



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Despliegue y evaluación de redes privadas virtuales con
dispositivos de bajo coste*

Grado en Ingeniería Mecánica

ALUMNO: Adrián Segura De Orta

DIRECTORES: Miguel Rodelgo Lacruz

CURSO ACADÉMICO: 2022-2023

UniversidadeVigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE GRADO

*Despliegue y evaluación de redes privadas virtuales con
dispositivos de bajo coste*

Grado en Ingeniería Mecánica
Intensificación en Tecnología Naval
Cuerpo General

UniversidadeVigo

RESUMEN

Las VPN (Redes Privadas Virtuales) son una tecnología muy utilizada en el ámbito civil y militar que permite extender una red local de manera segura sobre una red pública o no controlada como Internet. Proporciona acceso remoto, confidencialidad de la información y anonimato.

Para ello, se utilizan enrutadores y terminales de usuario con capacidad de cifrado por hardware. A medida que aumentan los requisitos de seguridad de la información y la popularidad de las VPN para proporcionar servicios seguros, se hace relevante evaluar la capacidad de dispositivos de bajo costo para su despliegue.

En este trabajo se crearán redes VPN con diferentes protocolos, configuraciones y algoritmos de cifrado utilizando hardware de bajo costo, como routers programables Mikrotik, Raspberry Pi y terminales Android. Se validará el correcto funcionamiento de las redes y se evaluarán las capacidades de los dispositivos para el cifrado/descifrado y la transmisión de tráfico con servicios demandantes de ancho de banda, como el video de alta definición.

PALABRAS CLAVE

Mikrotik, VPN, Red Privada Virtual, IPSec, Túnel

AGRADECIMIENTOS

En primer lugar, me gustaría agradecer a mis padres y mis hermanos el apoyo incondicional durante todos estos años, tanto en los buenos momentos como en los malos. Quienes conociendo mis ambiciones y mis metas no han dudado en ayudarme en todo lo posible. Así como a mi madrina quien, junto con mi familia, me ayudó también a tomar a tomar las mayores decisiones de mi actualmente corta carrera. Y en el ámbito familiar, me gustaría agradecer también a mis abuelos y a mis tíos el apoyo que me mostraron cuando decidí entrar en la Escuela Naval. En especial a mi abuelo Paco, donde quiera que estes, tu nieto te agradece todo lo que hiciste por él.

En segundo lugar, quiero mostrar mi agradecimiento a mi tutor Don Miguel Rodelgo Lacruz, por ayudarme en todo lo posible durante la realización de este trabajo, quien además tuvo una fe ciega en mí y quien me pegó su sed de mejora y perfeccionamiento constante.

En tercer lugar, me gustaría agradecer a mis compañeros de camarera, los Alférez de Fragata, Iván Méndez y Jose Antonio Muñoz, la paciencia que han tenido conmigo en los momentos de mayor tensión.

Y, por último, me gustaría mostrar mi gran y profundo agradecimiento a mis compañeros de promoción, con los que he pasado los mejores (y también los peores) momentos de mi vida y los cuales me han ayudado a formarme como oficial y como persona. Quien podría olvidar ese Crucero de Instrucción durante esos meses complicados donde únicamente los teníamos los unos a los otros.

