ceedcv

CENTRE ESPECÍFIC
D´EDUCACIÓ A DISTÀNCIA DE
LA COMUNITAT VALENCIANA

ACTIVIDAD EVALUABLE

SEGURIDAD Y ALTA DISPONIBILIDAD

UD5. Cortafuegos UFW e Iptables

Autor: Manuel Fernández

ECHA POR: ALEJANDRO ALMAGRO TORREGROSA

1. Comprobacion de la instalacion de ufw:

```
root@dislexia-VirtualBox:/home/dislexia# apt install ufw
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
ufw ya está en su versión más reciente (0.36.2-6).
fijado ufw como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no
son necesarios.
  libllvm17t64 python3-netifaces
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
root@dislexia-VirtualBox:/home/dislexia#
```

2. Configuracion de politicas:

```
dislexia@dislexia-VirtualBox:~$ sudo ufw default deny incoming
[sudo] contraseña para dislexia:
La política incoming predeterminada cambió a «deny»
(asegúrese de actualizar sus reglas consecuentemente)
```

dislexia@dislexia-VirtualBox: ~

```
dislexia@dislexia-VirtualBox:~$ sudo ufw default allow outgoing
La política outgoing predeterminada cambió a «allow»
(asegúrese de actualizar sus reglas consecuentemente)
dislexia@dislexia-VirtualBox:~$
```

3. Habilitar ssh y cat del servicio ssh:

```
dislexia@dislexia-VirtualBox:~$ sudo ufw allow ssh
Reglas actualizadas
Reglas actualizadas (v6)
dislexia@dislexia-VirtualBox:~$
```

```
dislexia@dislexia-VirtualBox:~$ cat /etc/services | grep "ssh"
ssh             22/tcp                          # SSH Remote Login Protocol
dislexia@dislexia-VirtualBox:~$
```

4. Comprobacion de que ufw esta activo:

```
dislexia@dislexia-VirtualBox:~$ sudo ufw enable
El cortafuegos está activo y habilitado en el arranque del sistema
dislexia@dislexia-VirtualBox:~$
```

5. Habilitar otras conexiones:

Protocolos por nombre:

```
dislexia@dislexia-VirtualBox:~$ sudo ufw allow http
Reglas actualizadas
Reglas actualizadas (v6)
dislexia@dislexia-VirtualBox:~$ sudo ufw allow https
Reglas actualizadas
Reglas actualizadas (v6)
dislexia@dislexia-VirtualBox:~$
```

```
dislexia@dislexia-VirtualBox:~$ sudo ufw allow 3006:3008/tcp
Reglas actualizadas
Reglas actualizadas (v6)
dislexia@dislexia-VirtualBox:~$ sudo ufw allow 3006:3008/udp
Reglas actualizadas
Reglas actualizadas (v6)
dislexia@dislexia-VirtualBox:~$
```

Permitir la conexión desde redes y una red a un puerto en espeficio:

```
dislexia@dislexia-VirtualBox:~$ sudo ufw allow from 192.168.1.0
Regla añadida
```

```
dislexia@dislexia-VirtualBox:~$ sudo ufw allow from 192.168.1.0 to any port 22
Regla añadida
```

Permitir tambien subredes y subred mas puerto en espeficico:

```
dislexia@dislexia-VirtualBox:~$ sudo ufw allow from 192.168.1.0/24
Regla añadida
dislexia@dislexia-VirtualBox:~$ sudo ufw allow from 192.168.1.0/24 to any port 22
Regla añadida
dislexia@dislexia-VirtualBox:~$
```

Conexiones a una interfaz de red especifica:

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group de
fault qlen 1000
    link/ether 08:00:27:4b:90:3b brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.186/24 brd 192.168.1.255 scope global dynamic noprefixroute enp0s3
       valid_lft 85935sec preferred_lft 85935sec
    inet6 fe80::a00:27ff:fe4b:903b/64 scope link
       valid_lft forever preferred_lft forever
dislexia@dislexia-VirtualBox:~$
```

```
dislexia@dislexia-VirtualBox:~$ sudo ufw allow in on enp0s3 to any port 80
Regla añadida
Regla añadida (v6)
dislexia@dislexia-VirtualBox:~$
```

6. Denegar conexiones

Denegacion de subred

