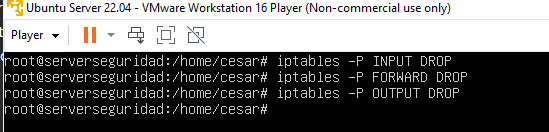
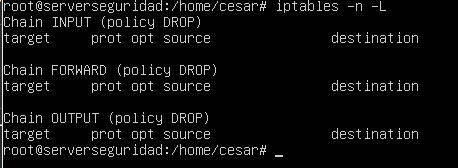
**Configuración de NAT en Iptables y ufw.**

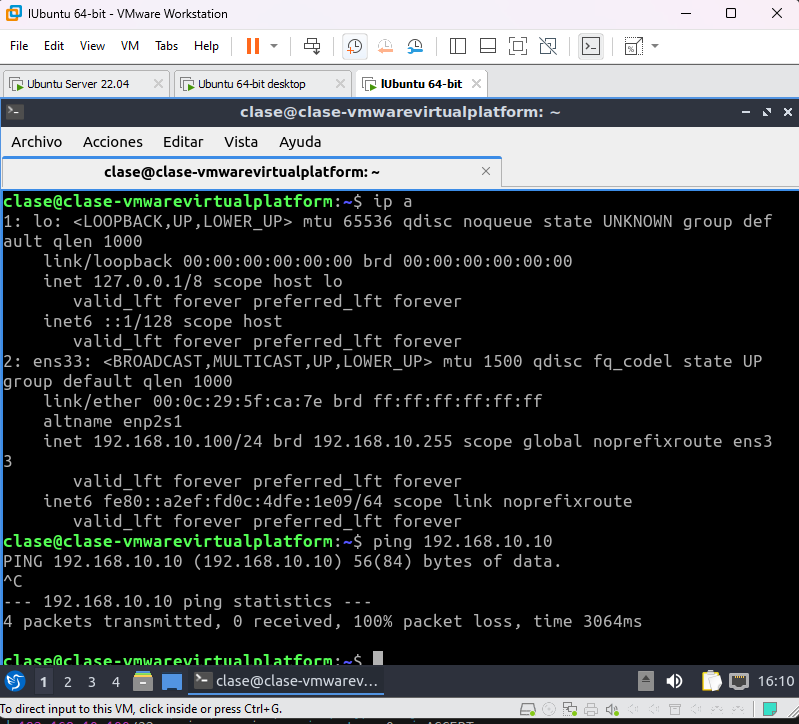
NAT con iptables.

Lo primero será establecer las póliticas por defecto que debe seguir iptables cuando reciba un paquete.

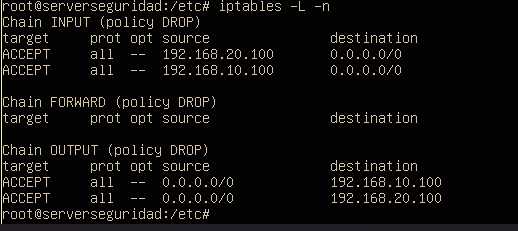


A continuación vamos a listar las reglas iptables que tenemos actualmente, es decir ninguna, para comprobar que las políticas por defecto efectivamente están en drop.

