Informe 7

Laboratorio 7: Firewall

SEGURIDAD DE LA INFORMACIÓN

Mateo Escobar Parra

CC 1.035.443.386

Juan Esteban Lopez Domínguez

CC 1.007.565.845

Universidad de Antioquia

Facultad de Ingeniería

Departamento de ingeniería de telecomunicaciones y electrónica

Medellín, Antioquia

Octubre 26, 2025

Actividad 01: Personal Firewall.

a. Ilustre el procedimiento a realizar para garantizar los siguientes requerimientos de operación en la topología de red sugerida.

- Solamente Alfa puede acceder al servicio WEB de SerTele
- Solamente Beta puede acceder al servicio FTP de SerTele
- Alfa y Gamma pueden acceder al servicio SSH de SerTele
- Todas las estaciones tienen conectividad, PING, con SerTele

Para este numeral se edita el archivo myfw, cuya plantilla inicial se da en la practica.

Ahora se añadieron las siguientes lineas:

- Para que solo ALFA pueda acceder al servicio WEB:

  iptables -A INPUT -i $INT_IF -s $ALFA -p tcp --dport 80 -j ACCEPT

- Para que solo BETA acceda al FTP:

  iptables -A INPUT -i $INT_IF -s $BETA -p tcp --dport 21 -j ACCEPT

- Para que ALFA y GAMMA acceden al SSH:

  iptables -A INPUT -i $INT_IF -s $ALFA -p tcp --dport 22 -j ACCEPT

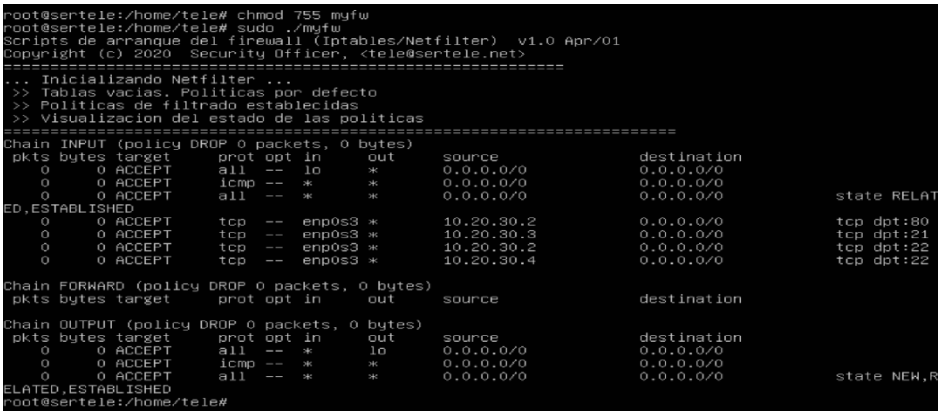
  iptables -A INPUT -i $INT_IF -s $GAMMA -p tcp --dport 22 -j ACCEPT

- Para que todos pueden hacer PING:

