



Universidad Internacional de La Rioja
Escuela Superior de Ingeniería y Tecnología

Grado en Ingeniería Informática

Seguridad en redes desconocidas para el teletrabajo.

Trabajo fin de estudio presentado por:	Ángel Jaén Galán
Línea de investigación:	Redes y Seguridad Informática.
Director/a:	Dra. Belén Bermejo González
Fecha:	Marzo - 2021

Agradecimientos

Quisiera agradecerles, en primer lugar, a mis padres, Ángel y Esperanza, la confianza depositada en mí a lo largo de esta etapa académica, así como todos los ánimos y cariño incondicional que me han mostrado a lo largo de mi vida. Agradecerles la educación recibida, por inculcarme la cultura del esfuerzo, pues todo esfuerzo tiene su recompensa, y agradecer enormemente el sacrificio que han realizado todos estos años para permitirme el estudio de esta titulación universitaria.

Agradecer de forma especial a mi hermano, José Luis, mi pareja Maite, y amigos, su cariño, apoyo y confianza a lo largo de estos años de estudio universitario. Gracias por estar en todo momento a mi lado y acompañarme en esta etapa.

Expresar toda mi gratitud a mi tutora, Belén, por haberme guiado y aconsejado a lo largo de este Trabajo Fin de Grado, por motivarme a adentrarme en un tema tan novedoso y actual como puede ser la seguridad informática en las redes usadas para el teletrabajo.

Agradecer a los compañeros de UNIR por el compañerismo y la ayuda que nos hemos ofrecido mutuamente, que me han servido para seguir adelante en los momentos más complicados, así como agradecer la amistad y los buenos momentos que hemos pasado juntos en la distancia.

Por último, y no por ello menos importante, agradecer a toda la comunidad universitaria de la Universidad Internacional de la Rioja, especialmente a los profesores, la formación recibida.

Este éxito académico es tan vuestro como mío.

¡Gracias a todos!

Resumen

En la actualidad, debido a la situación que se vive en el mundo a raíz de la pandemia de la Covid-19, el trabajador se enfrenta a una situación diferente ante la manera de trabajar. Comienza a realizar sus funciones laborales desde una red distinta a la que acostumbra a estar conectado, y desde un nuevo lugar de trabajo y conexión.

Como usuario no experto, el trabajador desconoce las medidas de seguridad y la manera de conexión remota, por este motivo, se propone en este TFG "SEGURITFG", un software que ofrece ayuda para que las conexiones sean los más seguras y fáciles.

SeguriTFG, es un software sencillo e intuitivo, en el que el trabajador de la empresa, puede seleccionar mediante un solo click de ratón la protección que desea obtener en su nuevo lugar de trabajo, este, ofrece la posibilidad de acceder a la red mediante una conexión de VPN, en el cual se puede seleccionar la opción de iniciar un firewall y un servidor proxy, estas protecciones en conjunto forman una red con seguridad mayor a la que se obtiene en la red doméstica.

Para la tranquilidad de la empresa en el ámbito de seguridad informática, SEGURITFG, ofrece la posibilidad, ventaja y tranquilidad de tener los datos más sensibles de los clientes, viajando por la red pública con la tranquilidad de viajar bajo una red segura.

Palabras clave: software, teletrabajo, VPN, firewall, proxy.

Abstract

Currently, due to the situation in the world as a result of the Covid-19 pandemic, the worker faces a different / new situation regarding the way of working. He begins to carry out his work functions from a different network than the one he is usually connected to, and from a new place of work and connection.

As a user and not an expert, the worker does not know the security measures and the way of remote connection, in this case "SEGURITFG" helps to make the connections the safest and easiest.

For this reason, a simple and intuitive software is proposed, in which the worker of the company, can select by means of a single mouse click the protection they want to obtain in their new workplace, said software offers the possibility of accessing the network Using a VPN connection, in turn, you can select the option to start a firewall and a proxy server, which together form a network with greater security than that obtained in a home network.

For the tranquility of the company in the field of computer security, SEGURITFG, offers the possibility, advantage and tranquility of having the most sensitive data of the clients, traveling through the public network with the tranquility of traveling under a secure network.

Keywords: software, teletrabajo, VPN, firewall, proxy.

Índice de contenidos

1.	Motivación del proyecto.	11
1.1.	Propósito del proyecto y objetivo	12
1.1.1.	Objetivos del TFE	12
2.	Conceptos básicos.	14
2.1.	Seguridad doméstica.....	14
2.1.1.	Definición de la problemática en la seguridad del ámbito doméstico.	15
2.1.2.	Tipos de seguridad en una red doméstica.	15
2.2.	Empresas y su seguridad.....	17
2.2.1.	Definición de seguridad informática para la empresa	17
2.2.2.	Prevención en la seguridad de red de la empresa.	17
2.3.	Conocimiento de Seguridad por el usuario para una red informática.	19
2.3.1.	Seguridad para el usuario novel	19
2.3.2.	Seguridad para el usuario avanzado	20
3.	Puesta en marcha de la solución.....	21
3.1.	Identificación del problema en el ámbito doméstico.....	21
3.1.1.	Tipos de conexiones seguras en el ámbito doméstico.....	21
3.1.2.	Solución a los problemas de seguridad en el ámbito doméstico.....	21
3.2.	Definición de las tecnologías de seguridad	22
3.2.1.	Definición de Firewall	22
3.2.2.	Definición de VPN	25
3.2.3.	Definición de Servidor Proxy	27
4.	Instalación y configuración de los servidores	30
4.1.	Servidor VPN	30
4.1.1.	Instalación.....	30

4.1.2.	Configuración.....	31
4.1.3.	Generación de claves y certificados del servidor VPN	33
4.1.4.	Configuración de parámetros en el servidor.....	35
4.1.5.	Configuración de las rutas de los certificados.....	36
4.1.6.	Direcciones IP de la red VPN	37
4.1.7.	Generación de ta.key, modificación del path y copia de certificados y claves a Config. 38	
4.1.8.	Arranque del servicio y VPN con OpenVPN.....	39
4.1.9.	Apertura de puertos en el router y DDNS	41
4.1.10.	Configuración del cliente VPN	45
4.2.	Servidor Proxy.....	48
4.2.1.	Instalación.....	48
4.2.2.	Configuración.....	50
4.2.3.	Funcionamiento.....	54
4.3.	Servidor Firewall	57
4.3.1.	Instalación.....	57
4.3.2.	Configuración.....	59
4.3.3.	Funcionamiento.....	64
5.	Conclusiones y trabajo futuro	67
5.1.	Verificación:	67
5.2.	Investigación:	67
5.3.	Desarrollo:.....	67
	Referencias bibliográficas.....	69
	Anexo A. Encuestas realizadas	73
	Índice de acrónimos	74

Índice de figuras

Figura 1: Conexión Segura	19
Figura 2: Conexión Insegura	19
Figura 3: Utilidad de Firewall.....	23
Figura 4: Esquema funcionamiento de Firewall	24
Figura 5: Funcionamiento de una red VPN.....	25
Figura 6: Proxy inverso	28
Figura 7: Selección EasyRSA 2 Certificate Management Scripts	30
Figura 8: Proceso de entrada a la edición de la configuración.....	31
Figura 9: Edición de los datos del propietario de la VPN	32
Figura 10: Ejecución del fichero " vars.bat"	32
Figura 11: Generación de la entidad certificadora.....	33
Figura 12: Creación claves de servidor	34
Figura 13: Encriptación de las claves de servidor.....	34
Figura 14: Protocolos de conexión	35
Figura 15: Ruta de los certificados por defecto.....	36
Figura 16: Ruta modificadas de los certificados.....	36
Figura 17: Selección de la red para la conexión VPN	37
Figura 18: Selección de valor de servidor.....	38
Figura 19: Añadir ruta al path de Windows.....	38
Figura 20: Creación de clave de última clave necesaria para el servidor.....	38
Figura 21: Colocación de archivos de autenticación	39
Figura 22: Conexión de la VPN	40
Figura 23: Conexión correcta en VPN.....	40
Figura 24: Apertura de puertos en el router	41

Figura 25: Obtención de dominio DDNS.....	42
Figura 26: Selección de DNS	42
Figura 27: Guardar configuración DDNS a router	43
Figura 28: Añadir DDNS en el router	44
Figura 29: Creación de la clave del cliente	46
Figura 30: Ficheros de configuración cliente VPN.....	46
Figura 31: Dirección IP servidor VPN.....	47
Figura 32: Dirección IP publica router alojamiento servidor VPN.....	47
Figura 33: Inicio asistente de instalación	48
Figura 34: Aceptación de términos	48
Figura 33: Selecccion ruta de instalación	49
Figura 37: Resumen de Instalación.....	49
Figura 39: Información tras la instalación	49
Figura 36: Nombre en carpeta programas Inicio.....	49
Figura 38: Progreso de la instalación.....	49
Figura 40: Finalización de la instalación de FreeProxy	49
Figura 41: Desactivar Firewall de Windows	50
Figura 42: Panel de configuración FreeProxy	50
Figura 43: Creación Servicio proxy	51
Figura 44: Restricciones establecidas.....	52
Figura 45: Panel de configuración servidor Proxy con configuración aplicada.....	53
Figura 46: Inicio/Parada servidor Proxy	53
Figura 47: Pestaña de entrada en el navegador para configuración Proxy	54
Figura 48: Configuración Servidor Proxy en navegador Mozilla Firefox	54
Figura 49: Conexión UNIR servidor Proxy Corriendo y configurado en navegador	55

Figura 50: Conexión rechazado por el navegador y el servidor Proxy	55
Figura 51: Búsqueda de URL denegada mediante Google	56
Figura 52: Acceso denegado por servidor Proxy en búsqueda mediante Google	56
Figura 53: Acceso a un portal de una Inmobiliaria con regla de prohibición en Proxy.....	56
Figura 54: Aceptación de términos ZoneAlarm.....	57
Figura 55: Progresos de Instalación.....	58
Figura 56: Registro correo para recibir actualización y mejoras de ZoneAlarm	58
Figura 57: Menú de configuración Firewall.....	59
Figura 58: Entrada Configuración Firewall	59
Figura 59: Nivel de seguridad	60
Figura 60: Programas configurados en Firewall	61
Figura 61: Pantalla de movilidad	61
Figura 62: Agregar sitios de confianza Firewall	62
Figura 63: Permitir o denegar url en sitios de confianza.....	62
Figura 64: Permisos de acceso en sitios de confianza Firewall	63
Figura 65: Permisos nuevo software	64
Figura 63: Programa TeamViewer en ejecución	65
Figura 67: TeamViewer en el panel de control de aplicaciones.....	66

Introducción

En el desarrollo de este proyecto, se tiene como propósito tratar sobre como tener una buena seguridad en una red desconocida para el teletrabajo, actualmente debido a la pandemia de la Covid-19, no todas las empresas se encuentran totalmente protegidas como para poder tener conexiones remotas desde los nuevos lugares de trabajo de los empleados (hogar, redes públicas como la de hotel, etc.).

Por ello se llevará a cabo la realización de un software, en el que el trabajador de una empresa podrá seleccionar mediante dicho software, que tipo de seguridad quiere aplicar en la red en la cual se encuentra conectado para la conexión con la red de la empresa.

Este software hará de puente entre el nuevo lugar de trabajo y la conexión de la empresa, en la que pueden ser tratados entre otros datos sensibles de los clientes.

Se creará una VPN, además de contar con un servidor Proxy en el que podrán monitorizar los cambios en la red, por si se detectase alguna intrusión en nuestra red (la red del lugar de trabajo).

A continuación, se enumeran algunos de los ejemplos de los tipos de seguridad que se podrán aplicar entre otros, estos son:

- Firewall: el firewall o cortafuegos será el encargado de bloquear el acceso a nuestra red en caso de detectarse una intrusión.
- VPN: será la encargada de crear un "puente" entre la red del nuevo lugar de trabajo con la red de la empresa, creando una red privada virtual entre ellas.
- Servidor Proxy: será el encargado de monitorizar los movimientos en la red, detectando alguna intrusión si fuera necesario y además avisando con una alerta para solucionarlo lo antes posible.

1. MOTIVACIÓN DEL PROYECTO.

La elección de dicho tema para el desarrollo de este trabajo, viene por la visión de la necesidad de seguridad en el teletrabajo. A raíz de la pandemia de la Covid-19, numerosas personas se vieron afectadas en su trabajo, dando lugar al teletrabajo. Esta metodología de trabajo que algunas empresas implantan desde hace bastante tiempo, para otras es una nueva manera de trabajar, así mismo no disponiendo de todas las herramientas necesarias para una total seguridad a la hora de tratar con datos sensibles, informáticamente hablando.

Para ello, se propone SeguriTFG en el que usuario pueda acceder antes de comenzar a trabajar, en el que se desglosan diversas opciones para elegir una buena y conexión segura con la red de la propia empresa.

Este, junto a una serie de protocolos de seguridad, es capaz de crear una red segura en la que el usuario desde su domicilio o cualquier lugar diferente al puesto de trabajo, puede conectar con su equipo de trabajo para visualmente seguir en el puesto de trabajo estando en cualquier lugar.

Las medidas que se proponen son, conexión por VPN a la red laboral, junto a un firewall y un servidor proxy, en el que el usuario en cuestión autentificará y tendrá conexión a la red de su empresa, para poder seguir ejerciendo las labores profesionales desde cualquier lugar que tenga conexión a la red pública (Internet).

1.1. Propósito del proyecto y objetivo

El problema que se puede encontrar a la hora de trabajar en una red privada de una empresa desde un nuevo lugar puede dar lugar a que otros usuarios de dicha red puedan acceder a datos que no deber, por ello, con la situación actual de la pandemia Covid-19, muchas empresas para no perder sus trabajadores y cesar su actividad, han optado por la elección del trabajo, esta opción como todas, lleva una cara negativa, y es la de la seguridad, en todos los hogares se dispone hoy en día de una conexión a red de internet, pero no en todas se tiene una serie de medidas de seguridad contra atacantes como puede ser un vecino hacker.

Para la solución de dicho problema, se propone un software, el cual se encargara de configuración una serie de medidas de seguridad a petición del usuario antes de comenzar la jornada laboral, en la que se podrá seleccionar la seguridad a aplicar a dicha red antes de conectar a la de la empresa para comenzar a desarrollar la jornada laboral

1.1.1. Objetivos del TFE

El objetivo principal de este proyecto, es el de ofrecer un conocimiento sobre sistemas de seguridad informáticos tanto en el ámbito laboral como en el ámbito doméstico.

En la actualidad y cada día que pasa, la red tanto pública como privada tiene un número elevado de nuevos usuarios, ya sea desde el más pequeño dispositivo como puede ser un smartwatch, hasta un servidor de red. Todos estos dispositivos, tienen una comunicación con la red pública (Internet) en la que rondan diversos ataques maliciosos y/o fraudulentos.

Por ello, el objetivo de este proyecto es el de transmitir conocimiento a un usuario de cualquier nivel a saber a qué se expone simplemente con estar conectado a la red. A pesar de ello, este proyecto va destinado en especial a usuario de un nivel más básico (también para usuarios de nivel más avanzado), para la realización de las funciones laborales, en el caso de poder ejercer su puesto de trabajo desde una red privada como puede ser la de un hogar para conectar con la red privada de un lugar concreto en el que se les ofrece a los trabajadores la opción de teletrabajar. Opción actualmente muy en auge debido a la pandemia de la Covid-19.

1.1.1.1. Objetivo General

El Objetivo general de este trabajo, es la de encontrar una solución a todos los posibles fallos y brechas de seguridad en la conexión con un puesto laboral conectado a una red privada en la que se trata con datos de carácter sensibles desde otra red privada, pasando por la red pública (Internet). Para ello se detallan algunos sistemas de seguridad en los que con una configuración detallada y a medida, el tráfico de dichos datos sensibles a priori no debería de tener problemas de filtrado mientras que dichas conexiones se encuentran establecidas.

1.1.1.2. Objetivos específicos

Los objetivos específicos son los de poder establecer una conexión segura mediante diversos software y protocolos a medida. Estos, en conjunto proporcionan una seguridad en la red mayor a la que puede ofrecer un simple antivirus. Al tratar con datos sensibles y propios de una empresa, es muy peligroso el tráfico en la red sin ofrecer una seguridad "Premium"

2. Conceptos básicos.

La intención del desarrollo de este capítulo del TFG, está hecho, con la intención de hacer llegar al usuario, unos mínimos conocimientos de lo que es y para que se utiliza la seguridad en redes informáticas, llegando a diferenciar de un simple antivirus o anti malware, a un firewall o servidor proxy dentro de una VPN. Además, se realiza con la intención de que el usuario se conciencie que, dentro de una red, o de un simple equipo de una red, existen diversas puertas de acceso a la red "ocultas", y varios tipos de datos dentro de un mismo equipo conectado, e interconectado, tanto a una red pública (Internet), como a una red privada.

2.1. Seguridad doméstica

En la actualidad, existen diversos tipos de usuarios de la red. En este capítulo del trabajo, serán tratados con especialidad, los usuarios de la red en el ámbito doméstico.

Hoy en día, cualquier persona tiene acceso a la red y desde cualquier dispositivo. Esto implica, que la protección de datos de todo tipo (desde más, a menos confidencial) es cada vez más escasa. No todos los usuarios aplican las mismas medidas de seguridad.

El uso de la red, viene desde una persona de avanzada edad que utiliza un dispositivo IoT para ponerse en contacto con sus familiares mediante una app de video llamadas como puede ser Skype, hasta un empleado de banca que a causa de la pandemia de la covid-19, debe permanecer en su domicilio con una conexión a internet, y a la red privada del banco en el que ejerce sus labores de ámbito laboral.

Por ello, en este trabajo se proponen una serie de medidas de seguridad, algunas pueden ser empleadas desde un ámbito doméstico en el que pueden ser implantadas una serie de medidas de seguridad virtual (configuraciones de software de los dispositivos comunes en una red doméstica) hasta una seguridad física (implantaciones de dispositivos de seguridad en la red).

2.1.1. Definición de la problemática en la seguridad del ámbito doméstico.

A pesar de ser un tema de interés actual, ya que cada día que pasa el usuario se encuentra más en contacto con la red, pocos son los usuarios que implantan unas medidas de seguridad en el ámbito doméstico.

Para el desconocimiento en la gran mayoría de los usuarios, cualquier dispositivo conectado a la red puede ser un portal de acceso para la vulnerabilidad de la red, y por ello, poder tomar el control total de la misma. Así mismo, pudiendo acceder a cualquier dispositivo de esta para la sustracción de datos entre otros muchos movimientos.

2.1.2. Tipos de seguridad en una red doméstica.

A continuación, se detallan una serie de medidas de seguridad informáticas, las cuales pueden ser implantadas en un ámbito doméstico por una gran número de usuarios, medidas de bajo coste, y que proporcionarán una conexión segura a cualquier.

1. Mantener actualizado cada dispositivo: Todo dispositivo conectado a una red, es un dispositivo expuesto, desde el dispositivo IoT más pequeño que es un aspirador wifi manejado desde una app móvil que puede transmitir mediante la red un pequeño mapa de nuestra casa, hasta el más grande servidor de almacenamiento privado en el que se encuentra información sensible particular del usuario deben estar actualizados a la última versión de firmware del fabricante.
2. El tipo de contraseña adecuado: Una de las medidas de seguridad más utilizadas por todos los usuarios en infinidad de dispositivos, son las contraseñas. Frecuentemente se utiliza una contraseña fácil de vulnerar como "hola" en lugar de "H0l@", a diferencia de una contraseña a la otra, la contraseña "rara" es la contraseña segura. Como es fácil observar, la contraseña "H0l@" se compone de diversos caracteres, Letra mayúscula, número, letra minúscula, símbolo adicional, mientras que "hola", únicamente contiene letras minúsculas. En el ámbito de la seguridad doméstica para un campo tan sencillo como puede ser la contraseña de cualquier dispositivo, es recomendable usar una contraseña fuerte, ya que será más complicada de descifrar por software específico destinado a ello.

3. Separar la información laboral, de lo personal: Quizás, junto a la contraseña, estos campos sean los pilares más fundamentales de una buena protección en la red doméstica. A la hora de recibir un ciber ataque, nuestro equipo está expuesto al ataque con la toda información contenida. Por ello, es recomendable separar la información personal de la información laboral. Una buena práctica es utilizar varios discos duros externos a los equipos de la red para poder almacenar información separada.
4. Utilidad de software de seguridad informática: El software por excelencia y altamente conocido por todo usuario de cualquier dispositivo conectado a la red, es el antivirus. Este es un software el cual gestiona diversos protocolos de seguridad y diversas protecciones frente a los diferentes ataques que navegan por la red, además, este software es capaz de albergar diversas protecciones. Gran parte de los software antivirus, ofrecen la posibilidad de crear y navegar mediante una red VPN.
5. Ofrecer protección a la red inalámbrica: En la mayoría de los casos, los usuarios domésticos, bien por desconocimiento o bien por comodidad, mantienen la contraseña por defecto establecida en el router. Esta práctica, es una práctica bajamente recomendable ya que los software de descifrados de claves de red (claves normalmente WEP y WAP), utilizan una auditoria de paquetes, analizando y comparando en una base de datos propia hasta encontrar una similitud. Una buena práctica, sería la de cambiar tanto el nombre de la red, como la contraseña dadas por defecto por la configuración del router en la compañía correspondiente.
6. Utilizar una red VPN: Tal y como fue nombrado en el punto número 4 de este capítulo del trabajo, las redes VPN son un tipo de redes, en el caso del ámbito doméstico, virtuales, que pueden ser generadas mediante un software específico para ello o incluso desde el software antivirus instalado en dicha máquina. Este tipo de red la característica principal, es la capacidad de crear un "túnel" en el que viajan los datos cifrados desde la red privada a la red pública o viceversa, así, siendo menos vulnerables a los ataques que rondan en la red.

