Trabajo Fin de Grado
Grado en Ingeniería de Tecnologías de Telecomunicación

Tunnel Broker IPv4/IPv6 mediante OpenVPN

Autor: José Luis Peña Higueras
Tutor: Francisco José Fernández Jiménez

Dpto. de Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla

Sevilla, 2019

Trabajo Fin de Grado
Grado en Ingeniería de Tecnologías de Telecomunicación

Tunnel Broker IPv4/IPv6 mediante OpenVPN

Autor:
José Luis Peña Higueras

Tutor:
Francisco José Fernández Jiménez
Profesor Colaborador

Dpto. de Ingeniería Telemática
Escuela Técnica Superior de Ingeniería
Universidad de Sevilla
Sevilla, 2019

Trabajo Fin de Grado: Tunnel Broker IPv4/IPv6 mediante OpenVPN

Autor: José Luis Peña Higueras

Tutor: Francisco José Fernández Jiménez

El tribunal nombrado para juzgar el Trabajo arriba indicado, compuesto por los siguientes miembros:

Presidente:

Vocales:

Secretario:

Acuerdan otorgarle la calificación de:

Sevilla, 2019

El Secretario del Tribunal

A mi familia

A mis maestros

Agradecimientos

En primer lugar, agradecer a mis padres, José Luis Peña Martínez y Francisca Higueras Ruiz por haberme ayudado durante todos los años de carrera y durante la realización de este proyecto. Ellos han estado en los buenos y malos momentos durante el paso por la carrera y me han proporcionado todo lo necesario para poder impartir estos estudios. Además me gustaría agradecer a mi hermano Francisco Javier por el apoyo durante la realización del proyecto.

En segundo lugar, quiero agradecer a todos los profesores que han estado a lo largo de la carrera por darme todo el conocimiento necesario tanto en el ámbito académico como en el ámbito laboral. En especial, me gustaría agradecer a mi profesor Francisco José Fernández Jiménez por toda su ayuda durante todo el proyecto, por haber adaptado su horario a las necesidades que en muchas ocasiones tenía y sobre todo, por la orientación que me ha dado a lo largo de todo el proyecto.

Por último, quiero agradecer a mis amigos por haberme motivado en aquellos momentos de mayor estrés y por su paciencia. Además me gustaría agradecer a "Marina García Vela" por su ayuda a la hora de organizar los formatos del documento.

José Luis Peña Higueras

Sevilla, 2019

Resumen

El uso global de IPv6 es algo inminente ya que se están agotando las direcciones IPv4 que proporciona IANA. IPv6 permite solucionar el problema de asignación de direcciones pudiendo tener direcciones de este tipo en cualquier dispositivo, lo que contribuye a una mejora en las tecnologías como IoT, robótica y domótica.

En este trabajo se presenta una aplicación que hará de Tunnelbroker IPv4/IPv6, proporcionando acceso a la red IPv6 mediante túneles VPN con la herramienta OpenVPN. Esta aplicación puede competir con otros TunnelBrokers como Hurricane, debido a que tiene características parecidas aunque la aplicación propuesta es más configurable tanto a nivel de usuario como de administración.

Tras diversas pruebas realizadas a la aplicación, se llega a la conclusión de que permite una velocidad adecuada, un buen rendimiento y sobre todo, una mayor seguridad debido al cifrado de las comunicaciones.

Abstract

The global use of IPv6 is something imminent because IPv4 adresses, which provide IANA, are running out. IPv6 allows to solve the asignation problem of adresses allowing to have this type in any device, which contributes to an improvement in technologies such as IoT, robotics and domotics.

This project presents an application that will generate a Tunnelbroker IPv4/IPv6, supplying access to the network IPv6 through tunnels VPN with the OpenVPN tool. This platform is meant to compete with other TunnerlBrokers as Hurricane, due to having similar characteristics. However, the application proposed is more configured as user and administrator level.

After various tests made to the application, it is reached to the conclusion that the application permits a suitable speed, a good output and, overall, a greater security due to the ciphered of the comunications.

Índice

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Glosario

IANA	Internet Assigned Numbers Authority	1
LACNIC	Registro de Direcciones de Internet de América Latina y Caribe	1
RIPE	Réseaux IP Européens	1
IoT	Internet of Things	2
VPN	Virtual Private Network	2
S.O	Sistema Operativo	4
RFC	Request for Comments	4
RIR	Regional Internet Registry	21
ARIN	American Registry for Internet Numbers	21
APNIC	Asia-Pacific Network Information Centre	21

1 INTRODUCCIÓN Y OBJETIVOS

En algunas ocasiones, aferrarnos a una zona conocida puede impedirnos adentrarnos en otros espacios de descubrimientos y evolución.

Mario Alonso Puig

1.1 Introducción

En la actualidad, se realiza la siguiente pregunta: ¿Cuándo se implementará IPv6?, Pues es algo más cercano de lo que parece, ya que se están agotando las direcciones IPv4 que puede dar IANA. El agotamiento total de direcciones IPv4 públicas está previsto en el periodo de 2020 a 2021, según indican los últimos estudios. Esta predicción se basa en la disponibilidad de direcciones IPv4 de RIPE, el registro regional a cargo de la asignación de direcciones IP en Europa, que espera que la reserva de direcciones IPv4 se agote en 2021.

¿De dónde viene este problema?, Pues este problema viene por la limitación de IPv4, ya que este tiene limitado el número de direcciones a 2^32, es decir a 4.294.967.296 de direcciones. Cuando se integró IPv4 (en 1983) no se pensó que fuese a tener problemas de dimensionamiento de direcciones, ya que en aquella época no todo el mundo utilizaba la tecnología en su día a día. Pero a día de hoy, el crecimiento poblacional es mucho mayor y el uso de las tecnología se ha generalizado a todos los niveles, tanto de diversidad de dispositivos (teléfonos móviles, tablets, ordenadores, etc.), usuarios (milenials, adultos, jubilados), usos (ocio, profesional, redes sociales, juegos, etc.) y nuevas utilidades (inteligencia artificial, robótica, IoT). Actualmente, la población mundial está alrededor de 7545 millones de personas, por lo que seguir utilizando IPv4 a la larga será inadecuado ya que se llegará a un punto donde no habrá direcciones públicas que asignar.

¿Por qué no se ha realizado aún el cambio?, la respuesta es doble, primero la incertidumbre a que el cambio a IPv6 dé los resultados esperados y segundo el miedo a salir de la zona de confort de los usuarios, familiarizados al uso de IPv4.Otro de los aspectos que frenan a las empresas a la hora de dar este paso, es que no todas las operadoras ofrecen IPv6 y por tanto, las empresas no quieren realizar el cambio por posibles problemas en sus comunicaciones con sus sedes o a nivel de servicios que tengan implementados y las posibles pérdidas económicas.

En la siguiente figura, se muestra un gráfico realizado por LACNIC donde se indica el número de direcciones IPv4 libres disponibles en cada año y el momento exacto donde predicen que se agotará IPv4.

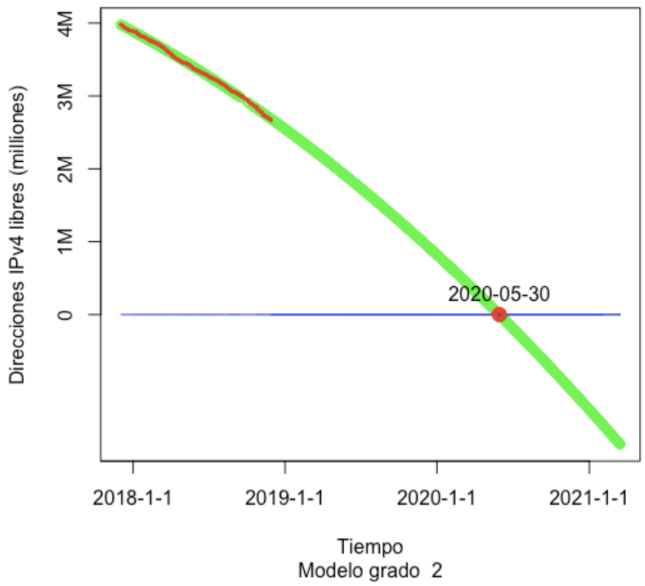


Figura 1-1. Gráfico agotamiento de direcciones [1]

1.2 Motivación

El cambio a IPv6 global será algo que iniciará una nueva era tecnológica ya que no se estará tan limitado a nivel de número de usuarios al tener una tecnología que a día de hoy no es dimensionable.

Según las estimaciones de Gartner, para el año 2020 habrá más de 26 millones de dispositivos IoT conectados a Internet. Además según Cisco, se cree que habrá más de 50 millones de dispositivos conectados en esa fecha. Por esto, la característica principal de este cambio es que ya no se necesitará preocuparse por las direcciones IP que asignar, ya que cualquier dispositivo podrá tener acceso Internet a través de IPv6. Las grandes ventajas del uso de IPv6 son su rendimiento, velocidad y seguridad. Aunque según RIPE, IPv4 es más rápido que IPv6, la diferencia es mínima debido a que el tamaño de datos es mayor en IPv6. Pero esto no quita el buen rendimiento y escalabilidad comparado con el uso de IPv4. Aun así, en un futuro se descubrirán nuevas mejoras para que la velocidad sea superior a IPv4. Actualmente, se está notando ya la evolución de las nuevas tecnologías en nuestro día a día, tanto en IoT, domótica, e incluso robótica. Con el paso a IPv6 será más fácil la conectividad a las actualizaciones de estas tecnologías y esto repercutirá en el mejor bienestar futuro.

Sin embargo, toda evolución requiere un cambio que no todos ven bien, debido a que hay que salir de la zona de confort. Este cambio es necesario y llevará a una revolución tecnológica donde el nivel de vida será mejor. Y usted, ¿se atreve a hacer el cambio?

1.3 Objetivos

El objetivo principal de este proyecto es hacer hincapié en el uso de IPv6 como una opción de presente y futuro. Para ello, el proyecto facilitará poder obtener direccionamiento IPv6 a través el uso de un Tunnel Broker realizado mediante VPN.

Este proyecto se realizará mediante túneles VPN donde se tendrá un cliente VPN que conectará con un servidor VPN, que le proporcionará acceso a la red IPv6 y la posibilidad de navegar a través de Internet IPv6. Esta aplicación puede competir perfectamente con el tunnel bróker actualmente más usado que es Hurricane Electric, debido a que permite al usuario poder configurar el direccionamiento que quiere tener pudiendo ser mediante DHCP (donde el servidor le servirá una dirección del rango de subred) o mediante IP estática. Además de esto, se tendrá un usuario administrador que se encargará de configurar parámetros del servidor VPN que actuará de tunnel bróker, por lo que se podrán configurar parámetros como el direccionamiento de IPv4 e IPv6, número de clientes VPN que puede haber y otros parámetros.

Por todo lo comentado anteriormente, este proyecto tiene como meta proporcionar otra alternativa a aquellos que quieran hacer uso de IPv6. Esta aplicación es más innovadora y más configurable respecto a otras existentes en el mercado como Hurricane Electric.

1.4 Metodología de trabajo

La metodología de trabajo que se ha realizado ha sido mediante la organización de distintas tareas para la ejecución de proyecto. Para una organización adecuada, se ha realizado conjuntamente tareas y comprobaciones buscando una estructura de trabajo adecuada. A continuación se adjuntan las tareas que se han realizado:

- **Investigación**: Se realizó una investigación de los distintos softwares VPN para ver cuál de ellos era el más adecuado, se hizo un estudio intensivo de la configuración de OpenVPN y de algunos aspectos importantes que se verán en el diseño web.
- **Preparación Entorno:** Se verificó el entorno de red que se tenía, si el proveedor de red daba servicio IPv6 y se realizaron pruebas de configuración del router para verificar si se permitía publicar el servicio.
- **Diseño Web y Scripts:** Se diseñó la web y los scripts que se utilizan en el proyecto, haciendo un diseño con el propósito de incluir la generación de certificados para OpenVPN mediante scripts que se ejecutarán a través de la web. A su vez, se diseñó la base de datos del proyecto, con las tablas y las columnas que se desean obtener.
- **Configuración OpenVPN:** Se hizo la configuración del servidor y del cliente, realizándose pruebas con distintos parámetros, con el fin de ver cuales podían ser configurables mediante web.
- **Implementación Web:** Se generó la aplicación completa página a página y script a script. Durante este periodo se configuró el estilo de cada página y el funcionamiento de cada una de ellas.
- **Pruebas:** Se realizaron pruebas de funcionamiento de la aplicación en todo tipo de S.O y en dispositivos móviles. Se generó un escenario de simulación con el software GNS3 para tener un escenario más realista con el que poder comparar. Para ello, se configuró el escenario completo tanto para equipos virtuales como para routers. Para finalizar, con los datos obtenidos de ambos escenarios, se generó un análisis de estos resultados.
- **Mejoras:** Se mejoró la aplicación a nivel de web y a nivel de configuración OpenVPN.
- **Documentación:** Se escribió un documento técnico con el proceso del proyecto.

1.5 Estructura del proyecto

La estructura del proyecto se va a dividir en los siguientes apartados:

- **Estado del arte:** Se introducirán los conceptos fundamentales que albergará el proyecto. Los conceptos fundamentales serán IPv6, VPN y de TunnelBroker IPv4/IPv6.
- **Sistema:** Se explicará el proyecto completo tanto en el aspecto de diseño como de implementación.
- **Pruebas:** Se adjuntarán los datos y pruebas obtenidas a través de gráficos.
- **Conclusiones y líneas futuras:** Se expondrán las conclusiones obtenidas tras la realización del proyecto así como las mejoras en futuro para un mayor rendimiento.

2 ESTADO DEL ARTE

Es un pequeño paso para un hombre, pero un gran salto para la humanidad.

Neil Armstrong

En ese apartado se van a introducir los conceptos más importantes para entender el funcionamiento y el fin de este proyecto. Esta sección se dividirá en tres apartados fundamentales: Introducción a IPv6, Túneles VPN y Tunnel broker IPv4/IPv6.

En primer lugar, se realizará una introducción teórica de los conceptos más importantes de IPv6, así mismo se mostrarán las diferencias respecto a IPv4 y el uso en la actualidad de IPv6.

En el segundo apartado, se abordará el concepto de Túnel VPN que es un término muy utilizado en numerosas empresas, así como sus características con el fin de introducir la herramienta OpenVPN.

Por último, se trabajará el concepto teórico de Tunnel Broker IPv4/IPv6 con sus características y el uso actual, todo ello con el fin de introducir la herramienta "Hurricane Tunnel Broker".

2.1. Introducción IPv6

El Protocolo de Internet versión 6 (*Internet Protocol version 6* o *IPv6*), es una versión del Internet Protocol (IP), definida en el RFC 2460 y diseñada para reemplazar a Internet Protocol versión 4 (IPv4) RFC 791. [2]

2.1.1 Características de IPv6

Las principales características de IPv6 son [3]:

- Capacidades de direccionamiento extendidas a 128 bits que provee una gran cantidad de direcciones IP, con la posibilidad de asignar direcciones únicas globales a nuevos dispositivos.
- Autoconfiguración y reconfiguración automáticas que permiten que los nodos de la red IPv6 configuren sus propias direcciones IPv6, facilitando su uso.
- La transición entre proveedores de IPv6 es transparente para los usuarios finales con el mecanismo de renumerado.
- Infraestructura de direcciones y enrutamiento eficaz y jerárquica.
- Mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de nuestro ordenador de redes IPv6 y, por tanto, el poder viajar con él sin necesitar otra aplicación que nos permita que ese enchufe/desenchufe se pueda hacer directamente.
- Seguridad Integrada (IPsec): IPv6 incluye IPsec, que permite la autenticación y la encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello.

- Capacidad de ampliación: el encabezado de IPv6 es más eficiente que el de IPv4: tiene menos campos y se elimina la suma de verificación del encabezado.
- Calidad del servicio: Puede hacerse diferenciación de tráfico utilizando los campos del encabezado.
- Velocidad.

2.1.2 Tipos de direcciones IPv6

Se pueden distinguir varios tipos de direcciones IPv6, las cuales se analizarán a continuación [4]:

- Unicast: 1-1
    - Globales: (2000::/3) Dirección utilizable para el encaminamiento.
    - Locales al enlace: (FE80::/10) Dirección encaminable dentro de un área limitada, no a Internet.
    - Locales a la ubicación (Obsoletas): (FEC0::/10) Son como direcciones privadas en IPv6.
    - Compatibles con IPv4 (En desuso): (Prefijo::/96) Para la formación de túneles automáticos.
- Anycast: 1-Más cercano: Dirección asignada a varias interfaces de routers distintos. No debe usarse como dirección origen, ni por un sistema final (host).
- Multicast: 1-N (FF00:/8): Dirección asignada a varias interfaces de equipos distintos. La difusión en IPv6 no existe y se sustituye por multicast limitado a la dirección de multicast.
    - Direcciones reservadas:
        - FF01::1: todas las interfaces del nodo.
        - FF02::1: todos los nodos del enlace.
        - FF02::2: todos los routers del enlace.
        - FF02::9: todos los routers RIP del enlace.
        - FF05::1:3: todos los servidores DHCP en la red local.
    - Dirección multicast de nodo solicitado: Dirección multicast que sólo escucha un nodo concreto (FF02::1:FFXX:XXXX, donde XX:XXXX tomadas de los 24 bits menos significativos del Identificador de Interfaz).
- Reservadas:
    - "::": No especificada (todo ceros), Cuando no se sabe cuál es la propia (al pedir dirección con DHCP), No debe asignarse a ninguna interfaz, ni será encaminada por los routers.
    - "::1" : Autodirección, equivalente a 127.0.0.1 en IPv4.

Las direcciones que se tienen que asignar a un equipo y a un router se muestran a continuación [4]:

HOST	ROUTER
Dirección unicast Global	Todas las direcciones que tiene el HOST
Dirección local al enlace (de autoconfiguración)	Dirección multicast "a todos los routers"
Dirección de bucle (autodirección o loopback)	Dirección anycast de las subredes en las interfaces en las que actúa de router
Dirección multicast "a todos los nodos"	anycast que tenga configuradas
Dirección multicast solicitada para cada unicast y anycast que tenga	

Direcciones multicast de los grupos a los que pertenezca	

Tabla 2-1. Direcciones de un host – Direcciones de un router

2.1.3 Diferencias entre Ipv4 e Ipv6

A continuación, se van a estudiar las diferencias existentes entre IPv4 e IPv6, destacando las ventajas e inconvenientes de utilizar cada uno:

Característica	*IPv4*	*IPv6*
Numero de bits	32	128
Numero de direcciones	2^32=4294967296	2^128= 3.4028237e+38
Representación	4 valores numéricos separados por "."	8 secciones con 4 valores hexadecimales separados por ":"
Cabecera IP	20 Bytes	40 Bytes
Fragmentación	Se realiza en hosts y routers	Se realiza solo en hosts
Solicitud ARP	Se utiliza para resolver la dirección MAC de una IPv4	En ICMPv6, se utilizan mensajes de establecimiento de vecindades (*Neigbour discovery*)
Descubrimiento de Router	Se proporciona con el protocolo ICMP Router Discovery que se usa de forma opcional. No realiza autoconfiguración en el equipo final.	En ICMPv6 se utilizan mensajes de solicitud y anuncio de router que contienen la IP del router y máscara (no hace falta configurarlo en el equipo final) y MAC del router (se ahorra un ciclo ARP)
Detección de direcciones duplicadas	Se utiliza ARP Gratuito	En ICMPv6, se utilizan mensajes de descubrimiento de direcciones duplicadas (DAD)
Mensaje de redirección a otro router	Se utiliza ICMP Redirect	En ICMPv6, se utilizan mensajes de redirección un router o destino(si éste está en el mismo enlace) mejores
Gestión de grupos Multicast	Se utiliza IGMP	En ICMPv6, se utilizan mensajes de descubrimiento de destinos multicast
Descubrimiento de MTU	Si se encuentra un enlace con MTU menor que el paquete, el router fragmenta, pero la MTU mínima es mucho menor (64 octetos). La MTU mínima que el enlace debe soportar es de 576 bytes.	La MTU mínima que el enlace debe soportar es de 1280 octetos. Si se desea mandar paquetes > 1280 octetos, se envía el paquete, si llega a un enlace que es demasiado grande, rebotará con un mensaje "paquete demasiado grande" indicando la MTU de ese enlace, se aprende la MTU y se reintenta hasta

		que cuela
DNS	Utiliza registros A para búsquedas directas y PTR para búsquedas inversas	Utiliza registros AAAA para búsquedas directas y PTR para búsquedas inversas
DHCP	Utiliza DHCP para direcciones IPv4	Utiliza DHCP para direcciones IPv6
Encaminamiento	Utiliza BGP, RIP y OSPF	Utiliza RIPng y OSPFv3

Tabla 2-2. Diferencias IPv4–IPv6

2.1.4 Transporte de IPv6 sobre IPv4

Para el transporte de IPv6 sobre IPv4 se suele utilizar tunelización. La tunelización es una familia de técnicas que encapsulan el paquete IPv6 en IPv4, con o sin cabecera GRE (cambia el protocolo encapsulado en IPv4). Los tipos de tunelado que se tienen son: [4]

- Manual.
- Semiautomático.
- Automático.

2.1.4.1 Tunelado Manual

El tunelado manual permite interconectar redes IPv6 a través de una red IPv4 configurando un nodo dual en cada extremo del túnel, donde se configuran las direcciones IPv4 e IPv6 tanto locales como remotas.

Dentro del tunelado manual se usarán las siguientes técnicas:

- IPv6-in-IPv4: Usado entre ambos puntos y que requiere la configuración de las direcciones de origen y destino del túnel.

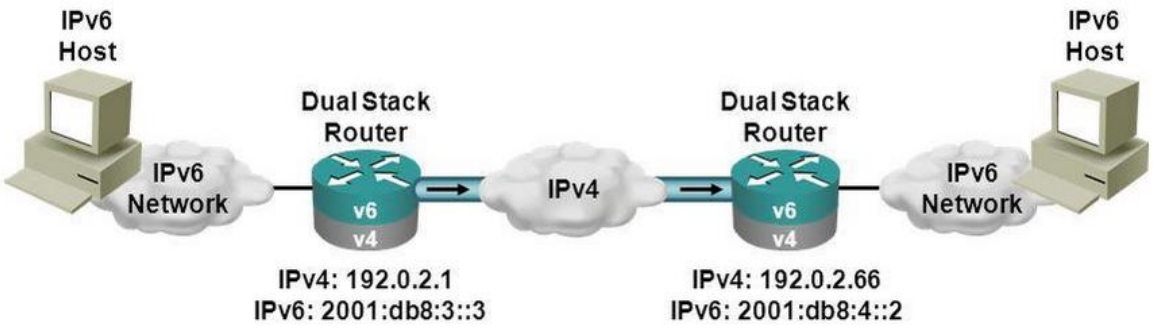


Figura 2-1. IPv6-in-IPv4 [5]

- IPv6 over GRE (*Generic routing encapsulation*): GRE es un protocolo de unidifusión que ofrece las ventajas de encapsular el tráfico de difusión y multidifusión (protocolos de enrutamiento o enrutamiento de multidifusión), u otros protocolos no IP y de estar protegido por IPsec. Para utilizar esta técnica se necesita:
  - Configurar las direcciones de pila dual IPv4 e IPv6 en la interfaz del túnel GRE
  - Identificar la entrada y salida del túnel con direcciones IPv4
  - Requiere usar el protocolo IS-IS manualmente.

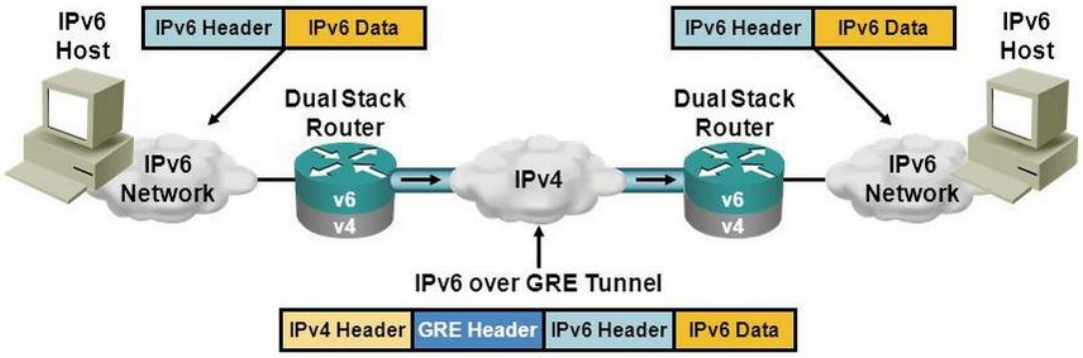


Figura 2-2. IPv6 over GRE [5]

- VPN.

2.1.4.2 Tunelado Automático

El tunelado automático permite a nodos duales comunicarse a través de una infraestructura IPv4. Para ello se utilizarán las siguientes técnicas:

- 6to4: Su principal aplicación es unir redes IPv6 dispersas en una red IPv4. Las características de esta técnica son las siguientes:
  - A cada red IPv6 se le asigna un prefijo IPv6: "2002:<Dirección IP Router Frontera>::/48".
  - El siguiente salto IPv4 está contenido en la dirección IPv6.
  - El encaminamiento entre las distintas redes Ipv6 se apoya en el encaminamiento IPv4 subyacente (por debajo de este).

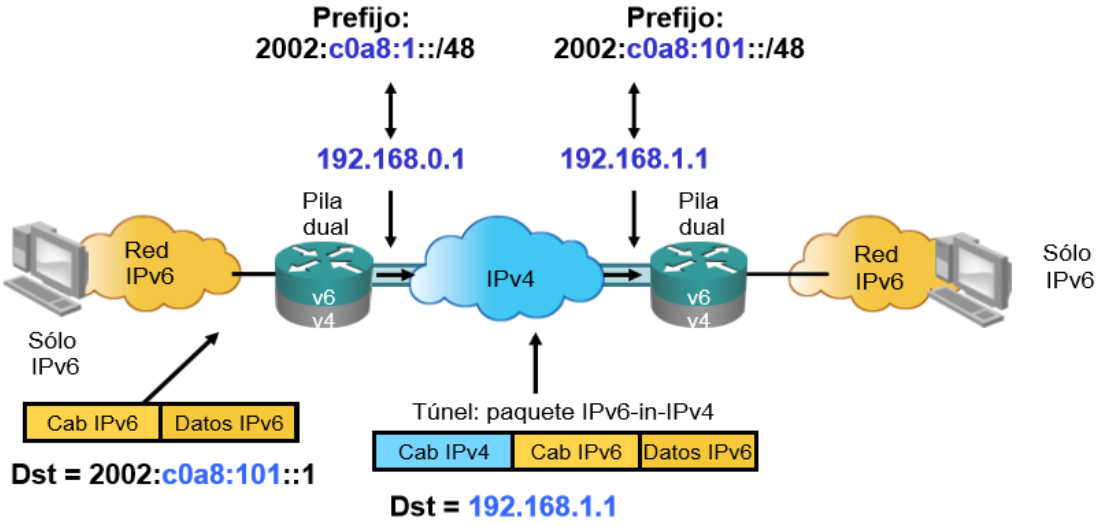


Figura 2-3. 6to4 [4]

- ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*): Permite migrar a IPv6 los sistemas finales de una red privada sin routers IPv6. Las características son:
  - Conexión al exterior requieren routers pasarela IPv6 o ISATAP.
  - Encapsula la dirección IPv4 en el EUI-64.
    - IPv6: "<Prefijo /64>: 0:5efe:<Ipv4/32>".
    - Ejemplo: "XXXX:XXXX:XXXX:XXXX:0000:5EFE:a.b.c.d", donde a.b.c.d es la dirección IPv4 del router ISATAP.

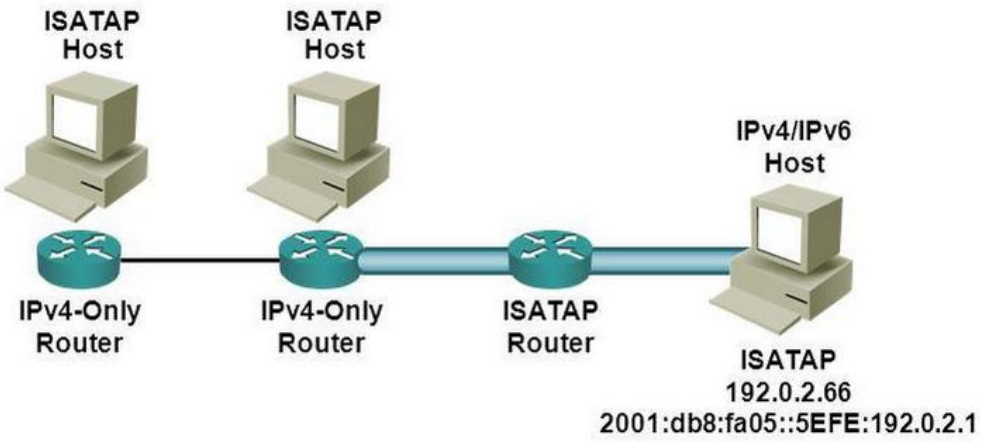


Figura 2-4. ISATAP [5]

- Teredo: Es una tecnología de transición IPV6-IPv4 que permite la tunelización automática de IPv6 entre los hosts que se encuentran a través de NAT de IPv4.Las características de Teredo son:
    - Encapsular IPv6 en (IPv4 + UDP, llamado Paquete burbuja (bubble)), sorteando así el NAT.

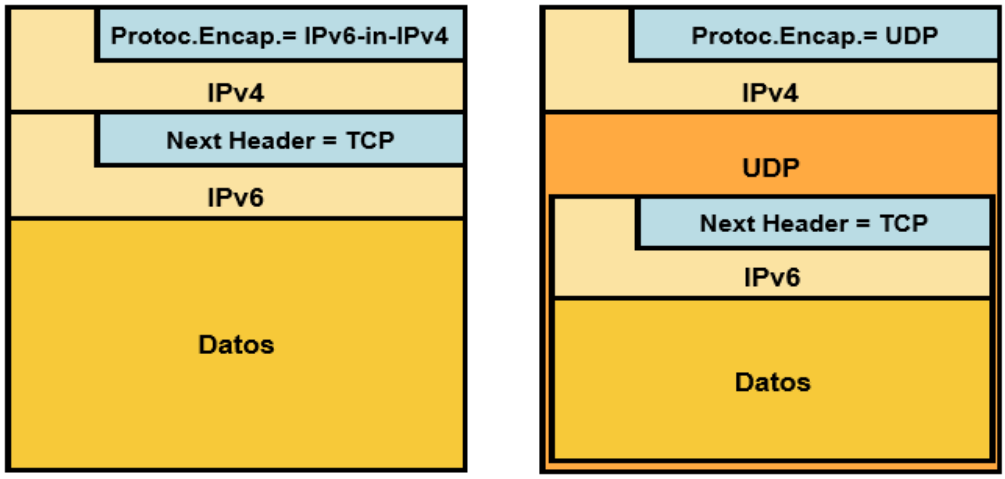


Figura 2-5. Encapsulación Teredo [4]

    - En flujos entrantes a la zona tras el NAT, envía primero un paquete de sondeo al que el host Teredo responde, abriendo así un puerto del NAT.
    - Último recurso: evidentes problemas de seguridad.
    - Direcciones: incorporan datos de NAT.

