PRÁCTICA : E6 – Instalar un cortafuegos en Windows y Linux **MF0486_3 : Seguridad en Equipos Informáticos**		**Fecha**	21 / 03 / 2022
			Página 1 de 5
Curso	**7.1. MF0486_3 Seguridad en equipos informáticos**	**Plan de Formación**	FC-2021.1/II.000/1914256

Nombre y Apellidos:	**ALEXIS VENTURA MEDINA**	**Firma del Alumno:**	Firmado por VENTURA MEDINA ALEXIS -
DNI:	49946563Q	**Firma del Profesor:**	

Apto: ☐ **No Apto:** ☐ **Calificación:**

Instrucciones Generales

La puntuación máxima será de 10 puntos.
Esta prueba tendrá una duración máxima de 1260 minutos
(Temporalizados durante la Unidad de Aprendizaje)

El alumno/a deberá acatar las siguientes normas durante la duración de la práctica :

- Rellene el encabezado con su nombre, apellidos y D.N.I.
- Firme en todas y cada una de las hojas entregadas, incluidas las que estén en blanco.
- Usar exclusivamente bolígrafo azul o negro
- Guardar los ficheros generados en una carpeta con nombre **MF0486_E6**
- El docente le indicará al final como entregar el contenido de dicha carpeta
- Al finalizar el ejercicio y antes de entregarlo **comprueba tus respuestas**, en caso de duda consulta al docente.

Equipo y material

- Bolígrafo azul.
- Folios.
- Ordenadores.
- Conexión a Internet. (Para buscar información a modo de ayuda)
- Pendrive.
- Bibliografía empleada en el Módulo.
- Sistema operativo Windows (virtualizado)
- Sistema operativo Linux (virtualizado)

Instrucciones específicas

El objetivo de esta práctica guiada será que el alumno elabore un Plan de seguridad de una empresa ficticia o real, en el cual se plasmen diversas políticas de seguridad vistas durante el módulo formativo.

Condiciones de realización:

La actividad se llevará a cabo en el aula y el alumnado contará en todo momento supervisión del docente.

El alumnado contará con una duración de 1260 minutos para realizar la práctica.
Se podrá realizar en varias partes con una duración cada una de 60 minutos aproximadamente.

El alumno podrá hacer uso de internet para su realización, y se detallan a continuación algunas webs de ayuda.

Páginas webs :

https://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica)

En ella se valorará la utilización de herramientas para la gestión del tiempo y secuenciación del uso de las aplicaciones necesarias. Y se observará especialmente la autonomía del alumnado a la hora de ejecutar y tomar decisiones. Como también la estructuración del ejercicio en donde se solicitará, orden, coherencia y limpieza.

Una vez terminado la práctica se le notificará al docente y pasará a su evaluación.

