Implementación de una red privada virtual de software libre en una empresa

Rafael Pomar Pascual
Grado de Ingeniería Informática
Área de Administración de Redes y Sistemas Operativos

Miguel Martín Mateo
Javier Panadero Martínez

06-2019

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Implementación de una red privada virtual de software libre en una empresa*
Nombre del autor:	*Rafael Pomar Pascual*
Nombre del consultor/a:	*Miguel Martín Mateo*
Nombre del PRA:	*Javier Panadero Martínez*
Fecha de entrega (mm/aaaa):	06/2019
Titulación::	*Grado de Ingeniería Informática*
Área del Trabajo Final:	*Administración de Redes y Sistemas Operativos (ARSO)*
Idioma del trabajo:	*Español*
Palabras clave	*ARSO, VPN, Redes*

Resumen del Trabajo (máximo 250 palabras): *Con la finalidad, contexto de aplicación, metodología, resultados i conclusiones del trabajo.*

El trabajo consiste en el análisis, y posterior implementación de una red privada virtual (VPN) en una empresa con la finalidad de que todos los empleados e incluso los proveedores puedan conectarse desde cualquier sitio geográfico donde estén a las dependencias de la sede central, ya sea para trabajar (empleados) o para realizar un proyecto o modificación puntual que no necesite desplazamiento (proveedores). Esta VPN será de software libre e irá completamente integrada en nuestro firewall.

Actualmente no hay ninguna forma que ningún empleado pueda trabajar desde fuera de la empresa con las herramientas necesarias (ERP, programa de nóminas, etc…) con este proyecto se pretende solucionar todas esas necesidades de todos los departamentos de la empresa y conseguir más productividad para la compañía.

El proyecto comprenderá desde un análisis de las soluciones que podrían solucionar las necesidades corporativas hasta la implementación de la solución escogida más adecuada.

Abstract (in English, 250 words or less):

The project consists of the analysis and subsequent implementation of a virtual private network (VPN) in a company so that all employees and even suppliers can connect from any geographical location where they are to the headquarters premises, either to work (employees) or to carry out a project or specific modification that does not require displacement (suppliers). This VPN will be free software and will be completely integrated into our firewall.

Currently there is no way that any employee can work from outside the company with the necessary tools (ERP, payroll program, etc ...) with this project is intended to solve all these needs of all departments of the company and get more productivity for the company.

The project will range from an analysis of the solutions that could solve the corporate needs to the implementation of the most appropriate solution chosen.

Índice

1. Introducción 1
1.1 Contexto y justificación del Trabajo 1
1.2 Objetivos del Trabajo 1
1.3 Enfoque y método seguido 2
1.4 Planificación del Trabajo 3
1.5 Breve sumario de productos obtenidos 5
1.6 Breve descripción de los otros capítulos de la memoria 6
2. VPN 8
2.1 Introducción a las VPN 8
2.2 Modelo OSI y TCP/IP. 9
2.3 Tipos de redes 11
2.4 Modos de operación 12
2.5 Ventajas de las VPN 13
2.6 Tipos de redes VPN 14
2.7 Protocolos VPN 15
2.8 Métodos de implementar VPNs 17
2.9 Cifrado de datos 19
3. Análisis de las necesidades y estudio de las soluciones. 22
3.1 Análisis de las necesidades 22
3.2 Estudio de las soluciones 24
4. Elección de la solución 29
4.1 Elección de la solución 29
5. Equipos que utilizarán VPN y perfiles de usuario VPN 30
5.1 Equipos que utilizarán VPN 30
5.2 Perfiles de usuario VPN 31
6. Estructura de la red y direccionamiento 34
6.1 Estructura de la red 34
6.2 Direccionamiento de la red 36
7. Configuración del firewall, vpn y cliente 38
7.1 Configuración del firewall 38
7.2 Configuración de la VPN 41
7.3 Configuración del cliente vpn 45
8. Conclusiones 48
9. Glosario 49
10. Bibliografía 50

Lista de figuras

Figura 1: Diagrama de Gantt……4
Figura 2: Mapa de una red VPN..……8
Figura 3: Modelo OSI vs TCP/IP……9
Figura 4: LogMeIn Hamachi VPN……..25
Figura 5: OpenVPN……..26
Figura 6: Radmin VPN……27
Figura 7: GlobalProtect VPN……..28
Figura 8: Mapa de equipos trabajando con VPN contra sede central……..30
Figura 9: Grupo de seguridad vpn.admon-rrh en Active Directory……32
Figura 10: Configuración LDAP autenticación usuarios……33
Figura 11: Ejemplo de configuración de direccionamiento de perfil vpn.admin..37
Figura 12: Regla de firewall de perfil vpn.admin……...38
Figura 13: Detalle de regla de firewall de perfil vpn.admin……38
Figura 14: Regla de firewall perfil vpn.local-resources acceso CIFS……...39
Figura 15: Detalle config regla firewall vpn.local-resources acceso a CIFS……39
Figura 16: Alias de CIFS direccionamiento……..39
Figura 17: Alias de Ports_CIFS, puertos usados CIFS……..39
Figura 18: Servidor OpenVPN perfil vpn.local-resources……...41
Figura 19: Detalle configuración servidor OpenVPN vpn.local-resources……...41
Figura 20: Certificado servidor perfil vpn.local-resources……..42
Figura 21: Detalle configuración certificado servidor perfil vpn.local-resources..42
Figura 22: Detalle configuración servidor autenticación perfil LDAP……43
Figura 23: Certificado cliente usado en el cliente perfil vpn.local-resources…..45
Figura 24: Configuración cliente VPN vpn.local-resources……45
Figura 25: Configuración servidor VPN, detalle configuración parte cliente…...47
Figura 26: Ejemplo de conexión cliente VPN perfil vpn.admin……..47

Lista de tablas

Tabla 1: Direccionamiento red empresa……34
Tabla 2: Relación direccionamiento red con aplicativos……..…34
Tabla 3: Relación direccionamiento perfil con aplicativo empresa……36

1. Introducción

1.1 Contexto y justificación del Trabajo

Cada día se necesita más, en según en qué empresas, el trabajar desde casa o cualquier lugar como si uno estuviera en su oficina. Además, lo tienen que hacer de forma segura porque los datos o ficheros con lo que trabajan contienen datos e información de la empresa muy sensible.

Cualquier empleado de una empresa puede necesitar acceder a las aplicaciones, archivos, impresoras, etc… que hay alojadas en la empresa desde cualquier lugar en el que se encuentren y hacerlo de manera segura. Además, muchos de los proveedores que brindan soporte a las empresas también necesitarán acceder a sus aplicaciones para poder desarrollar nuevos proyectos e implantaciones que necesiten de conectarse a las dependencias de la empresa para evitar trasladarse físicamente a las empresas donde dan servicio.

Para ello, se necesitará un acceso securizado y que sólo necesite conexión a internet para que todo lo anteriormente hablado sea posible y por eso necesitaremos una red privada virtual (VPN) que es la que implementaremos en este TFG.

1.2 Objetivos del Trabajo

El objetivo principal del proyecto es servir un método de conexión a los trabajadores y proveedores de una empresa para que se pueden conectar a las dependencias de la empresa y poder realizar sus trabajos desde cualquier sitio del mundo que haya conectividad a internet.

Para lograrlo se necesitará servir de las siguientes actuaciones:

- Entender las necesidades de los usuarios de la empresa para definir unos roles o perfiles según los requisitos del usuario.

- Con el punto anterior descrito, definir una solución real para la empresa que facilite y brinde movilidad a los empleados para que su productividad no decaiga dependiendo de donde estén.

- Explicar en qué consiste una red privada virtual (VPN), sus ventajas, los tipos de VPN que hay, los protocolos que usa, métodos de implementar VPNs, qué seguridad se puede dar a las VPNs.

1.3 Enfoque y método seguido

Habría muchas formas de actuar ante este proyecto como puede ser el crear una vpn sencilla en un servidor y configurar las conexiones entrantes, comprar un firewall de pago en el que configuraríamos posteriormente su cliente VPN o la opción que hemos elegido, una solución de código abierto.
Tendríamos las siguientes opciones para implementar una VPN:

- VPNs de firewalls, donde el propio firewall trae su solución de VPN.

- Equipo hardware dedicado VPN, donde el propio hardware hace las tareas de tunelización, cifrado y autenticación de usuarios.

- Solución de software dedicado, donde puedes crearte en un servidor con Windows server 2012 por ejemplo, una VPN para que desde cualquier cliente Windows 7,8,10… puedas conectarte con el cliente VPN que tienen.

- VPNs basadas en enrutadores, donde todo el tráfico lo securiza el router.

Creemos que la primera solución basada en código abierto, a corto y medio plazo puede darnos el servicio de calidad que queremos ya que una opción de seguridad media-alta como puede ser la elegida elimina el hacer una inversión en un firewall de pago.

1.4 Planificación del Trabajo

El trabajo empezará el 20 de septiembre y constará de los siguientes puntos:

- **Análisis y estudio del plan de trabajo.**

  Analizaremos todas las partes que necesitaremos para adentrarnos en este TFG. Lo estructuraremos siguiendo las necesidades de los usuarios para poder ver qué mejor solución escoger a nivel de hardware y de software para cumplir con lo que requiere la empresa.

- **Estudio de VPNs, tipos de VPN, Protocolos, etc.. y Análisis de necesidades y estudio de soluciones.**

  Analizaremos los tipos de VPNs que hay, las ventajas que nos ofrecen, los protocolos que usan y los cifrados de datos a usar. Veremos soluciones de software libre o de pago que nos ofrece el mercado.
  Estudiaremos el mejor método para implementar la solución analizando las necesidades de los usuarios y viendo la solución elegida entre el abanico de posibilidades.

- **Análisis de los equipos, estructura de perfiles de usuarios y estructura de subredes.**

  Una vez tengamos la solución tendremos que analizar los equipos que se conectarán a la VPN, los perfiles que definiremos de empleados y proveedores y estructuraremos la red en subredes para las conexiones VPN. Por último, realizaremos su parametrización en el firewall de las subredes para los distintos tipos de perfiles y la configuración del cliente VPN con la securización elegida a implementar.

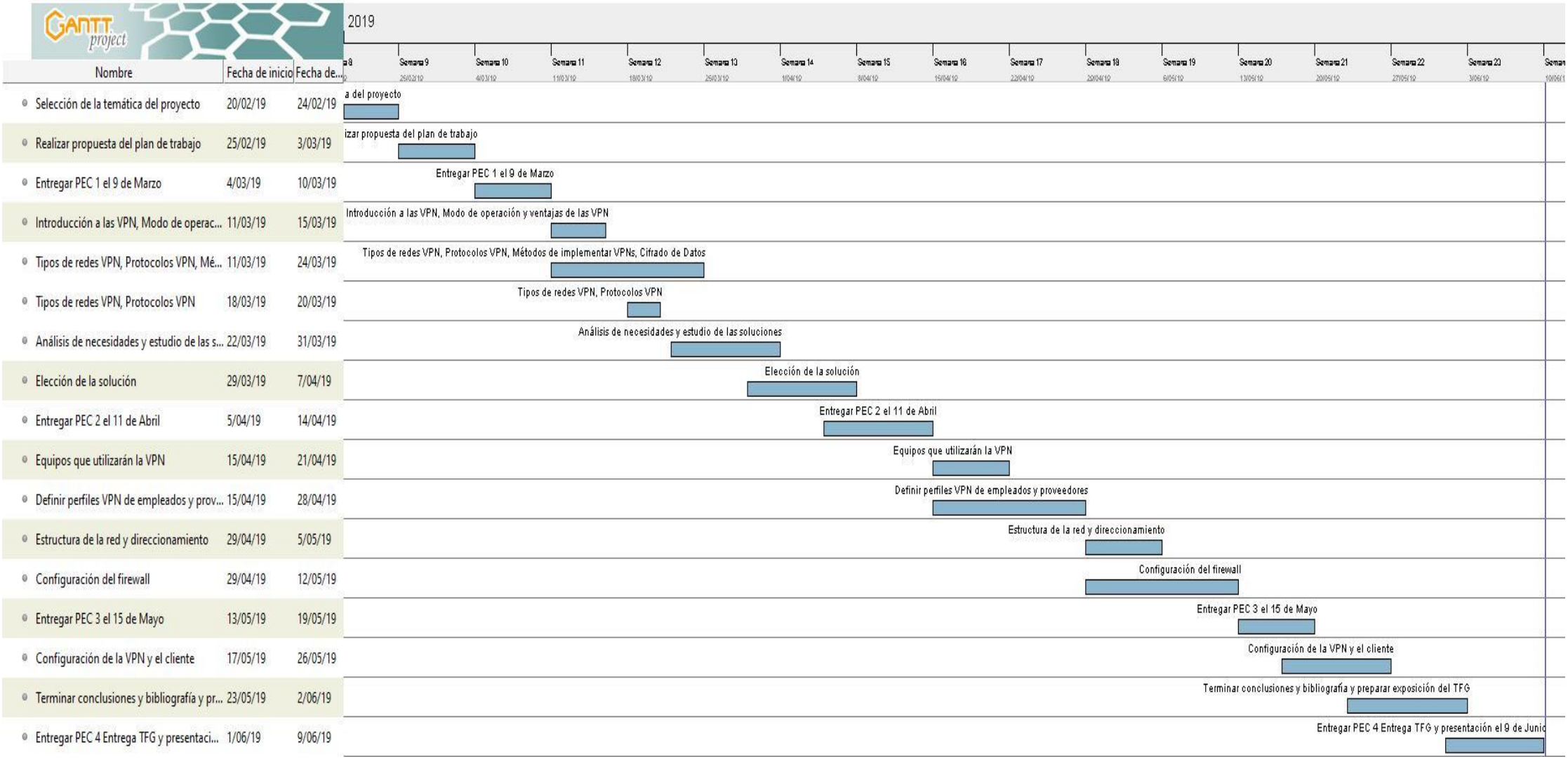

Figura 1: Diagrama de Gantt

1.5 Breve sumario de productos obtenidos

En nuestra empresa hay una necesidad alta que es el poder trabajar desde casa o cualquier lugar como si uno estuviera en su oficina ya que hasta ahora no tenían esta posibilidad. Además, lo tienen que hacer de forma segura porque los datos o ficheros con lo que trabajan contienen datos e información de la empresa muy sensible.