2.2. Empresas y su seguridad

Hoy en día la seguridad en el ámbito laboral es un tema cada vez más en auge. Las empresas se encuentran cada día más informatizadas, y por consiguiente, con mayor número de paquetes de información navegando por la red, para ello, la seguridad informática es un ámbito potencialmente interesante desde hace unos años.

2.2.1. Definición de seguridad informática para la empresa

La seguridad informática es la práctica de conocer los procesos de prevención y detección de posibles ataques y vulnerabilidades en la red de trabajo, para ello es importante en esta práctica el conocimiento del uso de la red, y la prevención de acceso a redes y

La empresa necesita certificar que los datos de sus clientes se encuentran a salvo, para ello, es primordial contar con unas medidas de seguridad informáticas elevadas, no siendo únicamente un software antivirus el que se utilice como protección de la red.

Los servidores nombrados en apartado siguientes, serán los servidores que deban estar instalados, configurados y funcionando en un servidor local de la empresa en cuestión para asegurar una buena protección.

2.2.2. Prevención en la seguridad de red de la empresa.

La prevención es un pilar fundamental a la red de trabajar en red. Para contar con una seguridad correcta en la red, son diversos los puntos a reforzar para conseguirla. Uno de los puntos fundamentales y más básicos, es el conocimiento del usuario para ello, pero no todos los usuarios tienen los suficientes conocimientos para ello.

Para ello, son algunas prácticas básicas las que se deben aplicar, tanto desde el lado del usuario, como del lado del administrador de la red.

El administrador de la red, es el encargado de que la red funcione correctamente y además, el encargado de revisar que no se produzca vulnerabilidades, unas de las prácticas básicas son las siguientes:

- Asegurar que el software instalado es legal y se encuentra con sus credenciales de autenticación y legalidad
- Software antivirus, anti espías y antimalware correctamente configurados y definidos con las reglas impuestas en la empresa en cuestión
- El uso de claves de acceso con alta protección, para ello es recomendable utilizar, mayúsculas, minúsculas, números y caracteres especiales.
- Limitar el uso de accesos a la red a los usuarios, permitir el acceso a sitios webs únicamente necesarios para la correcta práctica laboral
- Utilizar encriptación, es importante la utilización de la encriptación para los paquetes que naveguen por la red, ya que algunos pueden ser interceptados de manera maliciosa y ser utilizados fraudulentamente.
- Software antivirus instalado masivamente para la red, esta práctica asegura al administrador de red el control del software antivirus para toda la red, siendo capaz de configurar los análisis masivos por la red, la configuración de vulnerabilidades especificando la detección de posibles software maliciosos, detectando inclusión mediante dispositivos USB conectados a un equipo de la red y siendo capaz de meter en cuarentena a algún fichero contenido en un dispositivo USB, incluso eliminando, notificando al usuario de dicha acción entre otras.

Por otra parte, un papel importante es el usuario, es el que debe saber cómo utilizar la red correctamente, sabiendo donde debe acceder o no, aunque esa función es parte también del firewall (es el encargado de gestionar el tráfico de la red) y proxy (es el encargado de administrar el accesos a las diferentes URL).

Una de las pequeñas observaciones que debe saber poner en práctica el usuario a la hora de acceder a una URL cualquiera, es saber que está accediendo a un sitio seguro, esto es fácil de identificar si el usuario se fija en el icono del candado que aparece en el navegador, indicando este último si el sitio es correcto (debe aparecer en la barra de direcciones del navegador un candado relleno de color correctamente (Véase la figura 1)) o no (debe aparecer en la barra de direcciones del navegador un candado con una advertencia (Véase la figura 2))

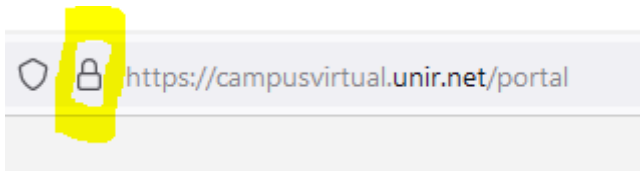


Figura 1: Conexión Segura

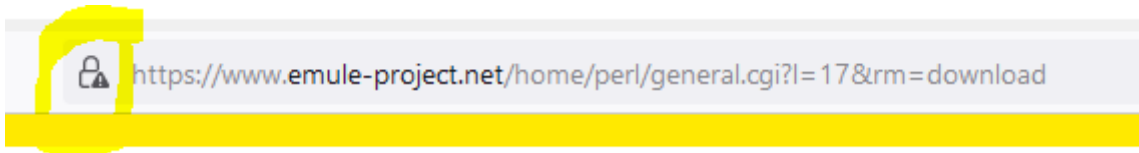


Figura 2: Conexión Insegura

2.3. Conocimiento de Seguridad por el usuario para una red informática.

A raíz de la pandemia de la Covid-19 la seguridad informática ha comenzado a tomar auge, el usuario por culpa del teletrabajo impuesto en muchas empresas, ha obligado al usuario a verse más informado en este sector dentro de la informática. Dicho usuario debe sentirse protegido en su red, ya que el tratamiento de datos sensibles en una red desprotegida puede involucrar en un problema tanto a trabajador como a empresa responsable de dichos datos sensibles.

2.3.1. Seguridad para el usuario novel

Se habla en este apartado del capítulo, del usuario novel, un perfil de usuario básico en la informática, conocedor de algunas medidas de seguridad para su equipo en la red, las cuales la mayoría de ellas se encuentran implementadas en el propio sistema operativo de la máquina. Este perfil suele ser conocedor de un software de antivirus instalado y configurado en su equipo.

SEGURITFG es un software diseñado para este tipo de usuario, el cual aun siendo desconocedor de medidas de seguridad informática, con solo pulsar el botón deseado o varios botones de SEGURITFG, obtendría la seguridad deseada, aplicando y activando la seguridad de una red VPN, junto a la que pueden ofrecer tanto firewall, como servidor proxy.

2.3.2. Seguridad para el usuario avanzado

El usuario avanzado, es un perfil de usuario más conocedor en informática y puesto en la seguridad de la misma. Este perfil de usuario suele tener conocimientos más avanzados con respecto a los usuarios del apartado anterior del capítulo, es posible que conozca el funcionamiento de las redes VPN, firewall, servidor proxy, antimalware, etc. y capa de poner en funcionamiento prácticas, para ello.

Este tipo de usuario, es el que intenta no realizar conexiones a sitios web no seguras, además de utilizar un escaneo de software malicioso en su equipo sin necesidad de la supervisión del administrador de la red, también, es conocer de posibles software maliciosos contenidos en dispositivos USB a la hora de conectar a la máquina que utiliza, por ello, este tipo de usuario al ser conocedor de los posibles ataques que puede sufrir su máquina, es capaz de ejecutar un análisis previo del dispositivo externo conectado recientemente a su máquina, mediante el software antivirus o anti espías o antimalware instalado en ella.

3. Puesta en marcha de la solución

A continuación, en este capítulo del proyecto, se llevará a cabo la puesta en marcha de la solución, en la que se incluyen los apartados de identificación del problema, tanto en el ámbito doméstico como en el laboral y como poder llevar a cabo una solución a dichos problemas de seguridad que el usuario puede encontrar, tanto en un ámbito como en otro, al igual que se nombrarán y definirán algunas de las diferentes tecnologías de seguridad que pueden ser implantadas para obtener una conexión de red segura y la explicación del funcionamiento de la tecnologías nombradas a lo largo de este capítulo.

3.1. Identificación del problema en el ámbito domestico

3.1.1. Tipos de conexiones seguras en el ámbito domestico

En la actualidad, los sistemas remotos ofrecen grandes ventajas, una de la gran ventaja es para los trabajadores de una empresa, en una situación extrema como es la vivida con la COVID-19, es capaz de ofrecer servicio de un trabajador desde un puesto diferente a la oficina, normalmente desde el ámbito doméstico.

A pesar de poder este ocupar su lugar de trabajo desde su domicilio y con una conexión remota, el usuario debe cumplimentar unas normas de seguridad, para proteger tanto su información personal, como la profesional (laboral)

3.1.2. Solución a los problemas de seguridad en el ámbito doméstico.

En este apartado es posible identificar una serie de Protocolos y software capaces de ofrecer la seguridad necesaria para la protección de dicha red (tanto la red laboral, como la red doméstica)

Una protección podría denominarse protección completa, con la aplicación de un Firewall, este sería quien formase una "barrera" entre la red pública y la red privada. La aplicación y puesta en marcha de una red VPN, proporcionaría la ventaja de poder navegar de modo incognito, esta enmascararía la dirección IP del equipo simulando una IP diferente a la real, así mismo, este pudiendo navegar sin ser localizado. El servicio de un servidor proxy es el de redirección de un equipo en la red pública, es el encargado de recibir las peticiones de navegación del equipo cliente, y

redireccionar a dicha página solicitada si tiene acceso establecido para poder navegar en ella o redireccionar a una página en la que se puede mostrar un mensaje diciendo que no está permitida la navegación a dicha dirección web.

Así mismo, para formalizar la conexión contra el servidor o el puesto de trabajo del ámbito laboral, lo recomendable es crear una conexión de escritorio remoto, ya que asegura que dicha conexión es directa con el puesto de trabajo y no pasando un servidor externo de un software de terceros de conexión remota como podría ser Teamviewer o Anydesk.

En cambio, existe software de terceros no pertenecientes a Windows como podría ser "VNC". Este tipo software está basado en un protocolo llamado RFB, este es un protocolo de acceso remoto a interfaces graficas de usuario.

3.2. Definición de las tecnologías de seguridad

A continuación, se detallan una serie de medidas de seguridad, las cuales aplicadas en conjunto, son capaces de ofrecer una gran seguridad para la protección los datos más o menos sensibles a la hora de conectar contra un servidor de una red privada de un puesto de trabajo.

3.2.1. Definición de Firewall

Un Firewall es una tecnología tanto física como virtual que puede gestionar el filtrado total del tráfico entre un equipo y otro de una misma red o una red distinta.

En este se declaran una serie de reglas, que han de ser cumplidas para así poder llevar a cabo el tráfico de paquete en la red, contando con la notación, de si no son cumplidas dichas reglas, el tráfico de paquetes en la red, no será llevado a cabo.

Este tipo de tecnología es usada para limitar el tráfico de la red acorde a la configuración reglada previamente cargada, así, pudiendo ser bloqueado un tráfico de paquetes con contenido malicioso.

3.2.1.1. Utilidad de un firewall

La función de un firewall en la red, es definida por un administrador de sistema.

Este es el encargado de la configuración de dicho Firewall, será el encargado de gestionar las reglas del Firewall para que este pueda realizar sus funciones en la red.

Las funciones del Firewall no son más que las de proteger a los equipos conectados a la red, de la intrusión e incluso del filtrado de paquetes maliciosos. Estos provenientes de un nodo emisor, pasando por el Firewall para cumplir las reglas definidas previamente por el administrador del sistema y finalmente acabar en un nodo destino.

Así mismo, el administrador del sistema siente la tranquilidad de saber que la red funciona correctamente y está estando protegida de ataques vulnerables a los equipos de dicha red, e incluso de los servicios de la red. (Obsérvese figura 3)



Figura 3: Utilidad de Firewall

3.2.1.2. Motivos por los que utilizar un firewall

- Preservar la seguridad y la privacidad de la red ya sea doméstica o empresarial.
- Preservar la seguridad y la privacidad de la información almacenada en la red, equipos o servidores.
- Evita la intrusión de usuarios no deseados en la red y en los equipos de la misma.
- Preserva la seguridad frente a ataques de denegación de servicios de la red.

3.2.1.3. Funcionamiento de un Firewall en la red

El Firewall tiene la función de "barrera" entre la red pública y la red privada. Dicha tecnología es implementada para el filtrado de paquetes maliciosos provenientes de la red pública (Internet) hacia la red privada a la que se encuentra protegiendo este.

En la figura 4 se muestra el funcionamiento de un Firewall en una red con un pequeño esquema para la aclaratoria visual.

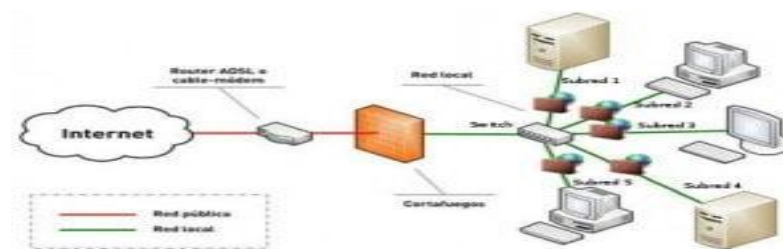


Figura 4: Esquema funcionamiento de Firewall

3.2.2. Definición de VPN

VPN son las siglas de "virtual private network (Red privada virtual)", es una tecnología que permite seguridad entre la red local y la red pública, conectando dos equipos de distintas redes locales privadas conectadas a la red pública, como si de una sola red local se tratase (Véase la Figura 5).

Dicho tipo de red, privadas virtuales, son utilizadas mayoritariamente por empresas para la transferencia de ficheros de datos de carácter sensible, en el momento que uno de sus empleados se encuentra realizando tareas laborales fuera de su lugar de trabajo, como puede ser en viajes de reuniones.



Figura 5: Funcionamiento de una red VPN

3.2.2.1 Protocolos en los que se basa VPN

Los servidores VPN, están basados en una serie de protocolos, los cuales en conjunto configuran una serie de seguridad, las cual conjuntamente funcionan formando la red privada virtual.

Los protocolos de seguridad son una serie de reglas que se establecen entre diferentes equipos de una red para poder comunicarse entre sí y formar un canal de transmisión de información. Los protocolos pueden ser establecidos tanto en hardware como en software, o ambos combinados entre sí.

3.2.2.1. IPsec(Internet Protocol Security):Es un protocolo que está formado por diferentes protocolos de seguridad. Dicho protocolo es utilizado por ser capaz de cifrar completamente un paquete de datos, este cifrado es utilizado para garantizar la confidencialidad y la autenticación. Entre muchas de sus ventajas, destaca la de poder operar a nivel de red a diferencia de otros sistemas como podría ser SSL, que es un protocolo capaz de operar en el nivel de aplicación, estos como complejidad, también necesitan realizar cambios en las aplicación, en cambio IPsec, únicamente necesita realizar cambios en el sistema operativo.

- Funcionamiento de IPsec

IPsec, es un protocolo de seguridad capaz de operar a nivel de red adquiriendo la ventaja de poder cifrar un paquete completo de IP. Para esto, utilizar dos operaciones:

- Encabezado de autenticación (AH):AH para ofrecer la protección de la red y los datos para interferencia de terceros, utiliza una firma digital en cada uno de sus paquetes, así ofreciendo verificación en los diversos extremos de la red.
- Carga de seguridad encapsulada (ESP):ESP, al contrario que AH, ofrece garantía de que la información contenida en el paquete esta encapitada y no puede ser manipulada.

- Funcionamiento de IPsec junto a otros protocolos utilizados en VPN.

IPsec, es un protocolo de seguridad aplicado a las VPN, cuya característica es la de poder trabajar con facilidad en la capa de red, y así poder aplicar cambios a nivel de sistema operativo. A continuación se detallan algunos protocolos con los que IPsec es capaz de trabajar de manera muy eficiente:

- I2tp: Es un protocolo de túnel. Como desventaja posee la incapacidad de trabajar por sí solo no siendo capaz de proporcionar ningún cifrado. En cambio, en la combinación que puede ofrecer con IPsec, forman un dúo perfecto. IPsec y I2tp combinados y utilizando códigos AES para el cifrado, ofrecen altas velocidades y niveles extremos en seguridad referentes a los paquetes de datos.
- IKEv2: Es un protocolo de túnel. Como ventaja, IKEv2 ofrece la capacidad de reconexión frente a pequeñas pérdidas de conectividad. Al ser combinado con IPsec, son capaces de ofrecer una alta capacidad de respuesta y flexibilidad.

3.2.3. Definición de Servidor Proxy

Un servidor proxy, es un equipo en la red situado en medio de una comunicación entre dos equipos de dicha red, este, es el encargado del filtrado de conexiones, para ello, se realiza una previa configuración de este servidor en el que se le dice cuáles son las conexiones permitidas, cuáles no, o incluso el grupo de usuarios que tiene acceso a unas direcciones URL específicas y quiénes son.

3.2.3.1. Utilidad de Servidor Proxy

Como se nombraba anteriormente en la descripción previa de este apartado del capítulo, el servidor proxy es aquel equipo intermedia entre un servidor final al que se le realiza o intenta realizar la conexión y el equipo del usuario en cuestión

Las funciones entre otras, son las de Controlar el acceso a la red, el filtrado del contenido y la función de caché.

Este, utiliza la función de caché, después de haber accedido a una web, el servidor Proxy es capaz de guardar la información contenida en el sitio web al que se quiere acceder, así permitiendo la visualización del contenido de dicha web sin tener que salir a la red pública (Internet).

3.2.3.2. Proxy Inverso

Como su propio nombre indica, este tipo de proxy, realiza las funciones inversas a las definidas anteriormente en la definición de un servidor Proxy. Este tipo de Proxy las solicitudes las realiza desde internet hasta el equipo servidor de la red privada (Véase la Figura 6).

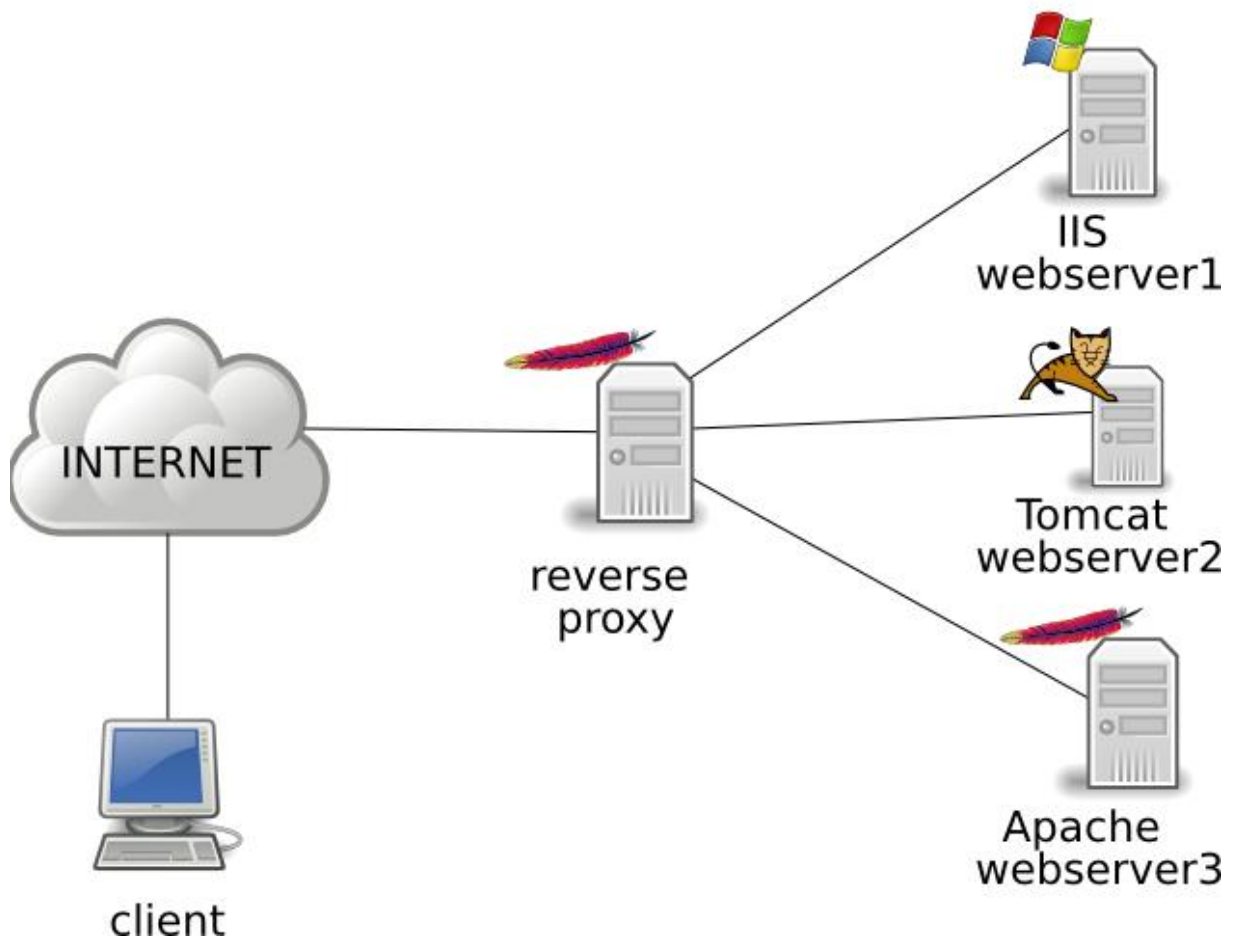


Figura 6: Proxy inverso

Normalmente este tipo de servidores (Servidor Proxy Inverso) se suelen utilizar para alojar páginas web ya que esto conlleva una serie de ventajas, algunas de ellas son:

- Equilibrio de carga: Este tipo de servidor tiene la particularidad de poder conectar a varios servidores destinos diferentes y dirigir las solicitudes a cada uno de ellos para no sobrecargar ninguno y dejar otros sin carga ninguna, la ventaja que ofrece es que las solicitudes desde la red pública (Internet) únicamente conocerán la dirección IP del Servidor Proxy y no la de cada uno de los servidores que componen la red en la que se encuentra alojada la página web que se desea visitar.
- Caché: Los servidores Proxy entre otras funciones, conllevan la de optimizar las solicitudes entre el origen y el destino. El servidor Proxy inverso, recopila y guarda información de páginas webs almacenadas en servidores internos, de vez en cuando actualizando la información contenida en él para que los servidores de las webs alojadas, reciban menor número de solicitudes de red, así funcionando mejor al no tener momentos de saturación de recepción de solicitudes y ni sobrecargas en momentos esporádicos.

