UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Cortafuegos y VPN para pymes con Raspberry

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Alapont Casañ, Jose

Tutor/a: Pons Terol, Julio

CURSO ACADÉMICO: 2021/2022

Resumen

Cortafuegos y VPN para pymes con Raspberry

Se ha desarrollado un sistema que permite a las pequeñas y medianas empresas mejorar su seguridad informática, creando una intranet que es accesible mediante una red privada virtual (VPN).

Se utiliza una Raspberry Pi con dos tarjetas de ethernet que actúa como un *router* y permite tener un cortafuegos (*firewall*) para monitorizar y bloquear el tráfico de red.

Palabras clave: cortafuegos, VPN, seguridad, raspberry, pymes.

Resum

Tallafocs i VPN per a pimes amb Raspberry

S'ha desenvolupat un sistema que permet a les petites i mitjanes empreses millorar la seva seguretat informàtica, creant una intranet que és accessible mitjançant una xarxa privada virtual (VPN).

S'utilitza una Raspberry Pi amb dues targetes de ethernet que actua com un *router* i permet tenir un tallafocs (*firewall*) per monitoritzar i bloquejar el trànsit de xarxa.

Paraules clau: tallafocs, VPN, seguretat, raspberry, pymes.

Abstract

Firewall and VPN for SMEs with Raspberry

A system has been developed that allows small and medium-sized companies to improve their IT security, creating an intranet that is accessible through a virtual private network (VPN).

A Raspberry Pi is used with two ethernet cards that acts as a router and allows to have a firewall to monitor and block network traffic.

Keywords : cortafuegos, VPN, seguridad, raspberry, pymes.

Tabla de contenidos

Tabla de figuras

1 Introducción

A medida que ha ido evolucionando la tecnología, nos hemos centrado en la optimización de esta, tomando como objetivo principal la rentabilidad económica, dejando de lado otros factores como el ambiental o el social. Aunque en la última década esta tendencia ha cambiado y cada vez está más presente la importancia de encontrar un equilibrio entre la rentabilidad económica y la sostenibilidad social y medioambiental.

Este equilibrio presenta un desafío para las empresas que han aumentado el parque tecnológico, ya que actualmente los servidores y recursos empleados consumen una gran cantidad de energía. Con el propósito de encontrar una alternativa más sostenible se presenta este TFG, donde, simulando el entorno de una oficina, luego de ver los aspectos de seguridad que afectan a una pequeña empresa y su relación con el marco legal, se busca desarrollar mediante el uso de una Raspberry Pi, un conjunto de servidores y un cortafuegos, que permitan el acceso a toda la infraestructura de red de la empresa sin estar conectados directamente en la misma, buscando así disminuir el consumo energético.

1.1 Motivación

La motivación principal por la que se ha impulsado este proyecto es para poder ayudar a pequeñas y medianas empresas a tener los datos disponibles y accesibles, así como tener la tranquilidad de llegar a ellos de una manera privada y segura teniendo una alternativa más económica y eficiente que las utilizadas actualmente. También es fácilmente exportable a cualquier entorno de producción privado, lo que permite que se pueda adaptar a muchas casuísticas diferentes.

Además, existe la posibilidad de hacerme un pequeño hueco en el mercado vendiendo una Raspberry Pi preconfigurada y terminar de ayudar al usuario final a entender su funcionamiento, ya que cada vez hay más empresas que se están concienciando de lo importante que es la seguridad informática y la eficiencia energética en el ámbito laboral.

Otro de los aspectos, es que se puede desarrollar de una forma muy económica. Esto hace que cualquiera que esté interesado pueda implementar un pequeño sistema

de seguridad informática utilizando una Raspberry Pi como cortafuegos y como servidor para tener una conexión de una red privada virtual, en adelante VPN.

1.2 Objetivos

El objetivo principal es desarrollar una herramienta utilizando un conjunto de software y hardware que permita crear una intranet segura y sostenible en una empresa y que sea accesible a través de una VPN.

Para que el proyecto tenga consistencia también se plantean los siguientes objetivos secundarios:

- Poner pautas claras de seguridad, utilizando el esquema de seguridad nacional y desglosarlo para tener una mejor visión a nivel empresarial. Así se podrá decidir qué tipo de jerarquía de red interesa tener y qué tipo de seguridad aplicar a cada una de las partes de la infraestructura de la organización.
- Elaborar un esquema de red funcional que se adapte a un modelo general y real de trabajo.
- Identificar el tipo de Raspberry que interesa utilizar, configurar el dispositivo para poder empezar a trabajar con él y analizar sus características y sus funcionalidades.
- Definir las herramientas que se pueden emplear para crear un cortafuegos en un sistema basado en la distribución GNU/Linux Debian, llamado Raspbian, e implementarlo con nuestra Raspberry Pi.
- Realizar la configuración de nuestro dispositivo Raspberry para crear un servidor de VPN, usando un túnel cifrado para acceder, lo que permite tener un punto de acceso a nuestra empresa desde cualquier equipo y de modo seguro.

1.3 Impacto Esperado

Se espera que cualquier interesado, en concreto una pyme, sea capaz de poder utilizar una VPN a través de una Raspberry Pi, para tener una intranet que permita el acceso a todos sus datos privados de la red de la forma más segura.

También se pretende configurar el cortafuegos utilizando reglas Iptables para restringir el contenido a nivel de red, tanto de los usuarios internos como externos, al que se accede desde la propia empresa, es decir, páginas y protocolos. De esta manera, se puede conseguir una movilidad más amplia, manteniendo el mismo grado de seguridad y sin depender de terceros para llegar a dicha información.

1.4 Metodología

Para conseguir que sea más fácil abordar el problema inicial se busca alcanzar todos los objetivos dividiéndolos en pequeñas partes:

- Se estudiará el “Esquema de Seguridad Nacional” (ENS) [1]
- Una vez se tengan claras las bases de seguridad que necesitan las empresas, se procederá a crear un esquema de red seguro para así tener claros los elementos que van a interactuar en nuestra pequeña oficina.
- Se montará y configurará una Raspberry Pi con dos tarjetas de Ethernet.
- Se implementará la puesta a punto de un cortafuegos utilizando la herramienta avanzada de filtrado de paquetes IPTABLES que es nativa de Linux. Para que el cortafuegos funcione correctamente también veremos la configuración de los *routers* correspondientes.
- Se montará un servidor de VPN utilizando el protocolo WireGuard.
- Y se realizarán pruebas de conexión y de rendimiento utilizando un teléfono móvil y un portátil.

1.5 Estructura

El contenido del documento está repartido en 8 apartados principales: en el primer apartado, se presenta una pequeña instrucción donde se exponen las motivaciones y los objetivos que se esperan cumplir, así como el impacto esperado el mismo y la metodología a seguir. Después, en el segundo apartado, se encuentra la situación actual de la tecnología y una pequeña crítica de la misma. Seguidamente, en el tercer apartado, se plantea el análisis del problema, detallando los materiales necesarios para el desarrollo del proyecto y el marco legal del mismo. A continuación, en el cuarto apartado, se exponen los pasos seguidos para la preparación y desarrollo del trabajo. Luego, en quinto apartado, se analizan los conocimientos extraídos. Siguiendo en el sexto apartado, con las conclusiones obtenidas, así como los posibles trabajos futuros. Finalmente, en el séptimo y último apartado se indican las referencias a los contenidos consultados durante la realización del trabajo y este documento.

2 Estado del arte

Como se ha comentado en el apartado 1 de este documento, se busca dar conexión y seguridad a una pequeña intranet local de una empresa. Para poder hacer una buena compresión del estado del arte se ha decidido dividir y estudiar diferentes temas que están englobados en este trabajo, con el propósito de facilitar la comprensión de la situación actual. Los puntos que se van a tratar son los siguientes:

- La seguridad para las pequeñas empresas, visto desde el marco legal.
- Cortafuegos que una empresa puede utilizar.
- Servidores de VPN.

2.1 Seguridad

La seguridad es un tema sobre el que hay muchos artículos puesto que es muy general. Se han encontrado, libros, proyectos, estándares y demás documentación en la que habla de cómo mejorar la seguridad de una empresa. Hay muchos modelos de seguridad desarrollados, de hecho, cada país puede tener uno propio con sus variaciones particulares.

En el ámbito internacional podemos considerar la ISO/27001 [2] como referencia mundial para gestionar la seguridad de la información, ya que ha sido desarrollada por la Organización Internacional de Normalización, como el estándar de la seguridad de la información. Si utilizamos este estándar podremos asegurar los activos críticos, así como gestionar los riesgos más eficientemente, lo que permite, además, evitar los daños a nuestra marca por posibles ataques o posibles multas debido a alguna regulación de expediente ya que estamos utilizando el estándar general.

En el ámbito nacional, existe el Centro Criptológico Nacional y Centro Nacional de Inteligencia CCN-CERT [3] que ha desarrollado el ENS. Debido a esto, se ha decidido no utilizar la ISO27000 directamente porque se tiene una variación desarrollada para las características apropiadas que se necesitan en España.

Por otro lado, en el ámbito local, uno de los últimos trabajos que se ha realizado es: “Mejora al sistema de seguridad de una empresa mediante gestión de identidades” desarrollado por Hector Sanchis[4]. En este proyecto se utiliza la tecnología *One Identity*

para la demostración de que la gestión de identidades, es la base de la seguridad para las empresas en la actualidad.

Actualmente, en RiuNet [5] si se utiliza la palabra clave “seguridad”, aparecen un total de 34668 resultados. Esto es debido a que la rama de la seguridad tiene muchas vertientes y es muy complicado abarcar todo.

También llama la atención es el siguiente proyecto: “Metodología para la gestión de ciberincidentes. Apoyo para la implantación de la guía CCN-STIC 817 a profesionales informáticos”, desarrollado por Carlos Zaragoza. [6] Donde proporciona un fichero que profundiza en el esquema de seguridad nacional, más concretamente en la parte de ciberincidentes CCN-STIC 817. Es digno de mención ya que en este proyecto también desarrolla una parte del ENS.

Luego de observar la situación actual en cuanto al marco legal y la seguridad, destaca el hecho de que para las empresas no es sencillo comprender la información disponible ya que consta de muchos puntos y aspectos, que además se encuentran en un lenguaje que no es coloquial, por eso se ha decidido dar unas pequeñas pautas que se pueden seguir.

2.2 Cortafuegos

Los cortafuegos son una de las barreras que tenemos para proteger nuestra red, pueden ser un dispositivo físico o virtual. También nos ayudan a analizar el tráfico que se produce en nuestros sistemas y permiten hacer un filtrado de los paquetes que entran y salen por un punto específico de nuestra red.

Hay empresas que venden dispositivos físicos y virtuales para actuar de barrera como por ejemplo SonicWall [7]. Pero el precio elevado de estos dispositivos dificulta para una pequeña empresa plantearse una instalación de este tipo, además, hay que hacer unos cursos y certificarse para poder llegar a entender su funcionamiento y aplicar las reglas de filtrado correctamente.

2.3 VPN

Las siglas VPN hacen referencia a *Virtual Private Network,* es una herramienta que permite redirigir el tráfico de internet a través de un túnel seguro. En la actualidad las VPN se han convertido en un medio de lo más extendido en internet para poder tener

seguridad en las comunicaciones, puesto que los datos que enviamos están cifrados y son más difíciles de leer. También, nos permiten tener acceso a contenido digital bloqueado en internet por las políticas de cada país, como, por ejemplo, series en empresas de *streaming*.

Hay muchas empresas que se dedican a ofrecer este servicio. Pero, si utilizamos este servicio hay que tener cuidado con la letra pequeña, ya que hay muchas VPN's que son gratuitas, pero en los términos y condiciones del servicio hay alguna cláusula que dice que vas a compartir el ancho de banda de tu conexión con otros usuarios.

En este proyecto lo que interesa es la creación de un servidor de VPN, habiendo muchos protocolos que nos permiten generar nuestro propio servidor para poder extender nuestra red de área local de manera segura por internet.

Algunos de los protocolos que existen en la actualidad son: OpenVPN [8], IKEv2 [9], L2TP/IPSec [10], Wireguard [11], …

Aunque en este proyecto se ha implementado el protocolo WireGuard. El protocolo más extendido en la actualidad es OpenVPN, ambos son protocolos de código abierto a continuación, se muestra una pequeña comparativa entre ambos.

OpenVPN

- + de 600.000 líneas de Código
- Inicio 2001
- Es más lento
- Es compatible prácticamente con todos los algoritmos de cifrado y de transferencia de datos que existen.
- En cuanto a la seguridad OpenVPN es muy seguro puesto que se han hecho ataques de todos los tipos contra este protocolo y no se ha conseguido vulnerar si se pone una clave segura.

WireGuard

- 3.700 líneas de Código
- Primera versión estable 2021
- Es más rápido
- Los algoritmos que se utilizan son los más modernos y para transferencia de datos solo se utiliza UDP.
- Wireguard también es igual de seguro, pero como a aparecido hace poco todavía no esta tan auditado como el otro protocolo.

3 Análisis del problema

En un trabajo de estas características, se puede analizar el problema desde muchos puntos de vista, tomando en este caso la perspectiva del problema desde la necesidad de los materiales que se van a utilizar, así como la seguridad y el marco legal, y la configuración de red.

3.1 Material para desarrollar el proyecto

Siguiendo la motivación de desarrollar un sistema que sea accesible y económico, se utilizan componentes que pueden ser adquiridos en tiendas habituales tales como Amazon[1], Ebay[2], pudiendo ser incluso productos de segunda mano, en vez de tener que acudir a tiendas especializadas que son más costosas. A continuación, se detallan los materiales necesarios.

3.1.1 Starter Kit

Se ha decidido trabajar con un *pack* de iniciación a Raspberry Pi 3 B+ este pack es todo material reacondicionado y así estamos contribuyendo a la sostenibilidad del medio ambiente reutilizando material que otros han descartado porque tenía algún defecto de fabrica que se ha reparado posteriormente. Este pack lleva todo lo necesario para poder empezar a desarrollar nuestro proyecto. En este caso hemos elegido el modelo 3 B+ debido a que tiene las prestaciones que necesitamos, a un precio muy económico, no es la última versión de Raspberry Pi, pero para la configuración que necesitamos hacer tiene los requisitos suficientes.

3.1.2 Ethernet RJ45

Adaptador USB a Ethernet RJ45, es el conector auxiliar que necesitaremos conectar a nuestra Raspberry Pi para poder tener 2 subredes.