Con la realización de este proyecto se quiere obtener un servicio de conexión con movilidad para cualquier empleado de la empresa que necesite acceder a sus aplicaciones, archivos, impresoras, etc… que hay alojadas en la empresa desde cualquier lugar en el que se encuentre y hacerlo de manera segura.

Además, muchos de los proveedores (ERP, CMS...) que brindan soporte a nuestra empresa también necesitarán acceder a sus aplicaciones para poder desarrollar nuevos proyectos e implantaciones que necesiten de conectarse a las dependencias de la empresa para evitar trasladarse físicamente a las empresas donde dan servicio.

Para ello, se necesitará un acceso securizado y que sólo necesite conexión a internet para que todo lo anteriormente hablado sea posible y por eso necesitaremos una red privada virtual (VPN) que es la que implementaremos en este TFG.

1.6 Breve descripción de los otros capítulos de la memoria

- **Análisis y estudio de las necesidades de los usuarios.**

  Análisis y estudio de las necesidades de los usuarios para poder ver qué mejor solución escoger a nivel de hardware y/o de software esto nos permitirá tener una visión general de lo que tenemos que buscar en el mercado para su compra.

- **Estudio de las soluciones de software libre.**

  Basándonos en el estudio estudio anterior, elegiremos la mejor solución que nos ofrece el mercado (Open Source) para según las necesidades que tiene la empresa. Esto es porque económicamente la empresa tiene que ahorrar en el presupuesto de TI.

- **Elección de la solución.**

  Se elegirá una solución que se integre más rápidamente en la empresa ya que impera la seguridad en ella y la producción de sus empleados. También se valorará que el soporte de pago que tenga (aunque sea open source) no sea caro pero sí de calidad.

- **Definir perfiles de sus empleados.**

  Se definirán los perfiles de los empleados en base a sus necesidades y departamentos. También se hará lo mismo con los proveedores creando un perfil por cada proveedor externo. Con todo ello, se procederá a parametrizar las reglas en el firewall y en los clientes VPN.

- **Determinar subredes, equipos, etc... y configuración del firewall.**

  Determinaremos las subredes que harán falta, servers específicos a los que se puedan conectar, aplicaciones que necesiten los usuarios. Además, se analizarán los puertos que se necesitarán abrir para las distintas aplicaciones a las que necesitarán conectarse desde cualquier lado en sus equipos.
  Posteriormente las parametrizaremos todas las reglas y rutas que hagan falta para que cada perfil acceda a sus determinadas dependencias.

- **Delimitar seguridad a implementar y configuración VPN.**

  Se delimitará qué tipo de securización dar a la conectividad usuario-empresa. Con esta seguridad se garantizará la integridad de la información con la que trabajarán los empleados de la compañía.
  En último lugar, se configurará el túnel vpn y el cliente vpn con la securización elegida.

2. VPN

2.1 Introducción a las VPN

Una red cualquiera se compone de dos o más dispositivos que pueden comunicarse libremente de forma electrónica entre sí a través de cables. Una VPN es una red al fin y al cabo, incluso una VPN debe ser concebida como una extensión de una infraestructura de red. Esto significa que también debe estar disponible para la red existente, o para un grupo de usuarios con permisos a esa VPN en esa red pública.

En una VPN, la comunicación privada entre dos o más dispositivos se ejecuta a partir de una red pública que es Internet. Por eso, esa comunicación privada es virtual con lo que no está “físicamente” presente.
La parte de “privada” se explica porque si los dispositivos que están conectados a esa VPN se comunican entre sí en un entorno público, no hay un tercero que pueda detener o inmiscuirse en esta comunicación recibiendo la información traspasada entre ellos.

Una red privada virtual (VPN - Red privada virtual - Figura 1) conecta los componentes de una red privada a través de una red pública. Explicado de otro modo, una red privada virtual es una red que podría ser de una empresa integrada en una infraestructura compartida. La tecnología de una red virtual privada permite que una empresa “propague” sus servicios a través de esa red remota y así facilitar a los usuarios, afiliados o compañías asociadas su conexión a través de Internet a esos servicios. Sus ventajas son evidentes: crear un vínculo de comunicación barato, seguro y rápido.

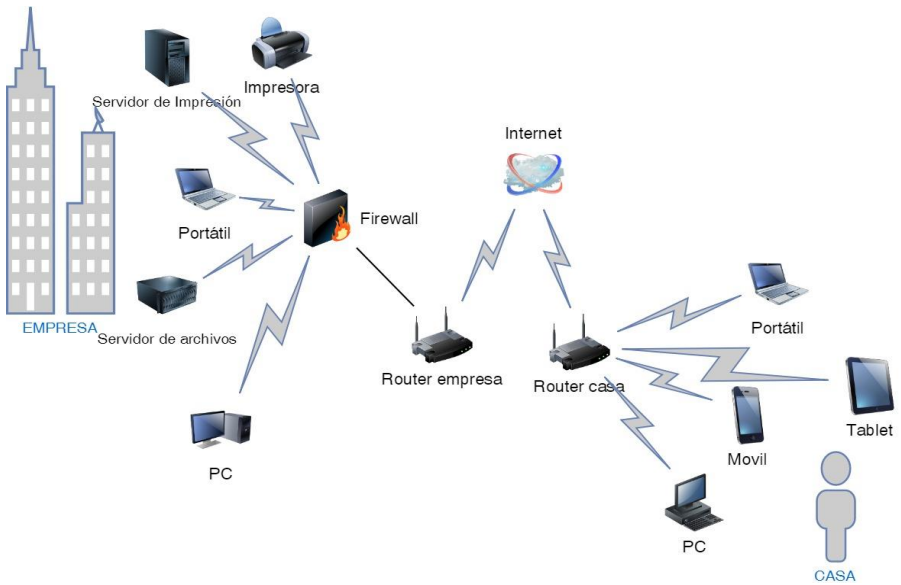

Figura 2: Mapa de una red VPN

2.2 Modelo OSI y TCP/IP.

El Protocolo de Control de Transmisión (TCP / IP) es un grupo de protocolos entre los que destacan son TCP e IP que se definieron como el estándar de Internet y que nos proporcionan la posibilidad de comunicarnos a través de las redes. El modelo OSI determina siete capas/niveles para el diseño de una red, por otro lado, el modelo TCP / IP define solo cuatro de las siete capas/niveles usados en el modelo OSI.

Estos modelos jerarquizados permiten diagnosticar a los expertos en redes de computadores diagnosticar problemas en una red y poder solucionarlos. Explicando el modelo OSI entenderemos el TCP-IP también.

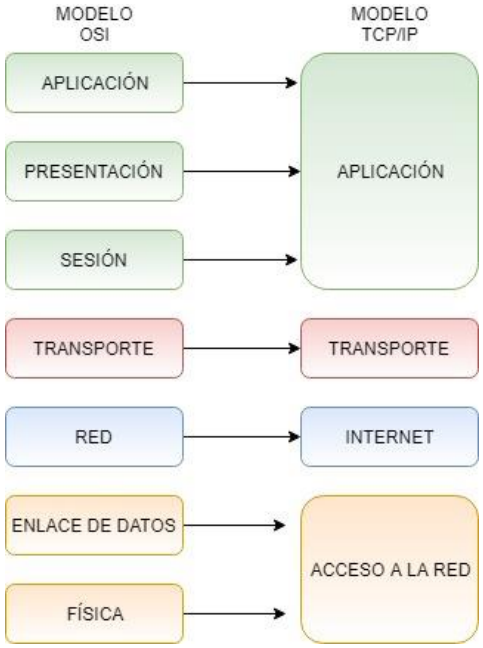

Figura 3: Modelo OSI vs TCP/IP

- Capa física (1): es la capa más baja de la jerarquía, se centraliza en el medio físico (cables de fibra o cobre) con en el que un ordenador se conecta a la red. En el modelo TCP equivale a la capa de acceso de red. La unidad de datos de esta capa es el Bit.

- Capa de enlace de datos (2): en esta capa se centra en el direccionamiento físico de los hosts (MAC address), la detección de errores y el control de flujo principalmente. La unidad de datos de esta capa es la trama. En esta capa funcionan los switch segmentando las tramas y enviándolas a sus respectivos destinatarios.

- Capa de red (3): es el encargado de reconocer el enrutamiento entre las redes que se vean afectadas y hacer que los datos que salen de un origen lleguen a su destino. El hardware de red que suelen hacer su trabajo en este nivel son los router, aunque algunos switches también pueden ser capa 3. La unidad de datos de esta capa es el paquete.

- Capa de transporte (4): esta capa tal como bien su nombre indica se dedica al transporte de los datos. Su unidad de datos (PDU) es el segmento y tenemos que tener en cuenta que puede ser de dos tipos:

    - TCP: asegura la entrega de toda la información enviada del origen al destino, esto lo garantiza gracias al control de errores y de flujo que provee este protocolo. Es un protocolo dirigido a la conexión entre hosts.

    - UDP: este protocolo no está dirigido a la conexión entre hosts, no provee un control de errores y puede perderse información por el camino. Este protocolo se usa preferentemente en las videollamadas, streaming de vídeo o audio, etc…

- Capa de sesión (5): esta capa permite establecer una sesión entre dos hosts distintos. Permite la reconexión si por lo que sea la sesión se ha suspendido. La unidad de datos (PDU) son los datos en esta capa.

- Capa de presentación (6): esta capa permite interpretar el formato y determina una sintaxis a los datos para su emisión en la red. La unidad de datos (PDU) son los datos en esta capa.

- Capa de aplicación (7): esta capa provee servicios de las otras capas/niveles a las aplicaciones y en ella se determinan los protocolos a usar como puede ser SMTP, FTP, HTTP, etc… La unidad de datos (PDU) también son los datos en esta capa.

2.3 Tipos de redes

Atendiendo a segmentar las redes según la distancia entre los hosts que la componen podemos tener las siguientes redes:

- LAN: si todos los hosts que pertenecen a una red en un mismo edificio, casa, empresa, etc… estamos hablando de una red de área local o LAN. Se definen para determinar redes de alta velocidad y su cobertura suele ser un edificio o un conjunto de ellos interconectados hasta un límite de 5kms.
  En este tipo de red se pueden determinar diferentes topologías de red, como puede ser en anillo, en estrella, en bus y en malla.

- MAN: varias redes de área local ubicadas en diferentes edificios de por ejemplo una ciudad definen una red de área metropolitana (MAN). Esta conexión se suele hacer a través de un operador ISP y sus conexiones son de fibra óptica.

- WAN: varias redes metropolitanas localizadas en distintos continentes definen una red WAN (red de área amplia). Las conexiones pueden ser de cualquier tipo satélite, fibra óptica, etc… y también los facilitan los operadores de servicios ISP.

2.4 Modos de operación

Una VPN proporciona a sus usuarios permitidos comunicarse mediante un túnel “virtual” de Internet y poseer una seguridad que únicamente se pueden dar en redes privadas.
Para usar Internet para una VPN, habría que tener en cuenta el problema principal que conlleva que se debe al hecho de que los paquetes con la información privada de la empresa viajan por Internet y esa información se puede robar y leer su contenido. Esto es el principal problema para las compañías que desean trabajar con información privada y también estar conectadas a Internet, pero hay una solución que es la tunelización. Los paquetes se envían encriptándolos primeramente y luego se encapsulan en paquetes IP y se transmiten mediante un túnel por medio de Internet.
Podemos decir entonces que una VPN a “grosso modo”, es un enlace punto a punto entre dos hosts.

La información transmitida por medio de la VPN estará asegurada por la encriptación de sus datos. Hace muchos años una red privada era una red dedicada contratada con un operador y que interconectaba diferentes centros. En estos días en el que se utiliza la red de redes (internet) para todo, se han establecido protocolos para tunelizar, dentro de internet, nuestras VPN.
La “tunelización” proporciona al origen de datos (remitente) encapsular en su datagrama otro paquete de datos que maneja otro protocolo de comunicación distinto. Además, estos paquetes encapsulados tendrán la posibilidad de darles protección contra lectura o modificación a través de diferentes protocolos de cifrado de datos.

Hay que tener en cuenta además que ambos hosts conectados a través de la VPN con cifrado deben entender y usar el mismo protocolo de comunicación.
Los túneles VPN suelen tener dos tipos de terminación final, puede tener un ordenador o una LAN (red de área local) con una puerta de enlace, este servicio suele ofrecerlo un firewall o también un router.
Para los túneles VPN que conecten una LAN a otra LAN la puerta de enlace de cada host se utiliza como una interfaz situada entre la LAN privada de ambos hosts y el túnel establecido. De este modo, los usuarios de ambos extremos pueden interconectarse a través del túnel de manera transparente.
En la opción de conectar con un cliente VPN a otra LAN se crea una conexión con la red destino y es el cliente VPN quien crea el túnel. Para ello, el usuario es el que tiene que correr un software (cliente VPN) que establece comunicación con la puerta de enlace de la LAN destino.

2.5 Ventajas de las VPN

Cada día el ambiente empresarial está necesitando más y más productividad, por eso, las empresas apuestan porque las comunicaciones tengan seguridad, fiabilidad y por supuesto rapidez entre las diferentes sedes que componen la compañía y los puestos desde que se conectan los trabajadores (hogares, oficinas remotas, etc…).

Para ello, las empresas suelen contratar líneas Macrolan para conectar las diferentes sedes a las que da cobertura geográfica, este servicio tiene un impedimento que es el precio, según la velocidad contratada (caudal contratado y garantizado en base a un porcentaje estipulado de velocidad).

Las VPNs traen las siguientes ventajas a las compañías:

- Movilidad: cualquier proveedor o empleado de la compañía pueden conectarse a la red empresarial desde cualquier lugar, solamente necesita conectividad a internet con la seguridad que provee el servicio.

- Unificación: se pueden implementar y unificar mediante esta conexión para distintos aplicativos como podría ser aplicaciones de videoconferencia, transferencia de archivos, voz IP, sistemas de información propios, etc…

- Disminución de gastos económicos: las VPNs son soluciones más baratas que las redes privadas de las propias empresas. Por eso, el coste de contratar a un ISP una línea de este tipo es mucho mayor, ya sin entrar en temas de los gastos de los empleados que las gestionan y el hardware de red que las soporta.

- Escalabilidad: a la hora de que la empresa crezca y tenga más necesidades de conectividad y movilidad para los empleados y proveedores, este servicio se puede dimensionar para que no se quede obsoleto o tenga falta de rendimiento.