CONTENIDO

Contenido	2
Índice de Figuras	4
1 Introducción y objetivos	6
1.1 Contexto y justificación del trabajo	6
1.2 Objetivos	7
1.3 Estructura del trabajo	7
2 Estado del arte	9
2.1 Descripción del apartado.....	9
2.2 Internet: arquitectura y redes.....	9
2.2.1 Historia de Internet	9
2.2.2 Arquitectura	10
2.2.2.1 Modelo OSI	10
2.2.2.2 Modelo Internet	11
2.2.3 Tipos de redes[9]	12
2.3 Redes Privadas Virtuales	13
2.3.1 Características de seguridad y requisitos básicos[12]	13
2.3.2 Tipos de VPN	14
2.3.2.1 VPN de acceso de remoto	14
2.3.2.2 Site to site VPN	15
2.3.2.3 VPN over LAN.....	16
2.4 Cifrado	16
2.4.1 Cifrado Asimétrico	17
2.4.1.1 Algoritmos de cifrado.....	17
2.4.1.1.1 RSA (Rivest-Shamir-Adleman).....	17
2.4.1.1.2 DSA (Digital Signature Algorithm)	18
2.4.1.1.3 SHA (Secure Hash Algorithm)[21]	18
2.4.1.2 Certificado digital[22]	18
2.4.2 Cifrado simétrico	19
2.4.2.1 Algoritmos de cifrado simétrico.....	19
2.4.2.1.1 Triple Data Encryption Algorithm (3DES/TDES)[23]	19
2.4.2.1.2 Cifrado AES	19
2.4.2.1.3 Blowfish 128[27].....	20
2.4.3 Protocolos VPN	21
2.4.3.1 IPsec[29].....	21
2.4.3.2 Transport Layer Security (SSL/TLS)	21

2.4.3.3 Microsoft Point to Point Encryption (MPPE)	22
2.4.3.4 Secure Socket Tunneling Protocol (SSTP)[34]	23
2.4.3.5 Secure Shell (SSH)	23
2.5 Herramientas de red.	23
2.5.1 Winbox	23
2.5.1 PuTTY	24
2.5.1 Xming	25
2.5.2 Wireshark	26
2.5.3 IPERF y JPERF	27
3 Desarrollo del TFG	29
3.1 Materiales	29
3.1.1 Router Mikrotik	29
3.1.1.1 Especificaciones	29
3.1.2 Ordenador HP Omen	29
3.1.3 Xiaomi mi A2 Lite	29
3.1.4 Raspberry Pi 3 modelo B	29
3.2 Creación de una red VPN con OpenVPN	30
3.2.1 Comprobación conexión OVPN	34
3.2.2 Comprobación conexión VPN AES 192 y AES 256	37
3.3 Creación de un túnel con IPSec	38
3.3.1 Comprobación túnel IPSec	40
4 Resultados y pruebas	44
4.1 VPN con OpenVPN	44
4.1.1 Tasa de transferencia con el teléfono móvil	44
4.1.2 Tasa de transferencia con el ordenador	46
4.2 Comprobación túnel IPSec	49
4.3 Resultados	53
5 Conclusiones y líneas futuras	56
5.1 Conclusiones	56
5.2 Líneas futuras	57
6 Bibliografía	58
Anexo I: Implicaciones Sociales, y/o Económicas, y/o Ambientales	61
Anexo II: Reflexiones Éticas y Sociales	63

ÍNDICE DE FIGURAS

Figura 2-1 Estructura modelo OSI [7].....	10
Figura 2-2 Modelo TCP/IP [8]	12
Figura 2-3 Ejemplo NAT	13
Figura 2-4 Tasas de transferencia necesarias [13].....	14
Figura 2-5 VPN de acceso remoto[14].....	15
Figura 2-6 VPN Site to Site[15]	15
Figura 2-7 VPN sobre LAN[16].....	16
Figura 2-8 Ejemplo cifrado[17].....	17
Figura 2-9 Ejemplo de sustitución-permutación[26].....	20
Figura 2-10 Cifrado simétrico y asimétrico	20
Figura 2-11 Ejemplo túnel IPsec[32].....	21
Figura 2-12 Programa Winbox.....	24
Figura 2-13 Menú principal del router	24
Figura 2-14 Interfaz PuTTY.....	25
Figura 2-15 Submenú SSH PuTTY.....	25
Figura 2-16 Programa Xming.....	26
Figura 2-17 Interfaces de red Wireshark	26
Figura 2-18 Captura interfaz de Wireshark	27
Figura 2-19 Programa Jperf.....	28
Figura 3-1 Arquitectura OpenVPN	30
Figura 3-2 Acceso router	30
Figura 3-3 Crear grupo de IP.....	31
Figura 3-4 Creación del perfil para la VPN	31
Figura 3-5 Creación de usuario y contraseña	31
Figura 3-6 Firma del certificado.....	32
Figura 3-7 Creación certificado usuario	32
Figura 3-8 Activación del server de Open VPN.....	33
Figura 3-9 Código OVPN.....	33
Figura 3-10 Interfaz cliente OpenVPN	34
Figura 3-11 Menú autenticación OpenVPN	34
Figura 3-12 IP asignada.....	35
Figura 3-13 Ejemplo establecimiento comunicación	35
Figura 3-14 Captura Wireshark	35
Figura 3-15 Captura ancho de banda.....	36

