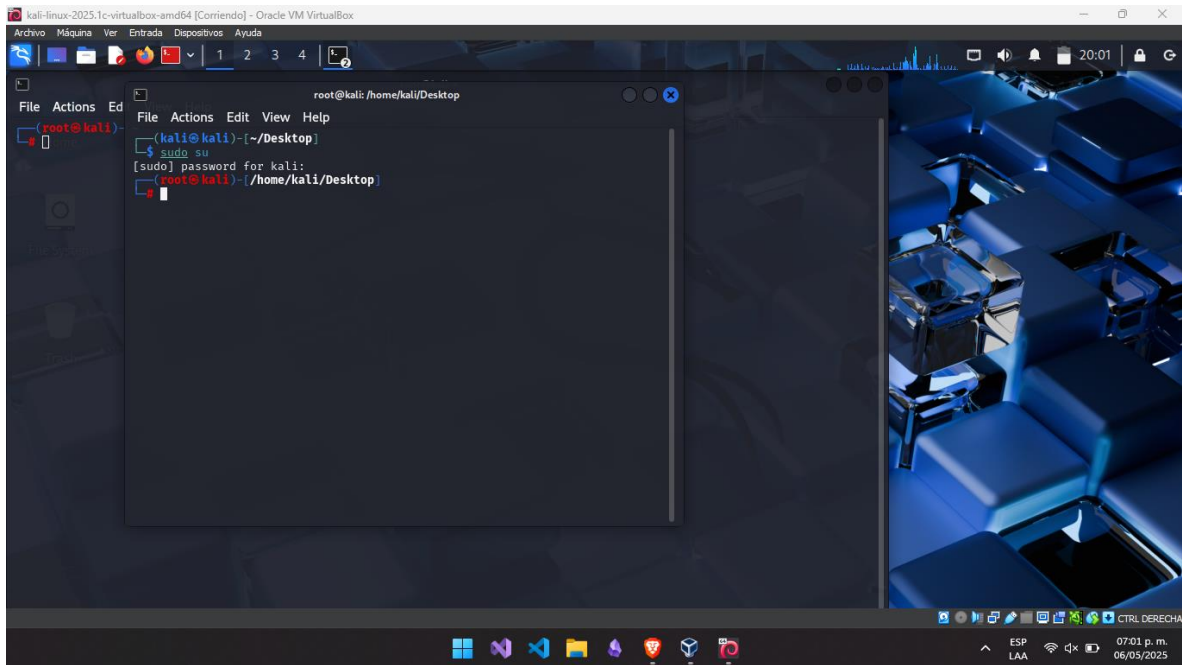
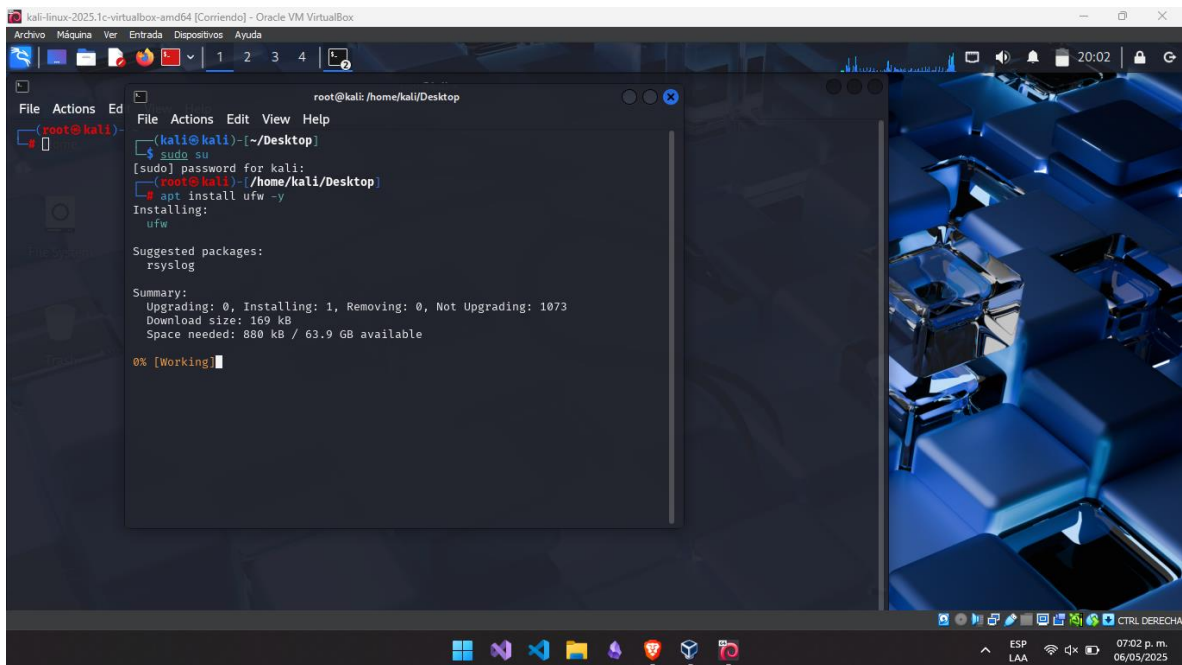