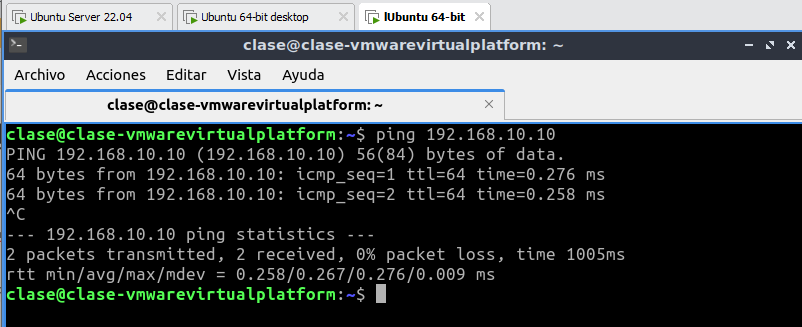


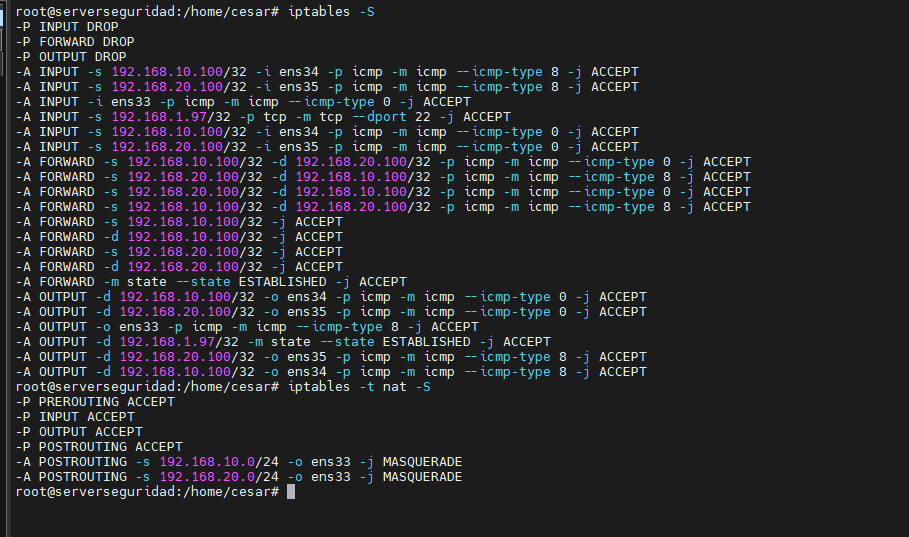
Si ahora probamos a hacer ping desde una maquina cliente al servidor con la ip en su misma subred, comprobaremos que no esta llegando el icmp.

Para ello hay que permitir el ping al servidor desde cada una de las máquinas, haciendo uso de las cadenas INPUT y OUTPUT.



Podemos ver que ahora el ping se realiza correctamente.



Ahora vamos a permitir el ping entre clientes en diferentes subredes mediante la cadena de FORWARD.(el comando iptables está omitido porque es una captura del iptables -S)

Pero el comando original es el siguiente:

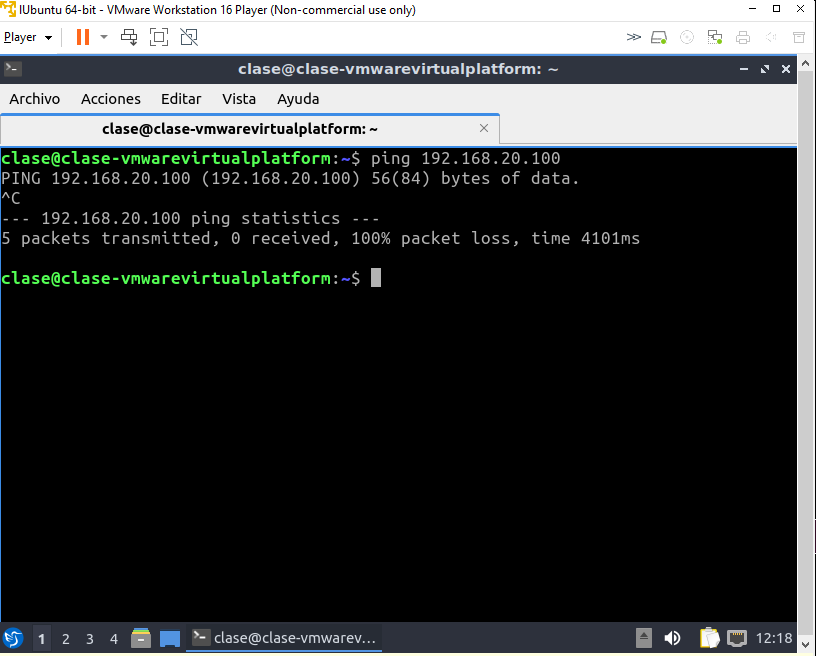
iptables -I FORWARD -p icmp --icmp-type echo-request -s 192.168.10.100/32 -d 192.168.20.100/32 -j ACCEPT

iptables -I FORWARD -p icmp --icmp-type echo-reply -d 192.168.10.100/32 -s 192.168.20.100/32 -j ACCEPT