  iptables -A INPUT -p icmp -j ACCEPT

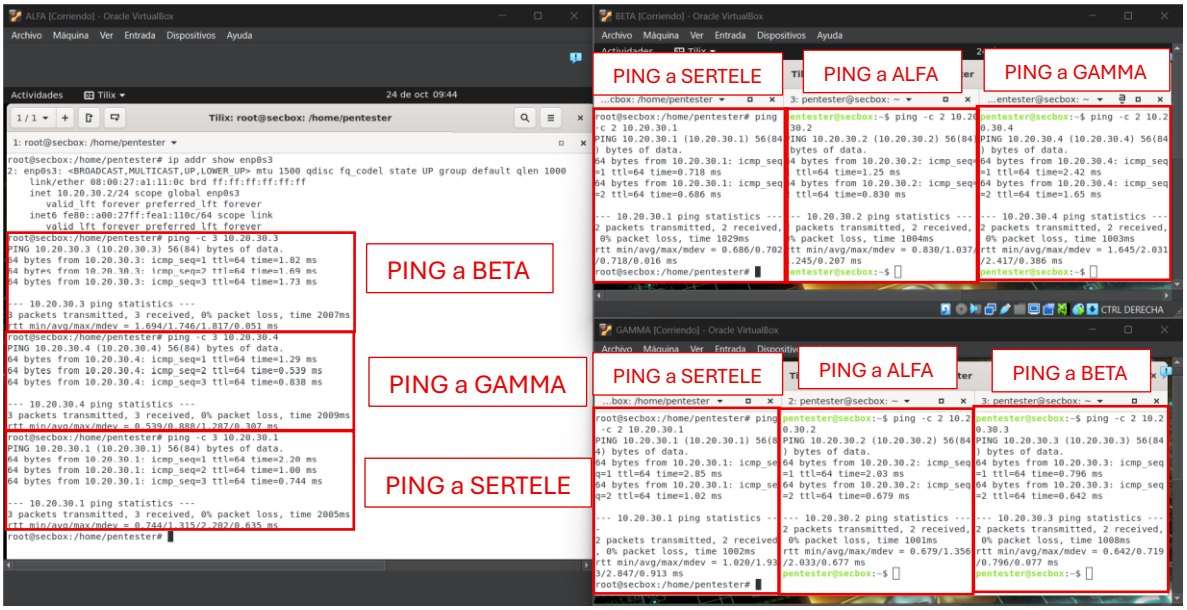
  iptables -A OUTPUT -p icmp -j ACCEPT

- Por ultimo para permitir tanto trafico entrante como saliente se agrego:
  iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
  iptables -A OUTPUT -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT

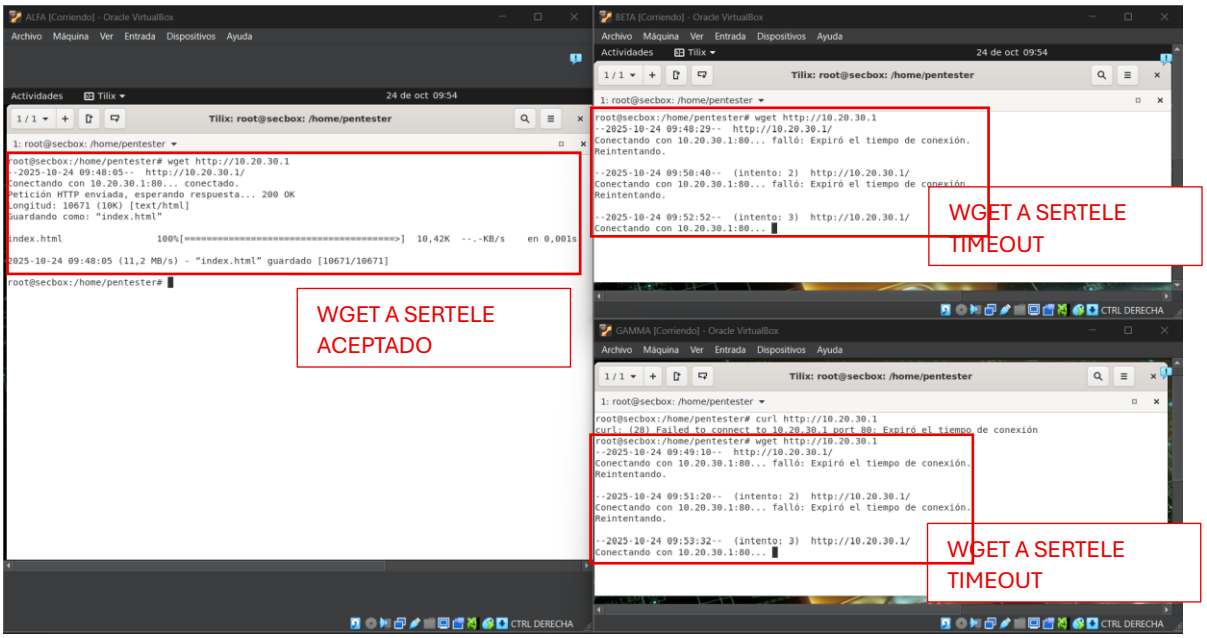


Firewall personal en funcionamiento con iptables cumpliendo todos los requerimientos de operación

- Prueba conexión PING entre ALFA, BETA y GAMMA, y PING al servidor SERTELE (10.20.30.1)

