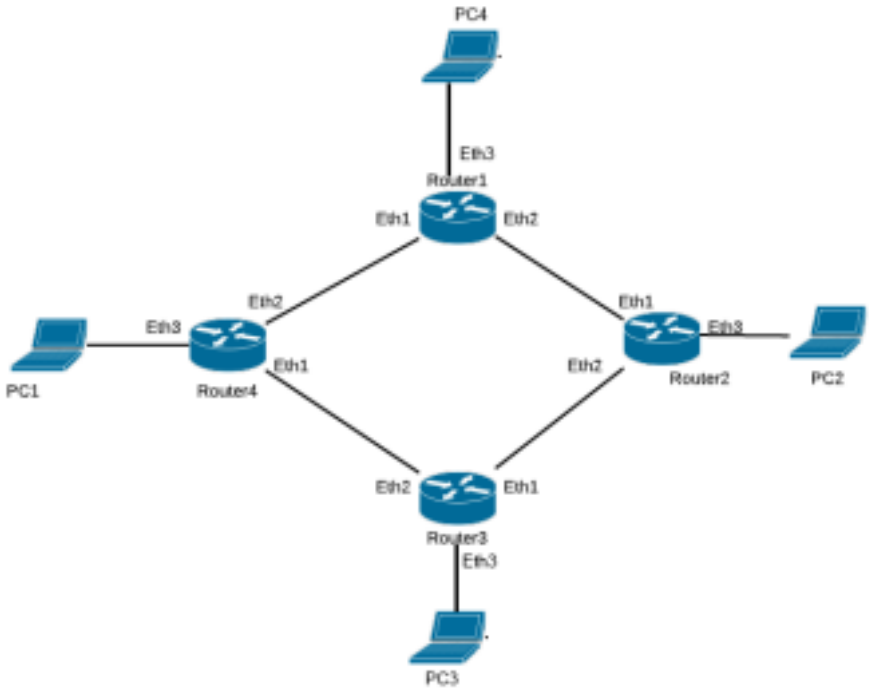
Laboratorio Nº 5

Seguridad

Objetivos:

- Vincular una red mediante la configuración de ruteo dinámico.
- Comprobar conectividad de redes.
- Configurar reglas de firewall.
- Configurar una VPN.
- Hacer uso de comandos aprendidos anteriormente.

Ingeniería de Red



Dispositivo	Interfaz	Dirección IP / Máscara	Gateway Predeterminado
Router 1	Eth1	172.16.0.1/16	No corresponde
	Eth2	172.17.0.1/16	No corresponde
	Eth3	192.168.4.1/24	No corresponde
	Loopback	10.255.255.1 /32	No corresponde
Router 2	Eth1	172.17.0.2/16	No corresponde
	Eth2	172.18.0.1/16	No corresponde
	Eth3	192.168.2.1 /24	No corresponde
	Loopback	10.255.255.2 /32	No corresponde

Router3	Eth1	172.18.0.2/16	No corresponde
	Eth2	172.19.0.1/16	No corresponde
	Eth3	192.168.3.1/24	No corresponde
	Loopback	10.255.255.3 /32	No corresponde
Router4	Eth1	172.19.0.2/16	No corresponde
	Eth2	172.16.0.2/16	No corresponde
	Eth3	192.168.1.1 /24	No corresponde
	Loopback	10.255.255.4 /32	No corresponde
PC 1	NIC	192.168.1.2 /24	192.168.1.1
PC 2	NIC	192.168.2.2 /24	192.168.2.1
PC 3	NIC	192.168.3.2/24	192.168.3.1
PC4	NIC	192.168.4.2/24	192.168.4.1

Configuración de ACL

La finalidad de ejercicio es que se pueda bloquear tráfico entre las distintas redes configurando reglas de firewall.

Tareas a Realizar:

Tarea 1: Conectar una red de acuerdo con el Diagrama de topología.

Tarea 2: Configuración básica de todos los dispositivos.

- Configurar interfaces de acuerdo a la tabla de direccionamiento proporcionada. • Crear y configurar interfaces de loopback.
- Configurar IP en las PCs de la topología.

Tarea 3: Configurar protocolo de ruteo OSPF.