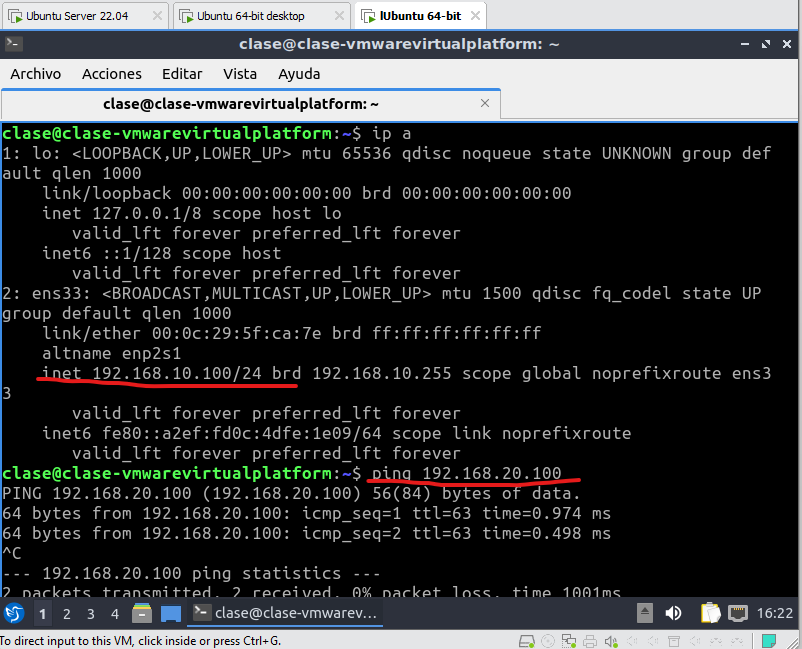
iptables -I FORWARD -p icmp --icmp-type echo-request -d 192.168.10.100/32 -s 192.168.20.100/32 -j ACCEPT

iptables -I FORWARD -p icmp --icmp-type echo-reply -s 192.168.10.100/32 -d 192.168.20.100/32 -j ACCEPT

Si probamos a hacer ping antes de configurar el FORWARD, veríamos que no funciona.



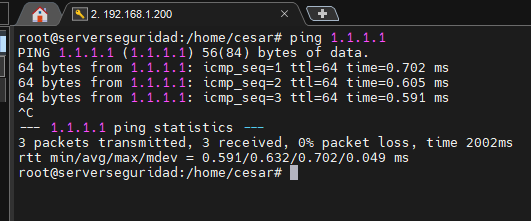
Pero después de incluir las reglas, sí.