Descripción de la práctica

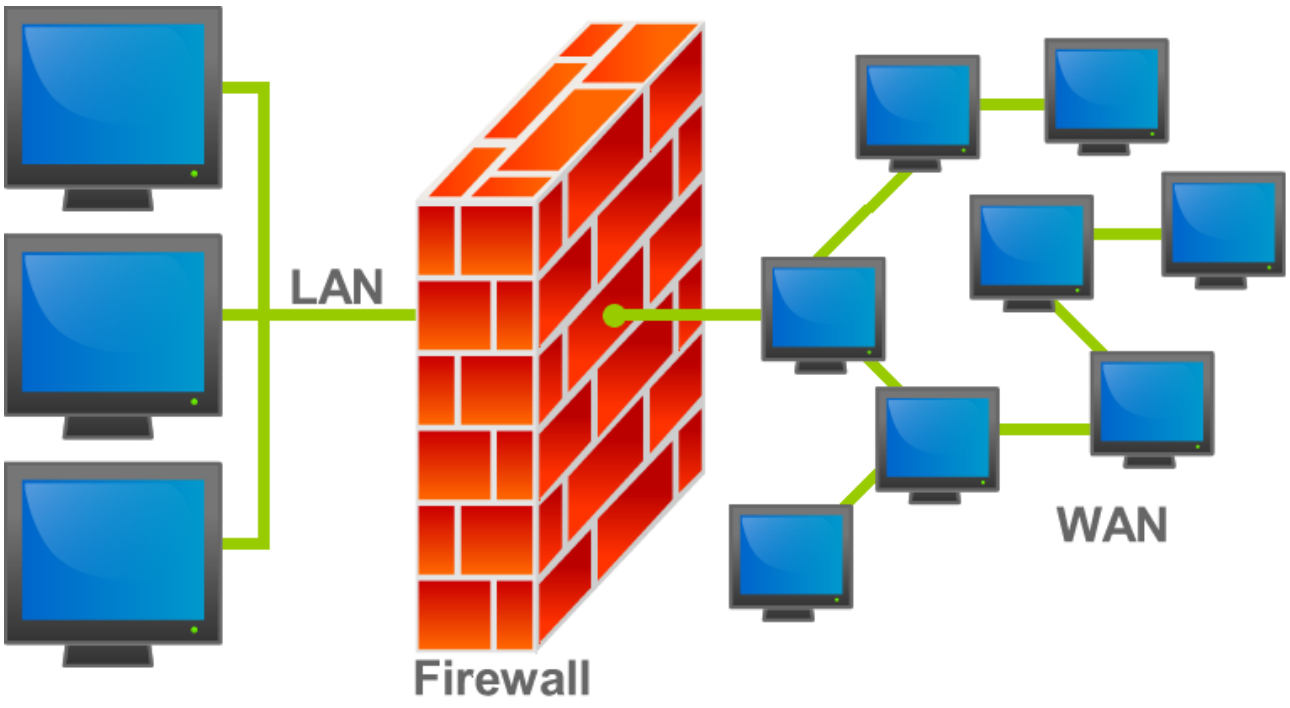
El concepto de Cortafuegos

Un **cortafuegos** (***firewall***) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o en una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar el cortafuegos a una tercera red, llamada *zona desmilitarizada* o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.



PRÁCTICA

1ª Parte : Instalación y configuración de un cortafuegos en Windows

En esta primera parte de la práctica el alumno eligirá la configuración o programa de los que se citan a continuación u otra configuración que proponga el alumno y que crea conveniente para instalar y configurar un firewall en entornos basados en Windows.

Una vez el alumno haya finalizado tendrá que documentar y presentar todo en un informe, detallando los principales pasos que ha realizado.

Configurar un cortafuegos Windows con Zonealarm
http://www.zonealarm.com/es/software/free-firewall/

Otras alternativas
http://www.xatakawindows.com/bienvenidoawindows8/este-es-el-firewall-de-windows-y-sus-mejores-alternativas

http://www.emezeta.com/articulos/10-firewalls-gratuitos-alternativos

2ª Parte : Instalación y configuración de un cortafuegos en Linux

En esta segunda parte de la práctica el alumno eligirá la configuración o programa de los que se citan a continuación u otra configuración que proponga el alumno y que crea conveniente para instalar y configurar un firewall en entornos basados en Linux.

Una vez el alumno haya finalizado tendrá que documentar y presentar todo en un informe, detallando los principales pasos que ha realizado.

Configurar un cortafuegos en Ubuntu con Gufw
https://es.wikipedia.org/wiki/Gufw

El alumno además podrá elegir alguno de los siguientes programas para configurar el cortafuegos :

CSF: uno de los más conocidos sin lugar a dudas. CSF (ConfigServer Security & Firewall) es un software desarollado por Configserver.com y se encuentra en constante actualización. No solamente es fácil de instalar, sino también de configurar y utilizar. CSF es compatible con muchas distros populares como CentOS, Ubuntu, Fedora, Debian y más.

APF: Advanced Policy Firewall es uno de los proyectos de R-fx Networks. APF es un cortafuegos que está basado en el conocido sistema iptables (que a su vez está construido sobre Netfilter). APF está diseñado con el fin de poder satisfacer las demandas más esenciales que hoy en día encontramos en la industria de Internet. Este software cuenta con un archivo de configuración bien detallado, de manera tal que configurar nuestro firewall se vuelve una tarea sencilla en la gran mayoría de sus aspectos.

Shorewall: su verdadero nombre es Shoreline Firewall. Es otra conocida herramienta y se encarga de simplificar en gran medida el uso de iptables, que para algunos usuarios puede resultar complejo. Podemos configurarlo fácilmente a partir de varias indicaciones según nuestros distintos requerimientos. La herramienta recibe actualizaciones periódicas y posee una detallada documentación.