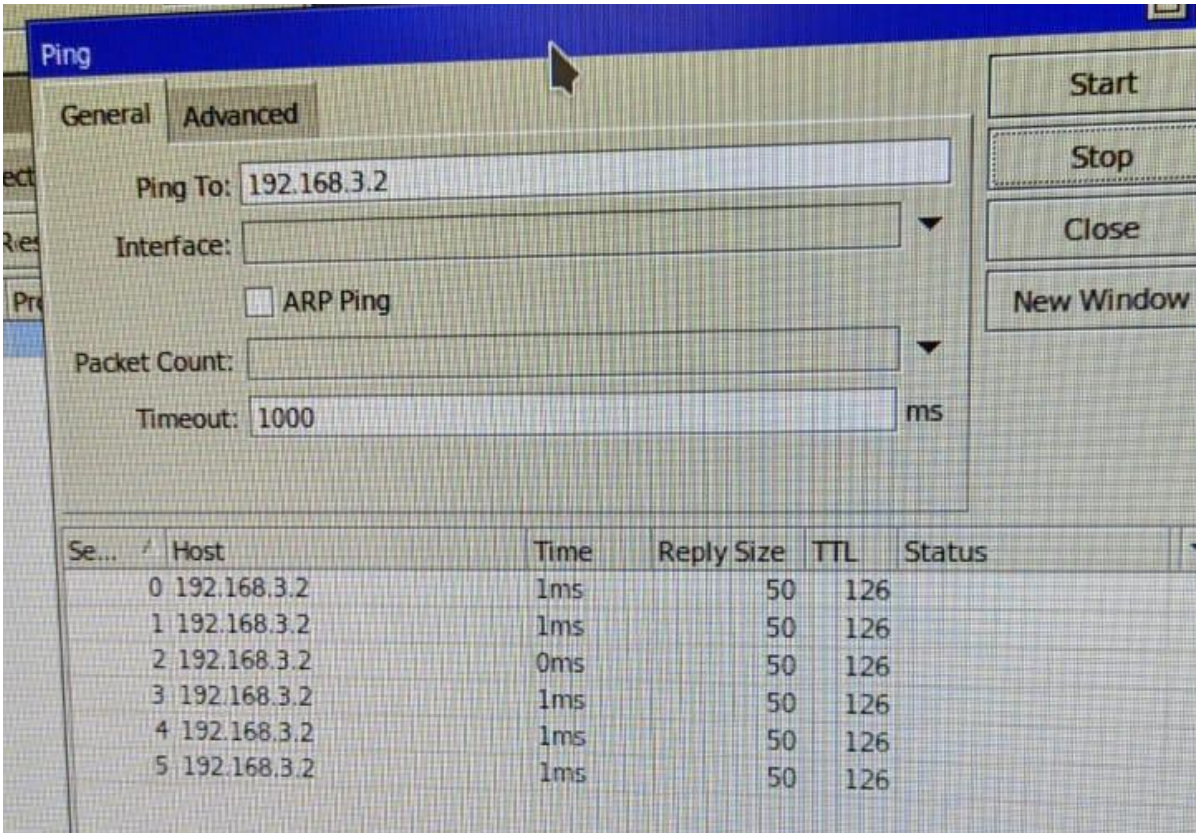
- Configurar ID router.
- Publicar redes que intervienen en el enrutamiento.

Tarea 4: Verificar configuraciones.

- Verificar que las interfaces necesarias estén activas.
- Verificar configuración OSPF.
- Verificar adyacencia con vecinos OSPF.
- Verificar Tablas de Ruteo.
- Mediante el comando PING, verificar que haya comunicación entre todos los dispositivos de la red.