Carlos Alberto Rasgo Solano

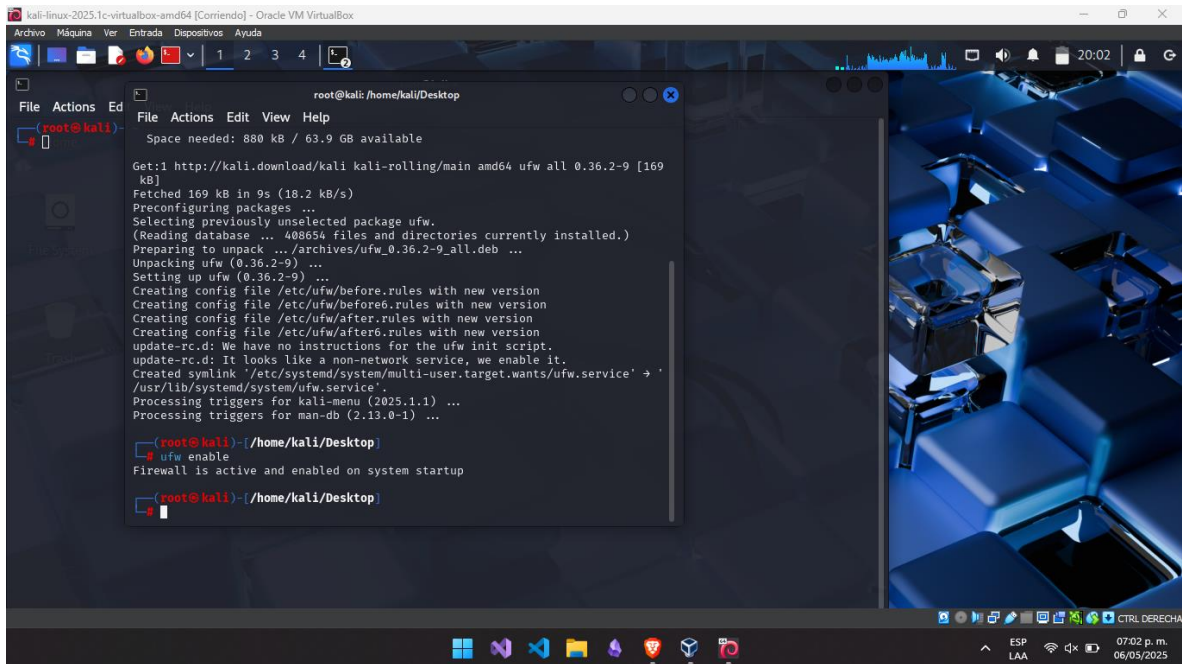
## Laboratorio de configuración de firewall



Una vez en la ubicación deseada instalamos ufw



## Carlos Alberto Rasgo Solano



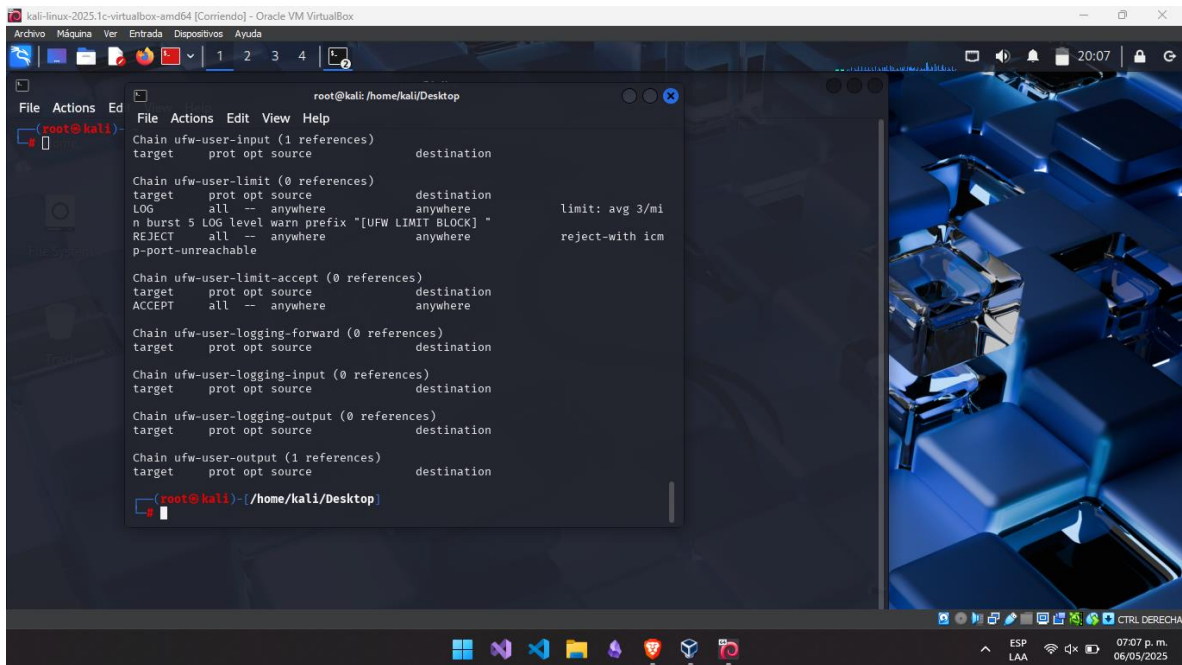
```
root@kali: /home/kali/Desktop
File Actions Edit View Help
Space needed: 880 kB / 63.9 GB available

Get:1 http://kali.download/kali kali-rolling/main amd64 ufw all 0.36.2-9 [169
kB]
Fetched 169 kB in 9s (18.2 kB/s)
Preconfiguring packages ...
Selecting previously unselected package ufw.
(Reading database ... 408654 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) ...

root@kali: /home/kali/Desktop
ufw enable
Firewall is active and enabled on system startup

root@kali: /home/kali/Desktop
```