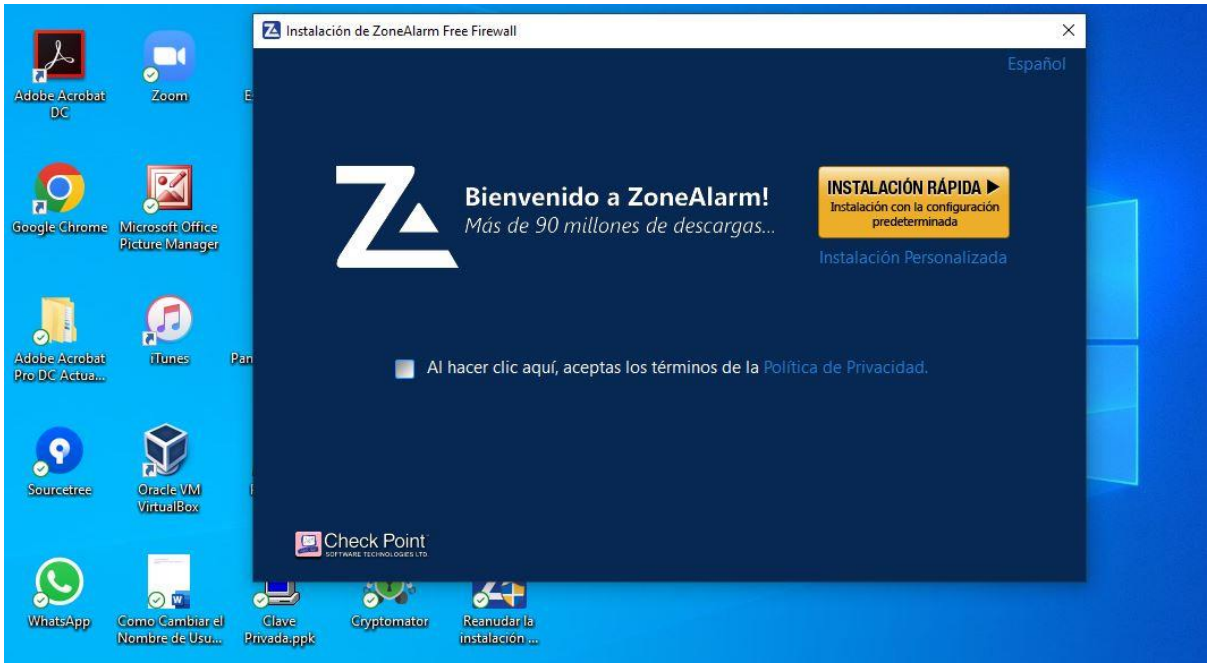
KISS Firewall: también conocido como KISS My Firewall. Se trata de un firewall totalmente gratuito basado en iptables y creado por Steve Eschweiler. KISS Firewall está diseñado para ser usado en un típico servidor web e incluso tiene métodos preventivos para evitar ataques DDOS, escaneo de puertos e incluso IP spoofing/suplantación de IP.

eBox Platform: Algo más que un simple software cortafuegos.
Monowall: La más liviana de las propuestas de la entrada.
PfSense: Si desea un servidor de seguridad integral y nada más, no busques más.
Smoothwall Advanced: Y su versión de pago, con asistencia técnica y más opciones.

El alumno también podrá elegir algunas de las siguientes distribuciones Linux :

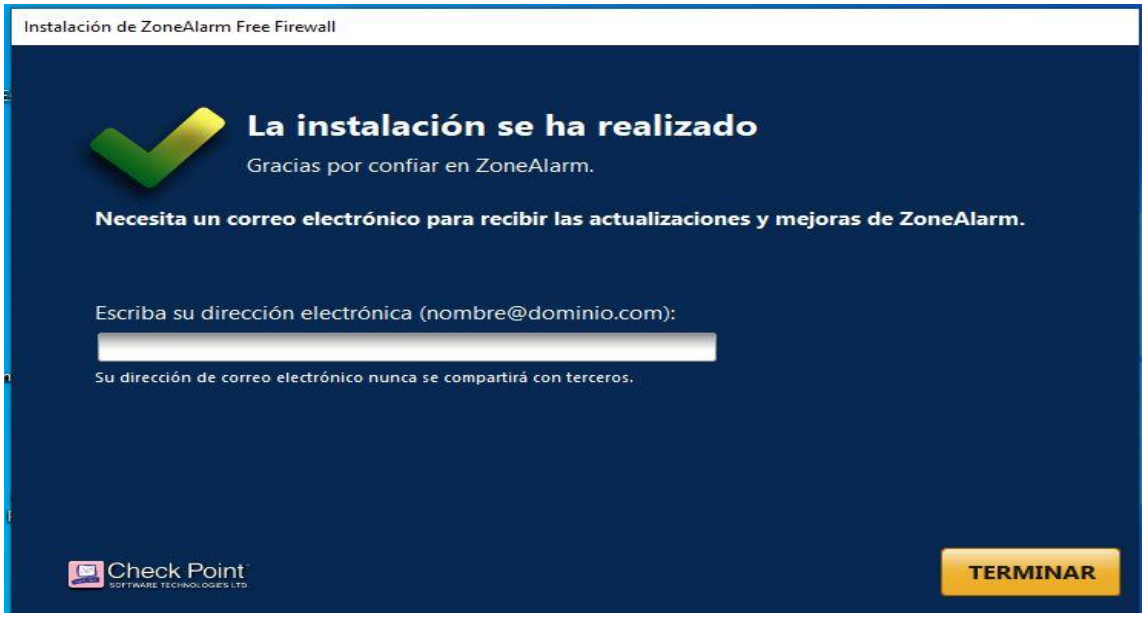
ClearOS: La distro que combina facilidad de uso con funcionalidad.
IPCop: Distribución versátil y rápida. Altamente configurable.
Smoothwall Express: Probablemente la distribución firewall con la mayor reputación.