4. Instalación y configuración de los servidores

En este capítulo del proyecto, se llevará a cabo una pequeña guía de cuál es el servicio que ofrece cada uno de los servidores seguidamente nombrados, como se realiza, tanto la instalación, configuración como el funcionamiento de los mismos.

4.1. Servidor VPN

La conexión a la red privada virtual (VPN), es la conexión mediante la cual los usuarios de una empresa pueden conectarse a equipo en su puesto de trabajo desde cualquier lugar, como si de una red local se tratase, pero con la ventaja de utilizar una conexión segura, viajando por la red con una nueva ip, distinta a la de su equipo local.

4.1.1. Instalación

En primer lugar, para poder conectar desde un equipo a otro, como si de una red local se tratase, pero sin ser así, y mediante la red pública, debemos crear una red VPN.

Para ello lo el primer paso a llevar a cabo, es la creación e instalación de un servidor de VPN, en este caso se utilizara el software OpenSource OpenVPN, descargando un software ejecutable, el cual está disponible en la web de [OpenVPN](https://openvpn.net/).

Una vez descargando, en la tercera pantalla, se debe seleccionar la opción "EasyRSA 2 Certificate Management Scripts" (Véase en la figura 7)



Figura 7: Selección EasyRSA 2 Certificate Management Scripts

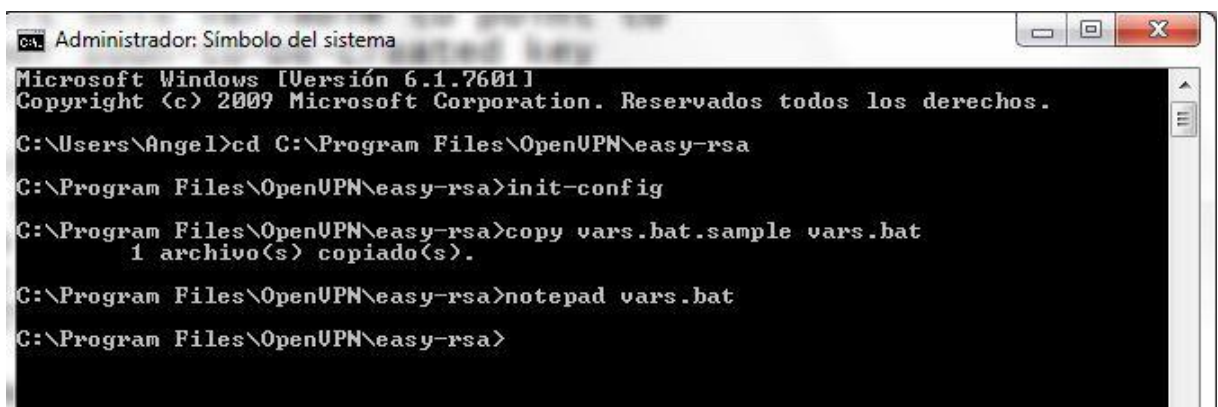
Esta casilla seleccionada a la hora de la instalación, manda a instalar la unidad certificadora encargada de generar en el servidor VPN los certificados para que los clientes puedan conectar a él. Durante la instalación, el software, preguntara si se desea instalar el adaptador virtual TAP, este es el encargado de efectuar la configuración de la IP para la red VPN y la comunicación.

4.1.2. Configuración

En este capítulo de dicho apartado del proyecto, se verá como configuración la red VPN anteriormente instalada con el instalador de OpenVPN OpenSource.

Para ello, en primer lugar se debe abrir una ventana de comandos (cmd.exe) la cual se usara para la configuración del fichero " vars.bat ", una vez dentro de la consola de comandos, se escribirá " cd C:\Program Files\OpenVPN\easy-rsa ", para entrar al directorio donde se aloja el fichero de configuración, una vez dentro, se escribirá una nueva orden " init-config " para acceder a la configuración

Una vez dentro de la configuración, se escribirá " copy vars.bat.sample vars.bat" para la creación de un archivo de respaldo, seguidamente, se llevara a cabo en el nuevo fichero la configuración, este se ejecutara y abrirá mediante notepad, para ello, se debe escribir " notepad vars.bat " (véase la figura 8)

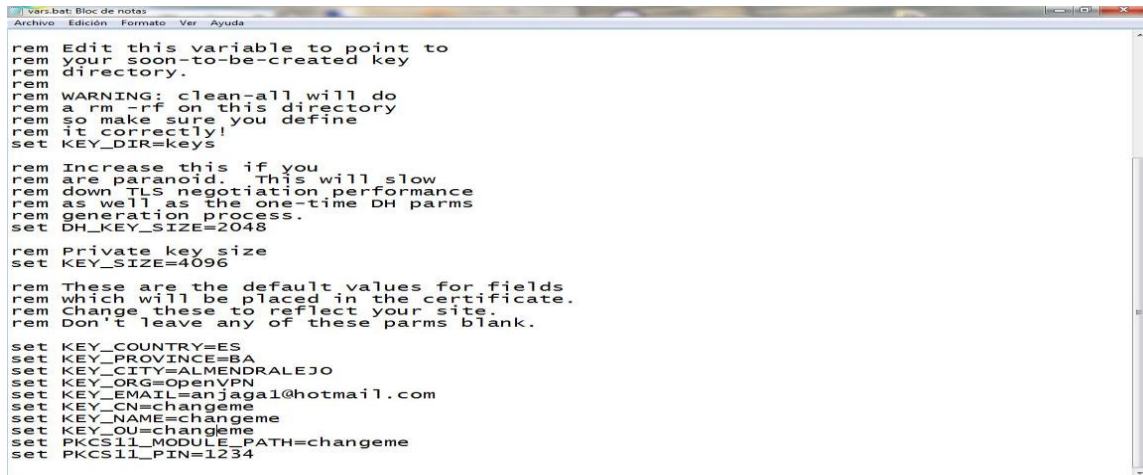


```
cs. Administrador: Símbolo del sistema
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Ángel>cd C:\Program Files\OpenVPN\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>init-config
C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
1 archivo(s) copiado(s).
C:\Program Files\OpenVPN\easy-rsa>notepad vars.bat
C:\Program Files\OpenVPN\easy-rsa>
```

Figura 8: Proceso de entrada a la edición de la configuración

A continuación se abrirá el bloc de notas, en donde se deben sustituir las líneas marcadas en la figura 9 por los datos del propietario del servidor VPN



```
rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this if you
rem are paranoid. This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set DH_KEY_SIZE=2048

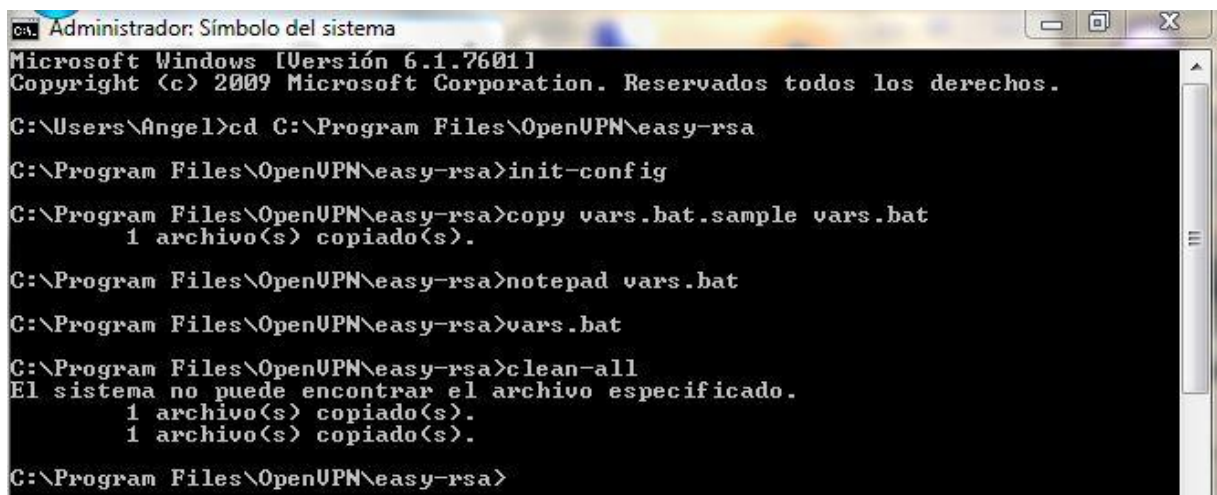
rem Private key size
set KEY_SIZE=4096

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=ES
set KEY_PROVINCE=BA
set KEY_CITY=ALMENDRALEJO
set KEY_ORG=OpenVPN
set KEY_EMAIL=anjaga1@hotmail.com
set KEY_CN=changeme
set KEY_NAME=changeme
set KEY_OU=changeme
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

Figura 9: Edición de los datos del propietario de la VPN

Una vez modificado el fichero " vars.bat ", se debe guardar los cambios, permaneciendo en la misa ruta en la que se encontraba. A continuación, se ejecutara el comando " vars.bat" de nuevo para la ejecución del fichero y el comando " clean-all" (Véase en la figura 10).



```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Angel>cd C:\Program Files\OpenVPN\easy-rsa
C:\Program Files\OpenVPN\easy-rsa>init-config
C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
1 archivo(s) copiado(s).
C:\Program Files\OpenVPN\easy-rsa>notepad vars.bat
C:\Program Files\OpenVPN\easy-rsa>vars.bat
C:\Program Files\OpenVPN\easy-rsa>clean-all
El sistema no puede encontrar el archivo especificado.
1 archivo(s) copiado(s).
1 archivo(s) copiado(s).
C:\Program Files\OpenVPN\easy-rsa>
```

Figura 10: Ejecución del fichero " vars.bat"

4.1.3. Generación de claves y certificados del servidor VPN

En este apartado de este capítulo del proyecto, se generaran las claves y certificados necesarios para la conexión con el servidor VPN. En primer lugar se crearan las claves, para ello se debe ejecutar el comando `build-ca` (Véase en la figura 11) en la línea de comandos. Una vez ejecutado el comando, se generara la entidad certificadora, la cual será la encargada de generar posteriormente los certificados de conexión.

Seguidamente, comenzaran a salir por pantalla las líneas de configuración anteriormente modificadas con notepad, por lo cual, se puede continuar con solamente pulsar la tecla Enter, a excepción de la línea " Common name " a la cual le tiene que decir el nombre del servidor VPN, en el caso de este proyecto, el nombre será " `vpn_tfg` "

```
C:\Program Files\OpenUPN\easy-rsa>build-ca
Generating a RSA private key
.....++++
.....++++
writing new private key to 'keys/ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
State or Province Name (full name) [BA]:
Locality Name (eg, city) [ALMENDRALEJO]:
Organization Name (eg, company) [OpenUPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:vpn_tfg
Name [changeme]:
Email Address [anjaga1@hotmail.com]:
C:\Program Files\OpenUPN\easy-rsa>
```

Figura 11: Generación de la entidad certificadora

El siguiente paso será el de la creación de las claves del servidor. Para ello se debe de escribir la línea de comandos " `build-key-server server` " y pulsar la tecla Enter, al instante comenzaran a salir diversas líneas por pantalla en la consola de comandos (Véase la figura 12), para la finalización de la creación de las claves, se debe teclear la letra " `y` " dos veces, para confirmar tanto la creación de la clave como la firma.

```
C:\Program Files\OpenUPN\easy-rsa>build-key-server server
Generating a RSA private key
.....
++++
.....
++++
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
State or Province Name (full name) [BA]:
Locality Name (eg, city) [ALMENDRALEJO]:
Organization Name (eg, company) [OpenUPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme:server]
Name [changeme]:
Email Address [anjaga1@hotmail.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Can't open keys/index.txt.attr for reading, No such file or directory
8828:error:02001002:system library:fopen:No such file or directory:crypto/bio/bss
_file.c:74:fopen<keys/index.txt.attr', 'r'>
8828:error:2006D080:BIO routines:BIO_new_file:no such file:crypto/bio/bss_file.c
:81:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
CountryName             :PRINTABLE:'ES'
StateOrProvinceName     :PRINTABLE:'BA'
localityName            :PRINTABLE:'ALMENDRALEJO'
organizationName        :PRINTABLE:'OpenUPN'
organizationalUnitName  :PRINTABLE:'changeme'
commonName              :PRINTABLE:'server'
name                   :PRINTABLE:'changeme'
emailAddress            :IA5STRING:'anjaga1@hotmail.com'
Certificate is to be certified until May 15 22:25:23 2031 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenUPN\easy-rsa>
```

Figura 12: Creación claves de servidor

El último proceso, en el capítulo de la creación de las claves de servidor, será la encriptación de las mismas, para ello se debe ejecutar la línea de comandos " build-dh ", este proceso dependiendo del hardware del equipo en el que se ejecute, puede tardar unos minutos más o menos en completarse (Véase la Figura 13)

[illegible]

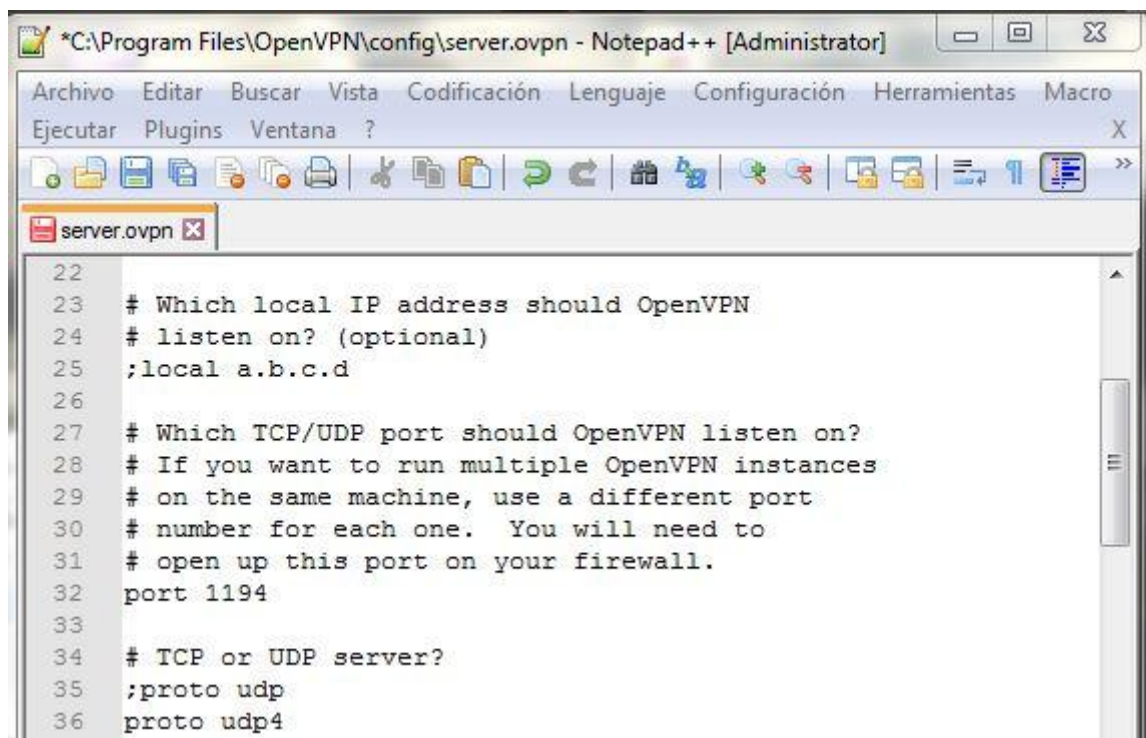
Figura 13: Encriptación de las claves de servidor

4.1.4. Configuración de parámetros en el servidor

Llegado a este punto, se pasa a la configuración de parámetros de conexión en el servidor, para ello, en primer lugar se debe navegar mediante la interfaz gráfica en la ruta de instalación, se debe copiar el fichero creado anteriormente de la carpeta “simple-config “y copiarlo a la carpeta “config “, que será donde queden alojados los ficheros de parámetros de configuración, claves y certificados.

Una vez situado el fichero en su nuevo destino, se pasa a la edición del mismo para llevar a cabo la configuración correspondiente para realizar la conexión VPN.

El primer cambio que se debe llevar a cabo, es el de decir al servidor VPN el tipo de conexión y protocolo de conexión que debe utilizar para la creación y cargo de la VPN, para ello, se deben modificar las líneas 35 y 36 (Véase en la figura 14)