Luego de instalarlo y habilitarlo nos dirigimos a la configuración principal básica:



```
root@kali: /home/kali/Desktop
File Actions Edit View Help
Chain ufw-user-input (1 references)
target prot opt source destination

Chain ufw-user-limit (0 references)
target prot opt source destination
LOG all -- anywhere anywhere limit: avg 3/mi
n burst 5 LOG level warn prefix "[UFW LIMIT BLOCK]"
REJECT all -- anywhere anywhere reject-with icmp
p-port-unreachable

Chain ufw-user-limit-accept (0 references)
target prot opt source destination
ACCEPT all -- anywhere anywhere

Chain ufw-user-logging-forward (0 references)
target prot opt source destination

Chain ufw-user-logging-input (0 references)
target prot opt source destination

Chain ufw-user-logging-output (0 references)
target prot opt source destination

Chain ufw-user-output (1 references)
target prot opt source destination

root@kali: /home/kali/Desktop
```

Carlos Alberto Rasgo Solano

A screenshot of a Kali Linux virtual machine running Oracle VM VirtualBox. The terminal window shows the user root@kali:/home/kali/Desktop configuring UFW rules. The output of ufw status shows several chains defined, including reject-with icmp, and the default policy is set to deny incoming traffic. The desktop background features a blue keyboard-themed wallpaper. The taskbar at the bottom includes icons for various applications and system utilities.

Kali Linux 2025.1c virtualBox and 64 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

1 2 3 4

File Actions Ed

File Actions Edit View Help

```

root@kali: /home/kali/Desktop

Chain ufw-user-logging-input (0 references)
target    prot opt source      destination

Chain ufw-user-logging-output (0 references)
target    prot opt source      destination

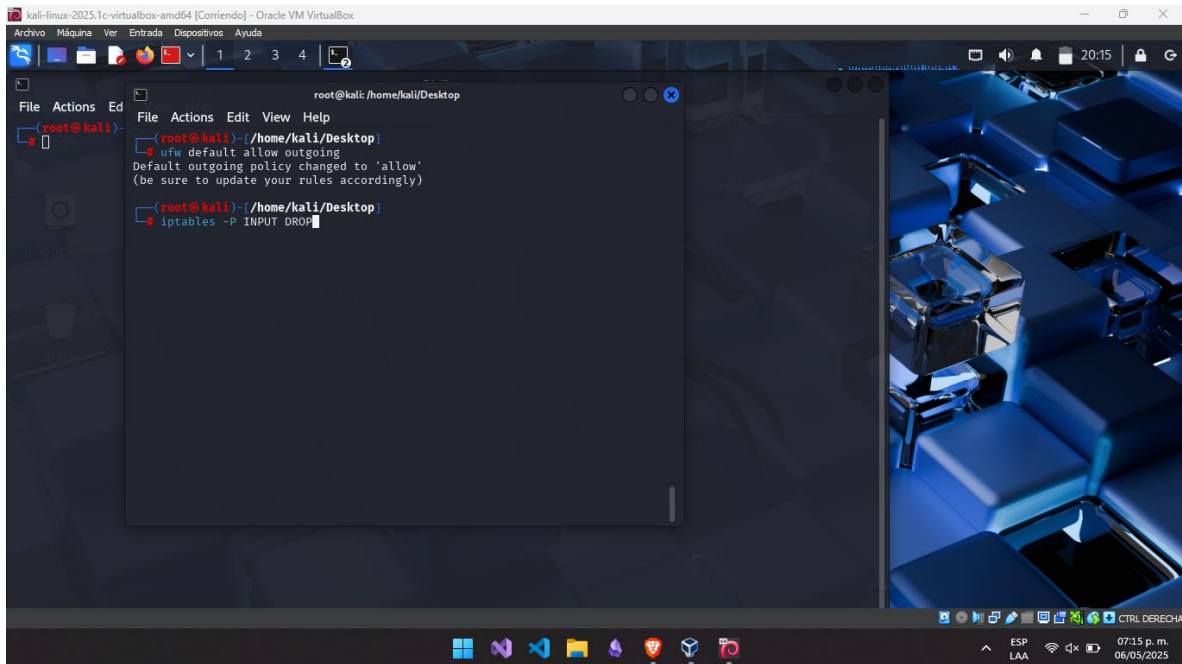
Chain ufw-user-output (1 references)
target    prot opt source      destination

root@kali:~# ls
root@kali:~# cd /home/kali/Desktop
root@kali:~/Desktop# ls -i
root@kali:~/Desktop# ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
root@kali:~/Desktop# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
root@kali:~/Desktop#

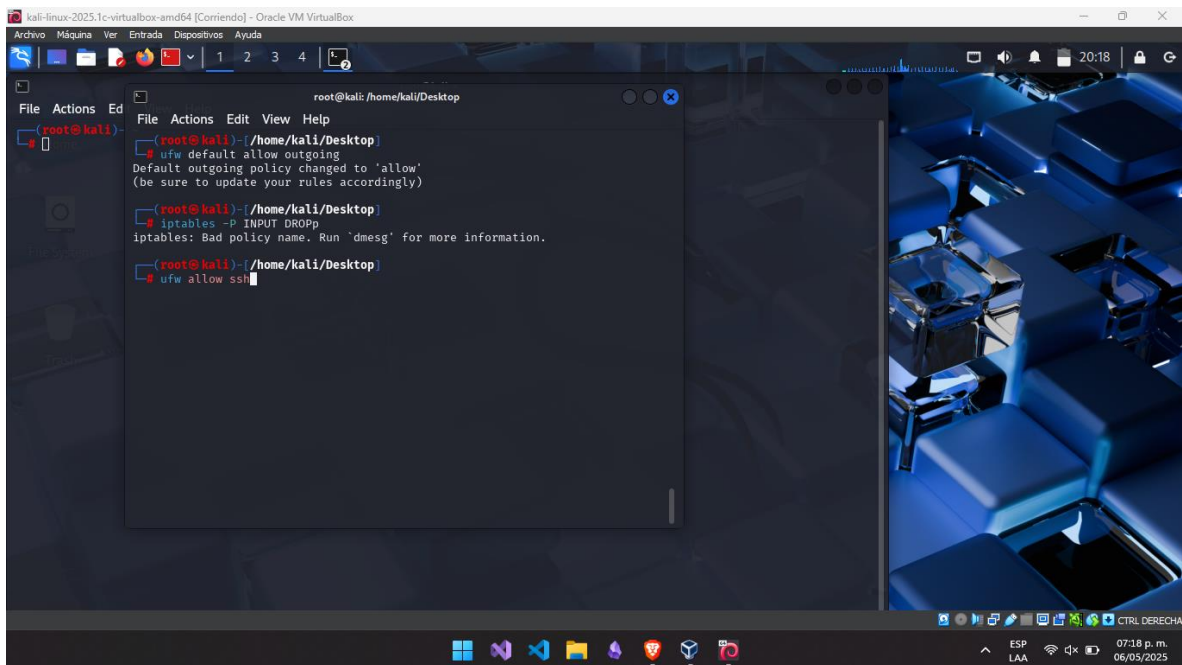
```