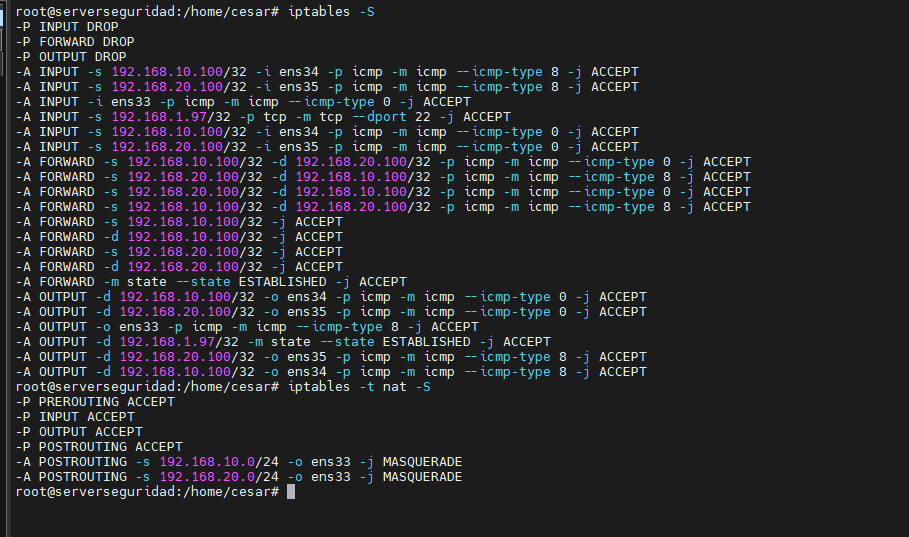
Por último solo falta tener conectividad a internet.Para ello usaremos la cadena FORWARD de la tabla filter y la cadena POSTROUTING de la tabla nat.



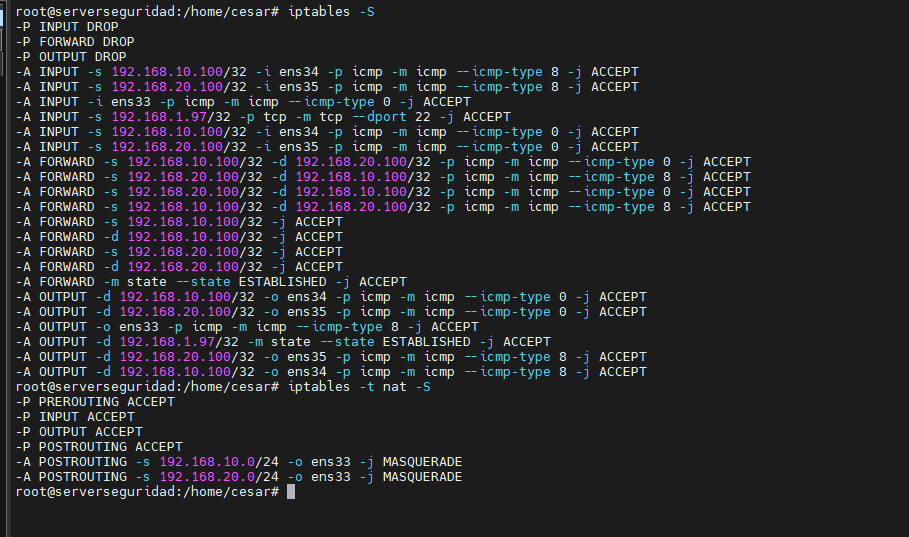
Esto sirve para permitir el ping del servidor a internet.



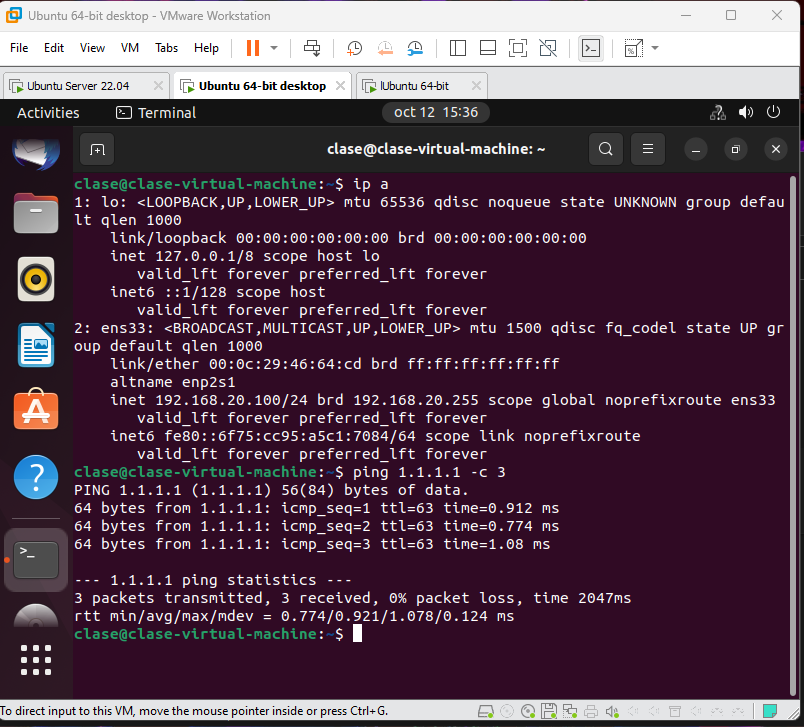
Pero permitir el tráfico web de un cliente requiere mas ordenes(el comando iptables está omitido porque es una captura del iptables -S).