Tarea 5: Configuración de las reglas de firewall.
Configurar las reglas necesarias en los routers correspondientes para que se cumplan las siguientes condiciones:

- Rechazar (Reject) todo el tráfico ICMP desde la PC1 a la PC3.
  - Antes de configurar la regla **hacer una captura del ping ejecutado desde la PC1 a la PC3 para verificar que está funcionando.**

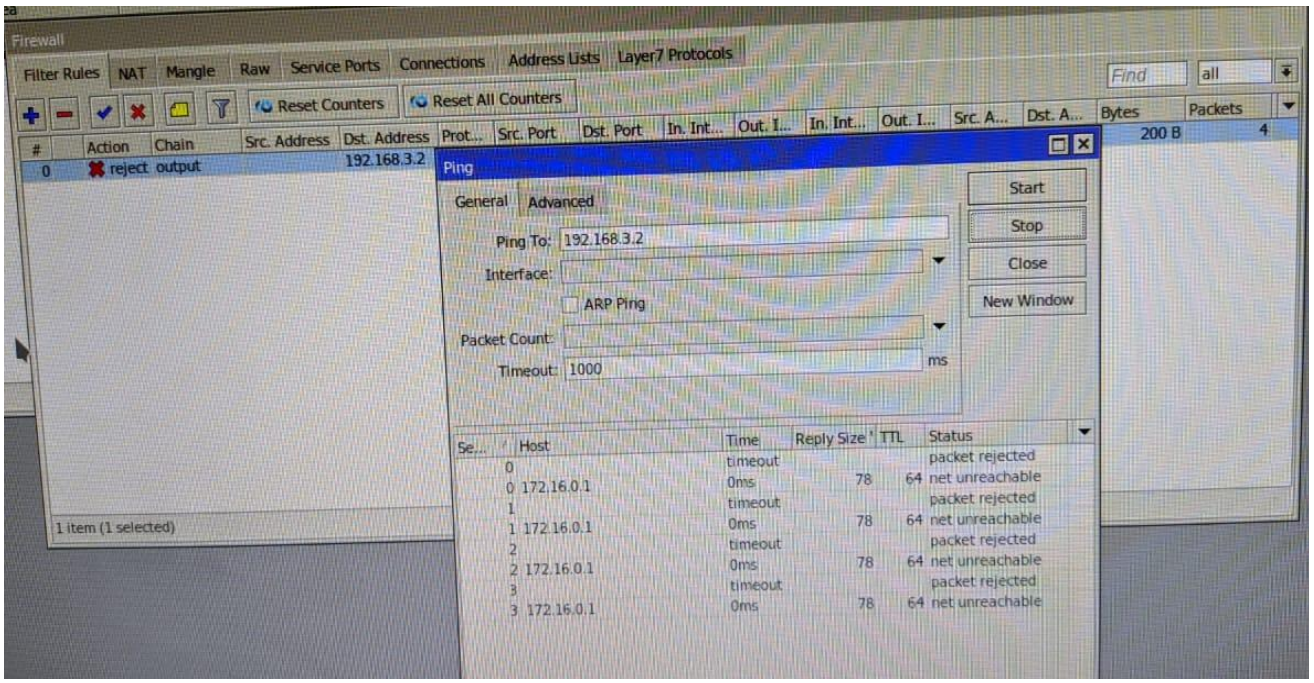


▪ Configurar la regla de firewall en R4 desde IP Firewall.

▪ **Hacer una captura de las ventanas de configuración firewall.**

▪ Una vez configurada la regla, **hacer una captura del resultado del ping desde la PC1 a la PC3.**

Configuracion y Ping rechazado debido al Firewall

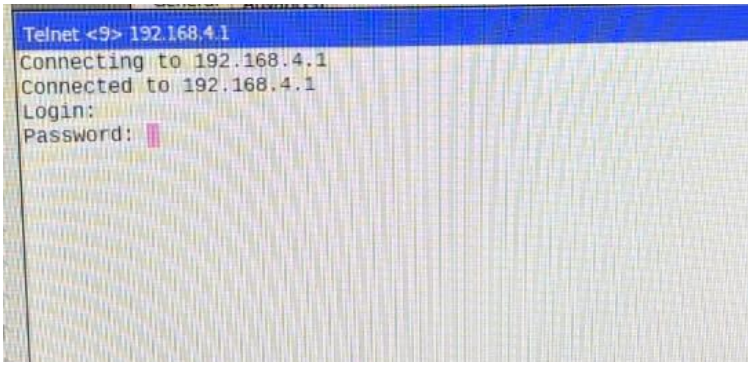


▪ <u>Bloquear todo el tráfico TELNET (protocolo TCP – puerto 23) desde cualquier origen al router R1.</u>