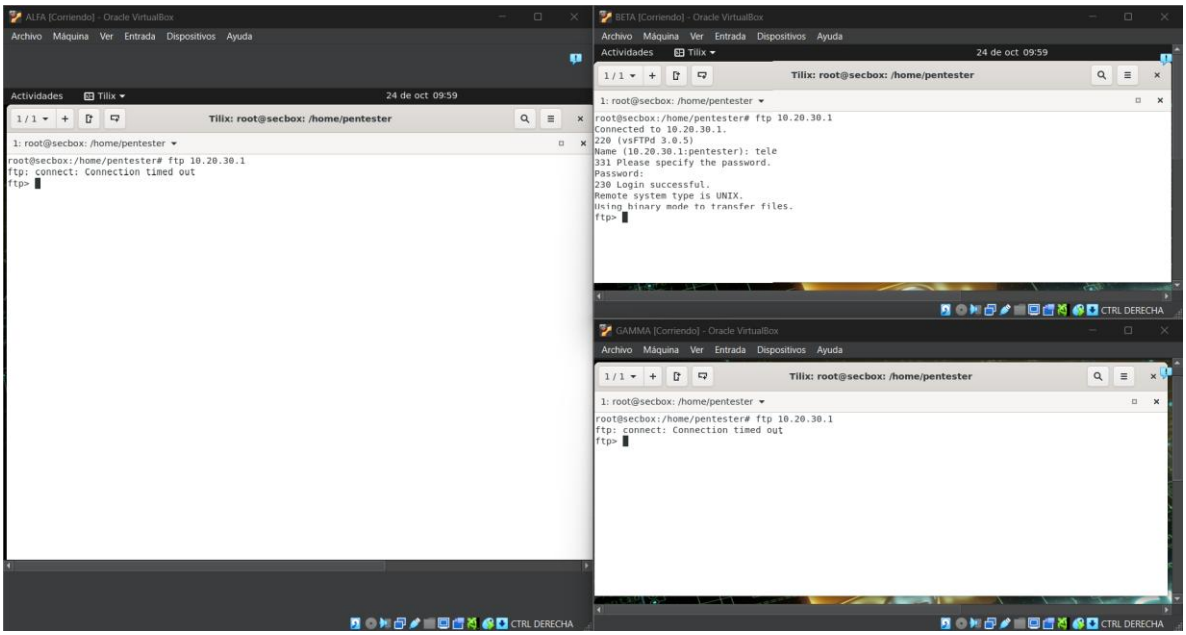


- Captura con wget para acceso al servicio web:



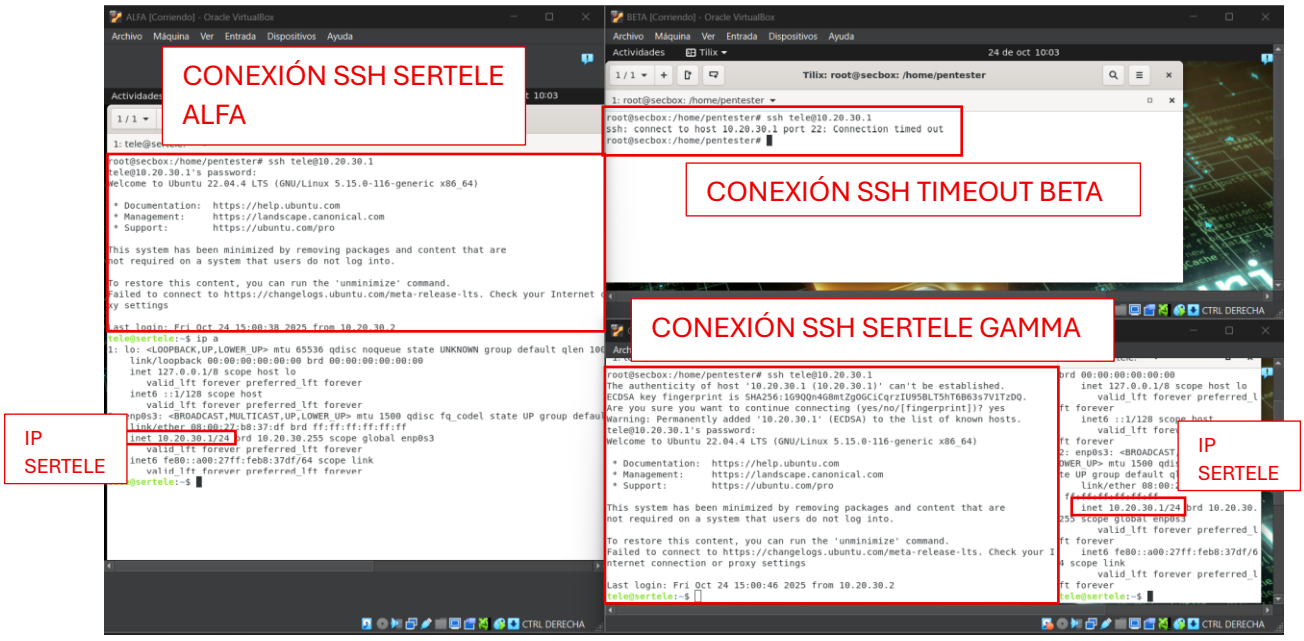
Se puede observar cómo únicamente en la estación ALFA tenemos acceso al servidor web, en las otras 2 estaciones (GAMMA y BETA) aunque se intenta el tiempo de conexión se agota.