```
dislexia@dislexia-VirtualBox:~$ sudo ufw deny  from 192.168.1.0/26
Regla añadida
dislexia@dislexia-VirtualBox:~$
```

Comprobación del estado actual de firewall:

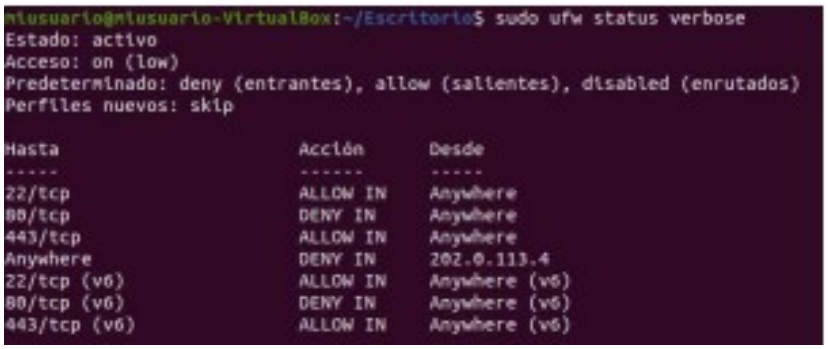
```
Predeterminado: deny (entrantes), allow (salientes), disabled (enrutados)
Perfiles nuevos: skip

Hasta                      Acción      Desde
-----                      ------      -----
22/tcp                     ALLOW IN    Anywhere
443                        ALLOW IN    Anywhere
80/tcp                     DENY IN     Anywhere
3006:3008/tcp              ALLOW IN    Anywhere
3006:3008/udp              ALLOW IN    Anywhere
Anywhere                   ALLOW IN    192.168.1.0
22                         ALLOW IN    192.168.1.0
Anywhere                   ALLOW IN    192.168.1.0/24
22                         ALLOW IN    192.168.1.0/24
80 on enp0s3               ALLOW IN    Anywhere
Anywhere                   DENY IN     192.168.1.0/26
22/tcp (v6)                ALLOW IN    Anywhere (v6)
443 (v6)                   ALLOW IN    Anywhere (v6)
80/tcp (v6)                DENY IN     Anywhere (v6)
3006:3008/tcp (v6)         ALLOW IN    Anywhere (v6)
3006:3008/udp (v6)         ALLOW IN    Anywhere (v6)
80 (v6) on enp0s3          ALLOW IN    Anywhere (v6)

dislexia@dislexia-VirtualBox:~$
```

***Aqui se ve todas las normas aplicadas, me salte las fotos del 443, 80, 3006:3008(tcp/udp) y la denegacion del puerto 80, se muestran aquí como aplicadas**

Explicacion de la foto del PDF:

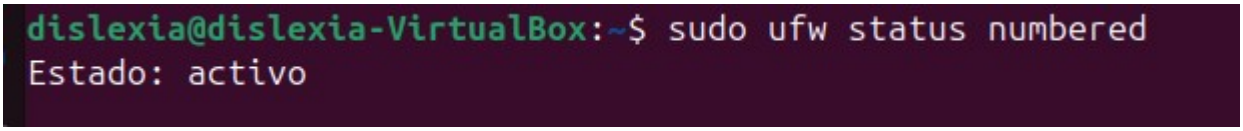


1. Tenemos permitidas las conexiones de los puertos ***22/tcp, 443/tcp*** *desde cualquier parte*
2. Tenemos restringidas las conexiones desde ***el puerto 80 o 88 (no se ve bien en la foto)/tcp y ademas la red 202.0.113.4 tiene denegada cualquier tipo de conexión en cualquier tipo de servicio.***

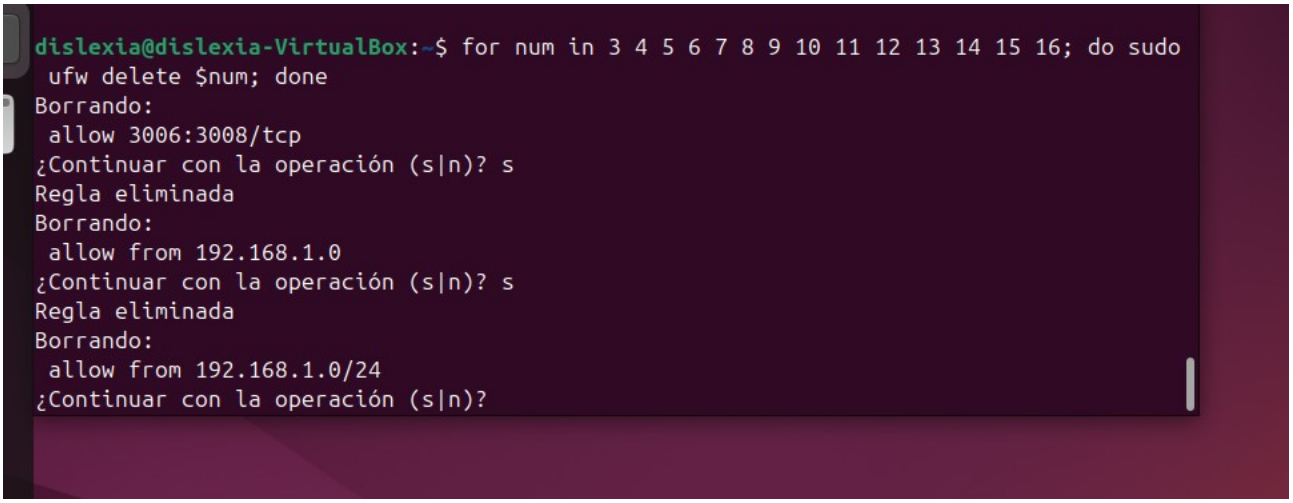
7. **Eliminar las reglas**

A. Por numero de regla:

Habra que mostrar la numeracion de las regla, con el siguiente comando:



Eliminacion multiple de normas según los numeros de manera continua:



8. Deshabilitar o reiniciar el servicio del firewall:

```
dislexia@dislexia-VirtualBox:~$ sudo ufw disable
El cortafuegos está detenido y deshabilitado en el arranque del sistema
dislexia@dislexia-VirtualBox:~$ sudo ufw reset
Reiniciando todas las reglas a sus valores predeterminados instalados.
¿Continuar con la operación (s|n)?
Interrumpido
dislexia@dislexia-VirtualBox:~$ sudo ufw reset
Reiniciando todas las reglas a sus valores predeterminados instalados.
¿Continuar con la operación (s|n)? s
Respaldando «user.rules» en «/etc/ufw/user.rules.20250202_191325»
Respaldando «before.rules» en «/etc/ufw/before.rules.20250202_191325»
Respaldando «after.rules» en «/etc/ufw/after.rules.20250202_191325»
Respaldando «user6.rules» en «/etc/ufw/user6.rules.20250202_191325»
Respaldando «before6.rules» en «/etc/ufw/before6.rules.20250202_191325»
Respaldando «after6.rules» en «/etc/ufw/after6.rules.20250202_191325»

dislexia@dislexia-VirtualBox:~$
```

Con el reset ganaremos dejar el ufw tal y como estaba antes de añadir las reglas.

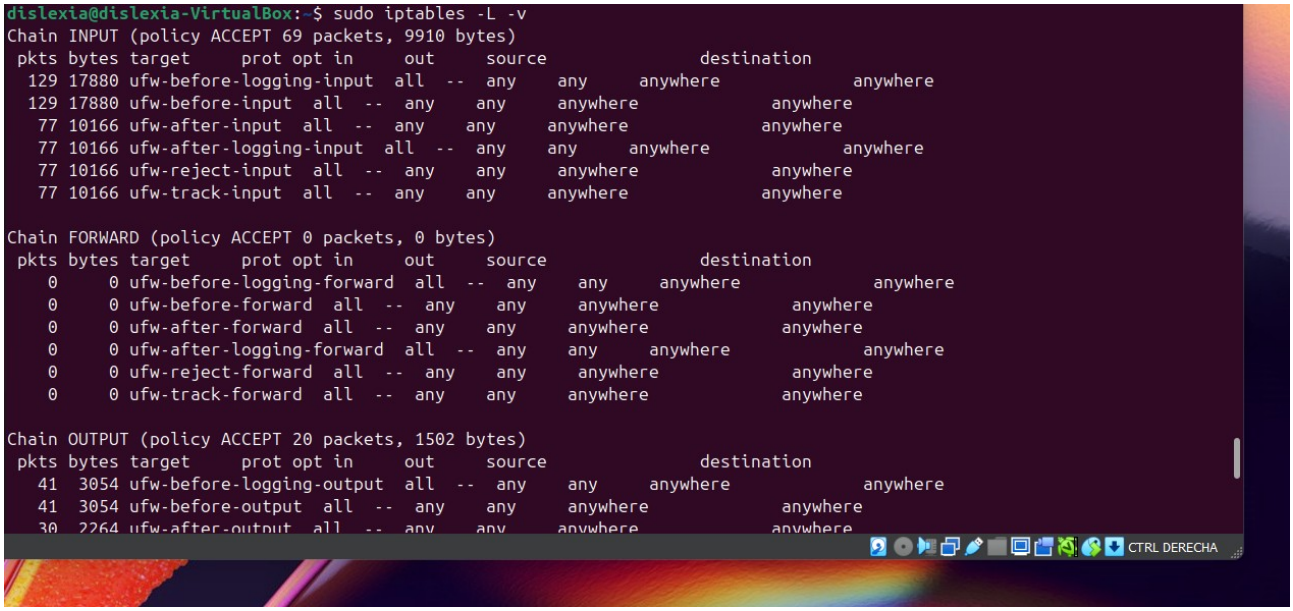