Para el caso Windows instalaremos ZoneAlarm:



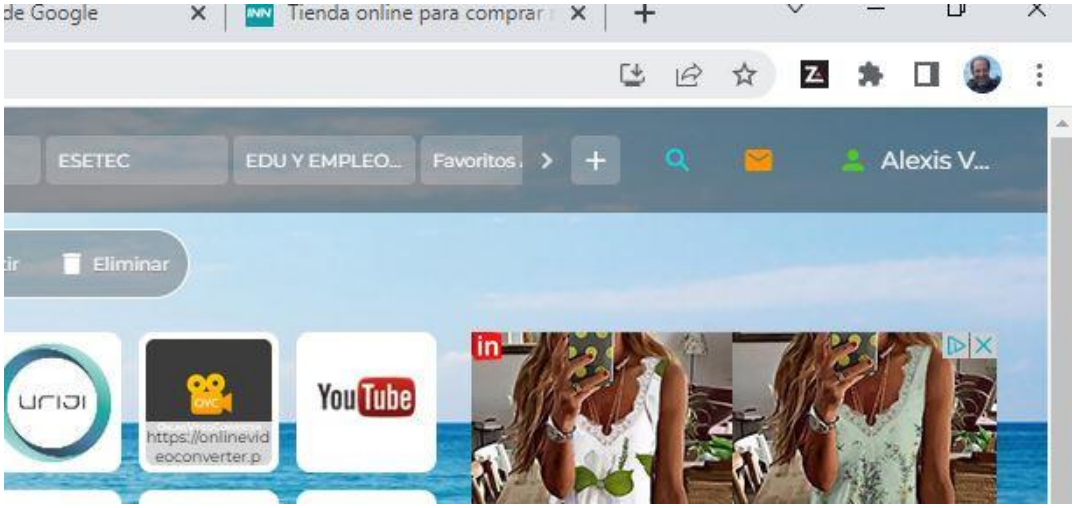
Vemos el Progreso de descarga

En este punto la Instalación se encuentra realizada

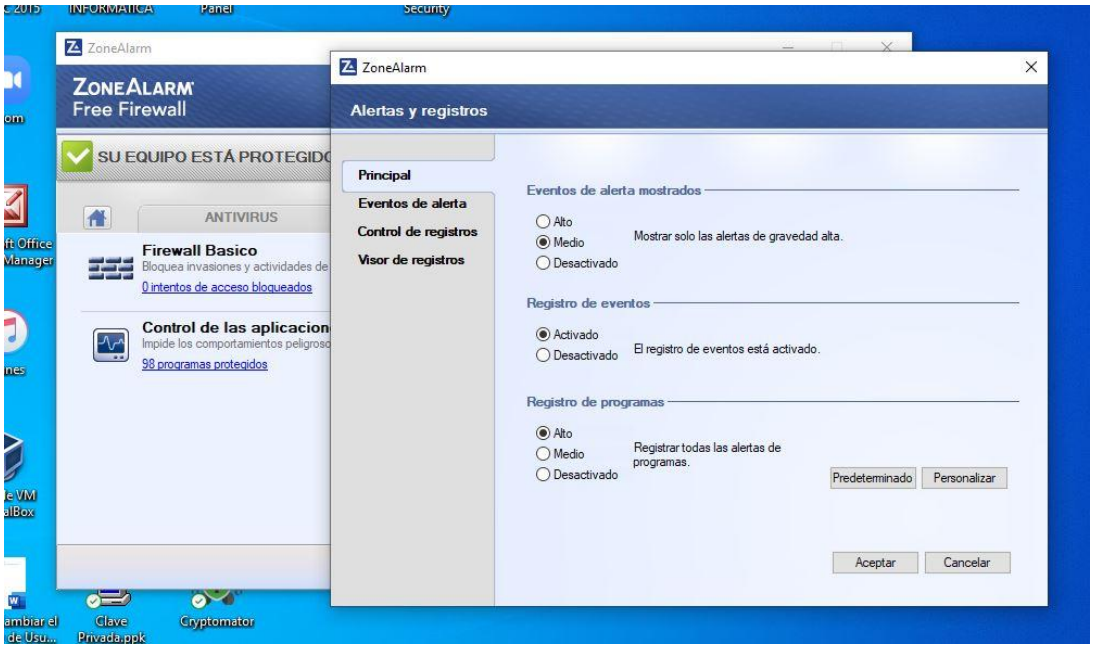


Vemos como ya el Firewall está instalado y Protegiendo al equipo.
No se activó el antivirus ya que el equipo posee uno con licencia.