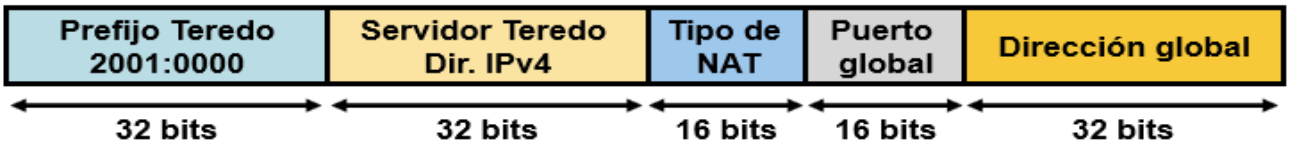
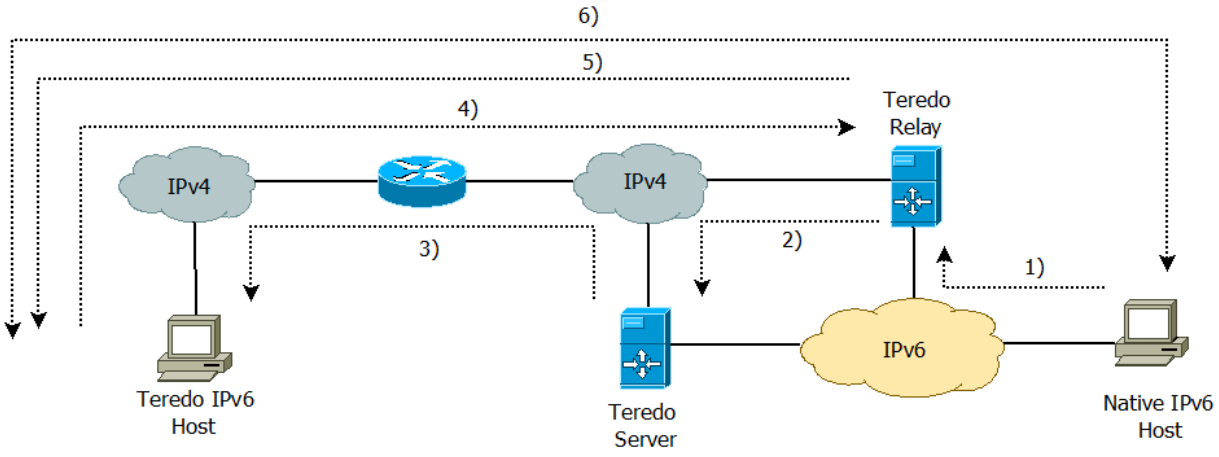


Figura 2-6. Formato de dirección IPv6 Teredo [4]



1) Teredo Relay no tiene una entrada para el host Teredo, por lo que pone en cola el paquete
2) Teredo Relay envía un paquete burbuja (bubble) al servidor Teredo
3) El servidor Teredo reenvía el paquete de burbuja al host Teredo, que contiene la dirección IPv4 del Teredo Rely.
4) El host de Teredo envía el paquete de burbujas de vuelta al Teredo Rely (abre un agujero en el NAT).
5) Teredo Rely transmite el paquete original al host Teredo
6) Los paquetes subsiguientes fluyen directamente

Figura 2-7. Funcionamiento Teredo

2.1.4.3 Tunelado Semiautomático

El tunelado semiautomático permite interconectar redes IPv6 a través de una red IPv4 configurando para ello, nodos en cada extremo del túnel y a su vez, utilizando características del tunelado automático. El tunelado semiautomático más común es Tunnel Broker que se verá en los siguientes apartados.

2.1.5 Uso actual

El 4 de febrero de 2008 se añade a los servidores raíz de la red (*Master Address books*) direcciones en IP versión 6 (IPv6). Esto significa que por primera vez las máquinas que utilicen IPv6 pueden encontrarse la una a la otra sin la participación de toda la tecnología IPv4 [2]. Desde ese momento hasta ahora, ha ido aumentado considerablemente el uso de IPv6. A continuación, se muestra un gráfico con el aumento que ha habido de la adopción de IPv6:

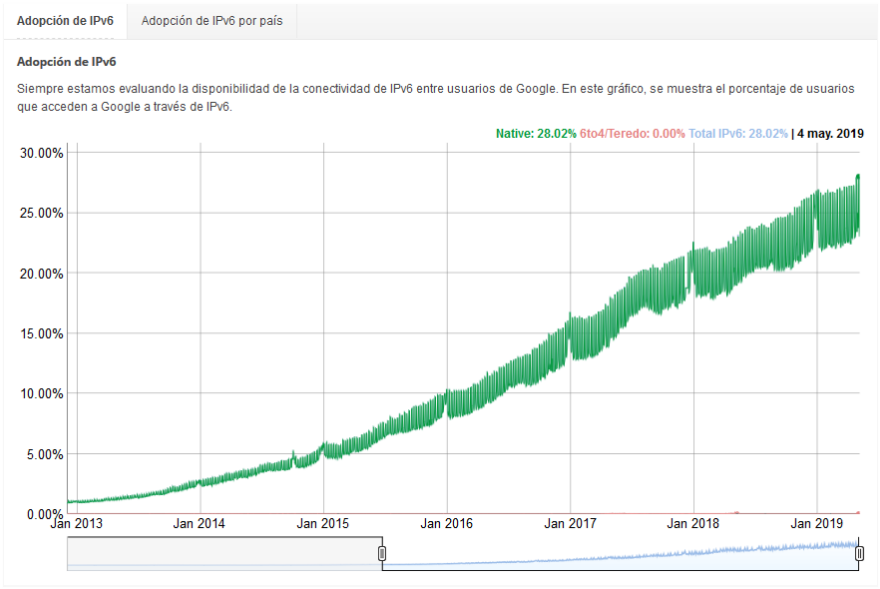


Figura 2-8. Adopción IPv6 [6]

Se puede ver a través del gráfico que el día 4 de Mayo se superó de nuevo el porcentaje de usuarios que utilizan IPv6 hasta el 28.02%. Esto es un gran paso para el cambio que se realizará más adelante.

Además, se puede observar que grandes potencias como EEUU o Alemania han promovido el uso de IPv6. Se puede ver a continuación dos gráficos donde se encontrarán el uso mundial de IPv6 y en Europa.

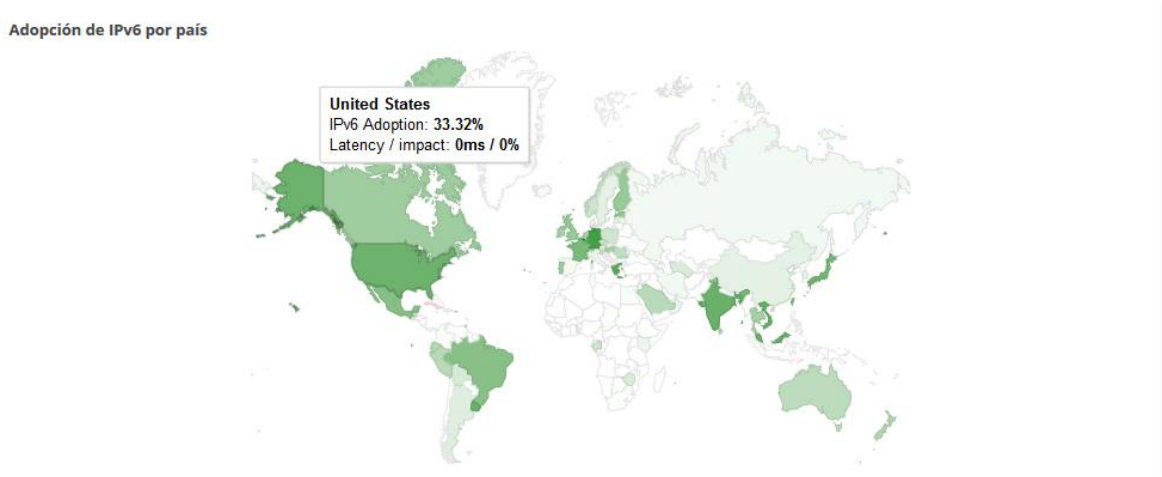


Figura 2-9. Adopción IPv6 Mundial [6]

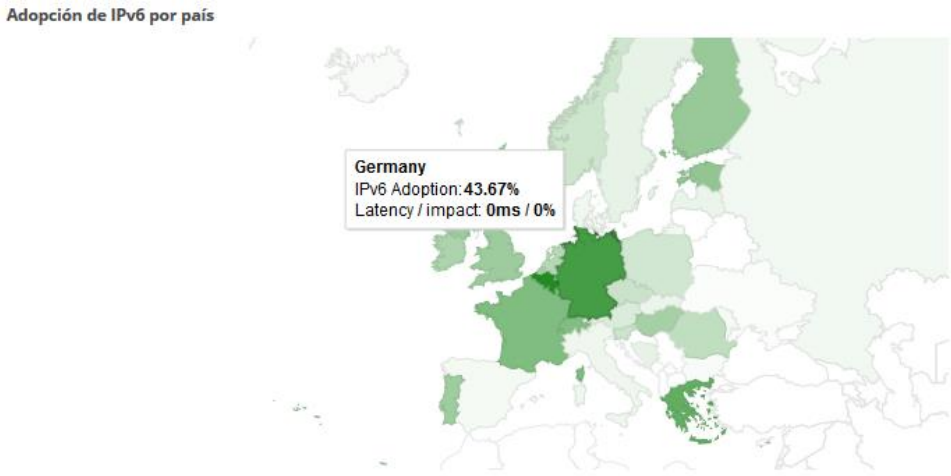


Figura 2-10. Adopción IPv6 Europa [6]

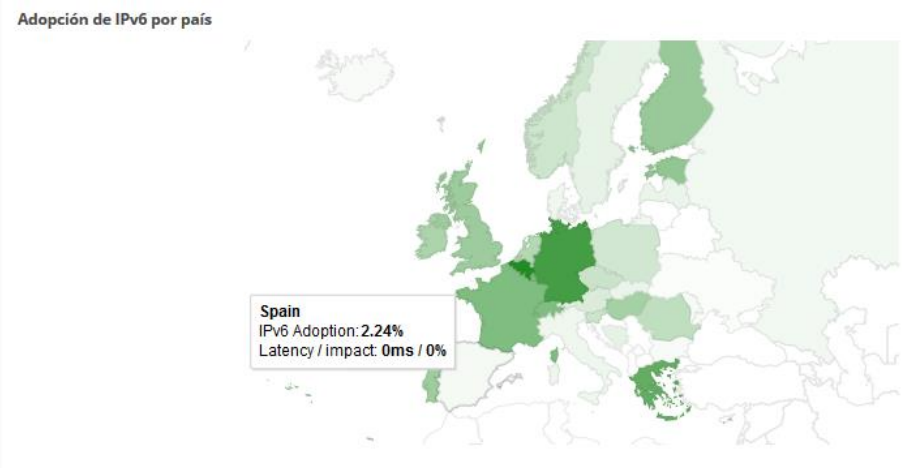


Figura 2-11. Adopción IPv6 España [6]

Como se puede observar la adopción en España es del 2.24 %, un porcentaje muy bajo comparado con Alemania (43.67%) o EEUU (33.32%). Aún es muy baja como en otros países de la Unión Europea. Se tiene que ir realizando el cambio poco a poco, pero ir adoptando estas medidas, ya que tarde o temprano no habrá direcciones IPv4 públicas que asignar y entonces se tendrá que realizar un cambio repentino que puede costar perdidas a las empresas por caídas en la red o en las comunicaciones.

La saturación total de direcciones IPv4 está prevista para el periodo 2020 a 2021, según indican los últimos estudios. Esta predicción se basa en la disponibilidad de direcciones IPv4 de RIPE, el registro regional a cargo de la asignación de direcciones IP en Europa, que espera que la reserva de direcciones IPv4 se agote en 2021. Cuando llegue esta fecha, las empresas de alojamiento no tendrán más remedio que recurrir a IPv6, lo que provocará una bifurcación de Internet en sitios IPv4 y sitios IPv6. El resultado será que los proveedores de servicios de Internet (ISP) que no ofrecen IPv6, se verán obligados a negar a sus clientes el uso de una parte de la web [7].

Todo está preparado para acelerar la transición de IPv6. La escasez de direcciones IPv4 está provocando un aumento en su coste, mientras que las direcciones IPv6 son gratuitas. Además, los fabricantes de dispositivos que desarrollan aplicaciones de IoT están optando por IPv6, ya que cada objeto debe tener su propia dirección IP [7].

2.2 VPN

VPN (*Virtual Private Network*) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada. Esto se realiza estableciendo una conexión virtual punto a punto mediante el uso de conexiones dedicadas, cifrado o la combinación de ambos métodos [8].

2.2.1 Características

Se pueden distinguir de los túneles VPN las siguientes características generales, donde algunas pueden ser configurables [8]:

- Fácil de usar.
- Autentificación y autorización: Usuario/equipo y qué nivel de acceso debe tener.
- Integridad de que los datos enviados no han sido alterados.
- Confidencialidad/Privacidad: Solamente puede ser interpretada por los destinatarios de la misma.
- No repudio: Un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.
- Control de acceso: Se trata de asegurar que los participantes autentificados tienen acceso únicamente a los datos a los que están autorizados.
- Auditoría y registro de actividades: Se trata de asegurar el correcto funcionamiento y la capacidad de recuperación.
- Calidad del servicio: Se tendrá que asegurar un buen rendimiento.
- Reducción de los costes en comunicación.
- Proporciona comunicaciones seguras con derechos de acceso específicos para los usuarios individuales, como empleados, contratistas, etc.
- Mejora de la productividad al extender la red empresarial y sus aplicaciones.

2.2.2 Tipos de VPN

Se pueden distinguir los siguientes tipos de VPN:

- VPN de Acceso Remoto.
- VPN Punto a Punto/ Sitio a Sitio.

- VPN interna (over LAN).

2.2.2.1 VPN de Acceso Remoto

Consiste en usuarios que se conectan a una empresa desde sitios remotos utilizando Internet, como vínculo de acceso. Una vez autenticados tienen un nivel de acceso similar a estar dentro de la red local.

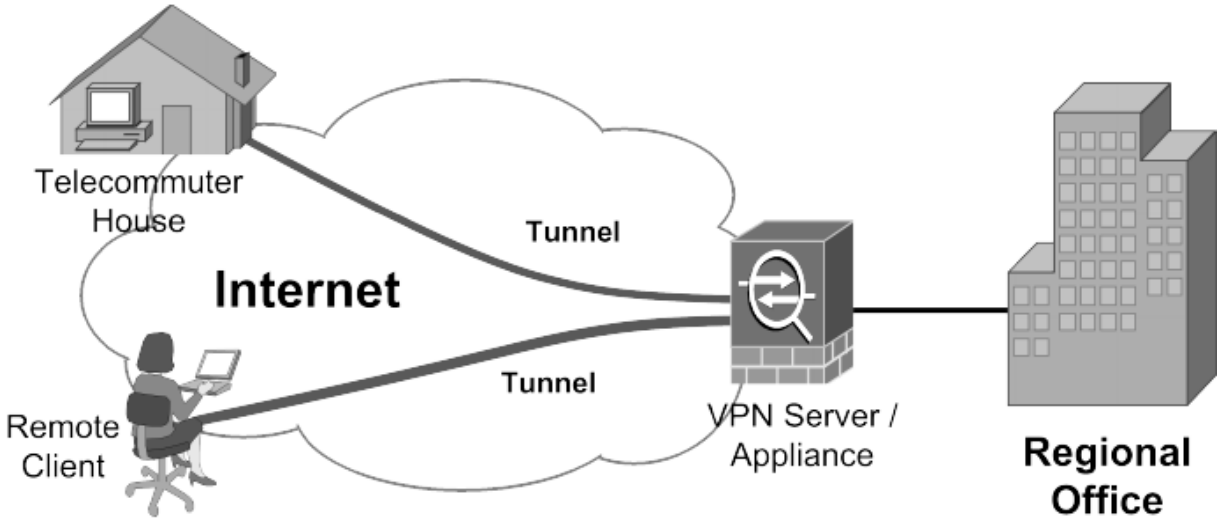


Figura 2-12. VPN de Acceso Remoto [9]

2.2.2.2 VPN Punto a Punto/Sitio a Sitio

Este esquema es el empleado para conectar oficinas remotas con una sede central. El servidor VPN está conectado permanentemente a Internet, acepta conexiones entrantes desde los sitios y establece el túnel VPN. Los servidores de las oficinas remotas se conectan a Internet y a través de esta al túnel VPN de la oficina central. Se utiliza para eliminar la conexión punto a punto tradicional.

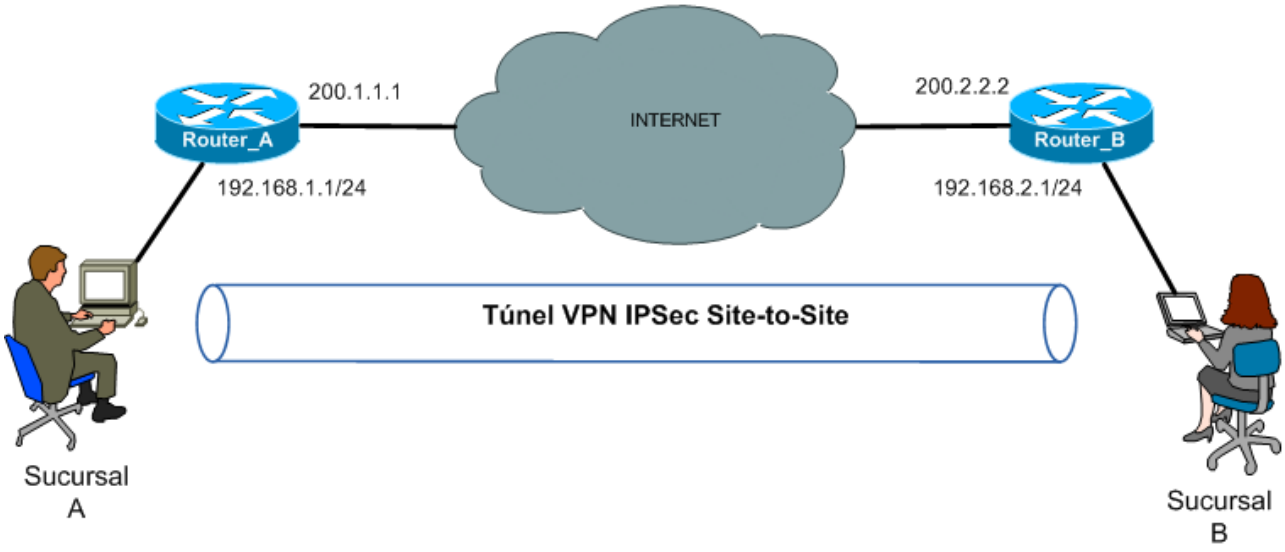


Figura 2-13. VPN Punto a Punto [10]

2.2.2.3 VPN interna (over LAN)

Funciona tal cual una red VPN normal, salvo que dentro de la misma red local LAN en lugar de a través de Internet. Sirve para aislar zonas y servicios de la misma red interna. Sirve también para mejorar las características de seguridad de una red inalámbrica WiFi.

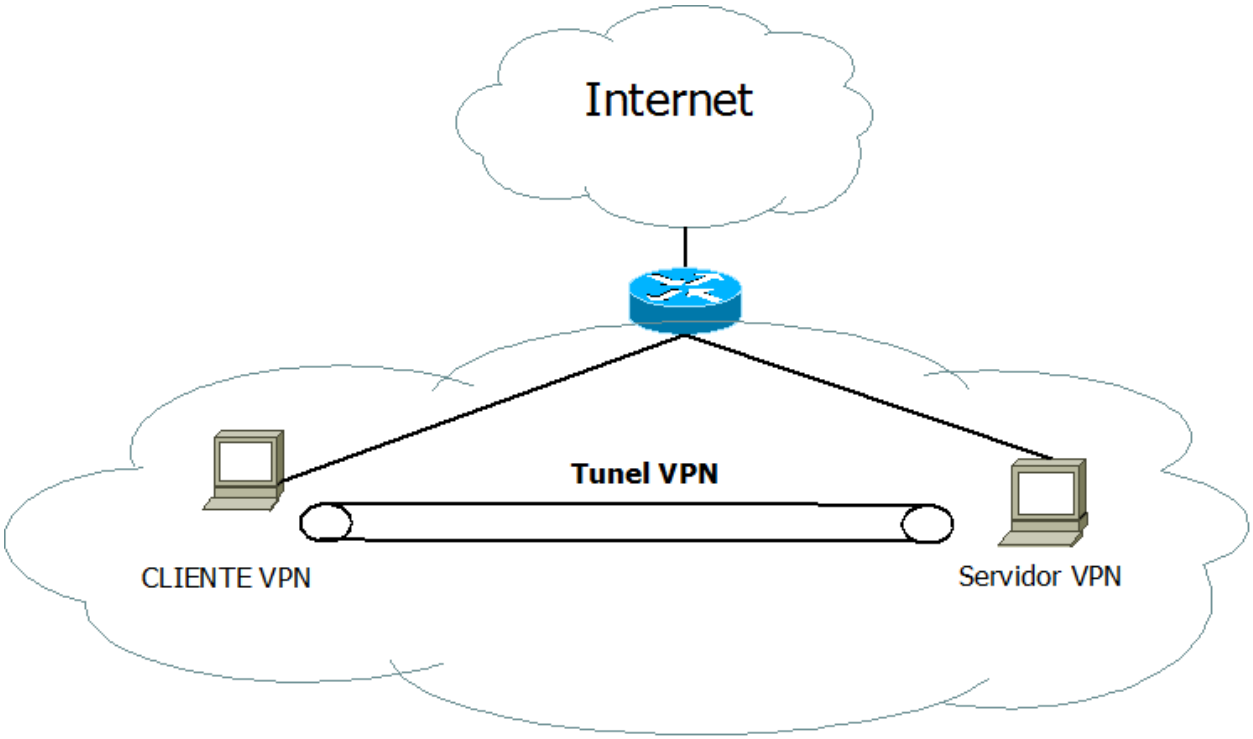


Figura 2-14. VPN over LAN

2.2.3 Protocolos VPN

En la siguiente tabla se explica las características de los protocolos VPN más importantes:

Protocolo	*Encriptación*	*Velocidad*	*Seguridad*
PPTP (*Protocol of Tunnel Point to Point*)	MPPE - 128-bits	Mayor velocidad debido a una encriptación básica, pero puede dar como resultado conexiones inestables.	Se han encontrado varias vulnerabilidades de seguridad conocidas en la implementación de PPTP.
L2TP/IPSec (*Layer 2 Tunneling Protocol*)	AES - 128 bits para datos y SHA256 para mensajes de control.	L2TP/IPsec tiene coste de túnelación, pero sigue siendo rápido por su eficaz encriptación/desencriptación.	La encriptación IPsec no tiene importantes vulnerabilidades conocidas cuando se implementa adecuadamente.
OpenVPN	AES - 256 bits para datos, SHA256 para mensajes de control y encriptación Handshake SSL/TLS de 2048 bits.	Incluso en conexiones con alta latencia y de larga distancia sigue manteniendo una gran velocidad, convirtiéndolo en el protocolo de mejor rendimiento.	OpenVPN puede considerarse verdaderamente seguro cuando se utiliza con un cifrado fuerte y claves efímeras.
IKEv2 (*Internet key Exchange v2*)	AES - 256 bits para datos y SHA256 para mensajes de control.	IKEv2 es más rápido que la mayoría de los protocolos VPN. El soporte para el Protocolo de Movilidad y Multihoming lo hace muy resistente y estable.	El protocolo VPN más novedoso, implementado sobre IPSec y considerado altamente seguro

Tabla 2-3. Características protocolos VPN [11]

Además se van a explicar las ventajas e inconvenientes de usar cada uno de ellos:

Protocolo	*Ventajas*	*Inconvenientes*
PPTP	Fácil de configurar. Cliente integrado en la mayoría de plataformas. Buenas velocidades. Soportado por el mayor número de dispositivos.	La estabilidad puede variar dependiendo de la red. Menor nivel de seguridad. Puede ser bloqueado.
L2TP/IPSec	Fácil de configurar. Atraviesa restricciones de redes o ISPs. Soportado por el mayor número de dispositivos. Disponible en todas las plataformas modernas.	Puede tener problemas con firewalls restrictivos. Puede tener una velocidad más lenta. Se bloquea con mayor facilidad.
OpenVPN	Altamente configurable. Muy rápido y seguro. Atraviesa la mayoría de las restricciones de red/ISP y los firewalls.	La configuración puede ser más complicada que en otros protocolos VPN. No soportado por algunos dispositivos móviles. Requiere instalación de software de terceros.
IKEv2	El protocolo VPN más rápido. Muy seguro. Fácil de utilizar para el usuario final. Muy estable, especialmente al cambiar de red o reconectar después de perder la conexión a Internet.	Limitado en configuración (no puertos UDP). No soportado en plataformas antiguas.

Tabla 2-4. Ventajas e inconvenientes protocolos VPN [11]

El protocolo que he utilizado para este proyecto es OpenVPN debido a que es más configurable, muy rápido y con más alcance a nivel de red respecto a los otros protocolos.

En la siguiente imagen, se indica donde está cada protocolo VPN ubicado en el modelo OSI:

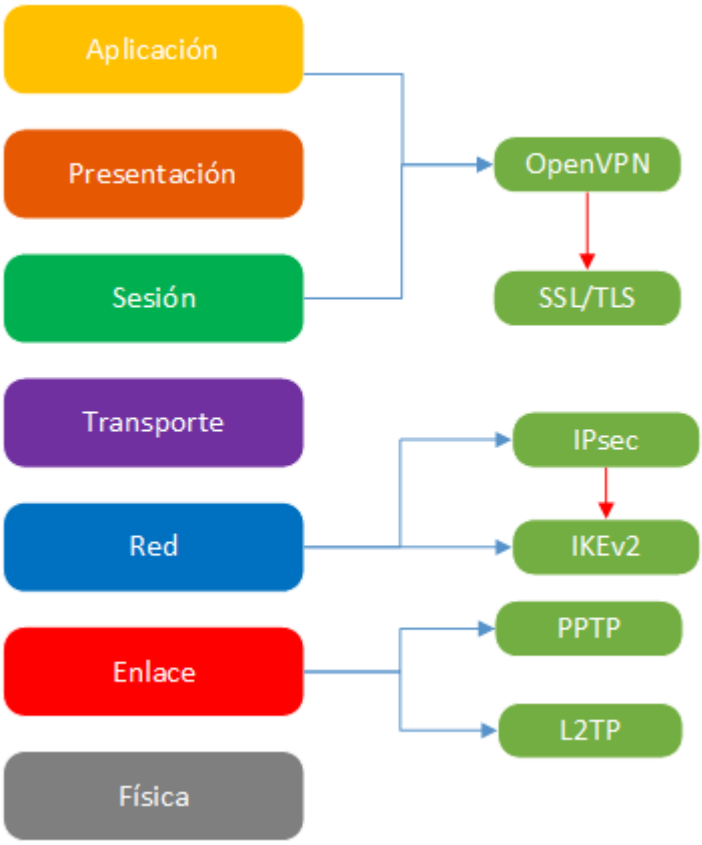


Figura 2-15. Protocolos VPN en modelo OSI

OpenVPN encapsula los paquetes mediante TCP o UDP, aunque por defecto utiliza UDP como protocolo de transporte para el funcionamiento óptimo, ya que es mejor que TCP en la mayoría de escenarios. En comparación con UDP, TCP es menos eficiente y menos robusto cuando es utilizado sobre redes que utilizan alguna capa fiable y con posibles congestiones. Sin embargo, el uso de TCP como protocolo de transporte puede tener ventajas de seguridad y robustez frente a la utilización de UDP en el caso de uso de túneles no IP o de utilizar protocolos que no tienen ningún nivel de fiabilidad. "OpenVPN tiene la posibilidad de utilizar un único puerto en el servidor para todas las conexiones VPN o de aguantar más de una conexión TCP" [12].

Los aspectos positivos de utilizar UDP frente TCP son [12]:

- Proporciona mejor protección frente a ataques de denegación de servicio (DoS) y frente al escaneo de puertos.
- En los sistemas de VoIP tiene un mayor rendimiento ya que VoIP utiliza el protocolo RTP (*Real-time Transport Protocol*) que es transportado sobre UDP. Por tanto, si se utilizase TCP, cuando un paquete es rechazado, el emisor vuelve a transmitir el paquete ante la petición del receptor o receptores lo que causaría que al reensamblar los paquetes de voz retransmitidos en un stream de audio podrían resultar llegar con retardo a la hora de obtener una reproducción fiable del sonido original. Sin embargo, si con UDP da por validos paquetes enviados fuera de orden y no existe verificación (ACK) de si el paquete llega, de esta forma llegaría sin retardo los paquetes de stream de audio y se tendría una reproducción fiable del sonido original.

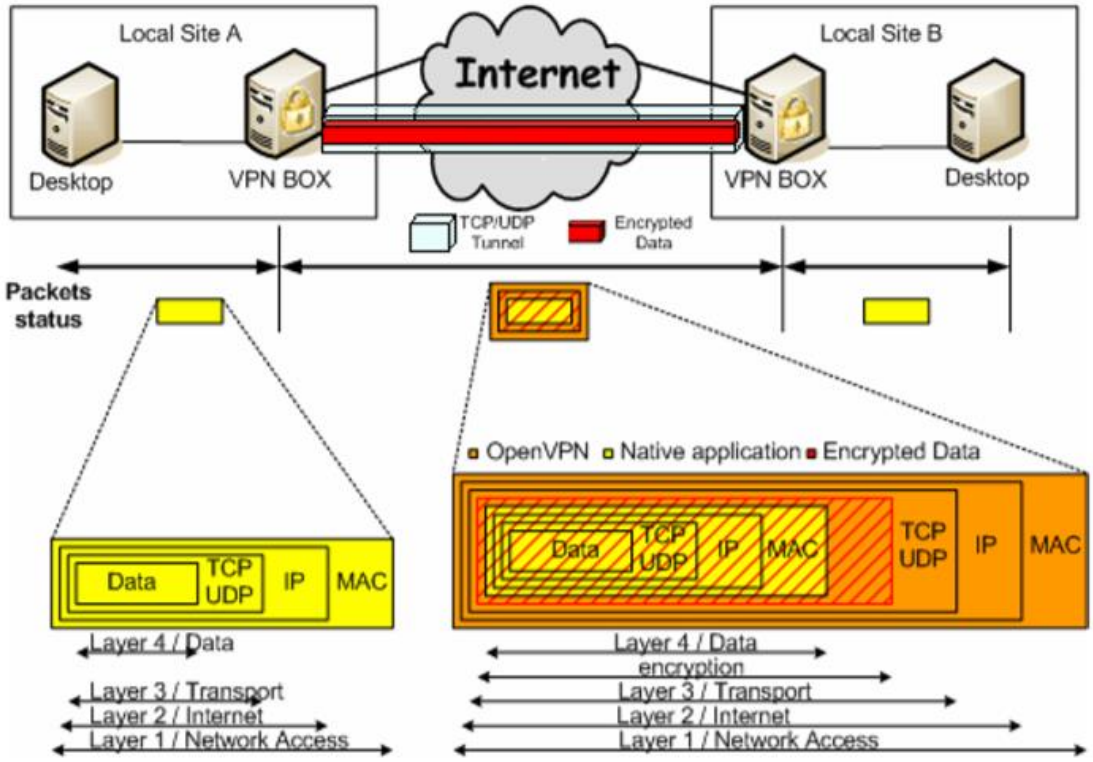


Figura 2-16 . Encapsulación de OpenVPN [12]

2.2.4 Software utilizado

Los softwares gratuitos que se suelen utilizar para una VPN son los siguientes:

1. HotSpot Shield [13].
2. OpenVPN [14].
3. Windscribe [15].
4. ProtonVPN [16].
5. Hide.me [17].
6. TunnelBear [18].
7. Freelan [19].
8. NordVPN [20].
9. PureVPN [21].
10. SlickVPN [22].
11. Wireguard [23].

Se utilizará OpenVPN como software VPN ya que tiene mayor rendimiento, seguridad, más configurable y sobre todo, proporciona una mayor velocidad.