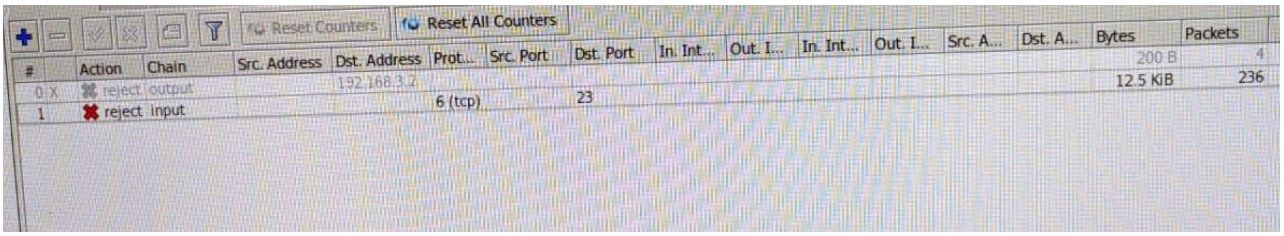
▪ Verificar en cualquier router la conexión por telnet a R1. Tools TELNET ▪

Hacer una captura de pantalla de la conexión telnet al router R1. ▪

Se puede establecer conexion. No se inició sesion para hacerlo.



Configurar la regla de firewall solicitada en R1 desde IP Firewall ▪ **Hacer una captura de las ventanas de configuración firewall.**

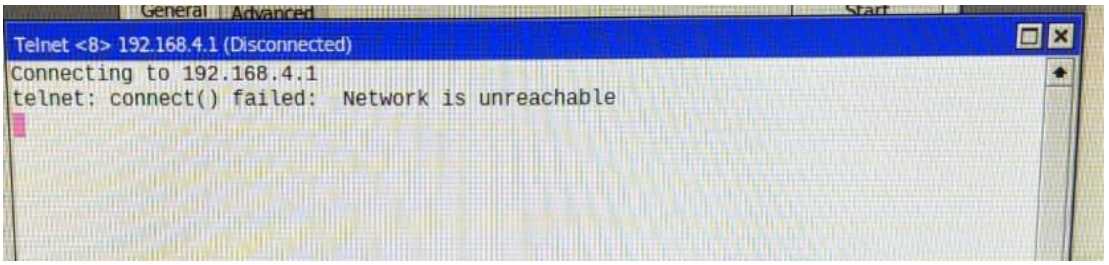


▪ Verificar en todos los routers el funcionamiento de la regla aplicada y probar establecer la conexión TELNET a través de las distintas interfaces de R1.

▪ Mediante el comando PING, verificar que solamente se haya bloqueado el tráfico de telnet.

▪ **Hacer una captura de pantalla del resultado de la conexión telnet a R1 desde el resto de los routers con la regla de firewall activa.**

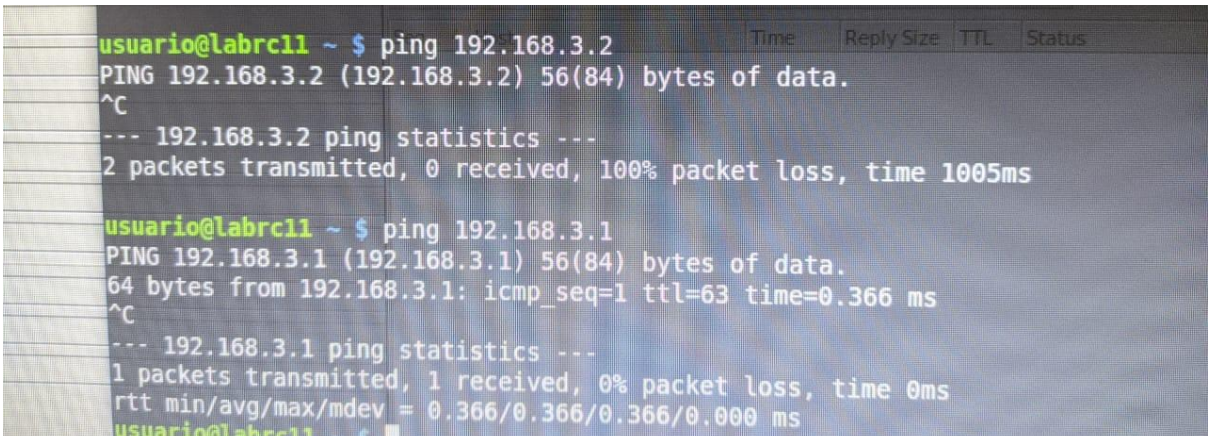
Esta conexion no se puede iniciar debido al firewall.
Muestra el mensaje que se le configuró en la regla.



