

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

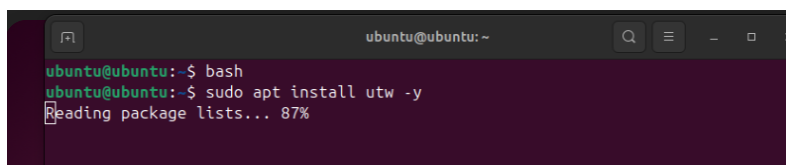
### Parte 1: Introducción al Firewall y Entorno de Configuración

#### Paso 1: Revisión de la Configuración de Red Actual

- Acción: Los participantes revisan la configuración de red existente, identificando qué servicios están activos y cuáles necesitan protección.
- Comando para Verificación en Linux: bash Copiar código `sudo netstat -tuln`
- Descripción: Este comando muestra qué puertos están abiertos y qué servicios están escuchando en esos puertos.

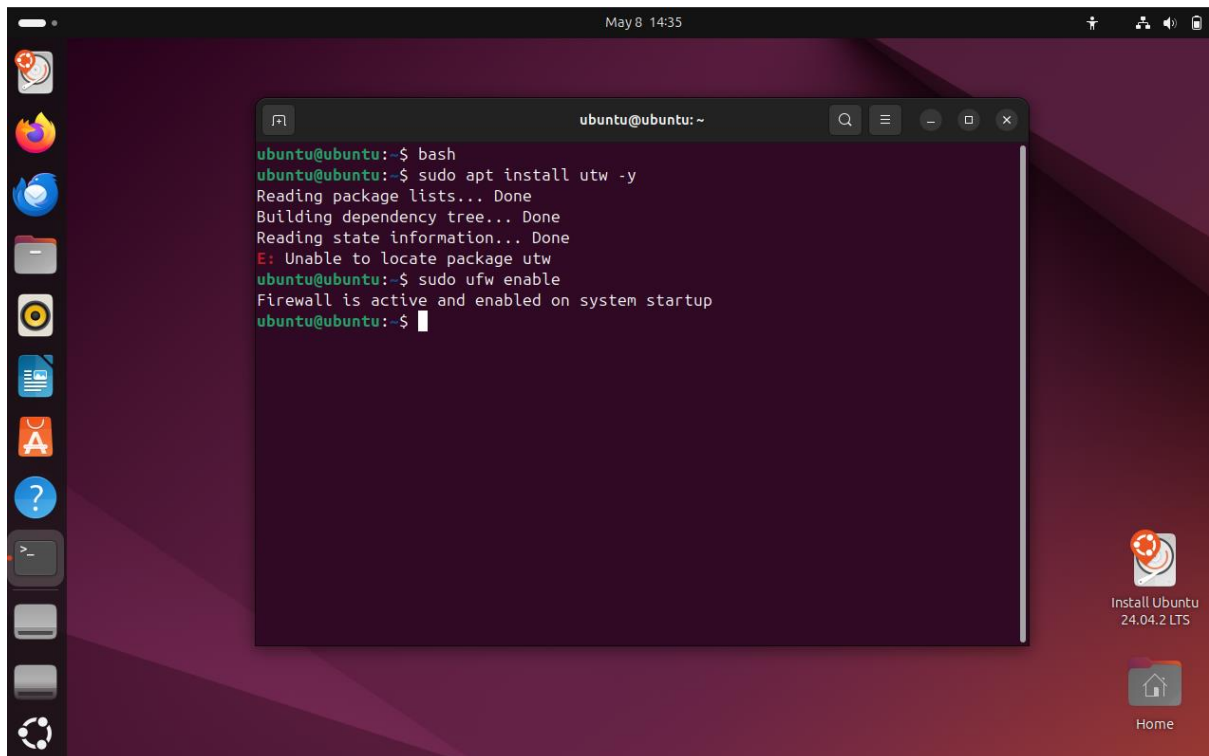
#### Paso 2: Instalación y Verificación del Firewall

- Acción: Verifica que el firewall esté instalado y habilitado en el sistema. Para UFW en Ubuntu: Instalación (si es necesario):



