



# Práctica 1 – Entregable

---

## Información básica y requisitos para la entrega de las tareas

- 1) Ser concisos y breves en la respuesta a cada tarea.
- 2) Ceñirse al espacio dedicado para cada tarea.
- 3) No olvidar escribir el nombre de cada integrante de la pareja y la isla en donde normalmente trabaja la pareja.
- 4) No se evaluarán tareas que ya se evaluaron en el laboratorio.
- 5) Adaptar el escenario virtualizado a la isla en donde normalmente trabaja la pareja.

**Pareja:** Leire Requena y Clara M.<sup>a</sup> Romero

**Isla:** 4, puestos 3 y 4

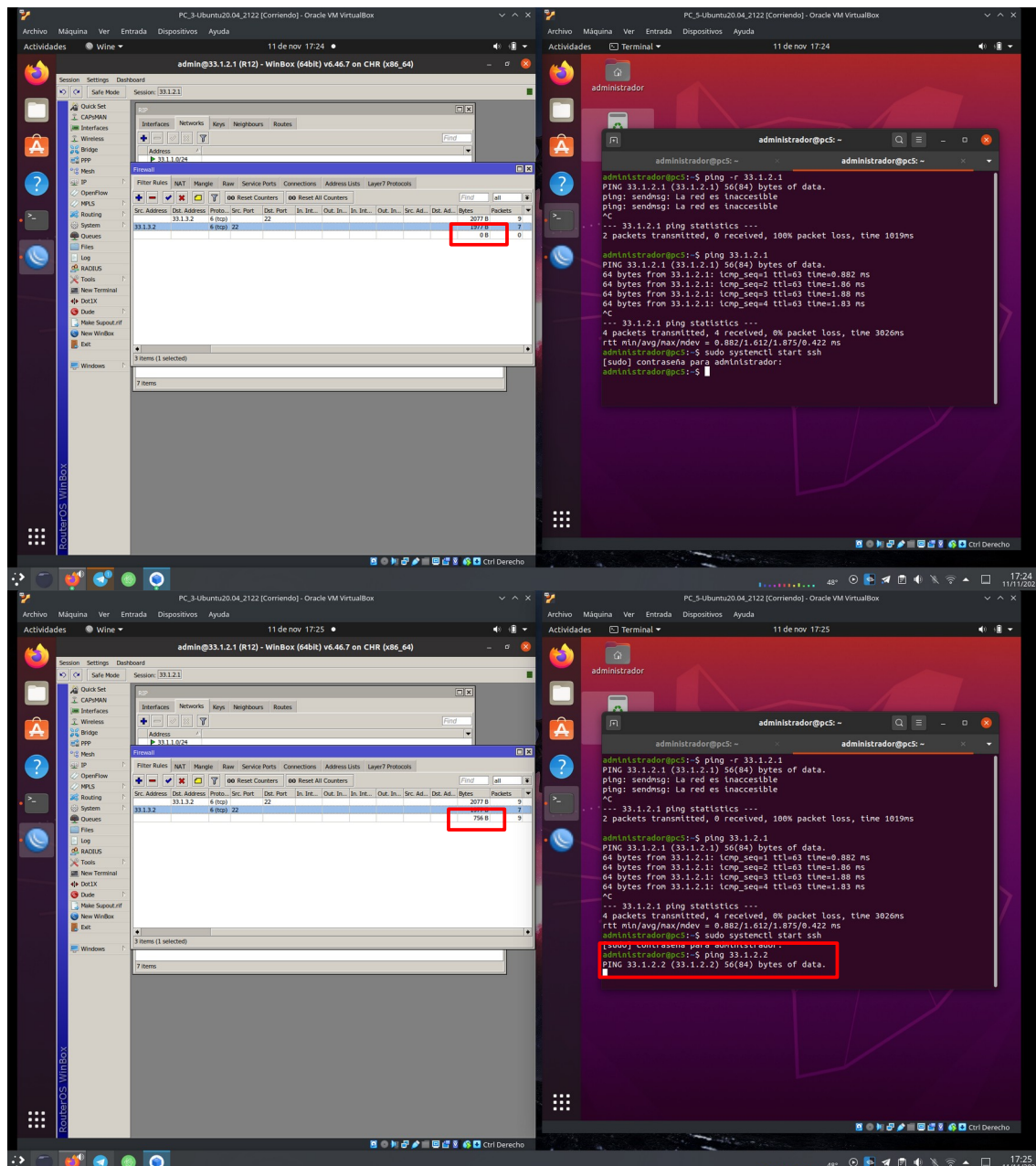
**Tarea a evaluar:** configuración de un *firewall*

## Realización práctica

### Cortafuegos

1) Configure su *router*, el que está directamente conectado a su subred, para que **NO** reenvíe ningún tipo de tráfico (acción "*drop*"). Habitualmente, al configurar un cortafuegos, inicialmente se deniega el reenvío de todo el tráfico, y luego se añaden reglas explícitas para el tráfico que sí se desea dejar pasar. Compruebe que ahora no es posible enviar o recibir tráfico entre los PC ubicados en diferentes subredes.

Como vemos en la parte resaltada de estas capturas, cuando hacemos ping fuera del ssh los paquetes hacen drop (ver el contador de bytes)



The screenshots show a virtual network setup in Oracle VM VirtualBox. The left column displays the configuration of a router (WinBox) for the 33.1.2.1 interface. The right column shows terminal outputs from a host (33.1.2.1) and a guest (33.1.2.2) performing ping tests.

**Router Configuration (WinBox):**

Filter Rules	NAT	Raw	Service Ports	Connections	Address Lists	Layer7 Protocols
33.1.2	4 (log)	22				
33.1.2	4 (log)	22				
33.1.2	4 (log)	22				

**Terminal Outputs:**

```

administrador@pc3: ~$ ping -r 33.1.2.1
PING 33.1.2.1 (33.1.2.1) 56(84) bytes of data.
ping: sending: La red es inaccesible
ping: sending: La red es inaccesible
^C
--- 33.1.2.1 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1019ms

administrador@pc3: ~$ ping 33.1.2.1
PING 33.1.2.1 (33.1.2.1) 56(84) bytes of data.
64 bytes from 33.1.2.1: icmp_seq=1 ttl=63 time=0.882 ms
64 bytes from 33.1.2.1: icmp_seq=2 ttl=63 time=1.86 ms
64 bytes from 33.1.2.1: icmp_seq=3 ttl=63 time=1.88 ms
64 bytes from 33.1.2.1: icmp_seq=4 ttl=63 time=1.83 ms
^C
--- 33.1.2.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3026ms
rtt min/avg/max/mdev = 0.882/1.612/1.875/0.422 ms
administrador@pc3: ~$ sudo systemctl start ssh
[sudo] contraseña para administrador:
administrador@pc3: ~$

administrador@pc3: ~$ ping 33.1.2.2
PING 33.1.2.2 (33.1.2.2) 56(84) bytes of data.

```



2) A continuación, configure el cortafuegos de su *router* para que permita a otros ordenadores conectarse únicamente al servidor de SSH instalado en uno de los PCs de su red (ver Figura 3).

Desde el PC3 nos conectamos via SSH al PC5. Podemos ver como la cuenta de Bytes en los forward aumenta.

