“Universidad Internacional de La Rioja en México”

Seguridad en Redes y Análisis Inteligente de Amenazas

Proyecto:

Actividad individual 1: Mecanismos de defensa en redes

Profesor:

Dr. Carlos Ramiro Soria Cano

Autor:

Ing. Juan Luis Cruz Aristeo

Fecha de entrega:

11/11/2024

Índice

Introducción

En la actualidad la seguridad en las redes es uno de los aspectos más importantes y críticos para proteger, pues por este medio se transmite todo tipo de información, por lo tanto, la confidencialidad y la integridad de los datos es de vital importancia, ya que el creciente aumento de ataques cibernéticos ha demostrado la necesidad de contar con sistemas de seguridad robustos, todo esto con el objetivo de prevenir y mitigar posibles vulnerabilidades en las diferentes partes que componen los sistemas, entre estos las redes.

En este contexto, el siguiente proyecto tiene por objetivo desarrollar una practica en el laboratorio NETinVM, el cual ofrece un entorno virtualizado para explorar y desarrollar habilidades en lo que respecta la seguridad de redes.

Si bien sabemos que los mecanismos de seguridad son herramientas y métodos que se utilizar para implementar algún servicio que funcione por si solo o con otros, es fundamental entender su importancia en el contexto de las redes. Por lo tanto, algunos de los mecanismos de defensa más comunes en redes, son:

1. Firewall
2. Sistemas de detección de intrusos (IDS)
3. Sistemas de prevención de intrusos (IPS)
4. Criptografía

Todos estos mecanismos tienen por objetivo intentar prevenir y mitigar posibles vulnerabilidades en las redes y asegurar la integridad, confidencialidad y la disponibilidad de la información, es importante resaltar que existen muchos más mecanismos de defensa de las redes, pero en este proyecto solo abordamos el primer mecanismo “Reglas en firewall”. Es así, que en nuestro laboratorio de NETinVM protegeremos la red virtual mediante una serie de reglas, que quedaran evidenciadas en una tabla proporcionada por el docente de la materia, además de la evidencia del proceso que se llevo acabo para elaborar dicha actividad.

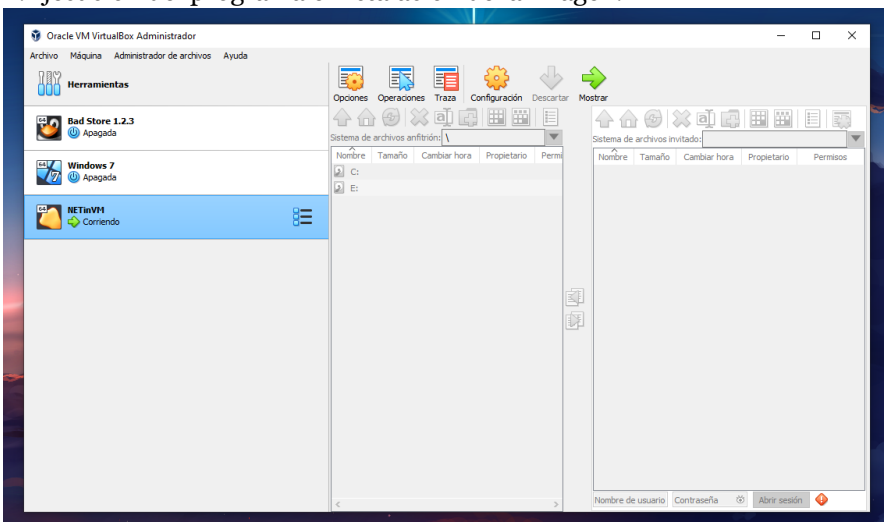
NETinVM.

Instalación de NETinVM.

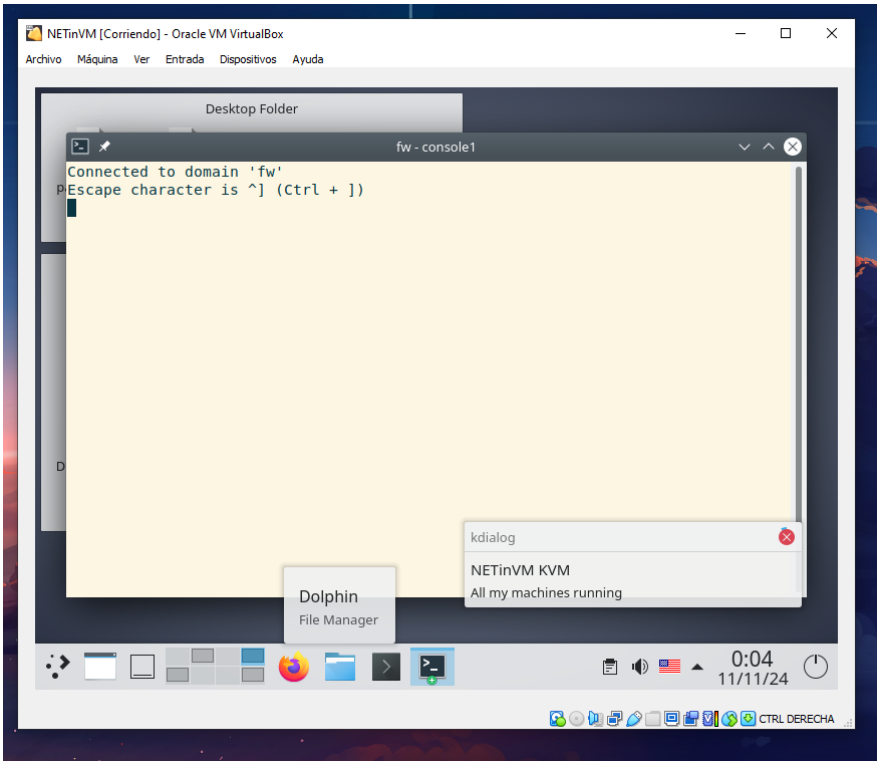
Debido a ciertos problemas en la ejecución de la imagen de NETinVM en “Workstation VMware”, se decidió correr la imagen en “VirtualBox”.