ESP LAA 07:12 p.m. 06/03/2025

Seguido de esto probamos la configuración en IPtables que es lo mismo de ufw pero desde otro entorno y configuracion

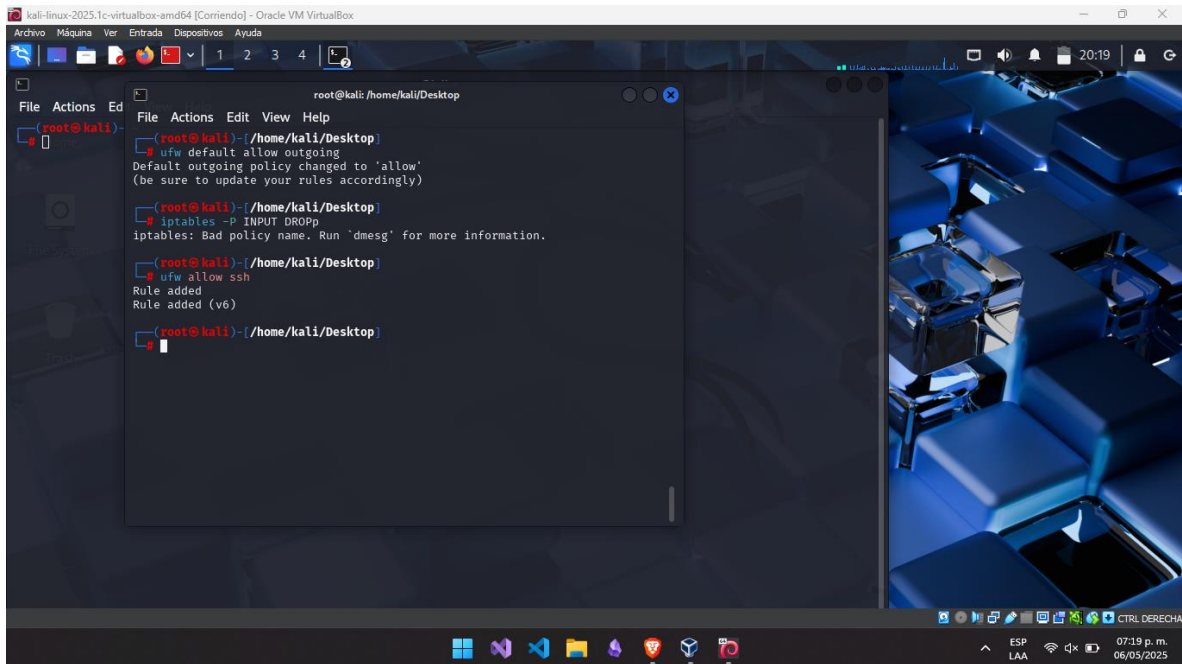


Como se observa son muy similares pero distintos en la sintaxis de configuración de las direcciones:



Añadimos las reglas:



