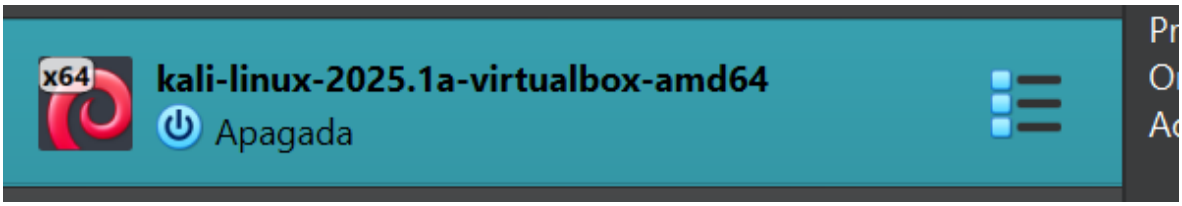
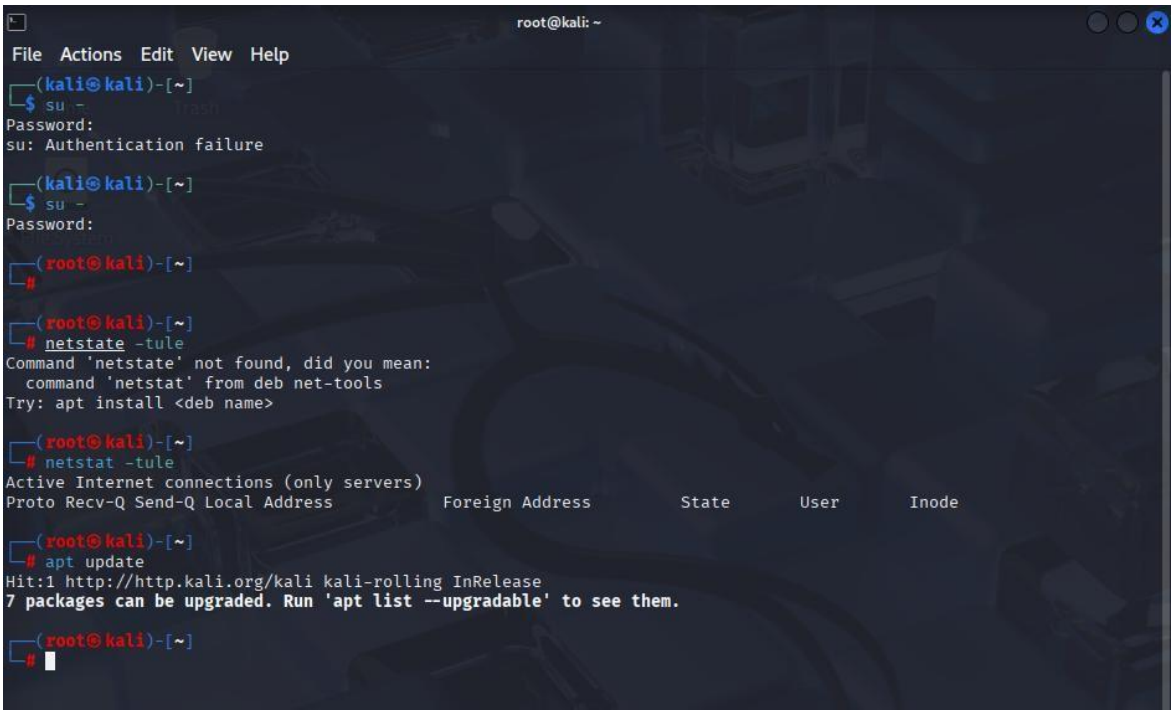
Laboratorio 7: Configuración de un Firewall en un Entorno de Red