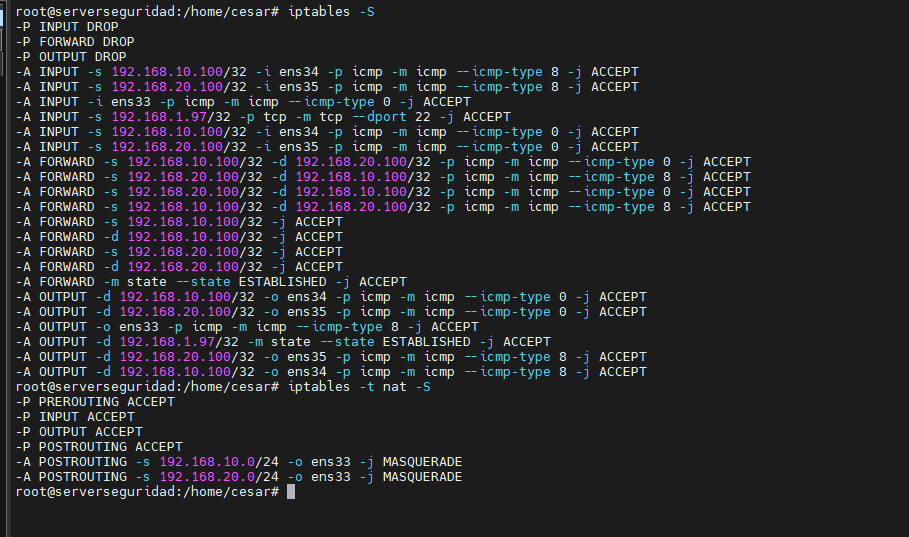


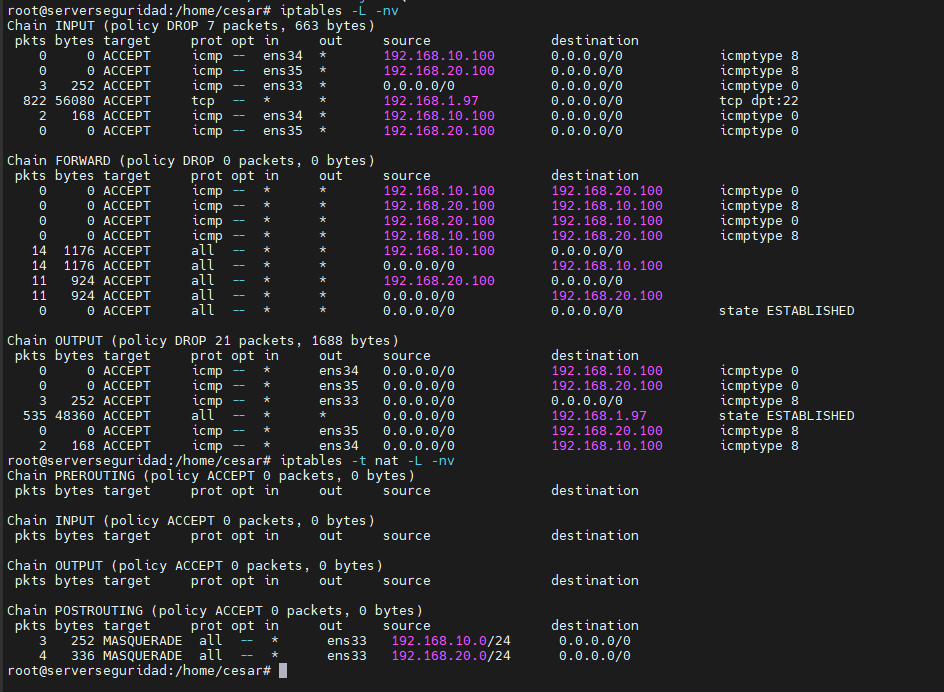
Aquí hemos permitido el paso de cualquier red con origen o destino las ips de los clientes. Pero aun falta convertir las ips privadas de los clientes a la ip publica de internet del router.  
Dado que la ip publica no es estática y depende de nuestro proveedor telefónico, vamos a usar enmascaramiento(el comando iptables está omitido porque es una captura del iptables -S).

