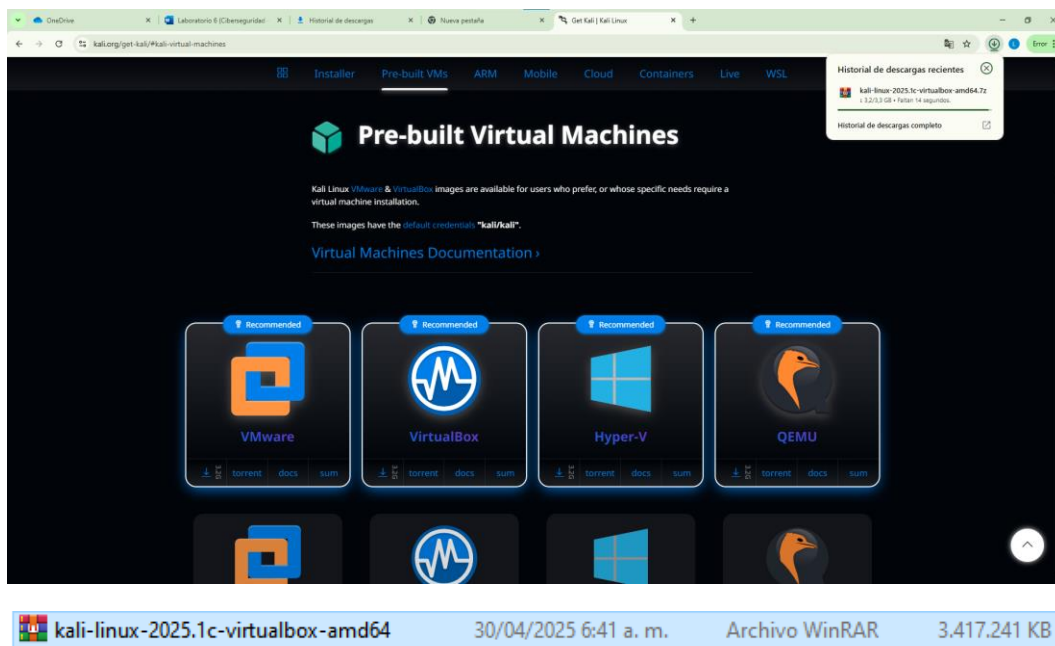
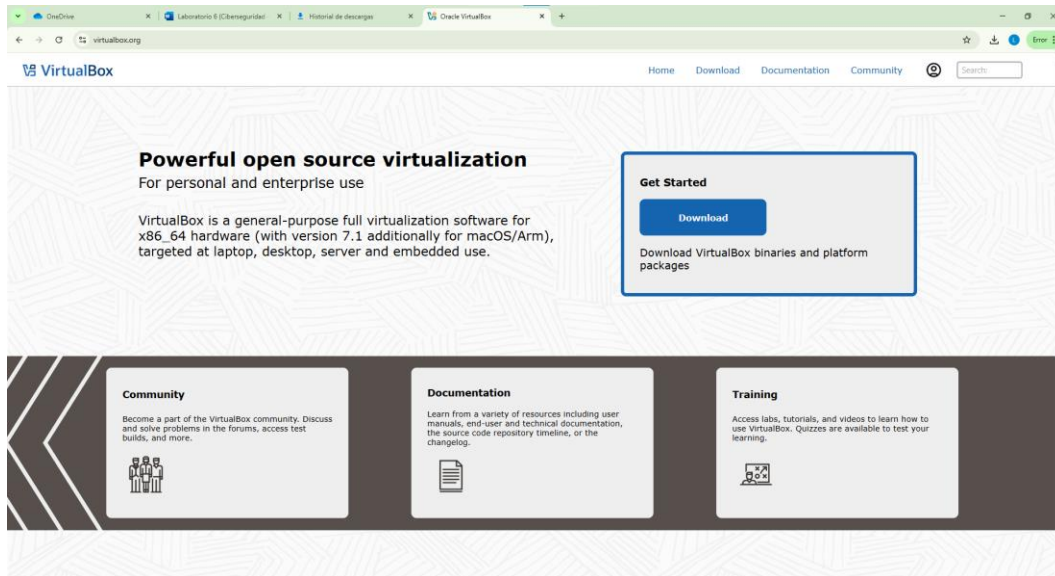
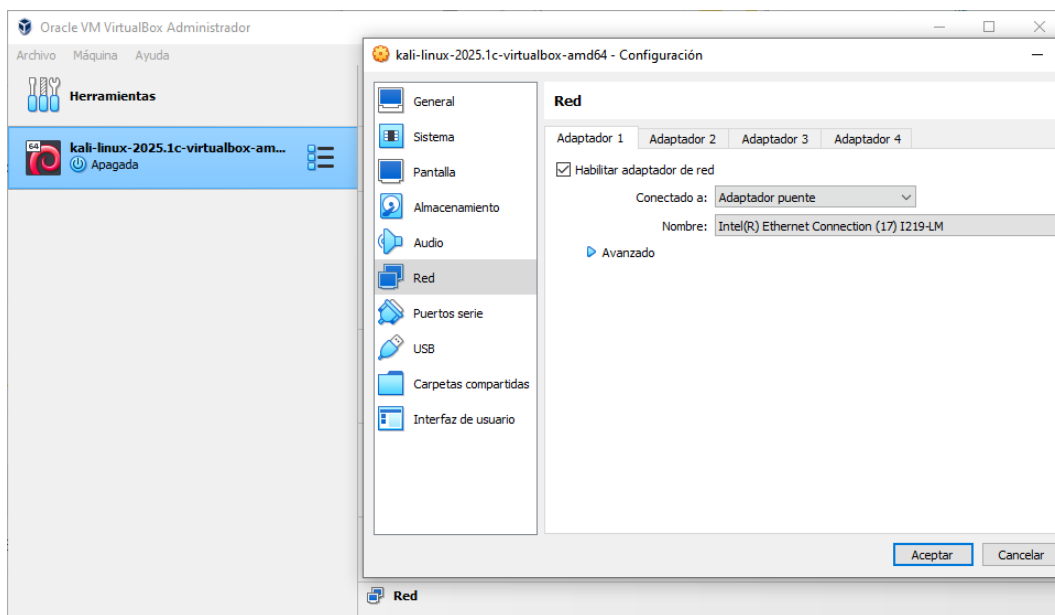
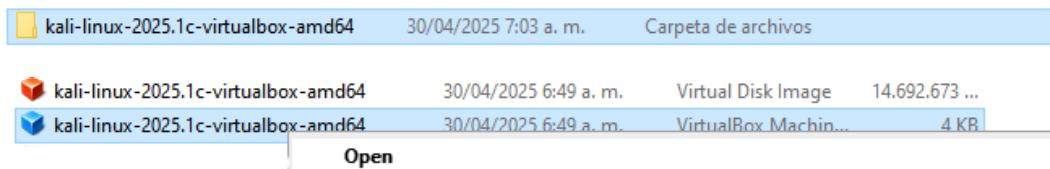