1.Instalacion de VirtualBox

2.Ejecucion del programa e instalación de la imagen.

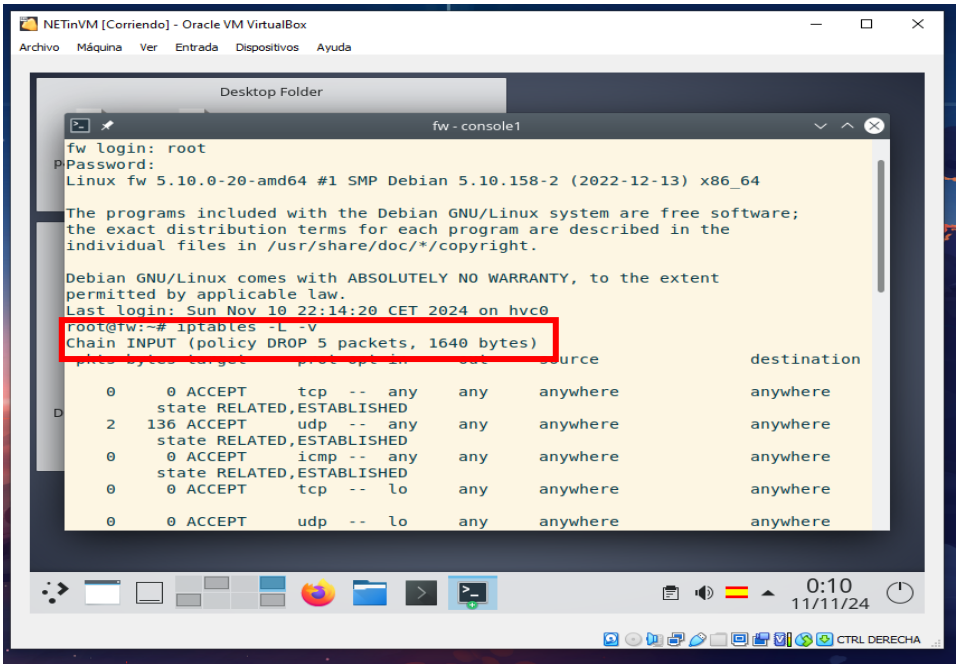


3. Inicio de la Imagen y las maquinas

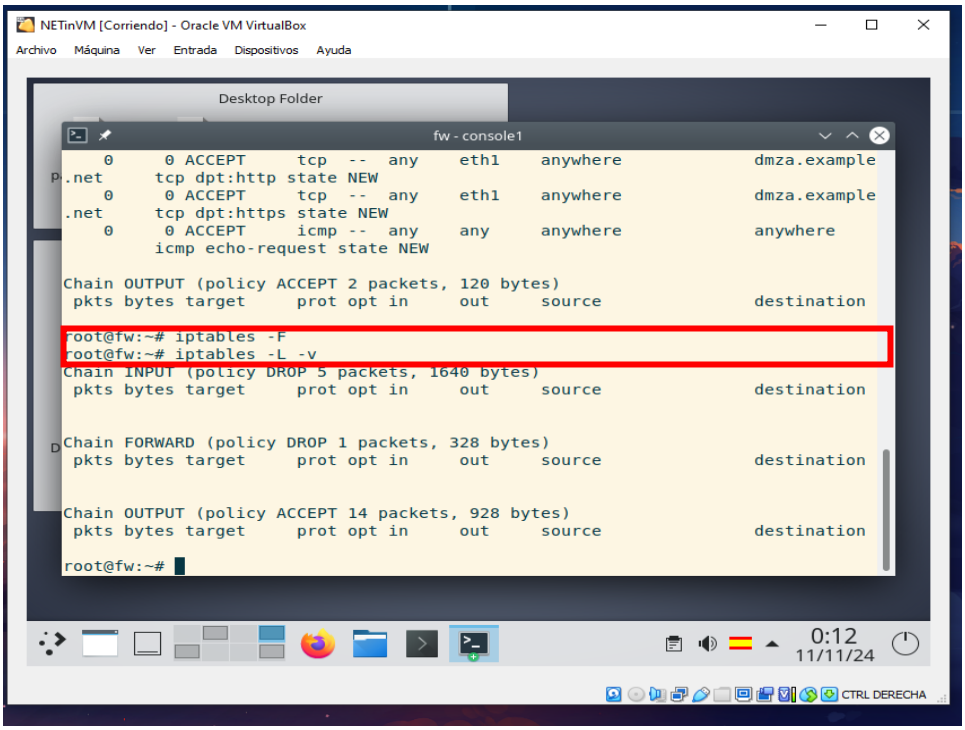


Desarrollo de la practica

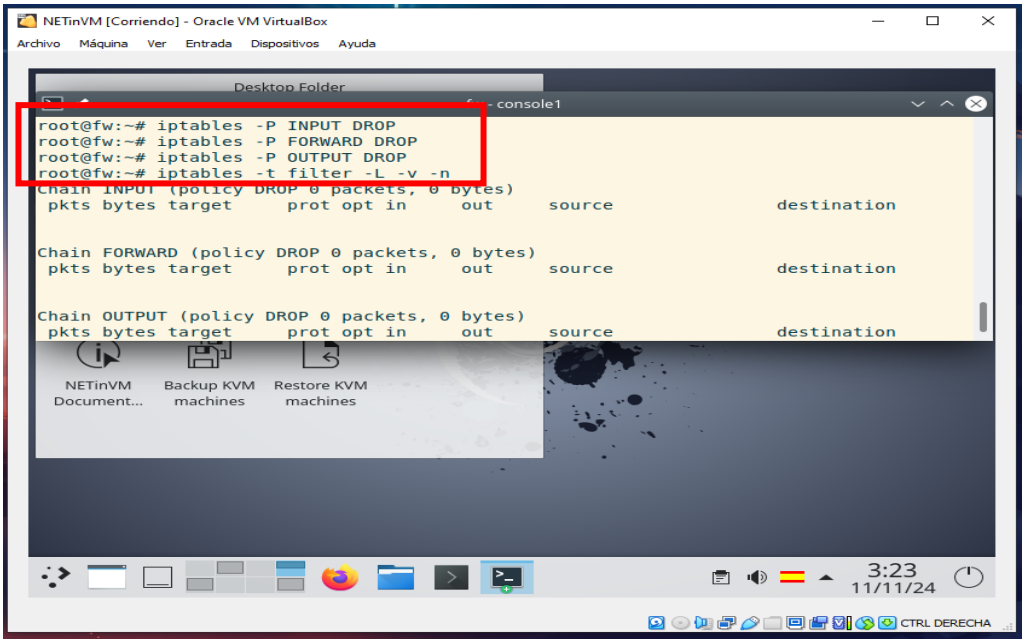