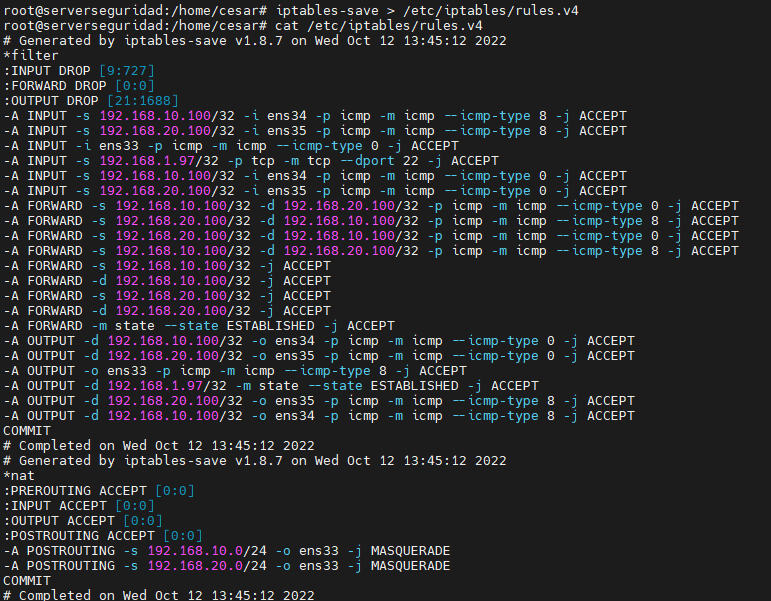


Ahora ya sí, podemos hacer ping a internet y navegar sin problema desde nuestros clientes.

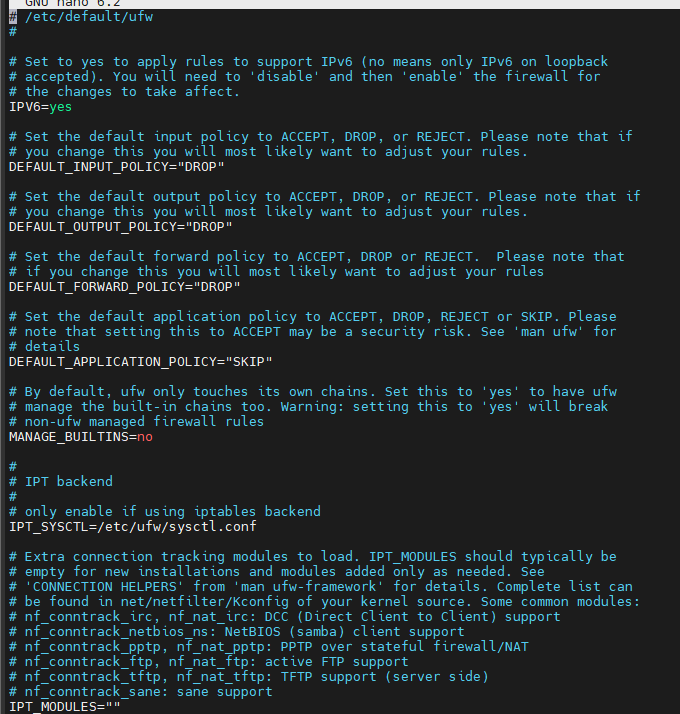


Aquí dejo un par de capturas con todos los comandos usados y las diferentes tablas.