▪ <u>Bloquear todo el tráfico desde la PC1 a la red 192.168.2.0/24.</u>

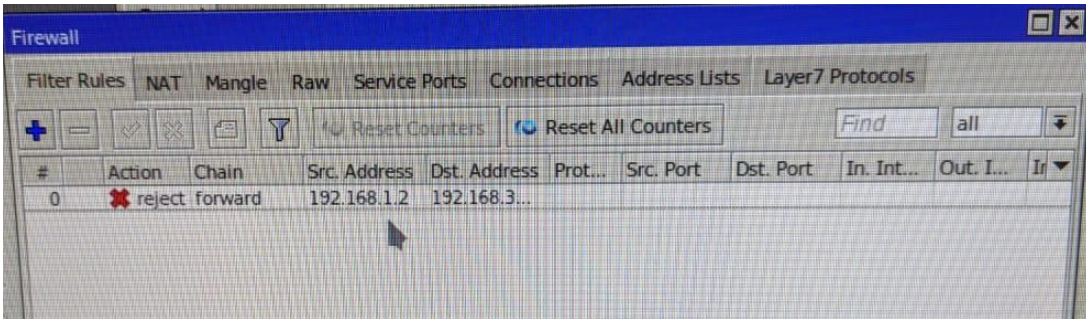
▪ Verificar que se puede hacer ping desde la PC1 a los destinos 192.168.2.1 y 192.168.3.2

▪ **Hacer una captura de pantalla del resultado de los pings.**



▪ Configurar la regla de firewall solicitada en R3 desde IP Firewall ▪

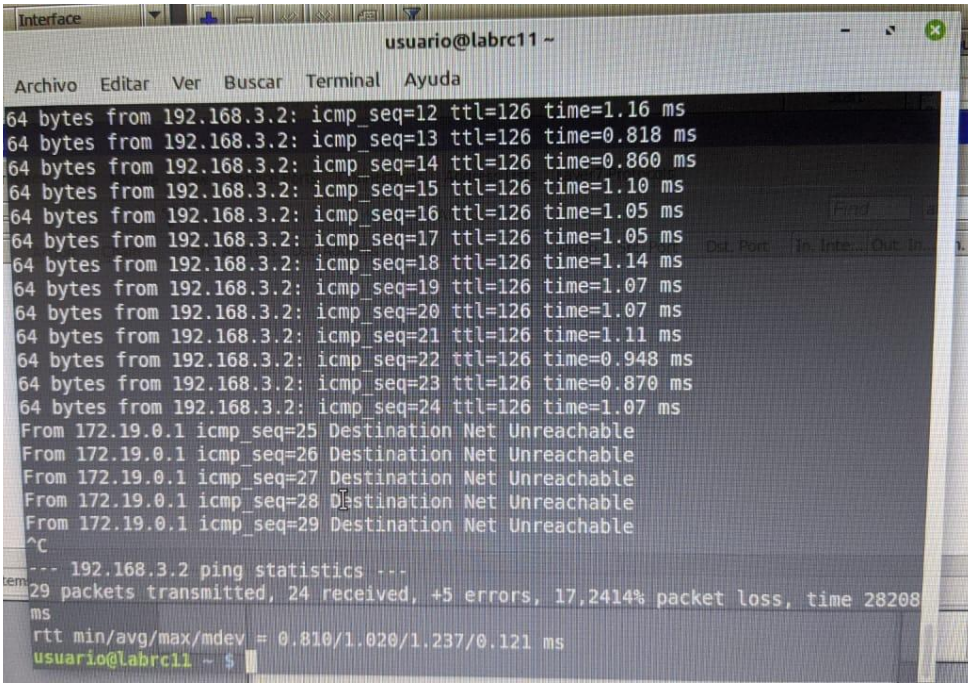
Hacer una captura de las ventanas de configuración firewall.