[1] https://www.amazon.es
[2] https://www.ebay.es

3.1.3 Routers

Vamos a utilizar dos *routers* diferentes, el primero es el que nos proporciona nuestro ISP, y el segundo es un *router* D-Link DWR-116.

3.1.4 Material Informático

El material informático es el equipamiento que hemos utilizado para que el proyecto tenga una consistencia real, esto nos ha ayudado para poder hacer pruebas de usuario final. Hemos decidido utilizar un *switch*, un ordenador de sobremesa, un portátil, dos dispositivos móviles y cables RJ45.

3.2 Seguridad y el marco legal

Este apartado está pensado para tener unas pautas iniciales de seguridad las cuales poder aplicar en una empresa, para ello hemos estudiado el Esquema Nacional de Seguridad, a partir de ahora ENS y se han implementado un sencillo esquema con los puntos que son más interesantes.

Hay que tener en cuenta, que, para una pequeña empresa, uno de los puntos más importantes es el de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales. Esta ley entró en vigor en diciembre de 2018 y recoge el tratamiento de todos los datos y ficheros de carácter personal que se tienen sobre los trabajadores o los clientes que utilizan nuestros servicios. En este trabajo no se profundiza más en esto porque se sale del ámbito de estudio del proyecto, pero puede consultarse en el boletín oficial del estado [12].

3.2.1 Medidas del ENS

El ENS tiene varios grupos de medidas y nosotros vamos a enumerarlos todos, siendo para este trabajo más destacable el tercer grupo, ya que es con el que vamos a lograr unas medidas básicas de seguridad, pero hay que tener en cuenta que si somos una empresa debemos tener otras precauciones, especialmente si recibimos algún tipo de ataque. Deberemos tener redactadas unas normas de cómo actuar y unos procedimientos a seguir, por ejemplo, si hemos perdido información sensible de nuestros trabajadores o nuestros empleados; habría que poner una denuncia ante la agencia española de protección de datos y para esto tendremos que contactar con un abogado.

- Marco Organizativo, las medidas que se incluyen en este apartado son las que están relacionadas con la organización en general de la seguridad.
    - Política de seguridad
    - Normativa de seguridad
    - Procedimientos de seguridad
    - Proceso de autorización

- Marco Operacional, estas medidas están centradas en proteger la operación del sistema.
    - Planificación
    - Control de acceso
    - Explotación
    - Servicios externos
    - Continuidad del servicio
    - Monitorización del sistema

- Medidas de Protección, este punto es el que más nos interesa debido a que se centra en proteger los activos que tenemos en la empresa, dependiendo del nivel de seguridad que queramos aportar.

  Hay tres niveles de seguridad: bajo, medio y alto. La elección del nivel de seguridad que queremos implementar para cada una de las partes de la organización está ligado a las consecuencias y repercusiones directas que tendría la caída o el fallo de este sistema en nuestra organización.

- Instalaciones e infraestructuras. Vamos a considerar nuestra infraestructura a los dispositivos esenciales para poder desarrollar una actividad laboral, esto quiere decir que tanto los *routers* como la Raspberry pi van a estar categorizados en este punto de seguridad, ya que sin estos no podríamos tener una conexión VPN y no podríamos desarrollar ningún trabajo desde otro punto que no fuera la propia oficina.

  Para segurizar las infraestructuras, se consideran dos aspectos diferentes. El aspecto físico, que tiene como punto de vista todas las posibles catástrofes naturales, como, por ejemplo, un incendio o un terremoto. Por otro lado, el aspecto virtual, donde nos referimos a las claves que podemos generar tanto de los *routers* como del usuario pi de la Raspberry pi.

Para el *router* R1, que es el que nos da el operador y que está directamente conectado a Internet, lo primero que vamos a hacer es desactivar la parte de la conexión wifi. Con esto, lo que conseguimos es que solo se puedan conectar equipos que estén cableados con el *router.* Esta zona la vamos a llamar zona desmilitarizada y es donde conectaremos los servidores web que tengamos públicos en nuestra organización.

También, tenemos que modificar la clave que nos proporciona nuestro proveedor de internet por defecto. Crearemos una más segura, para que si algún usuario se conecta a nuestra red no pueda manipular nuestro sistema. La clave debe tener caracteres especiales, mayúsculas, minúsculas y algún número. En este caso la longitud que hemos elegido es superior a 8 caracteres. Debido a que al hacer una auditoria a una red wifi utilizando Kali, que es un sistema operativo *open source* utilizado para hacer auditorias de seguridad. Al utilizar claves con menos de 8 caracteres, con un ataque de fuerza bruta a través de los diccionarios genéricos que existen se puede obtener la contraseña en menos de dos minutos. Se puede obtener más información de esto en el libro 0xWord Pentesting con Kali [13].

- Gestión del personal, este es uno de los puntos más vulnerables debido a que las personas cometemos errores y es más fácil encontrar puntos débiles que poder explotar para sacar la información.

  La manera de aumentar la seguridad en nuestro personal es proporcionando herramientas adecuadas a cada tipo de usuario que tengamos contratado. También la formación de nuestros empleados es un punto crítico puesto que cuanto más formados estén es más fácil que puedan detectar si están delante de un correo con una intención de phishing (correos fraudulentos que intentan engañar al destinatario), o si alguien encuentra un USB delante de su puesto de trabajo que tenga claro que como no conoce la procedencia no tiene que conectarlo a su estación de trabajo porque puede tener algún tipo de ransomware o malware, los cuales son programas con fines mal intencionados. El ransomware cifra la información del sistema que está almacenada en el disco duro. El malware disminuye la eficiencia de los equipos infectados.

- Protección de los equipos, que para nuestro caso no aplica.

- Protección de las comunicaciones. Para proteger las comunicaciones que tenemos en la empresa con los empleados que están teletrabajando, hemos

utilizado nuestro dispositivo Raspberry Pi, siendo este configurado como punto VPN. Para implementar dicha tecnología se ha utilizado WireGuard, esto está desarrollado en el apartado 4.2.7.

- Protección de soportes de información
- Protección aplicaciones informáticas
- Protección de la información
- Protección de los servicios

3.3 Configuración de la red

El uso de un buen diagrama de red nos permite tener una visión de nuestra organización clara y sencilla. Microsoft da unas pequeñas directrices las cuales nos pueden ayudar a desarrollar un buen diagrama [14]. De este modo, podremos ver cómo interactúan todos los equipos informáticos entre sí. Esto nos ayudará a la hora de tomar las decisiones de seguridad, por ejemplo, decidir dónde vamos a implementar un cortafuegos o ver qué dispositivos son más susceptibles de recibir ataques.

Para poder desarrollar un buen esquema de red, lo primero que tenemos que hacer es recopilar todos los dispositivos que tenemos en nuestra organización. De esta manera, cuando tengamos el diagrama de red, tendremos la capacidad de ver el funcionamiento de nuestra empresa de una forma relativamente sencilla. Los elementos que hemos identificado que van a ser utilizados, están recopilados en el punto 3.1. Usando para ellos el esquema de red que aparece en la Figura 1.

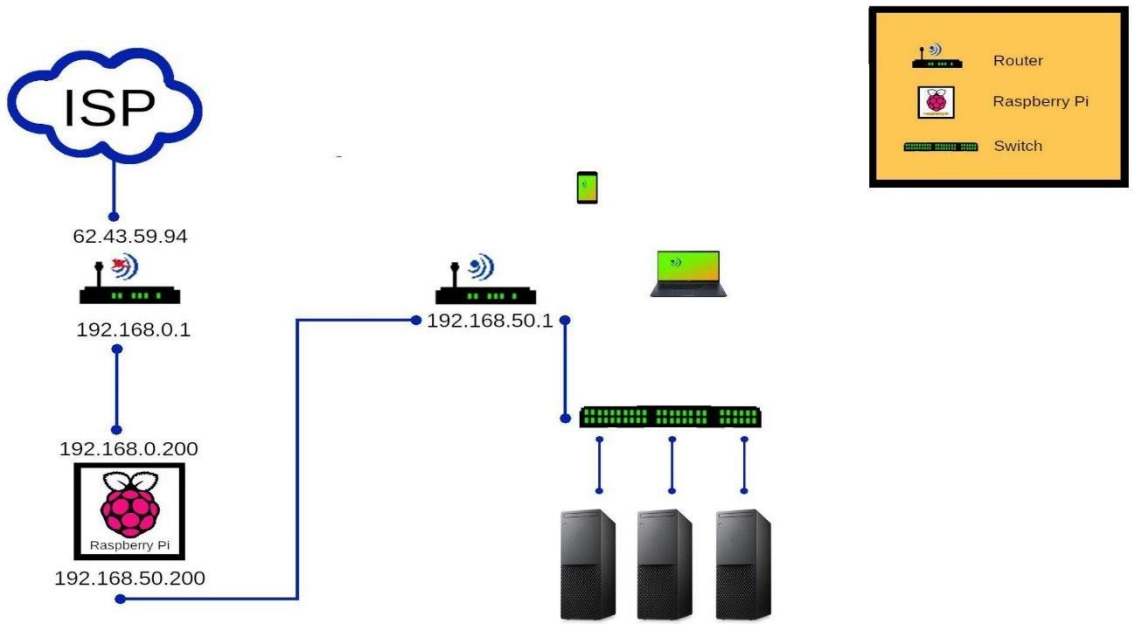

Figura 1 – Esquema de red

4 Desarrollo y comprensión

4.1 Fase de preparación

Esta fase se ha dividido en cuatro partes. El orden en las que se ejecutan es muy importante porque nos garantiza que posteriormente podamos desarrollar el proyecto sin problemas.

4.1.1 Raspberry Pi Imager

Se ha decidido utilizar Raspberry Pi Imager que es una herramienta que da formato a la tarjeta microSD y permite precargar el sistema operativo, hay muchas aplicaciones que pueden hacer esto, pero se ha elegido ésta, porque está diseñada especialmente para Raspberry. Es multiplataforma, por lo que se puede instalar tanto en Windows como en MAC o Linux. No es necesario descargar la imagen del sistema operativo que queremos instalar directamente, ya que nos da la opción de seleccionar el sistema operativo y lo descarga directamente de su repositorio.

Para la instalación de esta aplicación hay que tener en cuenta que es necesario utilizar un ordenador que tenga un sistema operativo, en este caso se ha utilizado un Windows y se ha descargado la aplicación desde la página de Raspberry Pi [15] seleccionando el sistema operativo de Windows. El proceso de instalación es muy sencillo, solo hay que presionar en instalar (ver Figura 2). Una vez descargado el ejecutable, este cargará una barra de estado indicando el estado en que se encuentra la instalación y finalmente se debe pulsar en finalizar.

Figura 2 – Instalador Raspberry Pi Imager

Una vez Instalado el programa, se debe seleccionar el Sistema operativo “Raspberry Pi OS 32b” que es el recomendado y además hace la descarga online.

Se selecciona la tarjeta microSD y con todo esto seleccionado ya da la opción de pulsar sobre “WRITE” se puede apreciar en la Figura 3, este proceso puede tardar un poco, ya que depende de cuanta memoria tenga la tarjeta. Una vez el proceso ha terminado avisa que ya se puede retirar la tarjeta y con esto, el sistema operativo estará preparado para el primer inicio.

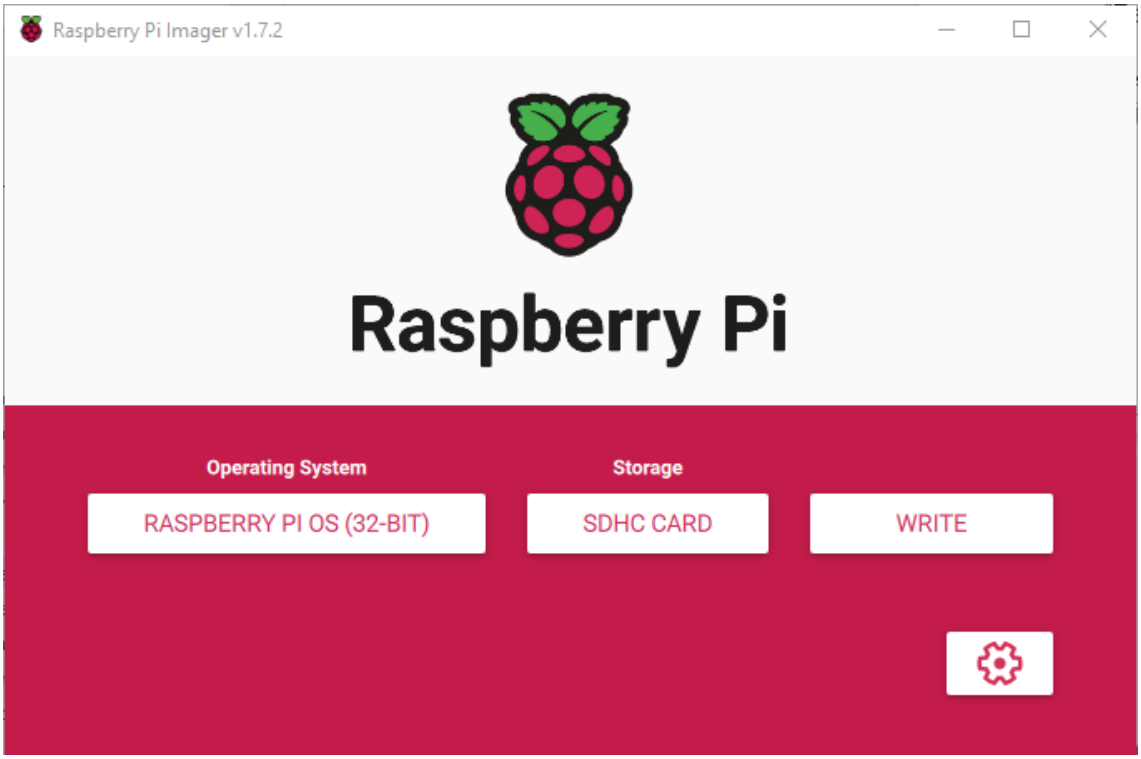

Figura 3 – Interfaz Raspberry Pi Imager

4.1.2 Montaje de la Raspberry Pi

Una vez la tarjeta está preparada con el sistema operativo, se procede a montar la Raspberry Pi. Hay muchas fuentes de información en internet que nos tutorizan en el montaje de dispositivos similares, un ejemplo del montaje sería el siguiente enlace [16]. Este proceso de montaje depende de la Raspberry que se utilice.

En la que se ha utilizado, se han tenido que ajustar dos disipadores, Figura 4 uno para la CPU y el otro para el chip LAN, hemos ajustado la placa base a la carcasa de plástico y hemos introducido la tarjeta microSD que viene en el kit de Raspberry Figura 5.