- Seguridad: todos los datos que viajan a través de las VPNs están preservados por muchas capas de seguridad como puede ser la autenticación de usuarios, encriptación y cifrado de datos, Ipsec, etc…

- Aplicaciones: se pueden integrar las aplicaciones empresariales en Cloud y utilizar las VPNs para conectarnos a ellas y trabajar bajo todas las posibilidades que nos brinda el servicio (seguridad, rapidez, fiabilidad).

2.6 Tipos de redes VPN

Existen diferentes tipos de VPN que explicaremos a continuación:

- VPN PPTP: este tipo de VPN es la más usada, la utilizan usuarios remotos para conectarse a través de internet. Simplemente se necesita un usuario y contraseña para autenticarse y acceder a ella. Sólo se necesita un cliente VPN (el de windows mismo) para conectarse, por lo que no necesita ningún hardware adicional, con lo que además es barata.
  Pero también tiene su contrapartida y es que no ofrece codificación de los datos, hoy en día con la importancia de la seguridad en los datos que hay hace que este tipo de VPN sea automáticamente rechazada en el entorno empresarial. Además utiliza Protocolo Punto a Punto (PPP) con lo que para integrar seguridad depende del marcado.
  Otra ventaja es que es compatible con Linux , Mac y Windows.

- VPN site to site: se utiliza para conectar diferentes compañías mediante una red pública. Este tipo de VPN utiliza en cada extremo de la conexión VPN un servidor VPN el cual hará las funciones de “enrutador”, el servidor VPN “origen” hará una llamada a un servidor VPN “destino” autenticándose en él y este a su vez le contestará haciendo lo mismo de manera inversa quedando establecida la conexión.
  Por otro lado, este tipo de VPN integra codificación que la hacen los “enrutadores”.

- VPN Híbrida: es una VPN MPLS cimentada sobre la seguridad que ofrece IPSec. El funcionamiento es el siguiente, al tener un coste tan alto para la empresa de una VPN MPLS se monta en un extremo un túnel VPN IPSec (hardware autogestionado por el departamento IT de la empresa) y en el otro extremo una VPN MPLS (gestionada por el ISP), esto hace que el coste sea menor y que tengas los beneficios de seguridad que te brinda IPSec.

2.7 Protocolos VPN

- VPN L2TP: en este protocolo VPN se fusiona adicionalmente con otro protocolo de seguridad (IPSec) para aumentar las opciones de seguridad en la conexión L2TP dejando la "tunelización" entre dos extremos a L2TP y la confidencialidad y la integridad de los datos a IPSec. La seguridad recae en el protocolo IPSec cifrando la información y brindando confidencialidad a la misma. También utiliza protocolo PPP como PPTP y añade autenticación de usuarios CHAP y MSCHAPv2.

- IPSec: es un protocolo de seguridad que se implementa en una comunicación entre dos redes distintas y opera en la capa de red (capa 3). Brinda protección comprobando cada sesión y cifrando todos los paquetes. Tiene dos modos de operación, transporte y túnel, la diferencia es que en transporte se cifra el mensaje directamente dentro del paquete y en el modo túnel todo el paquete va cifrado. Es protocolo nos ofrece adicionalmente el trabajar con otros métodos de seguridad como puede ser IKE (protocolo de ejecución de la negociación de asociaciones de seguridad "SA"), ESP (protocolo que sirve autenticación y cifrado) y AH (protocolo que sirve autenticación).

- SSL y TLS: estos protocolos se utilizan en VPNs donde se usar el navegador web para establecer la conexión, diríamos que lo trataríamos como el cliente VPN y operan en las capas 4 a 7 (transporte, sesión, presentación, aplicación). La diferencia con las otras es que no se tiene acceso a toda la red de la empresa sino a aplicaciones determinadas.
  Primordialmente se utilizan en portales de compras que securizan las sesiones de los potenciales clientes que van a comprar en sus portales, esas conexiones están securizadas desde el navegador web hasta el servidor web donde está alojado el portal de compras.
  Esto se debe a que todos los navegadores web son compatibles con SSL y TLS y ya vienen en ellos implementados por lo que al conectarse a un portal de compras de este tipo hacen uso de estos protocolos de seguridad y por eso al hacer uso de SSL nos conectaremos en modo seguro a través del protocolo de transferencia de hipertexto (https).

- VPN MPLS: mayormente utilizadas en conexiones VPNs site to site. Este tipo de VPNs se basa en asignar etiquetas a paquetes IP y enrutarlas con el fin de agilizar la entrega de paquetes de red en distintos protocolos. Este tipo de servicios hay que contratarlos a través de un ISP y que sea el mismo en todos los site.

Tiene el inconveniente de que tiene mayor complicación de configuración y modificación que los demás tipos de VPNs. Además, económicamente hablando es bastante cara ya que requiere de hardware de alto coste en el cliente y el servicio que sirve el ISP también lo es.

2.8 Métodos de implementar VPNs

Atendiendo a los distintos modelos de VPN (site to site o acceso remoto) se requieren de unos elementos u otros a la hora de crear una VPN en internet:

- Internet
- Centro de gestión de políticas en el servidor de una VPN
- Autoridades de certificación
- Puertas de enlace de seguridad

El medio sobre el que nos conectaremos será Internet, las puertas de enlace de seguridad delimitarán la red privada de la pública e impedirán accesos no permitidos en nuestra red privada y además cifrarán y tunelizarán nuestra información a su destino a través de internet.
Estas puertas de enlace de seguridad podríamos segmentarlas en:

- Routers
- Firewalls
- Hardware VPN dedicado (como concentradores VPN)
- Software cliente

VPNs basadas en routers

Teniendo en cuenta que los routers inspeccionan todos los paquetes que entran y salen de nuestra red privada es de lógica que el elemento que cifre los paquetes sean ellos.
Los hay de dos tipos, con software integrado que hace el cifrado o con un chip integrado en el procesador y este es el encargado del cifrado. Siempre son mejores las soluciones basadas en hardware que no las de software ya que una alta carga de trabajo en el router con cifrado en software puede tirar la conexión mientras que la basada en hardware al ser independiente del software no se ve afectado su rendimiento.

Estas VPNs basadas en routers tiene la desventaja de que se necesita un desembolso económico por parte de la empresa (hardware) y también en empleados espcializados en redes que administren ese hardware.

VPNs basadas en firewalls

Muchas marcas de firewalls implementan soluciones para montar túneles. Los firewall, al igual que los routers, inspeccionan cada paquete que entra o sale de la empresa. Por este motivo, no es la opción más recomendada para túneles con

un tráfico de red muy alto porque si así fuera la conexión VPN podría caerse y dejar de dar servicio.
Es una opción recomendada para empresas pequeñas-medianas con un tráfico medio de datos. Además dota de una mayor seguridad al tener como puerta de enlace el propio firewall pudiendo proteger mediante reglas todo el tráfico del túnel.

Hardware VPN dedicado

Otra opción es el hardware vpn dedicado creado para ejecutar los trabajo de autenticación de clientes, cifrado de datos y creación de túneles. Este hardware permite configurar túneles LAN to LAN y algunos de cliente a LAN.
Este hardware es la mejor opción, basándonos en rendimiento, que puede haber para una empresa con un volumen de tráfico de red alto dentro de la VPN. Los modelos altos de gama ya traen fuentes de alimentación redundadas y pueden dar servicio a múltiples túneles paralelamente.

Software VPN dedicado

También existen las soluciones basadas en software VPN dando servicio entre un cliente y una puerta de enlace de seguridad a LAN o entre dos puertas de enlace de seguridad. Esta opción es la que escogen las empresas pequeñas por el coste bajo que requiere esta solución.
El funcionamiento es que el software VPN esté instalado en un equipo cliente y este a su vez conectará con el servidor VPN, un ejemplo es el cliente VPN de Microsoft que lo incluye dentro de todas las versiones de Windows Xp,7,8,10. El servidor VPN, que también lo incluye cualquier servidor de Windows, recibirá la conexión del cliente (p.e el propio de Windows 10) y quedará conectado a la red interna que esté detrás del servidor VPN.
Además existe la posibilidad de administrar las políticas de seguridad en el servidor VPN (ACLs) en las que se podrán dar o restringir permisos a los clientes. El servidor VPN lee estas ACLs y permite determinado tráfico sobre según qué clientes.

Por último, existe la posibilidad de securizar la conexión con certificados de tal manera que si un usuario no tiene el certificado en su equipo no podrá conectarse aunque sí tenga permisos su usuario. La base de datos de estos certificados se encuentran alojados por lo general en el mismo servidor VPN.

2.9 Cifrado de datos

El cifrado es un proceso de codificar información a través de un algoritmo el cual se genera en un host origen (proceso de cifrado) y que se descodifica en el host destino (proceso de descifrado).
Sin este proceso de cifrado toda la información que se compartiese en una red pública o privada sería vulnerable y susceptible de ser interceptada.
Existen dos tipos de cifrado, con clave pública (cifrado asimétrico) y con clave privada (cifrado simétrico).

- **Cifrado asimétrico**

  Este tipo de cifrado contiene dos claves dentro de su algoritmo, una privada la cual no se conoce y que está integrada en el algoritmo y una pública la cual se puede conocer. Conociendo esta clave pública se pueden generar y repartir nuevas claves y esto facilita el proceso comparado con los de clave privada. Esto es así porque si un paquete IP es cifrado con la clave pública de un host origen solamente se podrá descifrar con la clave privada del host remoto, para eso el host remoto ha tenido que facilitar la clave pública al host origen.
  En el apartado que nos atañe (VPN) se usan principalmente dos algoritmos de cifrado, Rivest Shamir Adlemen (RSA) y Diffie Hellman (DH).

  - *Diffie-Hellman (DH):*

    En este algoritmo de cifrado el funcionamiento es el siguiente:
    Tenemos 3 clientes los cuales el cliente 1 quiere transmitir información a cliente 2, cliente 3 está en el mismo canal de comunicación que los otros dos y puede escuchar todo lo que hablan. Por lo tanto, para que cliente 3 no se entere aunque escucha, cliente 1 elige un número primo (p.e. 23) y un número aleatorio menor que 23 (p.e. 16) y le manda estos números a cliente 2, cliente 3 lo escucha todo. Cliente 1 elige otro número “x” menor que 23 y este se lo guarda para él, mediante este número “x” calcularemos otro número “y” que mandaremos a cliente 2 de la siguiente forma:
    x= 15
    y= 16^15 (mod 23) = 9

    Por lo que cliente 1 enviará “y=9” a cliente 2.
    Ahora cliente 2 elegirá un número “x” para él y menor que 23 (p.e. 8) con lo que a través de este número calculará “z” para enviárselo a cliente 1.
    z= 16^8 (mod 23) = 12

entonces cliente 2 manda a cliente 1 “z=12”. Con estos datos ahora tanto cliente 1 como cliente 2 calcularán las claves que van a usar en el canal de cifrado:
Clave cliente 1: 12^15 (mod 23) = 13
Clave cliente 2: 9^8 (mod 23) = 13
Así observamos que generan la misma clave los dos y el cliente 3 no puede acceder a esa clave porque no conoce ni x del cliente 1 ni x del cliente 2.
El funcionamiento real es el mismo pero con número muchísimos más grandes (hasta 300 dígitos). En líneas generales este tipo de cifrado no es autenticado y no se sabe a ciencia cierta quien está escuchando en el mismo canal y poder interceptar la información y enviar su propia clave privada con lo que tiene “ciertas” vulnerabilidades.
La solución es utilizar un algoritmo de clave pública con RSA junto con un firmas digitales para que la entrega de las claves sea lo más fiable y preservada posible.

- *Rivest Shamir Adleman (RSA)*:

  Este algoritmo de cifrado es el único que ciertamente cifra la clave pública. Esta clase de algoritmo se suelen usar para cifrado y para firmas digitales. Asimismo, un mensaje enviado encriptado (desde cliente 1) con clave RSA privada únicamente se podrá desencriptar con la clave RSA pública adecuada (de cliente 1) y por tanto todo aquel que tenga esta clave podrá descifrar el mensaje. Uno de los ataques que suelen hacerse contra este algoritmo es el de texto plano conocido que consiste en que el intruso puede adquirir texto encriptado con una clave desconocida, el objetivo es determinar la clave usada para encriptar y lo intentarán conseguir cifrando los mensajes que estén pendientes de enviar a sus destinatarios con distintas claves públicas mendiante el algoritmo RSA.

  El funcionamiento del algoritmo es el siguiente y pasará como con DH que en un sistema real los números utilizados serán muy altos:

  Se crean dos números primos grandes, “x” e “y”.
  Se calcula “a”= x * y
  Se calcula “b”= (x-1)*(y-1)
  Se elige un número “k”, co-primo de “b” de modo que el MCD (Máximo común divisor) entre “b” y “k” sea 1.
  Se busca un número “m” teniendo en cuenta que (“m” mod “b”) sea 1

Se publican a los destinatarios la clave pública “k” y “a” y se guarda como clave privada “m”.

Y por último para los mensajes cifrados se utiliza:

Mensaje a enviar cifrado = (mensaje plano)^k mod “a”

Mensaje plano = (Mensaje a enviar cifrado)^m mod “a”

3. Análisis de las necesidades y estudio de las soluciones.

3.1 Análisis de las necesidades

- **Contexto**

En la empresa donde trabajamos (un periódico por ejemplo) los redactores cada día necesitan estar más en continuo movimiento buscando la noticia y es un incordio para ellos el tener que ir a la redacción central cada día a meterse en el sistema editorial del periódico a escribir sus páginas diarias. Asimismo, en la empresa cada día se tienen más proveedores que llevan proyectos de todo tipo de la empresa y que se tienen que conectar más frecuentemente o viajar “in situ” a la sede física con la molestia y gasto que ello provoca.

- **Estado inicial**

Como se ha comentado anteriormente, los redactores del periódico tienen que ir cada día a la redacción para escribir la noticia en el sistema editorial del periódico. Esto supone una pérdida de tiempo para ellos porque pierden mucho tiempo entre el tiempo de ir a cubrir la noticia y volver a la sede central para redactarla en el sistema editorial.
Adicionalmente los colaboradores externos del periódico se tienen que desplazar también a la sede central cada vez que tienen que colaborar en la redacción de una publicación especial.
También concerniente al departamento de Administración y Dirección del periódico, no se pueden trabajar desde casa en fechas clave.
Al mismo tiempo, pasa algo parecido con los proveedores de la empresa (ERP, software de Business Intelligence, software de RRHH, etc…) que tienen que ir muchas veces físicamente a la sede central para desarrollar nuevos proyectos y modificaciones sobre los que hay desarrollados.