▪ Mediante el comando PING, verificar en la PC1 el funcionamiento de la regla aplicada.

▪ **Hacer una captura de pantalla del resultado de los pings ejecutados desde la PC1 a los destinos 192.168.2.1 y 192.168.2.2**

Se ejecutó el comando ping y mientras se enviaban los paquetes se puso en marcha la regla del firewall para el rechazo.



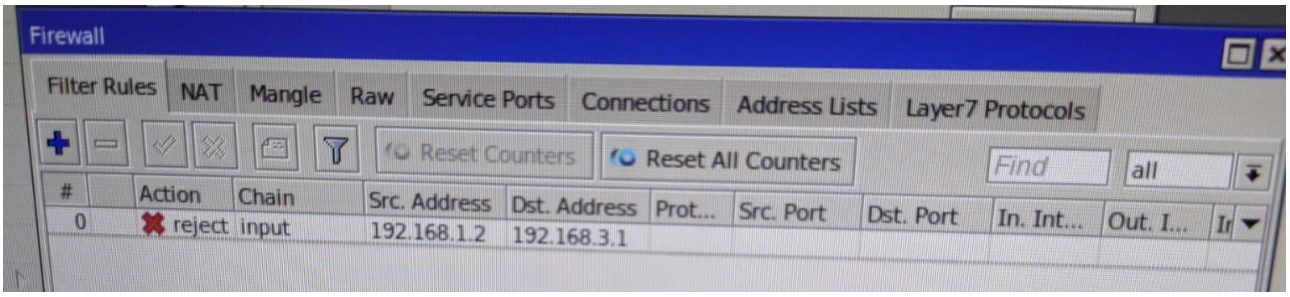
▪ Rechazar todo el tráfico ICMP desde la PC4 a la IP 192.168.3.1 (Interfaz del Router 3).

▪ Verificar que se puede hacer ping desde la PC4 al destino 192.168.3.1.

▪ **Hacer una captura de pantalla del resultado del ping.**

▪ Configurar la regla de firewall solicitada en R3 desde IP Firewall

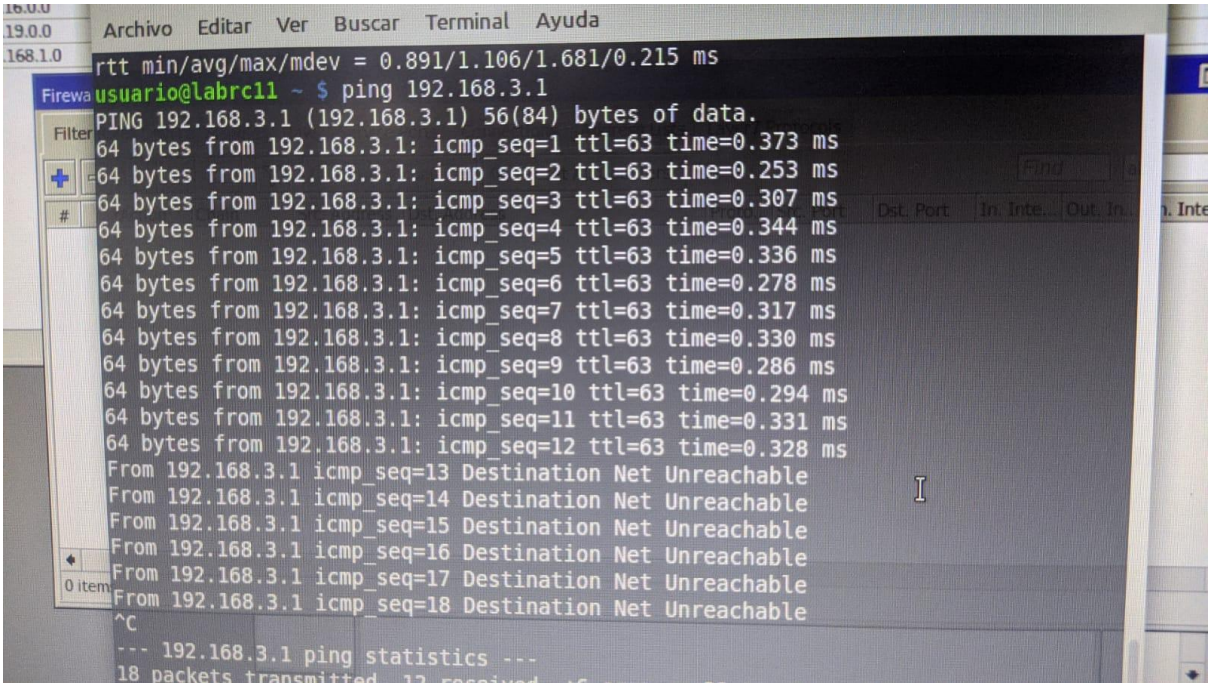
▪ **Hacer una captura de las ventanas de configuración firewall.**