Máquina virtual



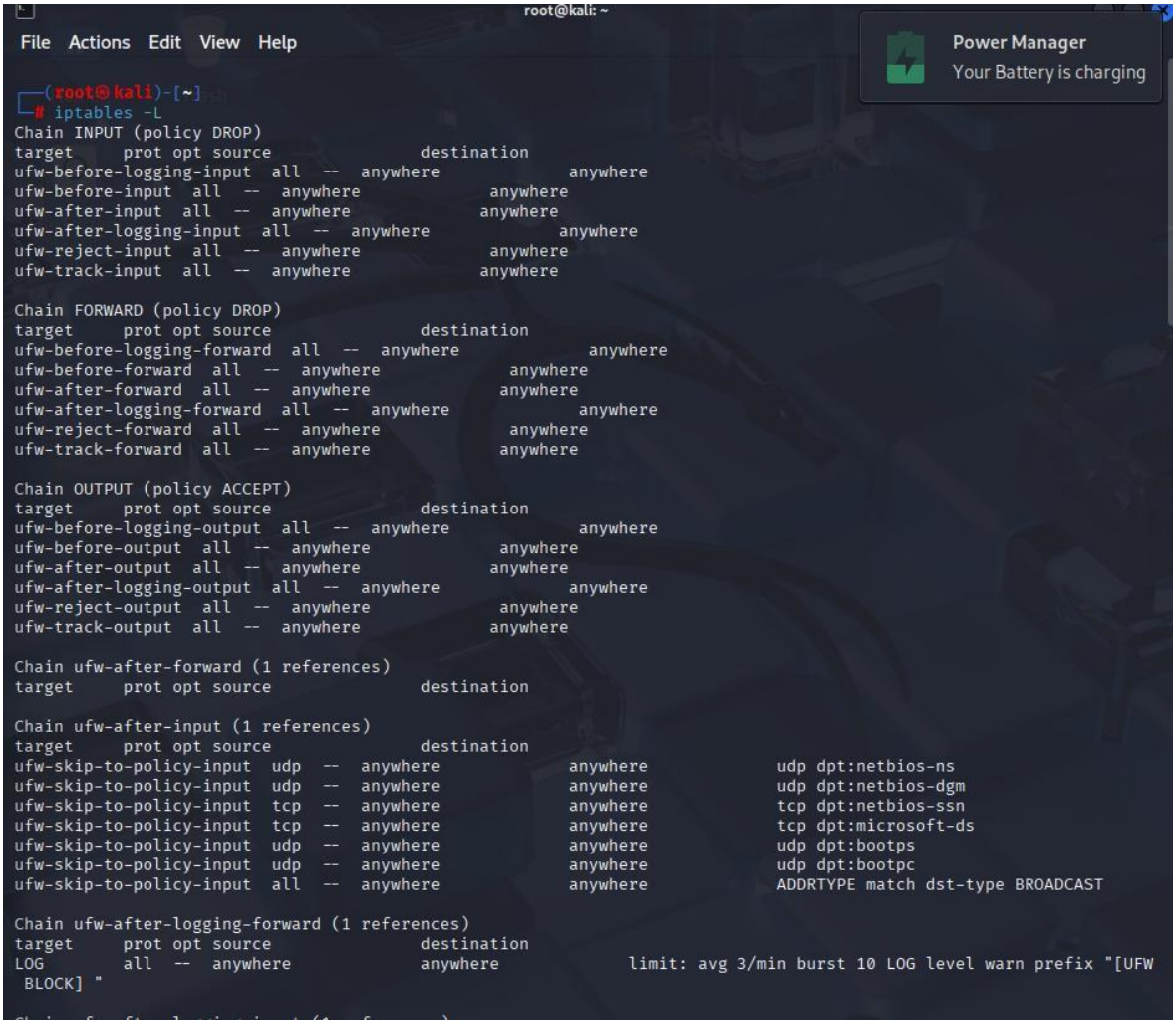
Entramos como usuario root:

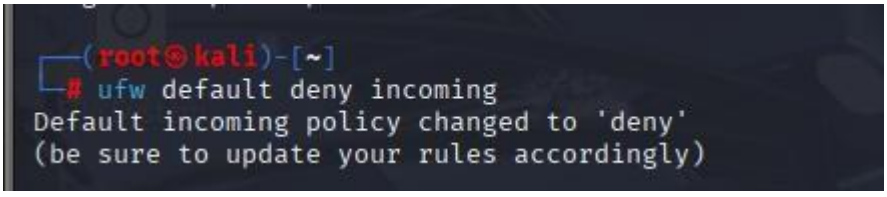


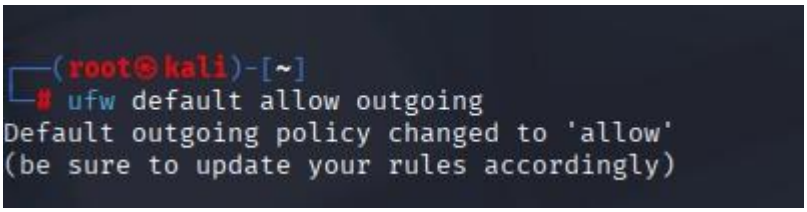
```
┌──(root㉿kali)-[~]
└─# apt update
Hit:1 http://http.kali.org/kali kali-rolling InRelease
7 packages can be upgraded. Run 'apt list --upgradable' to see them.

┌──(root㉿kali)-[~]
└─# ufw enable
Command 'ufw' not found, but can be installed with:
apt install ufw
Do you want to install it? (N/y)Y
apt install ufw
The following packages were automatically installed and are no longer required:
  icu-devtools  libgeos3.13.0  liblbfgsb0             libpython3.12-stdlib  python3.12-tk
  libflac12t64  libglapi-mesa  libpoppler145          libpython3.12t64      ruby-zeitwerk
  libfuse3-3    libicu-dev     libpython3.12-minimal  python3-setproctitle  strongswan
Use 'apt autoremove' to remove them.

Installing:
  ufw

Suggested packages:
  rsyslog

Summary:
  Upgrading: 0, Installing: 1, Removing: 0, Not Upgrading: 7
  Download size: 169 kB
  Space needed: 880 kB / 63.5 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 (176 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 416528 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)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# ufw enable
Firewall is active and enabled on system startup
```

```
┌──(root㉿kali)-[~]
└─# ufw status
Status: active
```


root@kali: ~
File Actions Edit View Help
Power Manager
Your Battery is charging
(root㉿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
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
BLOCK] "


(root㉿kali)-[~]
ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)


(root㉿kali)-[~]
ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

```
┌──(root㉿kali)-[~]
└─# iptables -P INPUT DROP

┌──(root㉿kali)-[~]
└─# iptables -P OUTPUT ACCEPT
```

```
┌──(root㉿kali)-[~]
└─# ufw allow ssh
Rule added
Rule added (v6)

┌──(root㉿kali)-[~]
└─# ufw allow ssh
Skipping adding existing rule
Skipping adding existing rule (v6)

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿kali)-[~]
└─# ufw allow http
Rule added
Rule added (v6)

┌──(root㉿kali)-[~]
└─# ufw allow https
Rule added
Rule added (v6)

┌──(root㉿kali)-[~]
└─#
```

```
Try 'iptables -h' or 'iptables --help' for more information.

┌──(root㉿kali)-[~]
└─# iptables -A INPUT -p tcp --dport 22 -j ACCEPT

┌──(root㉿kali)-[~]
└─# iptables -A INPUT -p tcp --dport 80 -j ACCEPT

┌──(root㉿kali)-[~]
└─# iptables -A INPUT -p tcp --dport 443 -j ACCEPT

┌──(root㉿kali)-[~]
└─#
```

```
┌──(root㉿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)


┌──(root㉿kali)-[~]
```

```
┌──(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     tcp  --  anywhere             anywhere             tcp dpt:https

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)
```

```
┌──(root㉿kali)-[/home/kali]
└─# ufw allow from 192.168.1.5
Rule added

┌──(root㉿kali)-[/home/kali]
```

```
┌──(root㉿kali)-[/home/kali]
└─# ufw deny from 192.168.1.5
Rule updated
```

```
┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -s  192.168.1.5 -j DROP

┌──(root㉿kali)-[/home/kali]
└─# iptables -A INPUT -s  192.168.1.5 -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     tcp  --  anywhere             anywhere             tcp dpt:https

DROP       all  --  192.168.1.5          anywhere
ACCEPT     all  --  192.168.1.5          anywhere

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