Figura 2-17. Logotipo OpenVPN [14]

A continuación, se verán las ventajas y desventajas de utilizar OpenVPN frente a IPsec VPN [24]:

- Ventajas:
    - Posibilidad de implementar dos modos básicos, en capa 2 o capa 3, con lo que se logran túneles capaces de enviar información en otros protocolos no-IP como IPX o broadcast (NETBIOS).
    - Protección de los usuarios remotos. Una vez que OpenVPN ha establecido un túnel el firewall de la organización, protegerá el equipo remoto aun cuando no es un equipo de la red local. Por otra parte, sólo un puerto de red podrá ser abierto hacia la red local por el remoto asegurando protección en ambos sentidos.
    - Conexiones OpenVPN pueden ser realizadas a través de casi cualquier firewall. Si se posee acceso a Internet y se puede acceder a sitios HTTPS, entonces un túnel OpenVPN debería funcionar sin ningún problema.
    - Soporte para proxy. Funciona a través de proxy y puede ser configurado para ejecutar como un servicio TCP o UDP y además como servidor (simplemente esperando conexiones entrantes) o como cliente (iniciando conexiones).
    - Sólo un puerto en el firewall debe ser abierto para permitir conexiones, dado que desde OpenVPN 2.0 se permiten múltiples conexiones en el mismo puerto TCP o UDP.
    - Las interfaces virtuales (tun0, tun1, etc.) permiten la implementación de reglas de firewall muy específicas.
    - Todos los conceptos de reglas, restricciones, reenvío y NAT pueden ser usados en túneles OpenVPN.
    - Alta flexibilidad y posibilidades de extensión mediante scripting. OpenVPN ofrece numerosos puntos para ejecutar scripts individuales durante su arranque.
    - Soporte transparente para IPs dinámicas. Se elimina la necesidad de usar direcciones IP estáticas en ambos lados del túnel.
    - Ningún problema con NAT. Tanto los clientes como el servidor pueden estar en la red usando solamente IPs privadas.
    - Instalación sencilla en cualquier plataforma. Tanto la instalación como su uso son muy simples.
    - Diseño modular. Se basa en un excelente diseño modular con un alto grado de simplicidad tanto en seguridad como red.
- Inconvenientes:
    - Carencia de masa crítica.
    - Todavía son relativamente pocos los que saben cómo usar OpenVPN.
    - A día de hoy mayormente se puede conectar a otras computadoras o dispositivos con IOS y Android. Sin embargo, esto está cambiando, dado que existen compañías desarrollando dispositivos con clientes OpenVPN integrados y haciendo llegar esta tecnología a otros ámbitos como la automatización industrial (como por ejemplo en Panasonic).

2.2.5 Uso en la actualidad

El uso de las VPN en la actualidad es cada vez mayor, sobre todo en el ámbito empresarial ya que todas las empresas quieren tener sus sedes interconectadas a través de túneles VPN. De esta forma pueden conectar sus redes unas con otras para el paso de información, realizar auditorías de seguridad y para una jerarquización de sus sedes.

En la siguiente imagen, se puede observar como el mercado de las VPN ha aumentado sobre todo en países como Indonesia, India y Malasia donde ronda entre el 30% y 40% de uso de VPN. También se puede observar cómo tanto la zona de Asia es la que más porcentaje de uso de VPN tiene con un 30% mientras que Norte América y Europa tiene el mismo porcentaje de uso de VPN y a la vez más bajo (18%).

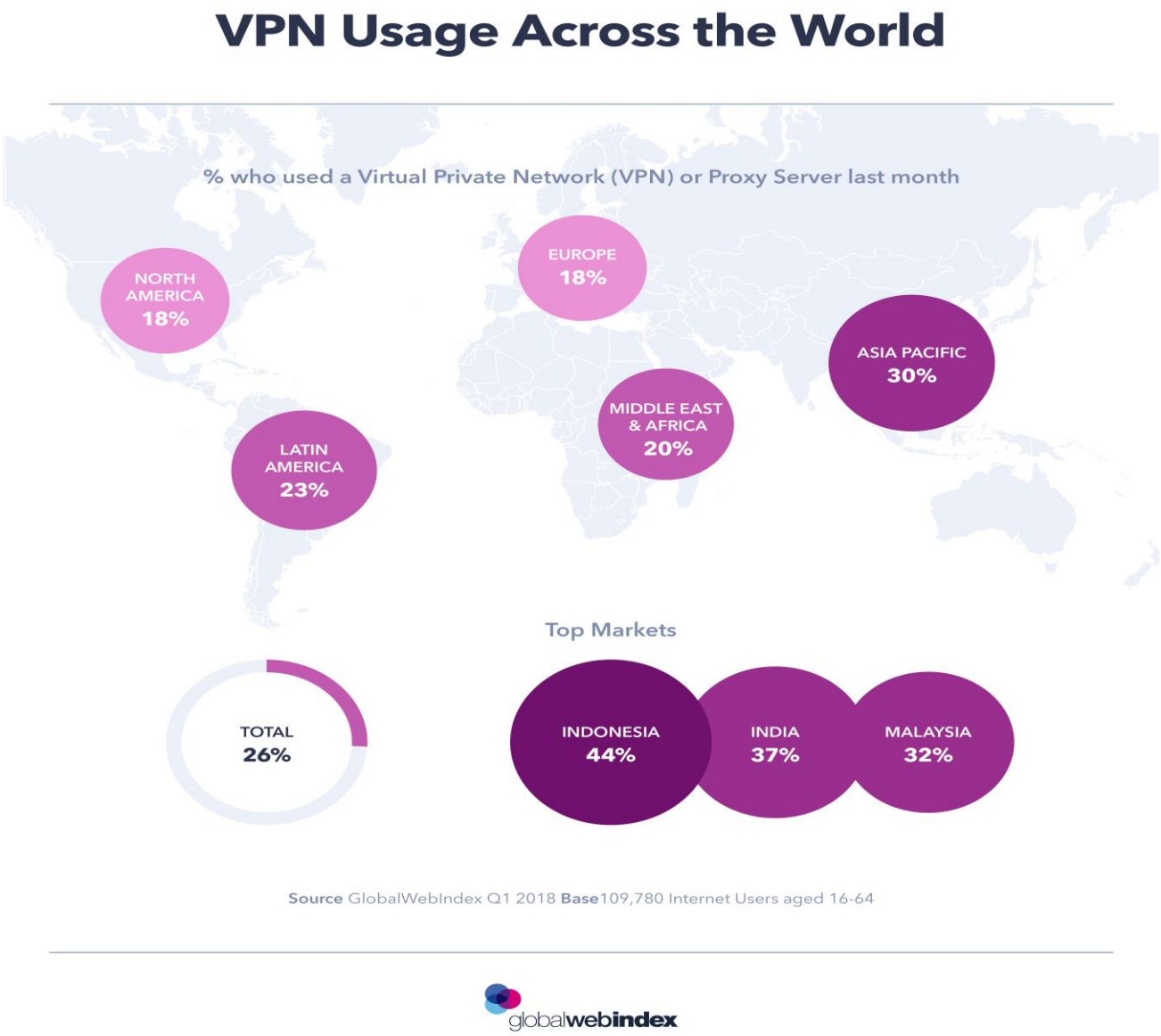


Figura 2-18. Uso de VPN Mundial [25]

2.3 Tunnel Broker IPv4/IPv6

Un tunnel broker es un servicio que provee un túnel de red. Estos túneles pueden proveer de conectividad encapsulada mediante la infraestructura existente hacia otra infraestructura.

Existen una amplia variedad de tunnel brokers, incluyendo tunnel brokers IPv4, aunque comúnmente este término es usado para referirse a los tunnel brokers IPv6, definidos en RFC:3053.

Los tunnel brokers normalmente ofrecen túneles IPv6 a webs o usuarios mediante IPv4. En general, los tunnel brokers IPv6 ofrecen lo que se llaman túneles 'protocolo 41' o proto-41. Estos son túneles donde IPv6 se tunela directamente en paquetes IPv4, fijando el campo de protocolo en '41' (IPv6) en el paquete IPv4. En el caso de los tunnel brokers IPv4 los túneles IPv4 se proveen a los usuarios encapsulando IPv4 en IPv6, como se define en RFC:2473 [26].

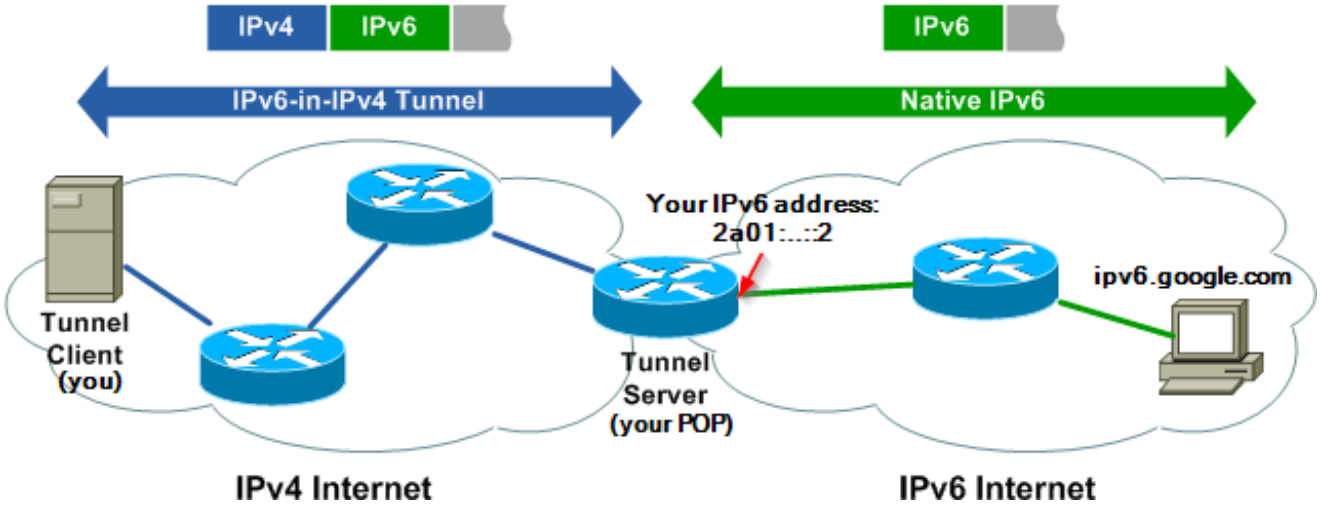


Figura 2-19. Ilustración funcionamiento Tunnel Broker [27]

2.3.1 Características

Las características de un túnel 6to4 dado por un Tunnel Broker son:

- Proporcionar conectividad IPv6 en redes que solo tienen soporte en IPv4.
- Se encapsulan paquetes IPv6 dentro de paquetes IPv4. Se suele hacer entre Nodo Final → Router y Router → Router. También es posible para Nodo Final → Nodo Final.
- Los paquetes resultantes viajan por redes IPv4.
- El túnel se considera como un enlace punto a punto desde el punto de vista de IPv6. Solo un salto, aunque existan varios saltos IPv4.
- Las direcciones IPv6 de ambos extremos del túnel son del mismo prefijo.
- Todas las conexiones IPv6 del nodo final pasan por el router que esta en el extremo del túnel.
- Los túneles 6to4 pueden construirse desde nodos finales situados detrás de NAT. Para ello, el router que tiene NAT tiene que tener soporte sobre el protocolo 41.

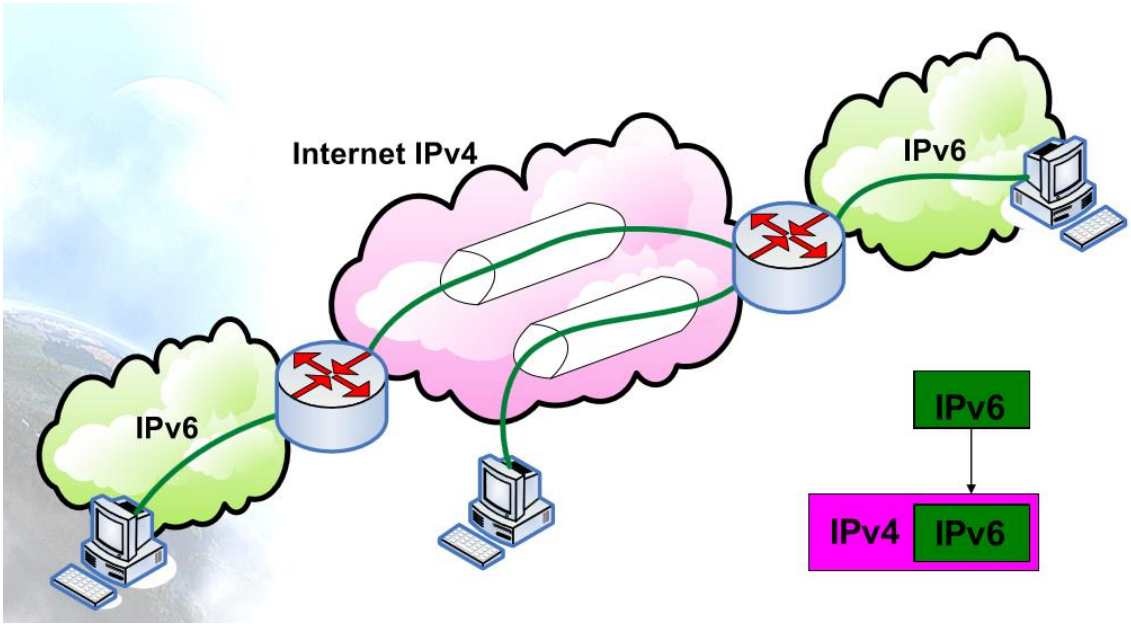


Figura 2-20. Esquema encapsulado IPv6 en IPv4 [28]

2.3.2 Software utilizado

Hay muchos Tunnel Brokers en el mercado, a continuación, una lista de los más usados y aún activos:

- Hurricane Electric [29].
- NetAssist [30].
- Got-root [31].
- IP4Market [32].
- ipv6onlyhosting (*) [33].
- 6project.org (*) [34].
- Pemsy (*) [35].

(*) son servicios de pago.

El Tunnel Broker que se utilizará será Hurricane Electric y sus características son [29]:

- Dirigido por un ISP empresarial con personal 24 x 7 en múltiples ubicaciones y una red troncal internacional.
- Posibilidad de obtener su propio prefijo / 48 una vez que su túnel esta levantado.
- Posibilidad de obtener una vista completa de la tabla de enrutamiento BGP4 y de IPv6.
- Posibilidad de utilizar su túnel después de un simple proceso de registro (Tarda menos de un minuto).
- Capacidad para crear su túnel en servidores de túnel geográficamente diversos (Dubái, Sydney, Ashburn, Calgary, Chicago, Dallas, Denver, Fremont, Honolulu, Kansas City, Los Ángeles, Miami, Nueva York, Lisboa…).
- Permite anunciar el espacio de direcciones IPv6 que le ha asignado directamente un RIR (ARIN, RIPE, APNIC, etc.) cuando se tiene una red que utiliza BGP como protocolo de encaminamiento y tiene propio ASN.
- Tras la activación del túnel, se generarán automáticamente los comandos de configuración del usuario para una variedad de plataformas. Una vez que se configure, podrá acceder a Internet IPv6.

Figura 2-21. Logo Hurricane Electric [29]

2.3.3 Uso en la actualidad

En la actualidad, el uso de Tunnel Broker solo puede ser posible en dispositivos con Pila de protocolos Dual (IPv4 e IPv6). Por lo que, no todos los dispositivos son compatibles a utilizar un túnel 6to4 puesto que no se tiene la opción de utilizar IPv6. Pero a día de hoy, todos los dispositivos tienen la Pila de protocolos Dual.

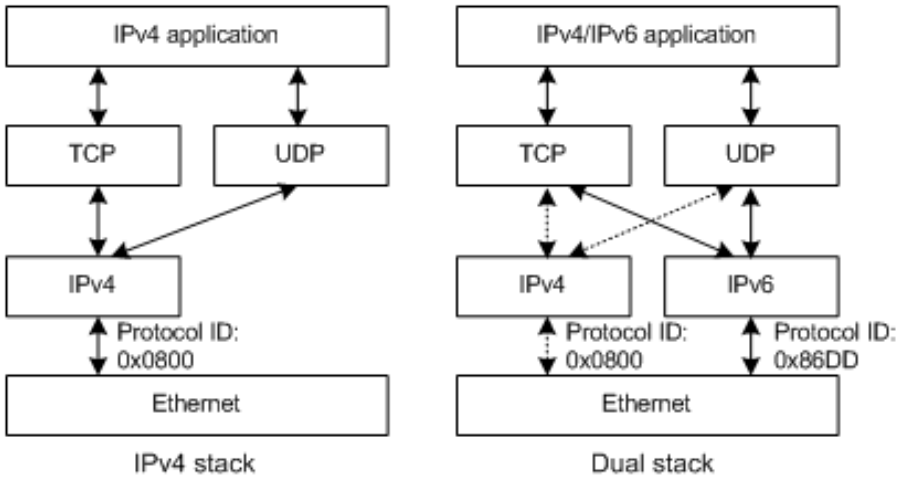


Figura 2-22. Pila IPv4 - Pila Dual [36]

El uso de Tunnel Brokers lo siguen liderando países como EEUU (23.51%), China (22.21%) y Rusia (7.08%). Mientras España tiene un 1.07% de uso de Tunnel Brokers según las estadísticas de tunelbroker.net. En el siguiente gráfico se muestra el top 20 países con más número de túneles IPv4/IPv6 activos:

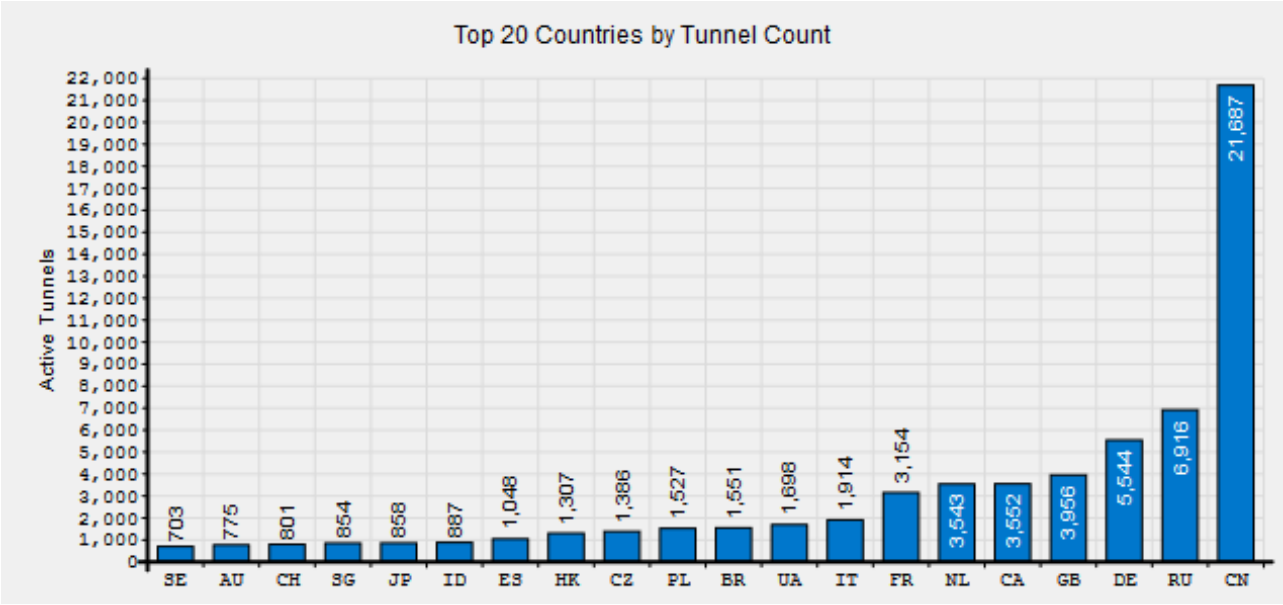


Figura 2-23. Número de Tunnel Brokers por país [37]

3 SISTEMA

Dos cosas contribuyen a avanzar: ir más deprisa que los otros o ir por el buen camino.

- René Descartes -

En este apartado se verá la metodología y la funcionalidad del proyecto, asimismo se realizará un estudio dividido en dos secciones: diseño e implementación.

3.1 Diseño

En este apartado se abordará el diseño del proyecto a todos los niveles, tanto a nivel de programación como a nivel de red. Se dividirán en distintos apartados para el mayor entendimiento de la estructura del trabajo.

3.1.1 Diseño

El objetivo del proyecto es la realización de un portal web que permita a los usuarios poder conectarse a una red VPN donde se podrán interactuar con otros usuarios que estén conectados en esta VPN, y a su vez, podrán conectarse a Internet mediante IPv4 e IPv6. Para ello, se necesitará un servidor web donde estará alojada la página y un servidor VPN, donde se conectarán los usuarios para estar dentro de la red VPN. Por tanto, el diseño del proyecto se dividirá en dos partes: Diseño Web y Diseño de servidor VPN. El diseño web se realizará mediante el diseño de código HTML, CSS, JavaScript, JSP, Java, C y scripts mediante ShellScript. Además de esto, dentro del diseño se incluirá el diseño de Base de Datos con las tablas necesarias para tener la página. Por otro lado, se tiene el diseño de la configuración OpenVPN donde se tendrá la instalación del software, la configuración de los certificados, la configuración del cliente y del servidor. En la siguiente figura se mostrará el esquema de diseño:

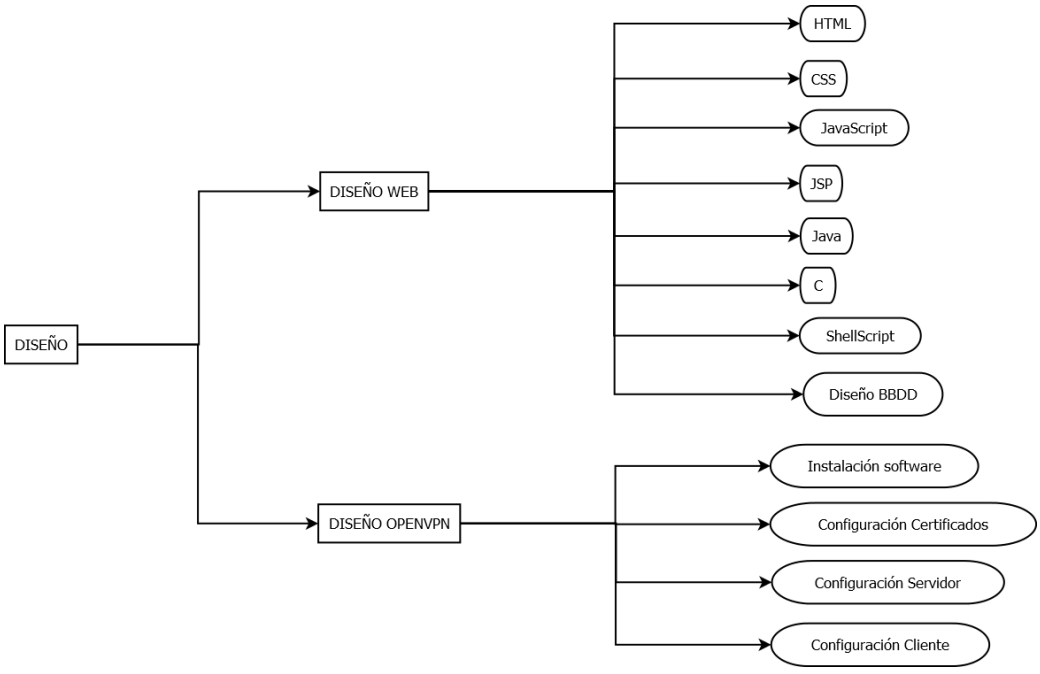


Figura 3-1. Esquema Diseño del proyecto

3.1.2 Esquema de red

El fin de este proyecto no es más que conseguir tener un túnel IPv4/IPv6 para poder tener salida a Internet mediante IPv6, y a la vez, tener una red VPN entre los clientes VPN. Para ello se propone realizar un portal web que proporcione a los usuarios facilidad para poder conectarse a la red VPN. Para ello, se ha propuesto utilizar en una máquina, un servidor Web, donde estará localizado el portal web y un servidor VPN, en el que se conectarán los usuarios para que este pueda darles un direccionamiento IPv4 e IPv6 de la red VPN, poder conectarlos entre sí y darles salida a Internet mediante IPv6.

El escenario ideal tendrá direccionamiento IPv6 en el router que será proporcionada por el operador de red, por lo que se asignarán direcciones IPv6 a los equipos de esa subred y se accederá a Internet IPv6 a través del router de operador. De esta forma, cuando los clientes VPN quieran conectarse a Internet IPv6, el servidor VPN reenviará la petición a Internet IPv6 a través del router.

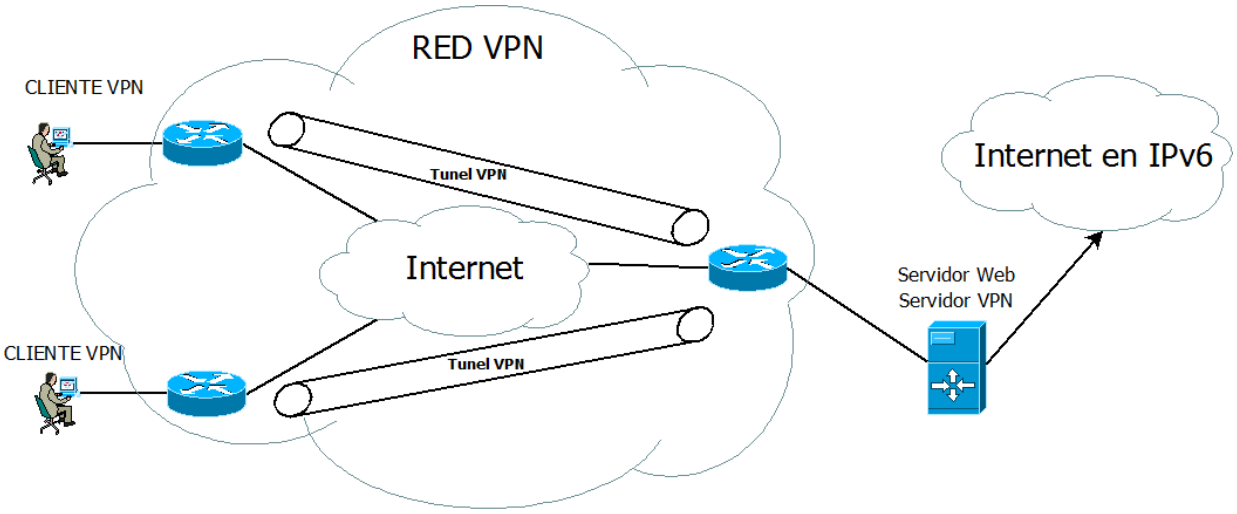


Figura 3-2. Esquema de Red

A continuación se verá el modelo de red utilizado, el cual será un tipo de VPN interna o Over LAN, la cual el equipo servidor y los clientes están en la misma subred y, por tanto, se crean túneles OpenVPN de forma Interna. Se ha decidido poner de esta forma, debido a que el operador de red contratado me proporcionó un router el cual no funcionaba correctamente la redirección de puertos.En este escenario se tiene NAT tanto en IPv4 como en IPv6. Además, este operador no proporcionaba IPv6, por lo que se ha creado un túnel con Hurricane a través de IPv6 para que todo el tráfico que vaya hacia Internet IPv6 se redirigirá a través de este túnel. Se tendrán tres interfaces dentro del equipo servidor:

- eth0: Salida normal hacia el router que proporciona Internet mediante IPv4.
- tun0: Túnel Interno creado por OpenVPN.
- sit1: Túnel creado mediante Tunnel broker de Hurricane y que proporciona Internet mediante IPv6.

En resumen, cada vez que se quiera salir hacia Internet mediante IPv6 se saldrá mediante la interfaz del túnel de Hurricane, mientras que si se sale a Internet mediante IPv4, saldrá por la interfaz eth0 que va hacia el router.

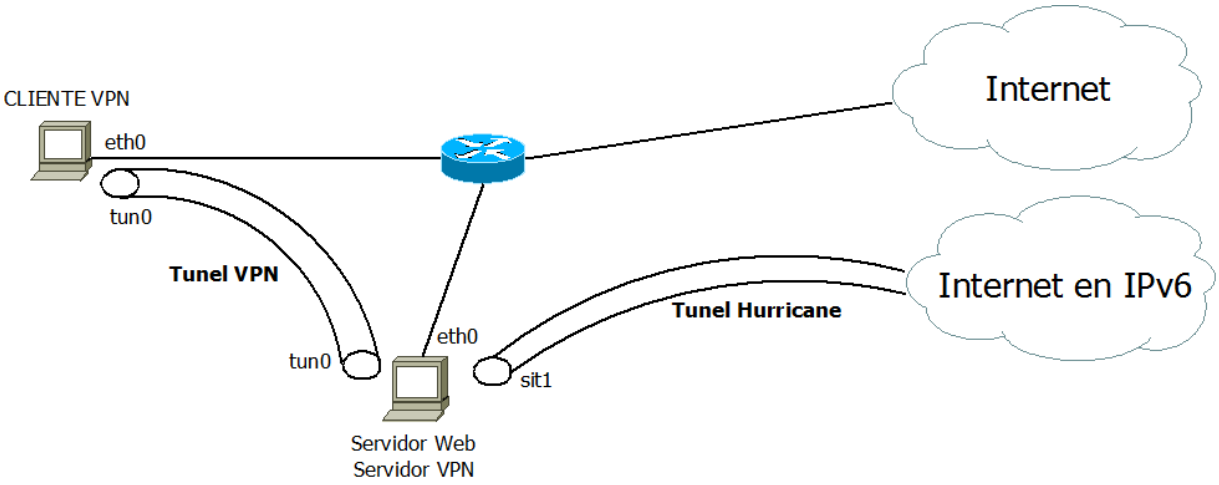


Figura 3-3. Modelo Real

3.1.3 Diagrama de Casos de uso

En el proyecto se van a tener definidos dos tipos de usuarios: usuario normal y usuario administrador. Cada uno de ellos podrá acceder a diferentes opciones. El usuario normal accederá al potencial de esta aplicación como un simple usuario sin muchos conocimientos de redes, que será la persona normal que trabaje con esta aplicación.Mientras que el usuario administrador tendrá que tener conocimientos avanzados de redes, tanto de VPNs como del uso de OpenVPN para el control y gestión de la aplicación.

En primer lugar, el usuario normal tras registrarse podrá realizar las siguientes opciones: ver información de usuario, ver instrucciones de uso, descargar fichero cliente OVPN y configurar IP de forma estática o por DHCP.

3.1.3.1 Usuario normal

El usuario normal podrá ver la información del usuario que será la que se utilizará para la creación de certificados en el servidor OpenVPN:

- Nombre.
- Usuario.
- Email.
- País (Aparecerá las dos letras iniciales).
- Provincia.
- Localidad.
- Empresa.

También se proporcionará información cuando el usuario se conecte al servidor por VPN que será:

- IPv4.
- IPv6.

En la segunda opción, se podrá ver las instrucciones de uso para crear el correcto funcionamiento e instalación de OpenVPN, y para la conexión con el servidor para los distintos SO como:

- Windows.
- Linux.
    - Ubuntu/Debian.
    - Fedora/CentOS/RedHat.

- MacOS.
- Android.
- IOS.

En la tercera opción, se podrá descargar el fichero cliente OpenVPN, necesario para poder conectarse con el servidor VPN. Esta opción se encuentra dentro de la información de usuario y dentro de las instrucciones de uso.