1. Decides conectarte al cortafuegos como *root* y **listar las reglas de la tabla filter en modo verbose.**



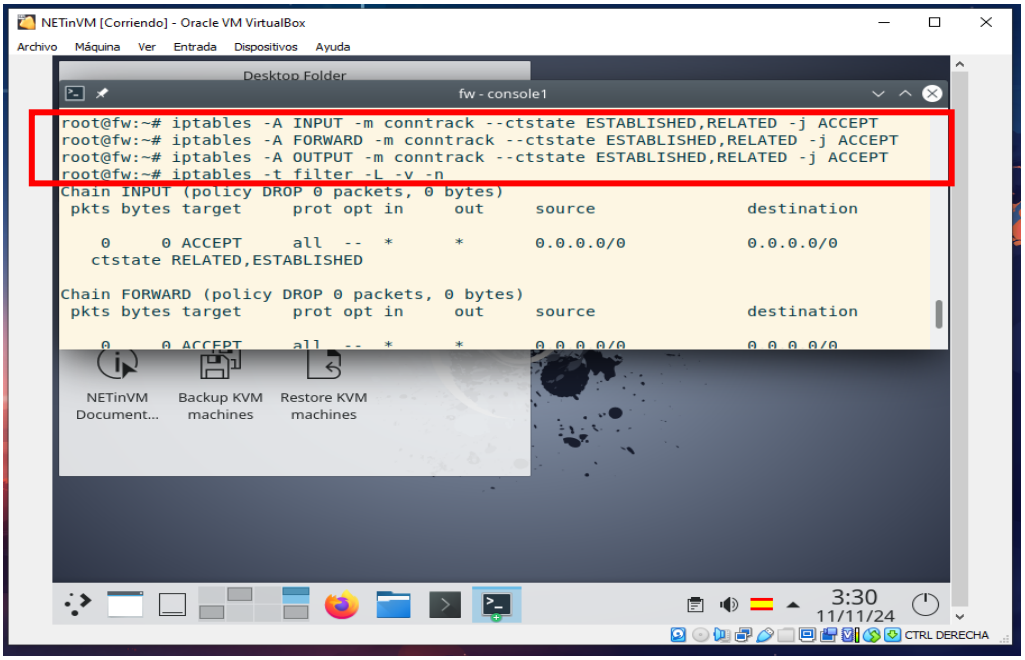
2. El listado te muestra que se permiten demasiadas conexiones. Decides que lo mejor es empezar desde cero y **borrar todas las reglas de la tabla filter.**