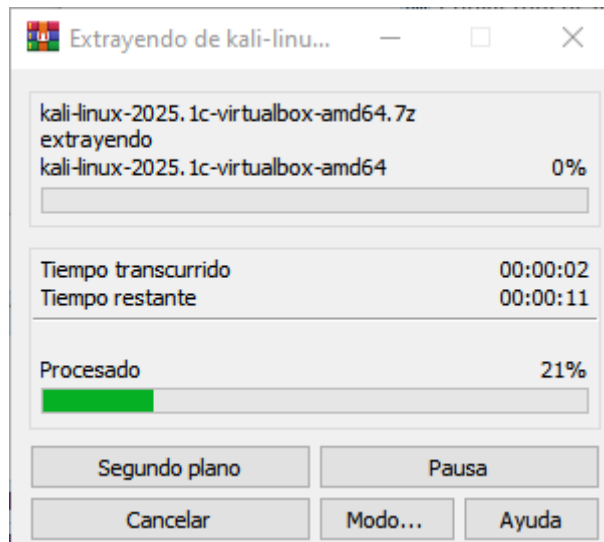
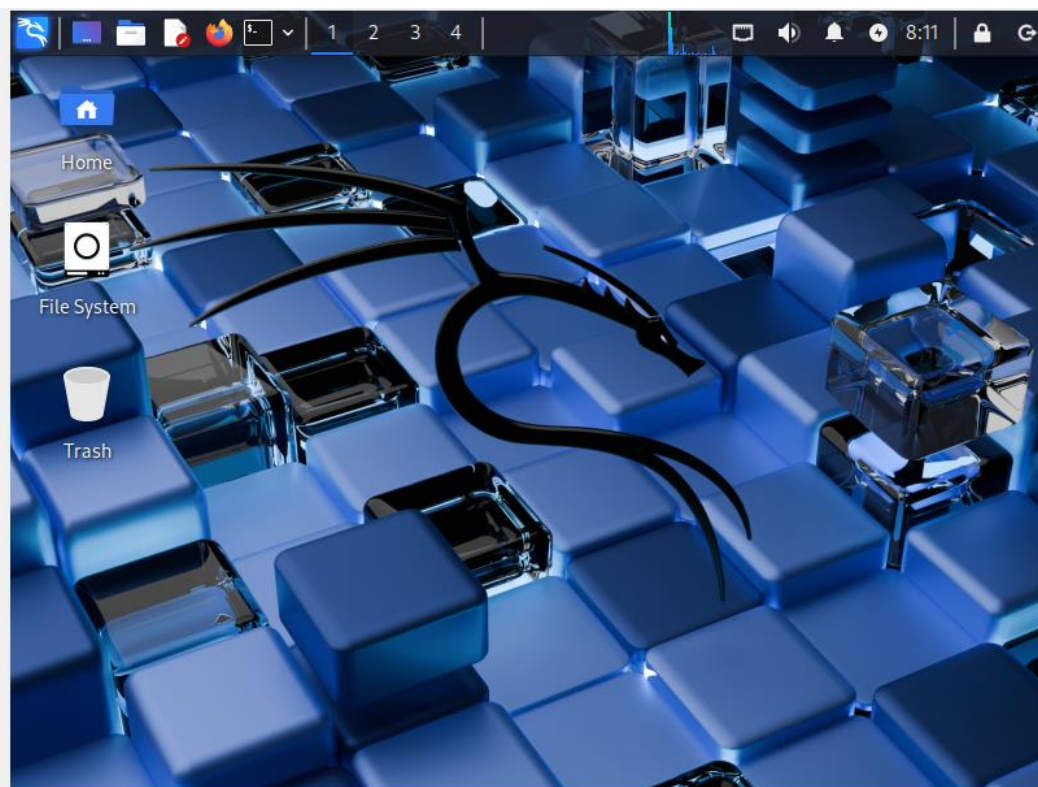
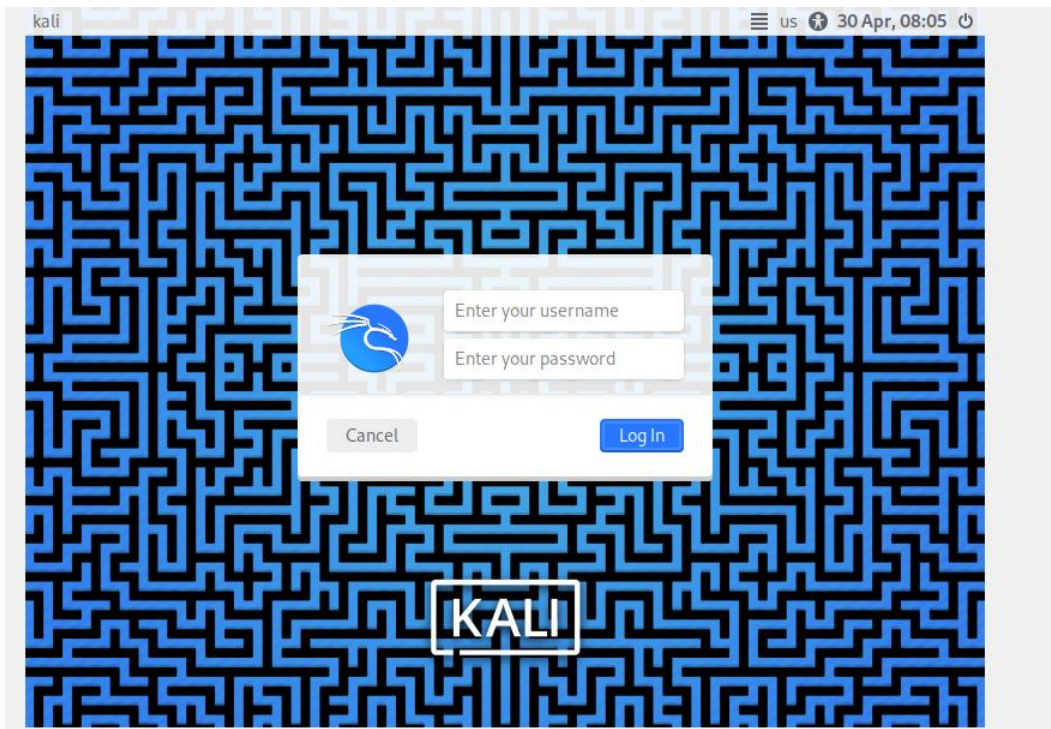