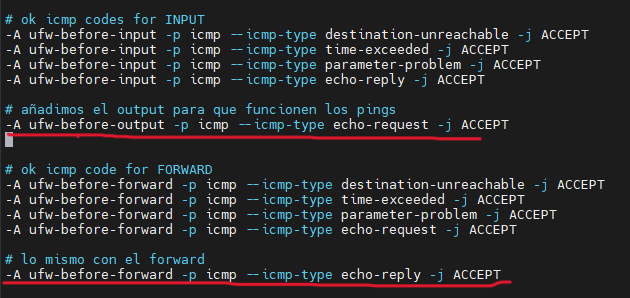


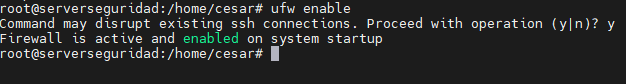
Para guardas las normas iptables es tan sencillo como crear un fichero /etc/iptables y redirigir las tablas actuales a un archivo en ese fichero, luego, tras reiniciar elv servidor,bastará con hacer un iptables restore y listo.

NAT con ufw.

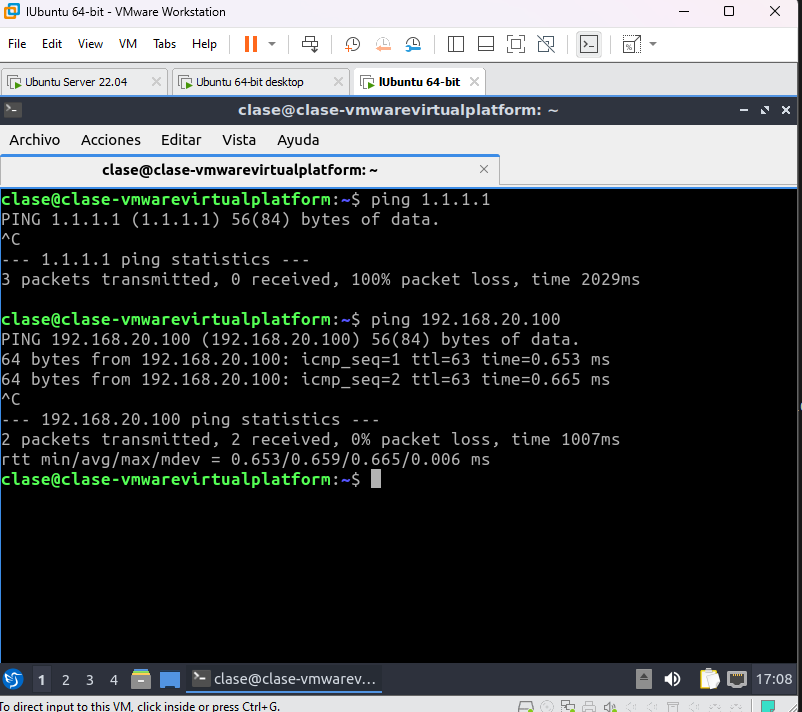
Lo primero es acceder al archivo con las politicas por defecto de ufw. Podemos comprobar que están en drop.

Ahora accedemos a las before rules y terminamos de arreglar el fichero para permitir los pings tanto entre clientes como a internet.

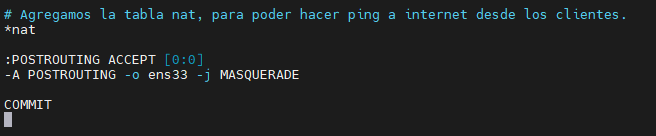


Habilitamos el servicio ufw.