- Prueba de acceso al servicio FTP por parte de las 3 estaciones



Se puede observar cómo únicamente en las estación BETA tenemos acceso a FTP, pues nos piden tanto usuario como contraseña, en las estaciones ALFA y GAMMA se acaba primero el tiempo de conexión.

- Prueba de conexión para acceder al servicio SSH de SerTele



Como se ve en la imagen anterior únicamente ALFA Y GAMMA pueden acceder via ssh a SERTELE, y BETA no puede acceder a la conexión.

b. Ilustre el procedimiento a realizar para garantizar los siguientes requerimientos de operación en la topología de red sugerida.

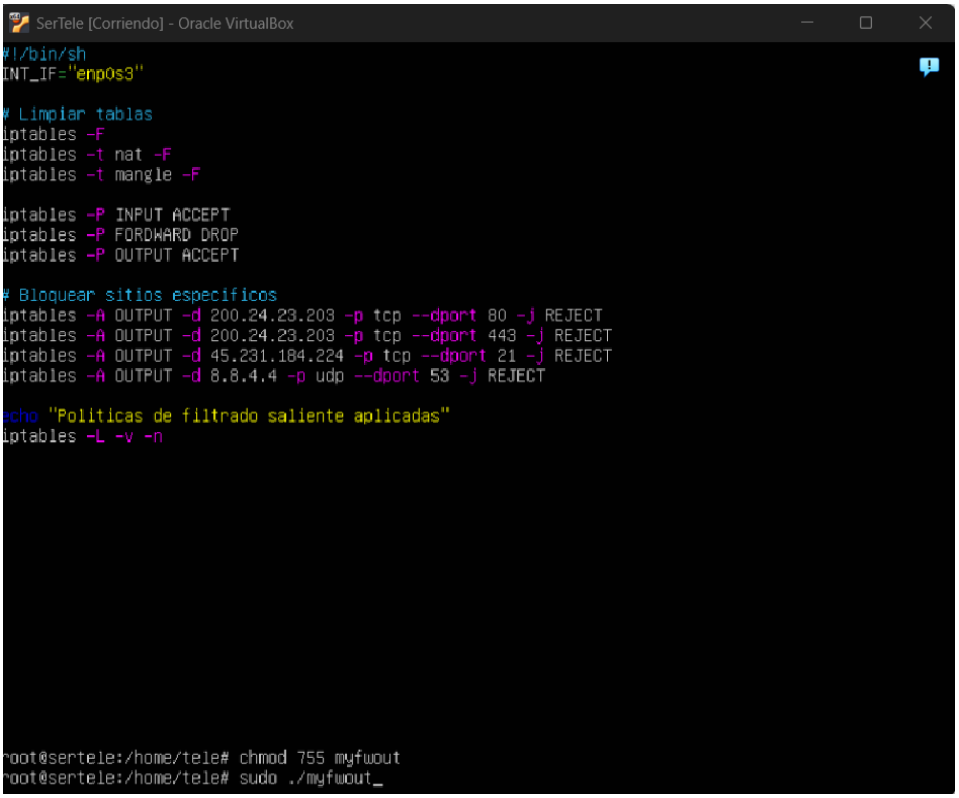
- SerTele no puede acceder al sitio web gita.udea.edu.co
- SerTele no puede acceder al sitio ftp ftp.unicauca.edu.co
- SerTele no puede usar el servidor DNS 8.8.4.4
- SerTele tiene conectividad a Internet y puede acceder cualquier sitio web el servidor.

Para este numeral se creó myfwout, un script que deja la política de salida en ACCEPT salvo excepciones específicas.