Figura 4 - Disipadores

Figura 5 - Raspberry Pi

4.1.3 Conexión del entorno

Se va a explicar la unión de todos los componentes físicos que se van a utilizar en la empresa, es importante realizar bien la instalación, ya que, si alguno no está bien conectado, cuando realicemos la configuración de la Raspberry, habrá partes que no funcionen correctamente.

Para que sea más fácil la identificación de los componentes, los vamos a nombrar, describir y explicar. Se puede ver en la Figura 6 para más facilidad visual.

- R1 – *Router* que nos proporciona nuestro ISP.
- R2 – *Router* que solo va a tener la función de punto de acceso.

- PI – Raspberry Pi es el componente más importante, ya que es donde se montará y configurará el cortafuegos, el servidor de VPN, el servidor de DHCP, el servidor de apache y PHP, en definitiva, toda la estructura del proyecto.
- USB-ETH – es el adaptador de USB a Ethernet que se utiliza para poner una segunda tarjeta de red a nuestra PI.

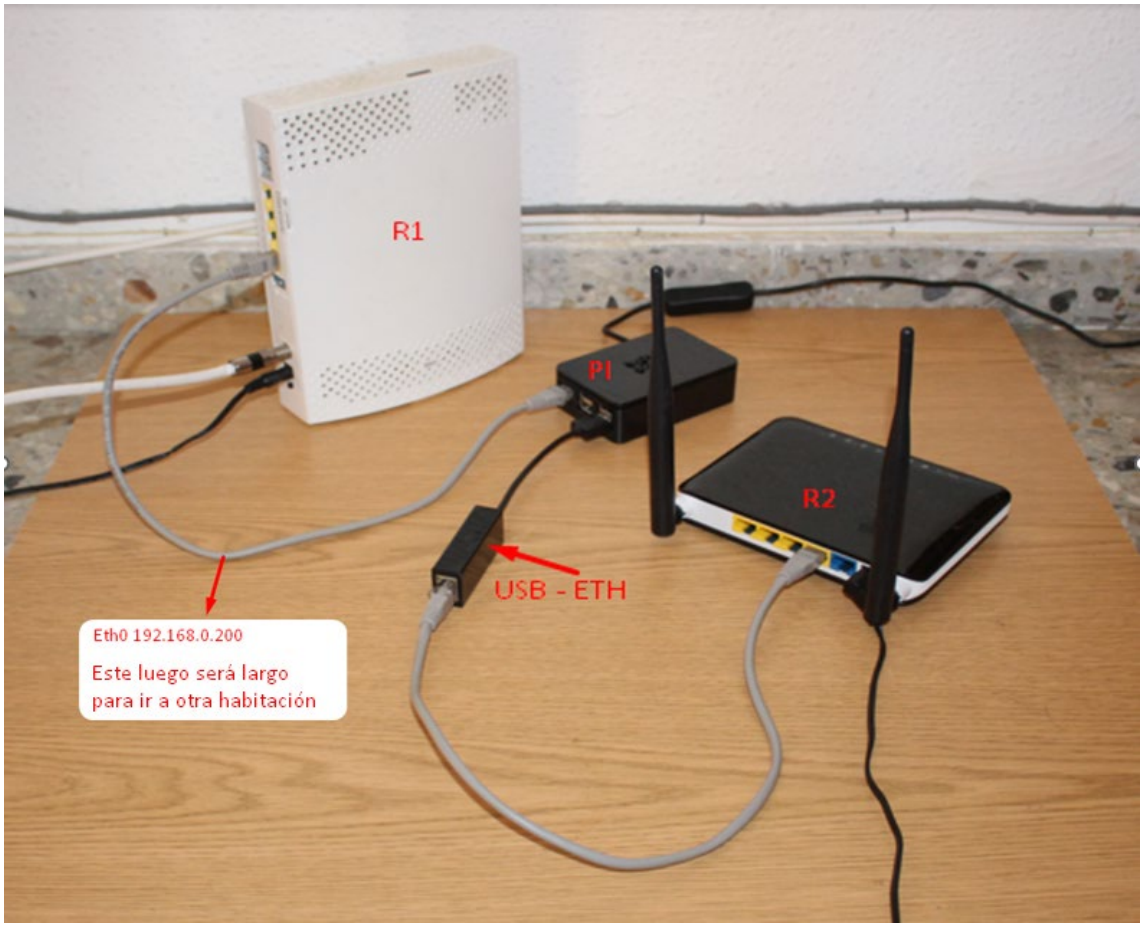

Figura 6 - - Red Física

Se ha decidido poner un cable corto desde R1 a PI en la Figura 7 para poder tener todos los elementos de conexión juntos, pero ahora cambiamos ese cable por uno más largo y movemos PI y R2 a otra habitación que es donde se encuentra el *switch*.

A la Raspberry conectamos un USB-ETH, un cable de alimentación, un teclado, un ratón y un monitor conectado por HDMI. En las ilustraciones, no se van a mostrar el teclado, el ratón, ni el monitor, porque a nivel visual enmarañan las conexiones que realmente nos interesan, pero es indispensable para poder configurar inicialmente la Raspberry.

Se conecta R1 con PI, PI con R2 y R2 con el *switch* al que tendremos conectado un PC. Tal y como se observa en la Figura 7.

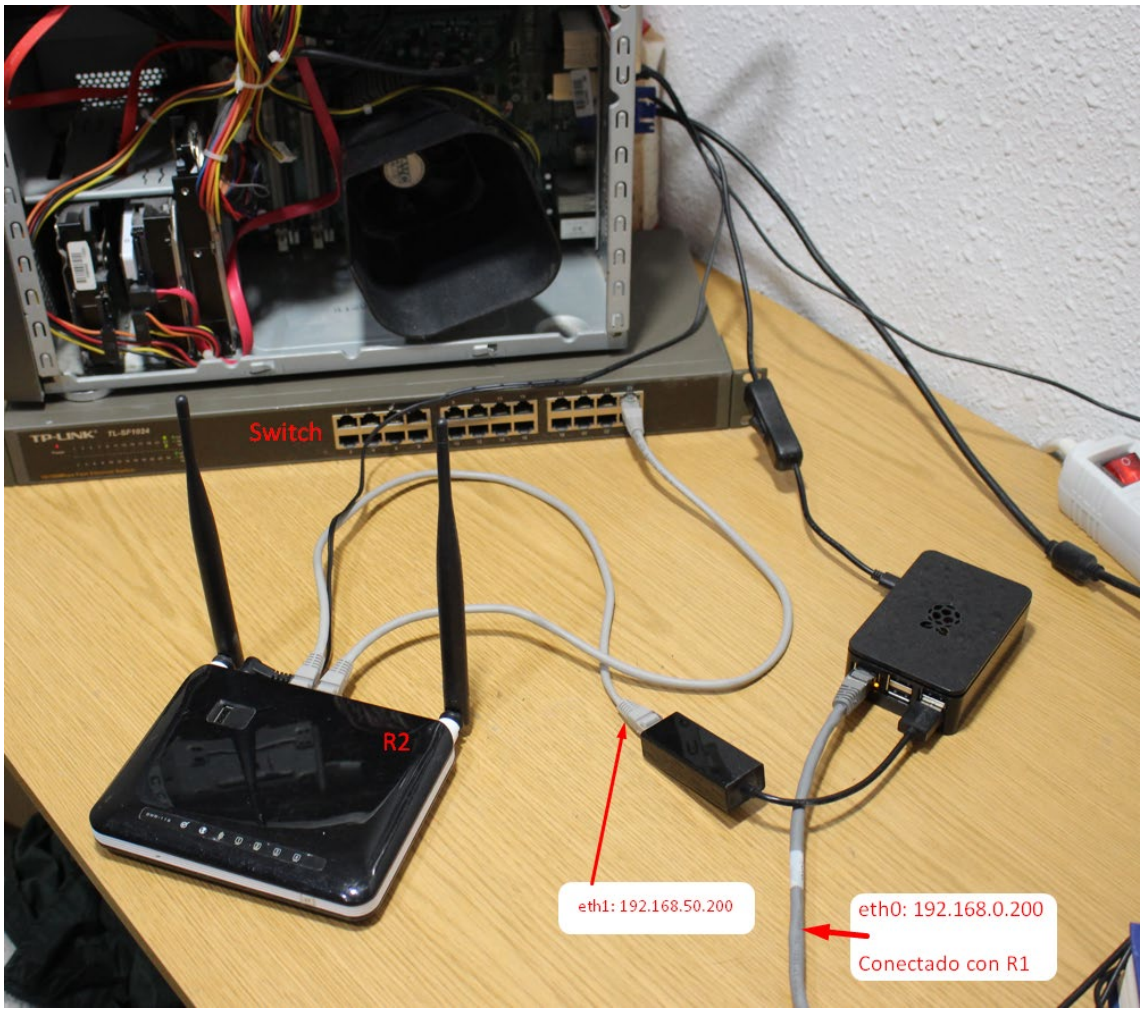

Figura 7 - Red física

En R2, todos los cables de red los ponemos en los puertos de LAN, el puerto de conexión WAN lo dejamos sin conectar, como se puede apreciar en la Figura 8.

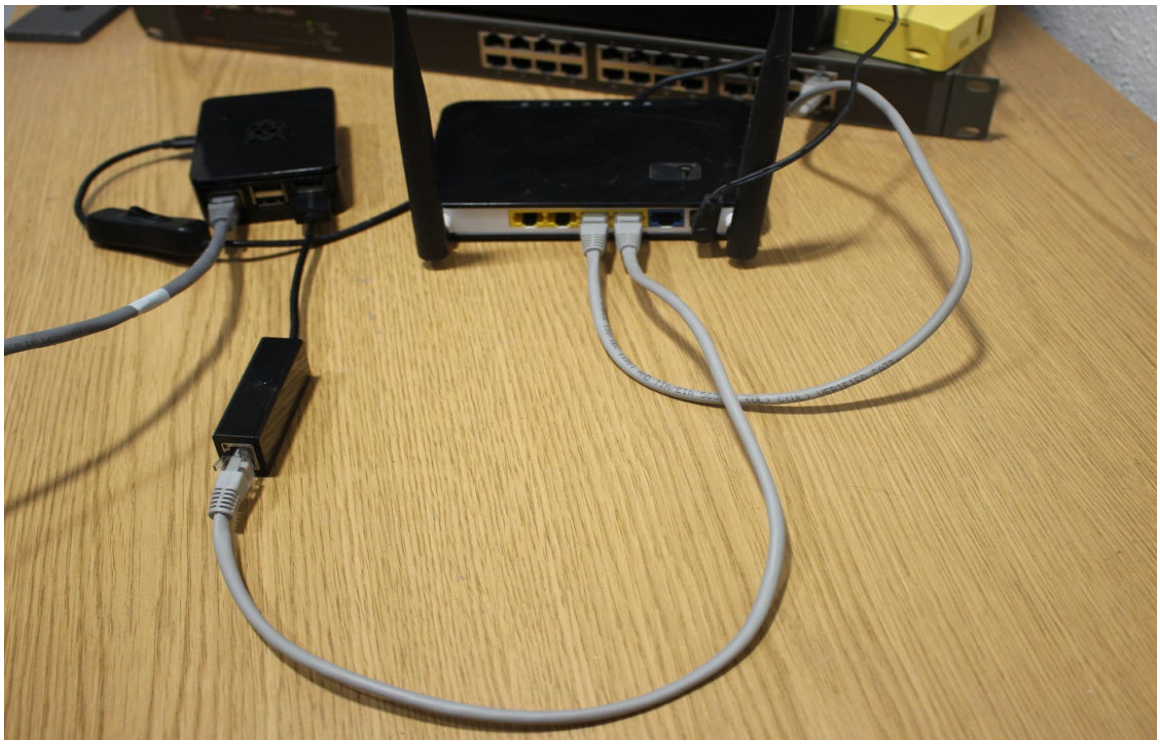

Figura 8 - Red física

4.1.4 Raspberry Pi primer inicio

Ahora que ya lo tenemos todo conectado, es el momento de arrancar nuestra Raspberry. Cuando presionamos el botón que le da corriente a nuestra Raspberry veremos una pantalla de arranque y tras unos segundos nos aparecerá la pantalla de bienvenida en la que se nos indica da la dirección IP que se nos ha asignado por DHCP ver Figura 9. En este caso no es muy importante porque más adelante configuraremos IP's estáticas.

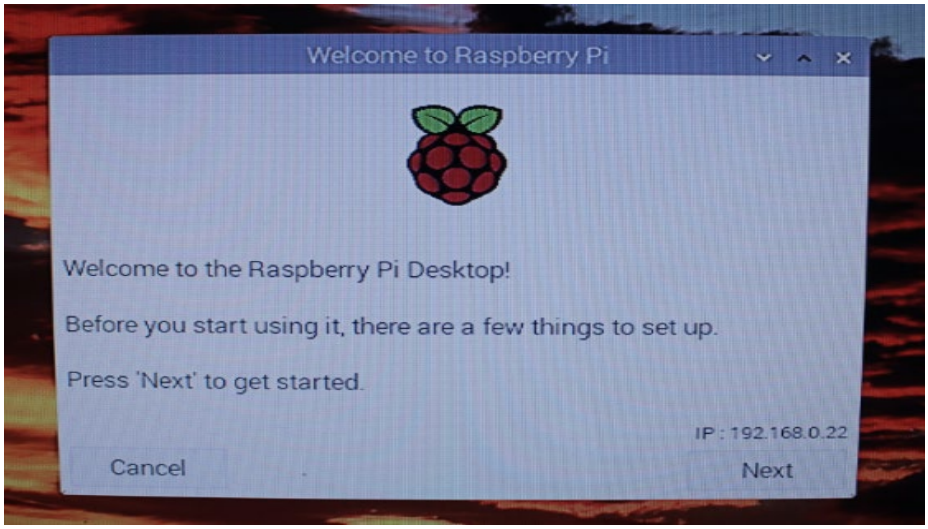

Figura 9 - Dirección IP

Seleccionamos el idioma como se muestra en la Figura 10.

Figura 10 - Selección de idioma

Introducimos la contraseña del usuario pi (administrador), ver Figura 11, que como hemos comentado en el apartado de análisis de seguridad, debe tener más de 8 caracteres y contener mayúsculas minúsculas números y algún carácter especial. Un ejemplo de contraseña segura sería “L0stransistor3s.8889” la contraseña que hemos utilizado todavía es más compleja.

Figura 11 - Contraseña Pi

Luego, nos solicita que conectemos la wifi nosotros. Este paso nos lo saltaremos porque solo nos interesa la parte de red cableada, ver Figura 12.