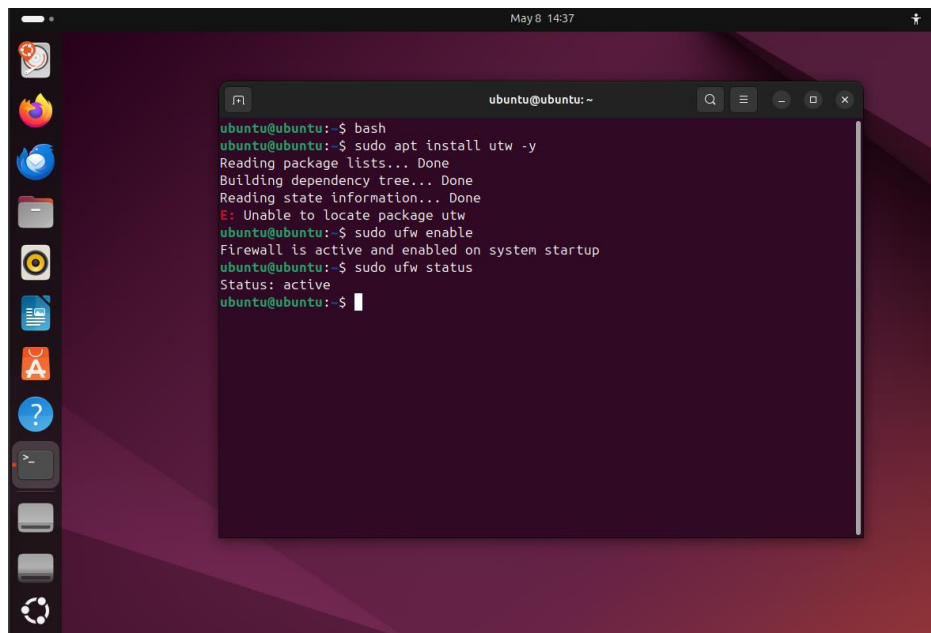
```
ubuntu@ubuntu: ~  
ubuntu@ubuntu:~$ bash  
ubuntu@ubuntu:~$ sudo apt install utw -y  
Reading package lists... 87%
```

- Habilitación:



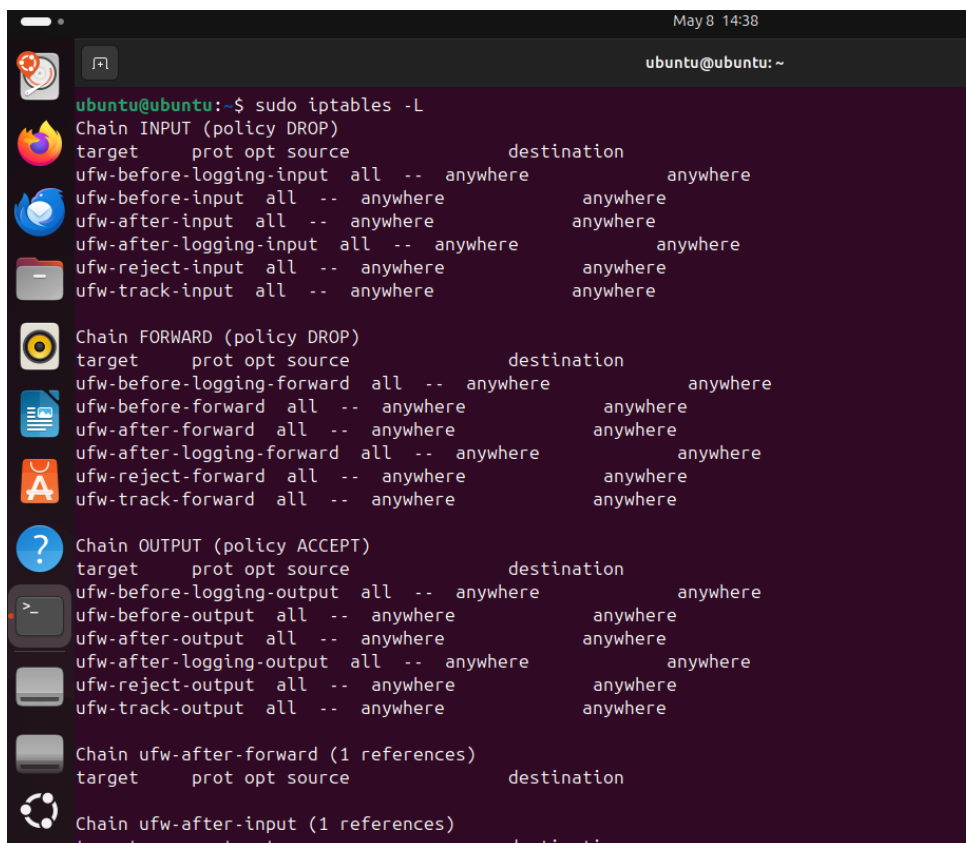
```
May 8 14:35  
ubuntu@ubuntu: ~  
ubuntu@ubuntu:~$ bash  
ubuntu@ubuntu:~$ sudo apt install utw -y  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
E: Unable to locate package utw  
ubuntu@ubuntu:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
ubuntu@ubuntu:~$
```