```
22
23 # Which local IP address should OpenVPN
24 # listen on? (optional)
25 ;local a.b.c.d
26
27 # Which TCP/UDP port should OpenVPN listen on?
28 # If you want to run multiple OpenVPN instances
29 # on the same machine, use a different port
30 # number for each one. You will need to
31 # open up this port on your firewall.
32 port 1194
33
34 # TCP or UDP server?
35 ;proto udp
36 proto udp4
```

Figura 14: Protocolos de conexión

A pesar de que no habría problema si no se modifica estos protocolos de conexión anteriormente mostrados en la figura 14, este tipo de cambios evitan el mensaje de warning inicial al conectar la VPN.

A continuación, se debe modificar en el mismo fichero de configuración, las líneas 78 y 79, como muestra la Figura 15, se recomienda habilitar el método de tunelización “dev tap”, ya que el nodo virtual tap, permite mayor cantidad de protocolos que el modo tun.

4.1.5. Configuración de las rutas de los certificados

Llegados a este punto del capítulo, se realizarán cambios en las líneas 78, 79 y 80 del mismo fichero que hasta ahora se estaba modificando para obtener la configuración correcta (Véase la Figura 15), estas líneas son las que cargaran los certificados y las claves necesarias para la autenticación en la red VPN (Véase la Figura 16).

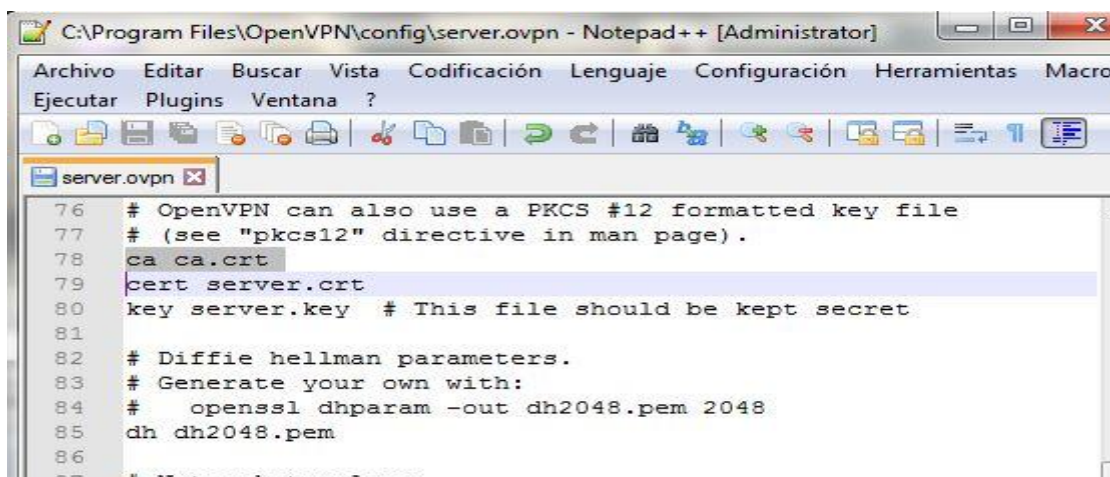


Figura 15: Ruta de los certificados por defecto

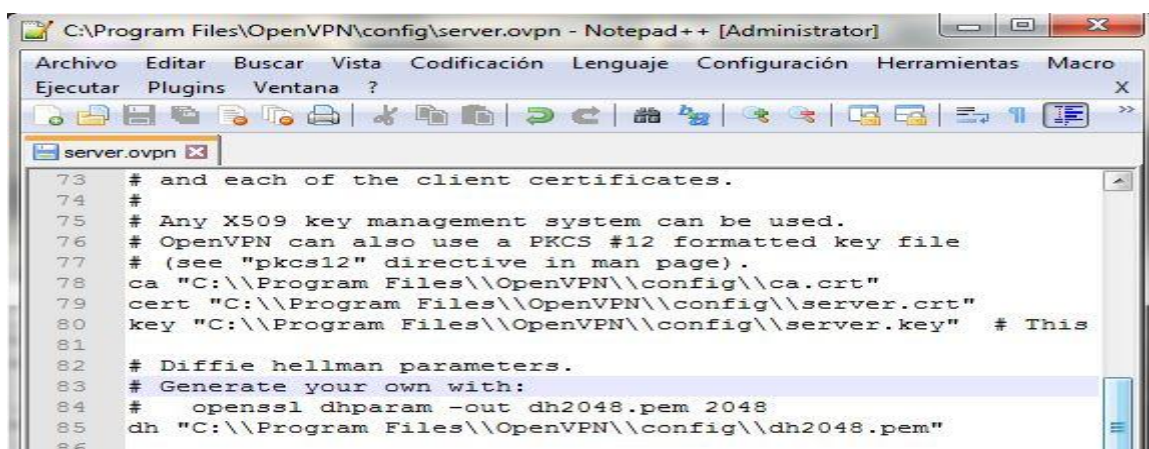


Figura 16: Ruta modificadas de los certificados

4.1.6. Direcciones IP de la red VPN

En este apartado del capítulo, se va a tratar el cambio y configuración correcta de las IP para la conexión de la red VPN en la línea 101 del archivo que hasta ahora se estaba tratando. Es importante, seleccionar una red diferente a la que tenga configurada la propia tarjeta física del servidor, ya que el adaptador virtual tap, pueden entrar en conflicto de red con la tarjeta de red física, así, no ofreciendo una conexión correcta de la VPN. Para ello se tomará la red “10.8.0.0” ya que la red del adaptador de red físico es “192.168.1.0” (Véase la figura 17)

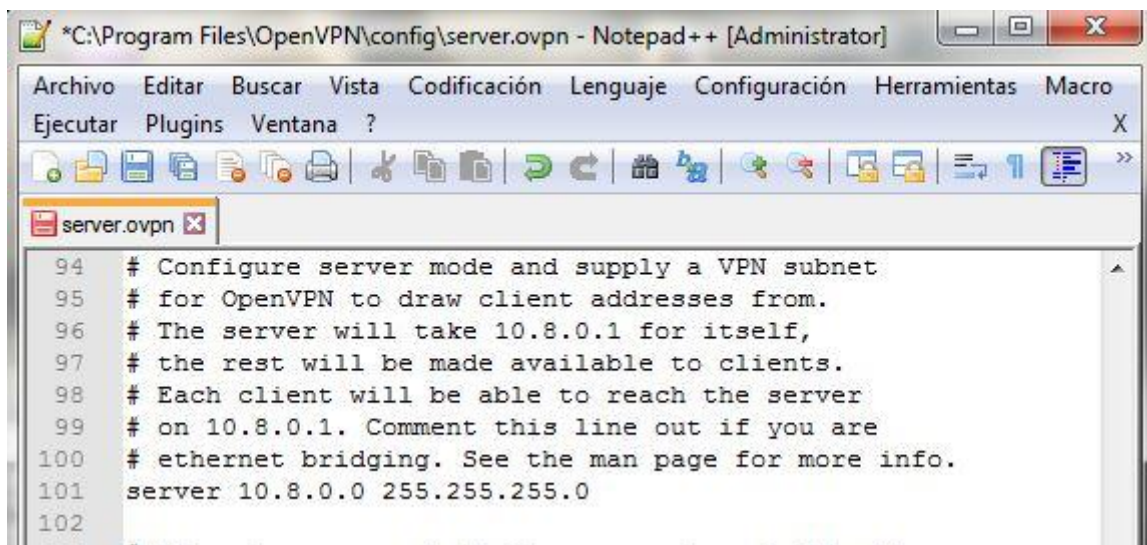


Figura 17: Selección de la red para la conexión VPN

Otro punto importante a tratar, es la línea 244, se debe tener el valor 0, ya que el valor 0 se obtiene para la conexión de servidor en la red VPN y el valor 1 para la conexión de cliente en la red VPN (se verá más adelante)(Véase la figura 18)

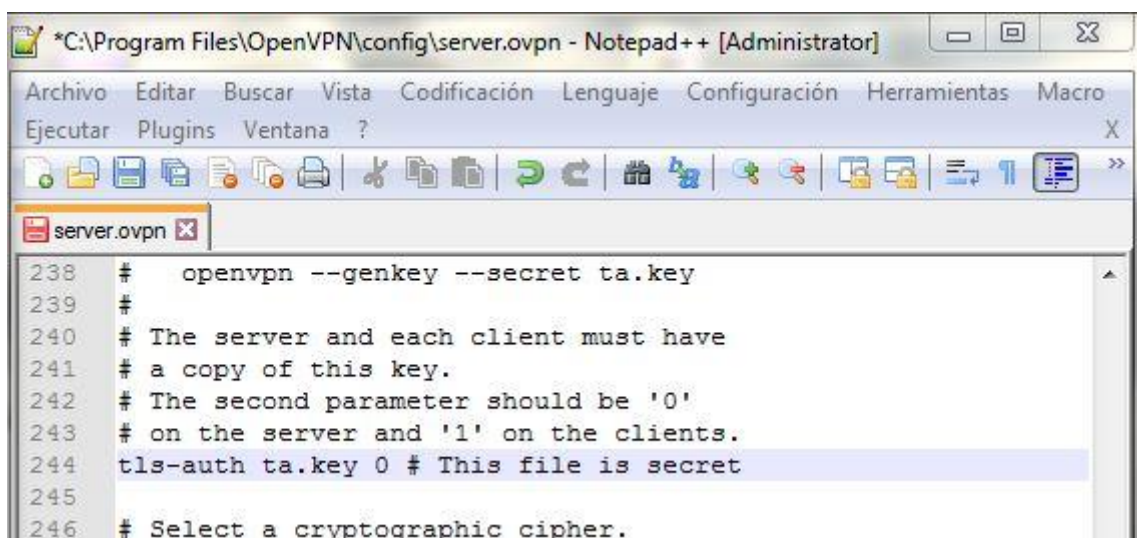


Figura 18: Selección de valor de servidor

4.1.7. Generación de ta.key, modificación del path y copia de certificados y claves a Config.

En primer lugar se debe modificar unas líneas en el path de Windows, el path es donde Windows busca los comando de ejecución en el terminal, en el caso de este proyecto y llegados a este punto, se debe agregar la ruta donde se encuentran los ficheros a ejecutar, dicha ruta es “C:\Program Files\OpenVPN\bin” (Véase la figura 19)

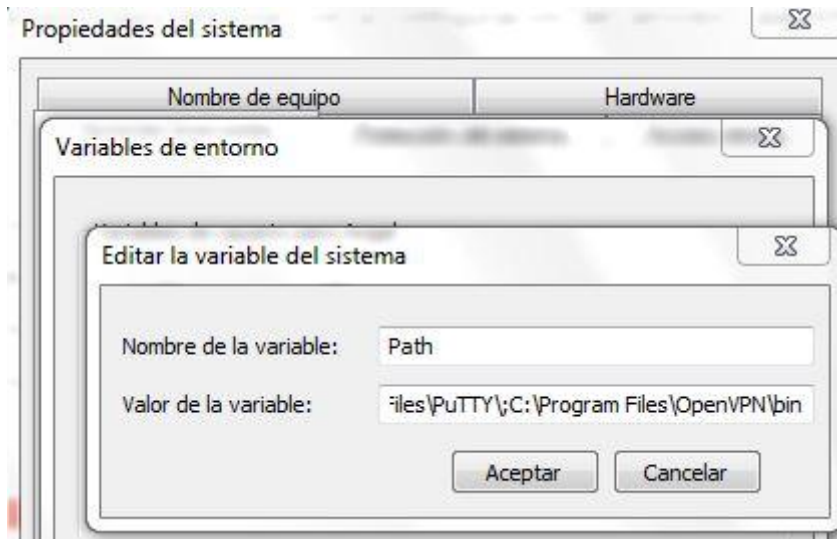


Figura 19: Añadir ruta al path de Windows

Una vez modificado el path, se debe de volver a abrir la consola de comandos para ejecutar la siguiente línea “openvpn --genkey --secret ta.key” (Véase la figura 20), estas líneas serán las encargadas de la creación de la última clave necesaria para el servidor.

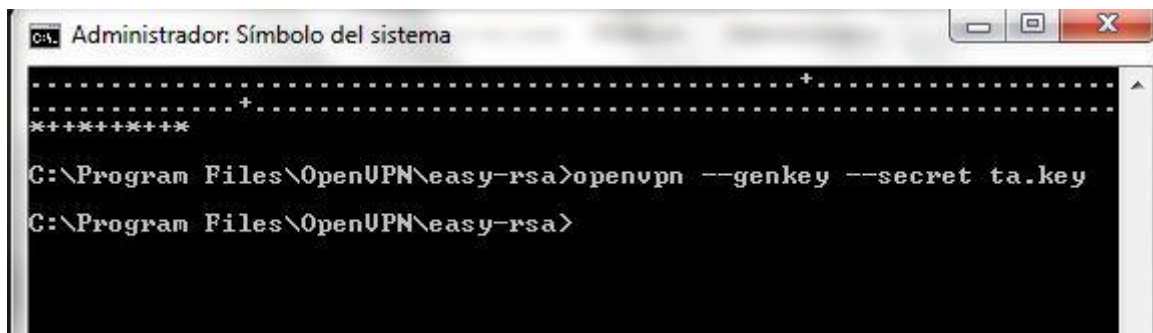


Figura 20: Creación de clave de última clave necesaria para el servidor

Para la finalización de la configuración en el servidor, se deben copiar los archivos generados en la ruta "C:\Program Files\OpenVPN\easy-rsa\keys" y en "C:\Program Files\OpenVPN\easy-rsa" y estos pegarlos en la ruta "C:\Program Files\openVPN\Config" quedando de la siguiente manera (Véase la figura 21)

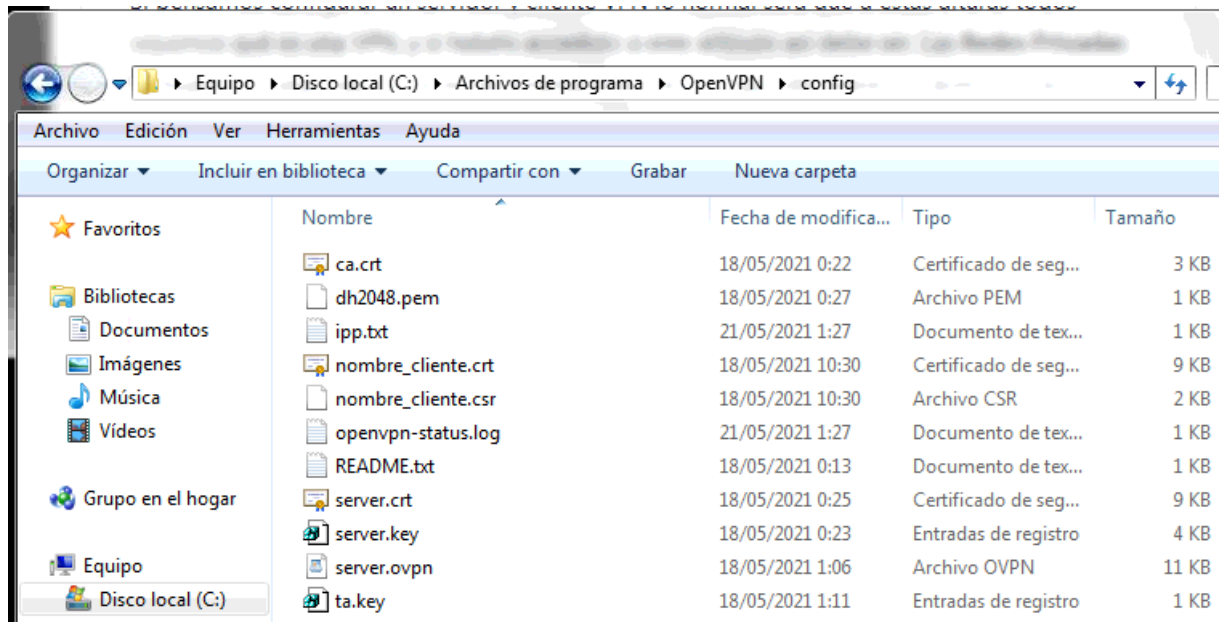


Figura 21: Colocación de archivos de autenticación

4.1.8. Arranque del servicio y VPN con OpenVPN

Llegados a este punto final, lo único que quedaría (teniendo en cuenta que aún se debe configurar e instalar el cliente VPN) sería el arranque del servicio de VPN, para ello, se debe seleccionar y ejecutar en el escritorio el acceso directo de OpenVPN Gui, pero cabe recordar antes de ello, que se debe aplicar una configuración de IP fija en el servidor, ya que todas las conexiones de clientes apuntarán a dicha IP, y si esta es modificada por el DHCP al sufrir un reinicio del equipo o un simple reinicio de la conexión a la red, la IP puede variar y dejar de funcionar el servicio de conexión de un cliente al servidor de VPN. Una vez asignada la IP fija en el servidor, dirigirse a la barra de herramientas en donde se debe pulsar el botón secundario el ratón sobre dicho icono y seleccionar la opción de "Conectar"(Véase Figura 22), en ese momento se abrirá una ventana en donde se pueden ver los procesos que ejecuta OpenVPN para la conexión a la VPN (Véase la Figura 23)

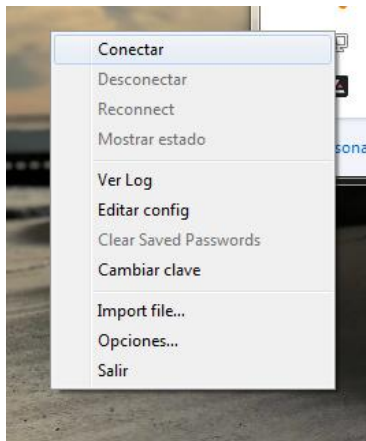


Figura 22: Conexión de la VPN

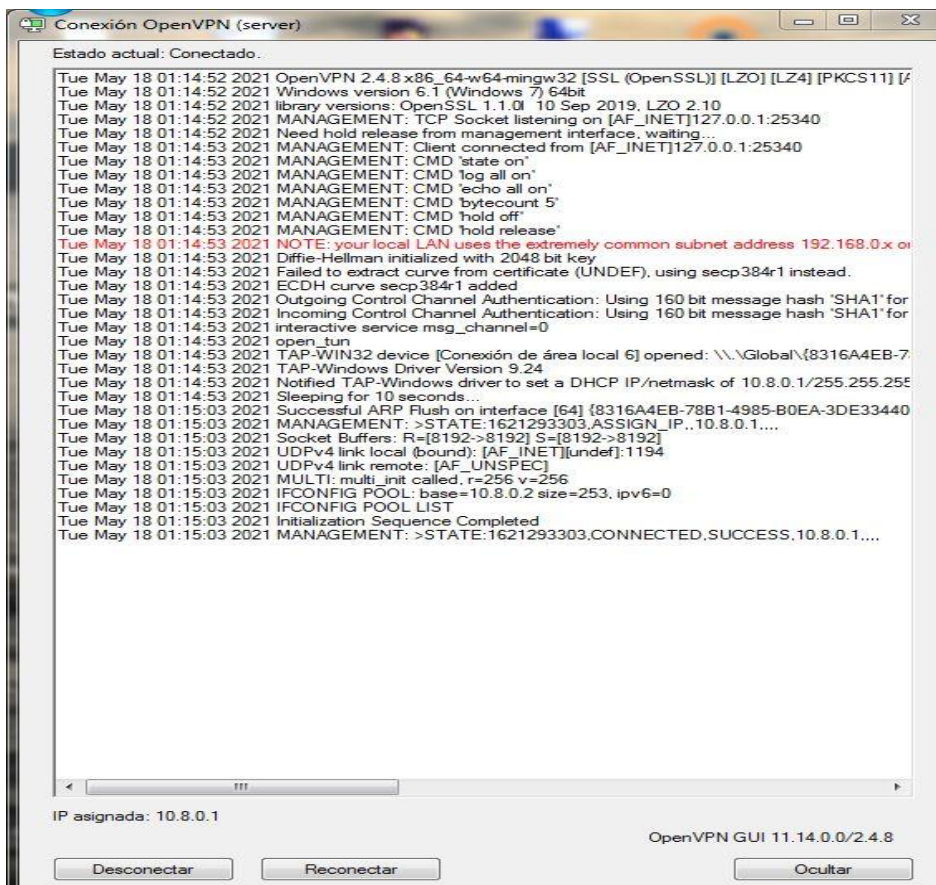



Figura 23: Conexión correcta en VPN

4.1.9. Apertura de puertos en el router y DDNS

Una vez configurada la VPN, asignada la IP fija en el servidor y arrancado el servicio, se pasa a la apertura de puertos en el router y la fijación del servicio DDNS para permitir conexiones externas remotas. Para ello se siguen los siguientes pasos (Véase las figuras 24, 27, 28)



Puerto único Rango de puertos

Dirección IP *

192.168.1.25

Puertos *

1194

Protocolo

UDP

Añadir

Dirección IP

Actualizando cambios

MIS PUERTOS

Figura 24: Apertura de puertos en el router

En la figura anterior se puede observar el procedimiento para llevar a cabo la apertura de puertos en el router, en el caso de este proyecto se trata con un router movistar, para este paso se utiliza el portalalejandra ofrecido por movistar para la configuración de sus routers.

A continuación, mediante el software “NO-IP” obtendremos un dominio DNS, para la redirección de conexiones externas. (Véase la figura 25)



Figura 25: Obtención de dominio DDNS

Una vez obtenida la IP de DDNS, el siguiente paso a llevar a cabo será la configuración de DNS en el propio router, esta vez, para acceder no será mediante el portalalejandra, sino en la dirección IP del propio router, se debe llegar a las configuración avanzada, dentro de la misma, acceder a la pestaña DNS y seguidamente entrar en DNS SERVER (Véase la figura 26)

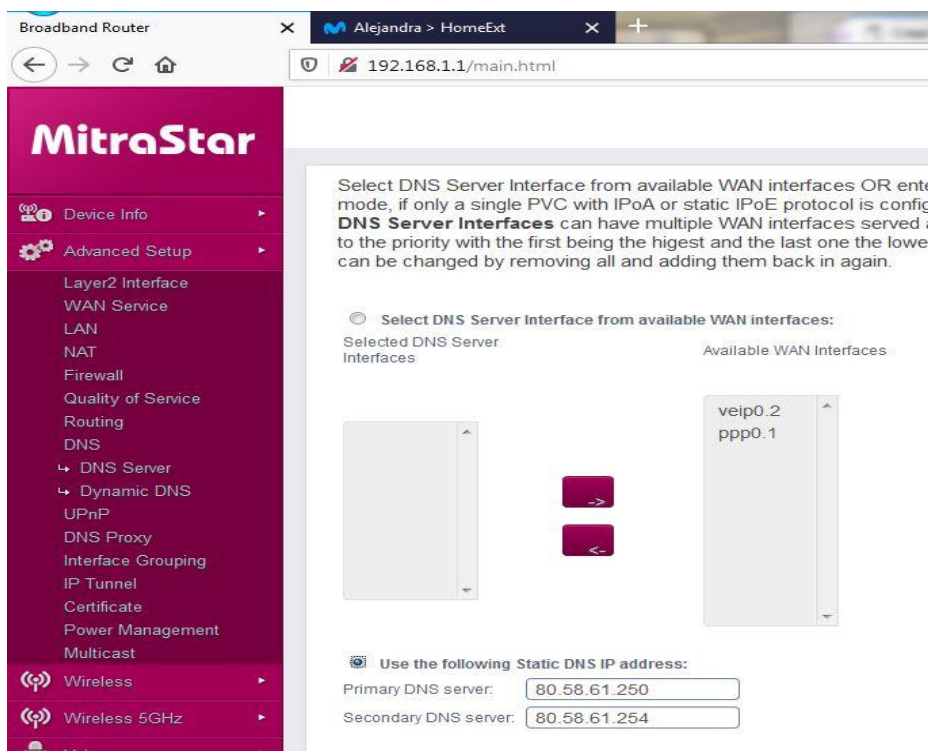


Figura 26: Selección de DNS

En la figura anterior, se puede observar que no existe ningún DDNS (DNS Dinámico), por lo cual en la siguiente pestaña que ofrece el router, se puede observar la opción “Dynamic DNS”, esta pestaña será la encargada de la creación del DDNS, se entra en ella, y se configura, señalando el proveedor de DDNS, (en el caso de este proyecto será “NO-IP”), el nombre del equipo servidor (Angel_Windows_7, en el caso de este proyecto), la interface que utilizará (“6/ppp0.1” en este caso), y por último la asignación de usuario y contraseña del DDNS (NO-IP), en este caso será anjaga1@hotmail.com el usuario junto a su password asociada (Véase la Figura 27)

MitraStar

1234 **Logout**

Add Dynamic DNS

This page allows you to add a Dynamic DNS address from DynDNS.org or TZO.

D-DNS provider

Hostname

Interface

NOIP Settings

Username

Password

Apply/Save

MSTC. All rights reserved.

Figura 27: Guardar configuración DDNS a router

Por último, quedaría únicamente, añadir el DDNS configurado al router (Véase la figura 28)

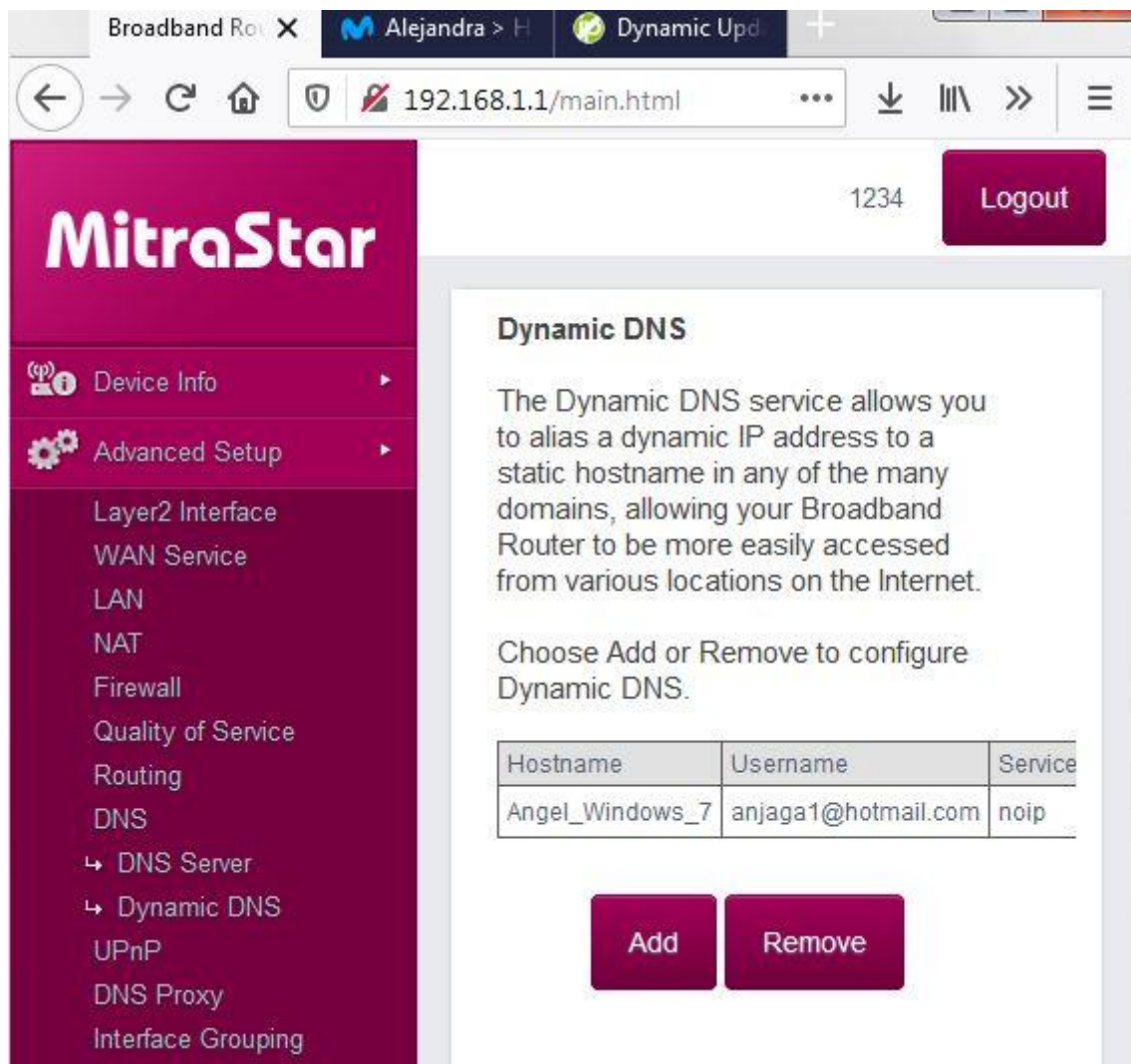


Figura 28: Añadir DDNS en el router

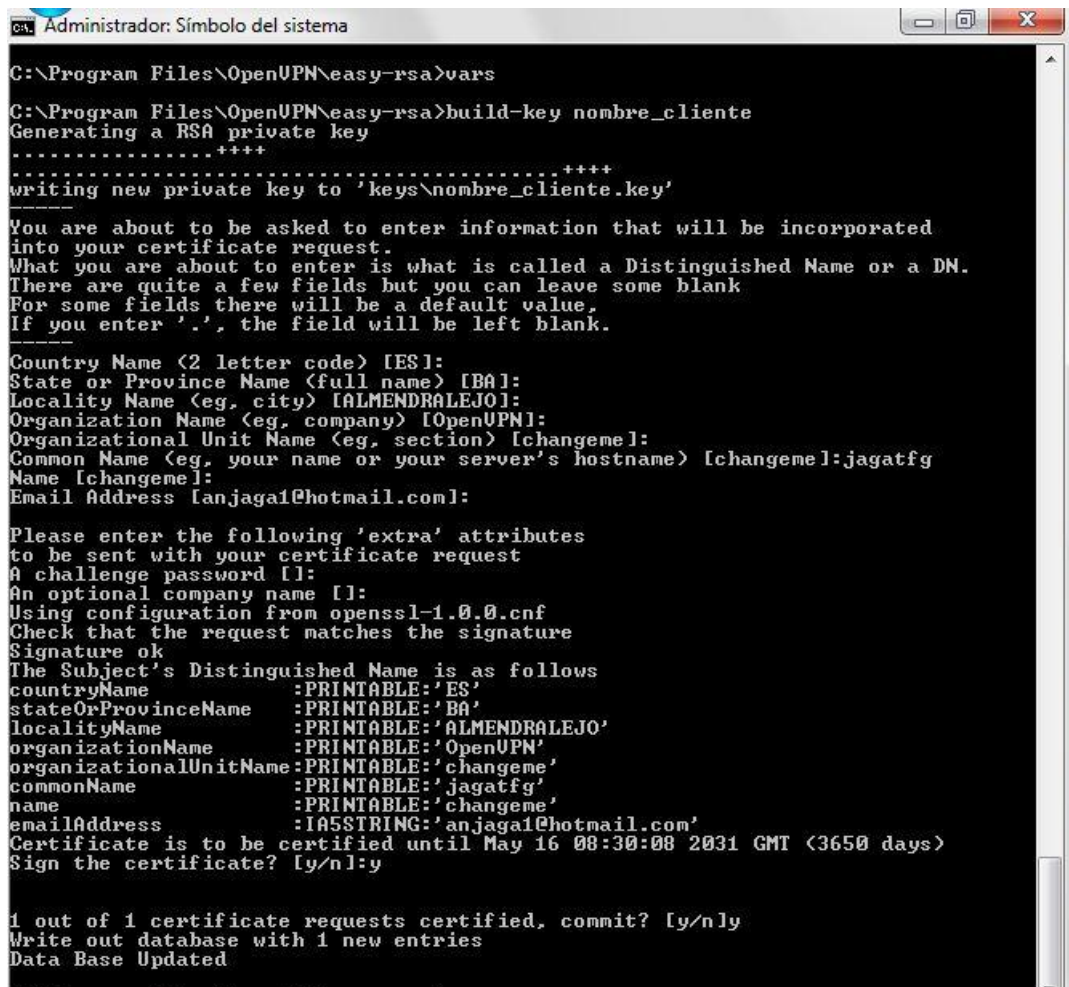
4.1.10. Configuración del cliente VPN

Una vez configurado, activado y puesto en funcionamiento el servidor, se pasará a la configuración del cliente para la conexión a la VPN del servidor. Este tipo de conexiones se puede realizar de varias maneras, tanto dentro de la red en la que se encuentra el servidor VPN, como fuera de la misma, en este apartado del capítulo, se hará un breve resumen de la configuración de las diferentes formas de conectar.

En primer lugar, se debe realizar la instalación del software OpenVPN al igual que en se realizó en el servidor, este punto es el mismo proceso, importante recordar a la hora de la instalación que es importante marcar la casilla “EasyRSA 2 Certificate Management Scripts”.

Una vez finalizada la configuración, pasaremos a la configuración de un equipo cliente de la red VPN asociado y conectado en la red local.

Los certificados y las claves correspondientes al cliente, como pega, deben generarse en el servidor. Para ello se debe dirigir de nuevo al terminal de comandos del servidor VPN de la red, en el que se ejecutara la línea de comandos “vars” y “build-key nombre-cliente” dentro del directorio easy-ras, al cual se accede mediante la siguiente ruta “C:\Program Files\OpenVPN\easy-rsa”. Una vez ejecutados dichos comandos, al igual que pasaba en el servidor, debemos continuar en el terminal con los valores predeterminados que se cambiaron en el fichero de configuración para la generación de certificados a la hora de configuración del servidor, teniendo en cuenta que en la línea “ Common Name” se debe seleccionar el nombre de usuario, en este proyecto para el ejemplo será “jagatfg” (Véase en la Figura 29) y terminar con la aceptación de la creación tanto de la clave como del certificado pulsando la tecla “y” .