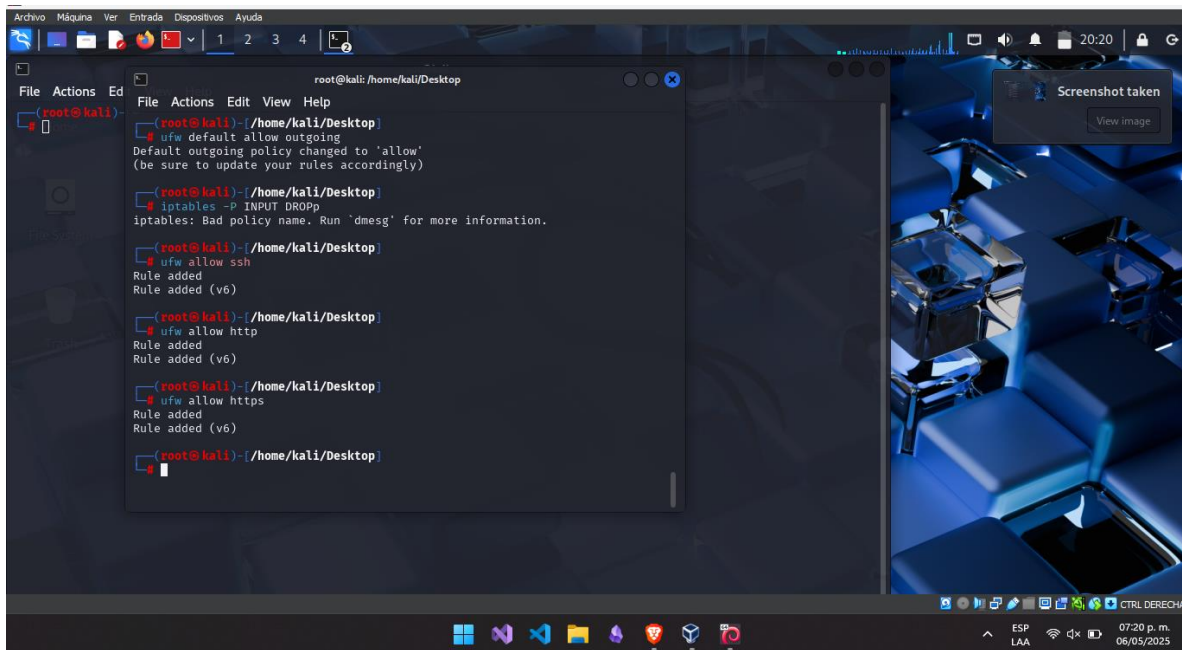


```
root@kali: /home/kali/Desktop
root@kali) ~
# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

root@kali) ~
# iptables -P INPUT DROPp
iptables: Bad policy name. Run 'dmesg' for more information.

root@kali) ~
# ufw allow ssh
Rule added
Rule added (v6)

root@kali) ~
#
```



```
root@kali: /home/kali/Desktop
root@kali) ~
# ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)

root@kali) ~
# iptables -P INPUT DROPp
iptables: Bad policy name. Run 'dmesg' for more information.

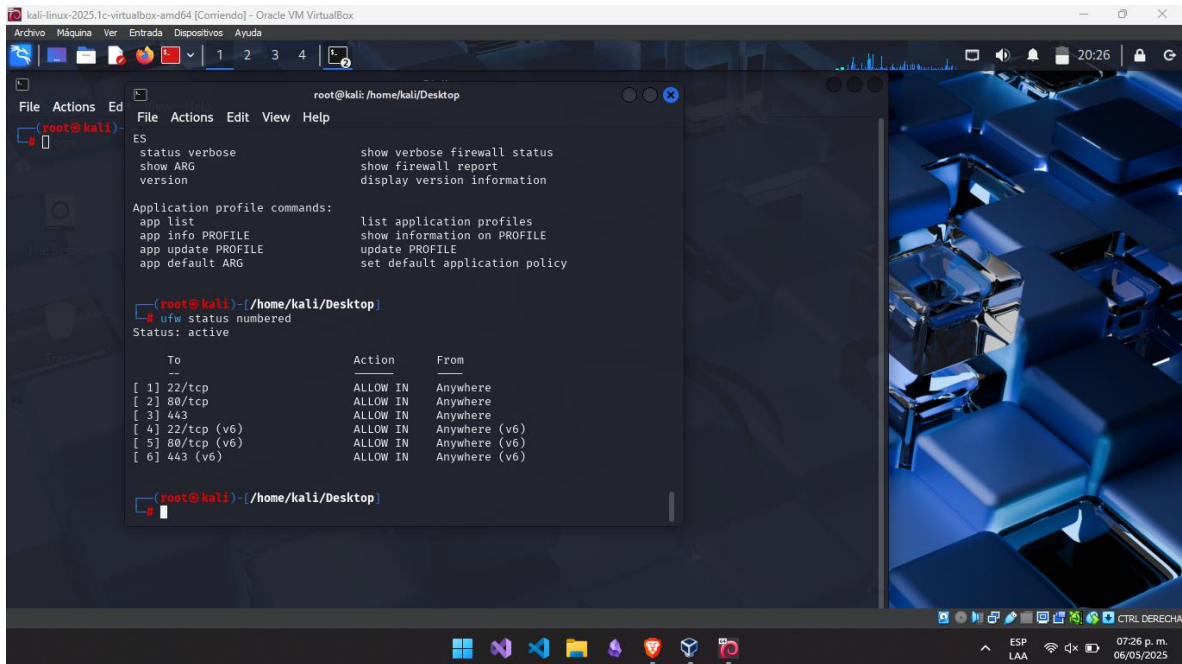
root@kali) ~
# ufw allow ssh
Rule added
Rule added (v6)

root@kali) ~
# ufw allow http
Rule added
Rule added (v6)

root@kali) ~
# ufw allow https
Rule added
Rule added (v6)

root@kali) ~
#
```