- Bloqueo de HTTP/HTTPS hacia gita.udea.edu.co:
  iptables -A OUTPUT -d 200.24.23.203 -p tcp --dport 80 -j REJECT
  iptables -A OUTPUT -d 200.24.23.203 -p tcp --dport 443 -j REJECT

- Bloqueo de FTP hacia ftp.unicauca.edu.co:
  iptables -A OUTPUT -d 45.231.184.224 -p tcp --dport 21 -j REJECT

- Bloqueo de consultas DNS hacia 8.8.4.4:
  iptables -A OUTPUT -d 8.8.4.4 -p udp --dport 53 -j REJECT



```
root@sertele:/home/tele# sudo ./myfwout
iptables: Bad built-in chain name.
Politicas de filtrado saliente aplicadas
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination

Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            200.24.23.203        tcp dpt:80
reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            200.24.23.203        tcp dpt:443
 reject-with icmp-port-unreachable
    0     0 REJECT     tcp  --  *      *       0.0.0.0/0            45.231.184.224       tcp dpt:21
reject-with icmp-port-unreachable
    0     0 REJECT     udp  --  *      *       0.0.0.0/0            8.8.4.4              udp dpt:53
reject-with icmp-port-unreachable
root@sertele:/home/tele# _
```

- Pruebas desde SERTELE con curl y wget para acceder al sitio web gita.udea.edu.co

```
root@sertele:/home/tele# curl gita.udea.edu.co
curl: (7) Failed to connect to gita.udea.edu.co port 80 after 243 ms: Connection refused
root@sertele:/home/tele# wget gita.udea.edu.co
--2025-10-24 16:59:02--  http://gita.udea.edu.co/
Resolving gita.udea.edu.co (gita.udea.edu.co)... 200.24.23.203
Connecting to gita.udea.edu.co (gita.udea.edu.co)|200.24.23.203|:80... failed: Connection refused.
```

Como se puede ver en la imagen anterior la conexión es rechazada.

- Pruebas desde SERTELE para acceder al sitio ftp ftp.unicauca.edu.co

```
root@sertele:/home/tele# ftp ftp.unicauca.edu.co
ftp: Can't connect to `45.231.184.224:21': Bad file descriptor
ftp: Can't connect to `ftp.unicauca.edu.co:ftp'
ftp> exit
```

- Conexión rechazada pues no se puede usar el servidor DNS 8.8.4.4

```
root@sertele:/home/tele# nslookup 8.8.4.4
;; communications error to 8.8.4.4#53: connection refused
;; communications error to 8.8.4.4#53: connection refused
;; communications error to 8.8.4.4#53: connection refused
;; no servers could be reached


root@sertele:/home/tele# _
```

- Prueba de conectividad a Internet y puede acceso a la web.

```
root@sertele:/home/tele# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=39.0 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=27.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=27.0 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=29.0 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 27.045/30.566/39.031/4.948 ms
```

```
root@sertele:/home/tele# wget www.google.com
--2025-10-24 17:05:11--  http://www.google.com/
Resolving www.google.com (www.google.com)... 172.217.30.164, 2800:3f0:4005:40b::2004
Connecting to www.google.com (www.google.com)|172.217.30.164|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/html]
Saving to: 'index.html'

index.html                  [ <=>                                ]  16.99K  --.-KB/s    in 0.02s

2025-10-24 17:05:11 (765 KB/s) - 'index.html' saved [17397]
```

Actividad 02: Firewall de red.