- **Objetivos**

Visto el estado inicial de la necesidad de la empresa, se han definido los siguientes objetivos para mejorar el rendimiento y productividad de la empresa y poder dar soporte a los proveedores:

- Poder conectarse cada redactor a la redacción central y a su vez al sistema editorial desde cualquier sitio y a cualquier hora, simplemente

tener una conexión de internet (Wifi, tethering con el móvil, etc…) para poder escribir en tiempo real en el sistema las noticias que estén cubriendo en ese momento.

- Dar conectividad a los colaboradores del periódico para que no se tengan que desplazar a la redacción y puedan colaborar en la redacción de las publicaciones especiales donde tengan que trabajar.

- Dar soporte de conectividad también al departamento de Administración y Dirección ya que en épocas de cierre del mes o fechas clave de consejo de accionistas necesitan conectarse desde casa o cualquier sitio fuera de la empresa al ERP corporativo, a documentos en el servidor de ficheros de la empresa, etc… y todo esto bajo en canal seguro y con garantía de integridad de los datos con los que se trabaja.

- Dar conectividad a los distintos proveedores de la empresa a las herramientas a las que dan soporte, asimismo solo tendrán acceso al servidor donde estarán alojadas sus respectivas soluciones. Esto hará que los costes de desplazar a un empleado de la empresa proveedora a redacción central sean cero y solo incurran en costes del desarrollo de la herramienta.

3.2 Estudio de las soluciones

Para la puesta en marcha de una VPN, es necesario saber sus características para poder decantarnos por la que más se ajusta a nuestras necesidades e infraestructura. En el mercado, existen muchas soluciones que pueden ser utilizadas para nuestro propósito, veremos algunas de software libre y otras de pago.

LogMeIn Hamachi VPN - https://www.vpn.net/

Normalmente, el parametrizar una VPN suele ser bastante tedioso ya que incurre en configurar el router, software, etc… Con esta solución de Hamachi ya no existe ese problema.

Esta solución se basa en la autenticación de los clientes contra un servidor donde existen todos los usuarios que tienen acceso a la vpn. El cliente se autentica con usuario y contraseña y ya se establece un túnel seguro entre el origen y el destino sin pasar por ningún servidor del fabricante de la solución. Sin embargo, los servidores de Hamachi pueden comprobar cada cierto tiempo si los usuarios siguen conectados entre sí.

Cuando se instala el cliente, se instala un adaptador de red virtual por el que estableceremos la conexión con el cliente y al establecer el túnel con el destino se nos dará un direccionamiento específico (en nuestro caso 25.55.76.0/24) que es propio del proveedor Hamachi distinto al que nosotros podamos tener (por ejemplo 192.168.1.0/24).
Tendremos que tener en cuenta que si estamos detrás de un firewall habrá que configurarlo para permitir el tráfico a la red que crea Hamachi.

Figura 4: LogMeIn Hamachi VPN

El problema de esta solución es que el coste es gratuito hasta 5 personas y luego va en tramos de entre 6-32 trabajadores, luego de 33-256 trabajadores y por encima de 256 trabajadores.

Open VPN - https://openvpn.net/

Esta solución es gratuita y de software libre y da soluciones para la generación de túnes de extremo a extremo. Al igual que la solución anterior, los clientes se autentican con usuario y contraseña para acceder al túnel.
Integrada en esta solución están los proyectos de código abierto OpenSSL y SSL embebido. Los usuarios se pueden autenticar utilizando PAM, Radius, LDAP, AD o una propia BBDD privada que se tenga.
No es una solución compatible con IPSec o PPTP, solamente lo es con su propia seguridad que utiliza sus propias librerías OpenVPN (OpenSSL).
Brinda autenticación con clave secreta fundamentada en certificados y con nombre de usuarios y contraseña en el que el servidor necesitará un certificado.

Ofrece compatibilidad con NAT (red origen y destino pueden ser nateadas).
OpenVPN facilita dos clases de interfaz de red mediante el controlador TUN / TAP. Con el controlador TUN se puede generar un túnel IP de capa 3 así se puede encapsular los paquetes como datagramas TCP o UDP y con el controlador TAP de Ethernet de capa 2 que puede transportar cualquier tipo de tráfico de paquetes ethernet.

Tiene una mayor compatibilidad con fabricantes de firewall para poder realizar conexiones con OpenVPN, simplemente abriendo un puerto en el firewall ya que OpenVPN 2.0 permite varias conexiones en el mismo puerto TCP o UDP.

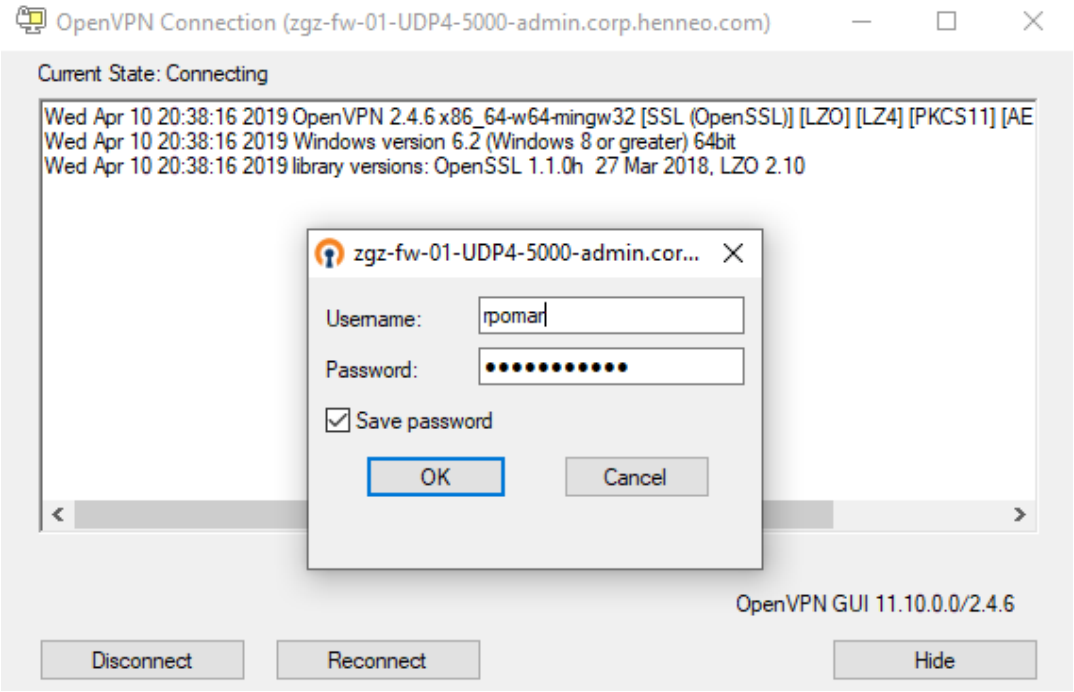

Figura 5: OpenVPN

Radmin VPN - https://www.radmin-vpn.com/es/

Esta solución gratuita es muy parecida a la primera de Hamachi. Es un software gratuito en el que te permite establecer una conexión segura de extremo a extremo a través de usuario y contraseña. Un extremo crea la red y el otro extremo se conecta a la red autenticándose con usuario y contraseña.
La velocidad de la conexión está limitada a 100Mbps lo cual está muy bien ya que en estos tiempos los ISP ofrecen esa velocidad como básica y está muy asentada en la mayoría de hogares de grandes urbes.
También provee cifrado de datos sobre un canal seguro y según el proveedor es muy fácil de configurar y administrar.

El direccionamiento de red una vez conectados al cliente es del rango (26.60.153.0/24) en el caso del ejemplo y la interfaz virtual creada es Radmin VPN con la que nos conectaremos a su red.

El problema de esta solución es que no encontramos sus algoritmos de cifrado que usa y no tenemos opiniones de su rendimiento cuando haya varias hosts funcionando en la misma red.

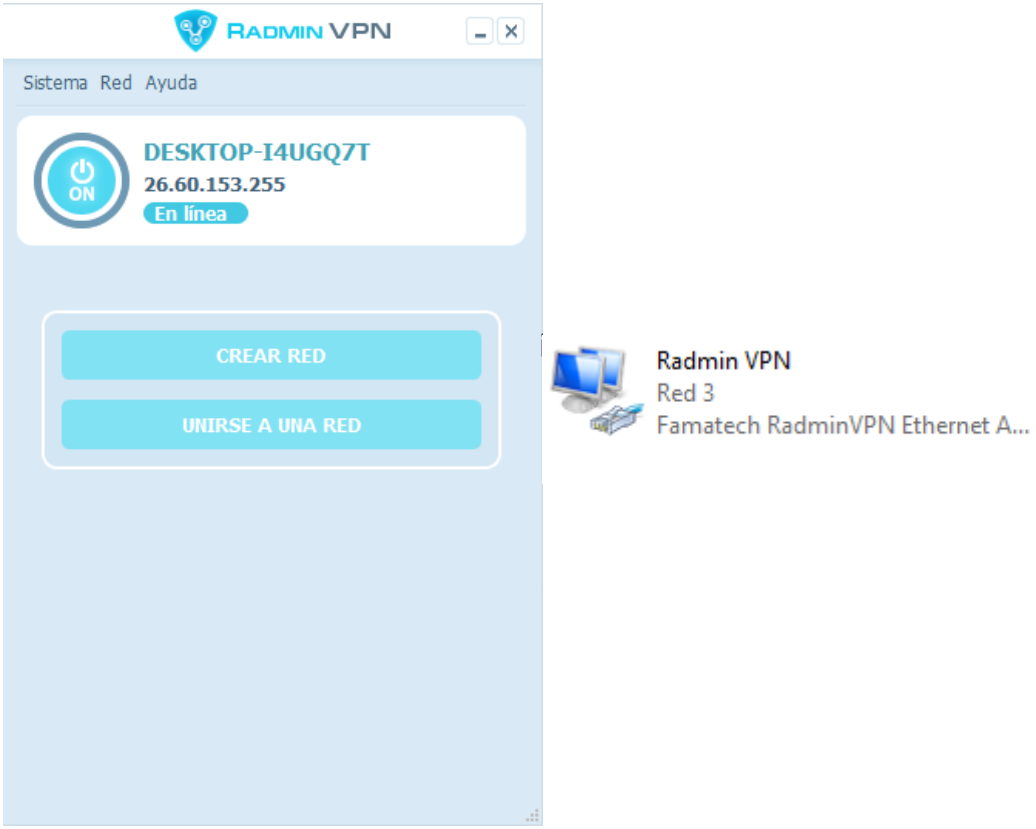

Figura 6: Radmin VPN

GlobalProtect VPN - https://www.paloaltonetworks.com/features/vpn

Esta solución de pago viene integrada con el firewall. Sin embargo, es una de las soluciones más completas que tenemos ya que incluye compatibilidad con VPN IPSec basada en estándares para túneles de extremo a extremo y adicionalmente para puestos móviles VPN SSL/IPSec como pueden ser ordenadores portátiles, smartphones, tablets, etc… y es como si estuvieran permanentemente securizados y conectados a la empresa.

Los túneles IPSec que brinda esta solución son compatibles mediante IPv4/IPv6 e IKEv1, IKEv2. IKE es un protocolo de seguridad que instaura una asociación de Seguridad (SA) en el protocolo IPSec.

Además, esta VPN se puede implementar con certificados para asegurar una conexión al túnel mayor, y así mejorar la seguridad, integridad y confidencialidad de la información de la empresa. Estos certificados irán tanto en el cliente VPN como en el firewall instalados y por lo tanto no podrán establecer una conexión VPN a este túnel ningún cliente que no tenga los certificados instalados.

Los usuarios se pueden autenticar utilizando los siguientes mecanismos: Radius, LDAP, AD, BBDD local, kerberos o tarjetas inteligentes.
Permite definir políticas de seguridad relacionadas con el estado del dispositivo en el que se va a establecer la conexión del túnel VPN, esto quiere decir que se puede obligar a que un host tenga que tener un nivel mínimo de seguridad como puede ser el tener todas las actualizaciones de Windows al día en el equipo antes de poder conectar con el destino.

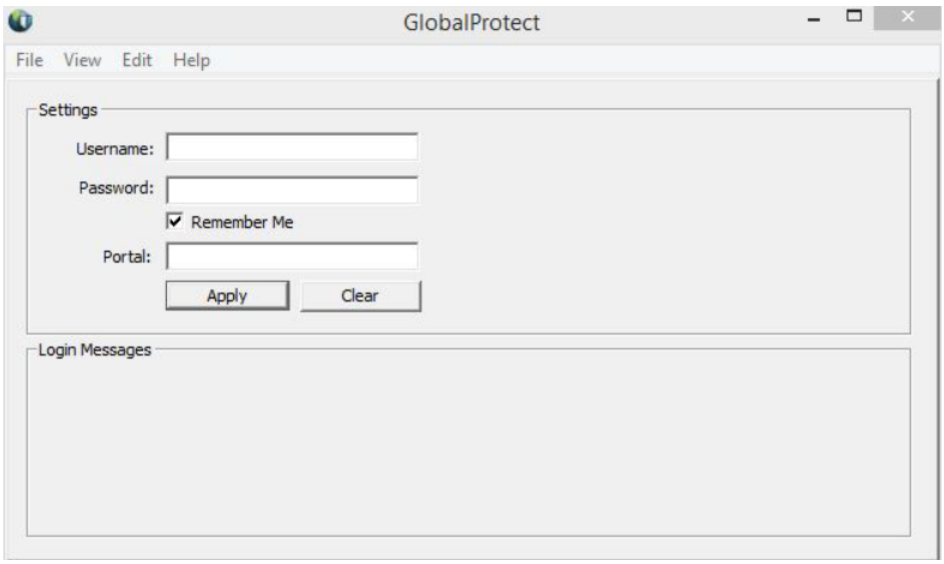

Figura 7: GlobalProtect VPN

4. Elección de la solución.

4.1 Elección de la solución

Una vez constituidas las necesidades, se ha elaborado un estudio sobre las distintas soluciones de VPN´s que nos podrían dar cobertura a nuestros objetivos principales de la empresa, sin olvidarnos del presupuesto económico a repercutir y que nos ofrece el mercado. Esta elección se centrará en las soluciones del apartado 3.2 de esta misma sección.
Tras haber analizado todas estas VPN´s, se ha procedido a elegir la mejor opción que se adapta a las necesidades de nuestra empresa.