El Firewall se instala como una extensión de Chrome,.



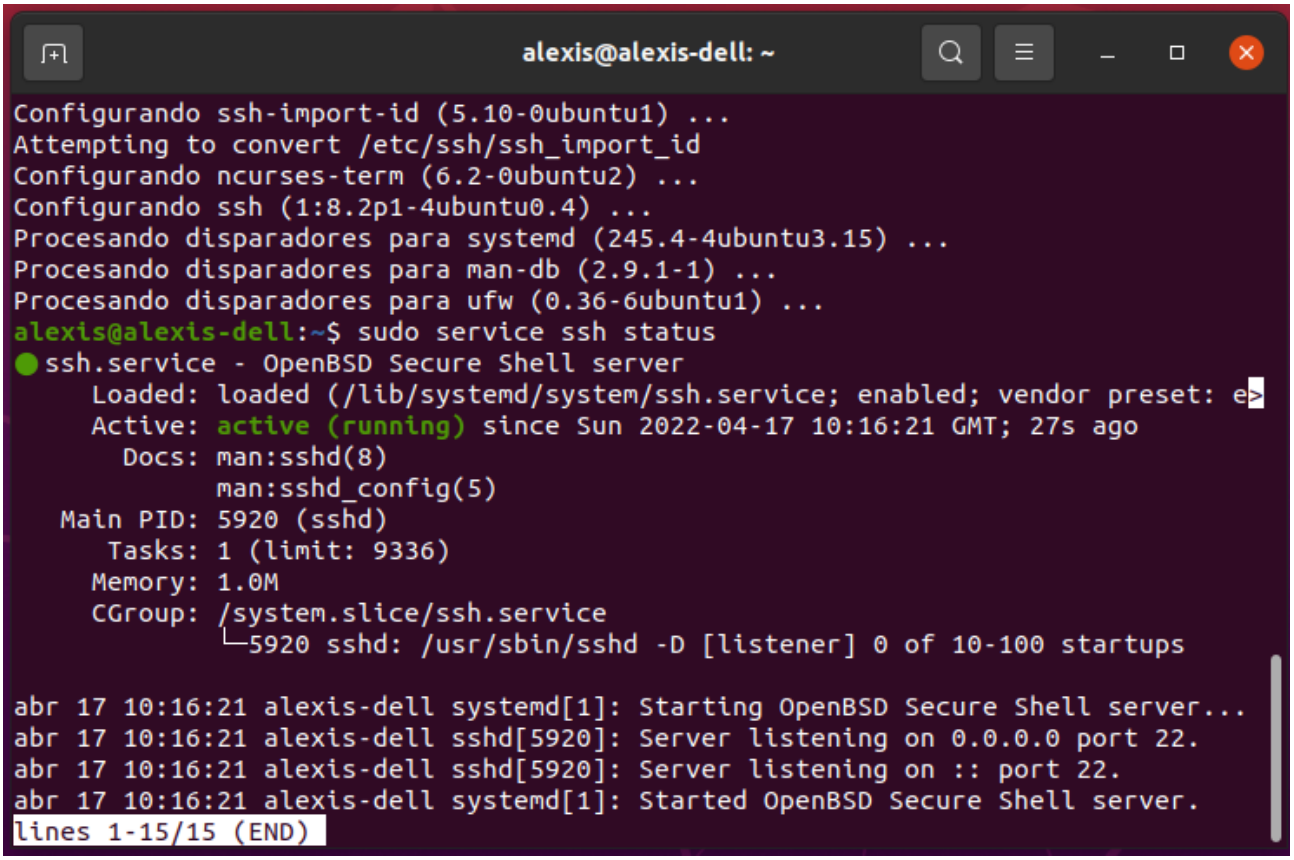
Podemos ver que no ha habido amenazas, sin embargo podemos situarnos en esa indicación y desplegar un menú adaptable.



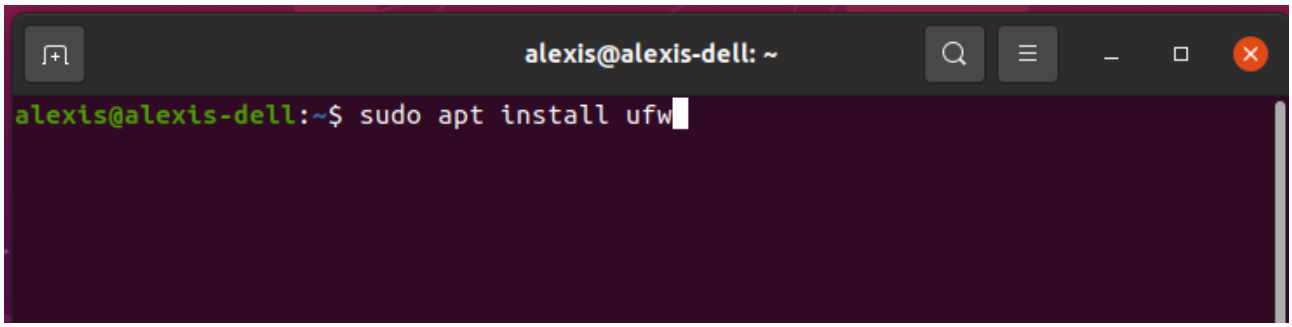
CASO UBUNTU:

El caso de UBUNTU, es particular ya que el cortafuego o Firewall UFW, ya viene instalado y su manejo, aunque puede ser utilizado en ordenadores personales, está más orientado a servidores.
La siguiente parte fue realizada viendo tutoriales de YouTube.

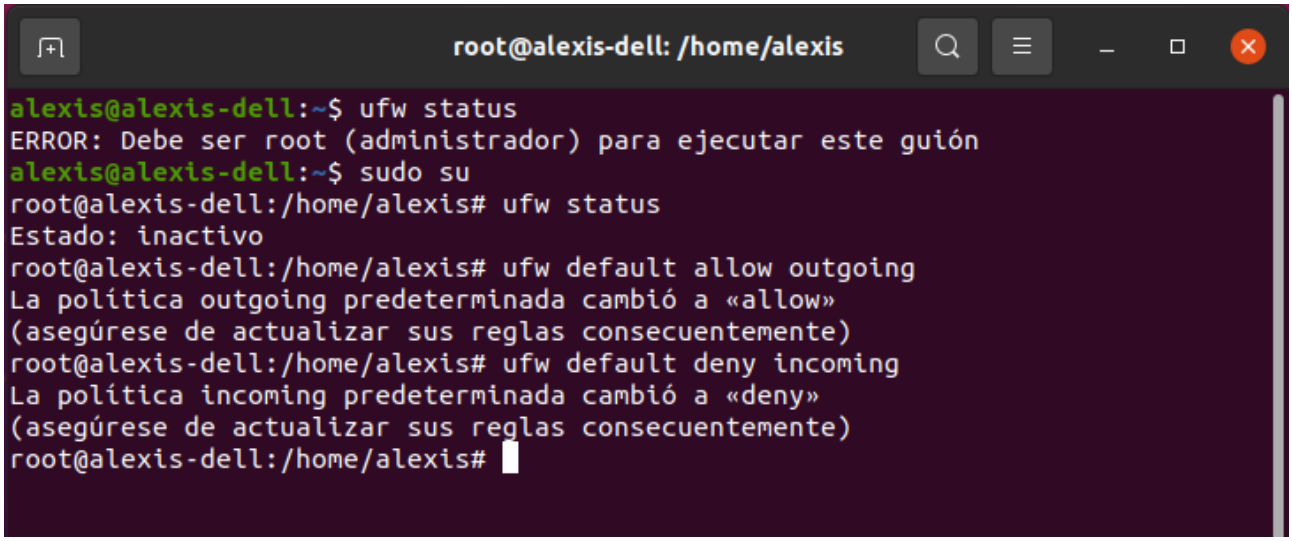
Lo primero que debemos estar pendientes es que el ssh se encuentre activo.
Para ello colocamos el comando correspondiente ssh status y nos presenta a siguiente pantalla.



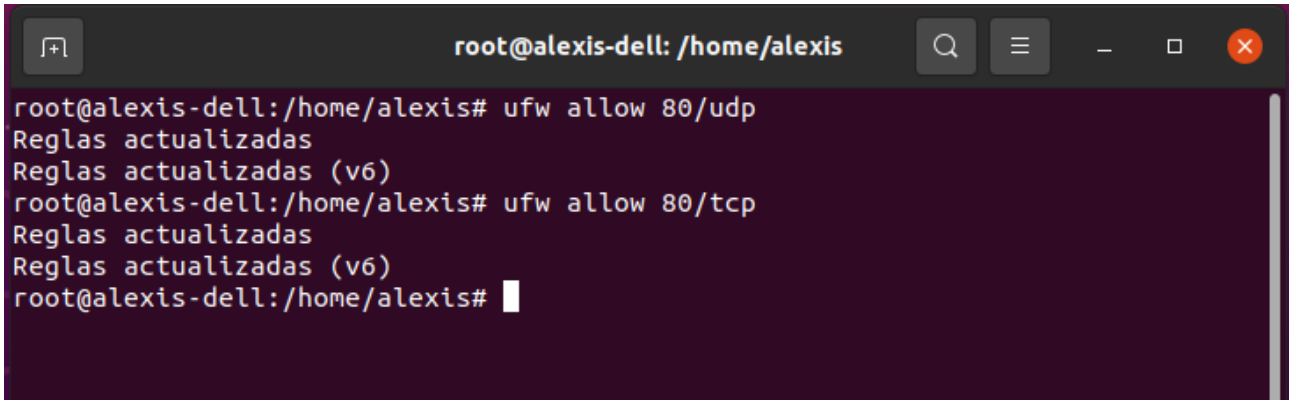
Como se dijo al Principio UFW, forma parte de los paquetes que ya tiene instalado UBUNTU, sin embargo para demostrarlo se pide instalarlo y ver el resultado.