```
C:\Program Files\OpenVPN\easy-rsa>vars
C:\Program Files\OpenVPN\easy-rsa>build-key nombre_cliente
Generating a RSA private key
.....++++
.....++++
writing new private key to 'keys\nombre_cliente.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ES]:
State or Province Name (full name) [BA]:
Locality Name (eg, city) [ALMENDRALEJO]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [changeme]:
Common Name (eg, your name or your server's hostname) [changeme]:jagatfg
Name [changeme]:
Email Address [an.jaga1@hotmail.com]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName             :PRINTABLE:'ES'
stateOrProvinceName     :PRINTABLE:'BA'
localityName            :PRINTABLE:'ALMENDRALEJO'
organizationName        :PRINTABLE:'OpenVPN'
organizationalUnitName  :PRINTABLE:'changeme'
commonName              :PRINTABLE:'jagatfg'
name                   :PRINTABLE:'changeme'
emailAddress            :IA5STRING:'an.jaga1@hotmail.com'
Certificate is to be certified until May 16 08:30:08 2031 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
Write out database with 1 new entries
Data Base Updated
```

Figura 29: Creación de la clave del cliente

Una vez creadas tanto la clave como el certificado, se debe de trasladar los ficheros de directorio, para ello, se trasladaran los ficheros al igual que en el servidor, a la carpeta de configuración (C:\Program Files\OpenVPN\config) quedando los siguientes ficheros dentro de dicho directorio (Véase la Figura 30)








 ca.crt	18/05/2021 0:22	Certificado de seg...	3 KB
 jagatfg.crt	18/05/2021 10:30	Certificado de seg...	9 KB
 jagatfg.key	18/05/2021 10:58	Archivo KEY	4 KB
 jagatfg.ovpn	20/05/2021 13:44	Archivo OVPN	4 KB
 nombre_cliente.csr	18/05/2021 10:30	Archivo CSR	2 KB
 README.txt	18/05/2021 10:26	Documento de te...	1 KB
 ta.key	18/05/2021 1:11	Archivo KEY	1 KB

Figura 30: Ficheros de configuración cliente VPN

Por último, se debe entrar a la configuración del fichero del usuario (jagatfg.ovpn) para verificar al servidor que apunta (Véase la Figura 31)

```
39 # The hostname/IP and port of the server.  
40 # You can have multiple remote entries  
41 # to load balance between the servers.  
42 remote 192.168.1.25 1194  
43 ;remote my-server2 1194  
44
```

Figura 31: Dirección IP servidor VPN.

Como se observa a continuación en la Figura 32, se puede configurar dicho equipo cliente para acceder a la red del servidor desde una red diferente a la que se encuentra esté conectado, y hacerlo mediante la red pública con la ip pública (8.11.99.46) de la red del servidor mediante el puerto 1194.