Atendiendo a todas las características definidas en el apartado anterior 3.2 la empresa se decanta por OpenVPN, esta solución de software libre nos permitirá ofrecer servicio a la empresa para todos sus requisitos detallados en el apartado 3.1. Además, al ser un proyecto de software libre a la empresa no le acarreará un gasto el coste de licencia, solamente el de su implantación y mantenimiento por parte del departamento de IT de la compañía.

Las principales características tecnológicas por las que se ha optado por esta opción han sido:

- Posibilidad de autenticación con LDAP.
- Autenticación fundamentada en certificados.
- Compatibilidad con NAT.
- Seguridad propia OpenSSL en la que al ser un software libre tendrá un desarrollo continuo.
- Compatibilidad con la mayor parte de los principales fabricantes de firewall.

Al tener en una empresa un firewall Pfsense (también de software libre) la integración de openVPN y Pfsense es completa y es una de las principales opciones que nos ha decantado su elección.

5. Equipos que utilizarán VPN y perfiles de usuario VPN.

5.1 Equipos que utilizarán VPN

Actualmente en nuestro periódico ficticio tenemos varios departamentos: el departamento de Administración que lo conforma Contabilidad y Control de Gestión, el departamento de RRHH y redacción.

Los redactores llevan todos portátiles y se conectarán a través del móvil vía tethering desde cualquier parte donde estén.

También tendremos necesidades en el departamento de Administración y RRHH donde todos los empleados trabajan con portátiles y acceden a un repositorio de almacenamiento CIFS y que solamente se necesitará en la sede de Zaragoza, además de acceder al programa de nóminas (RRHH) o al ERP de la empresa (Administración).

Además, tendremos la necesidad de que algunos proveedores del periódico se conecten a las dependencias de la empresa para realizar modificaciones o proyectos nuevos puntuales.

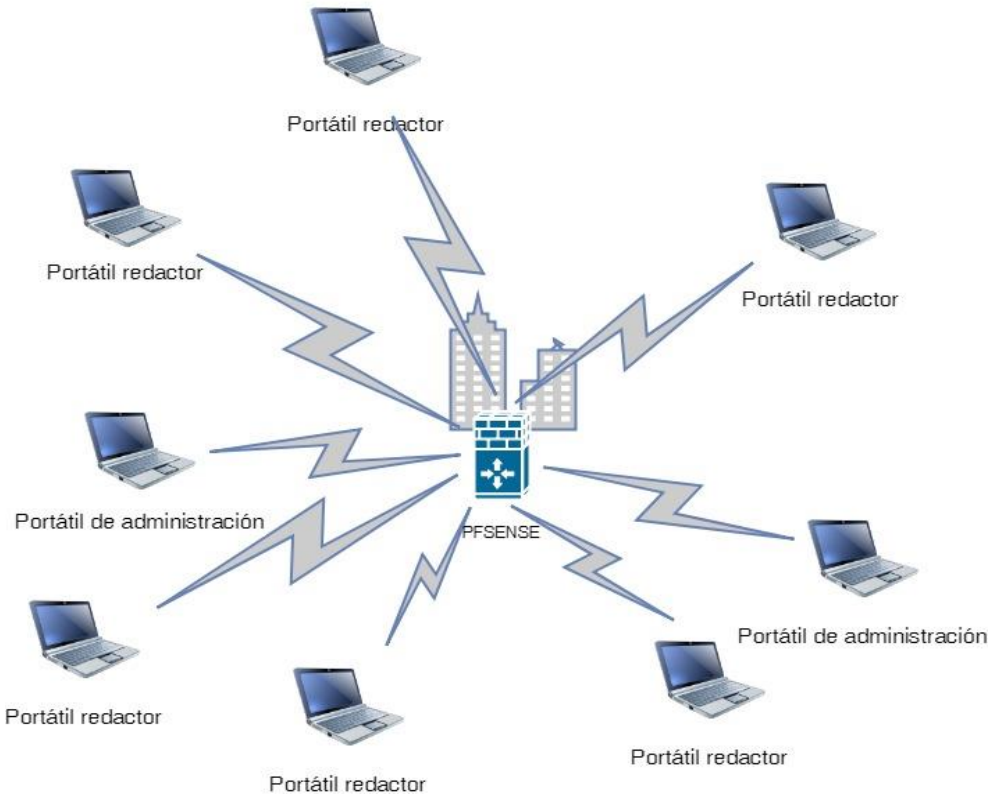

Figura 8: Mapa de equipos trabajando con VPN contra sede central

5.2 Perfiles de usuario VPN

Los perfiles de usuario necesarios serán en base a las necesidades de cada empleado.
Los tipos de perfil VPN serán los siguientes:

Vpn.local-resources

- Sistema editorial: tendrá acceso al sistema editorial del periódico desde cualquier sitio donde esté cubriendo la noticia para poder insertarla en el sistema sin tener que ir a la redacción central para hacerlo.
- Sistema documental: tendrá acceso al sistema documental del periódico para buscar noticias de agencias de información, fotos, periódicos de fechas pasadas.
- Acceso a las unidades de red mapeadas a recursos de almacenamiento de Cifs.

Vpn.admon-rrhh

- Programa de nóminas: acceso al programa de nóminas por parte de cualquier empleado de RRHH.
- Programa de seguridad social: acceso al programa de la seguridad social por parte de cualquier empleado de RRHH.
- ERP: acceso al ERP por parte de cualquier empleado de Contabilidad y Control de Gestión.
- Acceso a las unidades de red mapeadas a recursos de almacenamiento de Cifs.

Vpn.admin

- Acceso a todo por parte del departamento de Ti para la gestión de servidores e infraestructuras de la empresa. No tiene ninguna restricción.

Vpn.Prov-ERP

- Acceso exclusivamente a los servidores donde están corriendo las BBDD e instancias del ERP de la empresa.

La asignación será la siguiente:

Redactor -> vpn.local.resources
RRHH -> vpn.admon-rrhh
Contabilidad -> vpn.admon-rrhh
Control de gestión -> vpn.admon-rrhh
Departamento Ti -> vpn.admin
Proveedor externo de ERP -> vpn.Prov-ERP

Si hiciese falta en un futuro que más proveedores externos se conecten a nuestras dependencias se crearán otros nuevos perfiles de VPN dedicados para donde necesiten conectarse.

Los perfiles están configurados de la siguiente manera en el directorio activo, definidos como grupos de seguridad para la autenticación integrada en el directorio activo:

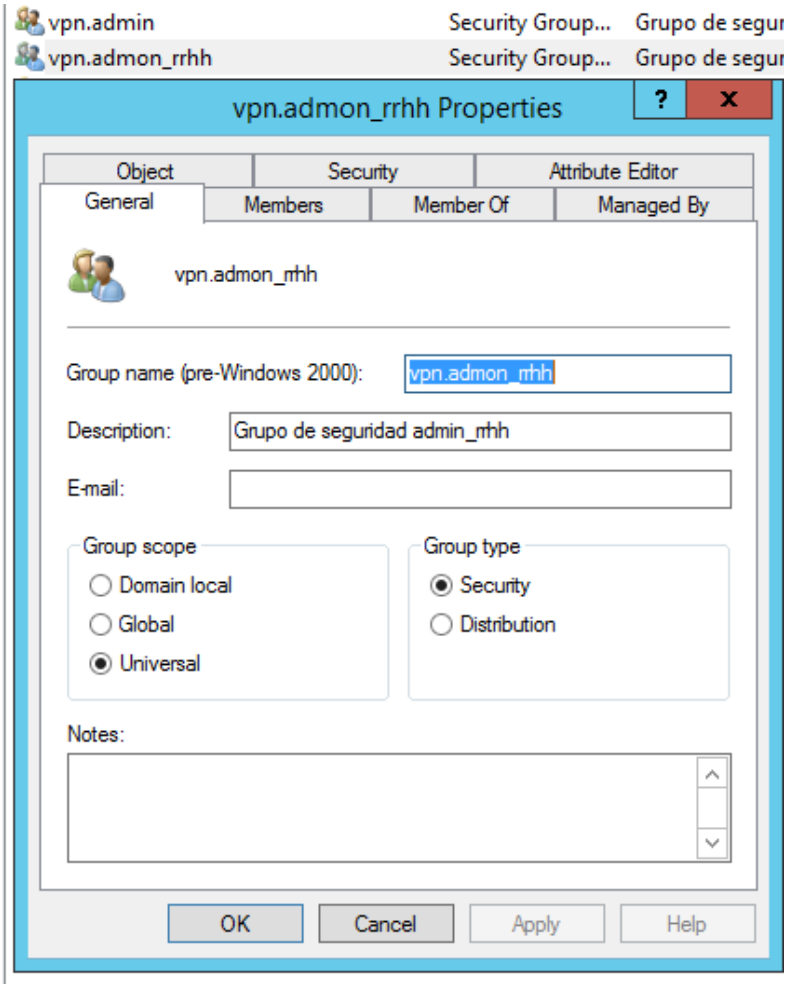

Figura 9: Grupo de seguridad vpn.admon-rrh en Active Directory

Esta configuración enlaza con la seguridad dentro del firewall Pfsense donde configuraremos los servidores de autenticación:

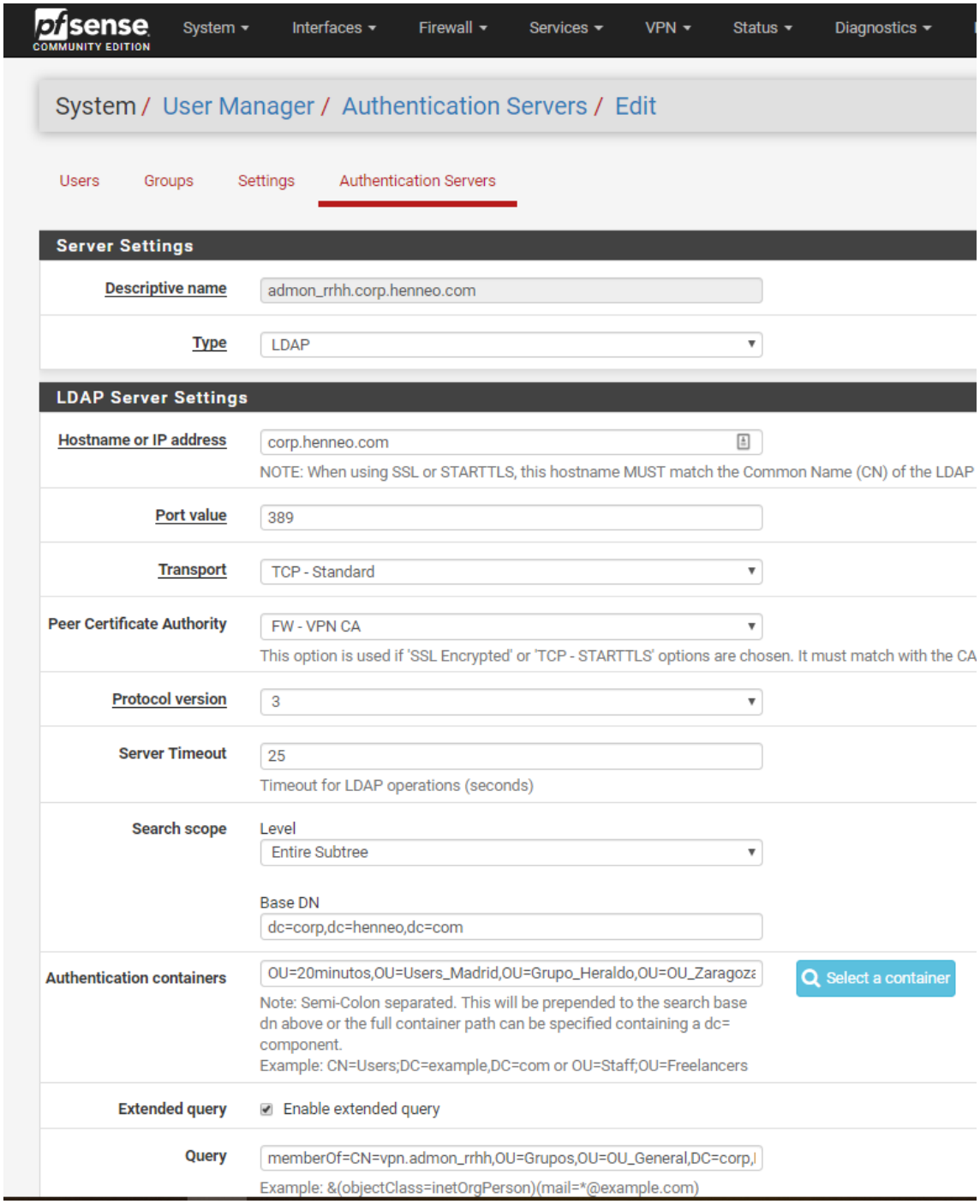

Figura 10: Configuración LDAP autenticación usuarios

En el que un usuario al autenticarse y pertenecer a un grupo de seguridad vpn.admon-rrhh perteneciente a este grupo, el firewall con la query hecha de ldap irá a consultar si ese usuario tiene permiso para ese perfil y si lo tiene establecerá el túnel.

6. Estructura de la red y direccionamiento.

6.1 Estructura de la red

La estructura de la red de la empresa será la siguiente:

Redes	
Red de servidores nueva	192.168.210.0/24
CIFS (almacenamiento de la empresa)	192.168.1.3/32
Red de área local empresa	Planta 0: 192.168.230.0/24
	Planta 1: 192.168.231.0/24
	Planta 2: 192.168.232.0/24
	Planta 3: 192.168.233.0/24
	Planta 4: 192.168.234.0/24
	Planta 5: 192.168.235.0/24
Red de servidores antigua	192.168.0.0/23
Red de gestión (switches, firewall, etc..)	172.16.16.0/24

Tabla 1: Direccionamiento red empresa

Los servidores necesarios para los perfiles de vpn serán los siguientes:

Aplicativo	Servidores
ERP	192.168.210.22/32 (Servidor de Base de datos)
	192.168.210.20/32 (Nodo 1 del ERP)
	192.168.210.21/32 (Nodo 2 del ERP)
Programa de nóminas	192.168.1.177/32 (Servidor del programa)
	192.168.210.25/32 (Servidor de Base de datos)
CIFS	192.168.1.3/32 (Almacenamiento de la empresa)
Sistema editorial	192.168.210.26/32 (Servidor de Base de datos)
	192.168.210.33/32 (Servidor de aplicaciones sistema editorial)
	192.168.210.10/32 (balanceador de carga conexiones al sistema editorial)
	192.168.210.11/32 (servidor 1 conexiones al sistema editorial)
	192.168.210.12/32 (servidor 2 conexiones al sistema editorial)
	192.168.210.28/32 (Servidor de entrada de agencias EFE, AFP, etc…)

Tabla 2: Relación direccionamiento red con aplicativos

Se les da acceso al área local de la empresa porque algunos empleados tienen otro equipo fijo de sobremesa en su puesto de trabajo y así podrán conectar a él para poder trabajar en remoto directamente sobre él.