PRACTICA 2 CORTAFUEGOS EN LINUX CON IPTABLES

1. Instalacion del servicio y comprobacion del estado de las reglas de iptables:

Comprobacion de instalacion:

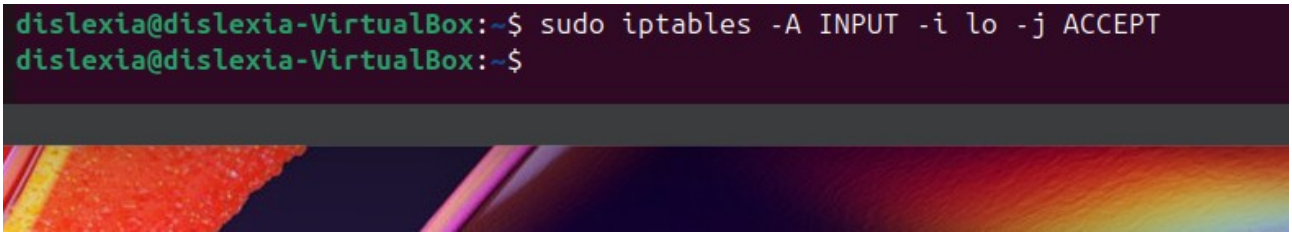
```
root@dislexia-VirtualBox:/home/dislexia# apt install iptables
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
iptables ya está en su versión más reciente (1.8.10-3ubuntu2).
fijado iptables como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son ne
cesarios.
  libllvm17t64 python3-netifaces
Utilice «sudo apt autoremove» para eliminarlos.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
root@dislexia-VirtualBox:/home/dislexia#
```

Comprobación de las reglas actuales con el comando iptables -L -v

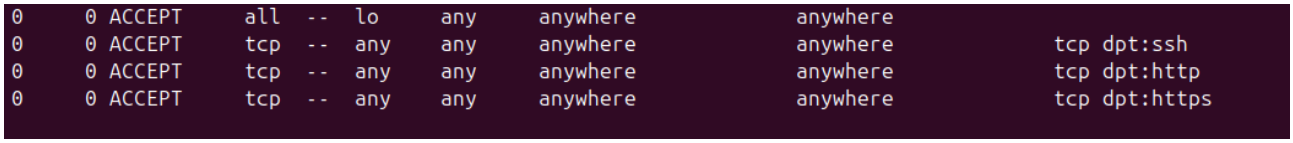


2. Definicion de reglas de cadena

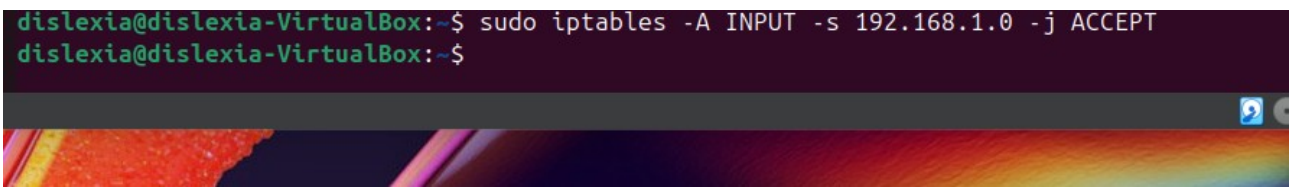
Habilitar el trafico en localhost:



*Añadir los puertos espeficios t**cp ssh, http y https:***



Basando en la fuente ip:



Comprobacion de las normas:

```
0     0 ACCEPT     all  --  lo     any     anywhere             anywhere
0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
0     0 ACCEPT     all  --  any    any     192.168.1.0          anywhere
```

Haciendo un drop de la misma ip y de un rango en especifico de ips:

```
    0     0 ACCEPT     all  --  any    any     192.168.1.0          anywhere
    0     0 DROP       all  --  any    any     192.168.1.0          anywhere
    1    32 DROP       all  --  any    any     anywhere             anywhere             source IP range 192.168.1.0-192
.168.1.200
```

Suprimiendo el resto del trafico:

```
  0     0 DROP       all  --  any    any     anywhere             anywhere
```

Ahora pasaremos a eliminar las reglas y para esto necesitaremos listar la numeración:

```
dislexia@dislexia-VirtualBox:~$ sudo iptables -L --line-numbers
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination
1    ufw-before-logging-input  all  --  anywhere             anywhere
2    ufw-before-input  all  --  anywhere             anywhere
3    ufw-after-input  all  --  anywhere             anywhere
4    ufw-after-logging-input  all  --  anywhere             anywhere
5    ufw-reject-input  all  --  anywhere             anywhere
6    ufw-track-input  all  --  anywhere             anywhere
7    ACCEPT     all  --  anywhere             anywhere
8    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:ssh
9    ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:http
10   ACCEPT     tcp  --  anywhere             anywhere             tcp dpt:https
11   ACCEPT     all  --  192.168.1.0          anywhere
12   DROP       all  --  192.168.1.0          anywhere
13   DROP       all  --  anywhere             anywhere             source IP range 192.168.1.0-192.168.1.200
14   DROP       all  --  anywhere             anywhere
```

Eliminacion de reglas:

```
dislexia@dislexia-VirtualBox:~$ sudo iptables -D INPUT 13
dislexia@dislexia-VirtualBox:~$ sudo iptables -D INPUT 14
iptables: Index of deletion too big.
dislexia@dislexia-VirtualBox:~$ sudo iptables -D INPUT 12
dislexia@dislexia-VirtualBox:~$
```

*Comprobacion del borrado de normas **13 y 12:***

```
 19  1656 ACCEPT     all  --  lo     any     anywhere             anywhere
  0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:ssh
  0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:http
  0     0 ACCEPT     tcp  --  any    any     anywhere             anywhere             tcp dpt:https
  0     0 ACCEPT     all  --  any    any     192.168.1.0          anywhere
152 18421 DROP       all  --  any    any     anywhere             anywhere
```

Paso 3 – Desactivar cortafuegos y cambios persistentes tras el reset:

*Para desactivar este cortafuegos, simplemente limpie todas las reglas **(-F)** y haga que los cambios sean persistentes.*

```
dislexia@dislexia-VirtualBox:~$ sudo iptables -F
dislexia@dislexia-VirtualBox:~$ sudo /sbin/iptables-save
# Generated by iptables-save v1.8.10 (nf_tables) on Sun Feb  2 19:36:57 2025
*filter
:INPUT ACCEPT [145:26509]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [283:27901]
:ufw-after-forward - [0:0]
:ufw-after-input - [0:0]
:ufw-after-logging-forward - [0:0]
:ufw-after-logging-input - [0:0]
:ufw-after-logging-output - [0:0]
:ufw-after-output - [0:0]
:ufw-before-forward - [0:0]
:ufw-before-input - [0:0]
:ufw-before-logging-forward - [0:0]
:ufw-before-logging-input - [0:0]
:ufw-before-logging-output - [0:0]
:ufw-before-output - [0:0]
:ufw-reject-forward - [0:0]
:ufw-reject-input - [0:0]
:ufw-reject-output - [0:0]
:ufw-track-forward - [0:0]
:ufw-track-input - [0:0]
:ufw-track-output - [0:0]
COMMIT
# Completed on Sun Feb  2 19:36:57 2025
dislexia@dislexia-VirtualBox:~$
```