```
39 # The hostname/IP and port of the server.  
40 # You can have multiple remote entries  
41 # to load balance between the servers.  
42 ;remote 192.168.1.25 1194  
43 remote 88.11.99.46 1194  
44
```

Figura 32: Dirección IP publica router alojamiento servidor VPN

A pesar de la configuración del fichero de configuración, también se deben establecer las claves y los certificados en todos los equipos clientes de la red VPN, y estén fuera como dentro de la red en la que se encuentra nuestro servidor VPN, al igual que se hizo con el equipo cliente de la red VPN, al configurarlo para la red local (Véase de nuevo la Figura 30).

4.2. Servidor Proxy

Un servidor Proxy es un equipo en la red, cuya función es hacer de equipo intermediario entre el equipo del cliente y la red pública. Este tiene la función de redirigir y dar permiso a un equipo con salida a la red pública. Las peticiones realizadas del equipo cliente, pasan por el servidor proxy, este verifica que la ruta a la que se quiere acceder es una ruta permitida o no, y da acceso o no al equipo cliente a dicha ruta. En cambio, sin un servidor proxy, todas las peticiones del equipo cliente, siempre serían válidas, ya que se permitiría realizar la conexión directa, desde el equipo cliente al destino en la red pública.

Este se puede configurar para que el equipo cliente solo pueda acceder a ciertas url, en ciertas horas, además de que ciertos usuarios sean únicamente los que naveguen en la red.

4.2.1. Instalación

La instalación del software OpenSource FreeProxy es bastante sencilla, a pesar de ello, a continuación se muestra paso a paso la instalación del mismo:

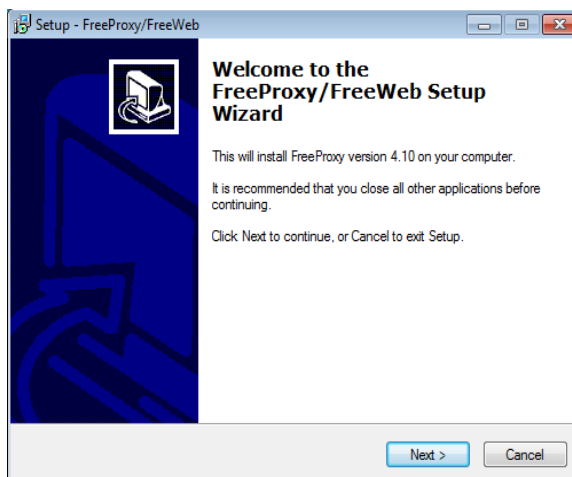


Figura 33: Inicio asistente de instalación

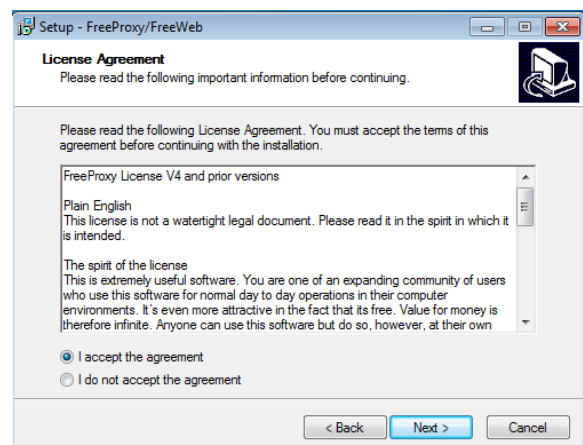


Figura 34: Aceptación de términos

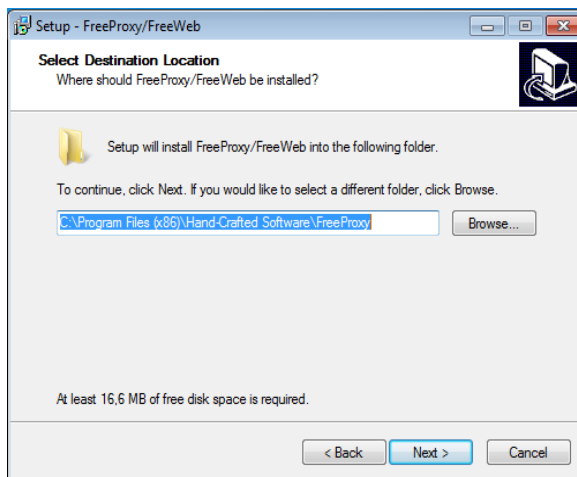


Figura 33: Selección ruta de instalación

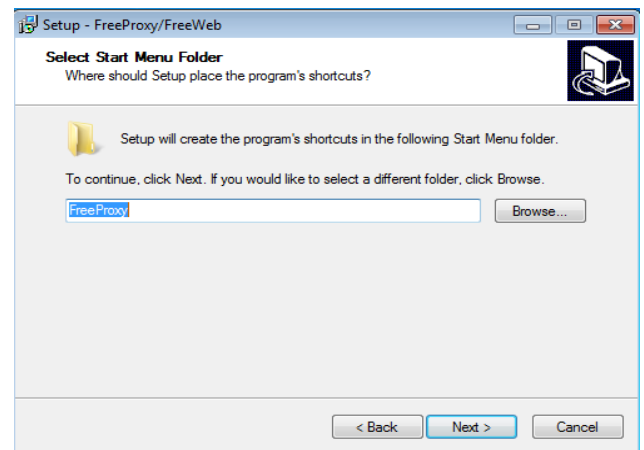


Figura 36: Nombre en carpeta programas Inicio

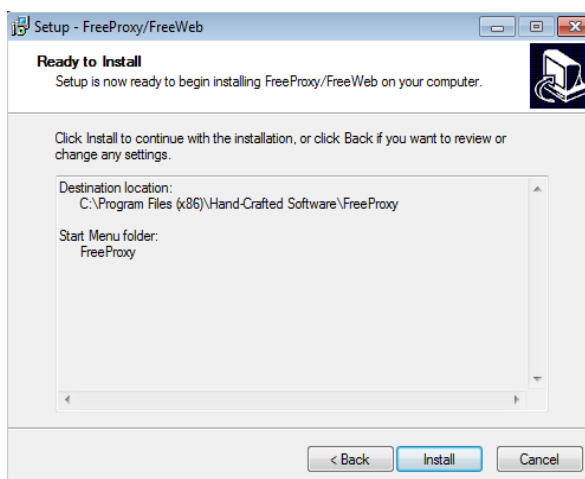


Figura 37: Resumen de Instalación

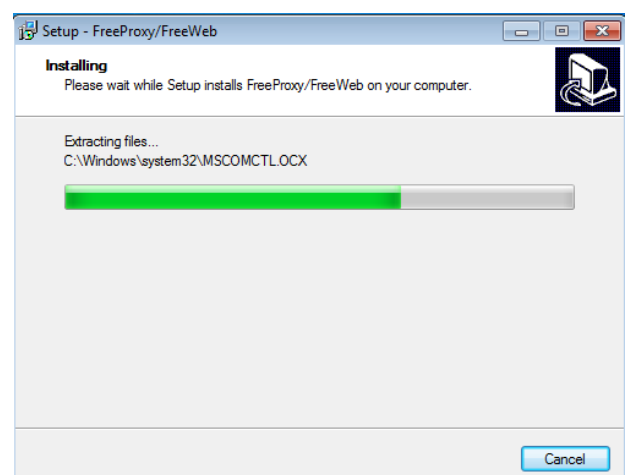


Figura 38: Progreso de la instalación

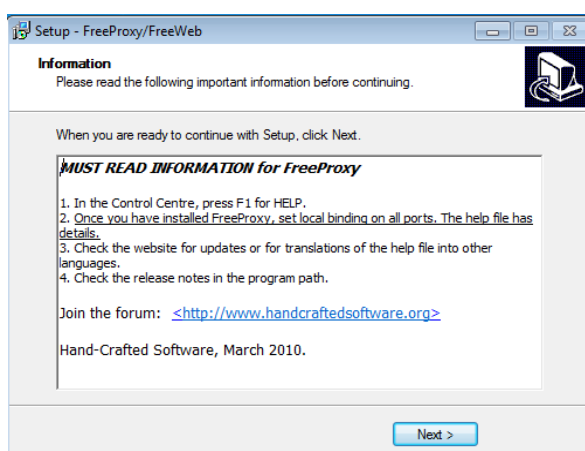


Figura 39: Información tras la instalación

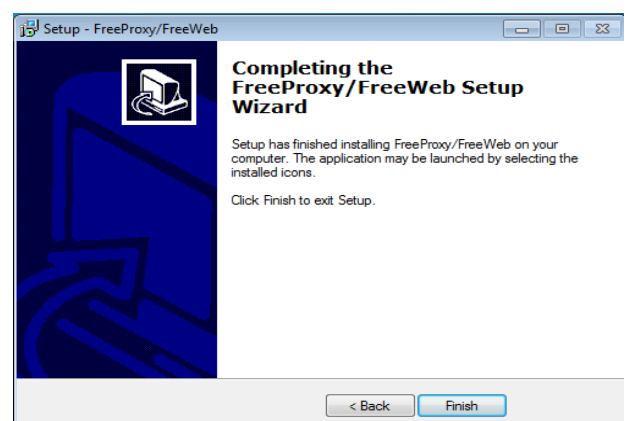


Figura 40: Finalización de la instalación de FreeProxy

4.2.2. Configuración

En este proyecto, el software que hará las funciones de servidor proxy, será un OpenSource llamada FreeProxy. Una vez descargado dicho software, el primer paso a llevar a cabo será la instalación del mismo en el equipo servidor de la red. Una vez instalado, se debe parar/deshabilitar el servicio de firewall de Windows para evitar conflictos con FreeProxy (Véase la Figura 41)

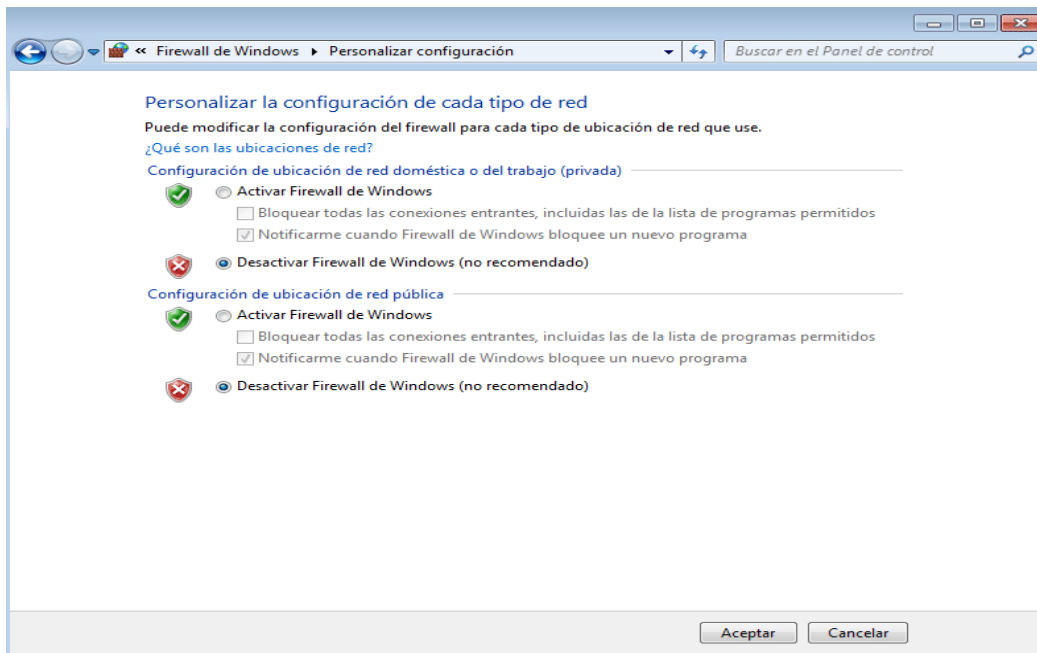


Figura 41: Desactivar Firewall de Windows

Una vez se encuentra parado/desactivado el firewall de Windows, se procede a acceder al panel de configuración del mismo. (Véase Figura 42)(en la figura 42 se muestra el panel de configuración de FreeProxy con un servidor proxy junto a sus usuarios ya configurados)

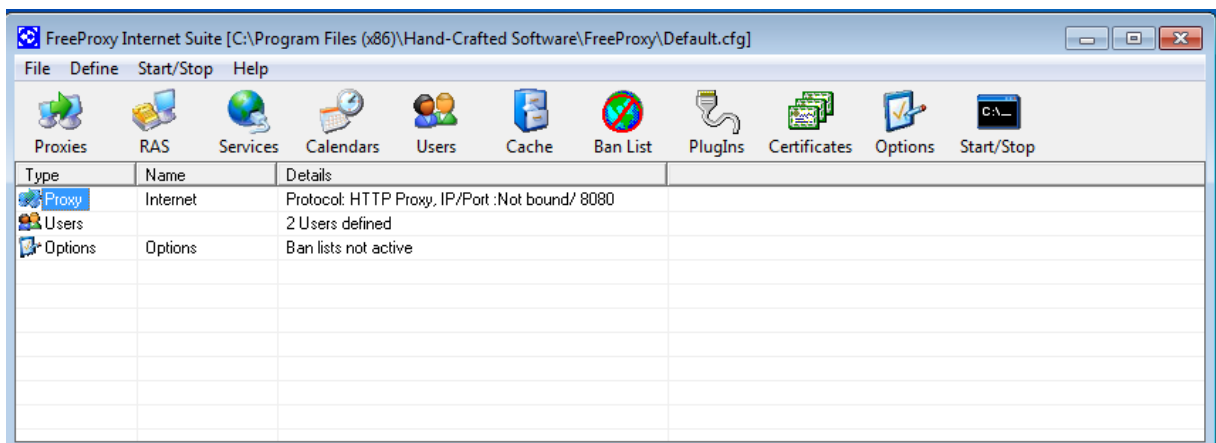


Figura 42: Panel de configuración FreeProxy

Una vez accedido a este panel de configuración, en primer lugar, debemos pinchar en el icono de proxis, abriéndose así el menú de creación del servicio proxy y a su vez su configuración. Para la configuración del servicio, se debe escribir y para este proyecto, la siguiente configuración: (Véase la Figura 43)

1. Nombre : JagaTFG
2. Puerto cliente: 8080
3. Enlace local: 192.168.1.25
4. Enlace remoto:192.168.1.25
5. Carpeta de log: C:\Proxy\logfile.log

Los demás apartados del menú se quedaran como vienen por defecto.

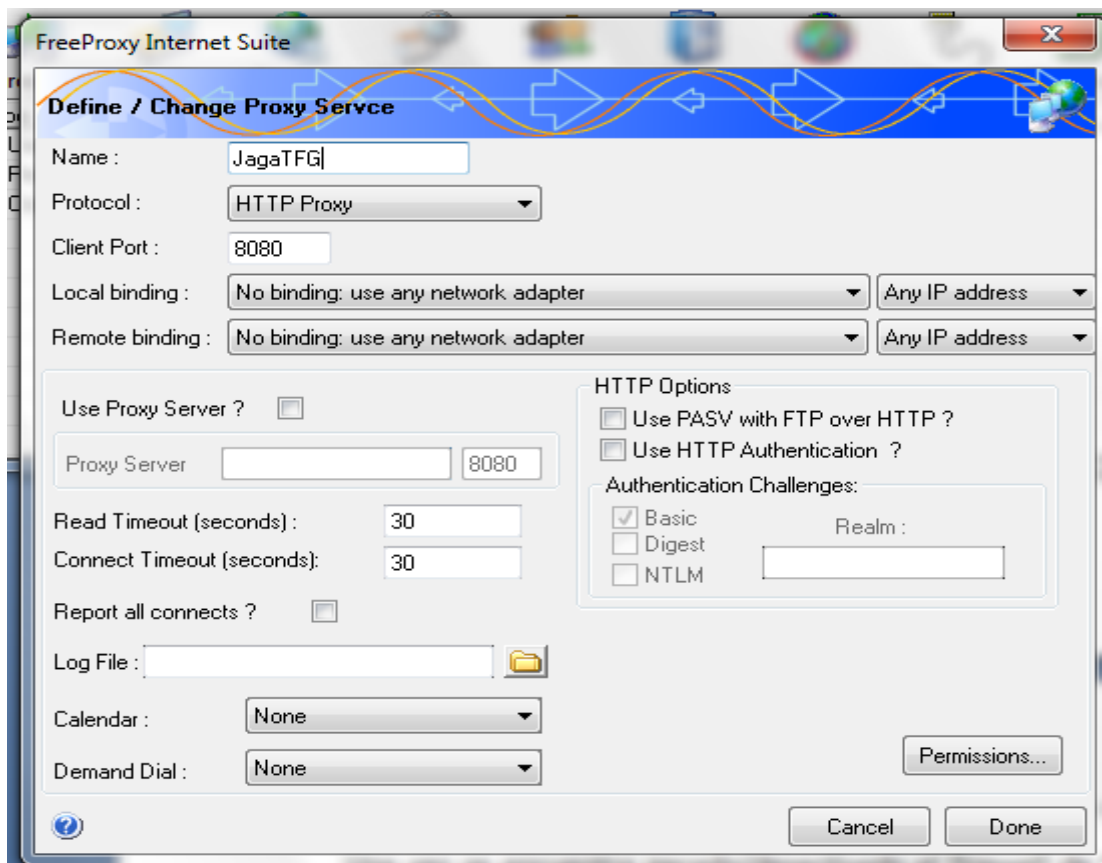


Figura 43: Creación Servicio proxy

Una vez establecidos los parámetros del servicio proxy, se pasará a la configuración de los permisos, en los que se podrá establecer una serie de permisos y parámetros, para todos los usuarios de la red, o para una serie de usuarios concretos (Véase la figura 44).

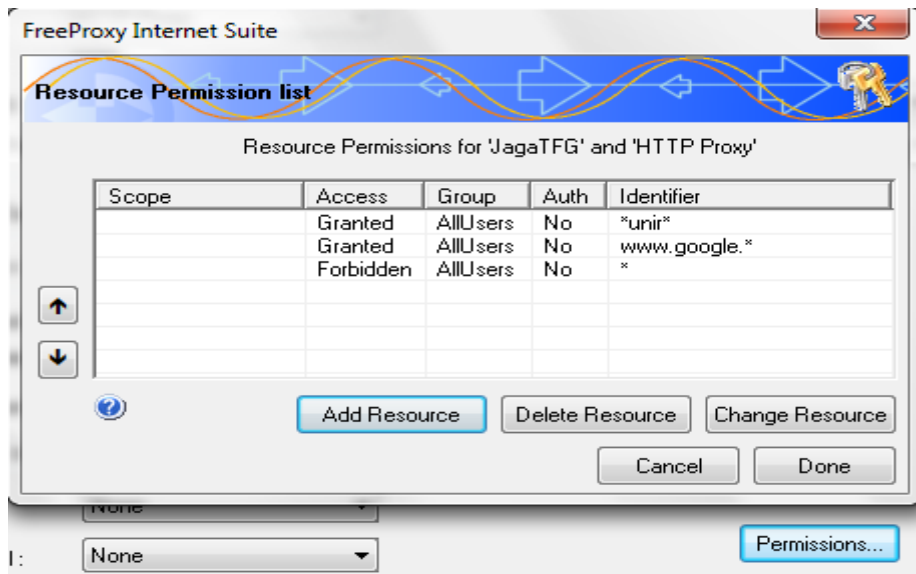


Figura 44: Restricciones establecidas

En la Figura anterior (Figura 44) se puede observar que se muestran una serie de líneas escritas, dichas líneas tienen un significado, cada una de ellas diferentes y cada una implanta una restricción diferente, a continuación son detalladas brevemente:

- ❖ Access
 - Granted --> Acceso permitido
 - Forbidden --> Acceso denegado
- ❖ Group
 - Allusers --> Permite a todos los usuarios
- ❖ Auth
 - NO --> No requiere autorización
- ❖ Identifier
 - *unir* --> Permite todas las conexiones las cuales tengan en su url la palabra unir
 - ww.google.* --> Permite todas las conexiones las cuales comiencen en su url por www.google.
 - * --> bloquea todas las urls (Recordar que esta regla se encuentra con acceso Forbidden)

Tras las configuraciones de reglas en el servidor Proxy, el menú principal de configuración quedaría de la siguiente manera, el cual muestra la configuración del mismo (Véase la Figura 45)

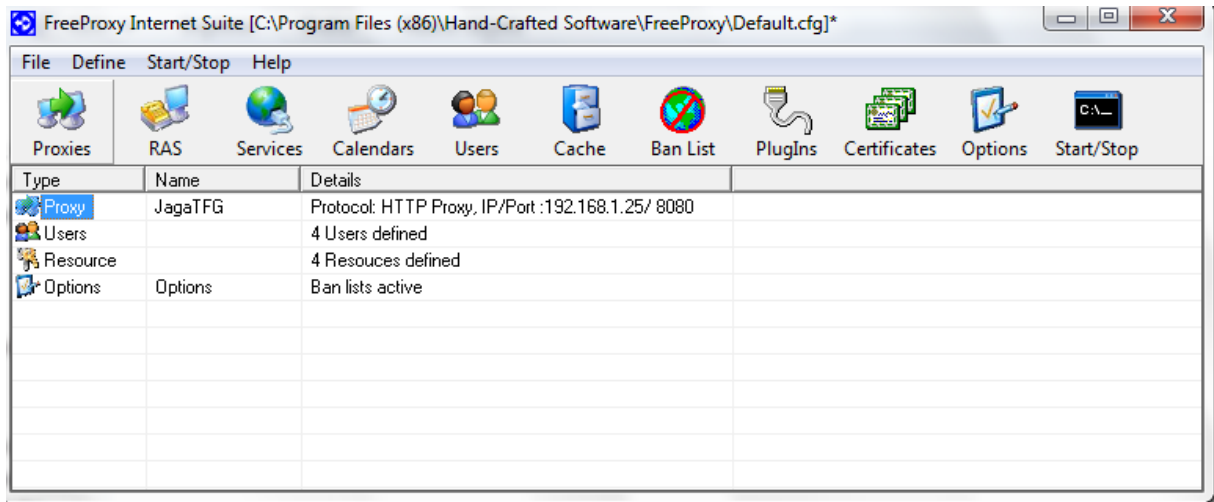


Figura 45: Panel de configuración servidor Proxy con configuración aplicada

Una vez finalizada la configuración en el panel de configuraciones de FreeProxy, el siguiente paso es la configuración del servidor Proxy en el/los navegadores de Internet, en el caso de este proyecto la configuración se llevará a cabo sobre el navegador Mozilla Firefox, pero antes de ello, se conectara el Servidor Proxy (Véase la Figura 46),se debe reiniciar servidor siempre que se encuentre conectado para que los cambios en la configuración surjan efecto sobre el servidor.

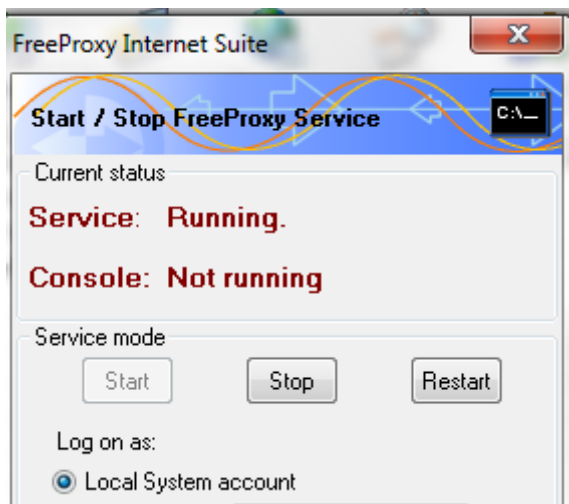


Figura 46: Inicio/Parada servidor Proxy

Una vez iniciado el servidor Proxy, se pasa a la configuración del servidor Proxy en el navegador (Véanse las figuras 47 y 48)

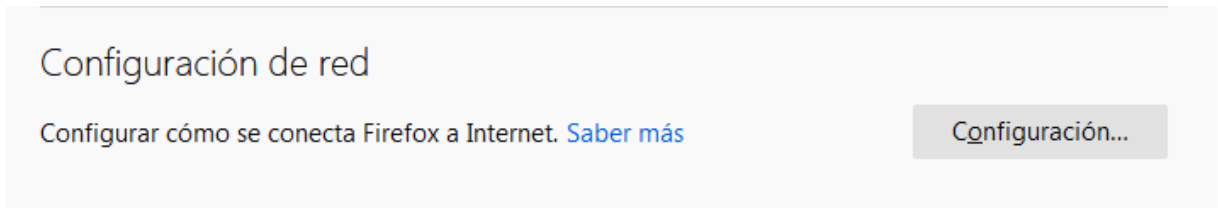


Figura 47: Pestaña de entrada en el navegador para configuración Proxy



Figura 48: Configuración Servidor Proxy en navegador Mozilla Firefox

4.2.3. Funcionamiento

Este software, funciona en modo LAN para ello deberemos abrir el puerto en el router 8080 y poder recibir conexiones remotas.

Una vez configurado y puesto en marcha el servidor Proxy, el siguiente y último paso es comprobar el correcto funcionamiento. En una primera prueba se intenta conectar con el portal [campus virtual de UNIR](https://crosscutting.unir.es) con el servidor proxy activado, y se comprueba que la conexión es correcta, ya que en el servidor Proxy está establecida la regla que permite cualquier url que contenga la palabra UNIR (Véase la Figura 49)

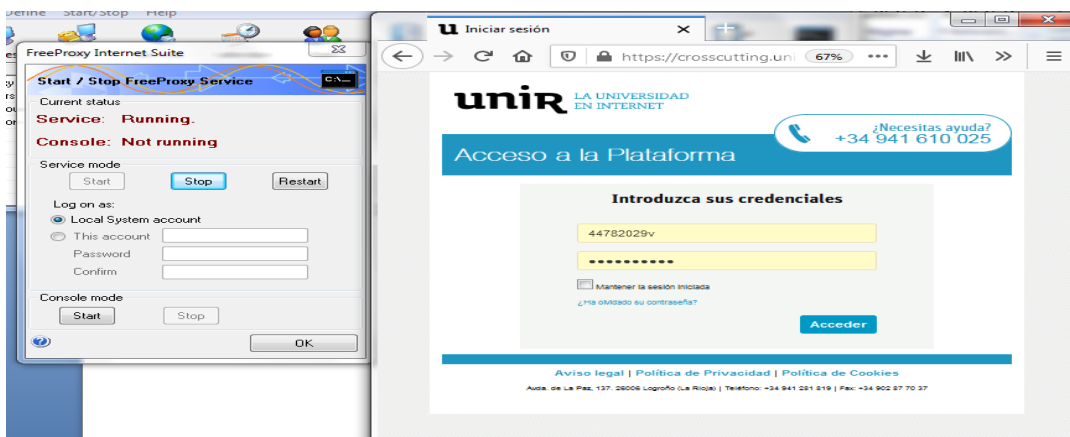


Figura 49: Conexión UNIR servidor Proxy Corriendo y configurado en navegador

En cambio, mientras que el navegador sigue con el servidor Proxy activo ,el servidor Proxy se encuentra parado, por lo que no se consigue acceder al portal web del campus virtual de UNIR (Véase la figura 50) y el navegador nos devuelve el mensaje El servidor proxy está rechazando las conexiones.

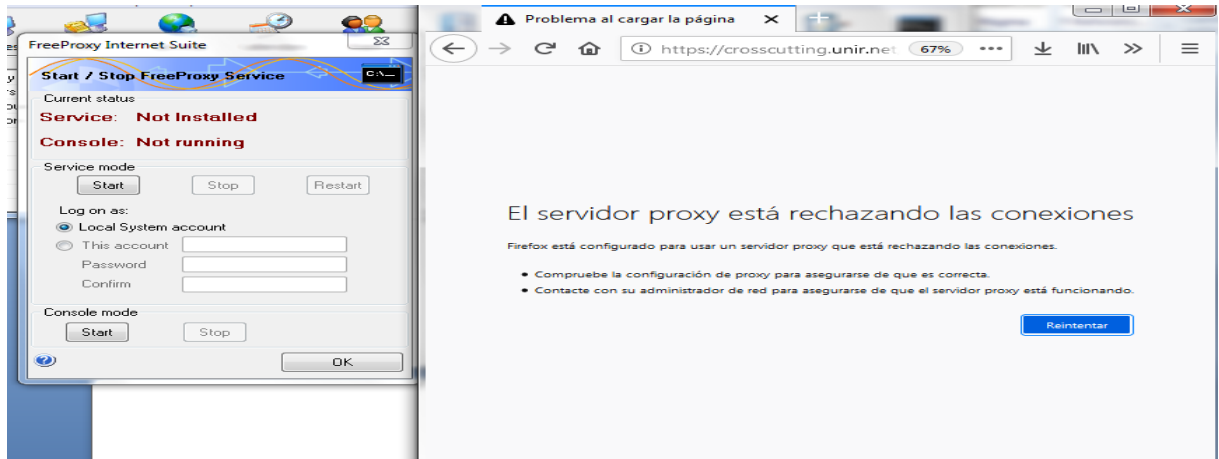


Figura 50: Conexión rechazado por el navegador y el servidor Proxy

Conforme a las reglas establecidas anteriormente en el servidor proxy, quedaría probar las dos restantes, ahora, será el momento de probar una de las dos reglas restantes. Será el caso de la siguiente regla. Para ello se hará la prueba de conectar a Google, buscar mediante el buscador de Google el diario [marca](https://www.marca.com) (Véase la figura 51)

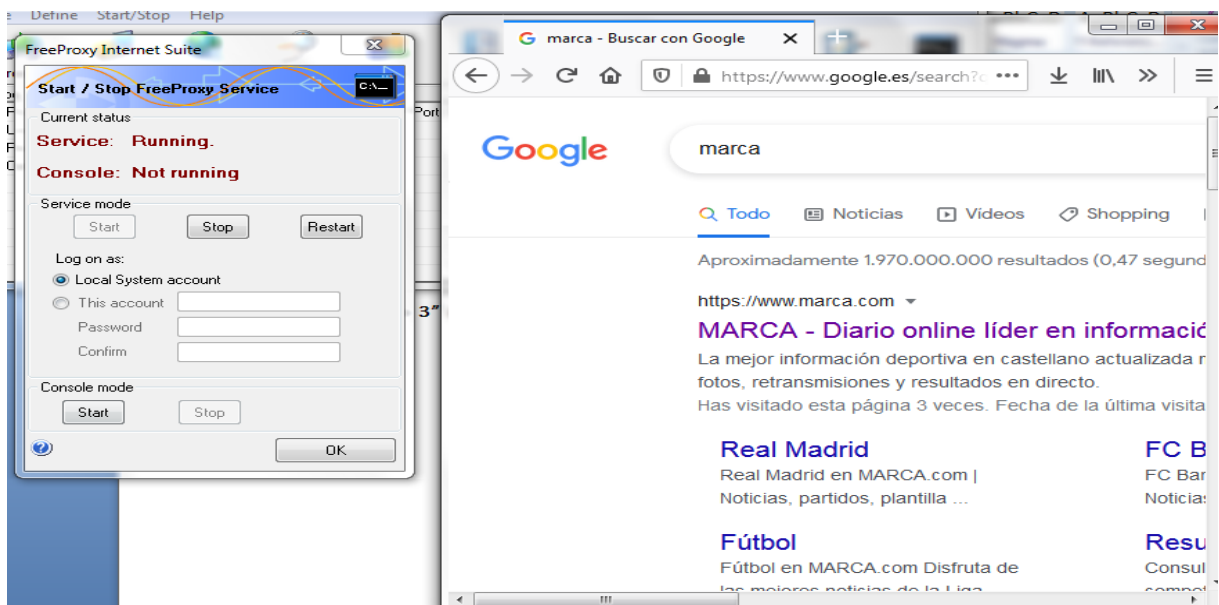


Figura 51: Búsqueda de URL denegada mediante Google

Como se observa en la figura anterior (Figura 51), a través del buscado de Google, el cual tiene permitido todo lo que comience con [www.google](http://www.google.com). si que se llega a la url, en cambio, en el momento en el que se pincha sobre [marca](http://marca.com) en este caso, siendo una url denegada por el servidor Proxy, este rechazara la conexión, y no permitirá acceder al portal de [marca](http://marca.com) (Véase la Figura 52)

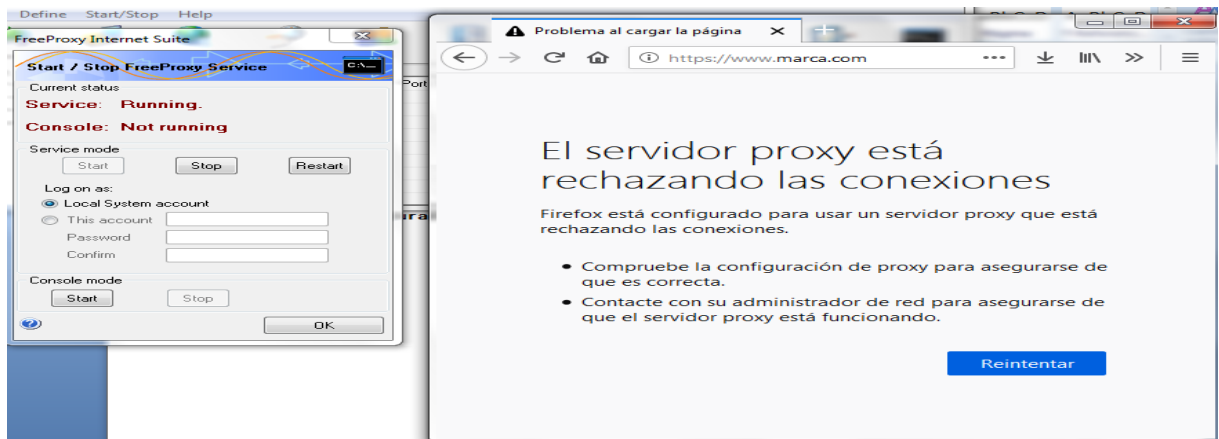


Figura 52: Acceso denegado por servidor Proxy en búsqueda mediante Google

Para finalizar con las pruebas del correcto funcionamiento del servidor Proxy, se realizara una conexión a cualquier portal web, en ese caso a una inmobiliaria, portal al cual no se debería acceder ya que el servidor Proxy contiene una regla establecida la cual prohíbe todas las conexiones web (Véase Figura 53)