▪ Mediante el comando PING, verificar en la PC2 el funcionamiento de la regla aplicada

▪ **Hacer una captura de pantalla del resultado del ping ejecutado desde la PC2 al destino 192.168.3.1**

Ping funcionando hasta que se activa la regla del firewall.



Configuración de una VPN

La finalidad de ejercicio es que se puedan traficar datos desde 2 PC de redes diferentes usando una VPN.

Tareas a Realizar:

Tarea 1: ELIMINAR TODAS LAS ACL DE LOS ROUTERS Y DESACTIVAR EL PROTOCOLO OSPF.

Tarea 2: Configuración del servidor VPN (Router1).

- Hacer clic en la opción PPP.
- Seleccionar la opción L2TP Server.
- Seleccionar la opción “Enable”, configurar los parámetros y hacer clic en “OK". ○
  - Default Profile: default-encryption
  - Use IPsec: required
  - IPsec Secret: 1234
- Dirigirse a la pestaña “Secrets” y hacer clic en “+” para agregar una conexión al servidor PPTP.
- Configurar los siguientes parámetros y hacer clic en “OK”:
  - Name: user
  - Password: 1234
  - Service: l2tp
  - Profile: default-encryption
  - Local Address: 10.0.0.1
  - Remote Address: 10.0.0.2

Tarea 3: Configuración del cliente VPN (Router2).

- Hacer clic en la opción PPP.
- Seleccionar la pestaña “Interface” y hacer clic en “+” para agregar una interfaz. ▪ Configurar los siguientes parámetros en la pestaña “General”:
  - Name: VPN.
  - Type: L2TP Client.
- Configurar los siguientes parámetros en la pestaña “Dial Out” y hacer clic en “OK”: ○
  - Connect to: 172.17.0.1
  - User: user
  - Password: 1234
  - Profile: default-encryption
  - Use IPsec habilitado
  - IPsec Secret: 1234

Tarea 4: Comprobación del túnel (ambos routers).

- Una vez que el túnel esté activo, se verá en la ventana de “IP Address” que se asignaron las direcciones IP a cada extremo del Tunnel “Server-Client”.

Tarea 5: Routear el tráfico por el túnel (ambos routers).

Se hará que el tráfico entre las redes 192.168.2.0/24 y 192.168.4.0/24 circule por el túnel.

- Hacer clic en la opción IP->Routes.
- Hacer clic en “+” para agregar una nueva ruta estática, configurar los parámetros correspondientes y hacer clic en “OK”.
  - Para el Router1: Dst. Address: 192.168.2.0/24 y Gateway: 10.0.0.2
  - Para el Router2: Dst. Address: 192.168.4.0/24 y Gateway: 10.0.0.1

Tarea 6: Comprobar el funcionamiento de la VPN.

- Realizar pruebas de conectividad entre los host usando el comando ping y traceroute.

Se puede observar que la conexion fue establecida con exito ya que se ejecuta el comando ping. Ademas podemos ver la actividad desde las columnas Tx y Rx del servidor vpn.