- Verificación del Estado del Firewall:



```
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ sudo apt install ufw -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package ufw
ubuntu@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
ubuntu@ubuntu:~$ sudo ufw status
Status: active
ubuntu@ubuntu:~$
```

- Verificación de la Instalación:



```
ubuntu@ubuntu:~$ sudo 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
```

- Instalación (si es necesario):

```
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/min burst 5 LOG level warn pref
BLOCK] "
REJECT       all  --  anywhere    anywhere    reject-with icmp-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
ubuntu@ubuntu:~$ sudo apt install iptables -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
iptables is already the newest version (1.8.10-3ubuntu2).
iptables set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

## Parte 2: Configuración Básica del Firewall Paso

### 3: Configuración de Políticas por Defecto

- Acción: Configura políticas predeterminadas para el tráfico entrante y saliente.

Para UFW: • Comandos:

```
ubuntu@ubuntu:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
```

Para iptables:

- Comandos:

```
ubuntu@ubuntu:~$ sudo ufw help
Commands:
enable                enables the firewall
disable              disables the firewall
default ARG          set default policy
logging LEVEL        set logging to LEVEL
allow ARGS           add allow rule
deny ARGS            add deny rule
reject ARGS          add reject rule
limit ARGS           add limit rule
delete RULE|NUM      delete RULE
insert NUM RULE       insert RULE at NUM
prepend RULE         prepend RULE
route RULE           add route RULE
route delete RULE|NUM delete route RULE
route insert NUM RULE insert route RULE at NUM
reload               reload firewall
reset                reset firewall
status              show firewall status
status numbered      show firewall status as numbered
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

ubuntu@ubuntu:~$ sudo iptables -P INPUT DROP
ubuntu@ubuntu:~$ sudo iptables -P OUTPUT ACCEPT
ubuntu@ubuntu:~$
```

#### Paso 4: Permitir Tráfico para Servicios Específicos

- Acción: Configura reglas para permitir el tráfico de servicios esenciales, como HTTP/HTTPS para servidores web o SSH para acceso remoto. Para UFW:
- Comandos:

```
ubuntu@ubuntu:~$ bash
ubuntu@ubuntu:~$ sudo ufw allow ssh
Rule added
Rule added (v6)
ubuntu@ubuntu:~$
```

```

ubuntu@ubuntu:~$ sudo ufw allow http
Rule added
Rule added (v6)
ubuntu@ubuntu:~$

ubuntu@ubuntu:~$ sudo ufw allow https
Rule added
Rule added (v6)
ubuntu@ubuntu:~$

```

Para iptables:

- Comandos:

```

Rule added (v6)
ubuntu@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 22 -j ACCEPT
ubuntu@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 80 -j ACCEPT
ubuntu@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 443 -j ACCEPT
ubuntu@ubuntu:~$

```

- Verificación: Revisa el estado del firewall para asegurarte de que las reglas se hayan aplicado correctamente:

	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)