En la última opción, el usuario podrá configurar la dirección IP que obtendrá su equipo tras conectarse con el servidor. Esto lo podrá realizar a partir de dos métodos: DHCP o IP estática. Si se escoge la primera opción, el servidor le pondrá una dirección IPv4/IPv6 disponible dentro de su rango, mientras que si se escoge la segunda opción, el usuario podrá definir una IPv4/IPv6 estática dentro del direccionamiento DHCP tanto de IPv4 como de IPv6 del servidor, donde se comprobará si las direcciones especificadas están asignadas a otro cliente, independientemente si este otro cliente se ha conectado por cualquiera de los dos métodos.

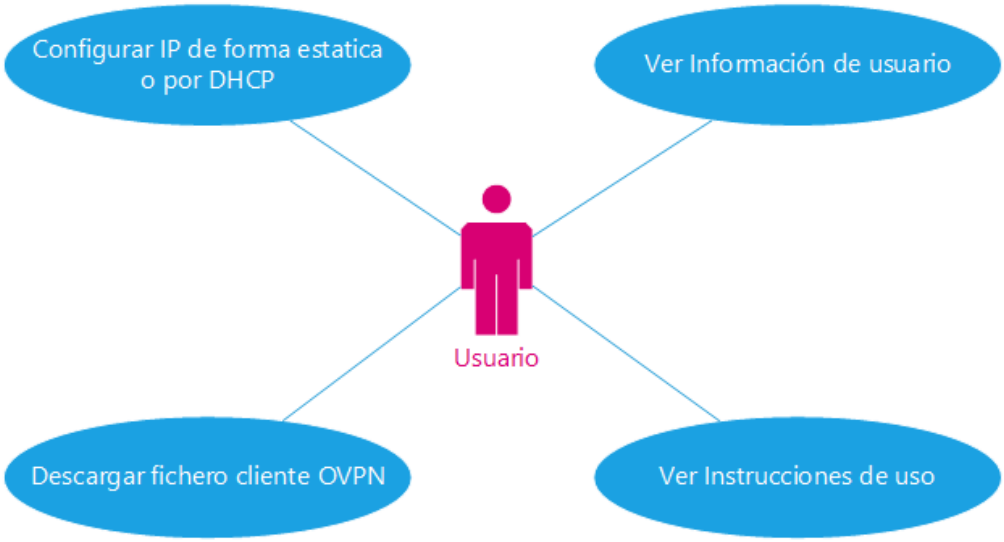


Figura 3-4. Diagrama de Caso de Uso para usuario normal

3.1.3.2 Usuario administrador

El usuario administrador podrá realizar las siguientes opciones: mostrar información de usuarios registrados, configurar parámetros del servidor OpenVPN y mostrar el fichero de configuración del servidor OpenVPN.

La primera opción permite ver al usuario administrador todos los usuarios que están registrados en el sistema, teniendo acceso a la siguiente información:

- Usuario.
- Email.
- País.
- Provincia.
- Localidad.
- Empresa.

También tiene 4 nuevos campos, los cuales indican el estado de conexión del usuario tanto con el portal web como con la conexión VPN. Estos parámetros son:

- ConexiónWeb: Permite saber si el usuario está conectado a la web.
- ConexiónVPN: Permite saber el estado de la conexión VPN del usuario.

- IPv4: Muestra la dirección IPv4 asignada al usuario por el servidor OpenVPN.
- IPv6: Muestra la dirección IPv4 asignada al usuario por el servidor OpenVPN.

La segunda opción, permite al usuario administrador configurar algunos parámetros del servidor OpenVPN para que se adapte al funcionamiento que el administrador desee tener para su subred VPN. Para ello, el administrador de red tiene que tener conocimientos sobre redes y sobre IPv6. Los parámetros que puede modificar el administrador serían los siguientes:

- IP servidor: Es la IP del servidor a la que se conectarán los clientes para establecer el túnel VPN.
- Keep Alive: Es el mensaje que se le envía a los clientes para chequear el enlace entre ellos. En este caso, hay que configurar dos parámetros:
    - Interval (ping): Realiza un ping si no se han enviado paquetes durante el intervalo (interval).
    - Timeout (ping-restart): Realiza un reinicio mediante la señal SIGUSR1 después de que pasen n segundos sin recibir un ping u otro paquete desde el cliente.
- Protocolo: Es el protocolo de transporte que se va a utilizar en el túnel. Será UDP o TCP.
- Clientes Máximos Conectados: Es el número de clientes que van a poder estar conectados con el servidor VPN.
- Direccionamiento DHCP (IPv4/Mask): Es el direccionamiento IPv4 que se le va a poner al servidor DHCP del servidor VPN para que asigne direcciones a los clientes del túnel. También se le podrá asignar una máscara para limitar el número de direcciones.
- Direccionamiento DHCP (IPv6/Mask): Es el direccionamiento IPv6 que se le va a poner al servidor DHCP del servidor VPN para que asigne direcciones a los clientes del túnel. También se le podrá asignar una máscara para limitar el número de direcciones.
- MTU: Es el tamaño máximo de transmisión a través del túnel VPN. Por ejemplo, si la MTU del túnel es de 1400 Bytes, solo se podrán enviar a través del túnel paquetes con hasta 1400 Bytes de tamaño.

La tercera opción, permite al administrador poder visualizar el fichero de configuración del servidor OpenVPN para verificar que la configuración esta correcta. En caso de querer cambiar otros parámetros de configuración distintos de los que se permite en la aplicación, se debe modificar manualmente este fichero en el equipo donde este ubicado el servidor.

Figura 3-5. Diagrama de caso de uso de administrador

3.1.4 Diagrama de funcionamiento

En lo que respecta a este apartado, se va a explicar el funcionamiento de la aplicación. Como se tienen dos perfiles de usuario (administrador y usuario), se realizará un esquema de funcionamiento para cada perfil, de tal manera que se tengan unas instrucciones sobre lo que el usuario normal tiene que realizar y puede modificar. A continuación, se va a mostrar el funcionamiento básico del proyecto para un usuario normal.

En primer lugar, el usuario entra en la página principal. Si este está registrado, solo tendrá que iniciar sesión con sus credenciales y de esa manera, accederá al sistema. En caso de que el usuario no esté registrado, tendrá que pulsar la opción "Registrarse" para registrarse en el sistema. En la página de Registrarse tendrá que rellenar los siguientes parámetros:

- Nombre.
- Usuario.
- Contraseña.
- Email.
- País.
- Provincia.
- Localidad.
- Empresa.

Una vez realizado el registro, el usuario será redireccionado al menú principal.

Dentro del Menú Principal, se pulsará "Instrucciones". En la página que aparece, se buscará las instrucciones de instalación del SO que el usuario quiera utilizar. En las instrucciones del SO, primero se descargará OpenVPN en el sistema a través de un link hacia el portal de OpenVPN o hacia el Market en caso de App donde se podrá descargar. Tras ello, descargar mediante el link el fichero "cliente.ovpn" para poder conectar al cliente con el servidor.

Por último, el usuario seguirá los pasos a seguir para poder conectar el cliente con el servidor mediante el fichero proporcionado. Tras esto, ya estaría realizada la configuración básica para conectarse al servidor. En la siguiente figura (3-6) se muestra el diagrama BPMN del funcionamiento básico para el usuario.

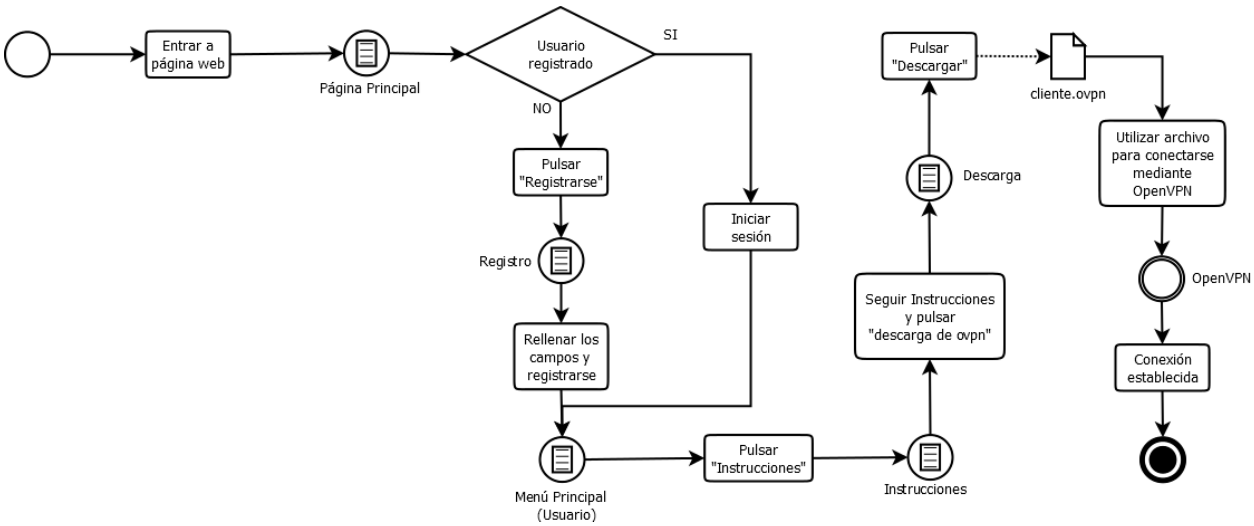


Figura 3-6. Diagrama BPMN del funcionamiento básico para usuario

En la siguiente figura (3-7) se puede ver el diagrama BPMN del funcionamiento básico del proyecto para el usuario administrador.

En primer lugar, el usuario entra en la página Principal e inicia sesión con las credenciales de usuario administrador. Tras esto, se pulsa configuración de usuario y se configura los parámetros del servidor para que

estén de la forma que el administrador quiera. Por último, se aplican los cambios y tras esto el servidor OpenVPN se reiniciará y nos redirigirá la página a la que contiene la configuración actual del servidor. De esta forma podremos comprobar que los cambios se han realizado correctamente.

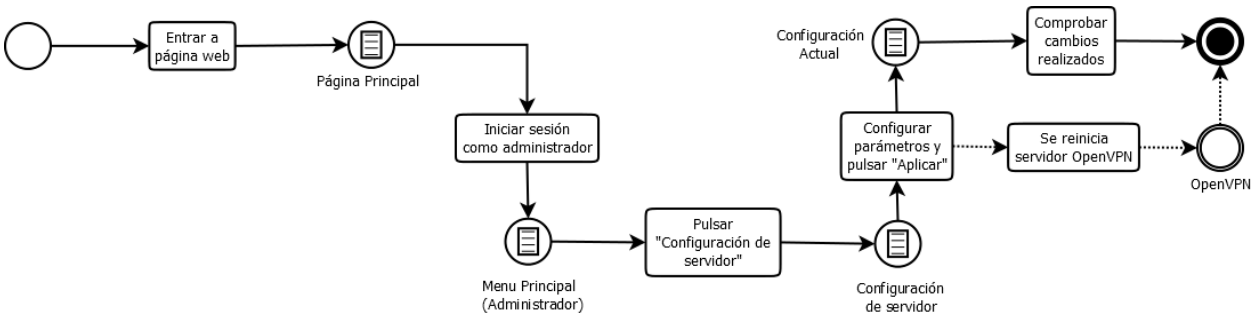


Figura 3-7. Diagrama de secuencia del funcionamiento básico para administrador

3.1.5 Estructura de páginas

En lo que respecta a este apartado, se va a explicar la estructura de páginas del portal web, donde se explicará la interacción entre cada una de ellas.

Para comenzar, se tiene "Principal.jsp" que será la página principal a la que se accede para iniciar sesión o registrarse. Esta página tiene un formulario o login y una pequeña descripción de la aplicación. A continuación, si se pulsa el botón "Registrarse" se tiene la página "Registro.jsp" donde el usuario se registrará en el sistema con las credenciales mencionadas anteriormente en la tabla de BD llamada "USUARIOS".

Tras registrarse o iniciar sesión, se tendrá la página "menú.jsp" en la que se tienen las opciones ya comentadas anteriormente. Si se pulsa "Información de usuario", se irá a la página "pagina_usuario.jsp" donde se verá la información relacionada con los datos de usuario y los datos de conexión VPN. Si se pulsa "Instrucciones", se irá a la página "instrucciones.jsp" donde se muestran las instrucciones de instalación de OpenVPN y del cliente OpenVPN para los distintos SO. Tanto "Información de usuario" como "Instrucciones" tienen un link que lleva a la página "Descarga.jsp" donde el usuario descargará el fichero "cliente.ovpn". Por último, en la opción "Configuración de IP" se usará "config.jsp", donde el usuario podrá configurar la dirección IP del cliente por DHCP o de forma estática.

Por otro lado, si se inicia sesión con el usuario administrador, se accederá a "menuadmin.jsp" donde se puede elegir las tres opciones indicadas anteriormente. Si pulsamos "Mostrar usuario", se irá a la página "muestra.jsp" donde se mostrarán los usuarios definidos en base de datos y su estado de conexión con OpenVPN. Si pulsamos "Configuración de servidor", se irá a la página "config_server.jsp" que muestra la página para configurar los parámetros de OpenVPN. Por último, si pulsamos "Ver configuración actual", se irá a la página "config_actual.jsp" donde se tendrá la configuración actual del servidor OpenVPN.

También hay que objetar que todas las paginas tienen la opción de "Volver a la página anterior" excepto la página Principal. No obstante, las paginas "menu.jsp", "menuadmin.jsp" y "Pagina_usuario.jsp" son las únicas páginas donde el usuario puede cerrar sesión. Se ha elegido estas tres páginas debido a que dos de ellas corresponden con el menú principal y la otra indica la información relativa al usuario.

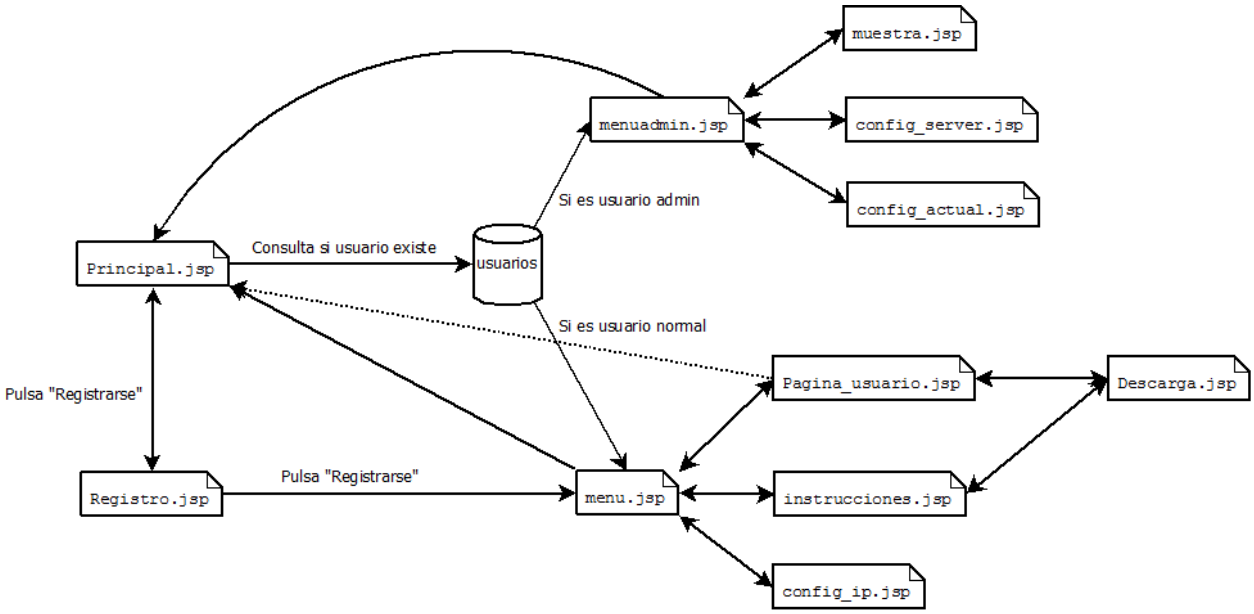


Figura 3-8. Estructura de páginas del proyecto

3.1.6 Diseño de BD

A continuación, se va a mostrar cómo se ha diseñado las tablas necesarias en BD para que el proyecto funcione correctamente, utilizadonse para ello, dos tablas.

La primera tabla es "USUARIOS", que se encargará de almacenar los datos personales del usuario y la información de conexión. En esta tabla, se tendrán como columnas los parámetros comentados anteriormente. Pero además de estos, se incluirá la columna "contraseña" que contendrá la contraseña que le quiera poner el usuario para luego iniciar sesión.

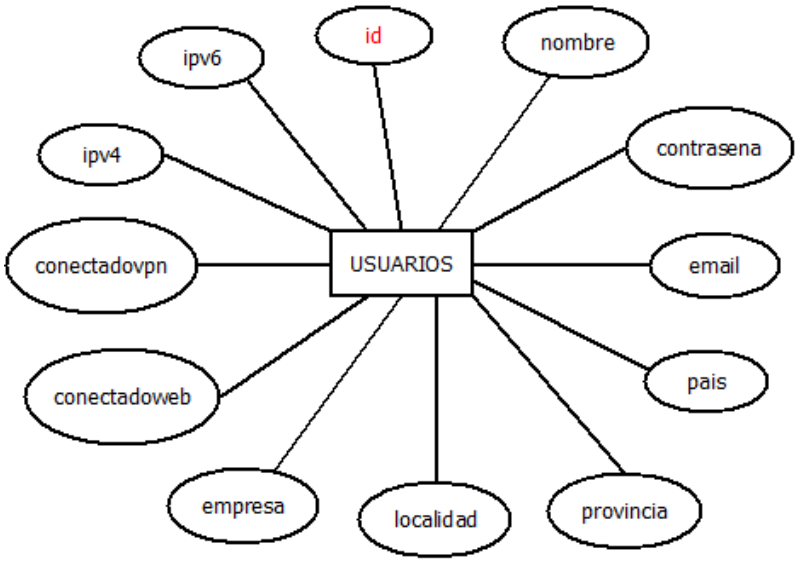


Figura 3-9. Tabla usuarios

En la siguiente tabla se muestra las columnas que se han configurado:

Columna	Tipo de dato
Id	SERIAL PRIMARY KEY
nombre	CHAR(20) NOT NULL
usuario	CHAR(20) NOT NULL
contrasena	CHAR(60) NOT NULL
Email	CHAR(40) NOT NULL
País	CHAR(2) NOT NULL
provincia	CHAR(20) NOT NULL
localidad	CHAR(40) NOT NULL
empresa	CHAR(40) NOT NULL
conectadoweb	int DEFAULT 0
conectadovpn	int DEFAULT 0
ipv4	CHAR(15)
ipv6	CHAR(39)

Tabla 3-1. Columnas tabla usuarios

Como se puede observar, todos los parámetros son cadenas de caracteres excepto "conectadoweb" y "conectadovpn". Se decidió ponerse como valor 0 cuando el usuario este desconectado tanto en VPN como en Web, y con valor 1, cuando el usuario esté conectado tanto en VPN como en Web. De esta forma, cuando el valor toma 1 se muestra en la página un icono de un tick verde indicando que está conectado, y un icono de una equis roja cuando está desconectado.

La segunda tabla es "PARAMETROS", que se encargará de almacenar los párameros de configuración necesarios para el servidor. Cuando el usuario administrador acceda a la página de configuración de párametros del servidor, aparecerán los datos correspondientes a las columnas de esta tabla.

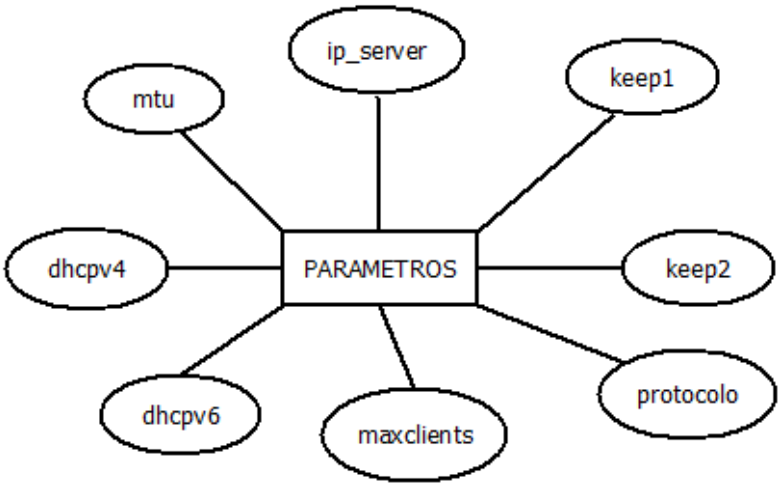


Figura 3-10. Tabla parámetros

En la siguiente tabla se muestra las columnas que se han configurado:

Columna	Tipo de dato
ip_server	CHAR(15) NOT NULL
keep1	int NOT NULL
keep2	int NOT NULL
protocolo	CHAR(3) NOT NULL
maxclients	int NOT NULL
dhcpv4	CHAR(20) NOT NULL
dhcpv6	CHAR(40) NOT NULL
mtu	int NOT NULL

Tabla 3-2. Columnas tabla parámetros

Como se puede observar, los valores que son enteros se especificarán en el fichero de configuración del servidor OpenVPN mediante scripts de sustitución de estos valores, que se verán en los siguientes apartados.

3.1.7 Diagrama de Actividades

En este apartado se elaborará un diagrama de actividades con la explicación del funcionamiento de cada una de las páginas. Para empezar, se va a realizar un diagrama de actividades con las páginas Principal y de Registro para acceder a la aplicación.

En la página principal, si el usuario no está registrado tendrá que pulsar el botón “Registrarse”, el cual le llevara a la página de registro. En esta página se tendrán unos campos a rellenar con datos del usuario. Tras rellenarlos y pulsar el botón “Registrarse”, se comprobarán que las credenciales son correctas. Para que esto ocurra, deberán de estar todos los campos rellenos y la contraseña deberá de tener una longitud mínima de 8 caracteres. Tras comprobar que las credenciales son correctas, se comprueba si el usuario es existente. En caso de que exista el usuario no se podrá crear indicándolo mediante un mensaje de error. Si el usuario no existe, se creará correctamente con sus certificados correspondientes, y se redirigirá al Menú Principal del usuario.

Si el usuario quiere iniciar sesión al estar registrado, debe rellenar los campos “Usuario” y “Contraseña”, comprobándose si el usuario en cuestión ya existe. Si el usuario no existe mostrará un mensaje de error. A continuación, se comprueba si la contraseña corresponde con la del usuario. Si la contraseña no corresponde se mostrará un mensaje de error. Por último, se comprueba si el usuario es el administrador. Si corresponde con el usuario administrador, se redirigirá al Menú Principal de administrador, sino se redirigirá al Menú Principal de usuario.

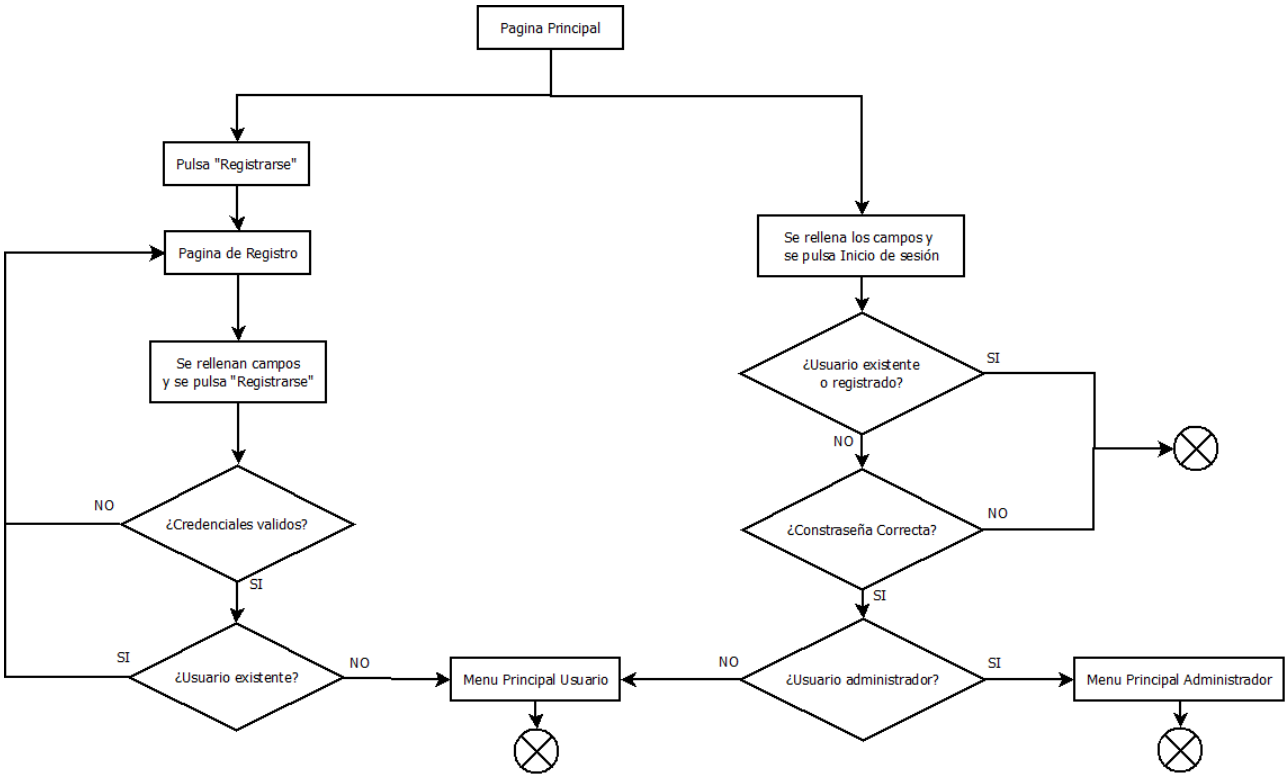


Figura 3-11. Diagrama de Actividades Página Principal

En segundo lugar, se va a realizar el diagrama de actividades para las funcionalidades de la página como un usuario normal.

La primera opción es "Información de usuario", donde al pulsar sobre esta aparecen los datos del usuario que están registrados en la Base de Datos. Antes de mostrar la información se comprueba si el usuario está conectado con OpenVPN al servidor. En caso de que esté conectado, aparecerán las direcciones IPv4 e IPv6 del usuario. En caso contrario, aparecerá vacía o con valor null. Tras mostrar los datos del usuario, se tienen tres opciones. La primera de ellas es "Eliminar cuenta" que al pulsar sobre ella eliminará la cuenta del usuario de base de datos, los certificados del usuario y la configuración de IP estática si tuviese. La segunda opción es "Descarga OVPN" que se encarga de redirigir a la página de descarga del fichero cliente.ovpn necesario para conectar con el servidor mediante OpenVPN. En esta página, se tiene la opción de "Descarga" que nos generará el fichero cliente.ovpn o de "Volver al Menú Principal" donde esta última nos redirigirá hacia el Menú Principal. La última opción es "Cerrar sesión" donde cerrará la sesión actual y redirigirá a la página Principal.

La segunda opción es "Instrucciones", donde al pulsar sobre esta nos aparecerá una página con las instrucciones de descarga de los distintos SO. Se tendrá links de descarga de OpenVPN para las diferentes plataformas, además de un link que nos llevará a la página de "Descarga" comentada anteriormente. Si se pulsa en el botón "Volver al Menú Principal", nos redirigirá hacia el Menú Principal.

La tercera opción es "Configuración de IP", donde se tendrán dos opciones a elegir. Si se pulsa DHCP se asignará la dirección IP mediante DHCP que tiene configurado el servidor OpenVPN. Si se pulsa "IP estática" aparecen los campos de IPv4 e IPv6 donde se pondrá la dirección estática que se quiere asignar. Tras poner las direcciones, se comprueba mediante patrones de HTML que corresponde con el formato para cada uno de los formatos de IP. Tras ello, se comprueba si la dirección corresponde a la del direccionamiento de la subred que se configura en el servidor tanto para IPv4 como IPv6. Después se comprueba si la IPv4 termina en ".0" o ".1" ya que son direcciones que son de subred y del servidor correspondientemente. A continuación, se comprueba si la IPv6 termina en "::" o "::1" ya que son direcciones de subred y del servidor correspondientemente. Por último, se comprueba si las direcciones han sido asignadas a otro usuario mediante DHCP o mediante IP estática. En caso de que se cumpla todo lo anterior, se creará un fichero de configuración con la configuración de las IPs estáticas específico para ese usuario y cuando se conecte se le asignará esas direcciones. En caso contrario, aparece el mensaje de error correspondiente con lo explicado anteriormente.

La última opción es “Cerrar sesión” que cerrará la sesión actual del usuario y redirigirá a la Página Principal.

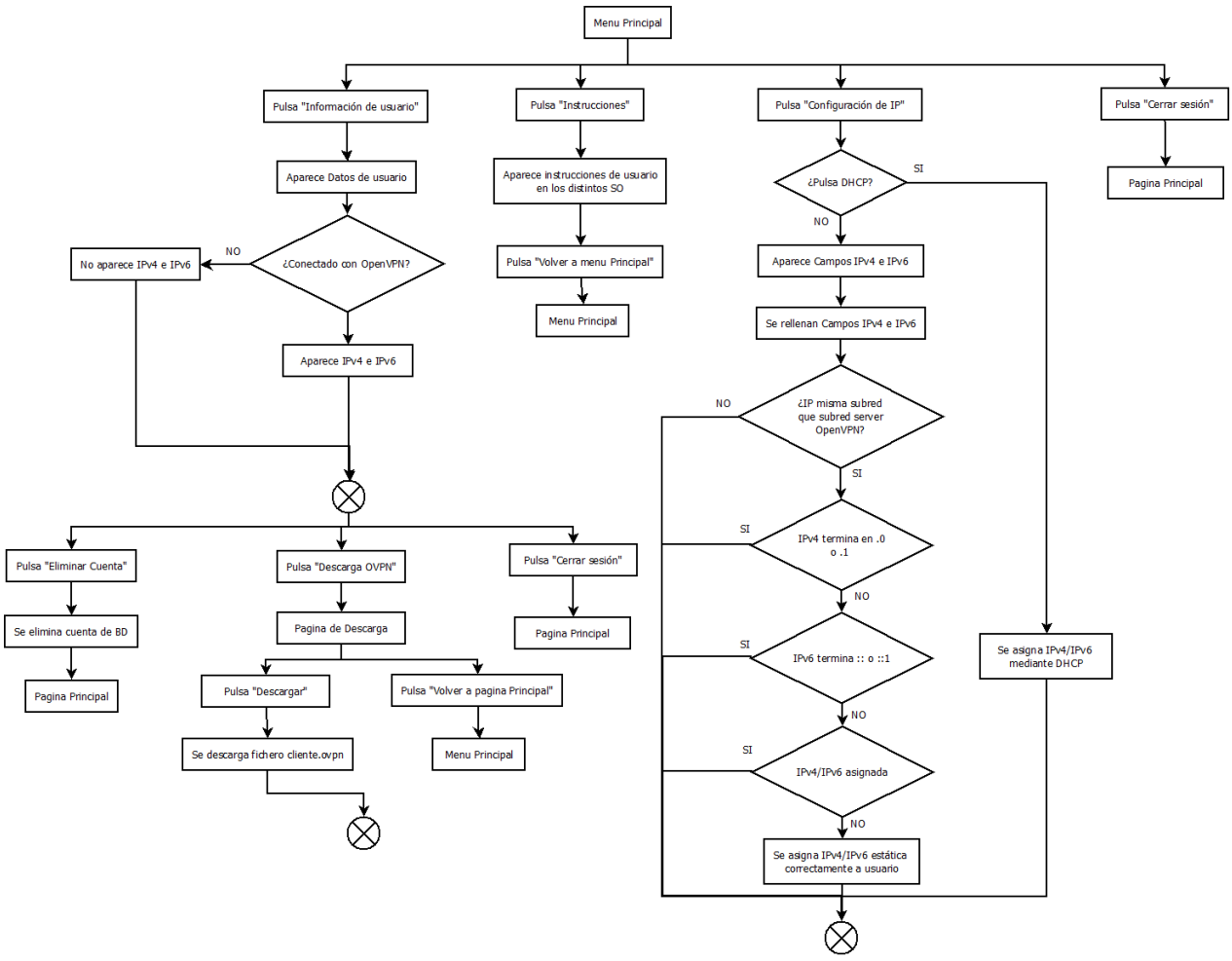


Figura 3-12. Diagrama de Actividades usuario

Por último, se va a realizar el diagrama de actividades para las funcionalidades de la página como usuario administrador, atendiendo a una serie de opciones al igual que en el diagrama anterior.