Figura 3-16 Importación del perfil a dispositivo	36
Figura 3-17 Conexión VPN dispositivo móvil	37
Figura 3-18 Código con AES 192	37
Figura 3-19 Arquitectura IPSec	38
Figura 3-20 Direcciones IP	38
Figura 3-21 Política IPSec	39
Figura 3-22 Establecimiento del Peer	39
Figura 3-23 Propuesta IPsec	39
Figura 3-24 Configuración del NAT	40
Figura 3-25 Captura a la salida del ordenador	40
Figura 3-26 Captura a la salida del router	40
Figura 3-27 Paquete de información a la salida del ordenador (arriba) y a la salida del router (abajo)	41
Figura 4-1 Tasa del móvil sin VPN	44
Figura 4-2 Tasa del móvil con AES 128	45
Figura 4-3 Tasa del móvil con AES 192	45
Figura 4-4 Tasa del móvil con AES 256	46
Figura 4-5 Tasa del móvil con Blowfish 128	46
Figura 4-6 Tasa del ordenador sin VPN	47
Figura 4-7 Tasa del ordenador con AES 128	47
Figura 4-8 Tasa del ordenador con AES 192	48
Figura 4-9 Tasa del ordenador con AES 256	48
Figura 4-10 Tasa del ordenador con Blowfish 128	49
Figura 4-11 Captura Wireshark con IPSec	49
Figura 4-12 Conexión con el puerto de conexión Raspberry 1 (derecha) y Raspberry 2 (izquierda)	50
Figura 4-13 Conexión con el router de conexión Raspberry 1 (derecha) y Raspberry 2 (izquierda)	50
Figura 4-14 Conexión con el router de otra red Raspberry 1 (derecha) y Raspberry 2 (izquierda).	50
Figura 4-15 Conexión con el otro dispositivo. Raspberry 1 (derecha) y Raspberry 2 (izquierda) ..	50
Figura 4-16 Túnel SSH.....	51
Figura 4-17 Comprobación Raspberry 1	51
Figura 4-18 Ejecución de la aplicación en la Raspberry 1 tras tunneling	52
Figura 4-19 Raspberry sin túnel SSH (izquierda) y con túnel SSH (derecha)	52
Figura 4-20 Tasa de transferencia con Windows	53
Figura 4-21 Gráfico tasas de transmisión teléfono móvil y ordenador	54
Figura 4-22 Gráfico tasas de transmisión Raspberry y ordenador	54

1 INTRODUCCIÓN Y OBJETIVOS

1.1 Contexto y justificación del trabajo

El presente trabajo se enmarca en el creciente entorno digital y tiene como objetivo el crear y evaluar distintas configuraciones de redes y poder conectarse a una red privada de forma remota, bien sea para poder trabajar desde casa o desde cualquier lugar, para poder transferir datos en streaming entre dos equipos o cualquier otro dispositivo, o poder acceder a aplicaciones, archivos o impresoras alojadas en otra red, como podría ser la del trabajo.

La conexión tiene que ser una conexión segura y auténtica, que solo necesite tener acceso a una red de internet, por este motivo se creará una red privada virtual con métodos de autenticación de acceso a la misma probando varias de las opciones utilizadas en la actualidad, comparándolas y evaluando las características de las distintas redes desplegadas.