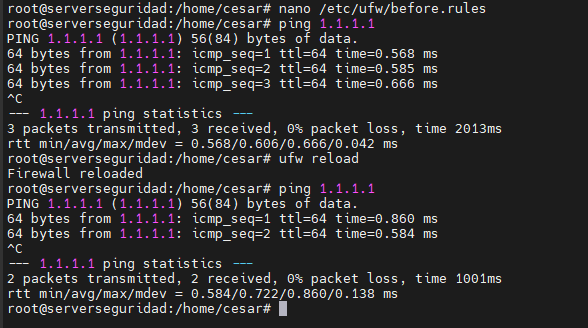
Vemos que no hay ping a internet pero si entre clientes, justo cómo hemos establecido.

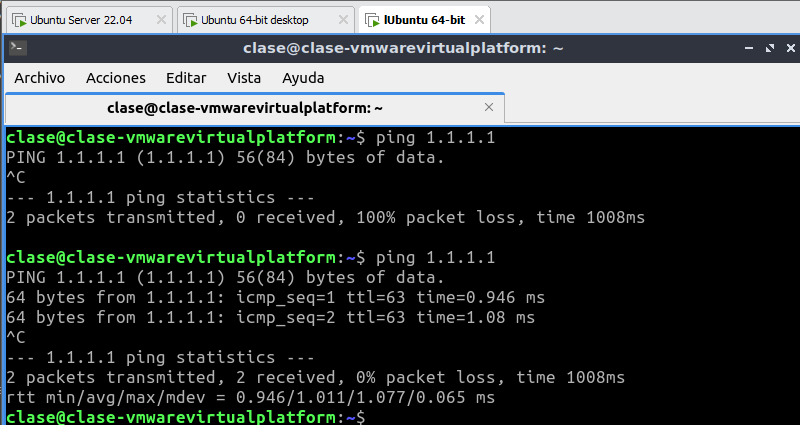


Ahora añadimos la tabla nat, con su correspondiente regla.

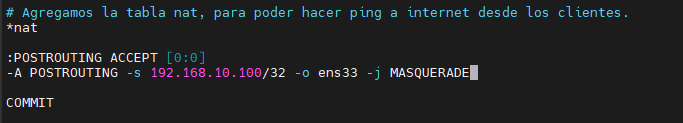


Vemos que ya tenemos conexión icmp a internet.

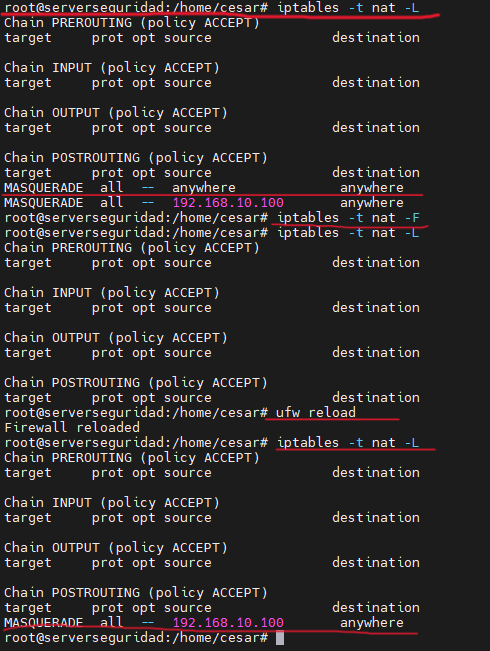




Pero supongamos que queremos ser más específicos y permitir solo el trafico a internet de una de las redes. En ese caso lo que habría que hacer es especificar el origen en la regla nat.



Pero hay que tener cuidado de borrar las tablas nat de iptables porque aunque cambiemos la configuración de ufw la de iptables se mantiene y puede darnos problemas.



Si vamos a la máquina cliente de la subred 192.168.20.0/24, vemos que efectivamente ya no tiene acceso a internet.