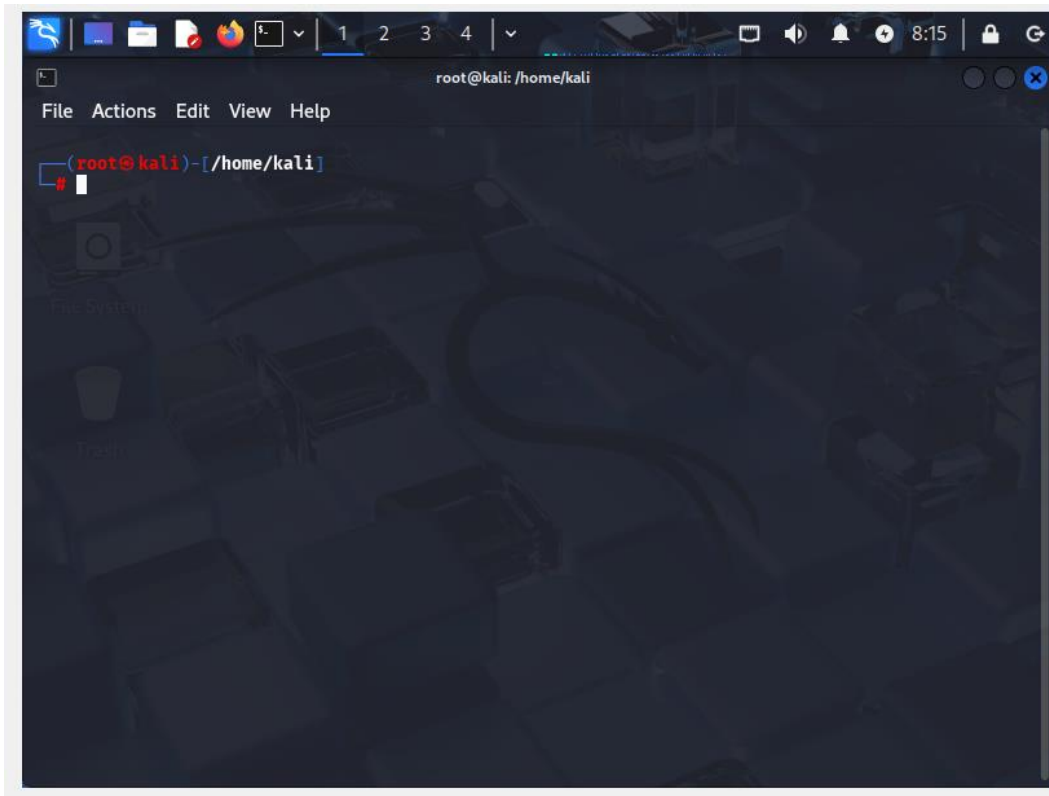
Laboratorio 6: Configuración de Firewall en un Entorno de Red