La justificación de este trabajo reside en la importancia y la necesidad de establecer comunicaciones seguras entre las partes debido al creciente aumento de la ciberpiratería, sobre todo en zonas con conexiones públicas. Ya que, muchas veces, en esas conexiones, se introducen datos personales como podría ser detalles de cuentas bancarias. El establecimiento de VPNs en este tipo de conexiones cifrarían la información que se introduce dificultando o incluso negando el acceso a la misma.

Además, hay que tener en cuenta que, como se explicará más adelante, Internet originalmente fue pensado con fines militares, por lo que no se le dio la importancia necesaria a la seguridad, habiendo incluido esta con el paso de los años “por encima”, lo que no lo hace del todo seguro.

Además, se va a tratar la aplicación y posibles usos que podría tener el presente trabajo en el ámbito de las fuerzas armadas, especialmente en el extranjero.

La primera opción y la más obvia es el uso de una red VPN para todas las dotaciones con salida a Internet en el extranjero para manejar los datos de los BYODs (móviles, tablets y ordenadores personales) de cada uno de la dotación. El objetivo es que cuando estos se conecten a una red WiFi en países extranjeros se pueda encriptar su conexión de internet a través del túnel proporcionado por la VPN. Esto garantiza así dicha conexión libre a internet asegurando que no pueda haber filtraciones de seguridad a través de ciertas aplicaciones como Whatsapp.

La segunda opción, aunque más complicada, a nivel CNI, es la utilización de esta VPN para la transferencia de información clasificada en el caso de conflicto o emergencia, debido a que se podría acceder a un servidor con dicha información a través de la tunelización de la conexión y conseguir acceder a la misma. Esta opción es más complicada debido a que se tendría que acreditar la red por el grupo de ciberdefensa de la armada GRUCIBER y el CNI tendría que validar el sistema para operar, que es un proceso lento y complicado.

La primera opción es la más viable a corto plazo y que aporta una capa de seguridad a las filtraciones de seguridad debidas al uso de redes WiFi no seguras, es sencillo de conseguir y no habría que modificar la infraestructura de telecomunicaciones de la Armada y simplemente habría que hacer es instalar una aplicación en los dispositivos del personal.

Esto hace que la implantación de arquitecturas como las que se van a desarrollar en este trabajo sean importantes para su implantación y normalización, tanto en la sociedad como en el ámbito militar.

1.2 Objetivos

El objetivo principal del trabajo es crear y evaluar maquetas de redes virtuales con routers de la empresa Mikrotik que permita al usuario conectarse la dicha red de forma segura y desde cualquier sitio con la única condición de poder tener un acceso a Internet, es decir, conseguir acceder a una LAN mediante el uso de la VPN.

Para lograr dicho objetivo es necesario:

- Entender la arquitectura de Internet para poder aplicar los distintos protocolos de cifrado adecuadamente. Explicar el concepto de red privada virtual, los tipos de redes que existen y los protocolos de seguridad utilizados comúnmente en estas aplicaciones.
- A mayores, el segundo objetivo de este trabajo es conseguir tunelizar una conexión entre dos dispositivos, diseñando e implementando maquetas de redes VPN utilizando distintos protocolos (OVPN, IPSec, SSH) y protocolos de cifrado (AES256, AES128, Blowfish).
- Tras conseguir estos objetivos se pasa a la razón de ser de este trabajo, la evaluación de dichas redes para llegar a la configuración más adecuada, teniendo en cuenta el coste del proceso.

Este trabajo, como ya se ha dicho, tiene como objetivo lograr la mejor configuración, para ello se va a crear la red virtual con varios routers Mikrotik. Se van a configurar esos routers para que uno de ellos pueda admitir conexiones a través de Internet para que se pueda conectar a la LAN. Para esto se van a utilizar como dispositivos de comprobación un teléfono móvil Android y un ordenador con Windows.