La primera opción es “Información de usuarios”, donde aparece una lista con los usuarios registrados en el sistema (en base de datos). Antes de mostrar la lista, se realizarán dos comprobaciones para rellenar los campos conectadoweb y conectadovpn. La primera comprobación es si el usuario está conectado a la web, que en caso de que esté conectado, aparecerá con un icono de tick verde. En caso contrario o por timeout de sesión, aparecerá con un icono con una equis roja. La segunda comprobación es si el usuario está conectado por VPN al servidor, en caso de que esté conectado aparecerá con un icono de tick verde. En caso contrario, aparecerá con un icono con una equis roja. Además, si el usuario está conectado por VPN aparecerán las direcciones IPv4 e IPv6 asignadas. Si no está conectado por VPN, aparecerá con valor null o vacío.

La segunda opción es “Configuración de servidor”, donde aparecen parámetros importantes a configurar en la VPN que son los comentados anteriormente. Al rellenar los parámetros y pulsar “Aplicar”, se comprueba para ello que los estos son correctos, en caso de los numéricos poniendo valores mínimos y máximos que debe tener. Para las direcciones de subredes IPv4 e IPv6 que proporcionará por DHCP el servidor, primero se comprueban que el formato de direcciones es correcto para IPv4 e IPv6. Después se comprueba si la dirección de subred IPv4 termina en “.0”. Por último, se comprueba si la dirección de subred IPv6 termina en “::”. Si hay algún error de comprobación aparecerá un mensaje de error con el error correspondiente. Después se aplicarán los cambios en el servidor y se reiniciará. Tras esto se reenvía a la página “Ver configuración Actual”.

La tercera opción es “Ver configuración Actual”, donde aparecerá el fichero de configuración actual del servidor.

La última opción es “Cerrar sesión” que cerrará la sesión actual del usuario y redirigirá a la página principal.

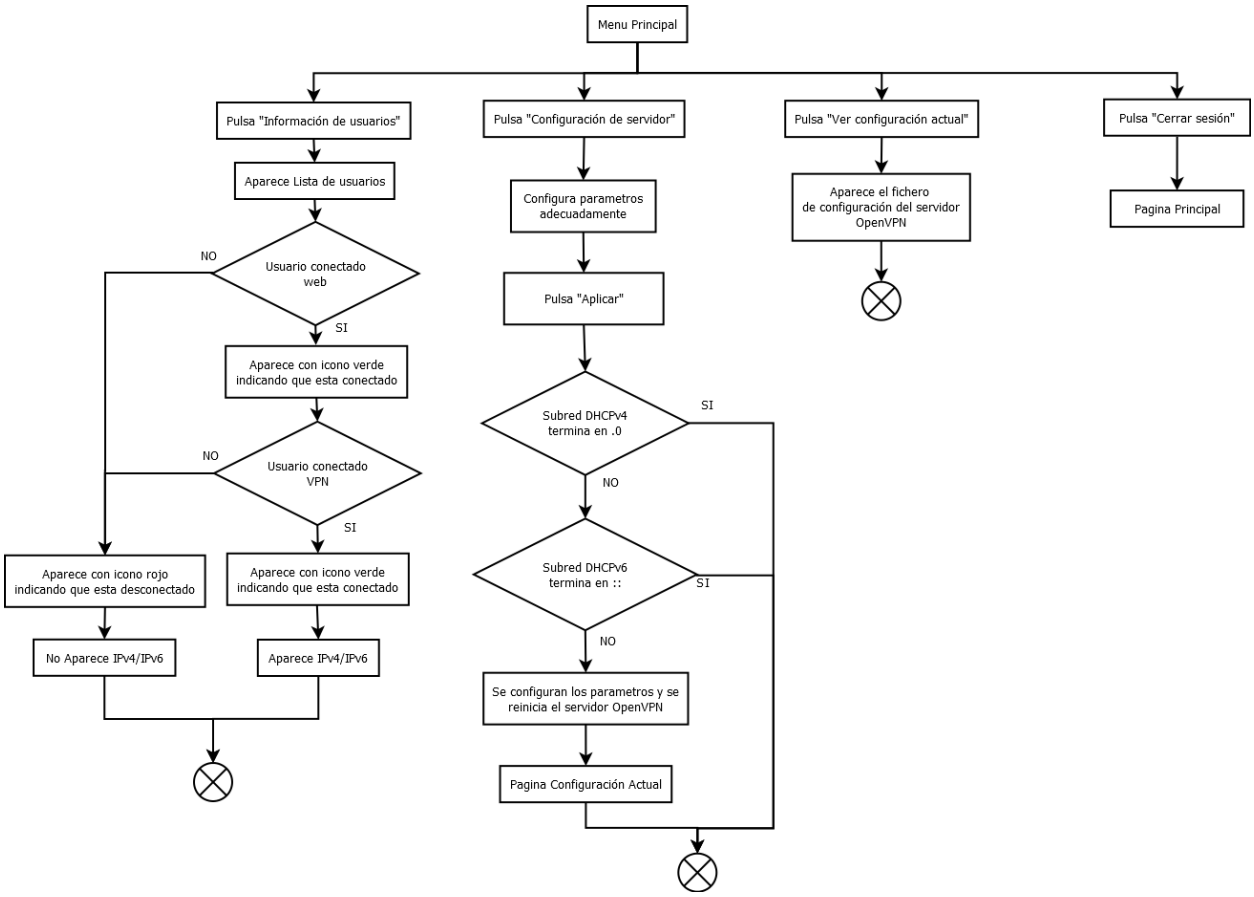


Figura 3-13. Diagrama de Actividades administrador

Además de lo anterior, se va a representar un diagrama con el uso de los scripts y clases en el proyecto en donde se explicará el funcionamiento de cada uno de ellos. Todos estos estarán incluidos en el Anexo A.

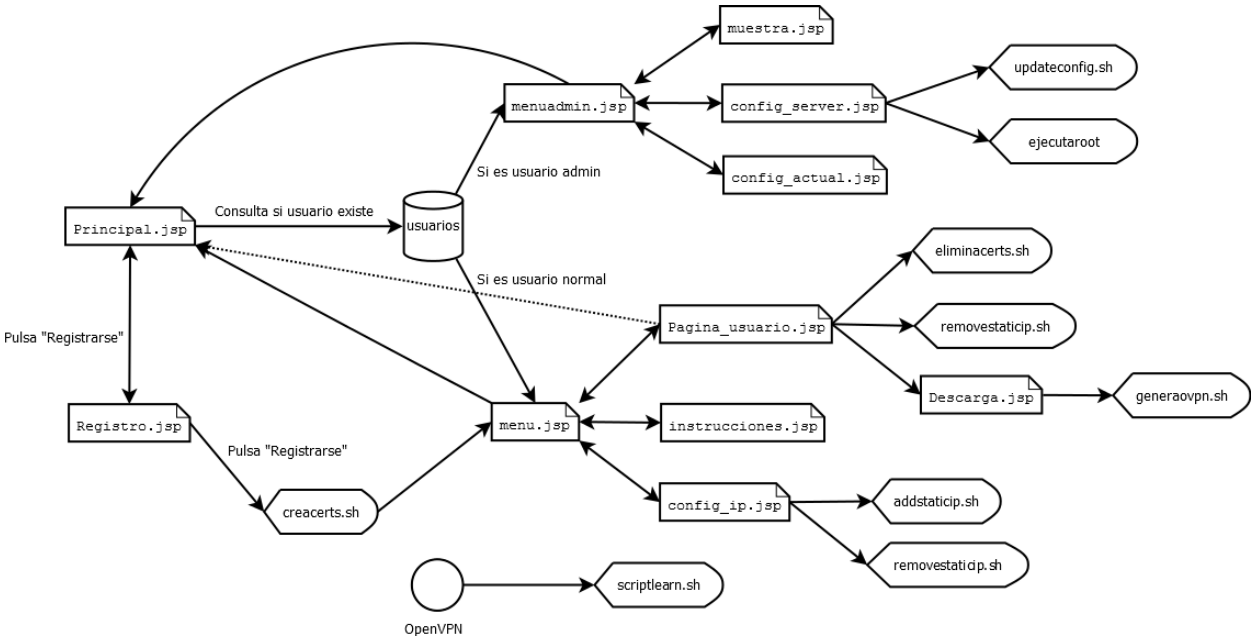


Figura 3-14. Diagrama de Scripts

El primer script que aparece en nuestra aplicación es “creacert.sh”, que se encarga de crear el certificado del cliente (cliente.cert) y la clave privada del cliente (cliente.key). Para ello se le pasa como parámetros los datos que se rellenan en “Registro.jsp”, los cuales se han explicado anteriormente. Este script utiliza los valores que

han sido validados en el registro de usuario para generar el certificado del cliente y su clave privada.

El segundo script que aparece en nuestra aplicación es “eliminacert.sh”, que se encarga de eliminar los certificados del cliente al realizar una revocación de certificado. Este script se le pasa como parámetro el usuario a eliminar que corresponde con el parámetro “common name” del certificado. Este script se utiliza solo cuando se elimina un usuario de la aplicación.

El tercer script que aparece en la aplicación es “addstaticip.sh”, que se encarga de crear un fichero de configuración para definir una IP estática a un usuario concreto. Este script se le pasa como parámetros los siguientes:

- Usuario: Corresponde al common name, que a su vez corresponde con el nombre del fichero de configuración para definir la IP estática que tendrá ese usuario. Este fichero estará en un directorio específico que se define en la configuración del servidor.
- IPv4: Dirección IPv4 asignada al usuario.
- Mask v4: Máscara de red IPv4 en formato normal (255.255.255.x).
- IPv6: Dirección IPv6 asignada al usuario.
- Mask v6: Máscara de red IPv6 en formato CIDR.

Este script se utiliza solo cuando se define una configuración de IP para el usuario en la opción “IP estática”, al rellenar los campos con la dirección IPv4 y máscara e IPv6 y máscara.

El cuarto script que se utiliza es “removestaticip.sh”, que se encarga de eliminar el fichero de configuración que define una IP estática a un usuario concreto. A este script se le indica como parámetro el nombre del usuario a eliminar que corresponde al “common name”, este será el nombre del fichero que se va a eliminar. Este script se utiliza en la configuración de IP cuando un usuario escoge la opción “DHCP”, que indica que el servidor OpenVPN le dará una dirección mediante DHCP. También se utiliza a la hora de eliminar un usuario, ya que el usuario a eliminar puede tener una IP estática definida, y por tanto, esta debe eliminarse.

El quinto script que se utiliza es “generaovpn.sh”, que se encarga de generar el fichero ovpn para el cliente cuyo nombre será “cliente.ovpn” cada vez que un usuario quiera descargar este fichero para conectarse con el servidor. Este script se le pasa como parámetro el usuario que corresponde con el “common name”, para que se inserten los certificados de este de forma embebida en un fichero que se llamará “<common_name>.ovpn” que será una copiará la configuración de una plantilla con nombre “cliente.ovpn”. Para ello, se copiará la configuración de la plantilla y se sustituirá en ““<common_name>.ovpn” los valores dentro de las etiquetas <ca>, <cert> y <key> por los valores etiquetados de la misma forma dentro de los ficheros ca.crt, common_name.crt y common_name.key. Este script se utiliza solo cuando se va a realizar la descarga del fichero ovpn, tanto en el botón dentro de la información de usuario, como en el link que aparece de descarga en “Instrucciones”.

El sexto script que se utiliza es “updateconfig.sh”, que se encarga de actualizar el fichero de configuración del servidor con la configuración puesta por el usuario administrador. Los parámetros que se le pasan al script son los parámetros a configurar por el administrador explicado anteriormente. Este script solo se utilizará en la opción “Configuración de servidor” al aplicar los cambios.

El séptimo script que se utiliza es “ejecutaroot” y no es un script, más bien es un ejecutable generado de un código en C. Este ejecutable se utilizará para reiniciar el servidor OpenVPN con los valores actualizados que ha puesto el administrador y para incluir las reglas necesarias para realizar el NAT y tener salida a Internet. Los parámetros que se le pasa son una cadena de caracteres con la IPv4 y máscara (formato CIDR), y otra cadena de caracteres con la IPv6 y máscara (formato CIDR). Este ejecutable solo se utiliza a la hora de aplicar los cambios en la opción “Configuración del servidor”.

Por último, el servidor OpenVPN ejecutará un script cada vez que se conecte o desconecte un cliente. Este script se llamará “scriptlearn.sh” y se encargará de añadir en base de datos las direcciones IPv4 e IPv6 asignadas al cliente. Este script recibirá como parámetros la IP la acción a realizar (que será añadir, eliminar o actualizar), la dirección (la dirección que aprende sea IPv4 o IPv6) y “el common user” (cliente conectado)

3.2 Implementación

En este apartado se mostrará cómo se ha llevado a cabo la realización del proyecto, tanto a nivel web como a nivel de red. La implementación se ha dividido en diversos apartados que serán importantes para la comprensión del proyecto.

3.2.1 Estructura de directorios

A continuación, se indica la estructura de directorios del proyecto donde se explicará el uso de cada uno de los directorios y los ficheros que contendrán.

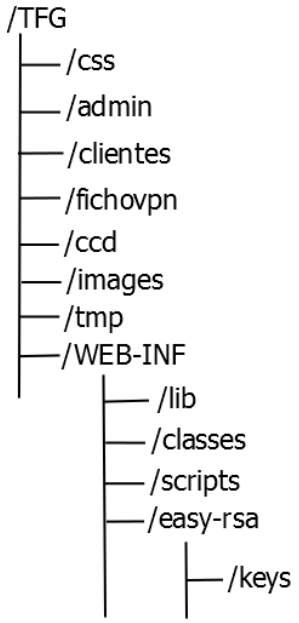


Figura 3-15. Estructura de directorios

En el directorio ***css*** se tendrán las hojas de estilos que se han utilizado en el proyecto. El formato de los ficheros por tanto será ".css".

En el directorio ***admin*** se tendrá el contenido web de las páginas relacionadas con el usuario administrador. El formato de los ficheros será ".jsp".

En el directorio ***clientes*** se tendrá el contenido web de las páginas relacionadas con los clientes o usuarios normales. El formato de los ficheros será ".jsp".

En el directorio ***fichovpn*** se tendrá el fichero cliente.ovpn que podrá ser modificado por el administrador y que se utilizará para que los clientes lo descarguen.

El directorio ***images*** tendrá las imágenes que se han utilizado en la aplicación. Estas imágenes serán utilizadas para fondos, logos o botones.

En el directorio ***WEB-INF*** se tendrá la parte privada del servidor Tomcat, es decir, se tendrán los directorios y carpetas que solo podrá controlar Tomcat. Dentro de este se tendrá distintos subdirectorios.

El subdirectorio ***lib*** tendrá las librerías necesarias para el funcionamiento de la página. En este caso, solo tendrá la librería utilizada para los métodos relacionados con PSQL.

El subdirectorio ***java*** tendrá el código fuente Java que utilice la aplicación para generar de estos las clases correspondientes. El formato de los ficheros será ".java".

El subdirectorio ***classes*** tendrá el código fuente Java y las clases generadas que se utilizan en la aplicación. En este caso, se utilizarán dos clases para verificar si una IP pertenece a una dirección de subred aplicando su máscara de red y una clase que servirá de SessionListener para cuando se cierre la sesión por timeout. El formato de los ficheros serán ".class" y ".java".

El subdirectorio ***scripts*** contendrá los scripts utilizados en la aplicación.

El subdirectorio ***easy-rsa*** tendrá todos los componentes del programa easy-rsa, que se encargará de gestionar los certificados a la hora de la configuración del cliente y servidor OpenVPN. En su interior contiene los scripts necesarios para la generación, gestión y destrucción de certificados.

Dentro de easy-rsa se tendrá un directorio ***keys*** que contendrá todos los ficheros de certificados, claves privadas y públicas, lista de certificados registrados en la BD de easy-rsa y lista de revocación de certificados.

3.2.2 Configuración de OpenVPN

En este apartado se verán los pasos a seguir para la configuración de OpenVPN para el escenario cliente-servidor. La configuración de OpenVPN sigue 3 pasos fundamentales:

- Generación de certificados.
- Configuración del fichero de configuración del servidor.
- Configuración del fichero de configuración del cliente.

Tras realizarse los tres pasos anteriores, que se irán comentando a continuación, cliente y servidor intercambiarán mensajes para sincronizarse uno con otro. En la siguiente imagen, se indicará el intercambio de mensajes para el establecimiento del túnel VPN entre el cliente y el servidor:

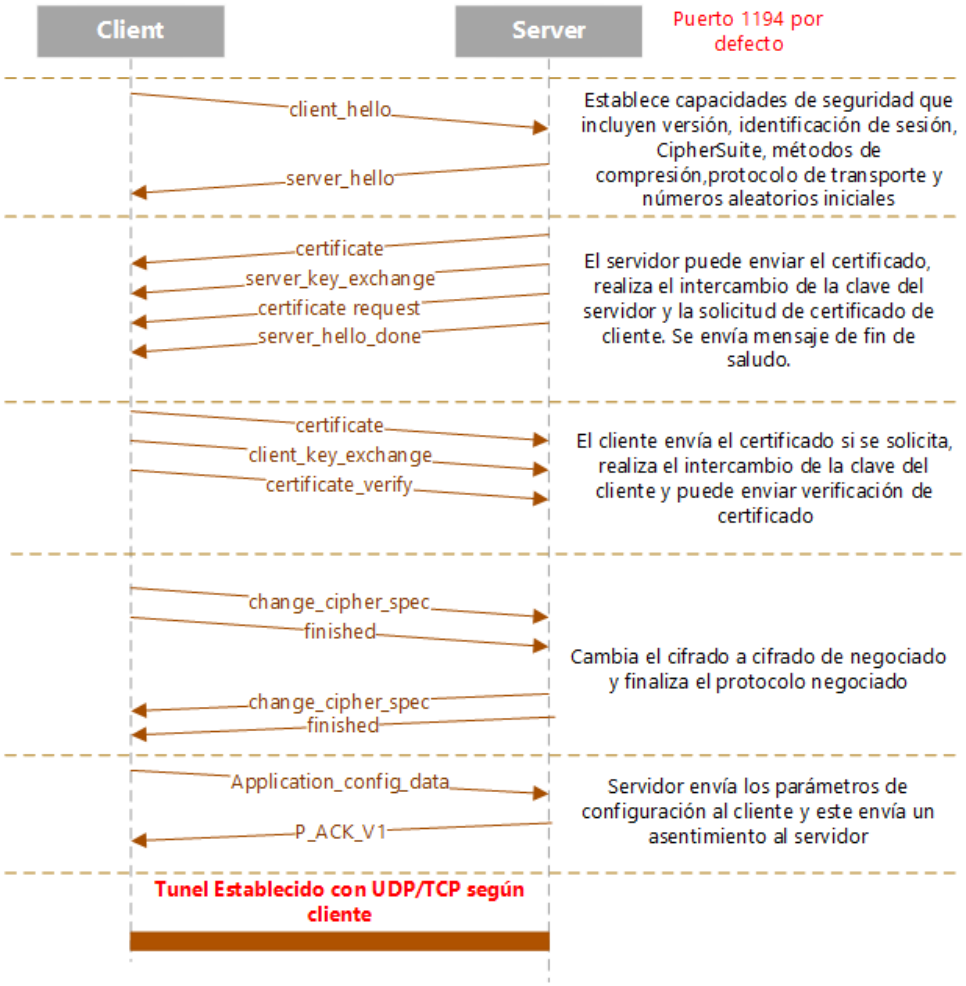


Figura 3-16. Diagrama paso de mensajes OpenVPN

Tras sincronizarse, el cliente ya tiene establecido un túnel con el servidor, y por tanto, podrá alcanzarlo ya que están en la misma subred. En el caso de que se conecten varios clientes, si se envía un mensaje desde un cliente a otro, este mensaje pasará primero por el servidor, y este reenviará los mensajes al otro cliente.

3.2.2.1 Generación de certificados

La generación de los certificados es la parte más importante a la hora de configurar OpenVPN, ya que sin estos no pueden comunicarse cliente y servidor. Los certificados necesarios para la comunicación entre cliente y servidor son los siguientes:

Nombre del archivo	Es necesario para	¿Qué es?	¿Debe ser secreto?
ca.crt	Servidor y todos los clientes	Certificado para el CA	NO
ca.key	Solo el ordenador con clave para firmar	Clave para el CA	SI
dh2048.pem	Servidor	Parámetros de Diffie Helman	NO
Servidor.crt	Servidor	Certificado para el servidor	NO
Servidor.key	Servidor	Clave privada para el servidor	SI
Cliente1.crt	Cliente	Certificado para el cliente 1	NO
Cliente1.key	Cliente	Clave para el cliente 1	SI
Ta.key (Opcional)	Servidor y Clientes	Llave TLS-AUTH	SI

Tabla 3-3. Certificados necesarios OpenVPN

Los certificados se gestionan dentro del equipo que ejerce de servidor OpenVPN. Para ello se utiliza easy-rsa, que es una gran herramienta de automatización en la creación de certificados digitales y claves RSA. También permite gestionar la revocación de estos certificados y generar módulos *Diffie-Hellman*, necesarios para ejecutar un servidor OpenVPN [38]. Dentro del directorio easy-rsa se tendrán los scripts para la generación, modificación y revocación de certificados. Todos los certificados y claves privadas y públicas estarán en el subdirectorio keys. Además, contendrá los siguientes ficheros que serán importantes a la hora de controlar la generación y revocación de certificados, ya que easy-rsa tiene una base de datos de certificados y puede saber en todo momento el total de certificados generados y cuales están activos o revocados. Estos ficheros son:

- index.txt: Esta es la "base de datos maestra" de todos los certificados emitidos.
- serial: Almacena el siguiente número de serie (incremento de números de serie) del siguiente certificado que se creará.
- crl.pem: Es una lista de revocación de certificados que proporciona una lista con los certificados que se han revocado.
- revoke-test.pem: Fichero que se utiliza para comprobar que el certificado ha sido revocado mediante openssl.

Para la generación de certificados se accederá al directorio easy-rsa y se utilizarán los siguientes scripts:

- source ./vars: Este comando sirve para cambiar los valores por defecto de las variables a configurar a la hora de crear los certificados. Es un comando opcional, ya que al crear los certificados nos preguntará por los parámetros para rellenarlos.
- ./clean-all: Elimina cualquier clave o certificado que se haya creado en la ruta del easy-rsa.
- ./build-ca: Crea un CA (Certificate autentity) mediante valores que se van mostrando por pantalla. Creará un fichero ca.crt y un fichero ca.key. El fichero ca.key es la clave privada utilizada para firmar los certificados de su servidor y de los clientes. Si se pierde, ya no puede confiar en ningún certificado de esta autoridad de certificación, y si alguien puede acceder a este archivo, puede firmar nuevos certificados y acceder a su VPN sin su conocimiento. Por esta razón, OpenVPN recomienda almacenar ca.key en una ubicación que pueda estar fuera de línea tanto como sea posible, y que solo debe activarse al crear nuevos certificados. Estos valores son:
    - KEY_COUNTRY: País (Solo las dos iniciales).
    - KEY_PROVINCE: Provincia.
    - KEY_CITY: Ciudad.
    - KEY_ORG: Organización.

- KEY_EMAIL: Email.
- KEY_OU: Nombre de unidad de organización. Será igual que la organización.
- KEY_NAME: Nombre.

- ./build-key-server server: Script para generar la clave y el certificado para el servidor llamados "server". Se irán rellenando los valores correspondientemente. Si se añade una contraseña, al conectar el cliente con el servidor por VPN, el cliente tendrá que escribir la contraseña. En nuestro caso, no se ha implementado contraseña, ya que se quiere en un futuro que empresas utilicen el túnel VPN.
- ./build-dh: genera un archivo de intercambio de claves Diffie-Hellman con nombre "dh2048.pem" o "dh1024.pem" dependiendo del tamaño en bits que puede ser de 1024 o 2048 bits. Se recomienda por seguridad que la clave sea de 2048 bits.
- ./build-key client: Script para generar clave y certificado para el cliente llamado "client". Para cada cliente, se tendrá que ejecutar este script. Esta clave y certificado servirán para que el servidor OpenVPN autentique a cada cliente.

3.2.2.2 Configuración de servidor

Tras la generación de certificados, se debe realizar la configuración del servidor para el funcionamiento de la red VPN, en donde se encontrarán los clientes y el servidor comunicándose mediante túneles VPN. El fichero de configuración que se ha usado se llama "server.conf", aunque puede tener cualquier otro nombre. Este fichero contendrá parámetros de configuración para la creación de un servidor OpenVPN.

A continuación, se explican los parámetros más importantes de este fichero de configuración (Ver fichero de configuración en Anexo 1).

Comando	Descripción
port 1194	Define el puerto en el que estará escuchando el servidor. Por defecto, es el puerto 1194.
proto udp	Indica el protocolo que se utiliza para la comunicación remota.
dev tun	Indica el dispositivo TUN/TAP de red virtual que se utilizará.
server ipv4_subnet subnet_mask	Configura un servidor OpenVPN que se comporta como un servidor DHCP que va dando direcciones a los clientes dentro de un rango "ipv4_subnet" y una máscara "mask" para IPv4.
ca /ruta/ca.crt	Indica el Archivo de autoridad de certificación (CA).
cert /ruta/server.crt	Indica el certificado para el servidor.
key /ruta/server.key	Indica la clave para el servidor.
dh /ruta/dh2048.pem	Indica el archivo de intercambio de claves Diffie-Hellman.
crl-verify /ruta/crl.pem	Verifica el certificado de pares con el archivo crl en formato PEM. Se utiliza cuando se utiliza un certificado que ha sido revocado pero no se ha eliminado los correspondientes .crt y .key.
reneg-sec n	Renegocia la clave de canal de datos después de n segundos.
push "redirect-gateway def1 bypass-dhcp"	Pone en la configuración del cliente, la opción "redirect-gateway" que ejecuta automáticamente los comandos de enrutamiento para hacer que todo el tráfico IP saliente se redirija a través de la VPN. Con el parámetro "def1" para anular la puerta de enlace predeterminada utilizando 0.0.0.0/1 y 128.0.0.0/1 en lugar de 0.0.0.0/0 pero sin eliminar la puerta de enlace predeterminada y "bypass-dhcp" que agrega una ruta directa al servidor DHCP (si no

	es local) que omita el túnel (Se usa generalmente para clientes Windows).
push "dhcp-option DNS X.X.X.X"	Pone en la configuración del cliente, utilizando dhcp-options DNS para establecer el servidor de nombres de dominio primario IPv4. En este caso, por ejemplo se puede poner "8.8.8.8" que se corresponde con los DNS de Google.
client-config-dir /ruta/	Especifica un directorio de directorio para los archivos de configuración de cliente personalizados. Los archivos de configuración se llamarán con el nombre común ("common name"), que es el nombre común en el certificado asociado con el cliente vinculado a esta dirección. En este caso, se utilizará para definir en el fichero de configuración una IP estática para el cliente que lo solicite. Para ello se han utilizado los siguientes comandos dentro del fichero de configuración concreto del cliente: • ifconfig-push ipv4 netmask: Define la IPv4 de la interfaz del túnel con su máscara de red. • ifconfig-ipv6-push: Define la IPv4 de la interfaz del túnel con su máscara de red.
topology subnet	Configura la topología de direccionamiento virtual cuando está activo –dev tun. Se ha puesto como parámetro "subnet", ya que se tratará el direccionamiento como si todos los clientes y el servidor estuviesen dentro de una subred para poder conectar entre ellos.
status /ruta/file n	Escriba el estado operativo de los equipos activos para archivar cada n segundos.
learn-address "/ruta/script.sh"	Ejecuta el comando/script script.sh para validar las direcciones o rutas virtuales del cliente. Dentro de este script, se puede validar las direcciones de los clientes que se añaden, actualizan o eliminan. En caso, de que pase alguna de estas, se pueden utilizar diferentes comandos. En nuestro caso, se ha utilizado para que cuando se añada o actualice la conexión de un cliente, para las direcciones asignadas, tanto ipv4 como ipv6, se ponga en BD la variable que se ha conectado por VPN con el servidor y se añadan en BD las direcciones que se han asignado. Y en caso de que se elimine la conexión del cliente, se elimine en BD las direcciones que se han asignado al cliente.
client-to-client	Se utiliza para que los clientes estén conectados entre sí y tengan comunicación entre ellos. Si no estuviese esta opción, los clientes solo estarían conectados con el servidor y solo tendrían comunicación con este.
mute-replay-warnings	Silencia la salida de las advertencias de repetición, que son una falsa alarma común en las redes WiFi. Es un parámetro opcional en caso de que el servidor esté conectado por Wifi.
server-ipv6 ipv6_subnet/mask	Configura un servidor OpenVPN que se comporta como un servidor DHCP que va dando direcciones a los clientes dentro de un rango "ipv6_subnet" y una máscara "mask" para IPv6.
push "route-ipv6 2000::/3"	Esta opción hace que el servidor indique al cliente que enrute el tráfico de ipv6 a 2000::/3 (es decir, a toda la red de ipv6) a través del VPN.
push "route-ipv6 ::/0"	Esta opción hace que el servidor indique al cliente que enrute el tráfico de ipv6 a ::/0 (es decir, a toda la red de ipv6) a través del VPN.

push "redirect-gateway def1 ipv6"	Similar a “redirect-gateway def1” pero con la opción “ipv6”, que redirige el enrutamiento de IPv6 en el túnel. Esto funciona de manera similar al indicador def1, es decir, se agregan rutas IPv6 más específicas (2000::/4, 3000::/4), que cubren todo el espacio de unidifusión IPv6.

Tabla 3-4. Parámetros de configuración servidor

Por último, tras tener preparado el fichero de configuración, el usuario administrador desde el equipo servidor realizarará lo siguiente (Estos comandos son para Linux, para otro S.O serán diferentes):

- Activar el servidor OpenVPN: systemctl restart openvpn@server.service.
- Activar IPv6: con los comandos “echo 0 > /proc/sys/net/ipv6/conf/all/disable_ipv6” o “net.ipv6.conf.all.disable_ipv6=0” en /et/sysctl.conf.
- Activar el reenvío IP mediante modificación de /etc/sysctl.conf poniendo “net.ipv4.ip_forward=1” y “net.ipv6.conf.all.forwarding=1” o realizar “echo 1 > /proc/sys/net/ipv4/ip_forward” y “echo 1 > /proc/sys/net/ipv6/conf/all/forwarding”.
- Configurar el cortafuegos de iptables para que se reenvié por la interfaz adecuada. Para ello, se pueden utilizar los siguientes comandos (en el caso de que el operador de red ofrezca IPv6 y para el caso en el que se utiliza NAT):
    - iptables -t nat -A POSTROUTING -s 10.11.0.0/24 -o eth0 -j MASQUERADE.
    - ip6tables -t nat -A POSTROUTING -s aaaa:bbbb:cccc:dddd:80::/112 -o eth0 -j MASQUERADE. (será eth0 si el operador de red ofrece IPv6 o sit1 que corresponde al túnel de Hurricane).