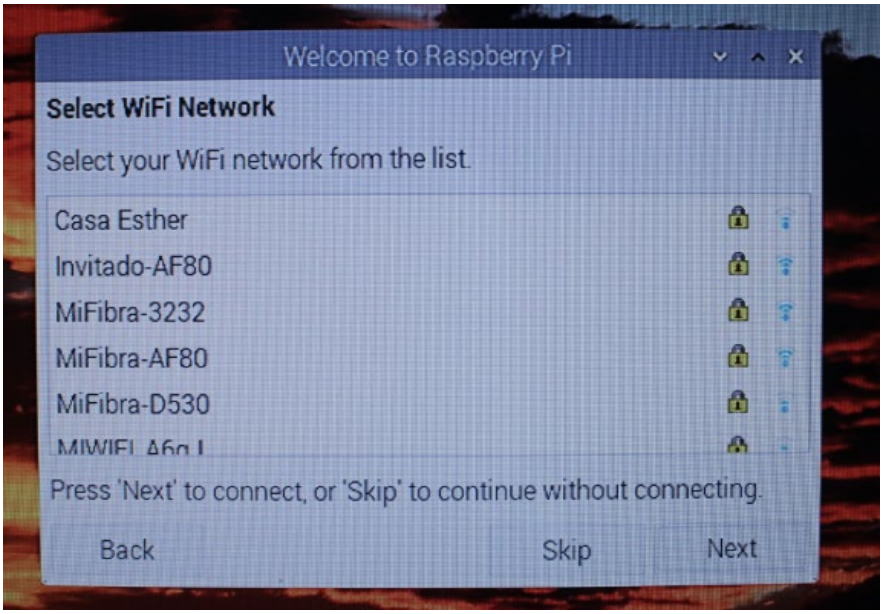

Figura 12 - Wifi

Actualizamos el Software, ver Figura 13

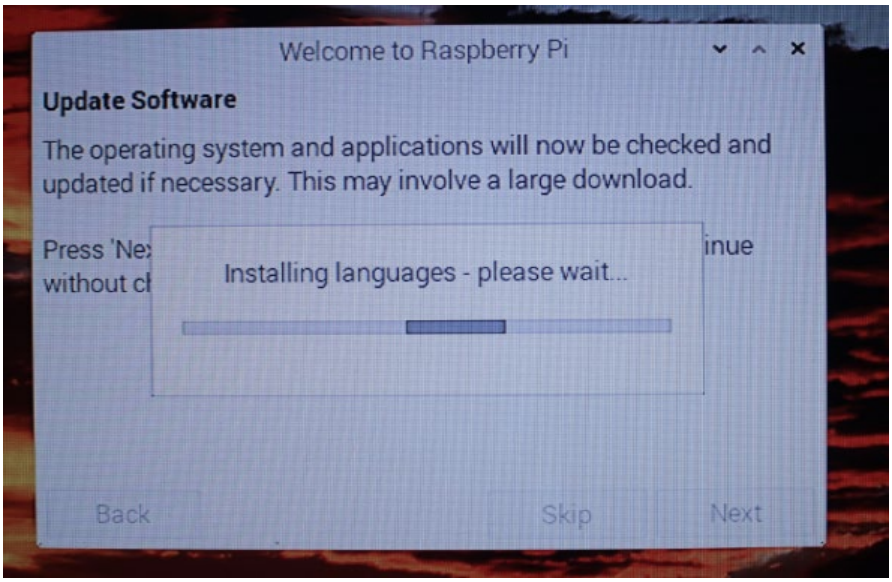

Figura 13 - Update Software

Por último, reiniciamos la Raspberry Pi, ver Figura 14

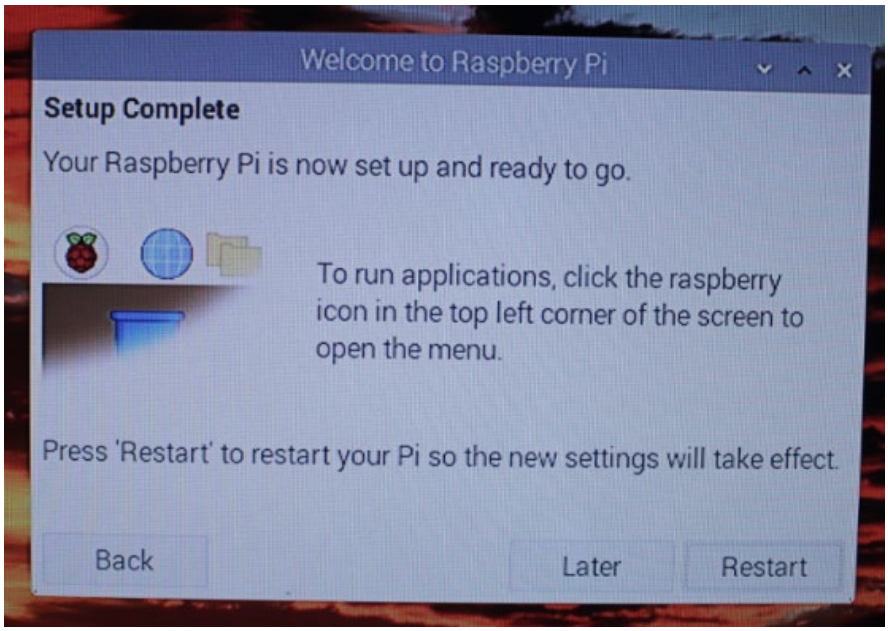

Figura 14 - Reiniciamos Raspberry Pi

Figura 15 - Primer inicio

Cuando termina de reiniciar, ver Figura 15, ya tenemos la fase de preparación correctamente finalizada. Ahora es cuando podemos empezar a configurar la Raspberry para que haga de servidor y de cortafuegos.

4.2 Fase de implementación

Se ha dividido esta fase del proyecto en seis pasos de configuración más pequeños, siendo el paso indicado en el punto 4.2.1 el único que con obligatoriedad se debe realizar en primer lugar, los demás pasos se pueden configurar independientemente los unos de los otros sin importar el orden a seguir. En este proyecto la mayoría de la configuración se ha realizado utilizando comandos desde la terminal de Linux.

4.2.1 Tarjetas de red

Lo primero que tenemos que hacer es abrir un terminal para poder instalar las actualizaciones que puedan quedar pendientes para ello vamos a utilizar los comandos ***update,*** ver Figura 17, y ***upgrade,*** ver Figura 16.

```
pi@raspberrypi:~/Desktop $ sudo apt-get update
Des:1 http://raspbian.raspberrypi.org/raspbian bullseye InRelease [15,0 kB]
Des:2 http://archive.raspberrypi.org/debian bullseye InRelease [23,6 kB]
Des:3 http://raspbian.raspberrypi.org/raspbian bullseye/main armhf Packages [13,2 MB]
Des:4 http://archive.raspberrypi.org/debian bullseye/main armhf Packages [257 kB]
Descargados 13,5 MB en 23s (601 kB/s)
Leyendo lista de paquetes... Hecho
pi@raspberrypi:~/Desktop $
```

Figura 17 - Update

```
pi@firepivpn:~ $ sudo apt-get upgrade
```

Figura 16 - Upgrade

Luego, se procede a la configuración de las tarjetas de red. Primero miramos el estado actual utilizando el comando ***ifconfig,*** ver Figura 18***.*** Donde lo que nos interesa ver es que la eth0 tiene la dirección 192.168.0.22 que es la que le ha dado el *router* del ISP por DHCP y la eth1 no tiene ninguna configuración.

```
pi@raspberrypi:~ $ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.0.22  netmask 255.255.255.0  broadcast 192.168.0.255
        inet6 fe80::b871:1359:8b6a:cdbc  prefixlen 64  scopeid 0x20<link>
        ether b8:27:eb:e6:c7:4c  txqueuelen 1000  (Ethernet)
        RX packets 237438  bytes 55681399 (53.1 MiB)
        RX errors 0  dropped 6  overruns 0  frame 0
        TX packets 5081  bytes 316317 (308.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

eth1: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
        ether 00:e0:4c:41:e1:f5  txqueuelen 1000  (Ethernet)
```

Figura 18 - ifconfig

Ahora editamos en el archivo Interfaces, ver Figura 19 para poner las tarjetas de eth0 y eth1 con una configuración estática, como se estableció en el diseño en el esquema de red, véase la Figura 1 .

```
pi@raspberrypi:~ $ sudo nano /etc/network/interfaces
```

Figura 19 – interfaces

La configuración del archivo Interfaces quedaría como se muestra en la Figura 20

```
  GNU nano 5.4                                    /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Include files from /etc/network/interfaces.d:
source /etc/network/interfaces.d/*

# Red eth0 con ip estatica 192.168.0.200
auto eth0
iface eth0 inet static
address 192.168.0.200
netmask 255.255.255.0
network 192.168.0.0
broadcast 192.168.0.255
gateway 192.168.0.1

# Red eth1 con ip estatica 192.168.50.200
auto eth1
iface eth1 inet static
address 192.168.50.200
netmask 255.255.255.0
network 192.168.50.0
```

Figura 20 - archivo interfaces

Se puede observar que a la tarjeta de eth0 le hemos puesto una IP estática que coincide con 192.168.0.200 y a la tarjeta de red eth1 le hemos puesto la dirección 192.168.50.200.

Es necesario reiniciar la Raspberry para que se apliquen bien los cambios y modificaciones que hemos hecho a las tarjetas de red. Una vez el sistema está operativo, ya podremos comprobar que las direcciones IP's que están establecidas para las tarjetas eth0 y eth1 son las correctas, ver Figura 21.

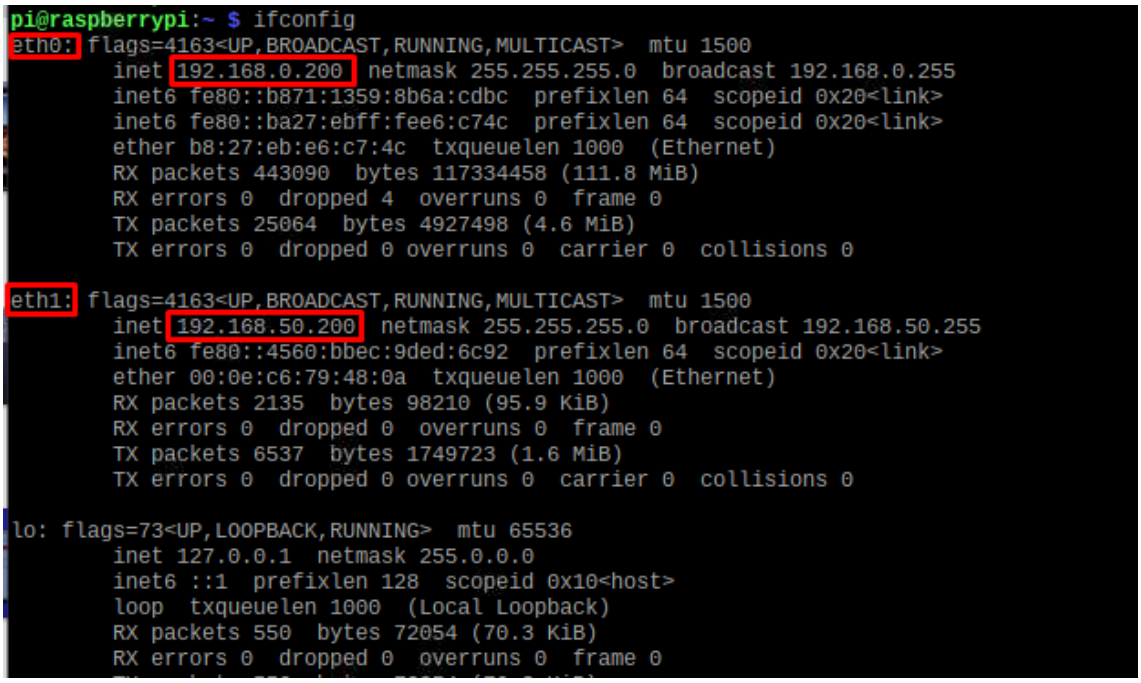

Figura 21 – Configuración eth

4.2.2 VNC

Ahora que ya tenemos las tarjetas de red configuradas correctamente vamos a configurar el VNC viewer. Este programa está desarrollado para conectarse de forma remota a un equipo y no tener que utilizar un monitor conectado directamente, permitiendo así poder trabajar en remoto [17].

Para ello ejecutamos los comandos install realvnc-vnc-server, ver Figura 22, install realvnc-vnc-viewer, ver Figura 23 y raspi-config, ver Figura 24

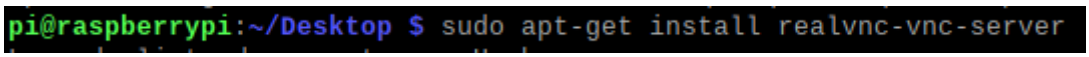

Figura 22 - vnc server

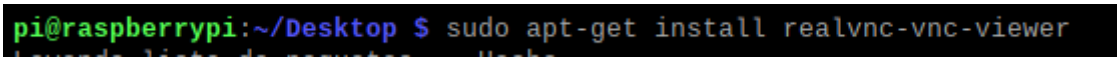

Figura 23 - vnc viewer

Figura 24 - raspi-config

Una vez escribimos el comando raspi-config, se despliega el menú para configurar la conexión remota de nuestro dispositivo. Tenemos que pulsar en el apartado de interfaces, ver Figura 25.

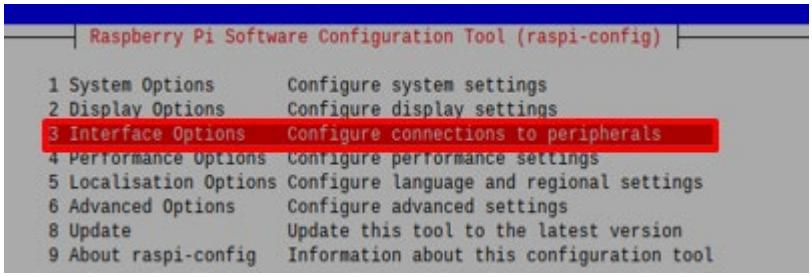

Figura 25 - interfaces

Ya dentro de este menú, seleccionamos el protocolo VNC y lo marcamos como "*Enable*", ver Figura 26.