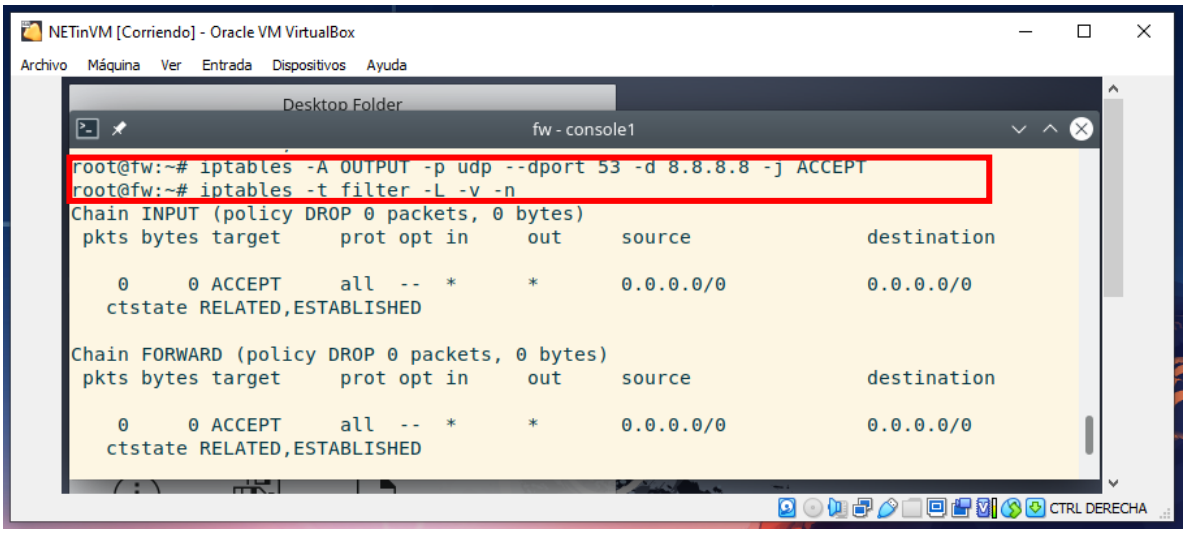
3. Además, no todas las cadenas de la tabla filter tienen una política restrictiva. **Estableces una política restrictiva en la cadena que falta.**

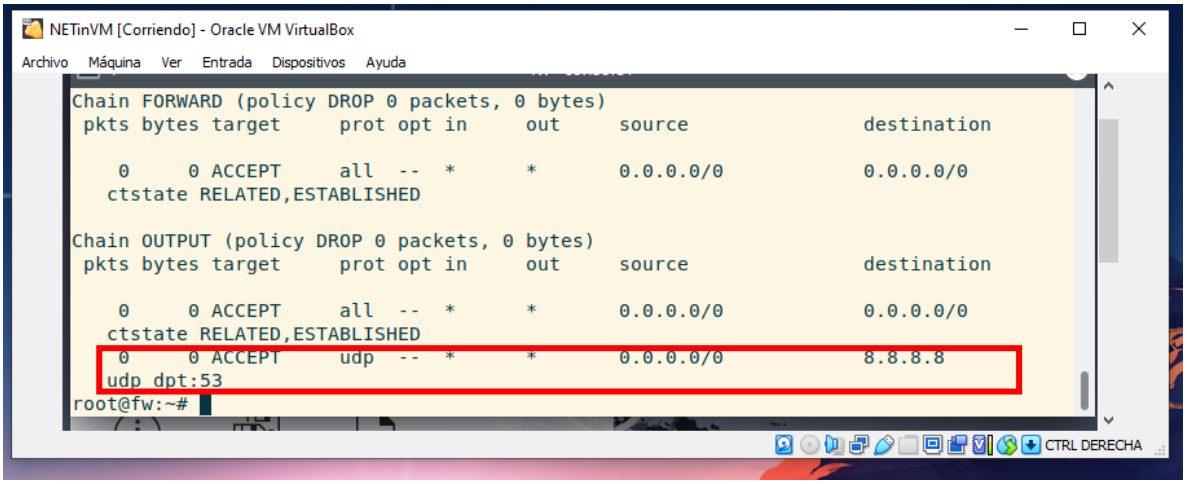


4. Una vez que has establecido una base segura, llega el momento de permitir las conexiones necesarias para Example. Lo primero es **permitir el tráfico de las conexiones ya establecidas en todas las cadenas de la tabla filter.**