Entramos a la terminal e ingresamos a la cuenta **root** con **sudo su**



Observamos la Ip de kali y de Windows:

```
(root@kali)~/home/kali$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.1.30  netmask 255.255.255.0  broadcast 192.168.1.255
    inet6 fe80::c146:4eb7:b234:8ed4  prefixlen 64  scopeid 0x20<link>
    ether 08:00:27:b4:a1:05  txqueuelen 1000  (Ethernet)
    RX packets 335  bytes 129567 (126.5 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 135  bytes 69076 (67.4 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1000  (Local Loopback)
    RX packets 28  bytes 1680 (1.6 KiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 28  bytes 1680 (1.6 KiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

Windows: [


```
C:\Users\Administrador>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet 2:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::a195:d468:f31b:95f6%13
    Dirección IPv4. . . . . : 192.168.1.22
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.1.1
```

]

```
(root@kali)-[/home/kali]
# netstat -tuln
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
```

Proceso de instalación de UFW (Uncomplicated Firewall)

```
(root@kali)-[/home/kali]
# apt update
Get:1 http://kali.download/kali kali-rolling InRelease [41.5 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [21.0 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.6 MB]
Ign:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb)
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [121 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [328 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [204 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [914 kB]
Get:8 http://kali.download/kali kali-rolling/non-free-firmware amd64 Packages [10.6 kB]
Get:9 http://kali.download/kali kali-rolling/non-free-firmware amd64 Contents (deb) [24.3 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [51.6 MB]
Fetched 71.0 MB in 23s (3,078 kB/s)
1073 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

```
(root@kali)-[/home/kali]
# apt install ufw -y
Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 1073
  Download size: 169 kB
  Space needed: 880 kB / 63.9 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 (191 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 408445 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 (2025.1.1) ...
Processing triggers for man-db (2.13.0-1) ...
```

Habilitamos UFW:

```
(root@kali)-[/home/kali]
# ufw enable
Firewall is active and enabled on system startup
```

Revisamos el estatus del Firewall:

```
(root@kali)-[/home/kali]
# ufw status
Status: active
```