3.2.2.3 Configuración de Cliente

La configuración del cliente se podría decir que es uno de los últimos pasos para el funcionamiento del túnel OpenVPN con el servidor. Este paso final tiene como objetivo el establecimiento de los parámetros del fichero de configuración del cliente que conectará con el servidor. A continuación, se indican los parámetros más importantes dentro del fichero de configuración:

Comando	Descripción
client	Indica que se trata de un cliente OpenVPN.
proto udp	Indica el protocolo que se utiliza para la comunicación remota.
remote 192.168.1.144 1194	Indica al cliente la dirección IP del servidor que quiere conectarse y el puerto con el que lo hará.
resolv-retry infinite	Nos indica que si la resolución del nombre de host falla para remoto, vuelva a intentar la resolución durante n segundos antes de fallar. En este caso, se reintenta indefinidamente (parámetro “infinite”).
route-delay 2	Espera n segundos después del establecimiento de la conexión antes de de agregar rutas.
pull	Esta opción debe utilizarse en un cliente que se está conectando a un servidor con varios clientes.
comp-lzo yes	Activar compresión LZO para la transmisión de datos.
dev tun	Indica el dispositivo TUN/TAP de red virtual que se utilizará.

nobind	No vincular a la dirección local y el puerto.
mute-replay-warnings	Silencia la salida de las advertencias de repetición, que son una falsa alarma común en las redes WiFi. Es un parámetro opcional en caso de que el servidor esté conectado por Wifi.
<ca> CERTIFICATE CA </ca>	Inserta el certificado ca a través etiquetas inline donde se indica el certificado completo en texto plano.
<cert> CERTIFICATE CLIENT </cert>	Inserta el certificado del cliente a través etiquetas inline donde se indica el certificado completo en texto plano.
<key> PRIVATE KEY </key>	Inserta la clave del cliente a través etiquetas inline donde se indica el certificado completo en texto plano.

Tabla 3-5. Parámetros de configuración cliente

Finalmente, tras tener preparado el fichero de configuración, en la ventana de comandos se ejecutan lo siguiente para Linux:

- echo 0 > /proc/sys/net/ipv6/conf/all/disable_ipv6: Activa IPv6.
- openvpn --config /ruta/cliente.ovpn &: Ejecuta OpenVPN con el fichero de configuración del cliente especificado en /ruta/cliente.ovpn.

Una vez ejecutado los comandos, ya tendríamos establecida la conexión con el servidor y se habrá creado correctamente el túnel IPv4/IPv6 entre el cliente y el servidor.

3.2.3 Despliegue

En este apartado se explicará el funcionamiento completo de la aplicación. Esta aplicación puede competir con Hurricane Electric, ya que en caso de tener un proovedor de red IPv6, no se necesitaría ningún uso del tunnelbroker de Hurricane Electric. Además, esta aplicación permite a los usuarios configurar el direccionamiento de forma estática o mediante DHCP, algo que no es posible con Hurricane Electric. También permite visualizar a los usuarios el direccionamiento que tienen dentro de la página información de usuario, ademas incluye una página específica con las instrucciones de la instalación para todos los S.O. Es importante destacar, la funcionalidad que tiene esta aplicación a nivel de administración, ya que el usuario administrador podrá configurar parámetros de funcionamiento de los tuneles VPN como el direccionamiento IPv4 e IPv6, MTU y los otros parámetros comentados anteriormente que se refieren. Esta funcionalidad, no se podría realizar mediante el tunnelbroker de Hurricane Electric. Tampoco se realizaría el control de usuarios conectados tanto a la página web como mediante OpenVPN y el poder visualizar el fichero de configuración del servidor desde la página web sin tener que acceder al directorio.

A continuación, se va a mostrar el funcionamiento de la página desplegada. Para ello, se necesitará un servidor Tomcat en la máquina que se encargará de publicar el contenido web. Opcionamente, se puede tener un servidor Apache funcionando con Tomcat. Dentro de la configuración de Tomcat, hay que configurar la exportación de la carpeta web que se quiere mostrar. Tras ello, ya estará accesible la web. A continuación, se muestran imágenes de las páginas del proyecto.

Figura 3-17. Página Principal

Figura 3-18. Página de Registro

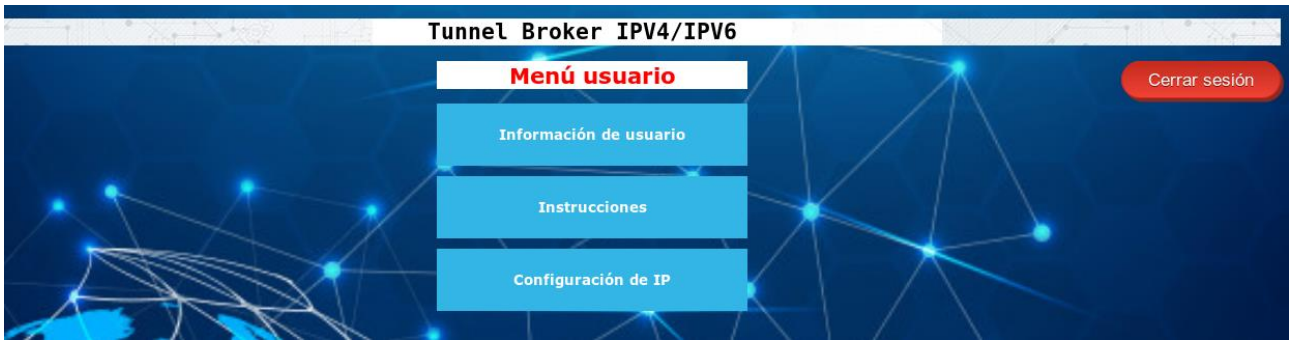


Figura 3-19. Menú usuario

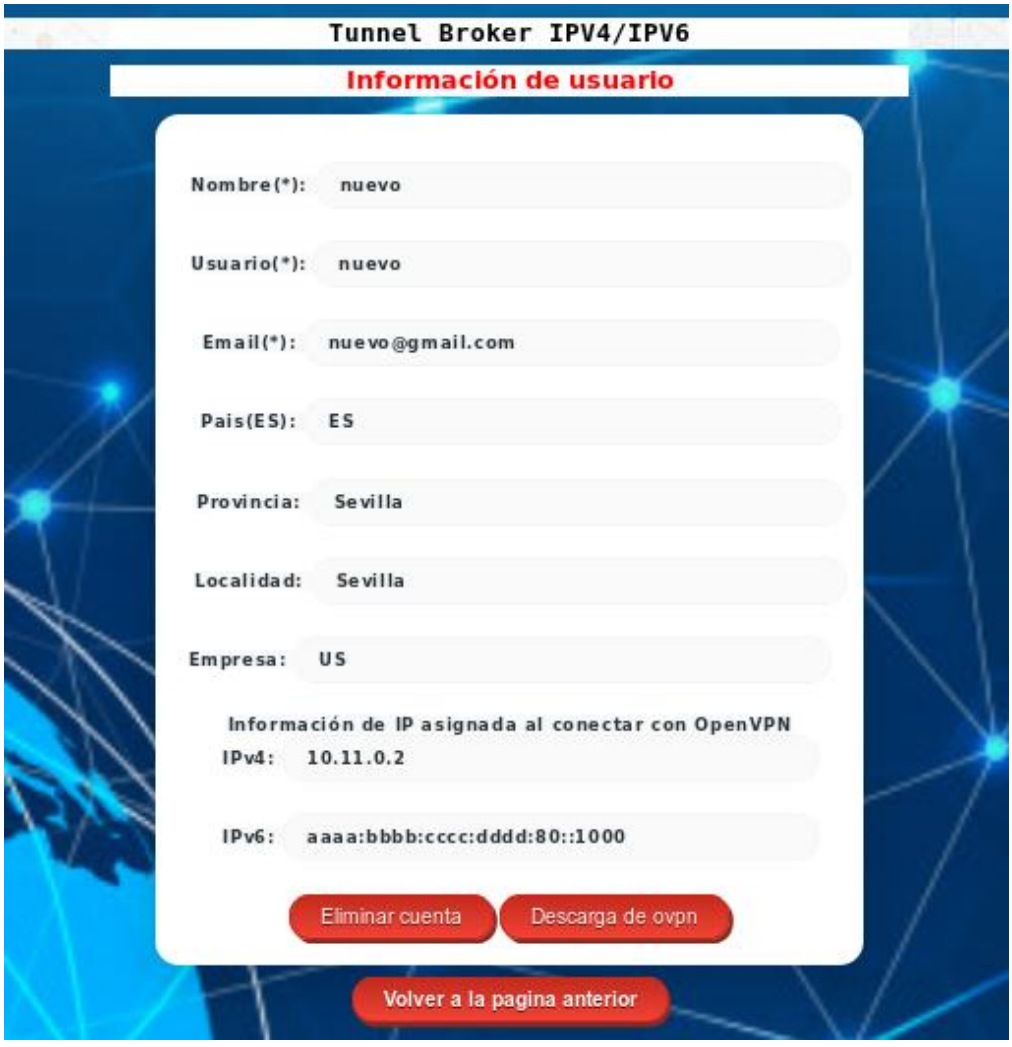


Figura 3-20. Información de usuario

Figura 3-21. Descarga

Figura 3-22. Instrucciones

Figura 3-23. Configuración IP 1

Figura 3-24. Configuración IP 2

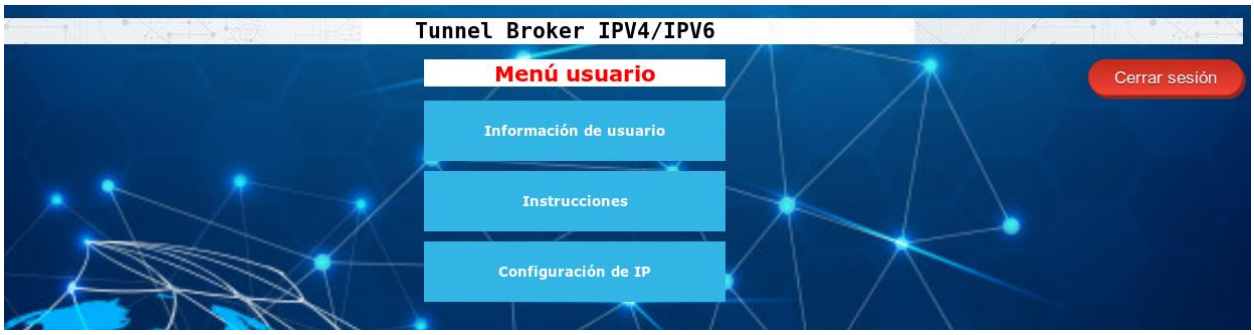


Figura 3-25. Menú administrador

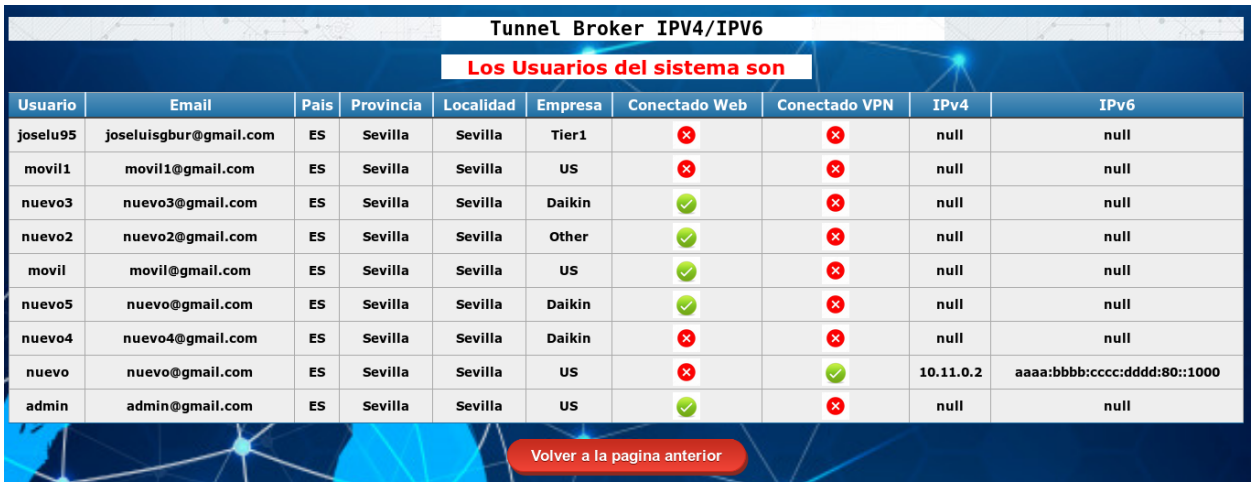


Figura 3-26. Usuarios del sistema

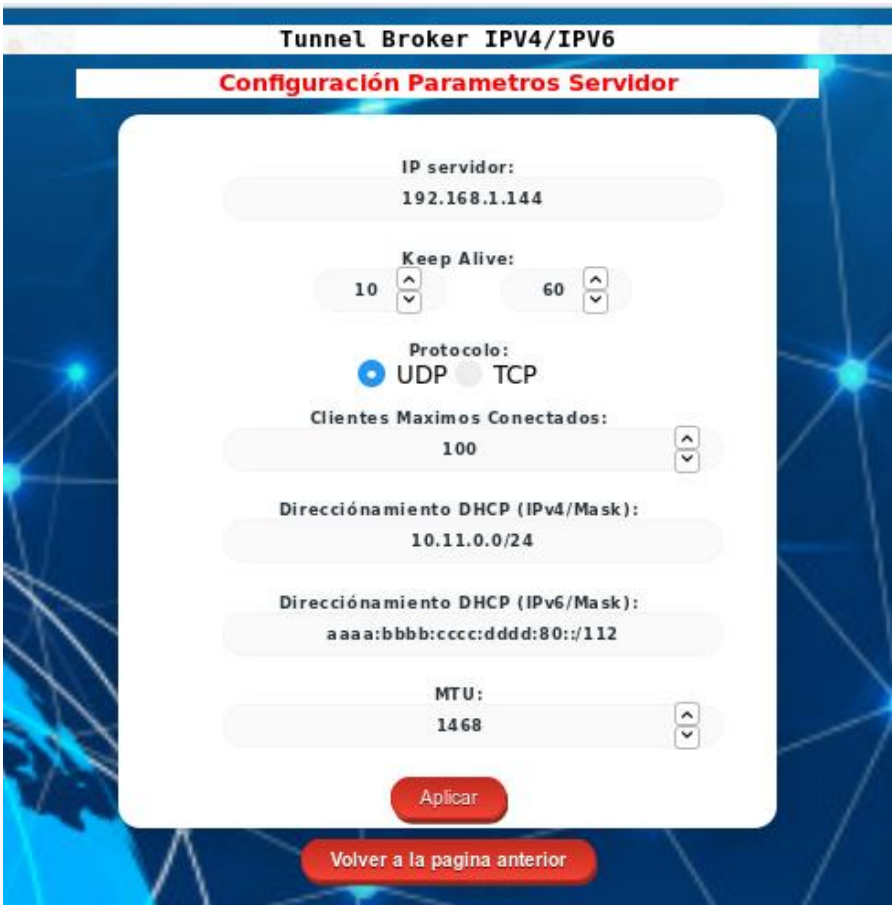


Figura 3-27. Configuración de parámetros

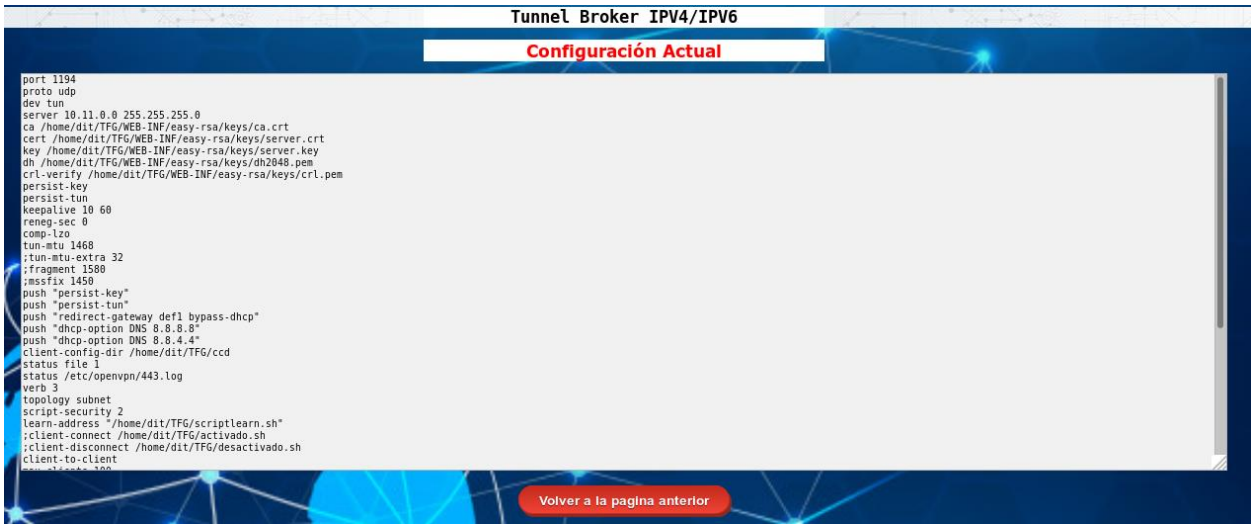


Figura 3-28. Configuración Actual

3.2.4 Comparativa entre modelo Real y modelo Simulado

El modelo comentado anteriormente en el diagrama de red, se corresponde con el modelo real que se va a utilizar. Sin embargo, el modelo simulado que se explicará será diferente, puesto que hay algunos aspectos que no se tienen en cuenta.

El modelo Simulado que se presenta utiliza un tipo de VPN Point-to-Point, es decir, que el túnel VPN no será dentro de la red interna, sino que será un túnel a través de Internet entre un equipo que está en una sede hacia el equipo servidor que estará en otra sede. En este escenario, el router tiene direccionamiento IPv6 incorporado y, por tanto, se redirigirá a Internet IPv6 a través del router de operador. Por lo que, en este escenario solo hará falta dos interfaces de red:

- eth0: Salida normal hacia el router que proporciona Internet mediante IPv4 e IPv6.
- tun0: Túnel Interno creado por OpenVPN.

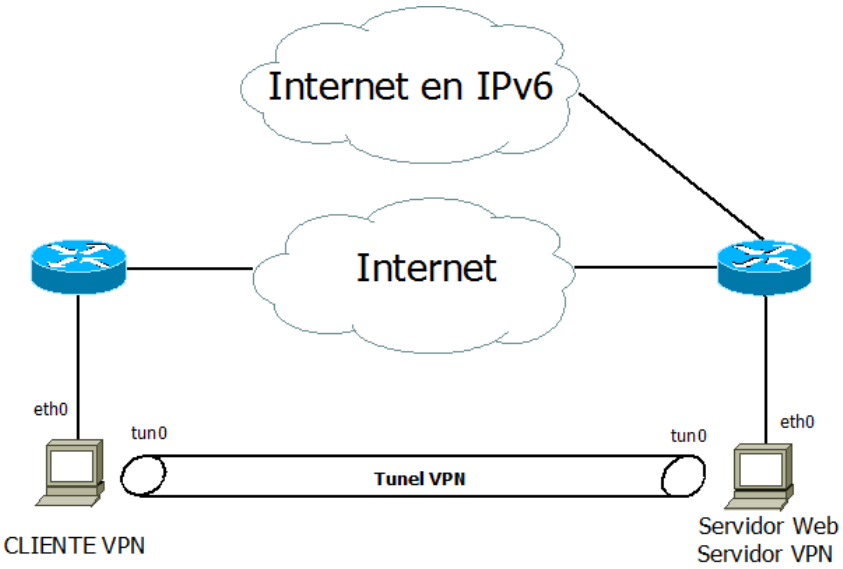


Figura 3-29. Modelo Simulado

Este modelo simulado se ha realizado mediante GNS3. Se han utilizado tres máquinas virtuales con Centos7:

- 2 clientes VPN.
- 1 servidor VPN.

La salida a Internet mediante IPv6 se muestra como la conexión con un servidor IPv6 que esta externo a nuestra red, aunque aparezca conectado al mismo router. Se ha realizado así, para simular que el router tiene IPv6 y, por tanto, puede redireccionar los paquetes a través de Internet IPv6.

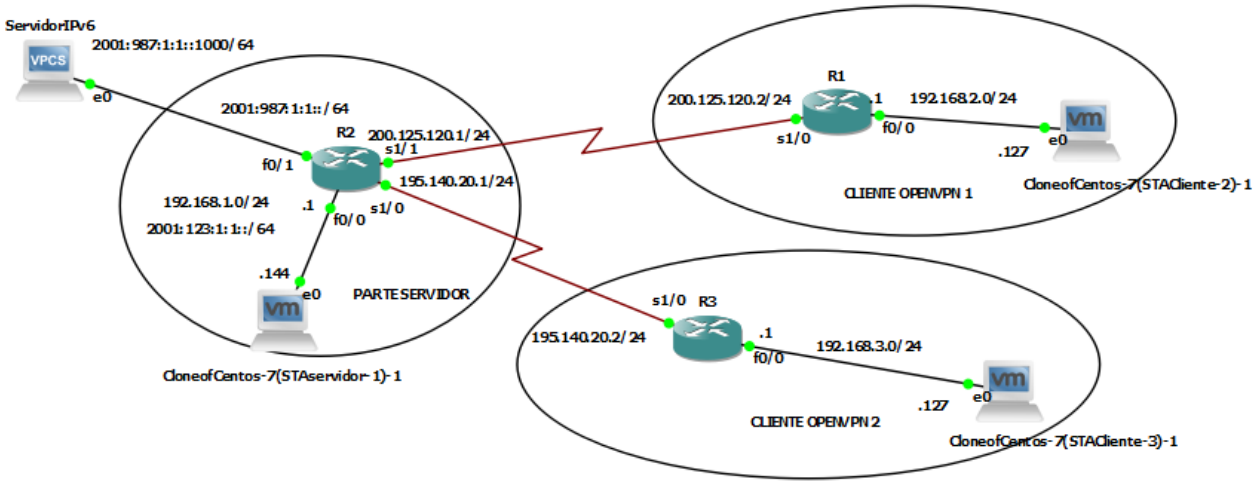


Figura 3-30. Modelo GNS3

Para completar este primer estudio, se va a realizar la siguiente comparativa entre ambos modelos:

Modelo Real	Modelo Simulado
Tipo de VPN interna (over LAN)	Tipo de VPN Point-to-Point
Necesita 3 interfaces (eth0,tun0 y sit1)	Necesita 2 interfaces (eth0,tun0)
Necesita un túnel de Hurricane para conexión a Internet por IPv6	Router de operador proporciona Internet IPv6
Limitado a usuarios que estén en la misma LAN	Para cualquier usuario de Internet
Uso de NAT para redirigir por las dos interfaces que proporcionan Internet tanto en IPv4 como IPv6	Uso de NAT solo en una interfaz que proporcionará tanto Internet IPv4 como IPv6
Retardo pequeño	Retardo Normal

Tabla 3-6. Comparativa Modelo Real – Modelo Simulado

4 PRUEBAS

El progreso y el desarrollo son imposibles si uno sigue haciendo las cosas tal como siempre las ha hecho.

-Wayne Dyer -

En este capítulo se va a describir las pruebas que se han realizado con los dos modelos: Modelo Real y modelo Simulado. Para ello se llevarán a cabo tres pruebas fundamentales para cada uno de los modelos que son las siguientes:

- Verificación de conectividad IPv6 entre los clientes: Se verificará si se tiene conectividad IPv6 entre los clientes mediante pings y conexiones ssh.
- Retardo medio con/sin OpenVPN: Se realizará una comparativa del retardo medio sin OpenVPN y con OpenVPN mediante pings que se realizará entre los equipos clientes.
- Conexiones/Desconexiones por segundo: Se realizará una conexión y desconexión instantánea para ver el tiempo en el que el servidor desvincula completamente el cliente VPN.

4.1 Modelo Simulado

En este apartado tendrá lugar las pruebas para el escenario de GNS3 que se ha comentado anteriormente.

4.1.1 Verificación de conectividad IPv6 entre los clientes

En esta prueba se ha comprobado que, cuando los clientes conectan con OpenVPN con el servidor, se les asigna un direccionamiento IPv6. Esto se puede comprobar viendo las interfaces correspondientes de los clientes. Teniendo en cuenta el esquema del modelo simulado, se tienen 2 clientes OpenVPN que se conectará con el servidor. Por tanto, cuando estos se conecten al servidor, tendrán la interfaz tun0 de la siguiente forma:

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.11.0.2  netmask 255.255.255.0  destination 10.11.0.2
        inet6 aaaa:bbbb:cccc:dddd:80::1000  prefixlen 112  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 72  bytes 7488 (7.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 400  bytes 29600 (28.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 4-1. Interfaz túnel cliente 1

```
tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1500
        inet 10.11.0.3  netmask 255.255.255.0  destination 10.11.0.3
        inet6 aaaa:bbbb:cccc:dddd:80::1001  prefixlen 112  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 68  bytes 7072 (6.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 100  bytes 9136 (8.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 4-2. Interfaz túnel cliente 2

Las interfaces de red del servidor son:

```
[root@linux dit]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.144  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fe91:a365  prefixlen 64  scopeid 0x20<link>
        inet6 2001:123:1:1::127  prefixlen 64  scopeid 0x0<global>
        ether 00:0c:29:91:a3:65  txqueuelen 1000  (Ethernet)
        RX packets 932  bytes 138833 (135.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 928  bytes 138083 (134.8 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 492  bytes 234256 (228.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 492  bytes 234256 (228.7 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1468
        inet 10.11.0.1  netmask 255.255.255.0  destination 10.11.0.1
        inet6 aaaa:bbbb:cccc:dddd:80::1  prefixlen 112  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 408  bytes 28406 (27.7 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 3064 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Figura 4-3. Interfaces de red servidor

También se puede comprobar que ambos clientes tienen conectividad entre ellos mediante un ping.

```
[root@linux Definitivo]# ping6 aaaa:bbbb:cccc:dddd:80::1001
PING aaaa:bbbb:cccc:dddd:80::1001(aaaa:bbbb:cccc:dddd:80::1001) 56 data bytes
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=1 ttl=64 time=73.5 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=2 ttl=64 time=66.7 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=3 ttl=64 time=70.2 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=4 ttl=64 time=61.7 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=5 ttl=64 time=77.3 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=6 ttl=64 time=82.0 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=7 ttl=64 time=74.4 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=8 ttl=64 time=68.6 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=9 ttl=64 time=63.9 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=10 ttl=64 time=82.2 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=11 ttl=64 time=74.4 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=12 ttl=64 time=82.1 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=13 ttl=64 time=89.8 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=14 ttl=64 time=74.4 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=15 ttl=64 time=94.0 ms
^C
--- aaaa:bbbb:cccc:dddd:80::1001 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 14059ms
rtt min/avg/max/mdev = 61.796/75.743/94.030/8.818 ms
```

Figura 4-4. Ping desde Cliente1 a Cliente2

```
[root@linux Definitivo]# ping6 aaaa:bbbb:cccc:dddd:80::1000
PING aaaa:bbbb:cccc:dddd:80::1000(aaaa:bbbb:cccc:dddd:80::1000) 56 data bytes
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=1 ttl=64 time=79.3 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=2 ttl=64 time=79.6 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=3 ttl=64 time=82.3 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=4 ttl=64 time=74.2 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=5 ttl=64 time=66.2 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=6 ttl=64 time=70.3 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=7 ttl=64 time=74.5 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=8 ttl=64 time=96.5 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=9 ttl=64 time=101 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=10 ttl=64 time=70.4 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1000: icmp_seq=11 ttl=64 time=74.1 ms
^C
--- aaaa:bbbb:cccc:dddd:80::1000 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 10046ms
rtt min/avg/max/mdev = 66.232/79.079/101.913/10.536 ms
```

Figura 4-5. Ping desde Cliente2 a Cliente1

4.1.2 Retardo medio con/sin OpenVPN

Esta prueba consiste en la recopilación de 10 muestras con 100 pings en el cual se observará los datos de RTT mínimo, medio, máximo y desviación estándar (mdev). Se realizarán diferentes medidas dependiendo del escenario.

En primer lugar, se medirán los datos de RTT para el escenario sin OpenVPN, donde un equipo conectará con otro simulando que se realiza a través de Internet. Los datos son los siguientes:

Medida en ms	SIN OPENVPN(Ping hacia los equipos de forma normal)										
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	38,922	43,160	36,105	39,040	38,901	36,863	36,815	37,259	38,708	39,198	38,497
Valor Medio	81,402	86,241	85,551	80,182	78,585	78,967	83,093	78,104	75,447	89,882	81,745
Valor Máximo	125,055	172,517	157,074	144,111	125,309	309,184	523,028	141,915	289,418	256,055	224,367
Desviación estandar	18,880	20,755	22,269	22,781	22,565	40,654	55,897	27,474	33,246	35,206	29,973

Figura 4-6. Datos RTT sin OpenVPN para IPv4 modelo Simulado

El valor marcado en amarillo corresponde al valor mínimo de las 10 muestras, que es el valor del mínimo absoluto.El valor marcado en rojo corresponde al valor máximo de las 10 muestras, que es el valor máximo absoluto.