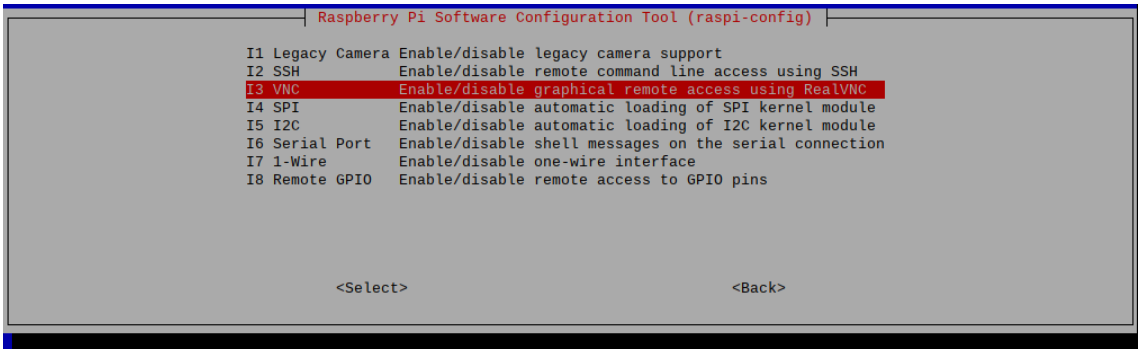

Figura 26 - VNC Enable

Otra opción es activar el escritorio remoto utilizando la interfaz gráfica pulsando en "Preferencias" y luego en "Configuración de Raspberry Pi" y en la pestaña de "Interfaces" dejamos activada la opción de VNC.

Luego, procedemos a cambiar el nombre de la Raspberry pi que tenemos en nuestra red. Esto lo hacemos para tener más seguridad, ya que por defecto siempre aparece con el mismo nombre "raspberrypi". Editamos el fichero de *hostname* utilizando "nano" y en este caso le hemos puesto el nombre de "firepivpn", luego lo presionamos los atajos de teclado "Ctrl + O" y "Ctrl + X" para guardar y salir y seguidamente para que los cambios sean efectivos, tenemos que reiniciar el sistema.

Probamos que está funcionando correctamente, para ello utilizando otro equipo conectado a la misma red que la Raspberry Pi y conectando con un cliente de VNC, podemos conectarnos a la dirección IP o al nombre directamente, ver Figura 27.

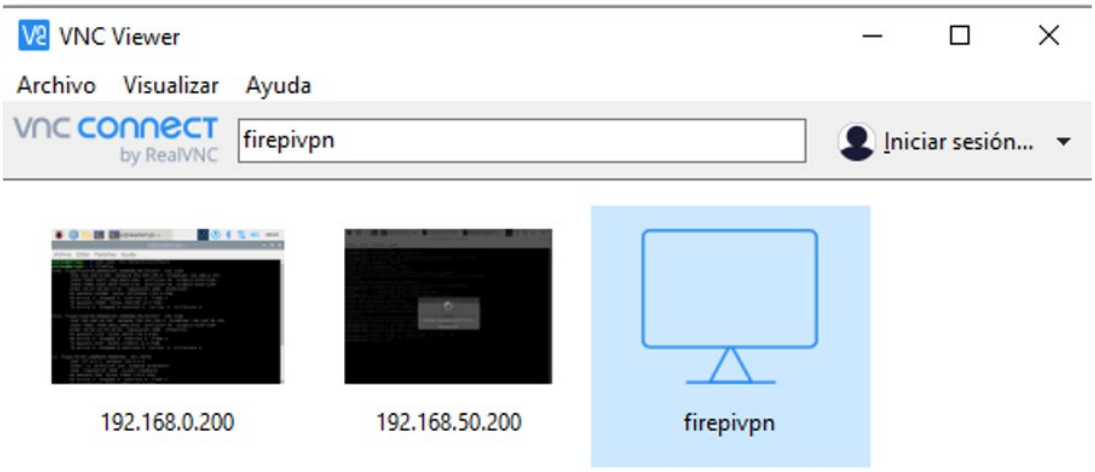

Figura 27 - Conexión VNC

4.2.3 Routers

Para que la red quede como en el esquema que hemos planteado tenemos que configurar los dos r*outers.*

Accedemos al *router* R1 proporcionado por la compañía introduciendo la dirección IP 192.168.0.1 en un navegador. Si es la primera vez que accedemos, le cambiamos la contraseña de administrador, ya que por defecto viene establecida una genérica contraseña idéntica para todos los *routers* de la misma compañía. Entramos en la pestaña de “WiFi” y procedemos a desactivarla para que solo tenga la conexión por cable con la Raspberry pi, ver Figura 28.

Figura 28 - Desactivar Wifi

A continuación, accedemos a la pestaña que pone “Internet” y creamos una redirección de puertos para el puerto 6149, tanto para el protocolo TCP como para el UDP. Esto lo que nos permitirá, es tener acceso a la VPN desde fuera de nuestra infraestructura, porque estamos redirigiendo el tráfico que llegue a este puerto a la tarjeta que tenemos conectada la Raspberry pi que tiene la dirección IP 192.168.0.200, ver Figura 29.

Figura 29 - Redirección de puertos

Nos conectamos al *router* R2 que solo va a tener la función de punto de acceso. Esto lo que quiere decir, es que no va a proporcionar un servicio de DNS, que es el que se encarga de traducir las páginas que utilizamos en internet por direcciones IP, ni de DHCP, que se encarga de asignar las IP's de nuestra red a cada equipo que tenemos conectado. Esta función queda delegada en nuestra Raspberry pi.

Para proceder a su configuración, lo que debemos tener en cuenta es que hay que deshabilitar el servidor DHCP que lleva el *router* ya que va a ser la propia Raspberry la que nos haga de servidor DHCP. También tenemos que decirle al *router* cuál es la dirección IP estática que nos da salida a internet, que en este caso sería la 192.168.50.200 y configuramos la wifi, ver Figura 30.

Figura 30 - Configuración Wifi

Le hemos puesto como nombre de red R2 y hemos configurado una clave de red con más de 20 caracteres, ver Figura 31.

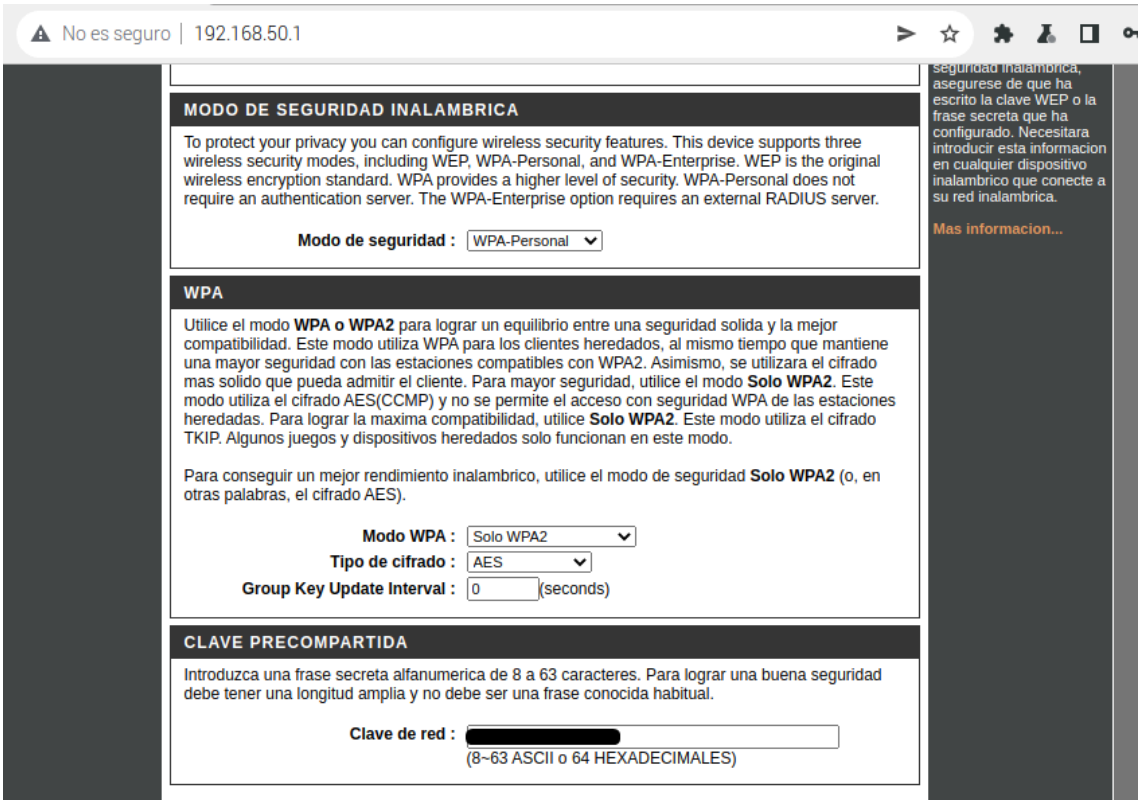

Figura 31 - Clave de red

4.2.4 Servidor DHCP (DNSMASQ)

DNSMasq es una aplicación de software libre que se puede ejecutar en diversos sistemas operativos como Linux o MAC. Sirve para tener un servidor de DNS y DHCP, no consume apenas recursos, por lo que es muy versátil para poderlo instalar en nuestra Raspberry Pi [18].

Optamos por crear el servidor de DHCP antes de empezar a aplicar las reglas de IPTABLES, que será la configuración del cortafuegos. Esto se ha decidido así para que al momento de ejecutar las reglas de IPTABLES para crear el cortafuegos, ya tengamos conexión a internet desde nuestra red de área local. Para instalar el servidor de DHCP instalamos “DNSMasq” ejecutando el comando “install dnsmasq”, ver Figura 32.

```
pi@firepivpn:~/Desktop $ sudo apt install dnsmasq
```

Figura 32 - DNSMasq

Ahora entramos en el archivo de configuración que se encuentra en la ruta “etc/”, ver Figura 33.

```
pi@firepivpn:~/Desktop $ sudo nano /etc/dnsmasq.conf
```

Figura 33 - DNSMasq configuración

Y aplicamos la siguiente configuración, ver Figura 34.

```
  GNU nano 5.4                                          /etc/dnsmasq.conf
# Set the interface on which dnsmasq operates.
# If not set, all the interfaces is used.
#interface=enp5s0

# To disable dnsmasq's DNS server functionality.
port=0

# To enable dnsmasq's DHCP server functionality.
dhcp-range=192.168.50.100,192.168.50.120,255.255.255.0,1h
#dhcp-range=192.168.0.50,192.168.0.150,12h

#ay as Router. Following two lines are identical.
#dhcp-option=option:router,192.168.0.1
dhcp-option=3,192.168.50.200

# Set DNS server as Router.
dhcp-option=6,8.8.8.8

# Logging.
log-facility=/var/log/dnsmasq.log   # logfile path.
log-async
log-queries # log queries.
log-dhcp    # log dhcp related messages.
```

Figura 34 - configuración

En este fichero indicamos el rango de direcciones IP que va a asignar a las maquinas que se conecten, que en este caso van desde la dirección IP 192.168.50.100 a la 192.168.50.120, esto quiere decir que podemos conectar un máximo de 20 equipos, pero se puede ampliar según las necesidades. También hemos configurado por defecto el DNS de Google que es el 8.8.8.8.

4.2.5 Cortafuegos con IPTABLES

Un cortafuegos puede ser un dispositivo físico o virtual y con el cual se puede filtrar el tráfico de la red, tanto lo que enviamos desde nuestra red, como lo que recibimos en nuestra red.

Para abordar la configuración del cortafuegos, se ha tenido que revisar mucha información. Una de las páginas donde podemos encontrar los comandos básicos y avanzados de cómo configurar un cortafuegos con IPTABLES, es la página del binario [19]. Ahora ejecutamos las reglas para que nuestra Raspberry se convierta en un cortafuegos completo. Podemos elegir que sea persistente si guardamos las reglas en el fichero y hacemos un *script* para que se ejecute cuando arranque el sistema. Para ello se crea en la carpeta "etc" el archivo "Firewall_INI", que es el que contiene todas las reglas del cortafuegos y se establecen permisos de ejecución, ahora solo hace falta ponerlo en el archivo de "rc.local", esto se ve en la Figura 35.

```
  GNU nano 5.4                                        /etc/rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.

./etc/Firewall_INI

# Print the IP address
_IP=$(hostname -I) || true
if [ "$_IP" ]; then
  printf "My IP address is %s\n" "$_IP"
fi

exit 0
```

Figura 35 - Fichero INI

Ahora vamos a analizar con más detalle la configuración del cortafuegos. Lo primero que hacemos cuando se inicia la Raspberry, es ejecutar línea a línea el fichero Firewall_Ini que contiene todas las reglas ordenadas para levantar el cortafuegos y eliminamos todas las reglas que existen por si hay alguna que este enganchada, ver Figura 36.

```
#!/bin/sh
# Cortafuegos Raspberry Pi

# Elimino todas las reglas que puedan existir
iptables -F
iptables -X
iptables -Z
iptables -t nat -F
```

Figura 36 - Borrar reglas antiguas

Lo siguiente, es establecer todas las políticas de todas las tablas que hay en IPTABLES en aceptar, ver Figura 37.

```
# Establezco por defecto todas las politicas en aceptar
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT
iptables -P FORWARD ACCEPT
iptables -t nat -P PREROUTING ACCEPT
iptables -t nat -P POSTROUTING ACCEPT
```

Figura 37 - aceptar

Después, aceptamos todo el tráfico proveniente de la red local y hacemos un nateo, que es una redirección para que todo el tráfico salga por la puerta del *router* principal 192.168.50.0/24, ver Figura 38.

```
# Fitros del CORTAFUEGOS
# Acepto el trafico desde la red local eth0

/sbin/iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -s 192.168.50.0/24 -i eth1 -j ACCEPT

# Enmascaro la red local de eth1 a eth0
iptables -t nat -A POSTROUTING -s 192.168.50.0/24 -o eth0 -j MASQUERADE
```

Figura 38 - Nat

Ahora, es muy importante activar el BIT de *forwardin* para poder tener tráfico de red, ver Figura 39.

```
# Activo el BIT de forwarding sin esto no se puede tener trafico de red
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Figura 39 - BIT Forward

Seguidamente, cerramos el acceso desde la parte exterior para que sea más seguro, ver Figura 40.

```
# Cerramos los accesos desde el exterior desde cualquier red 0.0.0.0
iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 1:1024 -j DROP
iptables -A INPUT -s 0.0.0.0/0 -p udp --dport 1:1024 -j DROP
```

Figura 40 - cerrar conexiones entrantes

Y permitimos las conexiones de la VPN, para que cuando tengamos el servicio nos podamos conectar desde el exterior de nuestra red, ver Figura 41.