Ejecutamos el siguiente comando **iptables -L**:

```
(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

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
```

Configuramos políticas para entradas y salidas en UFW y Iptables:

UFW:

```
(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)
```

Iptables:

```
(root@kali)-[/home/kali]
# iptables -P INPUT DROP
```

```
(root@kali)-[/home/kali]
# iptables -P OUTPUT ACCEP
iptables: Bad policy name. Run `dmesg' for more information.
```

```
(root@kali)-[/home/kali]
# iptables -P OUTPUT ACCEPT

(root@kali)-[/home/kali]
```

UFW:

```
(root@kali)-[/home/kali]
# ufw allow ssh
Rule added
Rule added (v6)
```

```
(root@kali)-[/home/kali]
#
```

```
(root@kali)-[/home/kali]
# ufw allow http
Rule added
Rule added (v6)
```

```
(root@kali)-[/home/kali]
# ufw allow https
Rule added
Rule added (v6)
```

Iptables:

```
(root@kali)-[/home/kali]
# iptables -A INPUT -p tcp --dport 22 -j ACCEPT
```

```
(root@kali)-[/home/kali]
# iptables -A INPUT -p tcp --dport 80 -j ACCEPT
```

```
(root@kali)-[/home/kali]
# iptables -A INPUT -p tcp --dport 443 -j ACCEPT
```

Acabando de configurar los permisos revisamos en los firewalls los resultados de los comandos ejecutados:

UFW:

```
(root@kali)-[/home/kali]
# ufw status numbered
Status: active
```

	To	Action	From
[1]	22/tcp	ALLOW IN	Anywhere
[2]	80/tcp	ALLOW IN	Anywhere
[3]	443	ALLOW IN	Anywhere
[4]	22/tcp (v6)	ALLOW IN	Anywhere (v6)
[5]	80/tcp (v6)	ALLOW IN	Anywhere (v6)
[6]	443 (v6)	ALLOW IN	Anywhere (v6)

Iptables:

```
(root@kali)-[/home/kali]
# iptables -L
```

```
Chain ufw-user-input (1 references)
target     prot opt source                destination           tcp dpt:ssh
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:http
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:https
```

Luego, bloqueamos o permitimos tráfico desde una dirección específica:

Permisos en UFW:

```
(root@kali)-[/home/kali]
# ufw allow from 192.168.1.100
Rule added
```



```
(root@kali)-[/home/kali]
# ufw logging on
Logging enabled
```

```
(root@kali)-[/home/kali]
# tail -f /var/log/ufw.log
```

Bloqueo en UFW:

```
(root@kali)-[/home/kali]
# ufw deny from 192.168.1.101
Rule added
```

```
(root@kali)-[/home/kali]
# ufw deny from any to any port 8080
Rule added
Rule added (v6)
```

Estatus UFW:

```
(root@kali)-[/home/kali]
# ufw status numbered
Status: active
```

	To	Action	From
[1]	22/tcp	ALLOW IN	Anywhere
[2]	80/tcp	ALLOW IN	Anywhere
[3]	443	ALLOW IN	Anywhere
[4]	Anywhere	ALLOW IN	192.168.1.100
[5]	Anywhere	DENY IN	192.168.1.101
[6]	8080	DENY IN	Anywhere
[7]	22/tcp (v6)	ALLOW IN	Anywhere (v6)
[8]	80/tcp (v6)	ALLOW IN	Anywhere (v6)
[9]	443 (v6)	ALLOW IN	Anywhere (v6)
[10]	8080 (v6)	DENY IN	Anywhere (v6)

Permisos en Iptables:

```
(root@kali)-[/home/kali]
# iptables -A INPUT -s 192.168.1.60 -j ACCEPT
```

Bloqueo en Iptables:

```
(root@kali)-[/home/kali]
# iptables -A INPUT -s 192.168.1.61 -j DROP
```

```
(root@kali)-[/home/kali]
# iptables -A INPUT -p tcp --dport 8080 -j DROP
```

Estatus Iptables:

```
(root@kali)-[/home/kali]
# iptables -L
```

```
Chain ufw-user-input (1 references)
target     prot opt source                destination           tcp dpt:ssh
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:http
ACCEPT     tcp  --  anywhere              anywhere              tcp dpt:https
ACCEPT     udp  --  anywhere              anywhere              udp dpt:https
ACCEPT     all  --  192.168.1.100         anywhere
DROP       all  --  192.168.1.101         anywhere
DROP       tcp  --  anywhere              anywhere              tcp dpt:http-alt
DROP       udp  --  anywhere              anywhere              udp dpt:8080
```