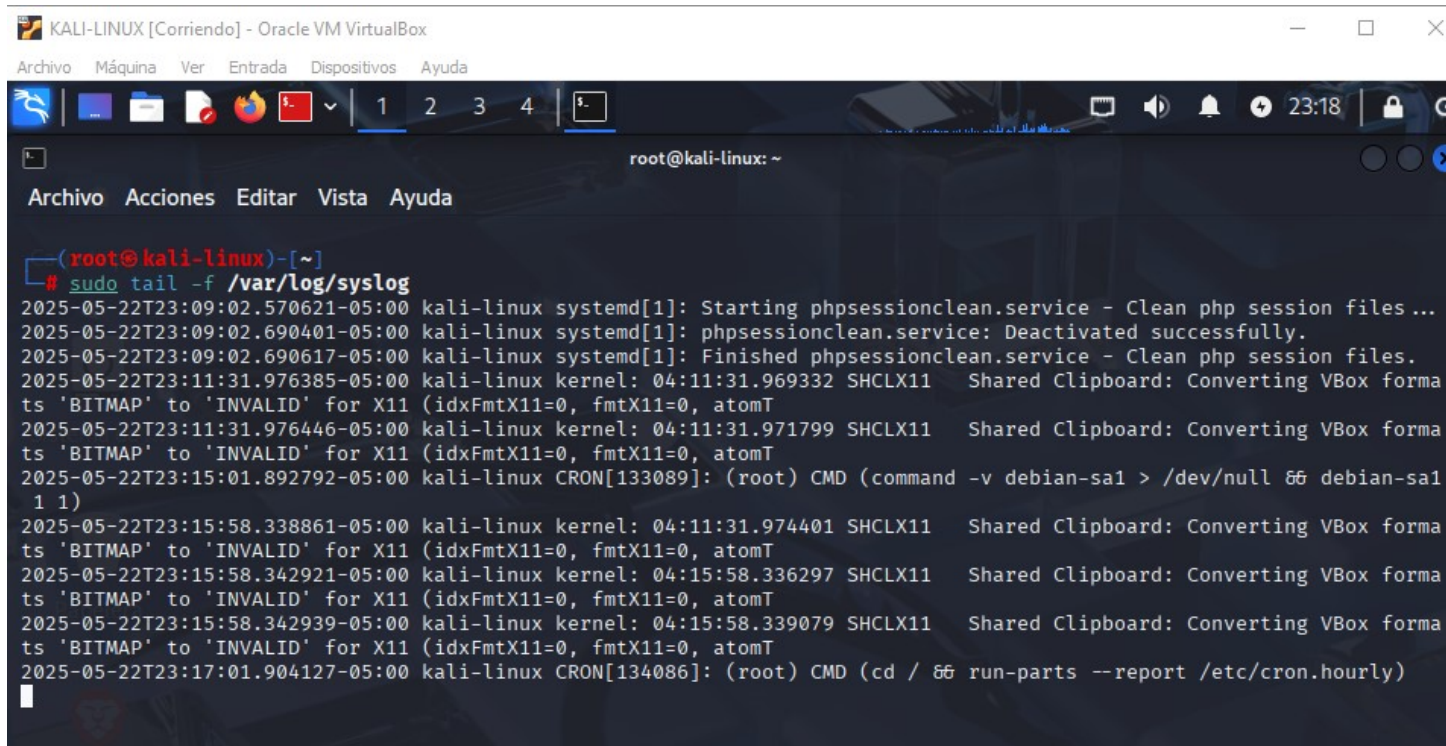
(root@kali-linux)-[~]
# sudo ufw logging on
sudo: unable to resolve host kali-linux: Nombre o servicio desconocido
Logging enabled
```

```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali-linux: ~
Archivo Acciones Editar Vista Ayuda
(root@kali-linux)-[~]
# sudo tail -f /var/log/ufw.log
2025-05-22T22:59:53.113783-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113783-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113784-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113784-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113784-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113784-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113785-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113785-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113785-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113785-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113786-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113786-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113786-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:
08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
```

Para iptables:

- sudo iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped: " --log-level
- sudo tail -f /var/log/syslog