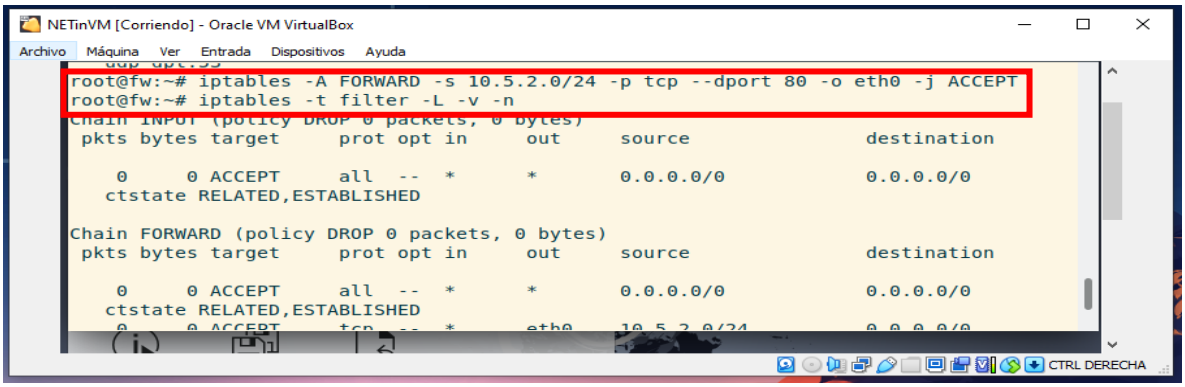


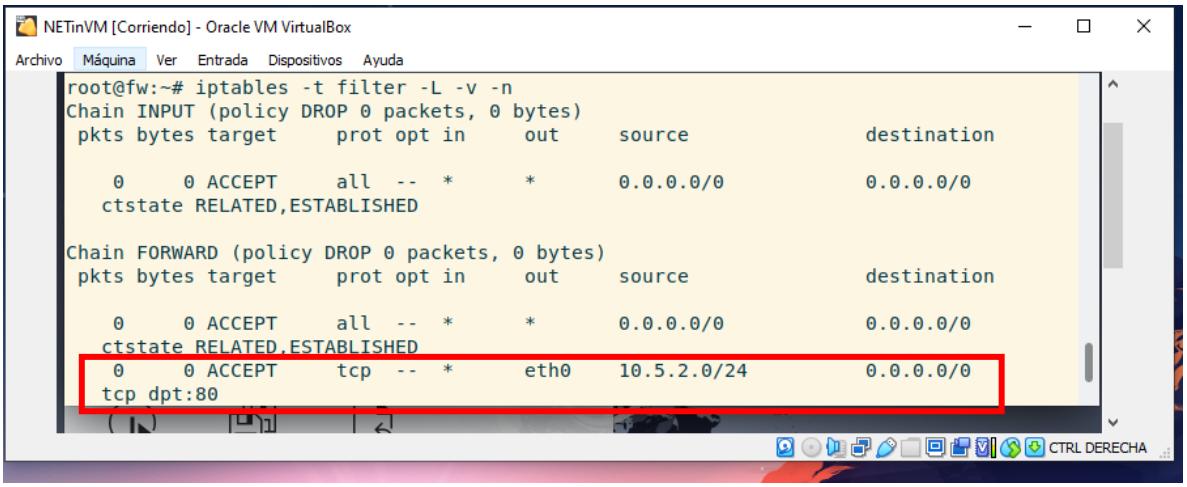
5. 5. A continuación, necesitas que la red local tenga capacidad de resolución de nombres. Desgraciadamente, Example no cuenta con DNS propio, así que seleccionas uno que crees seguro en Internet. **Permites las nuevas conexiones salientes desde la red local al servidor DNS (UDP) público de Google (IP: 8.8.8.8) que se encuentra en Internet.**