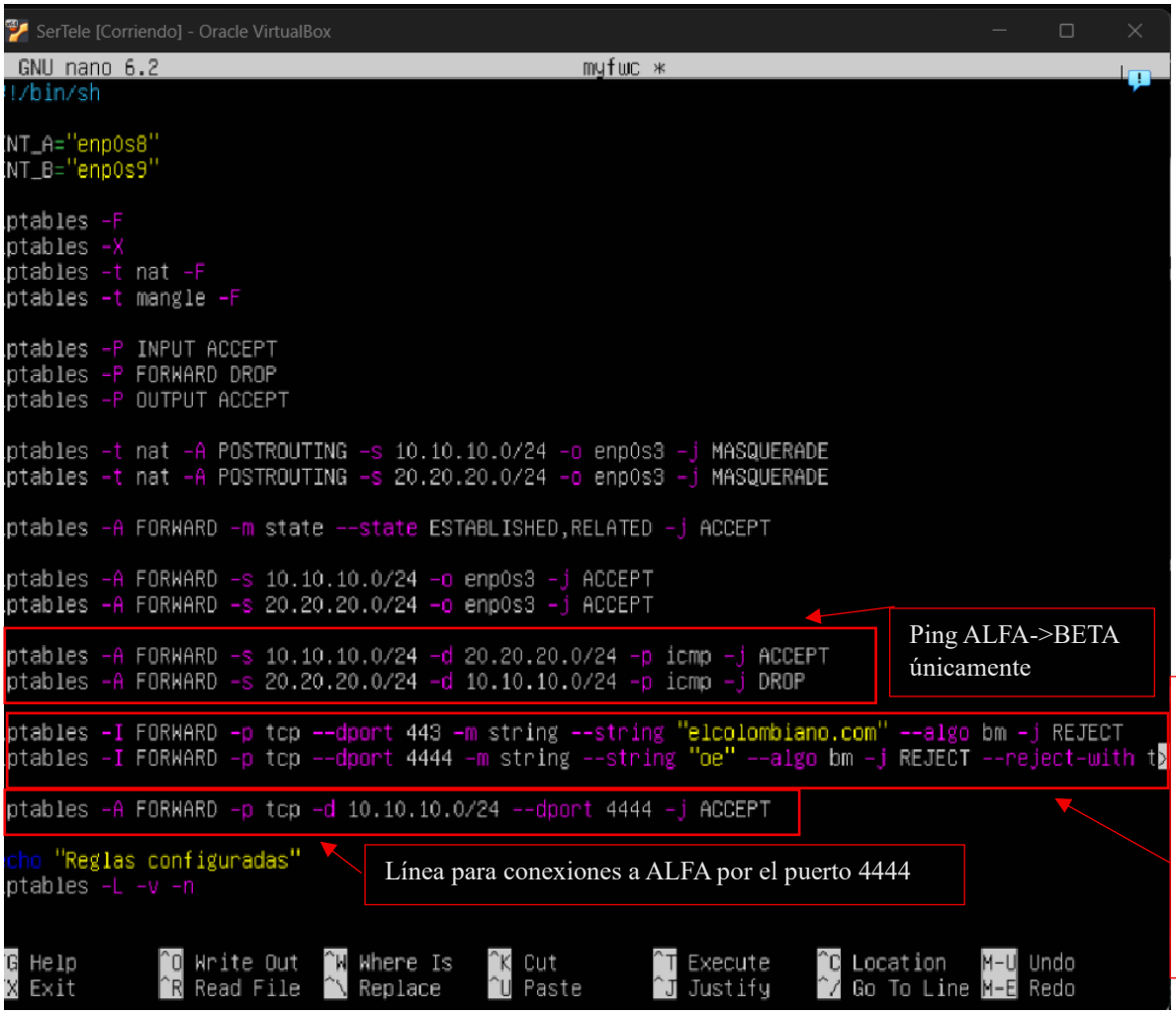
c. Ilustre el procedimiento a realizar para garantizar los siguientes requerimientos de operación en la topología de red sugerida.

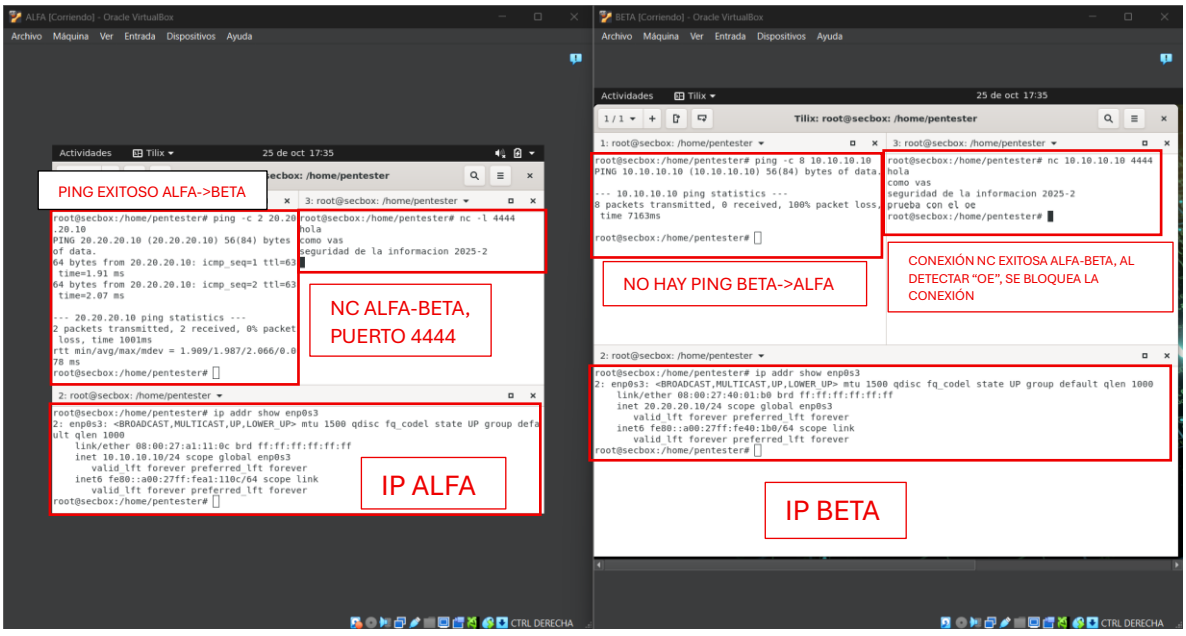
- Alfa puede hacer ping a Beta, pero Beta no puede hacer ping a Alfa
- Alfa puede recibir peticiones de conexión únicamente a su puerto TCP 4444. Es decir, si Alfa ejecutará nc -l 4444 admitiría la conexión, de lo contrario no.
- Si Alfa y Beta establecen una comunicación vía netcat, todos los mensajes que incluyan el texto "oe" serán bloqueados.
- Alfa y Beta pueden acceder cualquier sitio web excepto elcolombiano.