Seguido de esto comenzamos a identificar el estado de las reglas establecidas y su configuración:

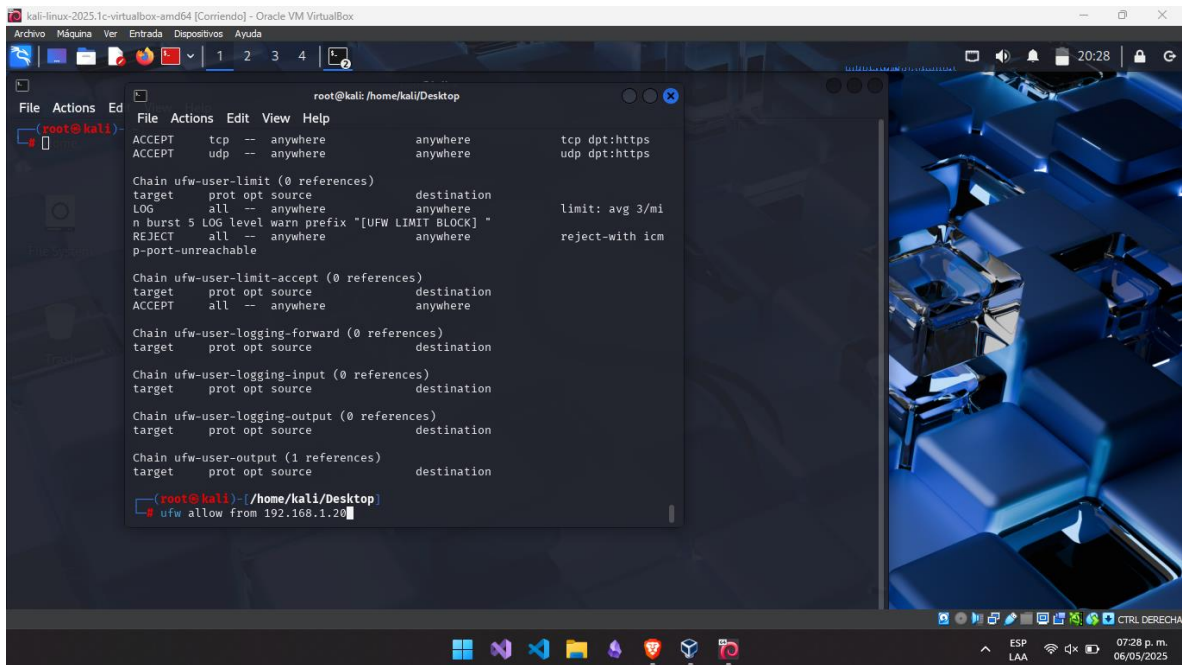


The screenshot shows a terminal window in a Kali Linux virtual machine. The user is at the root prompt in the directory /home/kali/Desktop. They have run the command `ufw status numbered`, which displays the current firewall status and a numbered list of rules.

```
root@kali: /home/kali/Desktop
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)
```

Aca se realizó una regla que permitiera a una dirección específica:

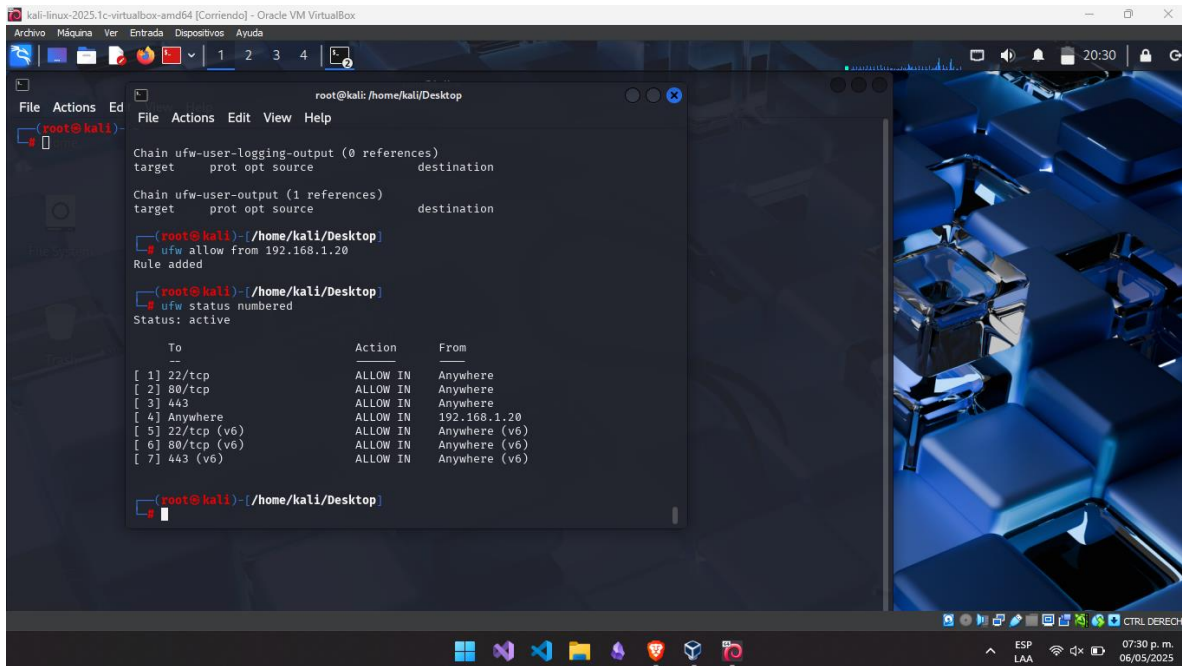


The screenshot shows the same terminal window. The user has run the command `ufw allow from 192.168.1.20`, which has added a new rule to the firewall. The terminal output shows the existing rules and the new rule being added.

```
root@kali:~# ufw allow from 192.168.1.20
ufw allow from 192.168.1.20
```