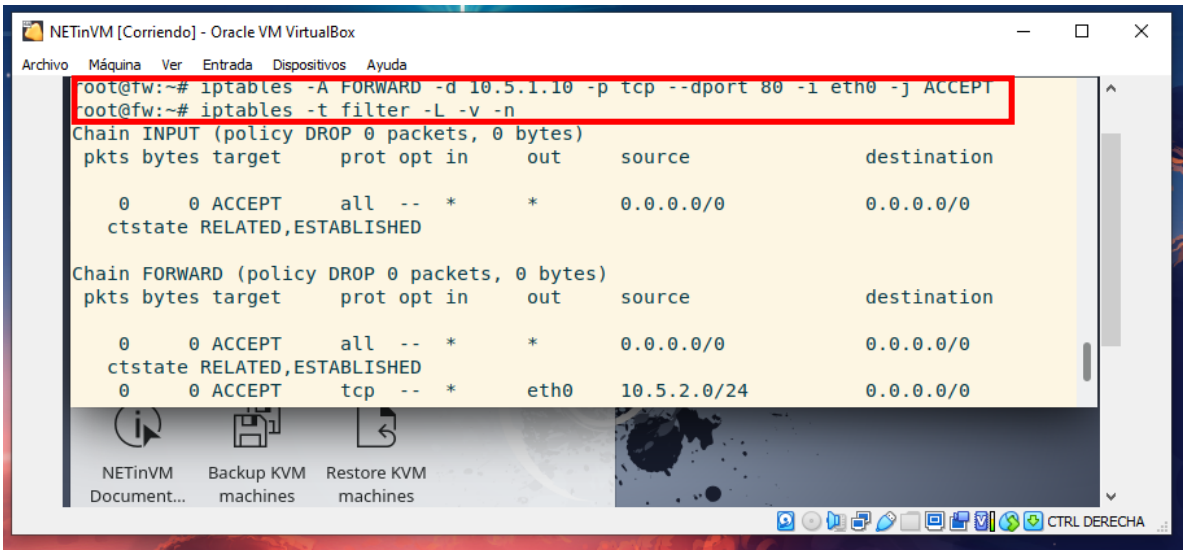


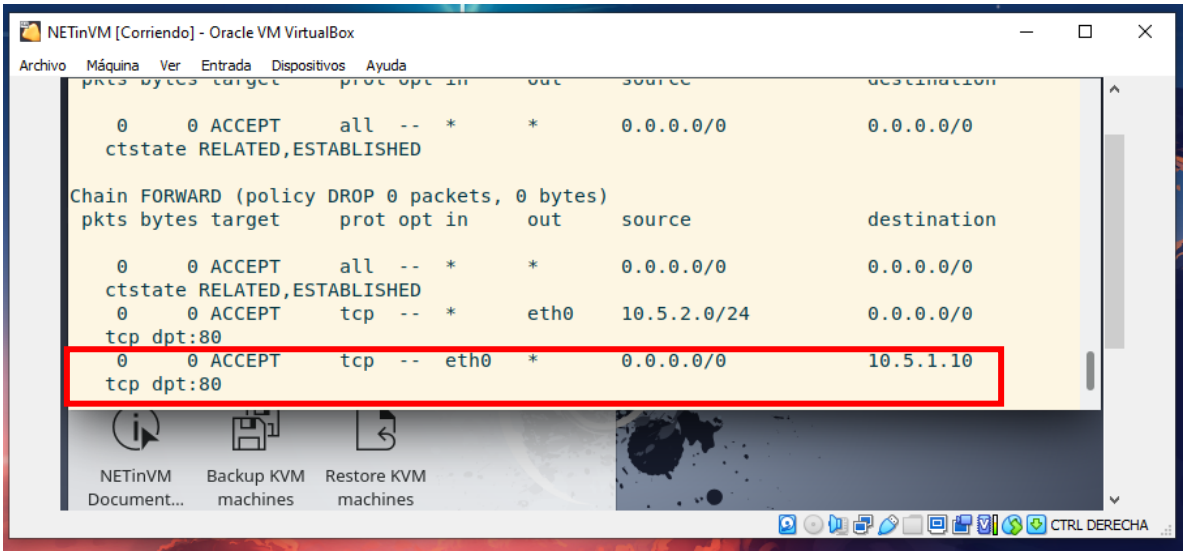
6. Los usuarios de la red local necesitan acceso a servidores web en Internet. **Creas una regla que permita nuevas conexiones desde la red local a servidores web en Internet.**



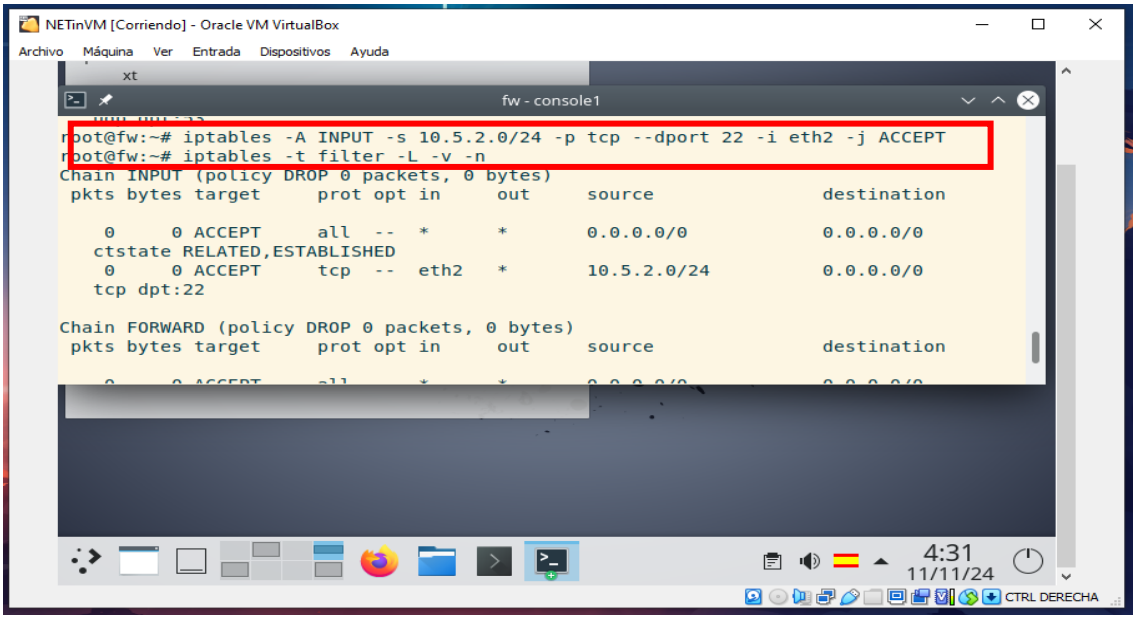


7. Example desea que su servidor web sea accesible desde Internet. **Creas una regla que permita las nuevas conexiones HTTP desde Internet al servidor web en la DMZ.**