```
# Permitimos las conexiondes de la VPN
iptables -I INPUT 1 -i wg0 -j ACCEPT
iptables -A INPUT -i wg0 -j ACCEPT
```

Figura 41 - se aprueban conexiones VPN

Con esta configuración, hemos conseguido tener internet en nuestra red de área local, atravesando un cortafuegos. Para ver que todo funciona como es debido, se ha creado una nueva regla para bloquear la página de YouTube desde la LAN. Utilizando esta misma sintaxis, se puede bloquear todas las páginas o contenido que se crea necesario, ver Figura 43.

```
# Cerramos el acceso desde la LAN a las Webs
sudo iptables -A FORWARD -s 0.0.0.0/0 -p tcp -m string --string "youtube.com" --algo kmp -j DROP
```

Figura 43 - Bloqueo de youtube.com

Tras reiniciar la Raspberry Pi, ya podemos hacer la prueba del funcionamiento del cortafuegos intentando entrar en YouTube y vemos que está bloqueado. Hay que tener en cuenta, que si un usuario ya tenía cacheada la página puede llegar a cargarla. Aunque una vez pierda la cache ya no cargará. Se puede ver en la Figura 42.

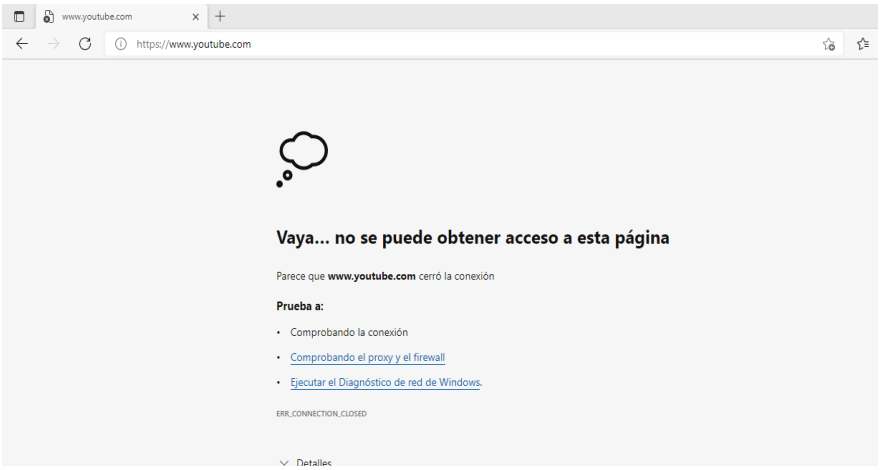

Figura 42 - Cortafuegos funcionando

4.2.6 Servicio NoIP

Actualmente, la IP que nos proporciona nuestro proveedor de internet suele ser dinámica, eso quiere decir que va cambiando y por esta causa si queremos conectarnos desde cualquier punto del mundo a nuestra red, necesitamos saber qué dirección IP tenemos en la parte exterior de nuestra red. Para averiguar esta IP, lo podemos buscar en Google "¿cuál es mi IP?" y en cualquiera de los enlaces al entrar nos pone nuestra IP.

El problema está, en que al ir cambiando, si no tenemos a alguien conectado que nos diga cual es la IP de nuestra red no podremos conectar si cambia, por eso hay muchos servicios que te dicen cuál es la IP y te dejan configurar un nombre DNS que directamente accede a la IP del equipo.

Por todo esto, nos hemos creado una cuenta en NoIP, la cual va a asociar la dirección física de red que nos da nuestro proveedor a un DNS.

- jalavoldemortTFG.ddns.net

Para que automáticamente cambie la IP cuando el proveedor de internet nos cambie la IP, se ha instalado el programa DUC (Dynamic Update Client) que es multiplataforma y se puede instalar sin problemas en linux [20].

4.2.7 VPN (WireGuard)

Una VPN sirve para poder acceder desde fuera de nuestra red de forma segura. Para ello hay un *script,* que ejecutándolo de la siguiente manera, ayuda con la instalación ya que está completamente guiado, ver Figura 44.

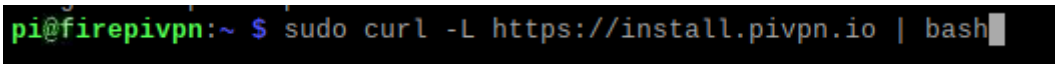

Figura 44 - Instalacion de VPN

Primero, nos aparece un aviso de que vamos a convertir nuestro dispositivo en un servidor de VPN de forma automática, verFigura 45.

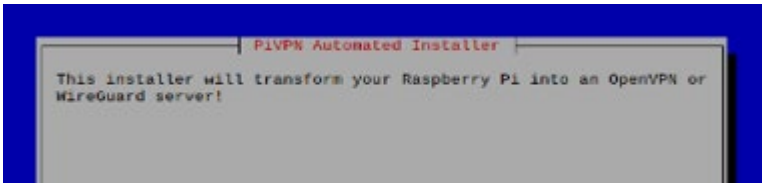

Figura 45 - VPN

Luego, se nos informa de que se necesita una dirección estática en este caso, ya hemos configurado las tarjetas de red para que tenga direcciones estáticas. Como lo que queremos es acceder desde fuera, utilizaremos la tarjeta de eth0 que tiene la dirección IP 192.168.0.200, nos pedirá confirmación para configurar esta IP y nos advierte que si el *router* tiene servidor de DHCP y asigna esta IP a otro dispositivo tendremos problemas para trabajar correctamente, ver Figura 46.

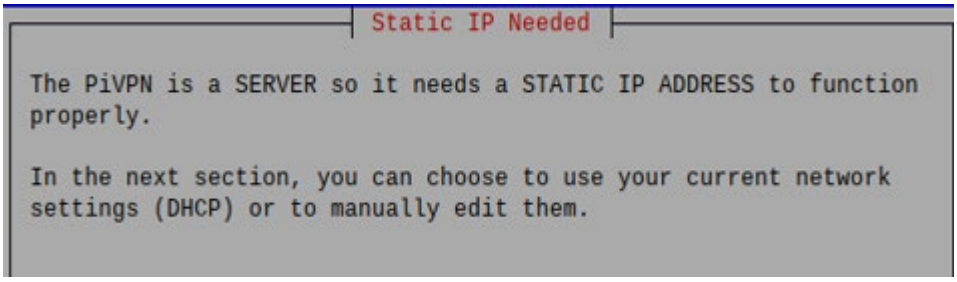

Figura 46 - VPN IP estática

Seguidamente, nos pedirá que le digamos qué usuario vamos a utilizar en este caso. Como no hemos creado ningún otro usuario, utilizaremos el usuario “pi” que es el administrador, ver Figura 47.

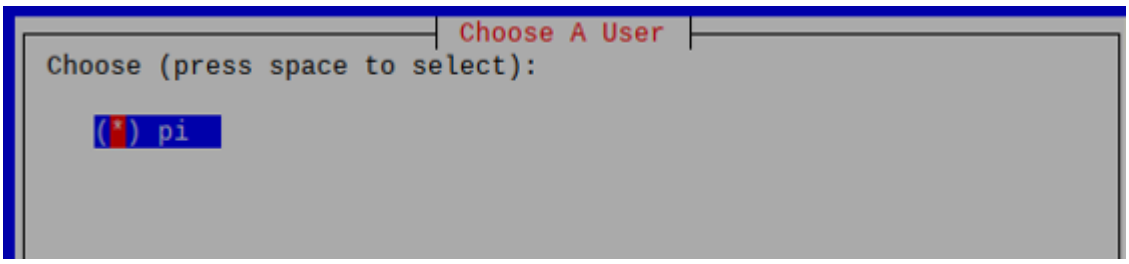

Figura 47 - User

A continuación, nos preguntará qué protocolo queremos utilizar. En este caso hemos decidido utilizar WireGuard porque es más moderno, ver Figura 48.

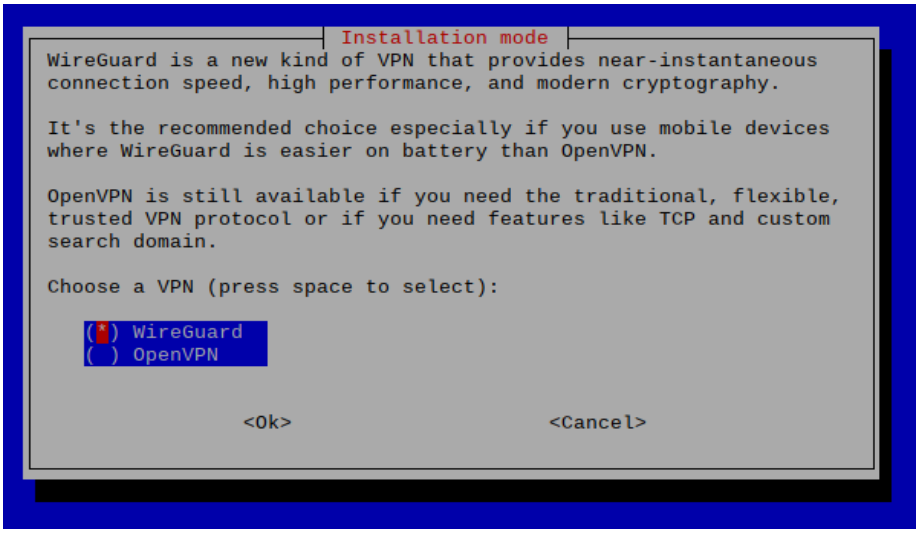

Figura 48 - WireGuard

Por último, configuraremos el puerto que va a escuchar las peticiones que hemos abierto en el *router* (R1). En este caso el puerto 6149, lo hemos elegido porque no hay ningún programa en concreto que lo utilice y además, forzamos a la utilización de un puerto que no es el que viene por defecto, para que sea un poco más difícil recibir un ataque, ver Figura 49.

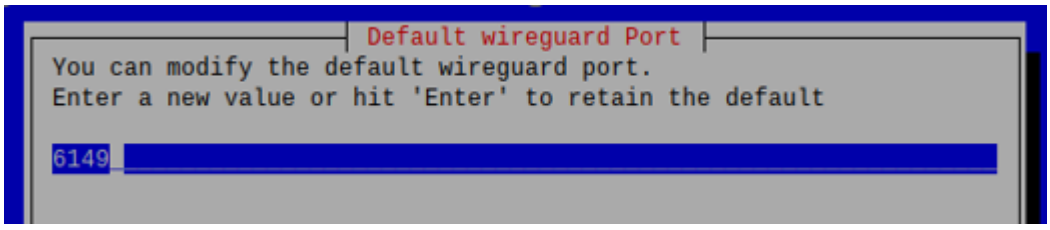

Figura 49 - Puerto VPN

Tras finalizar la instalación, se crearán automáticamente las claves privadas para poder conectar equipos a nuestra red, ver Figura 50.

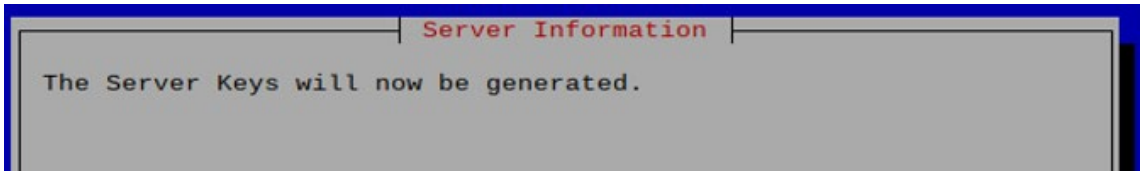

Figura 50 - VPN Keys

Ahora que ya hemos terminado de configurar la VPN, solo nos queda crear un acceso para un dispositivo en concreto. Se ha decidido crear la conexión “wiretfgpi” y la vamos a asociar a un teléfono móvil escaneando la aplicación de WireGuard y escaneando el QR generado. Para crear el nuevo cliente, ejecutamos el comando que se ve en la Figura 51 y le asignamos el nombre, en este caso wiretfgpi, ver Figura 52.

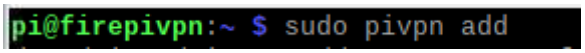

Figura 51 - Creación de usuario

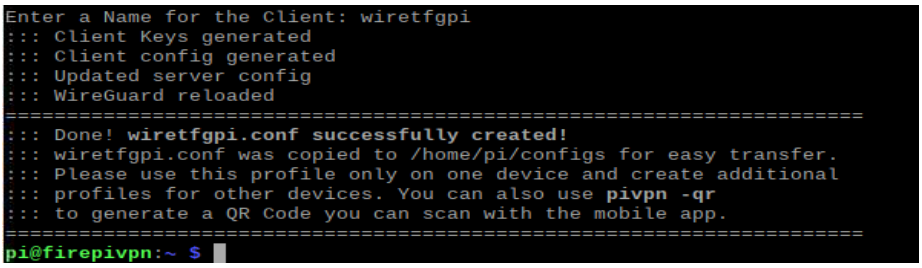

Figura 52 - Nombre del cliente

Se puede ver los clientes que tenemos configurados y las claves públicas y privadas en el archivo de configuración que se encuentra en “/home/pi/configs”, verFigura 53.

Figura 53 – Configuración de clientes

Para generar el QR y poder conectarlo en el móvil hay que ejecutar el comando pivpn -qr [CLIENTE] tal y como se muestra en la Figura 54.

Figura 54 - QR cliente

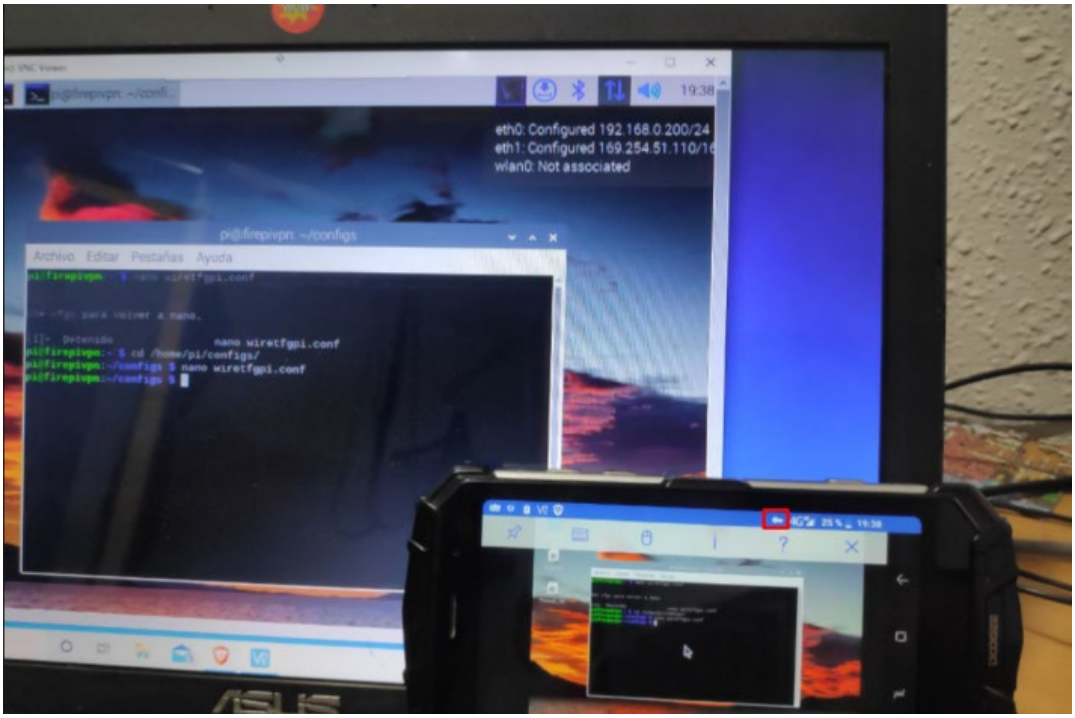

Figura 55 - Prueba de funcionamiento

Ahora escaneamos el código QR en el dispositivo que queramos levantar la VPN, previa instalación del Cliente de WireGuard y probamos a conectarnos a nuestra Paspberry como si estuviéramos conectados a nuestra LAN. En la Figura 55 tenemos

la conexión desde el móvil viendo que está la VPN activa y también se puede ver la conexión desde un pc de la red local.

4.2.8 Servidor Apache y PHP

Para darle mayor funcionalidad al proyecto, se ha decidido instalar un servidor de PHP [21] en la Raspberry pi para poder servir una página que modifique las reglas del cortafuegos que hemos implementado.

Apache 2 es un servidor de páginas web gratuito y multiplataforma que podemos instalar en nuestra máquina para poder acceder a una página desarrollada en PHP.

PHP es un procesador de texto que nos permite ejecutar código en un servidor y mezclarlo con una página de HTML.

Para instalar Apache, solo tenemos que ejecutar el siguiente comando en nuestro terminal "**sudo apt install apache2 -y**". En el caso de PHP ejecutamos el siguiente comando "**sudo apt install php -y**".

Los archivos para configurar la página se guardan en la carpeta "/var/www/html" y los que se utilizan en nuestro caso para que funcione correctamente son el index.html, que es el encargado de ejecutar la página cuando accedes a la dirección IP o localhost si lo miras directamente desde el servidor. El archivo Info.php, que ejecuta el código para poder ver el archivo de configuración del cortafuegos, también, se utiliza el archivo insertar.php, que es el que se encarga de guardar la dirección que queremos bloquear en el fichero local, donde está el cortafuegos y por último, utilizamos un fire.css para mejorar la usabilidad de la página web, ver Figura 56.

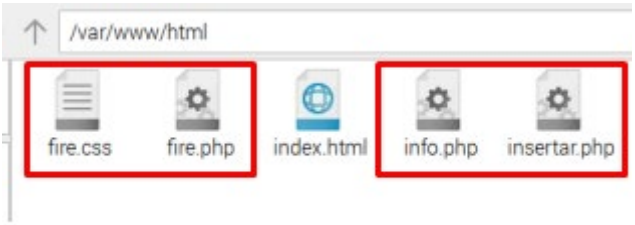

Figura 56 - HTML

En la Figura 57, vemos el código de la página de inicio. Cuando accedemos por primera vez indica gestión del *FireWall* by Jose Alapont, ver Figura 58. Al acceder por segunda vez, después de ejecutar el código de bloquear una URL, nos muestra un mensaje indicando qué URL se ha bloqueado y si lo ha hecho con éxito, ver Figura 59.

index.html | fire.php | insertar.php | fire.css