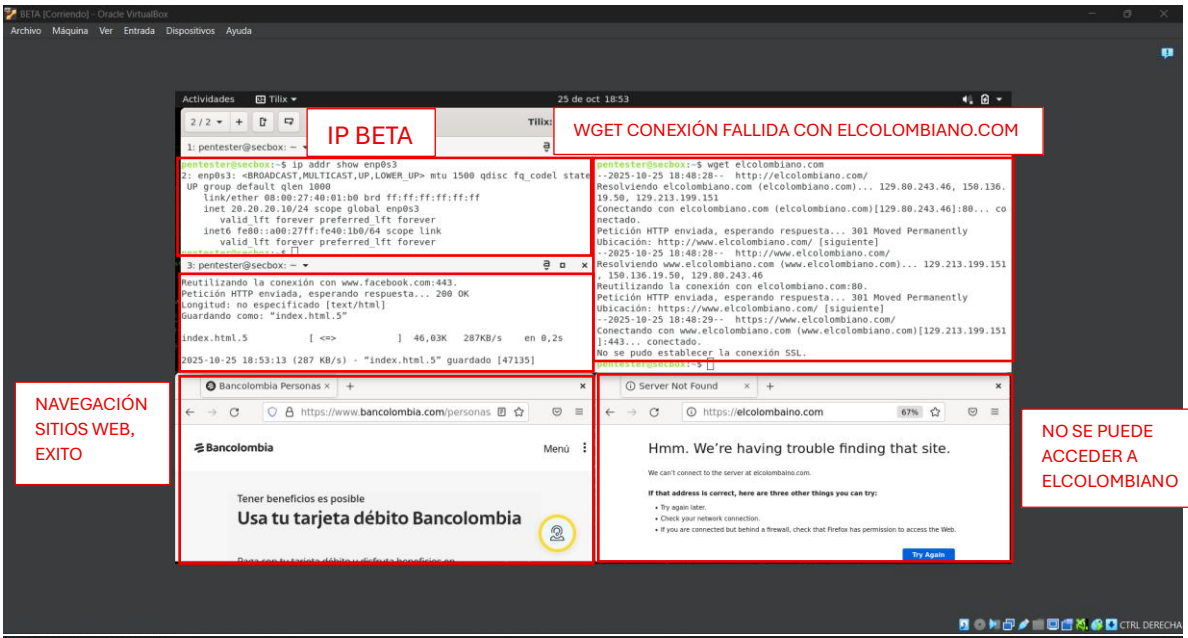
Tenemos tres máquinas virtuales ALFA, BETA Y SERTELE, en donde ALFA tiene un adaptador en modo Red interna (IntA), BETA también con una adaptador en modo red interna pero diferente (IntB) y por ultimo SERTELE que será el firewall y este tendrá 3 adaptadores, el primero es un adaptador puente para la conexión a internet, el segundo tendrá la red interna IntA y el tercero la red interna IntB, para la asignación de las IP, ALFA tendrá la dirección ip 10.10.10.10/24 con Gateway 10.10.10.1, BETA la dirección ip 20.20.20.10 /24 con Gateway 20.20.20.1, y por ultimo SERTELE con 3 adaptadores (enp0s3, enp0s8, enp0s9), de los cuales enp0s3 tendrá ip dada por DHCP, enp0s8 tendrá la ip 10.10.10.1 y enp0s9 la ip 20.20.20.1, como se muestra a continuación.