El sistema editorial es el programa donde los redactores escriben las páginas del periódico y en el que tienen que acceder desde cualquier parte geográfica donde estén cubriendo la noticia para escribirla directamente en el programa.

CIFS es el almacenamiento de la empresa donde está toda la información importante de cada departamento (Excel, powepoints, facturas, etc…) y desde donde se vinculas todas las unidades mapeadas de cada empleado.

6.2 Direccionamiento de la red

El direccionamiento que vamos a utilizar para los distintos perfiles va a ser el siguiente:

vpn.local.resources -> 10.135.0.0/24
vpn.admon-rrhh-> 10.139.0.0/24
vpn.admin-> 10.131.0.0/24
vpn.Prov-ERP-> 10.140.0.0/24

Cada perfil tiene unas redes que tienen que ver, algunas son comunes a varios perfiles:

Perfiles	Red de área local segmentada por plantas del edificio	CIFS (almacenamiento shares)	Programa de nóminas	ERP	Sistema editorial
vpn.local.resources (10.135.0.0/24)	192.168.230.0/24 192.168.231.0/24 192.168.232.0/24 192.168.233.0/24 192.168.234.0/24 192.168.235.0/24	192.168.1.3/32	No	No	192.168.210.26/32 192.168.210.33/32 192.168.210.10/32 192.168.210.11/32 192.168.210.12/32 192.168.210.28/32
vpn.admon-rrhh (10.139.0.0/24)	192.168.230.0/24 192.168.231.0/24 192.168.232.0/24 192.168.233.0/24 192.168.234.0/24 192.168.235.0/24	192.168.1.3/32	192.168.1.177/32 192.168.210.25/32	192.168.210.22/32 192.168.210.20/32 192.168.210.21/32	No
vpn.admin (10.131.0.0/24)	192.168.230.0/24 192.168.231.0/24 192.168.232.0/24 192.168.233.0/24 192.168.234.0/24 192.168.235.0/24	192.168.1.3/32	192.168.1.177/32 192.168.210.25/32	192.168.210.22/32 192.168.210.20/32 192.168.210.21/32	192.168.210.26/32 192.168.210.33/32 192.168.210.10/32 192.168.210.11/32 192.168.210.12/32 192.168.210.28/32
vpn.Prov-ERP (10.140.0.0/24)	No	No	No	192.168.210.22/32 192.168.210.20/32 192.168.210.21/32	No

Tabla 3: Relación direccionamiento perfil con aplicativo empresa

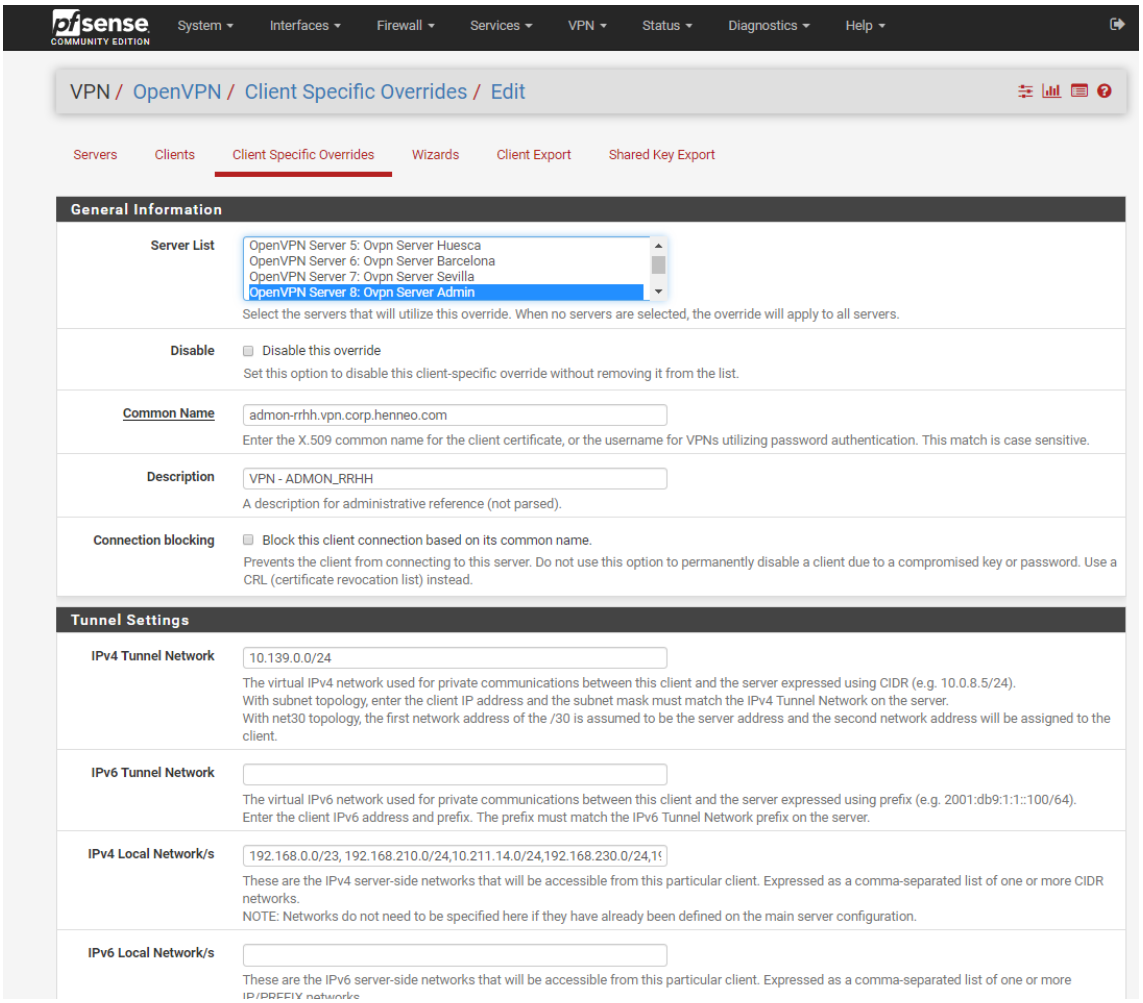

Figura 11: Ejemplo de configuración de direccionamiento de perfil vpn.admin

En esta captura se puede ver la configuración del perfil de vpn.admin, en el campo IPv4 Tunnel Network irá el direccionamiento que le dará al cliente cuando establezca el túnel para este perfil. Además, en IPv4 Local Network/s irán las redes a las cuales tendrán que tener acceso ese perfil de vpn.admin, en este caso tendrá acceso a la toda la red.

7. Configuración del firewall, VPN y cliente

7.1 Configuración del firewall

Dependiendo del perfil vpn que tenga configurado cada empleado, se establecerán una serie de reglas para que se de acceso a lo que necesita cada perfil de empleado.

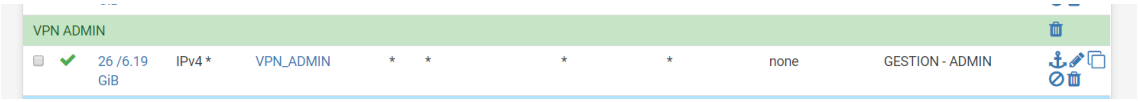

Figura 12: Regla de firewall de perfil vpn.admin

El perfil de admin como podemos ver tendrá acceso a todo, se establecerá acceso a todo desde cualquier origen a cualquier destino, a través de cualquier Gateway y por cualquier puerto.

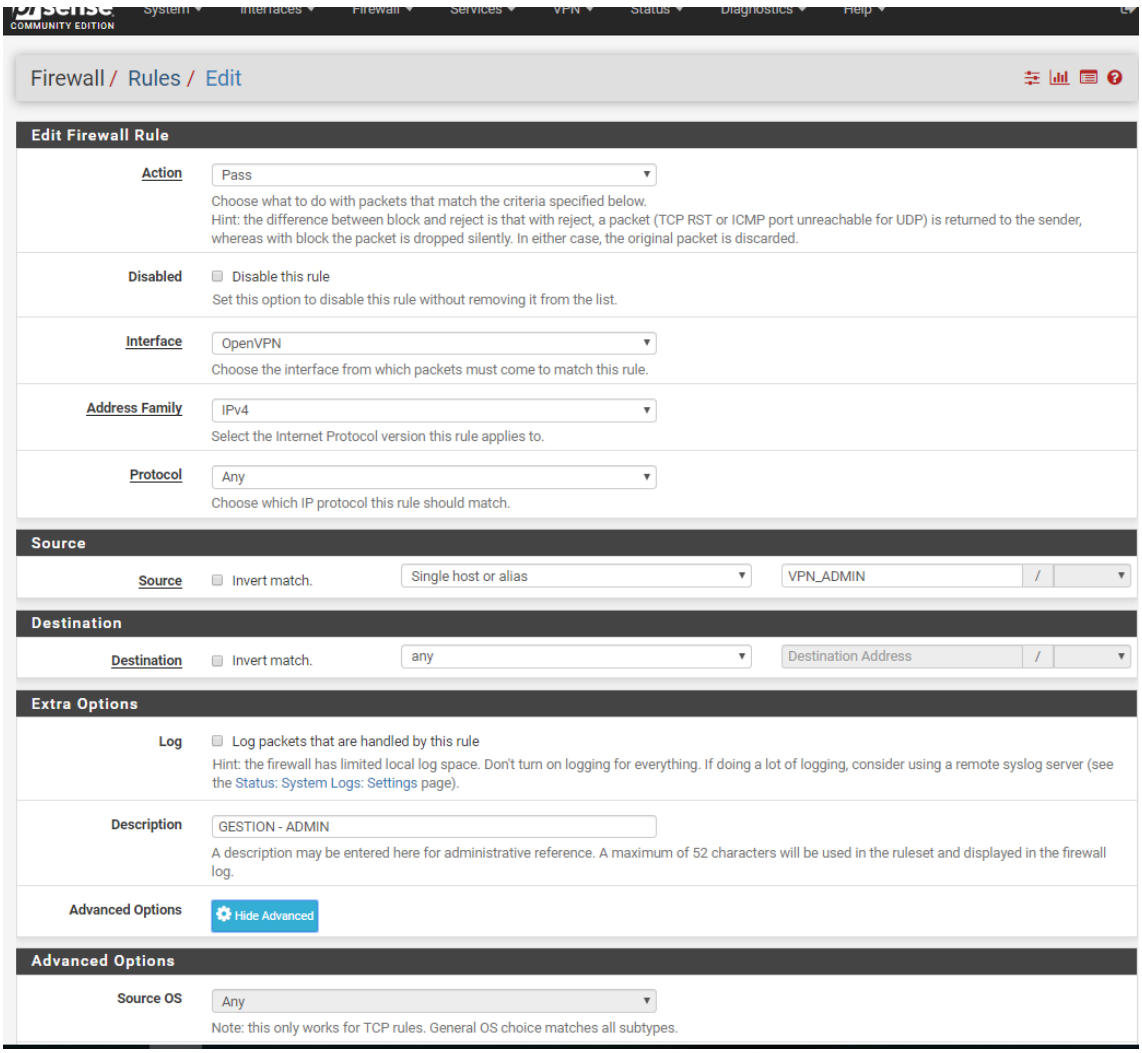

Figura 13: Detalle de regla de firewall de perfil vpn.admin

Seleccionaremos protocolo Ipv4 ya que en toda la empresa se tiene este protocolo implementado y el interfaz OpenVPN configurado previamente exclusivamente para todas las conexiones que se establecerán con el firewall relacionadas con OpenVPN.

Aquí un ejemplo de la regla configurada para permitir desde el perfil vpn.local-resources tener acceso a las unidades mapeadas de almacenamiento en CIFS.