```
<html>
  <head>
    <link rel="stylesheet" type="text/css" href="fire.css" />
    <title>FIREWALL</title>
  </head>
  <body>


        <ul>
                <li><a class="active" href="index.html">MENU</a></li>
                <li><a href="fire.php">Ver FIREWALL</a></li>
                <li><a href="insertar.php">INSERTAR</a></li>
        </ul>

        <div style="margin-left:22%;padding:1px 16px;height:1000px;">
                <h1>Gestion del FireWall</h1>
                <h2>by Jose Alapont</h2>
        </div>
  </body>
</html>

```

Figura 57 - index.html

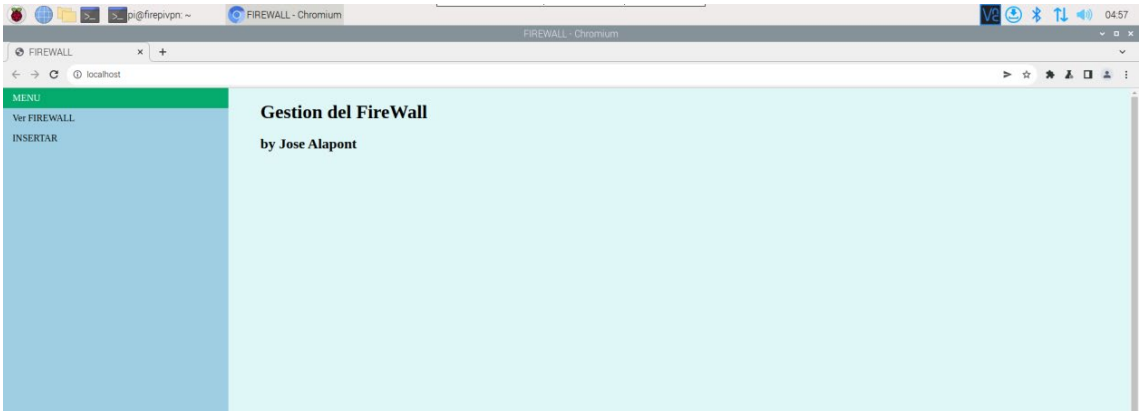

Figura 58 - index.html

Figura 59 - index.html

En la Figura 60, vemos el código de leer el fichero y mostrar los datos que hay en el cortafuegos configurado. Las líneas más importantes son las que están dentro del .php que es lo que hace que funcione correctamente, lo podemos ver en funcionamiento en la Figura 61.

index.html ✖ fire.php ✖ insertar.php ✖ fire.css ✖

```
<html>
  <head>
    <link rel="stylesheet" type="text/css" href="fire.css" />
    <title>FIREWALL</title>
  </head>
  <body>

        <ul class="menu">
                <li><a href="index.html">MENU</a>
                <li><a class="active" href="fire.php">Ver FIREWALL</a>
                <li><a href="insertar.php">INSERTAR</a>
        </ul>
        <div style="margin-left:22%;padding:1px 16px;height:1000px;">
                <?php
                $txt_file = fopen('/home/pi/Documents/Firewall_INI','r');
                $a = 1;
                while ($line = fgets($txt_file)) {
                echo($a." ".$line)."<br>";
                $a++;
                }
                fclose($txt_file);
                ?>
        </div>


  </body>
</html>
```

Figura 60 - fire.php

FIREWALL

localhost/fire.php

MENU
Ver FIREWALL
INSERTAR

```
1
2 #!/bin/sh
3 # Cortafuegos Raspberry Pi
4
5 # Elimino todas las reglas que puedan existir
6 iptables -F
7 iptables -X
8 iptables -Z
9 iptables -t nat -F
10
11 # Establezco por defecto todas las politicas en aceptar
12 iptables -P INPUT ACCEPT
13 iptables -P OUTPUT ACCEPT
14 iptables -P FORWARD ACCEPT
15 iptables -t nat -P PREROUTING ACCEPT
16 iptables -t nat -P POSTROUTING ACCEPT
17
18 # Fitros del CORTAFUEGOS
19 # Acepto el trafico desde la red local eth0
20
21 /sbin/iptables -A INPUT -i lo -j ACCEPT
22 iptables -A INPUT -s 192.168.50.0/24 -i eth1 -j ACCEPT
23
24 # Enmascaro la red local de eth1 a eth0
25 iptables -t nat -A POSTROUTING -s 192.168.50.0/24 -o eth0 -j MASQUERADE
26
27 # Activo el BIT de forwarding sin esto no se puede tener trafico de red
28 echo 1 > /proc/sys/net/ipv4/ip_forward
29
30 # Cerramos los accesos desde el exterior desde cualquier red 0.0.0.0
31 iptables -A INPUT -s 0.0.0.0/0 -p tcp --dport 1:1024 -j DROP
32 iptables -A INPUT -s 0.0.0.0/0 -p udp --dport 1:1024 -j DROP
33
34 # Permitimos las conexiondes de la VPN
35 #iptables -I INPUT 1 -i wg0 -j ACCEPT
36 iptables -A INPUT -i wg0 -j ACCEPT
37
38 # Cerramos el acceso desde la LAN a las Webs
39
40
41 sudo iptables -A FORWARD -s 0.0.0.0/0 -p tcp -m string --string "www.google.es" --algo kmp -j DROP
42
43 sudo iptables -A FORWARD -s 0.0.0.0/0 -p tcp -m string --string "www.start.es" --algo kmp -j DROP
44
45 sudo iptables -A FORWARD -s 0.0.0.0/0 -p tcp -m string --string "www.gmail.com" --algo kmp -j DROP
46
47 sudo iptables -A FORWARD -s 0.0.0.0/0 -p tcp -m string --string "www.ask.com" --algo kmp -j DROP
48 sudo iptables -A FORWARD -s 0.0.0.0/0 -p tcp -m string --string "www.superdeporte.es" --algo kmp -j DROP
49 sudo iptables -A FORWARD -s 0.0.0.0/0 -p tcp -m string --string "www.marca.com" --algo kmp -j DROP
```

Figura 61 - fire.php

En la Figura 62, vemos el código que bloquea una página web. Lo que hace es insertar una cadena de texto al final del documento donde se configura el cortafuegos, para así bloquear una nueva página. Se puede ver el funcionamiento en la Figura 63.

index.html fire.php insertar.php fire.css

```
<html>
  <head>
    <link rel="stylesheet" type="text/css" href="fire.css" />
    <title>FIREWALL</title>
  </head>
  <body>

        <ul class="menu">
                <li><a href="index.html">MENU</a>
                <li><a href="fire.php">Ver FIREWALL</a>
                <li><a class="active" href="insertar.php">INSERTAR</a>
        </ul>

        <div style="margin-left:22%;padding:1px 16px;height:1000px;">


        <form action="script.php" method="post">
          Web: <input type="text" size="50" name="webB" style="margin-top:4%; height:50px;"><br><br>
          <input type="submit" value="Enviar" style="width:25%; height:30px;">
        </form>