En segundo lugar, se medirán los datos de RTT para el escenario con OpenVPN para IPv4. Los datos son los siguientes:

	CON OPENVPN(Ping hacia los equipos de forma normal) con IPv4										
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	60,635	54,782	62,696	66,722	62,954	62,674	58,635	62,510	68,479	54,769	61,486
Valor Medio	99,499	99,323	107,231	106,985	113,150	101,837	89,785	100,647	124,678	117,969	106,110
Valor Máximo	158,500	172,674	211,020	203,419	205,126	176,006	199,441	172,493	268,389	192,836	195,990
Desviación estandar	24,814	27,386	29,919	25,585	28,006	27,103	24,798	26,199	31,425	24,024	26,926

Figura 4-7. Datos RTT con OpenVPN para IPv4 modelo Simulado

En tercer lugar, se medirán los datos de RTT para el escenario con OpenVPN para IPv6. Los datos son los siguientes:

	CON OPENVPN(Ping hacia los equipos de forma normal) para IPv6										
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	62,835	62,661	54,971	57,073	55,938	63,073	61,081	61,678	55,837	61,496	59,664
Valor Medio	92,744	93,754	93,032	92,265	85,121	83,995	83,956	89,945	85,937	92,489	89,324
Valor Máximo	208,806	211,394	148,324	266,904	176,347	171,837	156,645	199,254	160,558	203,441	190,351
Desviación estandar	22,649	27,062	25,019	30,503	18,667	16,482	14,465	24,482	18,758	30,299	22,839

Figura 4-8. Datos RTT con OpenVPN para IPv6 modelo Simulado

Por último, se medirán los datos de RTT para el escenario con OpenVPN para IPv6 cuando se conecta a un servidor IPv6 externo. Los datos son los siguientes:

		CON OPENVPN(Ping hacia servidor externo en Internet IPv6) para IPv6									
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	50,750	41,262	50,521	48,656	48,605	46,812	49,465	46,971	50,577	43,570	47,719
Valor Medio	72,497	72,054	80,234	79,474	72,297	79,206	76,220	76,839	80,294	74,790	76,391
Valor Máximo	109,810	125,355	250,013	173,125	187,478	190,385	142,682	141,448	191,402	180,326	169,202
Desviación estandar	19,167	18,686	23,613	25,734	25,248	24,768	22,109	21,947	21,482	20,451	22,321

Figura 4-9. Datos RTT con OpenVPN para IPv6 hacia externo modelo Simulado

En la siguiente gráfica se ilustra el valor mínimo y máximo absolutos, media muestral del valor medio y media muestral de la desviación estándar para cada uno de los escenarios comentados anteriormente:

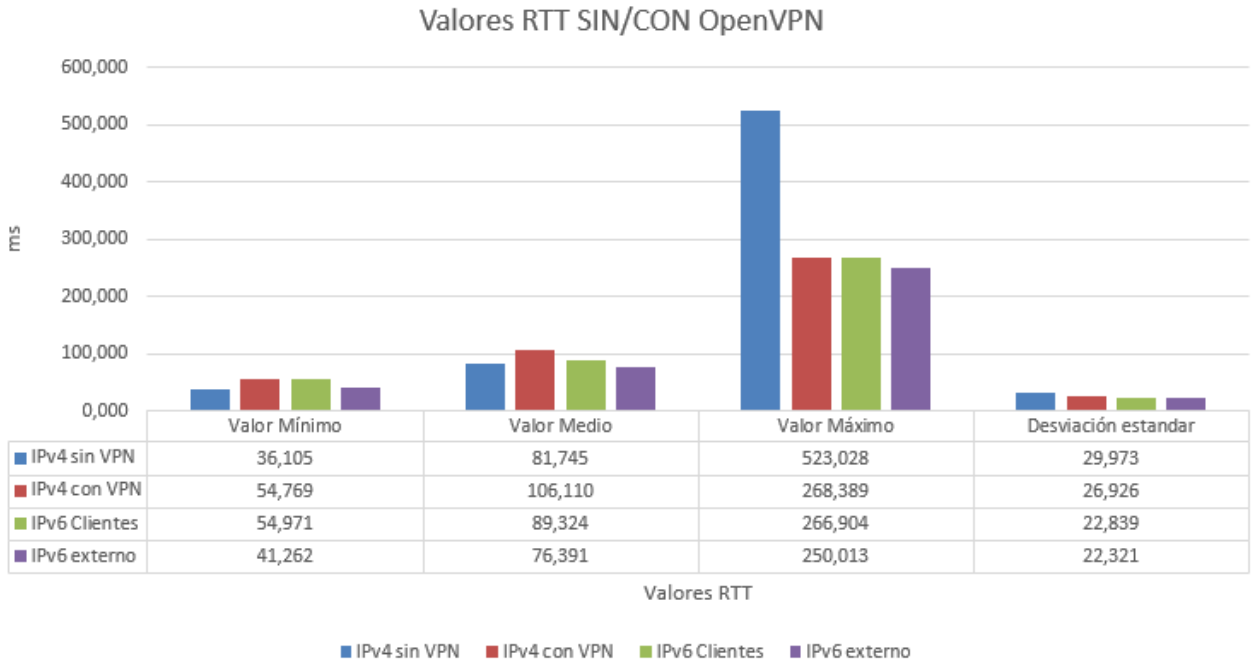


Figura 4-10. Gráfico de valores RTT sin/con OpenVPN modelo Simulado

Se puede observar con los datos obtenidos que los valores RTT medios son parecidos tanto para el uso de IPv4 sin OpenVPN como con OpenVPN, siendo algo mayor para el caso del uso de OpenVPN, pero no muy excesivo, siendo un valor adecuado para la conexión. Respecto a Ipv6, se puede observar que el valor medio de RTT se comporta de manera parecida respecto al retardo. También se observa en la desviación estándar, que el uso de IPv6 tiene la menor desviación tanto a clientes como hacia un servidor externo.

4.1.3 Conexiones/Desconexiones por segundo

Esta prueba consistirá en realizar una conexión y desconexión de OpenVPN en un cliente, donde se va a calcular el tiempo que tarda el servidor VPN entre la detección del cliente al conectarse y la eliminación de este tras desconectarse.

Para ello se ha implementado un script muy sencillo que consiste en los siguientes comandos:

- openvpn --config /home/dit/Downloads/Pruebas/Definitivo/cliente.ovpn &: Conecta con el servidor.
- sleep 3: Espera el tiempo suficiente para que se establezca la conexión (3s).
- pkill openvpn: Desconecta con el servidor.

A continuación, en la siguiente figura se puede observar mediante logs el momento cuando el cliente se conecta y se desconecta del túnel.

```
Jun  8 14:54:56 192 openvpn: Sat Jun  8 14:54:55 2019 nuevo/192.168.1.142:47050 MULTI: Learn: aaaa:bbbb:cccc:dddd:80::1000 -> nuevo/192
.168.1.142:47050
Jun  8 14:54:56 192 openvpn: Sat Jun  8 14:54:56 2019 nuevo/192.168.1.142:47050 MULTI: primary virtual IPv6 for nuevo/192.168.1.142:470
50: aaaa:bbbb:cccc:dddd:80::1000
Jun  8 14:54:57 192 openvpn: Sat Jun  8 14:54:57 2019 nuevo/192.168.1.142:47050 PUSH: Received control message: 'PUSH_REQUEST'
Jun  8 14:54:57 192 openvpn: Sat Jun  8 14:54:57 2019 nuevo/192.168.1.142:47050 SENT CONTROL [nuevo]: 'PUSH_REPLY,persist-key,persist-t
un,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,tun-ipv6,route-ipv6 2000::/3,route-ipv6 ::/0,redir
ect-gateway ipv6,redirect-gateway def1 ipv6,tun-ipv6,route-gateway 10.11.0.1,topology subnet,ping 10,ping-restart 60,ifconfig-ipv6 aaaa
:bbbb:cccc:dddd:80::1000/112 aaaa:bbbb:cccc:dddd:80::1,ifconfig 10.11.0.2 255.255.255.0,peer-id 0,cipher AES-256-GCM' (status=1)
Jun  8 14:54:57 192 openvpn: Sat Jun  8 14:54:57 2019 nuevo/192.168.1.142:47050 Data Channel: using negotiated cipher 'AES-256-GCM'
Jun  8 14:54:57 192 openvpn: Sat Jun  8 14:54:57 2019 nuevo/192.168.1.142:47050 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized
 with 256 bit key
Jun  8 14:54:57 192 openvpn: Sat Jun  8 14:54:57 2019 nuevo/192.168.1.142:47050 Incoming Data Channel: Cipher 'AES-256-GCM' initialized
 with 256 bit key
Jun  8 14:56:57 192 openvpn: Sat Jun  8 14:56:57 2019 nuevo/192.168.1.142:47050 [nuevo] Inactivity timeout (--ping-restart), restarting
Jun  8 14:56:57 192 openvpn: Sat Jun  8 14:56:57 2019 nuevo/192.168.1.142:47050 SIGUSR1[soft,ping-restart] received, client-instance re
starting
```

Figura 4-11. Log generado tras conexión-desconexión en modelo Simulado

Tras realizar estas pruebas se ha obtenido que el tiempo entre conexión y desconexión del equipo es de 2 min y 5 segundos. Se puede afirmar que este tiempo dependerá principalmente de la calidad de la conexión que se tenga entre el cliente y el servidor, que será mayor en caso de que la calidad de la conexión sea mala o menor en caso contrario. Además, también dependerá de otros parámetros como el tipo de dispositivo y el S.O que se tenga.

4.2 Modelo Real

4.2.1 Verificación de conectividad IPv6 entre los clientes

Esta prueba es la misma que se realiza en el escenario simulado, por lo que, los resultados a nivel de interfaces creadas es exactamente el mismo. En la siguiente figura se muestra las interfaces del servidor. Se puede observar como se tiene la interfaz sit1 y sit0 que se utilizan para el túnel de Hurricane, aunque realmente solo se usa sit1.

```
[root@192 dit]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.144  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::20c:29ff:fecb:4740  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:cb:47:40  txqueuelen 1000  (Ethernet)
        RX packets 176471  bytes 52102804 (49.6 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 121219  bytes 36167195 (34.4 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 0  (Local Loopback)
        RX packets 3339  bytes 1228571 (1.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 3339  bytes 1228571 (1.1 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

sit0: flags=193<UP,RUNNING,NOARP>  mtu 1480
        inet6 ::192.168.1.144  prefixlen 96  scopeid 0x80<compat,global>
        inet6 ::127.0.0.1  prefixlen 96  scopeid 0x90<compat,host>
        inet6 ::10.11.0.1  prefixlen 96  scopeid 0x80<compat,global>
        sit  txqueuelen 0  (IPv6-in-IPv4)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 0  bytes 0 (0.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

```
sit1: flags=209<UP,POINTOPOINT,RUNNING,NOARP>  mtu 1480
        inet6 fe80::c0a8:190  prefixlen 64  scopeid 0x20<link>
        inet6 fe80::a0b:1  prefixlen 64  scopeid 0x20<link>
        inet6 2001:470:1f20:1d9::2  prefixlen 64  scopeid 0x0<global>
        sit  txqueuelen 0  (IPv6-in-IPv4)
        RX packets 30864  bytes 16500130 (15.7 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18316  bytes 2307602 (2.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>  mtu 1468
        inet 10.11.0.1  netmask 255.255.255.0  destination 10.11.0.1
        inet6 aaaa:bbbb:cccc:dddd:80::1  prefixlen 112  scopeid 0x0<global>
        unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00  txqueuelen 100  (UNSPEC)
        RX packets 27598  bytes 3165020 (3.0 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39236  bytes 21808001 (20.7 MiB)
        TX errors 0  dropped 244 overruns 0  carrier 0  collisions 0
```

Figura 4-12. Interfaces servidor modelo Real

En la siguiente imagen se muestra que hay conectividad entre los clientes VPN, mediante el uso de un ping entre un cliente y otro.

```
[root@192 dit]# ping6 aaaa:bbbb:cccc:dddd:80::1001
PING aaaa:bbbb:cccc:dddd:80::1001(aaaa:bbbb:cccc:dddd:80::1001) 56 data bytes
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=1 ttl=64 time=1.74 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=2 ttl=64 time=2.53 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=3 ttl=64 time=2.52 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=4 ttl=64 time=1.49 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=5 ttl=64 time=2.97 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=6 ttl=64 time=2.42 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=7 ttl=64 time=2.43 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=8 ttl=64 time=2.48 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=9 ttl=64 time=2.47 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=10 ttl=64 time=2.51 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=11 ttl=64 time=2.33 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=12 ttl=64 time=2.81 ms
64 bytes from aaaa:bbbb:cccc:dddd:80::1001: icmp_seq=13 ttl=64 time=16.1 ms
^C
--- aaaa:bbbb:cccc:dddd:80::1001 ping statistics ---
13 packets transmitted, 13 received, 0% packet loss, time 12045ms
rtt min/avg/max/mdev = 1.492/3.452/16.119/3.675 ms
```

Figura 4-13. Ping entre clientes en modelo Real

Como se comentó, ahora se tiene un túnel con Hurricane que nos permite tener IPv6 para conectarnos a Internet. Por tanto, el equipo servidor se encarga de realizar unas reglas de NAT para reenviar el trafico ipv6 a través de esta interfaz. Se ha verificado mediante webs externas test-ipv6.com e ipv6-test.com que los clientes tienen conectividad IPv6.

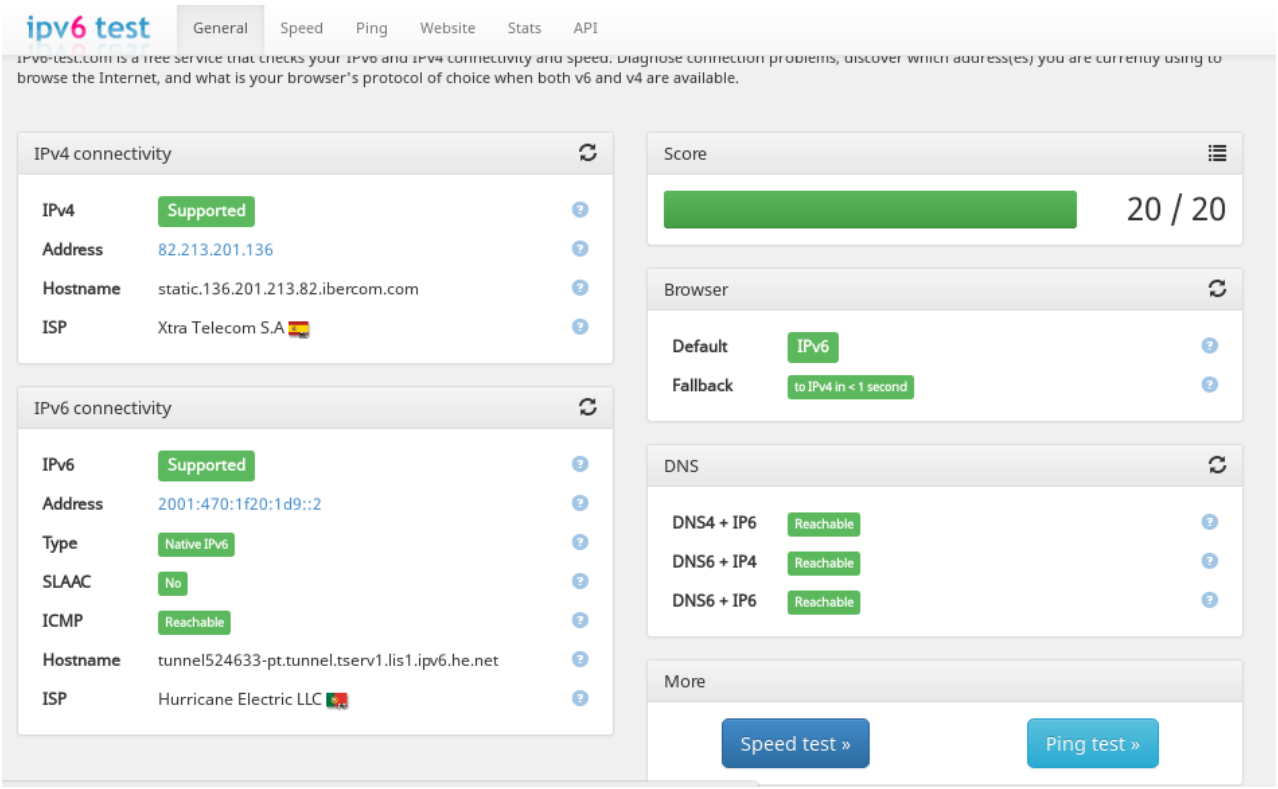


Figura 4-14. Prueba de conectividad mediante ipv6-test.com

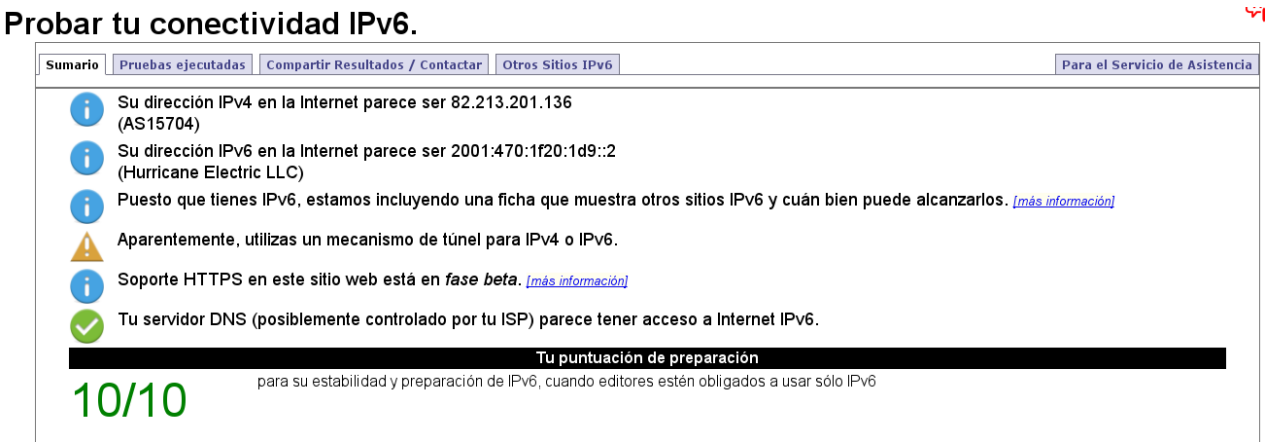


Figura 4-15. Prueba de conectividad mediante test-ipv6.com

Por lo que los clientes pueden conectarse a páginas o equipos en IPv6 sin ningún problema.

4.2.2 Retardo medio con/sin OpenVPN

Esta prueba consiste en la recopilación de 10 muestras con 100 pings en el cual se observará los datos de RTT mínimo, medio, máximo y desviación estándar (mdev). Se realizarán diferentes medidas dependiendo del escenario

En primer lugar, se medirán los datos de RTT para el escenario sin OpenVPN donde un equipo conectará con otro que están conectados en la misma subred. Los datos son los siguientes:

Medida en ms		SIN OPENVPN(Ping hacia los equipos de forma normal)									
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	1,221	1,200	1,229	1,057	1,087	1,172	1,183	1,185	1,099	1,291	1,172
Retardo Medio	1,571	1,592	1,574	1,622	1,641	1,478	1,615	1,639	1,499	1,614	1,585
Valor Máximo	3,636	3,225	2,182	2,385	3,113	1,841	2,199	2,534	2,363	1,973	2,545
Desviación estandar	0,324	0,285	0,164	0,188	0,229	0,146	0,175	0,178	0,186	0,132	0,201

Figura 4-16. Datos RTT sin OpenVPN para IPv4 modelo Real

El valor marcado en amarillo corresponde al valor mínimo de las 10 muestras, que es el valor del mínimo absoluto.El valor marcado en rojo corresponde al valor máximo de las 10 muestras, que es el valor máximo absoluto.

En segundo lugar, se medirán los datos de RTT para el escenario con OpenVPN para IPv4. Los datos son los siguientes:

		CON OPENVPN(Ping hacia los equipos de forma normal) con IPv4									
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	1,225	1,067	1,038	1,282	1,232	1,383	1,287	0,997	1,040	0,969	1,152
Retardo Medio	1,971	2,017	2,171	2,334	2,278	2,263	2,064	2,226	2,156	2,138	2,162
Valor Máximo	4,527	3,375	4,234	3,415	3,598	4,864	4,639	3,528	3,762	4,056	4,000
Desviación estandar	0,327	0,347	0,514	0,389	0,392	0,418	0,362	0,398	0,444	0,449	0,404

Figura 4-17. Datos RTT con OpenVPN para IPv4 modelo Real

Por último, se medirán los datos de RTT para el escenario con OpenVPN para IPv6. Los datos son los siguientes:

		CON OPENVPN(Ping hacia los equipos de forma normal) para IPv6									
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	1,458	1,253	1,538	1,564	1,569	1,738	1,545	1,535	1,801	1,691	1,569
Retardo Medio	2,542	2,288	2,269	2,452	2,230	2,461	2,398	2,286	2,392	2,503	2,382
Valor Máximo	5,791	4,089	3,923	5,218	4,630	4,229	4,675	3,997	4,620	3,841	4,501
Desviación estandar	0,620	0,503	0,412	0,582	0,567	0,424	0,555	0,442	0,431	0,462	0,500

Figura 4-18. Datos RTT sin OpenVPN para IPv6 modelo Real

En la siguiente gráfica se ilustra el valor mínimo y máximo absolutos, media muestral del valor medio y media muestral de la desviación estándar para cada uno de los escenarios comentados anteriormente:

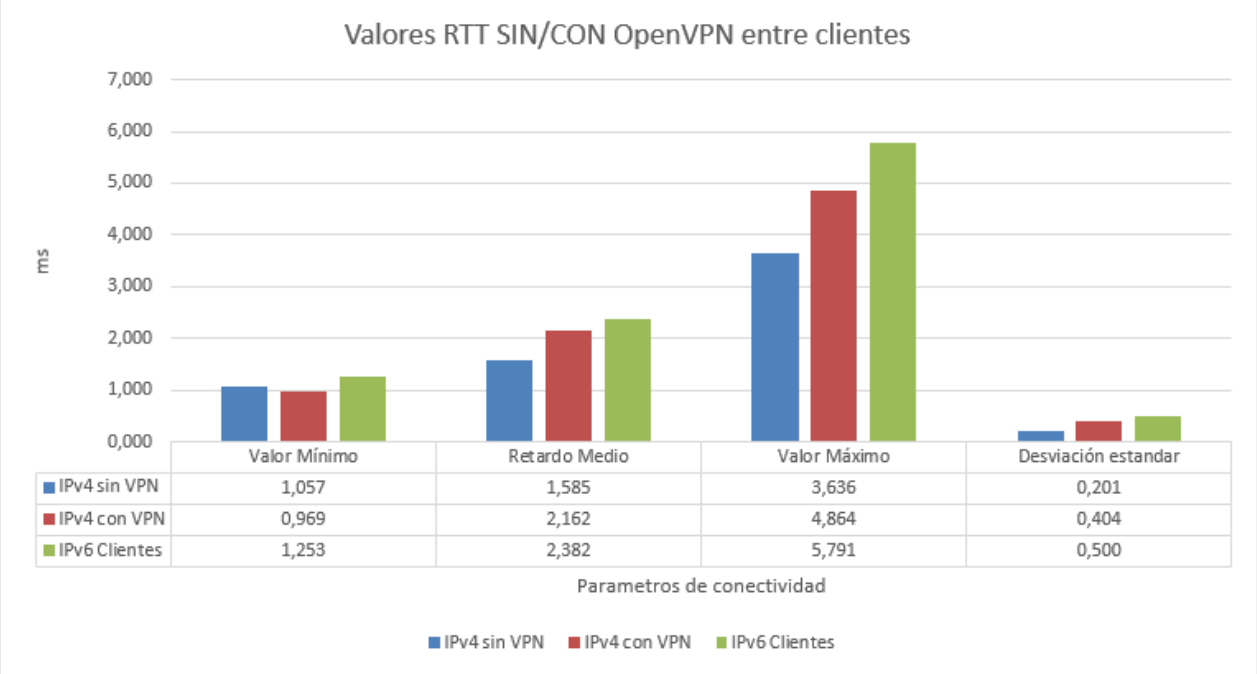


Figura 4-19. Gráfico de valores RTT sin/con OpenVPN modelo Real 1

Se puede observar como el valor medio de RTT menor se encuentra en el uso de IPv4 sin OpenVPN, aunque solo difiere en 0,600 ms con IPv4 con OpenVPN. Este valor no es alto y por tanto se puede considerar dentro del rango adecuado para una conexión. No obstante, el valor máximo de RTT que puede alcanzar para IPv6 es de casi 2 ms, lo cual puede llegar a ser algo apreciable pero no lo suficiente, ya que a nivel de desviación están tanto el uso de IPv4 con/sin VPN como con IPv6 parejos.

Además de este estudio, se va a realizar pruebas de conexión a Internet tanto sin OpenVPN como con OpenVPN en IPv4 e IPv6.

En el primer caso, se medirán los datos de RTT para el escenario sin OpenVPN donde un equipo conectado a Internet realizará pings hacia Google. Los datos son los siguientes:

	SIN OPENVPN(Ping hacia google en Internet) para IPv4										
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	9,958	9,989	9,406	9,413	9,412	9,441	10,024	9,959	9,890	9,899	9,739
Retardo Medio	13,054	11,683	11,271	10,897	11,562	12,165	12,021	11,295	11,319	11,121	11,639
Valor Máximo	35,699	22,808	31,706	28,619	35,036	38,052	33,073	25,724	23,218	19,883	29,382
Desviación estandar	5,277	2,416	2,874	2,216	3,657	4,826	3,476	2,374	2,119	1,421	3,066

Figura 4-20. Datos RTT sin OpenVPN hacia Internet para IPv4 modelo Real

El valor marcado en amarillo corresponde al valor mínimo de las 10 muestras, que es el valor del mínimo absoluto.El valor marcado en rojo corresponde al valor máximo de las 10 muestras, que es el valor máximo absoluto.

En segundo lugar, se medirán los datos de RTT para el escenario con OpenVPN para IPv4. Los datos son los siguientes:

	CON OPENVPN(Ping hacia google en Internet) para IPv4										
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	11,570	11,263	11,368	10,988	11,046	11,221	10,688	10,607	10,684	10,326	10,976
Retardo Medio	14,047	13,640	14,018	12,543	12,977	13,972	12,111	12,312	12,253	11,857	12,973
Valor Máximo	26,983	39,483	25,134	28,536	24,828	26,111	20,701	18,019	15,509	17,124	24,243
Desviación estandar	2,028	2,843	2,050	1,943	1,898	2,477	1,342	0,927	0,861	1,140	1,751

Figura 4-21. Datos RTT con OpenVPN hacia Internet para IPv4 modelo Real

Finalmente se medirán los datos de RTT para el escenario con OpenVPN para IPv6. Los datos son los siguientes:

	CON OPENVPN(Ping hacia google en Internet IPv6) para IPv6										
Muestras	1	2	3	4	5	6	7	8	9	10	Media
Valor Mínimo	25,286	24,604	25,298	24,755	24,670	25,481	24,623	26,503	25,406	25,002	25,163
Retardo Medio	27,191	26,421	27,190	26,581	26,383	27,317	26,220	28,080	27,324	27,415	27,012
Valor Máximo	34,610	36,823	38,728	36,724	34,320	37,874	30,210	39,576	35,727	38,165	36,276
Desviación estandar	1,587	1,796	1,793	1,809	1,423	1,639	0,933	1,714	1,455	2,335	1,648

Figura 4-22. Datos RTT con OpenVPN hacia Internet para IPv6 modelo Real

En la siguiente gráfica se ilustra el valor mínimo y máximo absolutos, media muestral del valor medio y media muestral de la desviación estándar para cada uno de los escenarios comentados anteriormente:

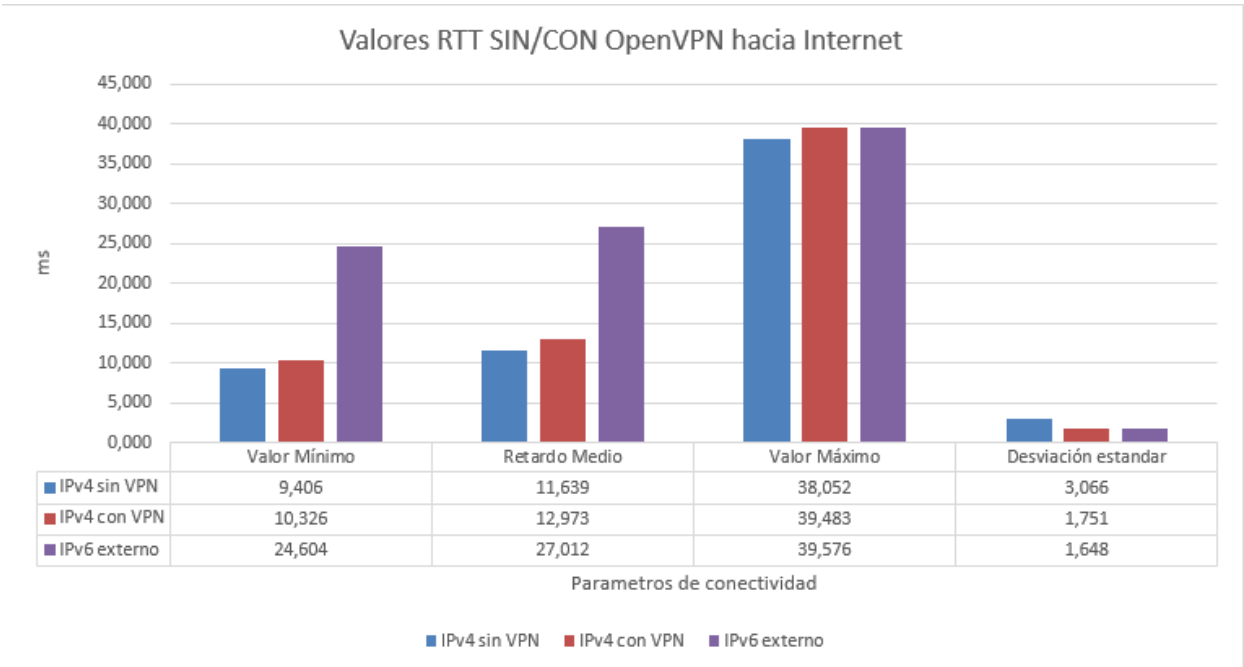


Figura 4-23. Gráfico de valores RTT sin/con OpenVPN modelo Simulado 2

Se puede observar en la gráfica anterior que el valor medio de RTT es muy parecido en IPv4 tanto sin VPN como con VPN, por lo que se comporta de manera similar y tiene una conexión adecuada. Sin embargo, con IPv6 se tiene un valor mucho más mayor que estos. Esto se puede justificar, ya que normalmente el tiempo de respuesta de webs IPv6 suele ser algo mayor.

En este escenario concreto, se puede realizar además una prueba de la estabilidad en el retardo en los túneles VPN dependiendo del número de clientes que haya conectados. Para ello, se han recogido datos del retardo medio tras la realización de un ping entre dos clientes OpenVPN. Se estudiará cómo afecta este tiempo cuando se van conectando más clientes a la red VPN.

Se realiza primero una obtención de muestras para IPv4:

		Retardo medio OPENVPN(Ping hacia los equipos de forma normal) para IPv4									
Clientes\Muestras	1	2	3	4	5	6	7	8	9	10	Media
1	0,580	1,022	0,830	1,114	1,097	0,857	0,942	0,880	0,764	0,992	0,908
2	1,971	2,017	2,171	2,334	2,278	2,263	2,064	2,226	2,156	2,138	2,162
3	2,504	2,350	2,841	2,290	2,021	2,597	2,095	2,283	2,139	2,437	2,356
4	3,241	3,230	3,440	3,269	3,657	3,270	2,991	3,058	3,188	3,166	3,251
5	4,245	4,856	4,222	4,269	4,217	3,634	5,481	3,098	4,020	4,849	4,289

Figura 4-24. Datos Retardo medio dependiendo de clientes para IPv4

Tras la obtención de muestras para IPv4, se realiza la obtención de muestras para IPv6:

		Retardo medio OPENVPN(Ping hacia los equipos de forma normal) para IPv6									
Clientes\Muestras	1	2	3	4	5	6	7	8	9	10	Media
1	1,575	1,071	1,021	0,955	0,875	1,359	0,868	1,929	1,077	0,865	1,160
2	2,542	2,288	2,269	2,452	2,230	2,461	2,398	2,286	2,392	2,503	2,382
3	2,47	3,168	3,628	2,233	3,668	2,547	3,335	2,726	4,301	5,164	3,324
4	3,457	4,313	3,999	3,649	3,439	3,525	2,777	2,887	2,978	2,380	3,340
5	3,858	3,927	3,9	3,966	3,988	4,070	4,214	4,248	4,304	4,085	4,056

Figura 4-25. Datos Retardo medio dependiendo de clientes para IPv6

Finalmente, con estos datos se puede sacar la siguiente gráfica comparativa:

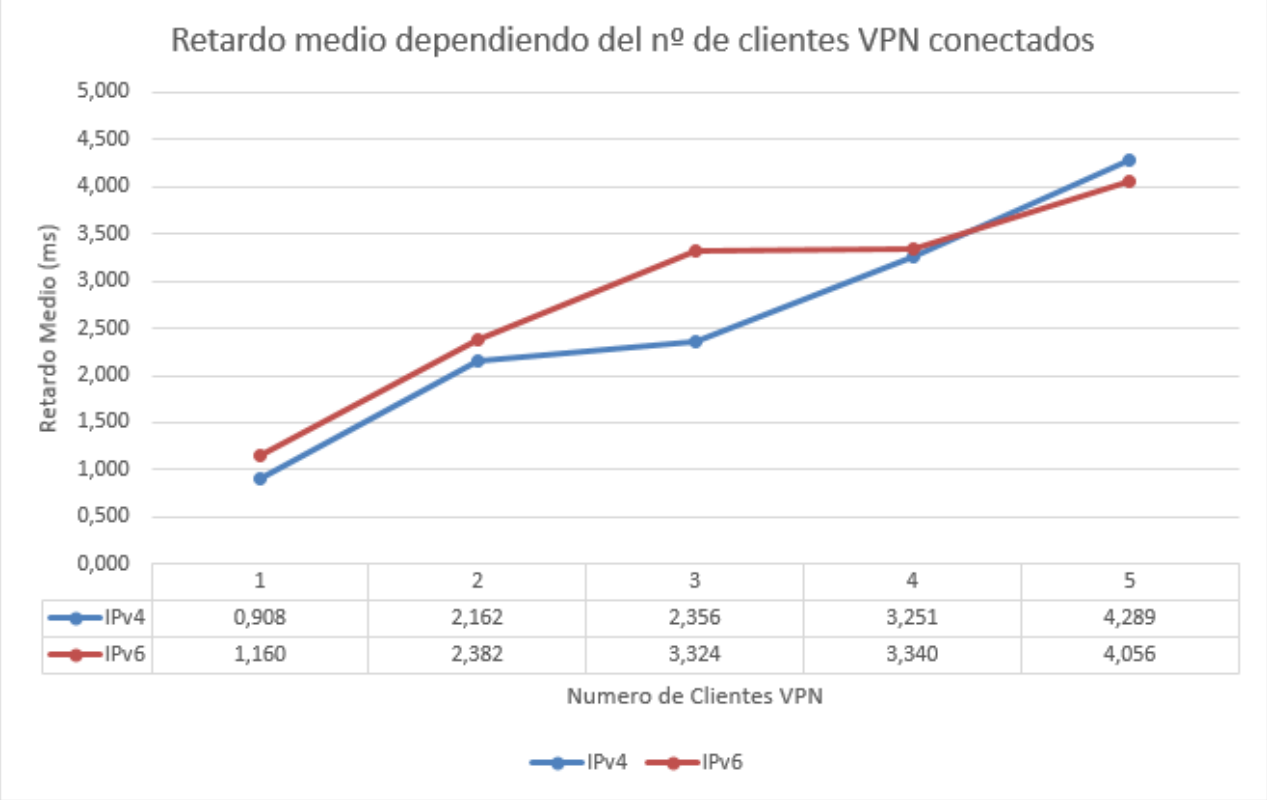


Figura 4-26. Gráfica comparativa del Retardo Medio dependiendo del nº de clientes VPN

Si se observa el gráfico, se puede apreciar que el retardo de IPv4 es menor que IPv6 cuando va aumentando el número de clientes, pero no difiere mucho de este ya que al aumentar el número de clientes, IPv6 puede tener un retardo similar o un poco mayor al de IPv4.

Una última prueba que se ha realizado ha sido verificar mediante un test de velocidad de "test-ipv6.com", el ancho de banda que tienen los clientes cuando se conectan al túnel VPN. En esta imagen se puede observar tanto el ancho de banda para navegar por IPv6 como por IPv4.

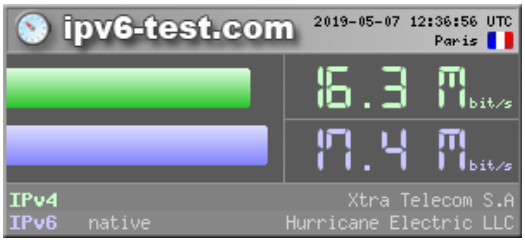


Figura 4-27. Prueba de conectividad mediante test-ipv6.com

4.2.3 Conexiones/Desconexiones por segundo

Esta prueba consistirá en realizar una conexión y desconexión de OpenVPN en un cliente, donde se va a calcular el tiempo que tarda el servidor VPN entre la detección del cliente al conectarse y la eliminación de este tras desconectarse.

Para ello se ha implementado un script muy sencillo que consiste en los siguientes comandos:

- openvpn --config /home/dit/Downloads/Pruebas/Definitivo/cliente.ovpn &: Conecta con el servidor.
- sleep 3: Espera el tiempo suficiente para que se establezca la conexión (3s).
- pkill openvpn: Desconecta con el servidor.

En la siguiente figura se puede observar mediante logs, el momento cuando el cliente se conecta y se desconecta del túnel.