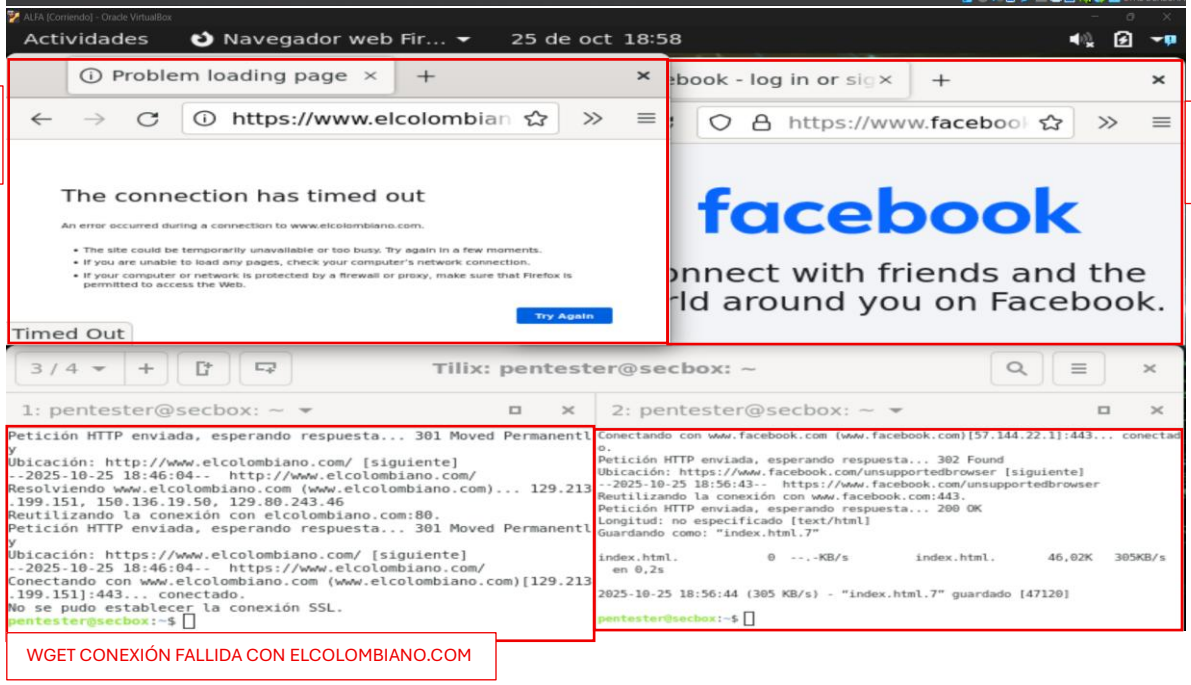
```
root@sertele:/home/tele# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:b8:37:df brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.12/24 brd 192.168.1.255 scope global dynamic enp0s3
       valid_lft 588908sec preferred_lft 588908sec
    inet6 2800:e2:bd80:18da:a00:27ff:feb8:37df/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 604800sec preferred_lft 604800sec
    inet6 fe80::a00:27ff:feb8:37df/64 scope link
       valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:8c:85:bf brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.1/24 scope global enp0s8
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe8c:85bf/64 scope link
       valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 100
0
    link/ether 08:00:27:f3:2a:96 brd ff:ff:ff:ff:ff:ff
    inet 20.20.20.1/24 scope global enp0s9
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fef3:2a96/64 scope link
       valid_lft forever preferred_lft forever
root@sertele:/home/tele# _
```

El script usado para este punto es:






IP BETA
WGET CONEXIÓN FALLIDA CON ELCOLOMBIANO.COM
NAVEGACIÓN SITIOS WEB, EXITO
NO SE PUEDE ACCEDER A ELCOLOMBIANO


NO SE PUEDE ACCEDER A ELCOLOMBIANO
NAVEGACIÓN SITIOS WEB, EXITO
NAVEGACIÓN SITIOS WEB, EXITO
WGET CONEXIÓN FALLIDA CON ELCOLOMBIANO.COM