        </div>


  </body>
  </html>
```

Figura 62 - Código

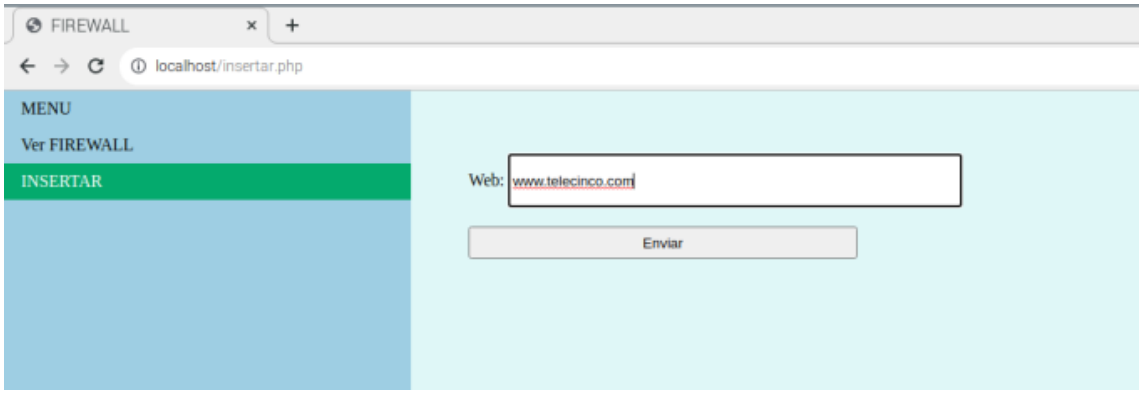

Figura 63 - insertar.php

Podemos observar el resultado de bloquear la página de www.telecinco.com en la Figura 64. El contenido del fichero .css que se utiliza para que se vean los colores azules está en la Figura 65.

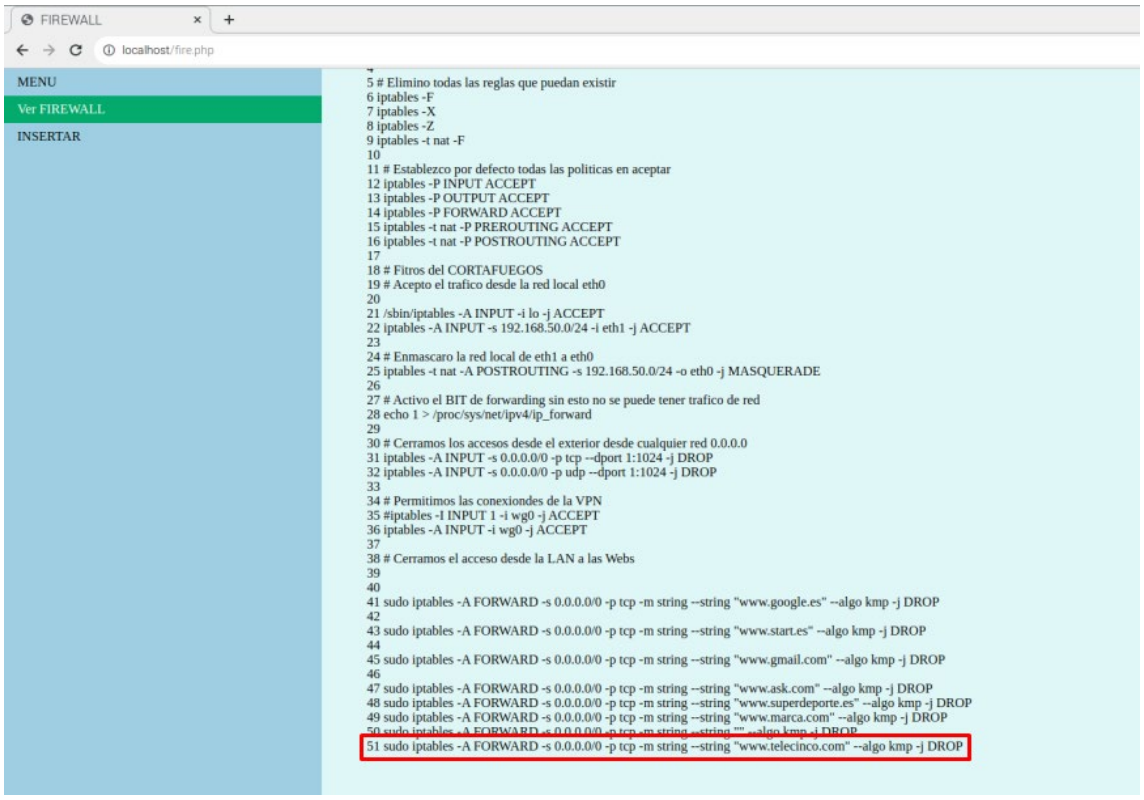

Figura 64 - Ver firewall

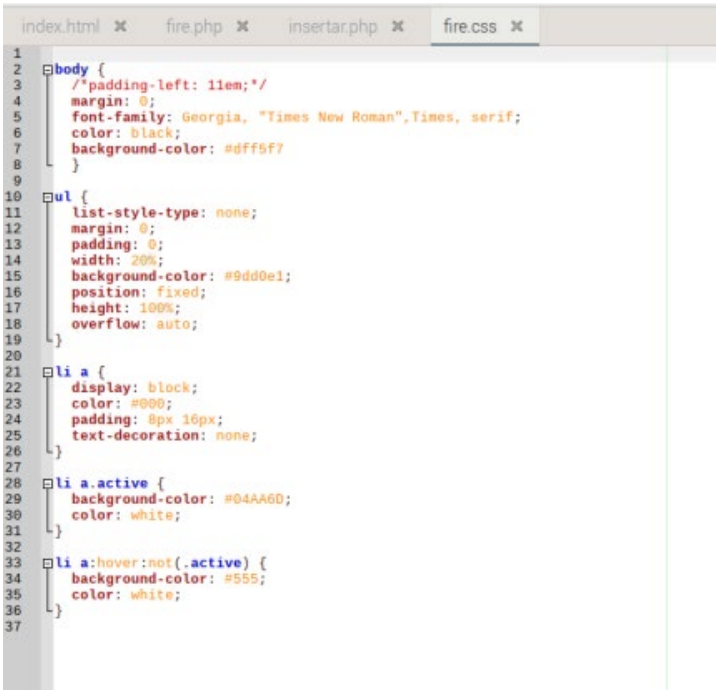

Figura 65 - css

5 Conocimientos extraídos

En este proyecto se he podido extraer muchos conocimientos sobre las características de la Raspberry Pi, *routers*, *switchs*, seguridad y de redes desconocidos hasta ahora, detallados a continuación.

Raspberry Pi es un ordenador reducido y muy económico que fue creado para que en los colegios y las universidades se pudiera promover la enseñanza y el desarrollo de la computación. Al inicio se utilizaba conectando cables y modificando los componentes electrónicos, pero en la actualidad se utiliza para desarrollar proyectos de todo tipo gracias a su versatilidad.

En el diseño de su placa base cuenta con 40 pines que permiten interconectar un sistema externo, como puede ser un sensor o un altavoz, de manera muy sencilla, permitiendo de así poder implementar todo tipo de proyectos, como, por ejemplo, consolas, sistemas de domótica para jardines, robots, etc.

Se ha elegido el modelo 3 B+ que fue lanzado al mercado el 14-03-2018, porque estaba en un kit de iniciación con todo lo necesario incluido para poder empezar a trabajar, a un precio muy económico y se adapta a las necesidades de nuestro proyecto.

Características de nuestro modelo:

- Procesador: Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC.
- Frecuencia de reloj: 1,4 GHz.
- GPU: VideoCore IV 400 MHz.
- Memoria: 1GB LPDDR2 SDRAM.
- Conexión inalámbrica: 2.4GHz / 5GHz, IEEE 802.11.b/g/n/ac, Bluetooth 4.2, BLE.
- Conexión de red: Gigabit Ethernet over USB 2.0 (300 Mbps de máximo teórico).
- Puestos E/S: GPIO 40 pines, HDMI, 4 x USB 2.0, CSI (cámara Raspberry Pi), DSI (pantalla táctil), Toma auriculares / vídeo compuesto, Micro SD, Micro USB (alimentación), Power-over-Ethernet (PoE).

En cuanto a la configuración de tarjetas de red estáticas, he aprendido que tienes que reiniciar para que funcionen correctamente y además hay que tener en cuenta que puede pasar algún problema eléctrico, como en mi caso que se me fue la luz y cuando

arranque el proyecto otra vez ya no funcionaba nada y el motivo estaba en que la tarjeta de eth1 se había convertido en eth2 y como en el proyecto hemos configurado para eth1 no funcionaba nada.

Otro de los aspectos que me ha tocado investigar, ha sido sobre la configuración de los *routers,* puesto que, como cada uno tiene unas características propias, también tienen su propia configuración, además, para que la red funcionara como yo quería, fue algo complicado porque al principio, al no desactivar el servidor DHCP del *router* R2, el que se utiliza para dar conexión a la LAN, me creaba un subdominio de red y en realidad lo único que me interesaba del *router,* era que hiciera de puente wifi.

6 Conclusiones

Para concluir el proyecto se va a hacer un pequeño repaso por los puntos que nos habíamos fijado al principio y cuál ha sido el resultado de su elaboración y si hubiera cambiado algo en el proceso.

El objetivo principal, era permitir que las pequeñas empresas puedan conectarse a una pequeña intranet utilizando una red privada virtual, esto se ha logrado. Aunque ha tocado rehacer toda la configuración en más de una ocasión, debido a problemas eléctricos, cambios en el domicilio; por esto, me he dado cuenta de que es muy importante tener capturas y respaldos de todo. Para poder ir haciendo la documentación a la par que se desarrolla el proyecto.

Otro de los objetivos que nos planteamos, es tener pautas de seguridad. Después de estudiar todas las leyes, me di cuenta de que ya utilizo las técnicas seguras inconscientemente. Se ha detectado, que el punto más débil es el usuario y al final tenemos que hacer un reciclaje constante de lo que sabemos. Gracias a todo esto he sido capaz de elaborar un esquema de red funcional, que se adapta a un modelo general y real de trabajo.

He visto el tipo de Raspberry que nos interesa para el desarrollo de este proyecto. También, he conseguido desarrollar un cortafuegos funcional que automáticamente se inicia con el sistema operativo y he configurado un servidor de VPN. Lo que nos permite poder tener un punto de acceso a nuestra empresa desde cualquier equipo y de modo seguro. También, se han hecho conexiones desde diferentes dispositivos como móviles y portátiles para comprobar que todo funcione correctamente.

Gracias a todo el trabajo de investigación que he hecho me he dado cuenta de que todavía tengo muchos proyectos que se podría realizar, por ejemplo, me he quedado con las ganas de utilizar un *router* portátil Nanopi que lleva integrado OpenWRT que se puede utilizar de cortafuegos

También quiero seguir mejorando en mis conocimientos de IPTABLES, puesto que se pueden hacer muchísimas cosas, como guardar logs y poder crear tus propias reglas para tener alertas que las veas directamente en el móvil creando así un sistema de seguridad propio.

Otro de los proyectos que me gustaría llevar a cabo, es el de ponerle a una Raspberry una interfaz táctil y un punto wifi activado que suministre wifi y poder tener un servidor rápido en cualquier sitio. Esto serviría para conectarte a una red no segura y poder tener control de los accesos de esta.

También me he quedado con ganas que conectar cosas con Arduino a la Raspberry pi.

7 Referencias

[1] ENS - Esquema Nacional de Seguridad – ENS Disponible en: https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1001 [consultado el 10 de marzo de 2021]

[2] NORMAS ISO Implementación efectiva de la seguridad de la información con las normas ISO 27001 / ISO 27002. Disponible en: https://www.normas-iso.com/iso-27001/ [consultado el 10 de marzo de 2021]

[3] CCN-CERT disponible en: https://www.ccn-cert.cni.es/sobre-nosotros.html [consultado el 15 de septiembre de 2021]

[4] Mejora al sistema de seguridad de una empresa mediante gestión de identidades disponible en: https://riunet.upv.es/handle/10251/171354 [consultado el

30 de septiembre de 2021]

[5] RiuNet repositorio UPV disponible en: https://riunet.upv.es/ [consultado el 15 de setptiembre de 2021]

[6] Metodología para la gestión de ciberincidentes. Apoyo para la implantación de la guía CCN-STIC 817 a profesionales informáticos. Disponible en: https://riunet.upv.es/handle/10251/171360 [consultado el 10 de noviembre de 2021]

[7] SonicWall disponible en: https://www.sonicwall.com/ [consultado el 21 de mayo de 2021]

[8] OpenVPN disponible en: https://openvpn.net/ [consultado el 2 de abril de 2021]

[9] IKEv2 C. Kaufman, "Internet Key Exchange (IKEv2) Protocol". Disponible en: https://ieeexplore.ieee.org/document/5766473 [consultado el 2 de abril de 2021]

[10] L2TP/IPSec. Disponible en: https://datatracker.ietf.org/doc/html/rfc2661 [consultado el 2 de abril de 2021]

[11] WireGuard: fast, modern, secure VPN tunnel. Disponible en: https://www.wireguard.com/ [consultado el 2 de abril de 2021]

[12] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Disponible en:

https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf [consultado el 15 de marzo de 2021]

[13] 0xWord Pentesting con Kali es un libro que se puede encontrar en: https://0xword.com/libros/40-libro-pentesting-kali.html [consultado el 4 de febrero de 2022]

[14] Sugerencias para crear un diagrama de red Disponible en: https://www.microsoft.com/es-es/microsoft-365/business-insights-ideas/resources/tips-for-mapping-your-network-diagram [consultado el 30 de abril de 2021]

[15] Install Raspberry Pi OS using Raspberry Pi Imager https://www.raspberrypi.com/software/ [consultado el 8 de mayo de 2021]

[16] Montaje de Raspberry Pi. Disponible en: https://www.youtube.com/watch?v=2D0F-uulR00 [consultado el 8 de mayo de 2021]

[17] VNC página oficial: https://www.realvnc.com/es/connect/download/vnc/raspberrypi/ [consultado el 15 de junio de 2021]

[18] DNSMasq página oficial: https://dnsmasq.org/ [consultado el 20 de julio de 2021]

[19] IPTABLES. Disponible en: https://elbinario.net/2019/03/18/iptables-para-torpes/ [consultado el 21 de julio de 2021]

[20] Instalación de DUC https://www.noip.com/support/knowledgebase/install-ip-duc-onto-raspberry-pi/ [consultado el 18 de mayo de 2022]

[21] PHP https://www.php.net/manual/es/intro-whatis.php [consultado el 28 de mayo de 2022]

ANEXO

OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	**Alto**	**Medio**	**Bajo**	**No Procede**
ODS 1. **Fin de la pobreza.**			**X**	
ODS 2. **Hambre cero.**				**X**
ODS 3. **Salud y bienestar.**				**X**
ODS 4. **Educación de calidad.**			**X**	
ODS 5. **Igualdad de género.**				**X**
ODS 6. **Agua limpia y saneamiento.**				**X**
ODS 7. **Energía asequible y no contaminante.**	**X**			
ODS 8. **Trabajo decente y crecimiento económico.**				**X**
ODS 9. **Industria, innovación e infraestructuras.**		**X**		
ODS 10. **Reducción de las desigualdades**.				**X**
ODS 11. **Ciudades y comunidades sostenibles**.	**X**			
ODS 12. **Producción y consumo responsables.**		**X**		
ODS 13. **Acción por el clima.**	**X**			
ODS 14. **Vida submarina.**				**X**
ODS 15. **Vida de ecosistemas terrestres.**				**X**
ODS 16. **Paz, justicia e instituciones sólidas.**				**X**
ODS 17. **Alianzas para lograr objetivos.**				**X**

Los objetivos del desarrollo sostenible establecidos en 2015, fueron diseñados por la Asamblea General de las Naciones Unidas y tienen la finalidad de lograr un futuro mejor y más sostenible.

Debido a este motivo, en el proyecto se ha intentado pensar en cómo puede afectar en el futuro de todos y por eso se ha intentado que el proyecto sea sostenible, para que tengamos un impacto medio ambiental lo más bajo posible y tener un nivel social más justo. Voy a explicar y analizar de los puntos con los cuales este trabajo está relacionado con los objetivos de desarrollo sostenible:

Fin de la pobreza, este objetivo se creó para combatir los problemas de desigualdad y actualmente solo las empresas grandes se pueden plantear la utilización de mecanismos de seguridad como cortafuegos debido a que son muy caros. Al utilizar una Raspberry Pi estos costes se reducen mucho.

Educación de calidad, en este objetivo se plantea que los estados garanticen el acceso gratuito a la educación, tiene mucho que ver con el proyecto ya que Rabian se desarrolló pensando en que los alumnos de todos los centros puedan aprender informática, tanto hardware como software, con una inversión económica muy pequeña.

Energía asequible y no contaminante, se quieren implementar energías limpias, gracias al poco consumo del dispositivo que estamos utilizando para desarrollar el proyecto, se puede colocar un panel solar y con esto es suficiente para mantener los servidores que están instalados y el cortafuegos.

Industria, innovación e infraestructuras, este punto está muy relacionado con el proyecto ya que estamos dando con una Raspberry pi, una herramienta de seguridad implementada para que cualquier persona con muy pocos conocimientos y recursos pueda plantear un nuevo tipo de negocio.

Ciudades y comunidades sostenibles, este punto esta enlazado con el proyecto debido a que si comparamos el consumo del material que utilizan ahora las empresas para poder implementar la misma seguridad, conseguimos reducir mucho el consumo energético puesto que la Raspberry pi requiere de muy poca electricidad para funcionar y se puede colocar directamente conectada a una placa solar y ya funcionaria sin ningún gasto energético, como se comenta en el punto anterior.

Producción y consumo responsables, como hemos empleado materiales reacondicionados estamos haciendo un consumo responsable y más económico, esto hace que no se necesiten utilizar nuevos materiales ya que estamos reaprovechando un material que otra persona lo ha descartado por que tenía algún problema de fábrica.

Acción por el clima, este apartado está relacionado con todos los anteriores porque lo que estamos haciendo es reducir el consumo eléctrico para poder crear empleos sostenibles tal y como es el de instalador de placas solares y también estamos reduciendo el consumo energético.