```
Jun  8 20:44:48 192 openvpn: Sat Jun  8 20:44:48 2019 MULTI: Learn: aaaa:bbbb:cccc:dddd:80::1000 -> nuevo/192.168.1.142:37860
Jun  8 20:44:48 192 openvpn: Sat Jun  8 20:44:48 2019 MULTI: primary virtual IPv6 for nuevo/192.168.1.142:37860: aaaa:bbbb:cccc:dddd:80
::1000
Jun  8 20:44:49 192 openvpn: Sat Jun  8 20:44:49 2019 nuevo/192.168.1.142:37860 PUSH: Received control message: 'PUSH_REQUEST'
Jun  8 20:44:49 192 openvpn: Sat Jun  8 20:44:49 2019 nuevo/192.168.1.142:37860 SENT CONTROL [nuevo]: 'PUSH_REPLY,persist-key,persist-t
un,redirect-gateway def1 bypass-dhcp,dhcp-option DNS 8.8.8.8,dhcp-option DNS 8.8.4.4,tun-ipv6,route-ipv6 2000::/3,route-ipv6 ::/0,redir
ect-gateway ipv6,redirect-gateway def1 ipv6,tun-ipv6,route-gateway 10.11.0.1,topology subnet,ping 10,ping-restart 60,ifconfig-ipv6 aaaa
:bbbb:cccc:dddd:80::1000/112 aaaa:bbbb:cccc:dddd:80::1,ifconfig 10.11.0.2 255.255.255.0,peer-id 0,cipher AES-256-GCM' (status=1)
Jun  8 20:44:49 192 openvpn: Sat Jun  8 20:44:49 2019 nuevo/192.168.1.142:37860 Data Channel: using negotiated cipher 'AES-256-GCM'
Jun  8 20:44:49 192 openvpn: Sat Jun  8 20:44:49 2019 nuevo/192.168.1.142:37860 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized
 with 256 bit key
Jun  8 20:44:49 192 openvpn: Sat Jun  8 20:44:49 2019 nuevo/192.168.1.142:37860 Incoming Data Channel: Cipher 'AES-256-GCM' initialized
 with 256 bit key
Jun  8 20:46:49 192 openvpn: Sat Jun  8 20:46:49 2019 nuevo/192.168.1.142:37860 [nuevo] Inactivity timeout (--ping-restart), restarting
Jun  8 20:46:49 192 openvpn: Sat Jun  8 20:46:49 2019 nuevo/192.168.1.142:37860 SIGUSR1[soft,ping-restart] received, client-instance re
starting
```

Figura 4-28. Log generado tras conexión-desconexión en modelo Real

Además de la conexión por cable, se ha probado la conexión desde un dispositivo móvil al servidor VPN, y se puede concluir tras realizar las mismas pruebas que el tiempo de conexión/desconexión depende de la calidad de la conexión sea mayor o menor, del dispositivo y del S.O. Se han obteniendo para la prueba los siguientes resultados:

Tipo de dispositivo	Tiempo Conexión-Desconexión
Ordenador	2 minutos y 5 segundos
Móvil	1 segundo

Tabla 4-1. Tiempo Conexión-Desconexión modelo Real

5 CONCLUSIONES Y LÍNEAS FUTURAS

Cuando llegues al final de lo que debes saber,
estarás al principio de lo que debes sentir.
Gibran Jalil Gibran, 1926

Después de la investigación, diseño, implementación y pruebas del proyecto, se debe analizar el resultado de todo el proyecto tanto a nivel técnico como general. Por ello, se llegará en este capítulo a conclusiones relacionadas con el desarrollo y resultado del proyecto. Así mismo se verán mejoras de este proyecto para el futuro.

5.1 Conclusiones

Tras la realización del proyecto se pueden sacar las siguientes conclusiones:

- El cambio a IPv6 es algo que tarde o temprano pasará y se tiene que estar preparado para ello.
- Los Tunnel Brokers es uno de los medios más cómodos a la hora de utilizar IPv6 a través de IPv4.
- El Tunnel Broker que se propone permite el control de los usuarios mediante portal web, además permite a los usuarios poder ver el direccionamiento proporcionado, y poder elegir el tipo de direccionamiento que quieran tener.
- La elección de OpenVPN como software permite una seguridad a nivel de encriptación mucho mayor que con otros softwares, además de permitir modificar parámetros del servidor y clientes.
- La generación de certificados y revocación de estos, es fundamental para que el servidor OpenVPN pueda tener controlado a nivel de seguridad si un usuario intenta acceder con un certificado el cual ya está revocado o que no puede usar. Además, puede bloquear a otro cliente si este está usando el mismo certificado.
- El retardo medio tanto con el uso de OpenVPN como sin él, es bastante similar, siendo el retardo medio de VPN mayor que sin este, ya que este dependerá de la conexión y el ancho de banda que tenga el cliente que quiera conectarse.
- La diferencia fundamental entre el uso o no de OpenVPN es sin duda el túnel encriptado que se crea entre cliente y servidor, donde nadie podrá interceptar cualquier comunicación. No solo eso, sino que además también permite la conexión entre clientes mediante varios túneles VPN conectando primero con el servidor, por lo que, el servidor se encargará de que los mensajes lleguen correctamente al cliente destinatario y nadie podrá interceptarlo al volver a estar encriptado el túnel.
- El tiempo de conexión/desconexión de un cliente es lo suficientemente pequeño para que el servidor tenga en todo momento un control sobre el estado de las conexiones.
- El retardo medio hacia Internet IPv6 sería mucho menor, si en el servidor, el proveedor de red le proporcionase salida a Internet IPv6 dándole direccionamiento IPv6 a este. Pero este retardo dependerá siempre del ancho de banda contratado por la persona que gestiona el equipo servidor.

5.2 Líneas Futuras

Las mejoras que se pueden realizar al proyecto son las siguientes:

- Realizar el proyecto para un escenario donde el proveedor de red proporcione IPv6 para el servidor.
- Añadirle de manera opcional a los clientes la posibilidad de añadir TLS a la encriptación.
- Añadir al administrador la posibilidad de poder desconectar un cliente cuando intente realizar algún ataque al servidor.
- Guardar datos adicionales identificativos de los usuarios como: Apellidos, Edad…Etc.
- Añadir funcionalidad de enviar email al correo del usuario en caso de que se le olvide la contraseña.
- Añadir la funcionalidad de cambiar la contraseña dentro de la información del usuario.
- Poder acceder remotamente a la página web abriendo para ello puertos en router, ya que mi operadora me proporcionó dos routers que no realizaban esta acción correctamente.
- Subir la web con un dominio y publicarla para que los usuarios puedan acceder desde Internet a esta.

5.3 Tiempo dedicado a cada tarea

En este apartado se añade un diagrama de Gantt, en el cual se indica el tiempo en el que se ha realizado cada una de las tareas citadas en el apartado "Metodología de trabajo". En este diagrama se pueden observar las fechas de comienzo y de fin de cada una de ellas y los meses correspondientes. Aquí se pondrán las fechas de realización de cada una de las tareas:

- Investigación: 1 de febrero – 28 de febrero.
- Preparación Entorno: 18 de febrero – 3 de marzo.
- Diseño Web y Scripts: 25 de febrero – 10 de marzo.
- Configuración de OpenVPN: 11 de marzo – 31 de marzo.
- Implementación Web: 1 de abril – 28 de abril.
- Pruebas: 29 de abril – 26 de mayo.
- Mejoras: 6 de mayo – 20 de mayo.
- Documentación: 13 de mayo – 5 de julio.

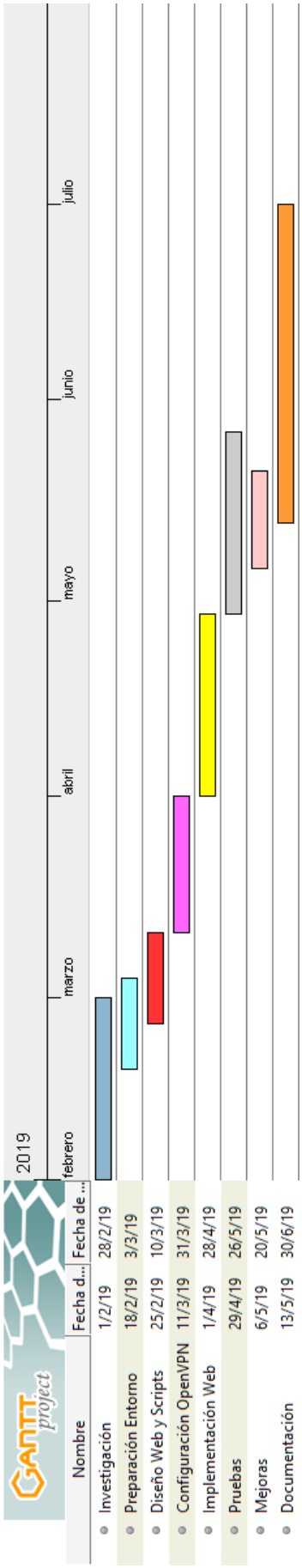


Figura 5-1. Diagrama de Gantt

REFERENCIAS

[1] LACNIC, «LACNIC,» [En línea]. Available: https://www.lacnic.net/1001/1/lacnic/fases-de-agotamiento-de-ipv4.

[2] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/IPv6.

[3] D. P. Valdés, «Maestros del web,» 10 Octubre 2007. [En línea]. Available: http://www.maestrosdelweb.com/evolucionando-hacia-el-ipv6/.

[4] J. M. V. Torres, Introducción a IPv6.

[5] C. Systems, «IPv6 Transition Mechanisms. Describing IPv6 Tunneling Mechanisms.,» 2006.

[6] Google, «Google IPv6,» [En línea]. Available: https://www.google.com/intl/es/ipv6/statistics.html.

[7] I. Elizalde, «directorTIC.es,» 1 abril 2019. [En línea].

[8] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Red_privada_virtual.

[9] Z. Yakova, «ResearchGate,» [En línea]. Available: https://www.researchgate.net/figure/Remote-access-VPN-1_fig2_256843676.

[10] S. Checa, «Informatica Digital,» 5 Abril 2018. [En línea]. Available: https://www.locurainformaticadigital.com/2018/04/05/que-es-vpn-definicion-tipos-caracteristicas/.

[11] «SaferVPN,» [En línea]. Available: https://www.safervpn.com/es/vpn-protocols.

[12] J. J. T. Cánovas, Servicio VPN de acceso remoto basado en SSL mediante OpenVPN, Cartagena, 2008.

[13] H. Shield, «Hotspot Shield,» [En línea]. Available: https://www.hotspotshield.com/es/.

[14] OpenVPN, «OpenVPN,» [En línea]. Available: https://openvpn.net.

[15] «windscribe,» [En línea]. Available: https://esp.windscribe.com/.

[16] «ProtonVPN,» [En línea]. Available: https://protonvpn.com/.

[17] «hide.me,» [En línea]. Available: https://hide.me/es/.

[18] «TunnelBear,» [En línea]. Available: https://www.tunnelbear.com/.

[19] «freelan,» [En línea]. Available: https://www.freelan.org/.

[20] «NordVPN,» [En línea]. Available: https://nordvpn.com/es/.

[21] «PureVPN,» [En línea]. Available: https://www.purevpn.com/es/.

[22] «slickVPN,» [En línea]. Available: https://www.slickvpn.com/.

[23] «WireGuard,» [En línea]. Available: https://www.wireguard.com/.

[24] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/OpenVPN.

[25] O. Valentine, «globalwebindex,» 2 Julio 2018. [En línea]. Available: https://blog.globalwebindex.com/chart-of-the-day/vpn-usage-2018/.

[26] «Wikipedia,» [En línea]. Available: https://es.wikipedia.org/wiki/Tunnel_broker.

[27] stretch, «PacketLife.net,» 17 Diciembre 2008. [En línea]. Available: https://packetlife.net/blog/2008/dec/17/creating-ipv6-tunnel-packetlifenet/.

[28] J. Palet, Mecanismos de transmisión de IPv6, Foz de Iguazu-Brasil, 2017.

[29] «Hurricane Electric,» [En línea]. Available: http://he.net/.

[30] «NetAssist IPv6 Tunnel Broker,» [En línea]. Available: https://tb.netassist.ua/.

[31] «Got-root,» [En línea]. Available: https://got-root.it/.

[32] «IP4market Tunnel Broker IPv6,» [En línea]. Available: https://ipv6.ip4market.ru/.

[33] «IPv6onlyhosting,» [En línea]. Available: https://ipv6onlyhosting.com/en-us/cms/.

[34] «6project,» [En línea]. Available: https://6project.org/.

[35] «Pemsy,» [En línea]. Available: https://www.pemsy.com/.

[36] «WhatIsMyIpAddress,» [En línea]. Available: https://whatismyipaddress.com/dual-stack.

[37] «Hurricane Electric,» [En línea]. Available: https://tunnelbroker.net/usage/tunnels_by_country.php.

[38] D. Córdoba, «JuncoTIC,» [En línea]. Available: https://juncotic.com/openvpn-easyrsa-3-montando-la-vpn/.

ANEXO A: INSTALACIÓN DEL PROYECTO

1. Configuración de escenario de red

Si no se dispone de conexión directa IPv6, hay que crear un tunnel broker con Hurricane, para ello hay que acceder a la página de Hurricane que se adjunta a continuación y seguir los siguientes pasos:

https://tunnelbroker.net/

1) Crear un usuario e iniciar sesión
2) Crear un tunnel bróker con la opción "Create Regular Tunnel"
3) En "IPv4 Endpoint (Your side)" añadir la IP pública, esta aparecerá debajo de este campo y se seleccionará un servidor de túnel.
4) Tras crear la configuración del túnel, en la pantalla principal del túnel creado, pulsar "Example configuration" y desplegar la pestaña donde se va seleccionar la configuración que se adapte al S.O utilizado. (En Centos7, se utiliza Linux-net-Tools)
5) Abrir una ventana de comandos y ejecutar los comandos uno a uno como usuario root.

2. Preparación herramientas necesarias para el proyecto

Se debe tener en el S.O las siguientes herramientas:

- Iptables e ip6tables
- Servidor Tomcat (opcional servidor Apache)
- PostgreSQL
- OpenVPN
- Easy-rsa

En estas instrucciones se verán como configurar cada una de ellas para el proyecto en el entorno Linux. El archivo comprimido "TFG.zip" contendrá los directorios TFG e Instrucciones que tendrán que estar ubicados en el mismo directorio para el desarrollo correcto de estas instrucciones. Por tanto, se descomprimirá el proyecto en el directorio de trabajo mediante el comando:

```
unzip TFG.zip
```

3. Instalación de Base de Datos

Para instalar PostgreSQL hay que seguir los siguientes comandos como root:

1) Instalación de PostgreSQL:
   ```
   yum install postgresql-server postgresql-contrib
   ```
2) Iniciar la Base de datos:
   ```
   postgresql-setup initdb
   ```
   (Si aparece el mensaje "Data not Empty", utilizar el comando
   ```
   rm -rf /var/lib/pgsql/data/
   ```
   para eliminar los datos que hayan en el interior)
3) Modificar el fichero `/var/lib/pgsql/data/pg_hba.conf` dejándolo de la siguiente forma:

```
local   all             all                                     md5
host    all             all             127.0.0.1/32            md5
host    all             all             ::1/128                 md5
```

4) Se inicia el servicio PSQL: `systemctl start postgresql`
5) Se activa en el arranque: `systemctl enable postgresql`
6) Ahora se inicia la Base de Datos con usuario postgresql con el comando: "`sudo -i -u postgres`" y se utiliza el comando "`psql`"
7) Se cambia al directorio donde se tenga las instrucciones con el comando en psql:
   `\cd </directorioprincipal/directoriotrabajo/instrucciones>`
8) Se ejecuta el script "`createbd.sql`" que se encargará de crear el usuario y la base de datos
9) Se accede a la base de datos dit con el usuario dit con el comando:
   `psql -U dit -h 127.0.0.1 dit`

   A continuación se ejecuta el siguiente script que se encargará de crear las tablas correspondientes en el directorio instrucciones:
   `\cd </directorioprincipal/directoriotrabajo/instrucciones/>`
   `\i creatablas.sql`

4. Configuración de exportación de página Tomcat

1) Editar el archivo `/etc/tomcat/server.xml` de Tomcat para que quede de la siguiente forma:

```
<Service name="Catalina">
    <Connector port="8009" protocol="AJP/1.3" redirectPort="8443" />
    <Engine name="Catalina" defaultHost="localhost">
      <Realm className="org.apache.catalina.realm.LockOutRealm">
        <Realm className="org.apache.catalina.realm.UserDatabaseRealm"
               resourceName="UserDatabase"/>
      </Realm>
      <Host name="localhost"  appBase="webapps"
            unpackWARs="true" autoDeploy="true">
        <Valve             className="org.apache.catalina.valves.AccessLogValve"
directory="logs"
               prefix="localhost_access_log." suffix=".txt"
               pattern="%h %l %u %t &amp;quot;%r&amp;quot; %s %b" />
            <!-- Contexto de TFG -->
            <Context path="/dit"
               docBase="<directoriotrabajo>/TFG/"
               debug="0"
               reloadable="true" />
      </Host>
    </Engine>
  </Service>
```

Donde `<directoriotrabajo>` corresponde con el directorio de trabajo donde estará el proyecto y las instrucciones, mientras "`/dit`" corresponde con el alias para el acceso a la página

2) (Opcional) Si se quiere tener el servidor Apache incluir en la carpeta "`/etc/httpd/conf.d/`" el siguiente fichero cuyo nombre puede ser por ejemplo, "`Jkmount-web.conf`" (donde /home/dit será sustituido por el directorio donde se tenga la carpeta TFG y `/dit` será el Alias que se pondrá para acceder a la página:

```
Alias /dit <directoriotrabajo>/TFG
<Directory "<directoriotrabajo>/TFG">
      Order deny,allow
      Allow from all
</Directory>
JkMount /dit/*.jsp tomcat
JkMount /dit/*.jspx tomcat

JkMount /dit/servlets/* tomcat
```

3) Tras esto reiniciar los servidores Tomcat y Apache de la siguiente forma:

```
service httpd stop
service tomcat stop
service  tomcat start
service httpd start
```

Para comprobar que esta todo correcto, se accede a las siguientes URLs:

http://localhost/dit/Principal.jsp

http://<IP_local>/dit/Principal.jsp

5. Creación de certificados de OpenVPN

Hay que instalar OpenVPN, para ello se debe realizar el siguiente comando:

```
yum -y install openvpn easy-rsa
```

1) Ubicarse en el directorio <directoriodetrabajo>/TFG/WEB-INF/easy-rsa/

2) Se ejecuta los siguientes comandos para borrar cualquier certificado que hubiese creado:

- `source ./vars`
- `./clean-all`

3) Se crea el certificado ca, rellenando los campos de información que vayan apareciendo

- `./build-ca`

4) Se crea el certificado y la clave del servidor con el siguiente comando:

- `./build-key-server server`

Nota: Los campos "`password`" y "`optional company`" no se rellenan, por lo que solo hay que pulsar espacio y pulsar "y" para confirmar la creación del certificado.

5) Se genera el archivo de intercambio de claves Diffie-Helman

- `./build-dh`

6. Configuración de entorno y aplicación

Los pasos que se realizarán a continuación deben hacerse con usuario "root":

1) Configuración de directorios en el proyecto:

Se utiliza el script changedirectory.sh para cambiar el directorio en todos los ficheros donde se tenga un "`/home/dit/`" por el directorio nuestro "`<directorio_principal>`":

```
./changedirectory.sh  <directorioprincipal>
```

Nota Importante: Es fundamental que se ponga con el siguiente formato: "/home/dit/" con las barras correctamente puestas ya que el script está diseñado para que se ponga de esta forma.

2) Configuración de propietarios de los archivos del proyecto:

Se debe configurar algunos permisos de algunos archivos concretos que pertenecerán al usuario "tomcat". Se realizará con el siguiente script:

```
./changeuserproperty.sh
```

3) Copiar el ejecutable ejecutaroot ubicado en la carpeta codigoc en la carpeta "/usr/local/bin/" desde la carpeta TFG con el comando como usuario root:

```
cp ./codigoc/ejecutaroot /usr/local/bin/
```

A continuación, utilizar el siguiente comando para darle permiso especial:

```
chmod +s ejecutaroot
```

7. Inicio de servicios fundamentales

Se van a iniciar los servicios más importantes del proyecto:

- Habilitar IPv6:
  - "echo 0 > /proc/sys/net/ipv6/conf/all/disable_ipv6"
  - "net.ipv6.conf.all.disable_ipv6=0" en /etc/sysctl.conf
- Activar el reenvío IP en IPv4 e IPv6:
  - "echo 1 > /proc/sys/net/ipv4/ip_forward"
  - "echo 1 > /proc/sys/net/ipv6/conf/all/forwarding"
  - "net.ipv4.ip_forward=1" en /etc/sysctl.conf
  - "net.ipv6.conf.all.forwarding=1" en /etc/sysctl.conf
- Activar el servicio OpenVPN mediante los siguientes comandos:

```
systemctl -f enable openvpn@server.service
systemctl start openvpn@server.service
systemctl status openvpn@server.service
```

8. Configuración de parámetros de openvpn a través de la web

1) Conectarse a la página web con: <IP_local>/dit/Principal.jsp e iniciar sesión con las siguientes credenciales:

```
Usuario: admin
Contraseña: admin
```

Nota: Es recomendable cambiar las credenciales anteriores, esto se puede cambiar con los siguientes comandos:

```
psql -U dit -h 127.0.0.1 dit
UPDATE usuarios SET contrasena='<contraseña>'
```

Donde <contraseña> es el nuevo valor que tendrá nuestra contraseña.

2) Ir al apartado "Configuración de Servidor" y configurar el siguiente parámetro:

```
                                                                IP_s
Server: <IP_local>
```

Donde <IP_local> corresponde a la IP interna del equipo

3) Se aplican los cambios y se realizan pruebas, donde se va a necesitar otro equipo que se registre en la página con un nuevo usuario y seguir las instrucciones proporcionadas en la web para conectarse al servidor.

ANEXO B: SCRIPTS UTILIZADOS

```
#! /bin/bash
cd /home/dit/TFG/WEB-INF/easy-rsa/
. ./vars

export KEY_COUNTRY=$1
export KEY_PROVINCE=$2
export KEY_CITY=$3
export KEY_ORG=$4
export KEY_OU=$4
export KEY_EMAIL=$5
export KEY_EMAIL=$5
export KEY_CN=$6
export KEY_NAME=$7

./pkitool $6
```

creacert.sh

```
#! /bin/bash
cd /home/dit/TFG/WEB-INF/easy-rsa/
. ./vars

./revoke-full $1

cd ./keys
rm $1.*
```

eliminacert.sh

```
#! /bin/bash

# Nos colocamos en el directorio donde tenemos los certificados
cd /home/dit/TFG/WEB-INF/easy-rsa/keys/

#Definimos las variables que seran necesarias
VAR1=`sed -n '/-----BEGIN/,$p' $1.crt`
CRT="$VAR1"
VAR2=`cat $1.key`
KEY="$VAR2"
VAR3=`cat ca.crt`
CA="$VAR3"

# Ahora nos movemos al directorio donde tendremos la plantilla .ovpn
cd /home/dit/TFG/fichovpn/

#Ahora realizamos una copia con el nombre del usuario y lo guardamos en el
directorio temporal (/tmp)
cat cliente.ovpn > /home/dit/TFG/tmp/$1.ovpn

# Eliminamos la linea del fichero plantilla que tengan certificados
sed -i '/<ca>/,$d' /home/dit/TFG/tmp/$1.ovpn


#Añadimos los certificados en concreto del usuario al fichero plantilla
echo -e "<ca>\n""$CA""\n</ca>" >> /home/dit/TFG/tmp/$1.ovpn
echo -e "<cert>\n""$CRT""\n</cert>" >> /home/dit/TFG/tmp/$1.ovpn
echo -e "<key>\n""$KEY""\n</key>" >> /home/dit/TFG/tmp/$1.ovpn
```

generaovpn.sh

```
#! /bin/bash
USER=$1
IPV4=$2
MASK4=$3
IPV6=$4
MASK6=$5

echo "ifconfig-push" "$IPV4" "$MASK4" > /home/dit/TFG/ccd/$USER
echo "ifconfig-ipv6-push" "$IPV6""/$MASK6" >> /home/dit/TFG/ccd/$USER
```

addstaticip.sh

```
#! /bin/bash
USER=$1

rm /home/dit/TFG/ccd/$USER
```

removestaticip.sh

```
#!/bin/bash

action="$1"
addr="$2"
common="$3"

if [[ "${addr//:/}" == "$addr" ]]
then
    # Is an IPv4 address
    case "$action" in
    add|update)
    # Is an Ipv6 address
    PGPASSWORD=dit psql -U dit -d dit -c "UPDATE usuarios SET conectadovpn=1
where usuario='${common}';"
    PGPASSWORD=dit psql -U dit -d dit -c "UPDATE usuarios SET ipv4='${addr}'
where usuario='${common}';"
        ;;
    delete)
    PGPASSWORD=dit psql -U dit -d dit -c "UPDATE usuarios SET conectadovpn=0
where ipv4='${addr}';"
    PGPASSWORD=dit psql -U dit -d dit -c "UPDATE usuarios SET ipv4='null'
where ipv4='${addr}';"
        ;;
    esac
    exit
fi

case "$action" in
    add|update)
    # Is an Ipv6 address
    PGPASSWORD=dit psql -U dit -d dit -c "UPDATE usuarios SET ipv6='${addr}'
where usuario='${common}';"
        ;;
    delete)
    PGPASSWORD=dit psql -U dit -d dit -c "UPDATE usuarios SET ipv6='null'
where ipv6='${addr}';"
        ;;
esac
```

scriptlearn.sh

```
#!/bin/bash
IPSERVER="remote $1"
KEEP="keepalive $2 $3"
PROTO="proto $4"
CLIENTS="max-clients $5"
MTU="tun-mtu $6"
DHCPva="server $7 $8"
DHCPvb="server-ipv6 $9"

sed -i "/remote/c$IPSERVER" /home/dit/TFG/fichovpn/cliente.ovpn
sed -i "/keepalive/c$KEEP" /home/dit/TFG/server.conf
sed -i "/proto/c$PROTO" /home/dit/TFG/server.conf
sed -i "/max-clients/c$CLIENTS" /home/dit/TFG/server.conf
sed -i "/tun-mtu /c$MTU" /home/dit/TFG/server.conf
sed -i "/proto/c$PROTO" /home/dit/TFG/fichovpn/cliente.ovpn
sed -i "/server /c$DHCPva" /home/dit/TFG/server.conf
sed -i "/server-ipv6 /c$DHCPvb" /home/dit/TFG/server.conf
```

updateconfig.sh

```
#include <stdio.h>
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>
#include <string.h>
int main(int argc, char **argv)
{
  if (argc >= 3)
    {
      char linea[2048] = "/usr/sbin/service openvpn@server restart";
      char prev1[2048] = "/usr/sbin/iptables -t nat -F";
      char prev2[2048] = "/usr/sbin/ip6tables -t nat -F";
      char linea2[2048] = "/usr/sbin/iptables -t nat -A POSTROUTING -s ";
      char linea3[2048] = "/usr/sbin/ip6tables -t nat -A POSTROUTING -s ";
      char cont2[2048] = " -o eth0 -j MASQUERADE";
      char cont3[2048] = " -o sit1 -j MASQUERADE";
      char * ipv4subred = argv[1];
      char * ipv6subred = argv[2];

      printf("La ipv4 subred es %s\n",ipv4subred);
      printf("La ipv6 subred es %s\n",ipv6subred);

      strcat(linea2, ipv4subred);
      strcat(linea3, ipv6subred);

      strcat(linea2, cont2);
      strcat(linea3, cont3);

      printf("%s\n",linea2);
      printf("%s\n",linea3);

      setuid(0);
      system(linea);
      system(prev1);
      system(prev2);
      system(linea2);
      system(linea3);
    }
  return 0;
}
```

ejecutaroot.c