```

ubuntu@ubuntu:~$

```

```

ubuntu@ubuntu:~$ sudo 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

```

### Parte 3: Configuración Avanzada del Firewall

#### Paso 5: Crear Reglas de Filtrado por IP

- Acción: Configura reglas para permitir o denegar tráfico basado en direcciones IP específicas.

Para UFW:

```

ubuntu@ubuntu:~$ sudo ufw allow from 192.168.1.100
Rule added
ubuntu@ubuntu:~$

```

- Ejemplo para denegar una IP específica:

```

ubuntu@ubuntu:~$ sudo ufw deny from 192.168.1.100
Rule updated
ubuntu@ubuntu:~$

```

- Ejemplo para permitir una IP específica:

- Ejemplo para denegar una IP específica:

```
ubuntu@ubuntu:~$ sudo iptables -A INPUT -s 192.168.1.100 -j ACCEPT
ubuntu@ubuntu:~$ sudo iptables -A INPUT -s 192.168.1.100 -j DROP
ubuntu@ubuntu:~$
```

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

- Acción: Configura reglas para diferenciar el tráfico interno del tráfico externo, protegiendo mejor los recursos internos.

Para UFW:

- Ejemplo para denegar tráfico externo a puertos no esenciales: bash Copiar código  
sudo ufw deny from any to any port 8080

```
ubuntu@ubuntu:~$ sudo ufw deny from any to any port 8080
Rule added
Rule added (v6)
ubuntu@ubuntu:~$
```

Para iptables: • Ejemplo para permitir todo el tráfico interno:

```
ubuntu@ubuntu:~$ sudo iptables -A INPUT -s 192.168.1.0/24 -j ACCEPT
ubuntu@ubuntu:~$
```

Ejemplo para bloquear puertos no esenciales desde redes externas

```
ubuntu@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 8080 -j DROP
ubuntu@ubuntu:~$
```

## Parte 4: Monitoreo y Ajustes del Firewall

### Paso 7: Monitoreo de Logs del Firewall

- Acción: Habilita el registro de los intentos de acceso denegados y revisa los logs para identificar patrones sospechosos.

Para UFW:

- Habilitar el registro:

```
ubuntu@ubuntu:~$ sudo ufw logging on
Logging enabled
ubuntu@ubuntu:~$
```

Revisar los logs::

```
ubuntu@ubuntu:~$ sudo tail -f /var/log/ufw.log
tail: cannot open '/var/log/ufw.log' for reading: No such file or directory
tail: no files remaining
ubuntu@ubuntu:~$
```

Para iptables: • Habilitar el registro:

```
ubuntu@ubuntu:~$ sudo iptables -A INPUT -j LOG --log-prefix "IPTables-Dropped:"--log/level
ubuntu@ubuntu:~$
```

- Revisar los logs:

```
ubuntu@ubuntu:~$ sudo tail -f /var/log/syslog
2025-05-08T15:10:14.386397+00:00 ubuntu systemd[1]: Starting sysstat-collect.service - system
.
2025-05-08T15:10:14.450545+00:00 ubuntu systemd[1]: sysstat-collect.service: Deactivated succ
2025-05-08T15:10:14.450643+00:00 ubuntu systemd[1]: Finished sysstat-collect.service - system
2025-05-08T15:13:15.617167+00:00 ubuntu systemd[1]: Starting fwupd-refresh.service - Refresh
otd...
2025-05-08T15:13:15.781139+00:00 ubuntu fwupdmgr[6178]: Updating lvfs
2025-05-08T15:13:21.050504+00:00 ubuntu fwupdmgr[6178]: Successfully downloaded new metadata:
2025-05-08T15:13:21.126278+00:00 ubuntu systemd[1]: fwupd-refresh.service: Deactivated succes
2025-05-08T15:13:21.126612+00:00 ubuntu systemd[1]: Finished fwupd-refresh.service - Refresh
otd.
2025-05-08T15:15:01.764020+00:00 ubuntu CRON[6224]: (root) CMD (command -v debian-sa1 > /dev/
2025-05-08T15:17:01.788284+00:00 ubuntu CRON[6237]: (root) CMD (cd / && run-parts --report /e
```