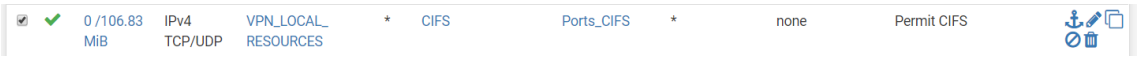

Figura 14: Regla de firewall perfil vpn.local-resources acceso CIFS

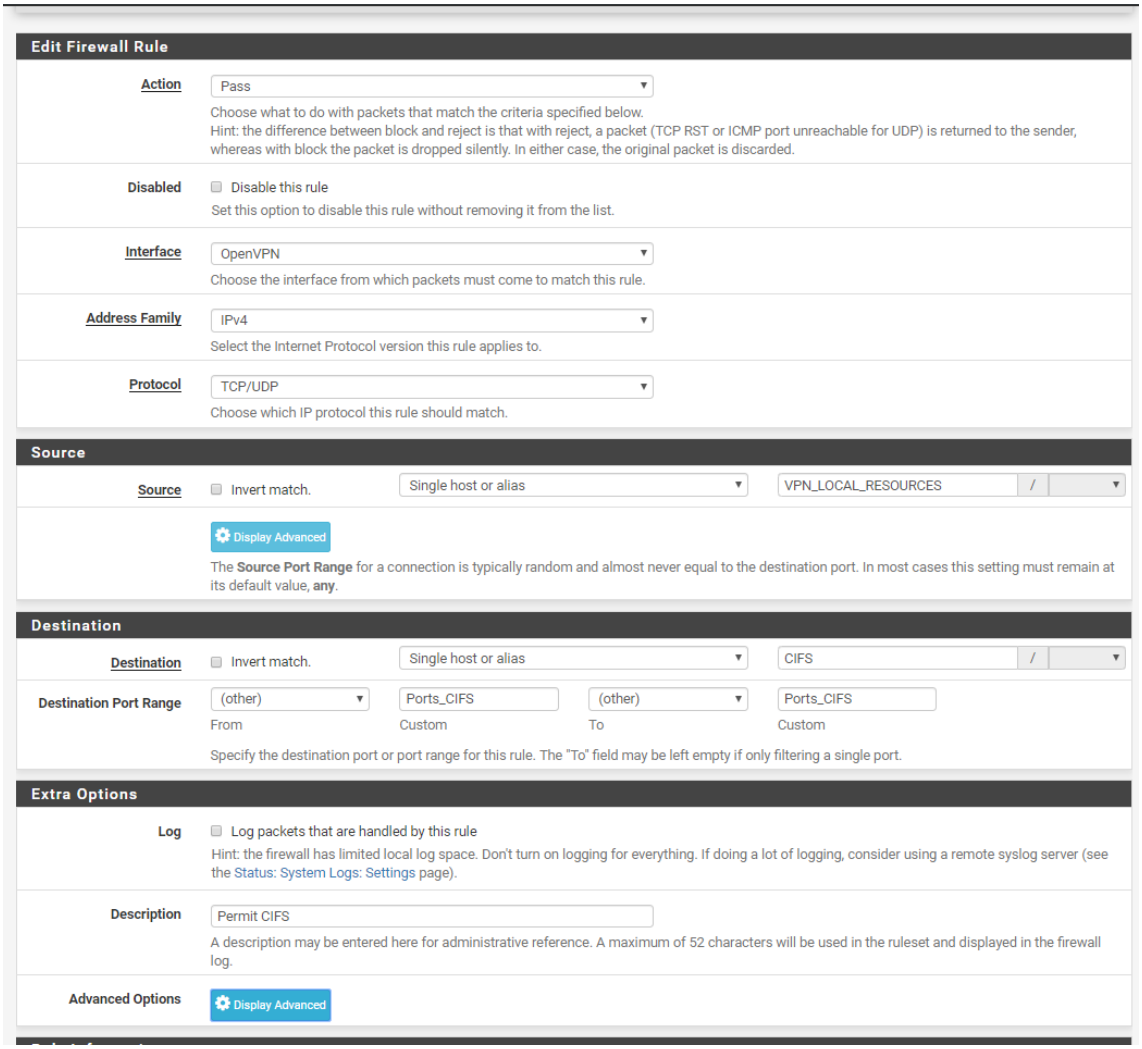

Figura 15: Detalle config regla firewall vpn.local-resources acceso a CIFS

Los alias de Ports_CIFS y CIFS tienen esta configuración:

Figura 16: Alias de CIFS direccionamiento

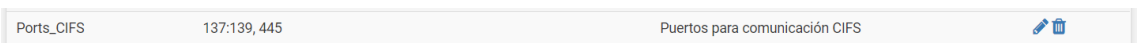

Figura 17: Alias de Ports_CIFS, puertos usados CIFS

Así quedará que cualquier conexión desde VPN_LOCAL_RESOURCES y desde cualquier puerto con destino 192.168.1.3, 192.168.1.1 (Controlador de dominio), 10.211.14.62 (Otro controlador de dominio) y puerto destino 137,138,139 y el 445 y a través de cualquier Gateway se permitirá la conexión desde dentro del túnel vpn con el perfil vpn.local-resources.

7.2 Configuración de la VPN

Lo primero que tenemos que tener en cuenta es que en el servidor de OpenVPN tendrá que tener un certificado de servidor en el que validará la conexión de un cliente si tiene el certificado válido del cliente correspondiente a su perfil de vpn. Además, validará que el usuario cliente que se autentique pertenezca al grupo de seguridad de LDAP de su perfil de vpn.

Vamos a poner el ejemplo siguiente con el servidor OpenVPN del perfil de vpn.local-resources:

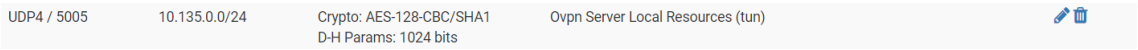

Figura 18: Servidor OpenVPN perfil vpn.local-resources

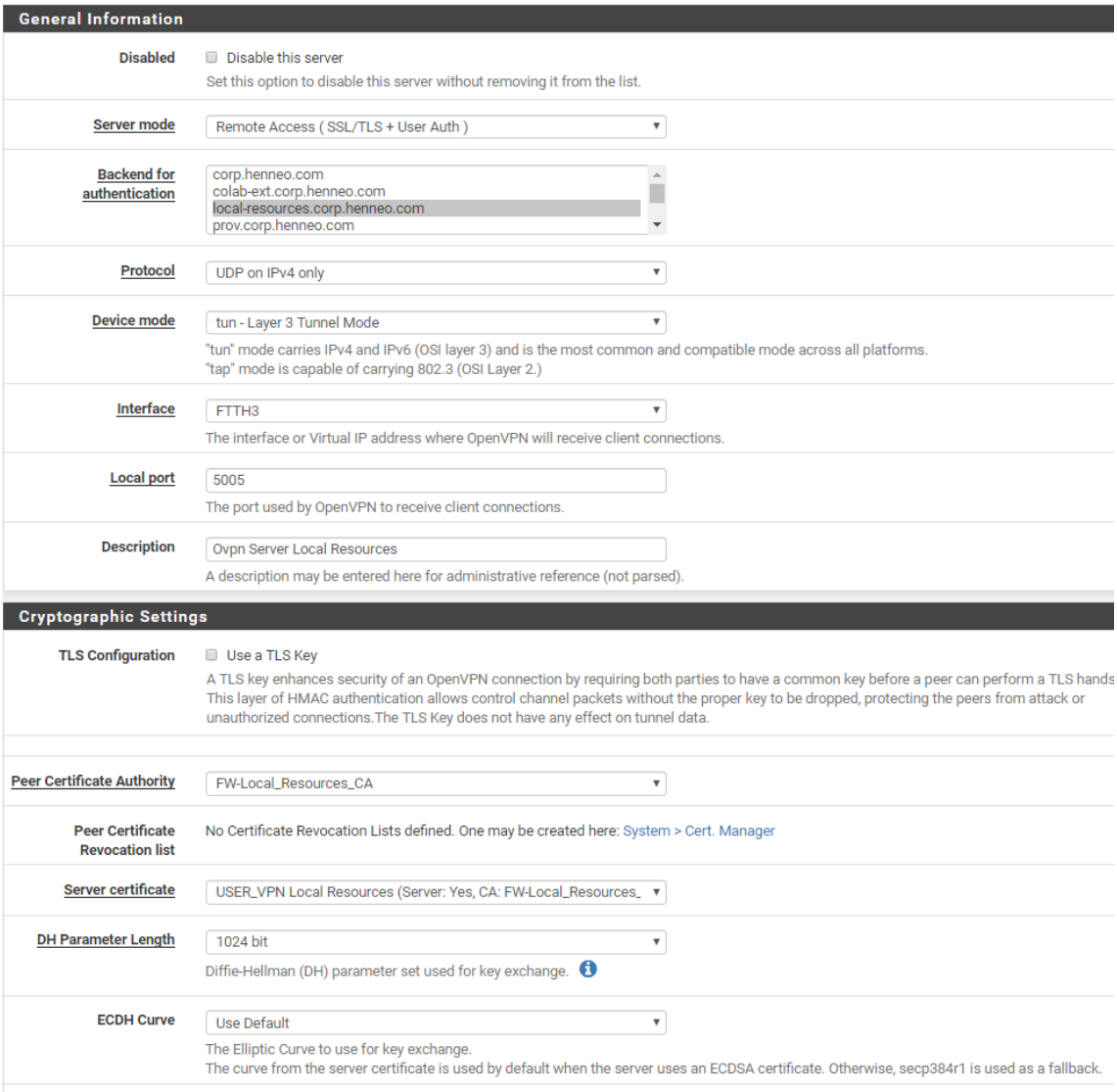

Figura 19: Detalle configuración servidor OpenVPN vpn.local-resources

En esta primera parte de la configuración vemos el tipo de autenticación que tendrá el servidor que será SSL/TLS + Atenticación de usuario a través de LDAP, protocolo UDP sobre Ipv4 y el tipo de controlador TUN (explicado en el punto 3.1) para construir un túnel de capa 3. El interfaz sobre el que recibirá OpenVPN las conexiones clientes será una conexión FTTH con un ISP y el puerto usado por lo clientes VPN (5005).

En la parte de seguridad está la parte del certificado del servidor del perfil VPN.local-resources, la complejidad del intercambio de claves Diffie-Hellman (1024bits).
La configuración del certificado del servidor para este perfil de vpn.local-resources será:

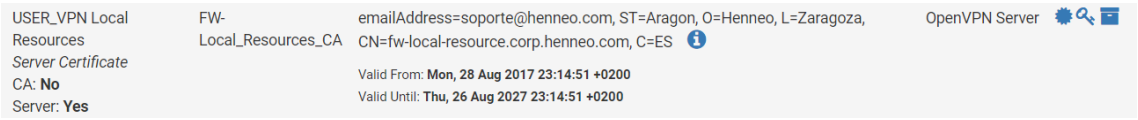

Figura 20: Certificado servidor perfil vpn.local-resources

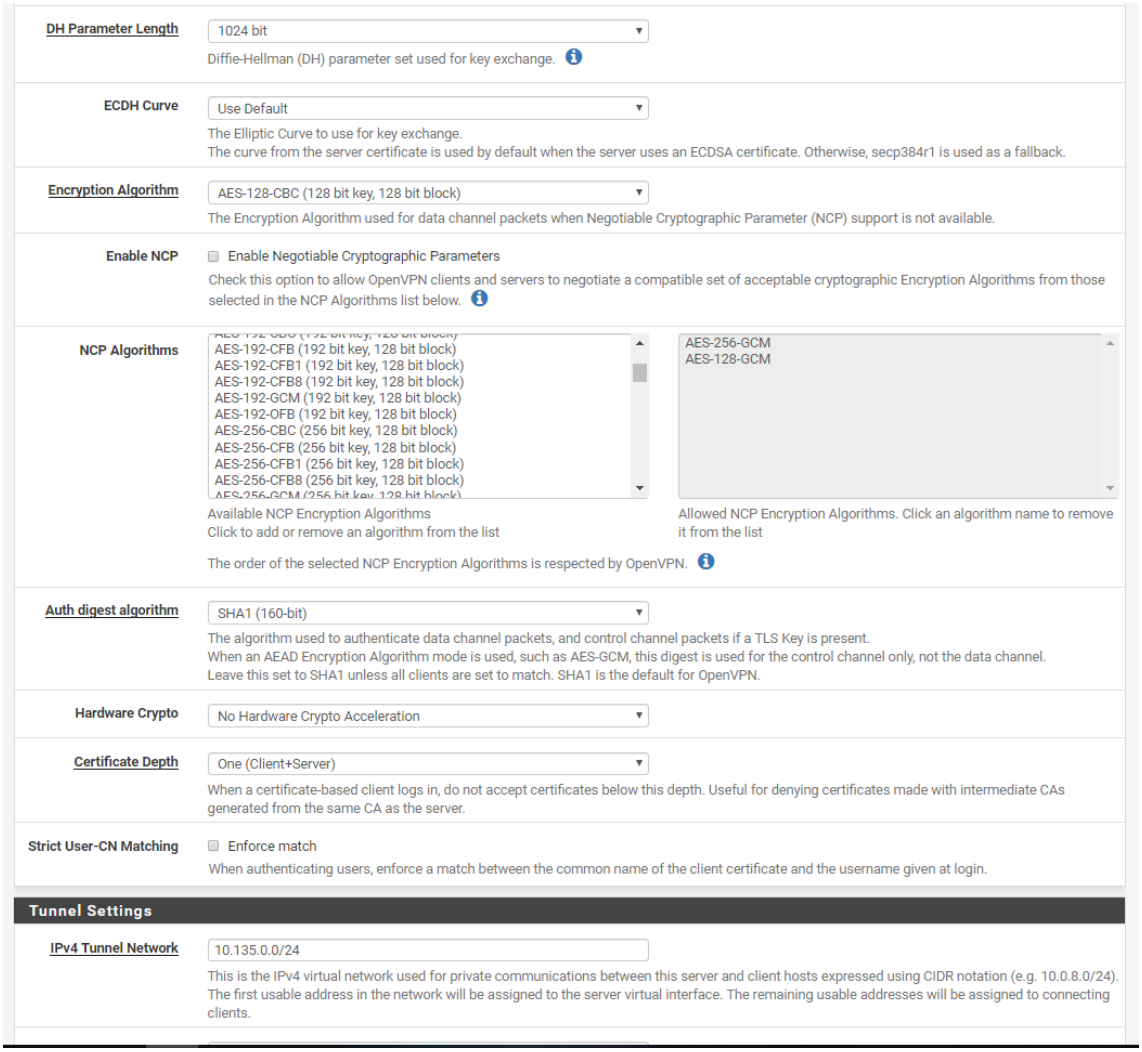

Figura 21: Detalle configuración certificado servidor perfil vpn.local-resources

El tipo de algoritmo de encriptación que será “AES 128 CBC de 128bit”, CBC es el modo de encriptación CBC="Cipher Block Chaining”, ya que ofrece un nivel equilibrado entre lo rápido que trabaja y el nivel de seguridad que ofrece. El algoritmo de autenticación será SHA1 que es el que viene por defecto con OpenVPN.

La profundidad de seguridad del certificado será 1 (cliente más servidor) esto será así porque el cliente llevará el certificado del perfil a validar contra el certificado del servidor del perfil local-resources. También existe más posibilidad como el poner otro servidor intermediador (entidad certificadora) entre el cliente y el servidor que haga las tareas de comprobación de certificados.