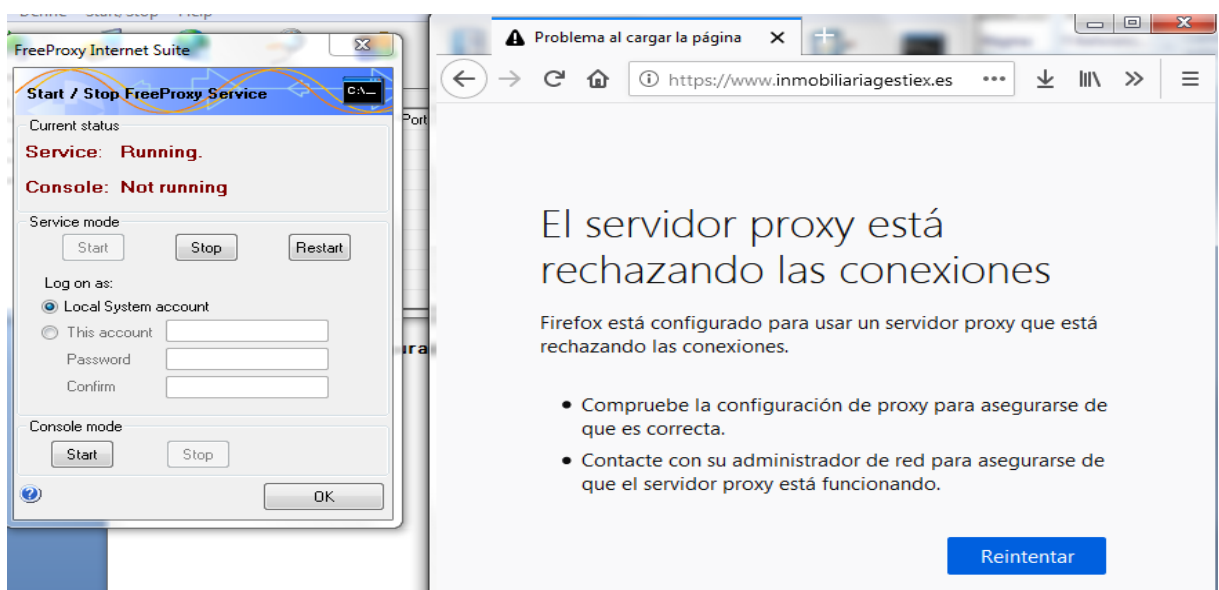


Figura 53: Acceso a un portal de una Inmobiliaria con regla de prohibición en Proxy

4.3. Servidor Firewall

Un servidor Firewall es un equipo configurado y conectado a la red, cuya función es la de gestionar la totalidad del tráfico en dicha red.

Este servidor puede ser tanto físico como virtual, en el son configuradas una serie de reglas, la cual permitir o limitan el tráfico en la red, tanto en la misma red como en las conexiones entrantes o salientes.

Así mismo, se podría considerar que un servidor Firewall bien configurado en la red, será el encargado de filtrar las entradas no deseadas a la red, como las salidas desde cualquier equipo a la red pública que no sean deseadas.

Los servidores Firewall se pueden establecer de forma física o de forma virtual, en este proyecto se llevará a cabo de forma virtual con el software ZoneAlarm.

4.3.1. Instalación

Para la correcta instalación del software de ZoneAlarm, se debe ejecutar con permisos de administrador el archivo de instalación.

Una vez iniciada la instalación, el software pedirá la aceptación de sus términos para continuar con dicha instalación (Véase la Figura 54)



Figura 54: Aceptación de términos ZoneAlarm

Seguidamente, comenzara el proceso de instalación, el cual habrá que esperar a que termine sus procesos (mostrados en la barra de progreso)(Véase la figura 55)



Figura 55: Progresos de Instalación

Una vez finalizada la instalación, el propio software pedirá un correo para la recepción de actualizaciones y mejoras de ZoneAlarm (Véase la Figura 56)



Figura 56: Registro correo para recibir actualización y mejoras de ZoneAlarm

Una vez realizados correctamente los pasos anteriores, ya estaría instalado en el equipo servidor de la red, el software de Firewall.

4.3.2. Configuración

En primer lugar para la configuración del firewall en la red se debe pulsar sobre el botón ver detalles (Véase la Figura 57) encapsulado en la pestaña Firewall del menú de configuración de ZoneAlarm



Figura 57: Menú de configuración Firewall

Una vez pulsado el botón ver detalles señalado en la anterior figura (Figura 57) el siguiente paso será el de acceder a la pestaña de configuración de dicho Firewall (Véase la figura 58)



Figura 58: Entrada Configuración Firewall

Seguidamente, dentro de dicha pestaña de configuración, el siguiente paso será establecer el nivel de seguridad que se quiere ofrecer, en el caso de este proyecto, se establecerá el nivel de seguridad medio, ya que en el equipo servidor en el que se instala Firewall necesita obtener conexiones entre otros equipos de la red para compartir las impresoras, carpetas compartidas en las que los usuarios de la red alojaran sus documentos, etc. (Véase la Figura 59 señalados en un círculo de color azul)

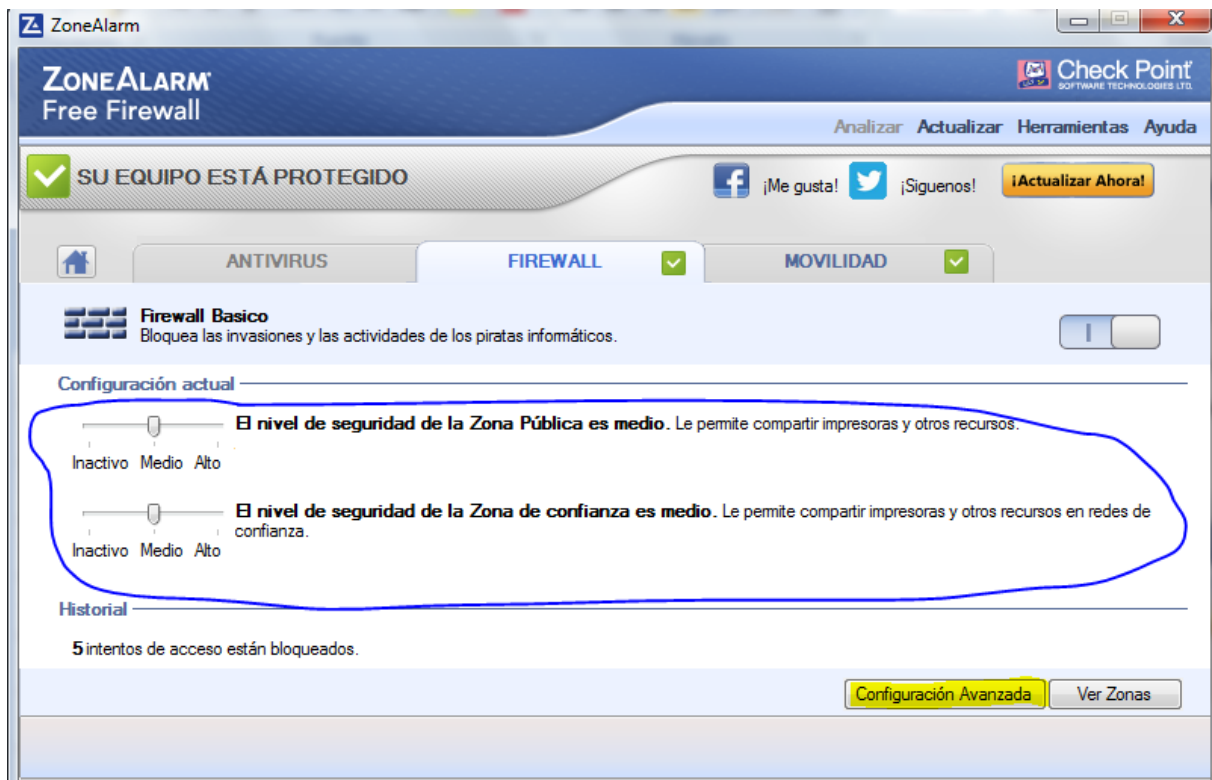


Figura 59: Nivel de seguridad

A continuación se pulsa sobre el botón Configuración Avanzada (Señalado en la Figura 59 de color amarillo), en esta pestaña se establecerán las reglas sobre los programas que funcionara y actuara el Firewall (Véase la Figura 60)

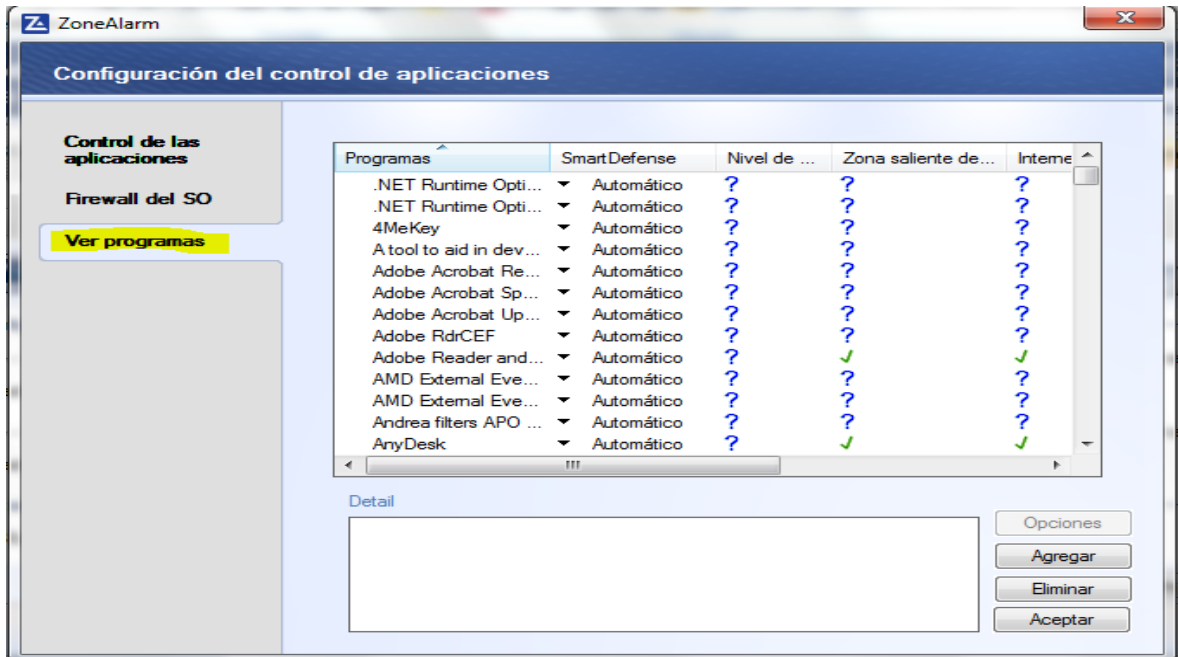


Figura 60: Programas configurados en Firewall

Como se puede observar en la Figura anterior (Figura 60), en el menú de configuración de Firewall se establecen los diferentes programas que pueden ejecutarse con permiso de firewall, este permite la ejecución o el bloqueo de los programas instalados o que quieran ejecutar en el equipo.

El siguiente paso a realizar, es la configuración de los sitios de confianza de movilidad, para ello se debe pulsar el botón que indica sitios de confianza (Véase la Figura 61)

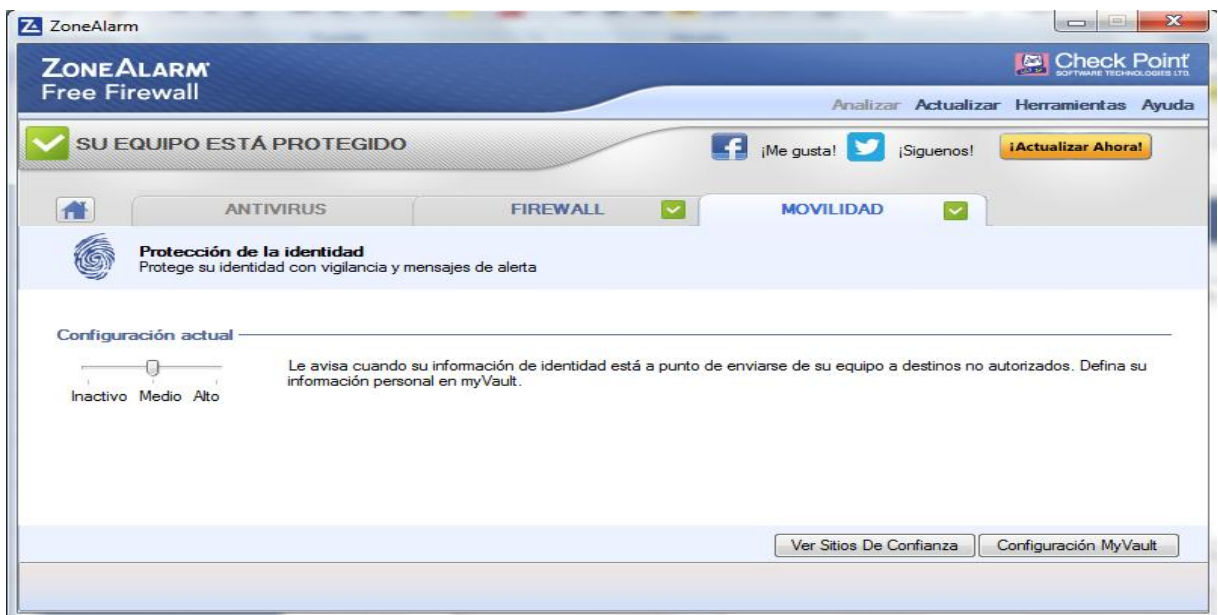


Figura 61: Pantalla de movilidad

Al pulsar el botón de sitios de confianza, se abrirá la ventana correspondiente a la figura 62, en la que se debe de agregar una a una las URL de confianza que se quieren agregar al Firewall, en el caso de este proyecto la URL de prueba es www.milanuncios.com

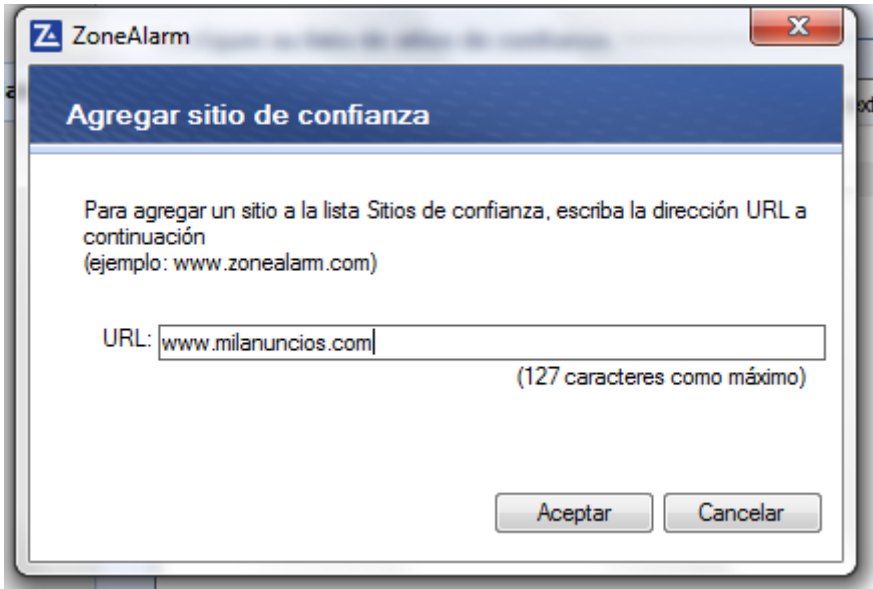


Figura 62: Agregar sitios de confianza Firewall

Una vez agregado los sitios de confianza, estos aparecerán en la venta de sitios de confianza, con la excepción de no saber el firewall como catalogarlos, para ello, debe ser el usuario quien los configure, así permitiendo (en el caso de este proyecto con www.milanuncios.com) o denegando el acceso a dichas URL (Véase la figura 63)

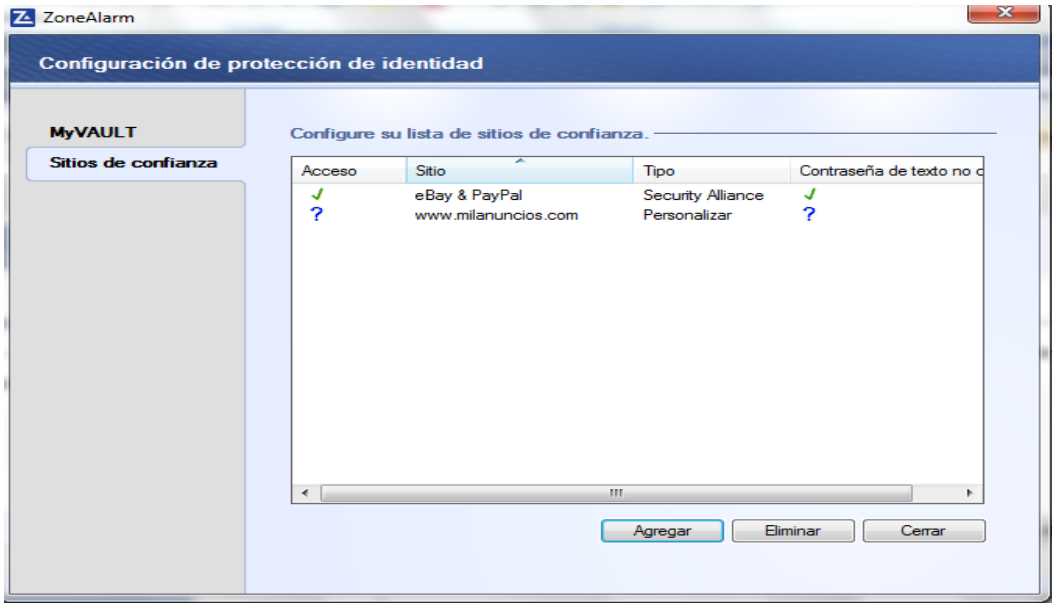


Figura 63: Permitir o denegar url en sitios de confianza

Para ello, es tan sencillo como pulsar con el ratón encima de la interrogación azul predeterminada por la configuración del Firewall y permitir o denegar el acceso a dicha url configurada (Véase la figura 64, en ella se muestra como permitir los accesos)

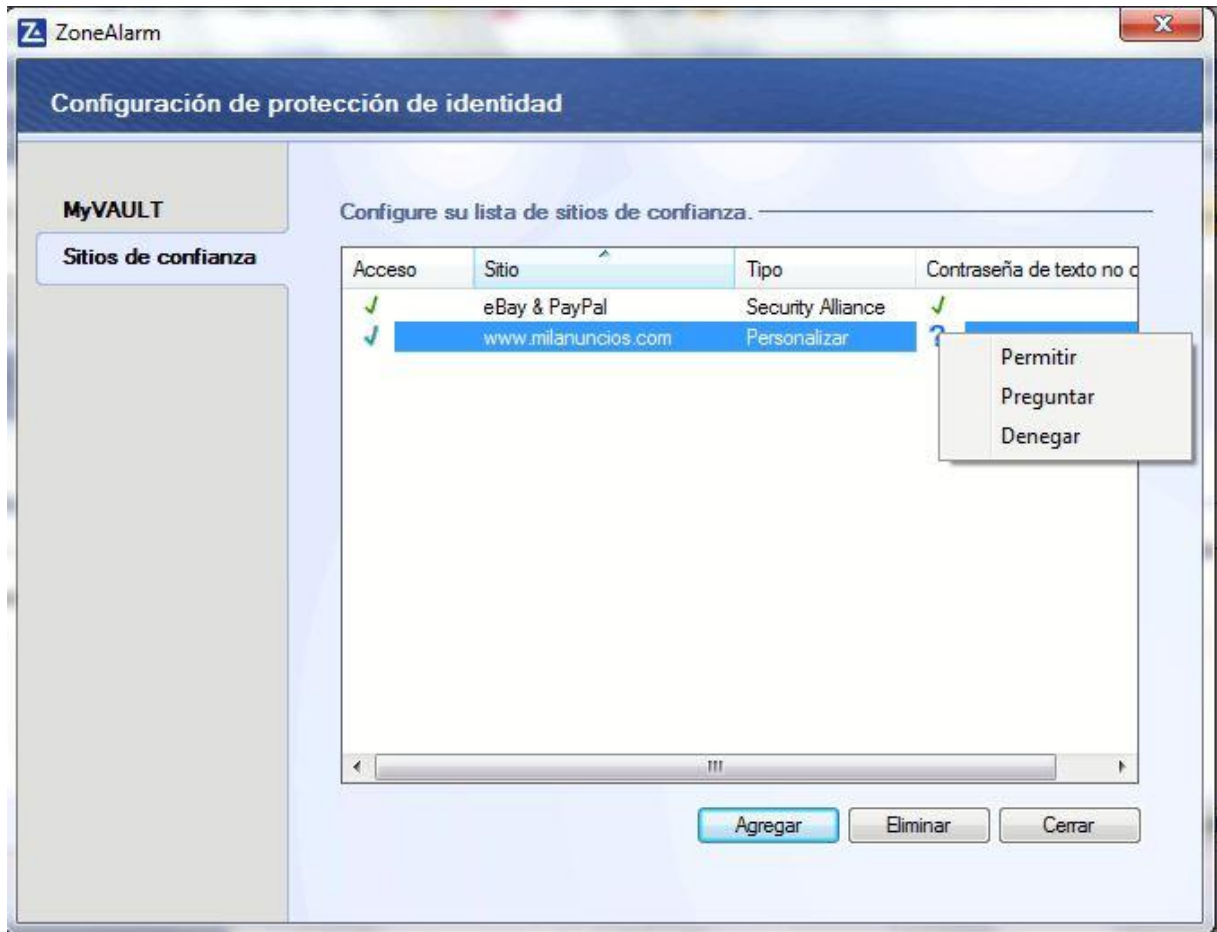


Figura 64: Permisos de acceso en sitios de confianza Firewall

4.3.3. Funcionamiento

Una vez realizadas las operaciones correspondientes a la configuración y los permisos o denegaciones de los programas o URL en firewall, se procede a la ejecución de un programa el cual no está registrado en Firewall. Dando doble click de ratón para la ejecución de un programa (en el caso de este proyecto se probará con el software de control remoto TeamViewer), se puede observar que dicho programa no es ejecutado, mostrando el Firewall una notificación en la que se pide permiso para la ejecución de dicho software (Véase la Figura 65).



Figura 65: Permisos nuevo software

En la figura anterior (Figura 65) se observa que el propio Firewall lanza una ventana en la que se pueden pulsar dos botones, permitir, que será la opción que añada como excepción al firewall el programa en cuestión (en el caso de este proyecto, como anteriormente se nombraba, TeamViewer) y otro botón en el que se da la opción de denegar, en el caso de pulsar el botón denegar, el Firewall agregará como programa de no confianza a TeamViewer, para no dejarlo ejecutarse en el equipo en ningún momento.

Como la opción era la de Permitir para la ejecución de pruebas de este proyecto, al ser pulsado dicho botón, automáticamente se abrirá el programa TeamViewer (Véase en la Figura 66)

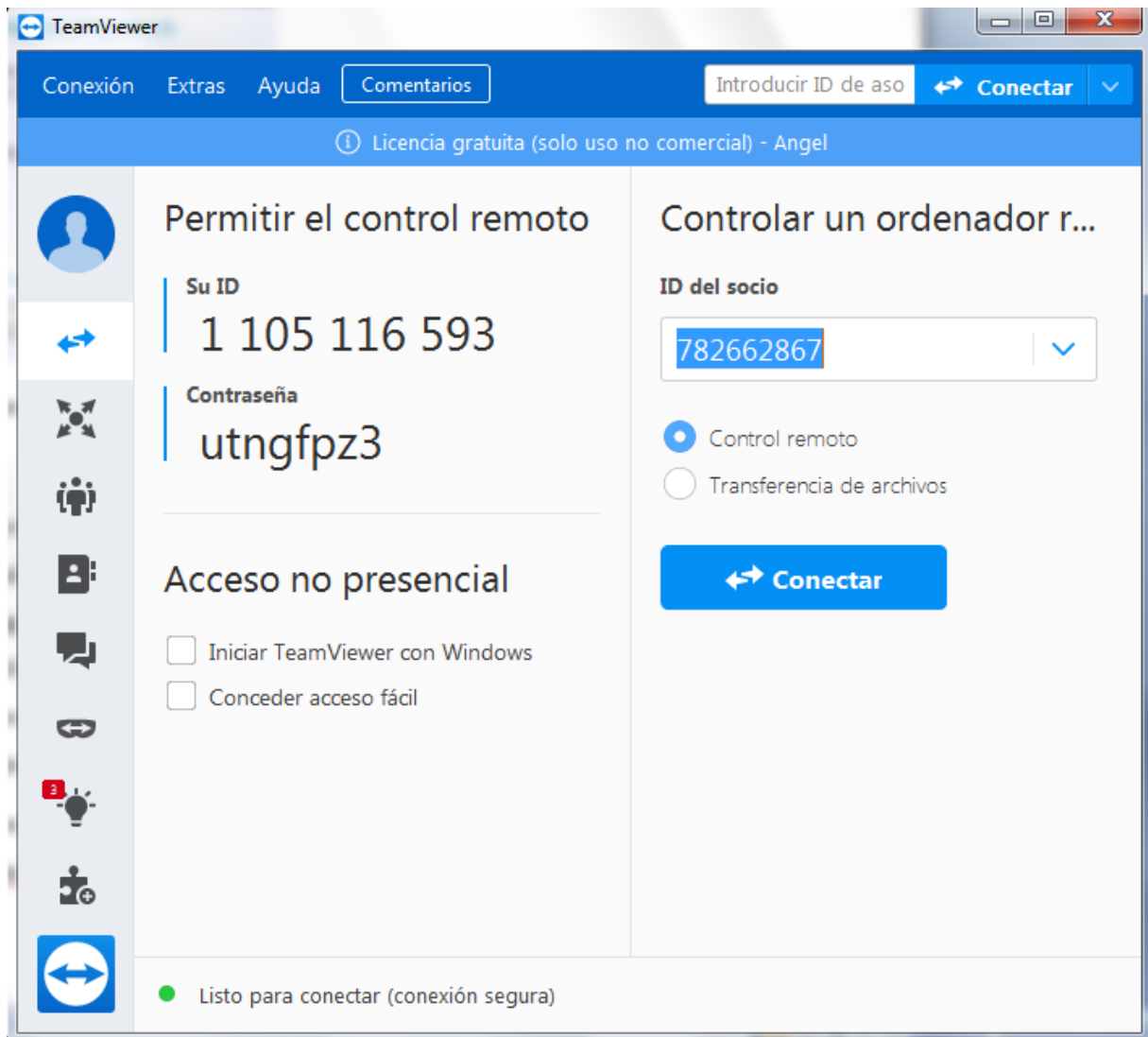


Figura 63: Programa TeamViewer en ejecución

Para finalizar, se puede acceder al Firewall y observar que programas son los que tienen permisos de ejecución y a los que se les ha otorgado dicho permiso, en este proyecto, como bien se viene hablando a lo largo de este apartado del capítulo, se observa que TeamViewer tiene nivel de confianza completa (Véanse las marcas amarillas de la Figura 67)

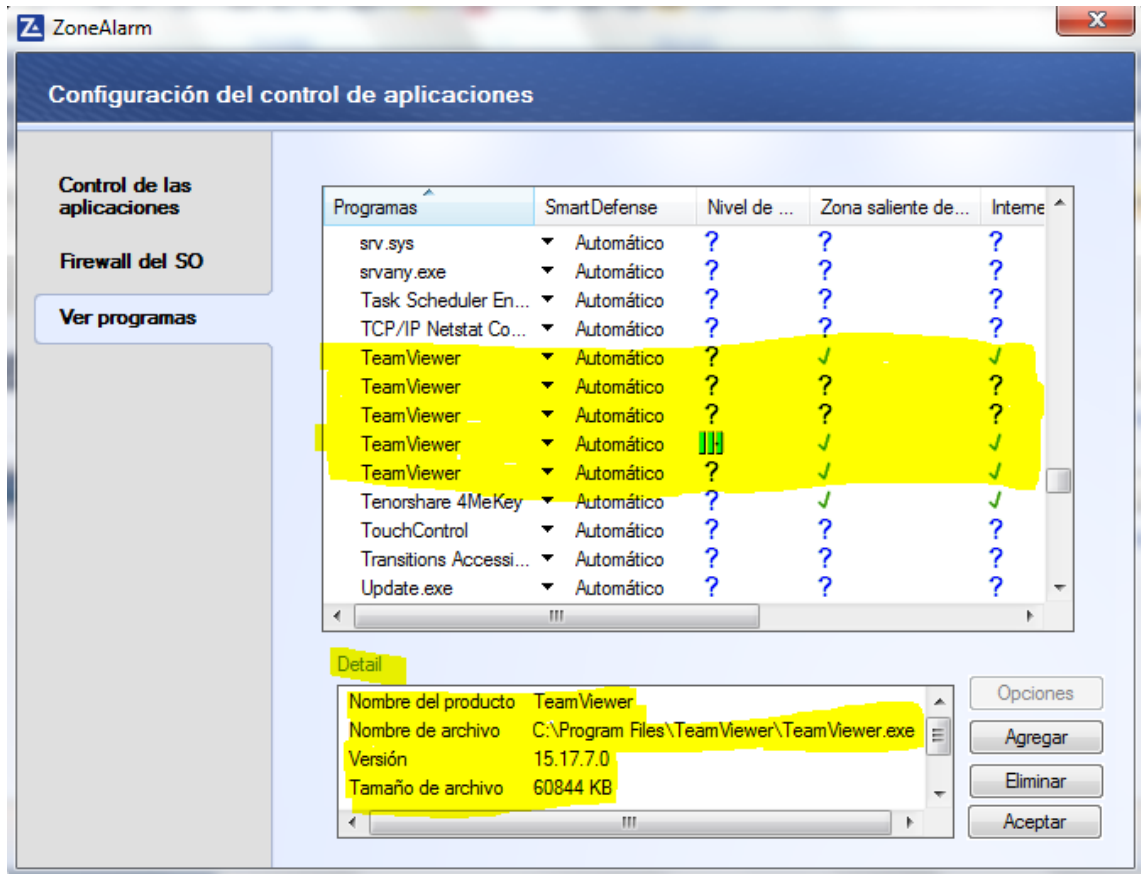


Figura 67: TeamViewer en el panel de control de aplicaciones

5. Conclusiones

Las conclusiones obtenidas con la elaboración de este proyecto, se obtienen a partir de los siguientes puntos de estudio y redacción:

5.1. Verificación:

Se verificaron posibles ataques y soluciones propuestas a lo largo del desarrollo de este proyecto para usuarios novatos y experimentados en el ámbito de la seguridad informática, estableciendo una serie de normas, reglas y puestas en marcha de algunas soluciones informáticas para la correcta navegación y el correcto tráfico de datos en una red utilizada para el teletrabajo con datos sensibles de diversos perfiles tanto de trabajadores como de clientes.

5.2. Investigación:

Se investigó sobre las distintas modalidades de seguridad de red para las conexiones remotas en las que el equipo cliente es gestionado en tráfico de red, por un servidor firewall, a la vez que es supervisado en la navegación de diferentes url en las que se encuentra limitado por un servidor proxy previamente establecido y configurado y finalmente todos ellos funcionando a la par y de la mano con la conexión segura que ofrece el túnel VPN en el que se navega por una red de modo incognito.

5.3. Desarrollo:

Se desarrolló el correcto funcionamiento de las medidas de seguridad, nombradas, explicadas y puestas en funcionamiento a lo largo de todo este proyecto. Para poder llevar a cabo una conexión segura en la que los paquetes de datos que se aseguran su correcta y segura navegación mediante la red desde un equipo origen, hasta un equipo destino

6. Trabajo futuro