El ufw, ya se encontraba instalado y se le pidió su estatus, pero para ello uno debe encontrarse en modo administrador

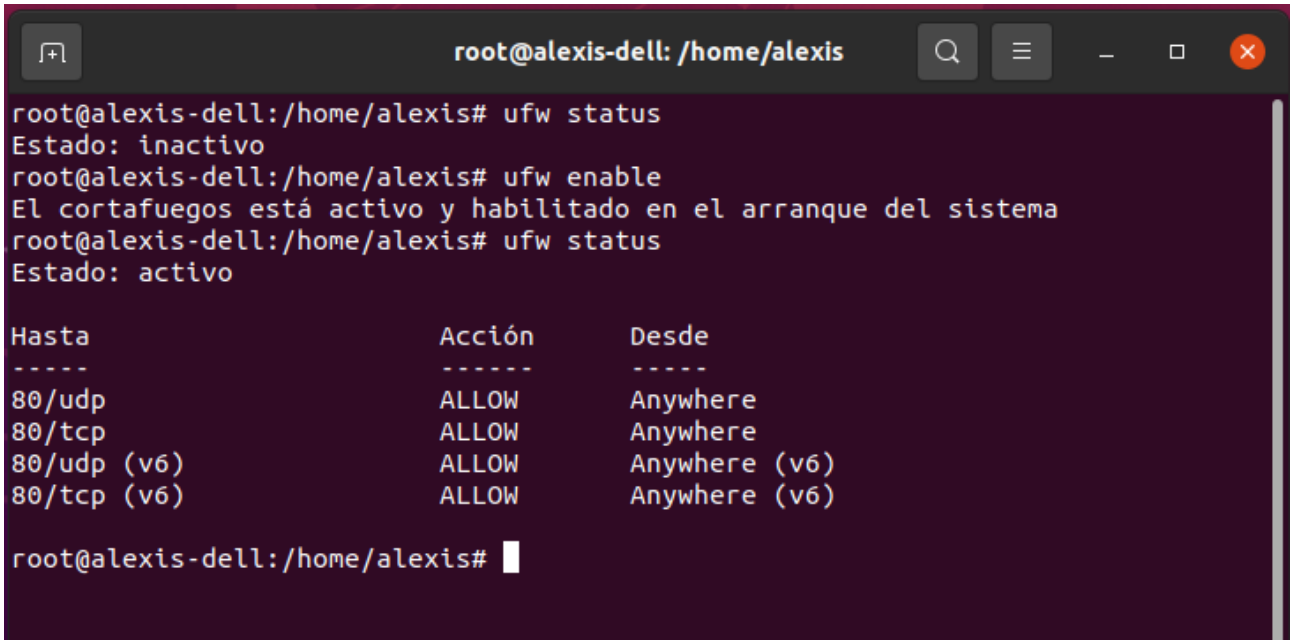


Antes de activarlo colocamos algunas reglas como permitir que todo salga pero no entre nada.