La parte de autenticación con LDAP lo describimos brevemente en el anterior punto, aquí lo vamos a desarrollar más poniendo el mismo ejemplo del perfil vpn.local-resources:

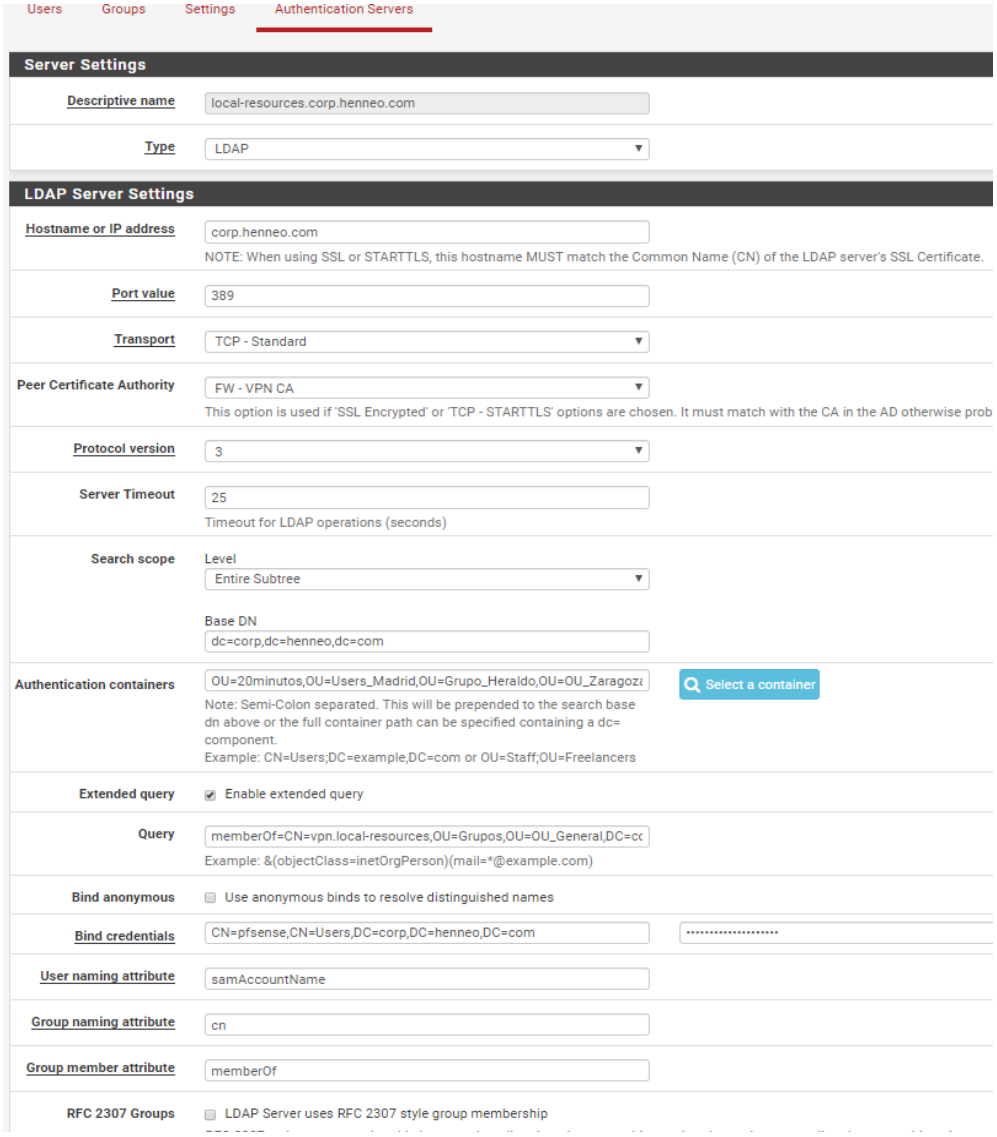

Figura 22: Detalle configuración servidor autenticación perfil LDAP

El tipo de servidor de autenticación de usuarios será LDAP, esto hará que esté todo integrado con el Directorio Activo. El puerto a usar será el 389 que es el propio de LDAP y el protocolo a usar para la autenticación TCP.

La autoridad certificadora para este servidor de autenticación “FW-VPN CA” que es la misma que utilizaremos en todos los demás servidores de autenticación de usuarios.
El timeout del servidor de autenticación por el cual pasará a estado de sleep mientras no se esté usando.

La versión de protocolo de LDAP que se está utilizando, “3” que es la última.
Luego irá el ámbito de búsqueda dentro del árbol del LDAP de nuestro controlador de dominio. Dentro de LDAP le diremos en qué OU (Unidades organizativas) debe realizar la comprobación de los usuarios permitidos y la query de consulta a LDAP que haremos para hacer esa comprobación.

Bind Credentials será el usuario de directorio activo con el que realizaremos la consulta, ya que para hacer cualquier consulta a LDAP se tiene que hacer con un usuario de LDAP que tenga suficientes permisos.

User naming, Group naming y Group member son atributos de cualquier elemento de LDAP con el que se pueden realizar consultas, por ejemplo, saber si existe un elemento con samAccountName: rpomar en el árbol LDAP del dominio y devolverte si existe ese elemento.

7.3 Configuración del cliente VPN

Esta configuración será sencilla ya que se basa principalmente en la asignación de un certificado en el cliente, ponemos el ejemplo del perfil de vpn.local-resources:

Figura 23: Certificado cliente usado en el cliente con perfil vpn.local-resources

En el que vemos las fechas de vigencia del certificado del cliente y que no es el certificado de servidor de ese perfil. La entidad certificadora que emitió el certificado cliente "FW-Local_Resources_CA" y el distinguished name del certificado del cliente.

Figura 24: Configuración cliente VPN vpn.local-resources

Esta es la configuración propia del cliente con el perfil de vpn.local-resources. En ella podemos ver:

- **Dev tun:** el tipo de dispositivo/interfaz TUN que utilizaremos en el túnel, está descrito en el punto 3.2 pero viene a ser que "tun" se utiliza para construir túneles de capa 3.

- **Persist-tun:** es una opción de reinicio del dispositivo utilizado para el túnel. Al reiniciar el cliente VPN, mantendrá abierta la interfaz TUN de esa manera cuando vuelva a renegociar con el servidor VPN chequeará si le está dando la misma dirección IP, si es la misma estará todo ok, pero sino cerrará la interfaz TUN y la volverá a abrir.
- **Persist-key:** con esta opción al reiniciar el cliente vpn no volverá a leer los archivos de claves.
- **Cipher AES-128-CBC:** encripta los paquetes de datos con el algoritmo AES-128-CBC enviados por el cliente en el túnel.
- **Auth SHA1:** Es el algoritmo utilizado para autenticar los paquetes de canales de datos. Es el valor por defecto que tiene OpenVPN.
- **Tls-Client:** Habilita TLS y asume el rol de cliente durante el protocolo de negociación TLS.
- **Client:** Asume el rol de cliente el cliente VPN.
- **Resolv-retry infinite:** Si una resolución de nombre de un host falla, que lo vuelva a reintentar hasta que lo resuelva correctamente.
- **Remote vpn.henneo.com 5005 udp:** será la dirección del interfaz de servidor VPN donde se conectará el cliente, será a través del puerto 5005 y a través del protocolo udp.
- **Setenv opt block-outside-dns:** bloquea los servidores DNS de cualquier otro adaptador de red que utilice el host donde corra el cliente para que no haya problemas de resolución de nombres DNS.
- **Lport 0:** El puerto local del pc utilizado para conexión local, no se utiliza.
- **Verify-x509-name "fw-local-resource.corp.henneo.com" name:** verifica que el certificado del servidor es fw-local-resource.corp.henneo.com.
- **Auth-user-pass:** requiere que el cliente VPN provea un usuario y contraseña.
- **Pkcs12 fw-01-udp-5005-uvpn-local-resource.corp.henneo.com.p12:** le decimos que incluya el archivo pkcs #12 donde está la clave privada local, el certificado local y el certificado raíz de la entidad certificadora (CA).
- **Ns-cert-type server:** Comprueba si el certificado provisto en la conexión es de servidor.
- **Auth-nocache:** No cachea el usuario y contraseña en la memoria virtual del equipo donde corre el cliente VPN.
- **Inactive 3600:** Desconexión del cliente sino hay intercambio de datos en el túnel en 1 hora (3600 segundos).
- **Ping 10:** comprobará a través de un ping si el servidor VPN sigue conectado.
- **Ping-exit 60:** si se usa en servidor y cliente hará que OpenVPN se desconecte en 60 segundos si el servidor o cliente se desconecta.

- **Reneg-sec 0:** que no se renegocie la clave del canal de datos nunca mientras dure la conexión.

Desde la parte de la configuración del servidor VPN en la parte de la configuración avanzada se puede parametrizar también, además de en el cliente VPN como hemos visto, el tiempo de renegociación de la conexión y cuanto tiempo puede estar sin intercambio de datos antes de desconectar el túnel.

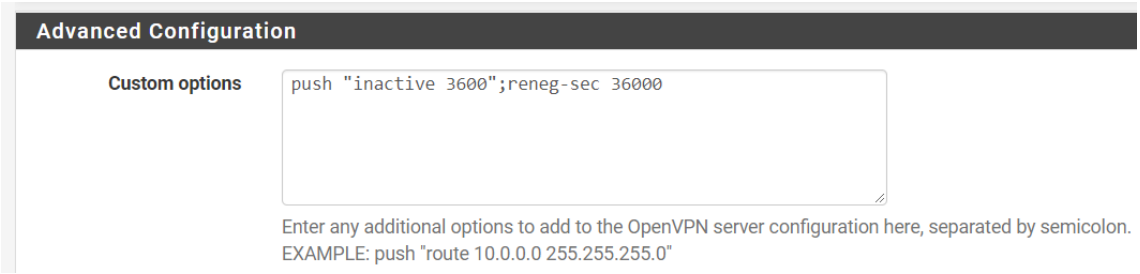

Figura 25: Configuración servidor VPN, detalle configuración parte cliente

Finalmente, tras conectar con el cliente VPN al servidor VPN, nos dará una dirección interna del túnel. El direccionamiento correspondiente respecto al perfil de VPN empleado está detallado en el punto 6.2.

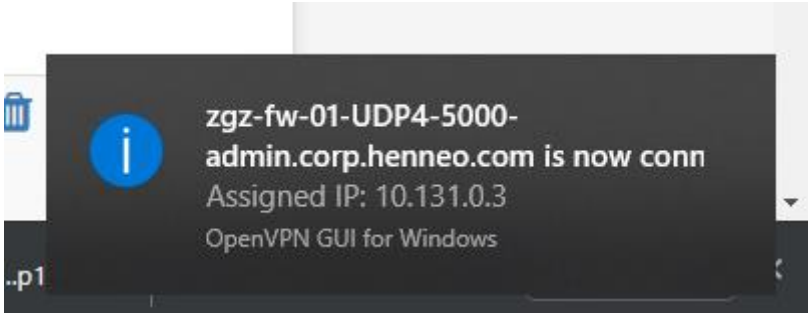

Figura 26: Ejemplo de conexión cliente VPN perfil vpn.admin

8. Conclusiones

Una vez terminada la integración de la red privada virtual, hemos visto que ha sido posible la adecuación de la empresa para que todos los empleados de esta puedan acceder de forma remota y con únicamente una conexión a internet, a la red de la empresa desde cualquier punto geográfico ofreciendo un coste económico muy bajo a la empresa, pero por el contrario un nivel de seguridad alto de la información.

El objetivo general del proyecto era el implantar una red privada virtual de software libre (por temas de coste económico) y podemos decir que se ha cumplido completamente. Se ha visto una comparativa entre distintas soluciones, tanto de pago como de software libre, y nos hemos decantado por la que mejor se adaptaba a nuestras necesidades.

La planificación del proyecto se ha seguido tal como se definió en el diagrama de Gantt, no ha habido problemas a la hora de seguirlo y se ha conseguido llegar a las fechas establecidas. La parte de la integración se hizo en un laboratorio virtual en el que, mediante diversas pruebas, se replicó la implementación de la configuración de OpenVPN sobre una máquina virtual con Pfsense instalado llegando a la conclusión de que la metodología de trabajo fue la correcta.

Se podría ampliar este trabajo mirando el unir diferentes sedes de una empresa sobre una VPN de extremo a extremo con Ipsec posibilitando que tengan visibilidad de todas las sedes como si estuvieran en la misma red con el nivel de seguridad que nos ofrece Ipsec.

9. Glosario

PPTP: (Point to Point Tunneling Protocol) Protocolo de comunicaciones ya en desuso que posibilitaba la creación de túneles VPN.

L2TP: (Layer 2 Tunneling Protocol) Protocolo de mayor seguridad que PPTP, posibilita encriptar tráfico de diferentes protocolos por cualquier canal punto a punto establecido.

IpSec: (Internet Protocol Security) Protocolo para securizar comunicaciones VPN de extremo a extremo sobre el protocolo de Internet IP en el que cifra y autentica cada paquete en un flujo de datos.

VPN: (Virtual Private Network) Red virtual creada para unir dos diferentes redes mediante el establecimiento de un túnel y en el que todo el tráfico de red debe de ir securizado ya que la comunicación viaja a través de internet.

WAN: (Wide Area Network) Red de área amplia, une distintas redes más pequeñas. Un ejemplo de red WAN sería internet ya que está basada en redes WAN.

LAN: (Local Area Network) Red de área local que abarca un área menor que las LAN. Un ejemplo podría ser la red que crea el router de nuestra casa.

Diffie-Hellman: Protocolo de intercambio de claves en el que no hace falta autenticación a través de un medio no seguro.

Active Directory: Integración de servicio de directorio en una red distribuída de ordenadores, normalmente usando el protocolo LDAP.

10. Bibliografía

Enlace Web	Fecha consulta
https://es.wikipedia.org/wiki/Modelo_OSI#Capa_de_red	18/03/2019
https://latam.kaspersky.com/resource-center/definitions/tunneling-protocol	20/03/2019
https://es.vpnmentor.com/blog/diferentes-tipos-de-vpn-y-cuando-usarlas/	22/03/2019
https://www.muycomputerpro.com/2016/03/03/diffie-martin-rsa-cifrado-asimetrico	23/03/2019
http://wiki.elhacker.net/seguridad/criptograf%C3%ADa/algoritmo-diffie-hellman	24/03/2019
https://juncotic.com/rsa-como-funciona-este-algoritmo/	25/03/2019
https://es.wikipedia.org/wiki/Internet_key_exchange	26/03/2019
http://blog.smartekh.com/blog/global-protect-de-palo-alto-networks-proteccion-en-todo-lugar	28/03/2019
https://stackoverflow.com/questions/33121619/is-there-any-difference-between-aes-128-cbc-and-aes-128-encryption	29/04/2019
https://www.privateinternetaccess.com/helpdesk/kb/articles/what-s-the-difference-between-aes-cbc-and-aes-gcm	30/04/2019
https://clouding.io/kb/como-configurar-openvpn-server-con-pfsense/	01/05/2019
https://drivemeca.blogspot.com/2016/03/como-configurar-openvpn-en-pfsense-paso.html	03/05/2019
http://www.3ops.com/implementacion-de-vpn-cliente-servidor-con-openvpn-y-pfsense/	06/05/2019
https://openvpn.net/community-resources/reference-manual-for-openvpn-2-4/	12/05/2019