El objetivo era comprobar en el estado la actualización y los cambios que obtenia el firewall:

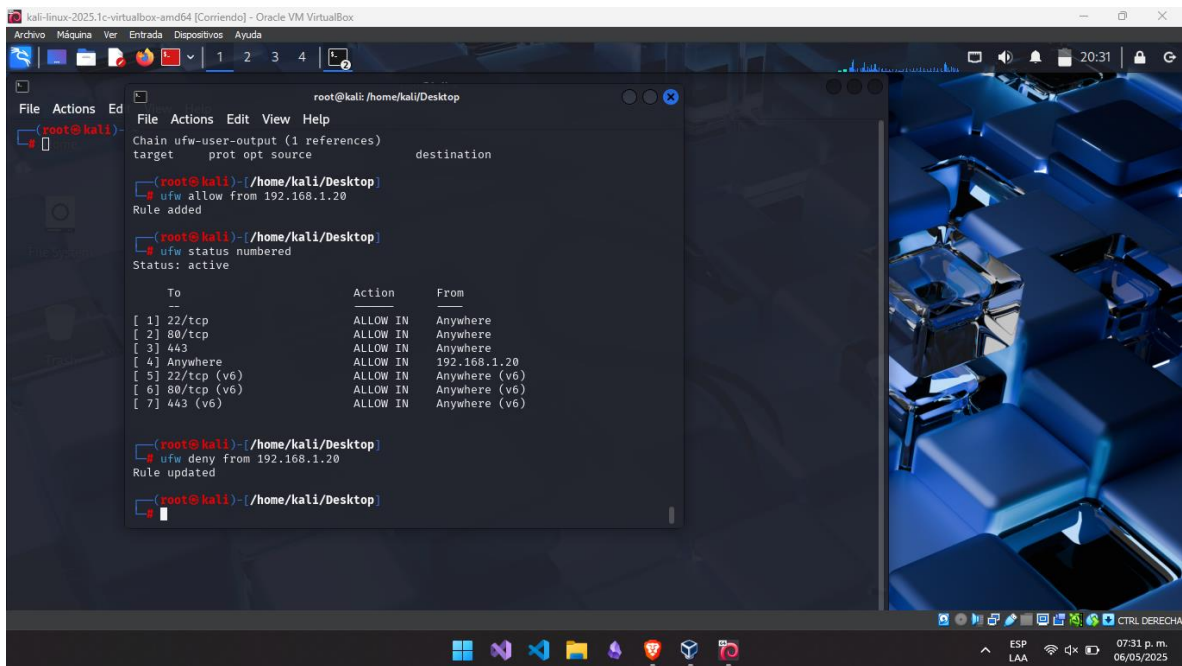
## Carlos Alberto Rasgo Solano



```
root@kali: /home/kali/Desktop
Chain ufw-user-logging-output (0 references)
target    prot opt source      destination
Chain ufw-user-output (1 references)
target    prot opt source      destination
root@kali: /home/kali/Desktop
# ufw allow from 192.168.1.20
Rule added
root@kali: /home/kali/Desktop
# 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 192.168.1.20
[ 5] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 7] 443 (v6) ALLOW IN Anywhere (v6)
root@kali: /home/kali/Desktop
```

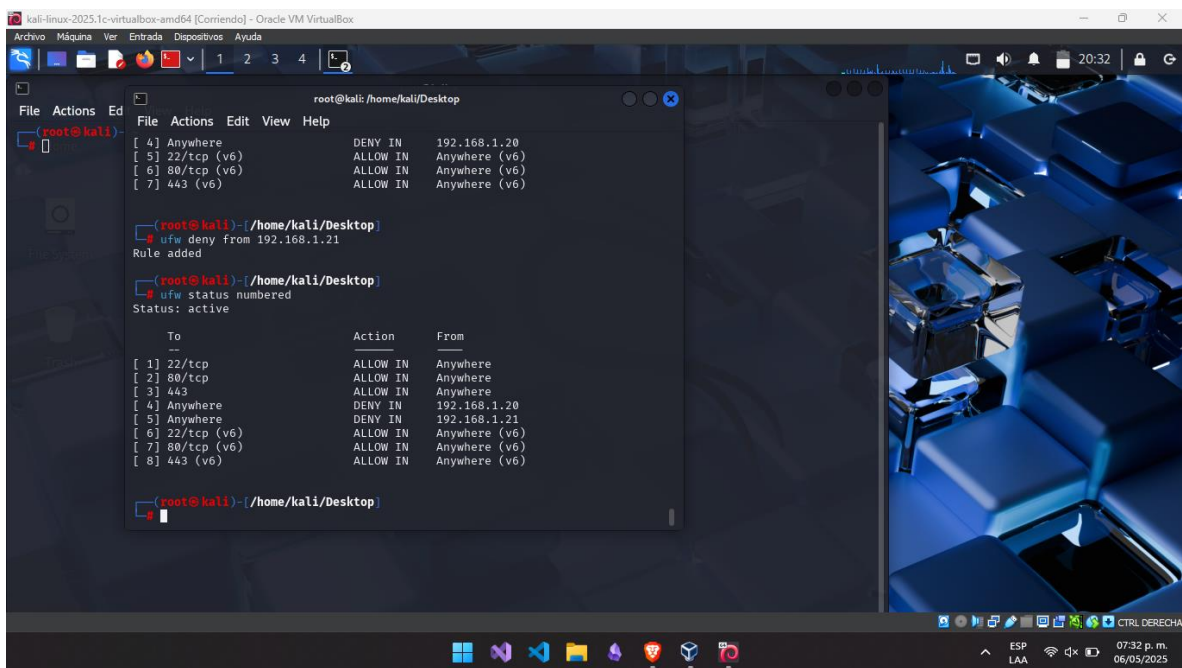
Lo mismo para estos ejemplo pero ahora es en el caso de denegar la dirección en específica:



```
root@kali: /home/kali/Desktop
Chain ufw-user-output (1 references)
target    prot opt source      destination
root@kali: /home/kali/Desktop
# ufw allow from 192.168.1.20
Rule added
root@kali: /home/kali/Desktop
# 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 192.168.1.20
[ 5] 22/tcp (v6) ALLOW IN Anywhere (v6)
[ 6] 80/tcp (v6) ALLOW IN Anywhere (v6)
[ 7] 443 (v6) ALLOW IN Anywhere (v6)
root@kali: /home/kali/Desktop
# ufw deny from 192.168.1.20
Rule updated
root@kali: /home/kali/Desktop
```