Este proyecto esta ideado y diseño, con el propósito de ser utilizado en un conexión externa a la del puesto de trabajo habitual, así, siendo segura la conexión con dicho puesto de trabajo. El objetivo del proyecto esta conseguido, ya que SeguriTFG ofrece una conexión vpn, además de contar con un servidor proxy y un firewall, encargados de limitar tanto el trafico de la red como las conexiones a algunas url consideradas maliciosas.

No obstante, SeguriTFG, no es una aplicación finalizada y cerrada, está expuesta a futuras ampliación de servicios y mejoras de la misma, las cuales son enumeradas a continuación:

1. Inserción de servicio antivirus.
2. Inserción de Sniffer de red.
3. Adaptación a diferentes sistemas operativos.

A pesar de las modificaciones, estas antes de pasar a producción, deben pasar por el proceso de preproducción, en donde se realiza una batería de pruebas, para la futura en marcha correcta de SeguriTFG y futuras versiones

Referencias bibliográficas

1. (Limari Ramirez, 2004) Recuperado a partir de [https://d1wqtxts1xzle7.cloudfront.net/43995208/bmfci1732p_1.pdf?1458663105=&response-content-disposition=inline%3B+filename%3DProtocolos de Seguridad para Redes Priva.pdf&Expires=1615892590&Signature=CgAkDHUwlb4GS-R3xFRvxUprhW1BaJ2XQiew2Tzgg7B0ArsmwvJm7fAs9sz5r~jI4s5EppdaXeiWDYM49-~bFQaUUc4APJFhi91RFA2afAMAS6vmrShqlqsWXCPvwxvBd4I8ym6ATkxavhYiE-gygxIhDQJgQnxQL4gITzfZfgimByLzuvqvLxteYESvQnIPmhyJP7hG-dRmWzUw0-bLDtEfQXN7FTzIZTj4bA-m9oeKZh-xTkLMAwmSchinlv8UhU5uVD9q6lCoEaP5eaDjYJzbHlass0b9uIVJOMnaAEsGfoLzXVFA DC0WdwxPWm5xiAzF-YUnLE7xDzIP4N5ig_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA](https://d1wqtxts1xzle7.cloudfront.net/43995208/bmfci1732p_1.pdf?1458663105=&response-content-disposition=inline%3B+filename%3DProtocolos+de+Seguridad+para+Redes+Priva.pdf&Expires=1615892590&Signature=CgAkDHUwlb4GS-R3xFRvxUprhW1BaJ2XQiew2Tzgg7B0ArsmwvJm7fAs9sz5r~jI4s5EppdaXeiWDYM49-~bFQaUUc4APJFhi91RFA2afAMAS6vmrShqlqsWXCPvwxvBd4I8ym6ATkxavhYiE-gygxIhDQJgQnxQL4gITzfZfgimByLzuvqvLxteYESvQnIPmhyJP7hG-dRmWzUw0-bLDtEfQXN7FTzIZTj4bA-m9oeKZh-xTkLMAwmSchinlv8UhU5uVD9q6lCoEaP5eaDjYJzbHlass0b9uIVJOMnaAEsGfoLzXVFA DC0WdwxPWm5xiAzF-YUnLE7xDzIP4N5ig_&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA)
2. Castillo, A. N. (2019, 4 octubre). *Seguridad en las VPN'S*. Ardila Castillo.
<http://repository.unipiloto.edu.co/handle/20.500.12277/6435>
3. (Marín Valencia, Patiño Valencia, & Acevedo Bedoya, 2020) Recuperado a partir de <http://revistas.uco.edu.co/index.php/uco/article/view/284>
4. (Valencia) Recuperado a partir de https://riunet.upv.es/bitstream/handle/10251/75628/Servidor%20AccesoRemoto Windows%202012%20r2_v2.pdf?sequence=1
5. (Fondo Ferreiro, 2016) Recuperado a partir de http://castor.det.uvigo.es:8080/xmlui/bitstream/handle/123456789/52/TFG_PabloFondo.pdf?sequence=1
6. (Rodríguez Espinosa, Expósito González, Saiz Cabrera, & Rodríguez González, 2020) Recuperado a partir de <http://www.informaticahabana.cu/sites/default/files/ponencia-2020/SLD049.pdf>

7. Gómez Montoya, C., Sepúlveda Rodríguez, L., & Candela Uribe, C. (2012). Servidor proxy caché: comprensión y asimilación tecnológica. INGE CUC, 8(1), 149-162. Recuperado a partir de <https://revistascientificas.cuc.edu.co/ingecuc/article/view/228>
8. (Gomez, Sepúlveda, & Candela, 2012) Recuperado a partir de <http://repositorio.cuc.edu.co/bitstream/handle/11323/2661/Servidor%20proxy%20cach%c3%a9%20comprensi%c3%b3n%20y%20asimilaci%c3%b3n%20tecnol%c3%b3gica.pdf?sequence=1&isAllowed=y>
9. Mocan, T. (2019, 30 agosto). *¿Qué Es IPSec y Cómo Funciona?* CactusVPN. <https://www.cactusvpn.com/es/la-guia-para-principiantes-de-vpn/que-es-ipsec>
10. Jiménez, J. (2020, 1 noviembre). *Protege la seguridad en tu hogar con estos consejos.* RedesZone. <https://www.redeszone.net/tutoriales/seguridad/consejos-seguridad-informatica-hogar/>
11. Luz, S. (2021, 27 abril). *Mejores prácticas para configurar cualquier firewall en cualquier sistema.* RedesZone. <https://www.redeszone.net/tutoriales/seguridad/configurar-firewall-mejores-practicas/>
12. Gestor, C. (2021). *VPN - definición y características.* Ciset. Centro de Innovación. <https://www.ciset.es/glosario/494-vpn>
13. Quero, J. (2020, 8 junio). *Qué es una conexión VPN y para qué sirve.* Jessica Quero. <https://jessicaquero.com/que-es-una-conexion-vpn/>
14. L. (2020, 1 octubre). *Principales protocolos de comunicación VPN.* OSTEC | Segurança digital de resultados. <https://ostec.blog/es/acceso-remoto/protocolos-comunicacion-vpn/>
15. *¿Qué es VNC y para qué sirve? [Mayo 2021].* (2021, mayo). GEEKNETIC. <https://www.geeknetic.es/VNC/que-es-y-para-que-sirve>

16. Gomez, C. E. G. (2012, 1 agosto). *Vista de Servidor proxy caché: comprensión y asimilación tecnológica.* Revista INGE CUC.
<https://revistascientificas.cuc.edu.co/ingecuc/article/view/228/216>
17. Baquía, R. (2016, 30 marzo). *La seguridad informática, al alcance de los usuarios domésticos.* BAQUIA.
<https://www.baquia.com/emprendedores/2011-05-23-la-seguridad-informatica-al-alcance-de-los-usuarios-domesticos>
18. *¿Qué es un Proxy y para qué sirve? - Conocimiento - Certerus.com.* (2020). *¿Qué Es Un Proxy y Para Qué Sirve?*
<https://mi.certerus.com/knowledgebase/124/iQue--es-un-Proxy-y-para-que-sirve-.html>
19. *Diferencias Proxy y cortafuegos.* (2012, 19 enero). segurtasuna.
<https://segurtasuna.wordpress.com/2012/01/19/diferencias-proxy-y-cortafuegos/>
20. *¿Qué es la seguridad informática y cómo puede ayudarme? / VIU.* (2021). Universidad Internacional de Valencia.
<https://www.universidadviu.com/es/actualidad/nuestros-expertos/que-es-la-seguridad-informatica-y-como-puede-ayudarme>
21. Jiménez, J. (2021, 1 junio). *Consigue que el Internet vaya más rápido con estas súper ofertas.* RedesZone.
<https://www.redeszone.net/noticias/ofertas/repetidores-wifi-sistemas-mesh-routers-junio-21/>

22. Lorenzo, J. A. (2021, 10 abril). *ZoneAlarm Free firewall: configura este cortafuegos para controlar Windows*. RedesZone.
<https://www.redeszone.net/tutoriales/seguridad/zonealarm-free-firewall-configurar-cortafuegos-windows/>
23. Instalación y configuración de servidores. (2021). *Servidor Firewall*.
<http://www.todoenservidores.com/servidores-en-linux-o-windows/servidor-firewall/>
24. Grup, I. D. (2020, 21 julio). ▷ *Qué es un Firewall y cómo funciona?* ID Grup.
<https://idgrup.com/firewall-que-es-y-como-funciona/>
25. Cunha Barbosa, D. C. B. (2020, 2 enero). *Qué es un proxy y para qué sirve*. Daniel Cunha Barbosa. <https://www.welivesecurity.com/la-es/2020/01/02/que-es-proxy-para-que-sirve/>
26. Alami, Z. (2021, 14 enero). *7 consejos de seguridad informática para empresas*. Internacionalmente - Internacionalización, marketing y tecnologías.
<https://internacionalmente.com/consejos-seguridad-informatica-empresas/>
27. *Plug-in WindowBuilder para crear interfaces visuales*. (2021). tutoriales de programación.
<https://www.tutorialesprogramacionya.com/javaya/detalleconcepto.php?codigo=128&punto=&inicio>
28. *¿Cómo crear Jpanel dinámicamente?* (2017, 5 diciembre). Stack Overflow en español. <https://es.stackoverflow.com/questions/122593/c%C3%B3mo-crear-jpanel-din%C3%A1micamente>
29. *Tema 3: Interfaz Gráfica*. (2021). Universidad de Alicante.
<http://www.jtech.ua.es/historico/plj/restringido/ejercicios/sesion09/sesion09.html>

Anexo A. Encuestas realizadas

<https://www.vpnunlimited.com/es/help/vpn-protocols/ikev2-protocol>

Índice de acrónimos

A.-

Ah: Authentication Header Protocolo de Autenticación

D.-

DNS Domain name system Sistema de Nombres de Dominio

DDNS Dynamic Domain Name System Sistema Dinámico de Nombres de Dominio

E.-

ESP Encapsulating Security Payload Carga Útil de Seguridad Encapsulada

I.-

Ip Internet Protocol Protocolo de Internet

IoT Internet of things Internet De Las Cosas

IPSEC Internet Protocol security Protocolo de seguridad de internet

IKEV2 Internet Key Exchange v2 Intercambio de Claves de Internet Versión 2

L.-

LAN Local Area Network Red de Área Local

L2TP Layer 2 Tunneling Protocol Protocolo de Túnel de Capa 2

O.-

OpenSource Fuente Abierta

R.-

RFB Remote From Buffer Remoto desde Buffer

S.-

Smartwatch Reloj Inteligente

T.-

TAP Terminal Access Point Punto de acceso terminal

TFE Trabajo Fin de Estudios

TFG Trabajo Final de Grado

U.-

UNIR Universidad Internacional de la Rioja

URL Uniform Resource Locator Localizador de Recursos Uniforme

USB Universal Serial Bus Bus Universal en Serie

V.-

VPN Virtual Private Network Red Privada Virtual

W.-

WEP Wired Equivalent Privacy Privacidad Equivalente a Cableado

WAP Wireless Application Protocol Protocolo de Aplicación Sin Hilos