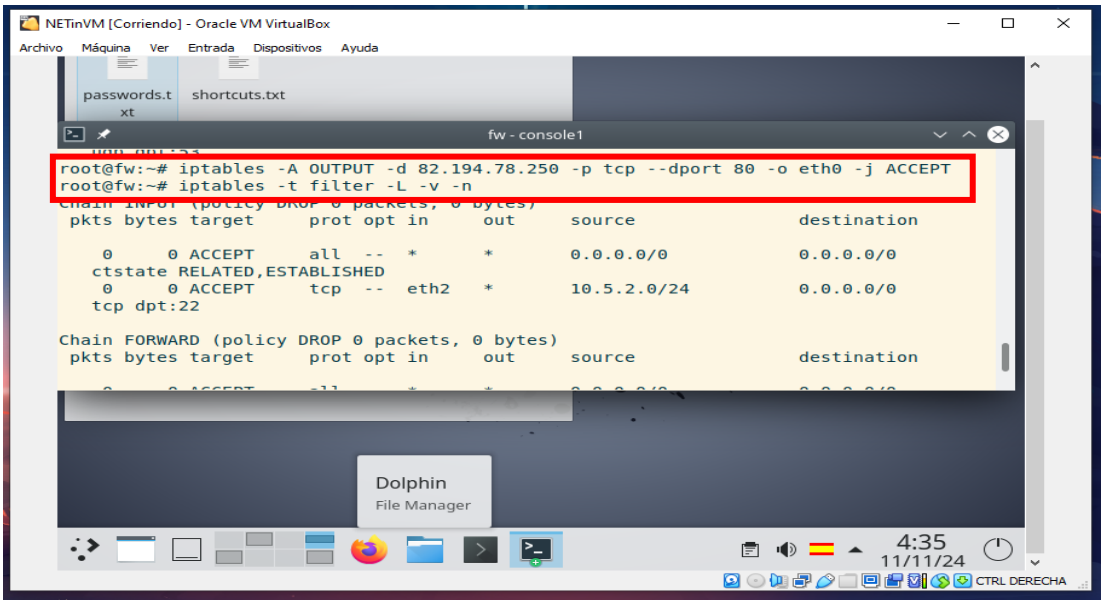


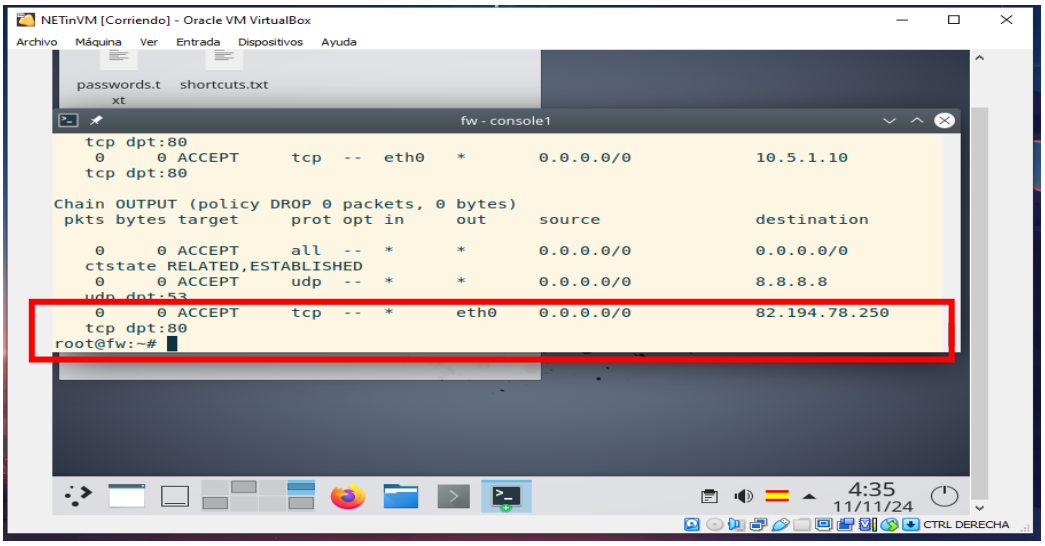


8. Example te pide que se pueda administrar el cortafuegos de forma remota desde la red local. **Creas una regla que permita las nuevas conexiones SSH desde la red local al cortafuegos.**