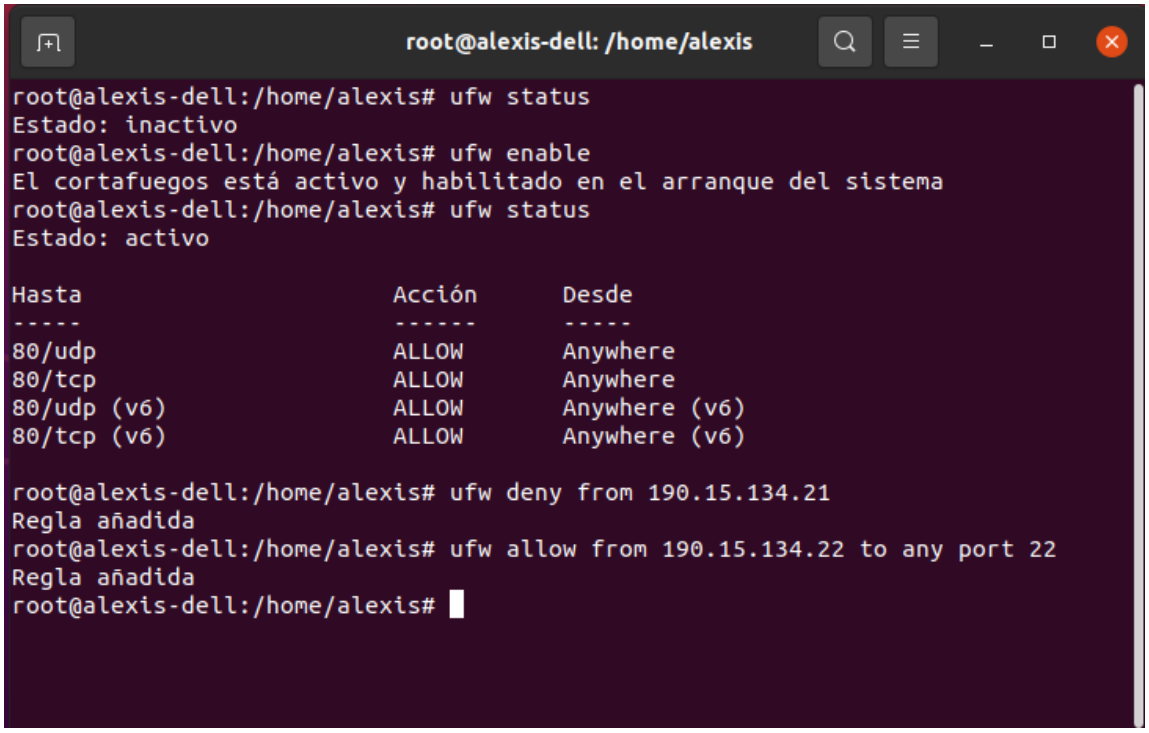


Ahora verificamos su estatus que sigue inactivo después de colocarles las reglas y pasamos a activarlo con el comando**: "ufw enable"**

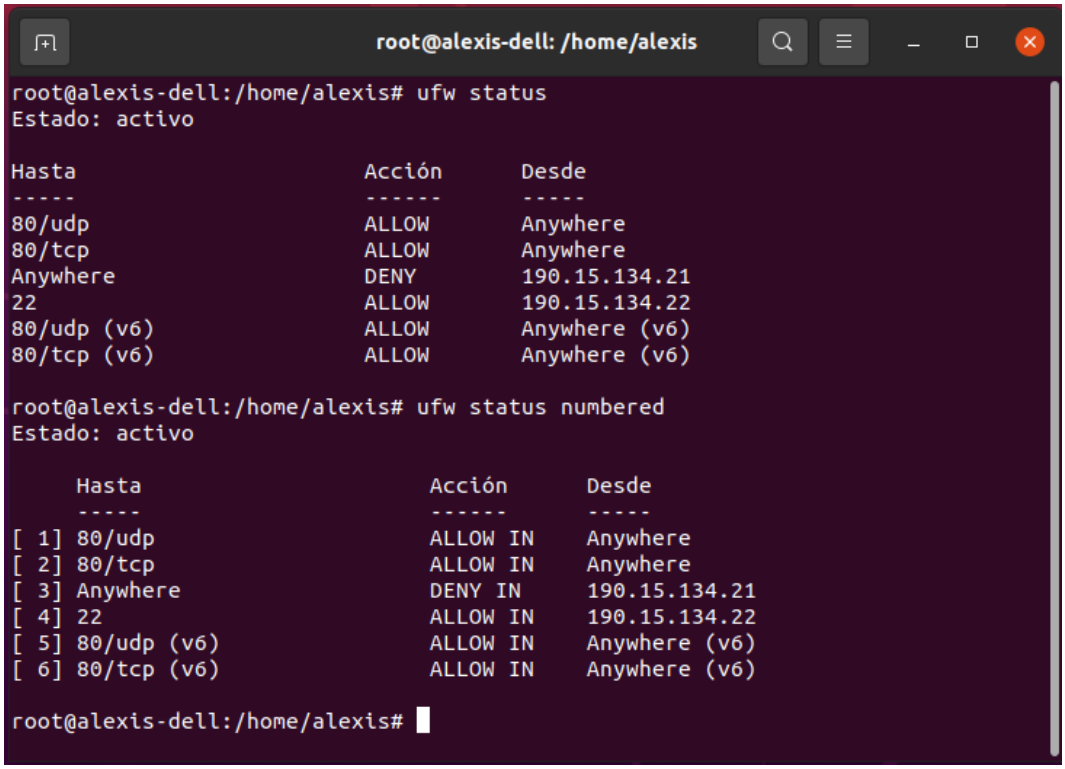
Al pedirle el estatus nos muestra que está activo y las reglas que colocamos



Si nosotros queremos manejar las reglas le pedimos que las enumere



Una vez enumeradas podemos eliminarlas por números:



Y el resultado se muestra a continuación.
Se denegó o quitó la regla Número 3.

Aquí se muestra el antes y el después