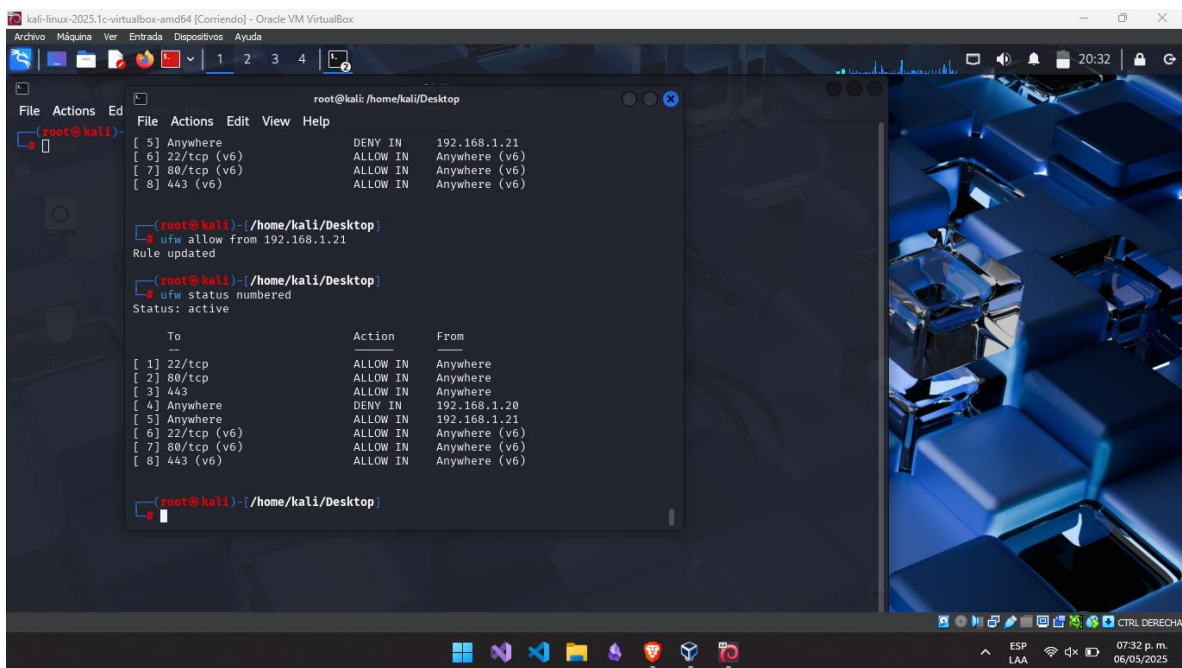


The screenshot shows a terminal window titled 'root@kali: /home/kali/Desktop' within an Oracle VM VirtualBox environment. The terminal displays the following commands and output:

```
root@kali: /home/kali/Desktop
# ufw deny from 192.168.1.21
Rule added

root@kali: /home/kali/Desktop
# 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	DENY IN	192.168.1.20
[ 5 ] Anywhere	DENY IN	192.168.1.21
[ 6 ] 22/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 7 ] 80/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 8 ] 443 (v6)	ALLOW IN	Anywhere (v6)



The screenshot shows a terminal window titled 'root@kali: /home/kali/Desktop' within an Oracle VM VirtualBox environment. The terminal displays the following commands and output:

```
root@kali: /home/kali/Desktop
# ufw allow from 192.168.1.21
Rule updated

root@kali: /home/kali/Desktop
# 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	DENY IN	192.168.1.20
[ 5 ] Anywhere	ALLOW IN	192.168.1.21
[ 6 ] 22/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 7 ] 80/tcp (v6)	ALLOW IN	Anywhere (v6)
[ 8 ] 443 (v6)	ALLOW IN	Anywhere (v6)

Concluyendo así con las primera configuración básica con ufw o iptables de un firewall