```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali-linux: ~
Archivo Acciones Editar Vista Ayuda
(root@kali-linux)-[~]
# sudo tail -f /var/log/syslog
2025-05-22T23:09:02.570621-05:00 kali-linux systemd[1]: Starting phpsessionclean.service - Clean php session files ...
2025-05-22T23:09:02.690401-05:00 kali-linux systemd[1]: phpsessionclean.service: Deactivated successfully.
2025-05-22T23:09:02.690617-05:00 kali-linux systemd[1]: Finished phpsessionclean.service - Clean php session files.
2025-05-22T23:11:31.976385-05:00 kali-linux kernel: 04:11:31.969332 SHCLX11 Shared Clipboard: Converting VBox forma
ts 'BITMAP' to 'INVALID' for X11 (idxFmtX11=0, fmtX11=0, atomT
2025-05-22T23:11:31.976446-05:00 kali-linux kernel: 04:11:31.971799 SHCLX11 Shared Clipboard: Converting VBox forma
ts 'BITMAP' to 'INVALID' for X11 (idxFmtX11=0, fmtX11=0, atomT
2025-05-22T23:15:01.892792-05:00 kali-linux CRON[133089]: (root) CMD (command -v debian-sa1 > /dev/null && debian-sa1
1 1)
2025-05-22T23:15:58.338861-05:00 kali-linux kernel: 04:11:31.974401 SHCLX11 Shared Clipboard: Converting VBox forma
ts 'BITMAP' to 'INVALID' for X11 (idxFmtX11=0, fmtX11=0, atomT
2025-05-22T23:15:58.342921-05:00 kali-linux kernel: 04:15:58.336297 SHCLX11 Shared Clipboard: Converting VBox forma
ts 'BITMAP' to 'INVALID' for X11 (idxFmtX11=0, fmtX11=0, atomT
2025-05-22T23:15:58.342939-05:00 kali-linux kernel: 04:15:58.339079 SHCLX11 Shared Clipboard: Converting VBox forma
ts 'BITMAP' to 'INVALID' for X11 (idxFmtX11=0, fmtX11=0, atomT
2025-05-22T23:17:01.904127-05:00 kali-linux CRON[134086]: (root) CMD (cd / && run-parts --report /etc/cron.hourly)
```


- Paso 8: Ajuste de Reglas Basado en Monitoreo

- Para ips de virtualBox detectado en logs anterior permiten los accesos y se agregan otros puerto adicionales para bloqueo

```
KALI-LINUX [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
root@kali-linux: ~
# sudo systemctl restart rsyslog
# sudo ufw status
Status: active

To Action From
--
22/tcp ALLOW Anywhere
80/tcp ALLOW Anywhere
443 ALLOW Anywhere
Anywhere ALLOW 192.168.1.100
Anywhere ALLOW 192.168.1.0/24
8080 DENY Anywhere
Anywhere ALLOW 192.168.56.0/24
Anywhere ALLOW 10.0.2.0/24
23 DENY Anywhere
135 DENY Anywhere
139 DENY Anywhere
445 DENY Anywhere
1433 DENY Anywhere
3389 DENY Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
443 (v6) ALLOW Anywhere (v6)
8080 (v6) DENY Anywhere (v6)
23 (v6) DENY Anywhere (v6)
135 (v6) DENY Anywhere (v6)
139 (v6) DENY Anywhere (v6)
445 (v6) DENY Anywhere (v6)
1433 (v6) DENY Anywhere (v6)
3389 (v6) DENY Anywhere (v6)

# sudo tail -f /var/log/ufw.log
2025-05-22T22:59:53.113783-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113783-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113784-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113784-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113784-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113785-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113785-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113785-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
2025-05-22T22:59:53.113786-05:00 kali-linux kernel: [UFW BLOCK] IN=eth0 OUT= MAC=01:00:5e:00:00:01:74:93:da:2b:74:00:08:00 SRC=192.168.1.1 DST=224.0.0.1 LEN=28 TOS=0x00 PREC=0x00 TTL=1 ID=0 DF PROTO=2
```