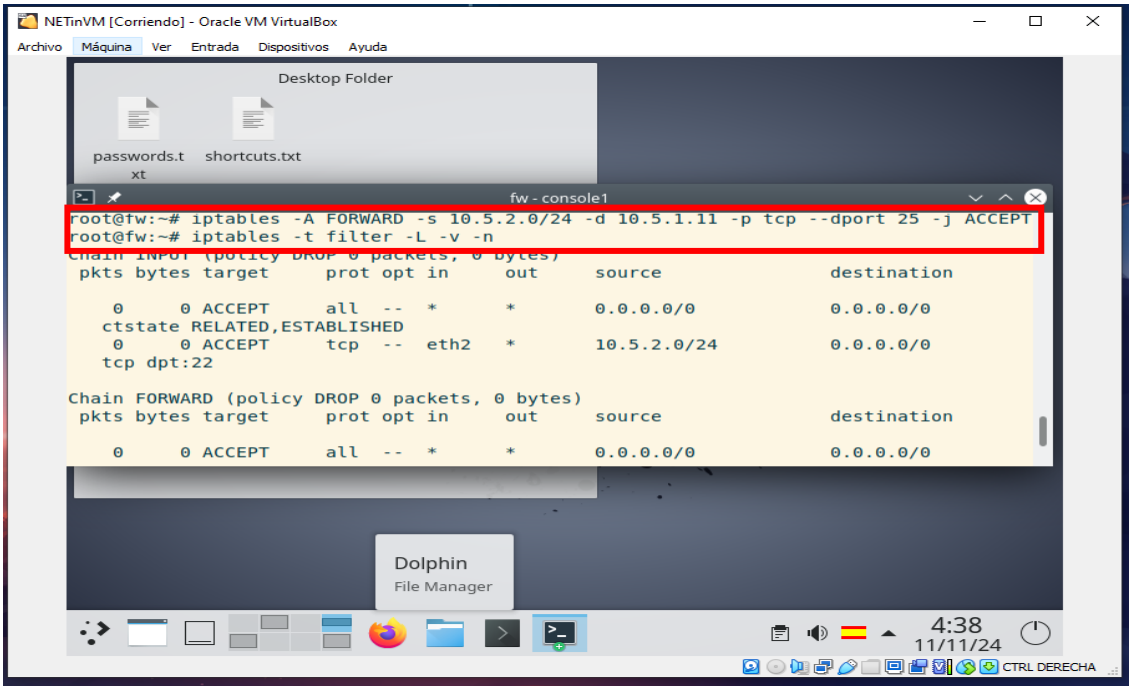


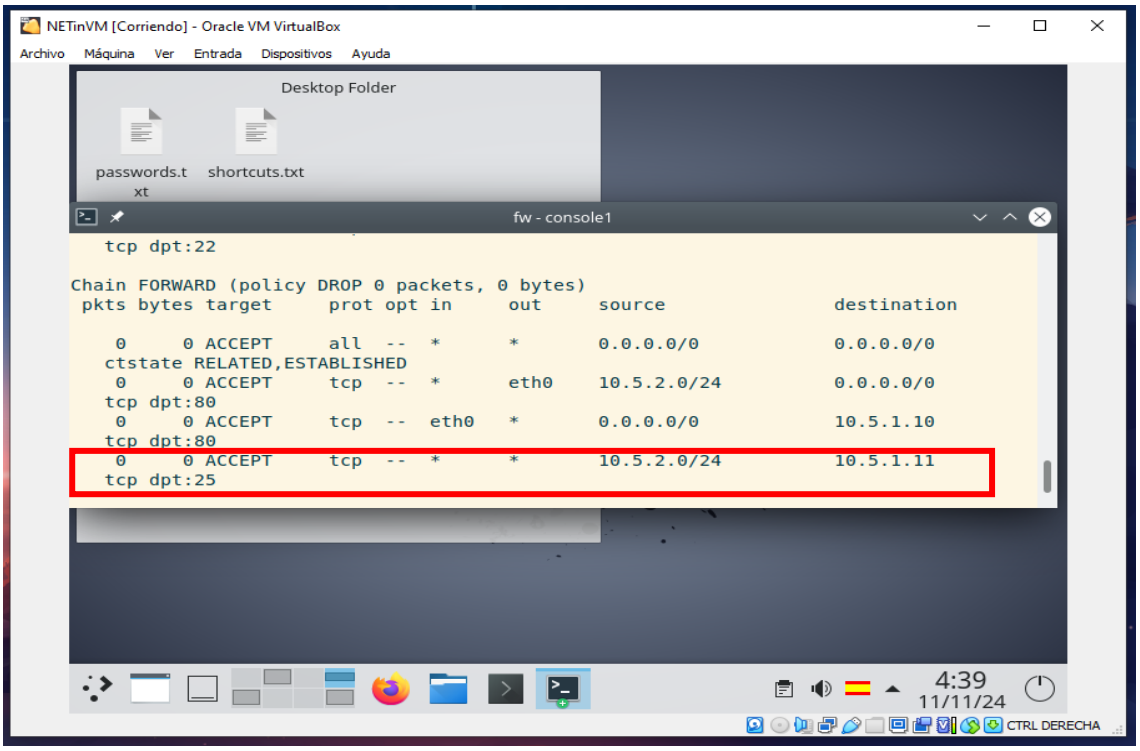
9. Example quiere que el cortafuegos pueda descargarse actualizaciones de seguridad de Internet. **Permites las nuevas conexiones HTTP desde el cortafuegos al servidor de actualizaciones de Debian en España (IP: 82.194.78.250) que se encuentra en Internet.**





10. Por último, Example quiere desplegar próximamente un servidor de correo (SMTP) en su DMZ con la IP 10.5.1.11 y te pide que dejes el acceso permitido en el cortafuegos para evitar volver a requerir tus servicios. **Permites las nuevas conexiones desde la red local al futuro servidor de correo (SMTP) que se encontrará en la DMZ (10.5.1.11).**





Documentación de reglas

Acción	**Regla**
1. Listar las reglas de la tabla *filter* en modo detallado	Iptables -L -v
2. Borrar todas las reglas de la tabla *filter*	Iptables -F
3. Establecer una política restrictiva en la cadena que falta	iptables -P INPUT DROP iptables -P FORWARD DROP iptables -P OUTPUT DROP
4. Permitir el tráfico de conexiones ya establecidas en todas las cadenas de la tabla *filter*	iptables -A INPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT iptables -A OUTPUT -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

5. Permitir las nuevas conexiones salientes desde la red local al servidor DNS (UDP) público de Google (IP: 8.8.8.8) que se encuentra en Internet	iptables -A OUTPUT -p udp --dport 53 -d 8.8.8.8 -j ACCEPT
6. Permitir las nuevas conexiones desde la red local a servidores WEB en Internet	iptables -A FORWARD -s 10.5.2.0/24 -p tcp --dport 80 -o eth0 -j ACCEPT
7. Permitir las nuevas conexiones HTTP desde Internet al servidor Web en la DMZ	iptables -A FORWARD -d 10.5.1.10 -p tcp --dport 80 -i eth0 -j ACCEPT
8. Permitir las nuevas conexiones SSH desde el PC inta al cortafuegos	iptables -A INPUT -s 10.5.2.0/24 -p tcp --dport 22 -i eth2 -j ACCEPT
9. Permitir las nuevas conexiones HTTP desde el cortafuegos al servidor de actualizaciones de Debian en España (IP: 82.194.78.250) que se encuentra en Internet	iptables -A OUTPUT -d 82.194.78.250 -p tcp --dport 80 -o eth0 -j ACCEPT
10. Permitir las nuevas conexiones desde la red local al futuro servidor de correo (SMTP) que se encontrará en la DMZ (10.5.1.11)	iptables -A FORWARD -s 10.5.2.0/24 -d 10.5.1.11 -p tcp --dport 25 -j ACCEPT