Y el segundo objetivo se llevará a cabo mediante la configuración de dos routers Mikrotik para el establecimiento de ese túnel entre dos dispositivos, los cuales serán dos Raspberries. Y en segundo lugar se comprobará dicha configuración entre una Raspberry y un dispositivo con Windows

1.3 Estructura del trabajo

La estructura seguida en el trabajo es la siguiente:

- El primer capítulo, el presente, quedan establecidos la justificación y los objetivos a cumplir del trabajo. Tras haber leído este apartado, el lector podrá entender el tema principal del proyecto y cuáles son las motivaciones que han hecho del presente un trabajo necesario.
- El segundo capítulo, “Estado del arte” tiene como objetivo una pequeña contextualización histórica de lo que es Internet, la historia, su arquitectura junto a sus dos modelos y los tipos de redes que hay. A continuación, se hablará de los que son las redes privadas virtuales (VPN) junto con sus características y requisitos básicos y los tipos de VPN que existen. Justo después, se describirá lo que es el cifrado, se profundizará en los cifrados simétricos y asimétricos, explicando los principales sistemas de cifrado que existen de cada tipo, así como de los principales protocolos de redes privadas virtuales. Y, por último, se dará una pequeña noción de las herramientas de red que se han usado para el desarrollo del trabajo.
- El tercer capítulo, “Desarrollo del TFG”, empezará hablando de los materiales que se han usado para el mismo. Para justo después comenzar la creación de una red VPN usando el protocolo OpenVPN, combinando distintos tipos de cifrado y distintos dispositivos. Después

se explicará la creación de un túnel, siguiendo el protocolo IPSec (apartado 2.4.3.1), entre dos dispositivos.

- El cuarto capítulo, “Resultados y pruebas”, comentará las capacidades que se han obtenido con las distintas maquetas creadas durante el desarrollo del trabajo, finalizando con una comparativa de los distintos métodos y analizado los resultados obtenidos en esas pruebas.
- El quinto capítulo, “Conclusiones y líneas futuras”, se valorarán los resultados obtenidos comparándolos con los esperados durante la realización del trabajo. El objetivo final es que el lector, habiendo llegado a este apartado, sepa valorar la necesidad de la implantación de sistemas de este tipo, así como el proceso de creación de estos para facilitar su implantación. También se indagará en las posibles líneas futuras del trabajo, con la esperanza de poder continuar el mismo aumentando la cantidad de protocolos utilizados.
- En el sexto capítulo, “Bibliografía”, se podrán encontrar todas las referencias utilizadas para la realización del trabajo.
- En el primer anexo “Implicaciones Sociales, y/o Económicas, y/o Ambientales” se podrán encontrar las implicaciones sociales y económicas que se han tenido en cuenta para la realización del trabajo.
- En el segundo anexo, “Reflexiones Éticas y Sociales”, se podrá encontrar una pequeña reflexión del autor acerca del impacto ético-social del trabajo.

2 ESTADO DEL ARTE

2.1 Descripción del apartado

En el presente apartado se va a contextualizar y definir el marco tecnológico en el que se basa este trabajo. Comenzando por una breve introducción a Internet, así como su arquitectura para poder explicar los distintos protocolos de cifrado que se van a utilizar las capas en las que estos se aplican.

2.2 Internet: arquitectura y redes

2.2.1 Historia de Internet

En el año 1969 comenzó un programa de DARPA (Defense Advanced Research Projects Agency) denominado inicialmente como “Resource Sharing Computer Networks” y, posteriormente, como ARPANET. Tenía como objetivos desarrollar técnicas y obtener experiencia en la interconexión de ordenadores y mejorar su productividad mediante la compartición de recursos [1]. Este programa fue una revolución y se convirtió en el programa más importante de DARPA, que en 1975 fue transferido a la Defense Communication Agency quien lo lleva operando desde entonces dando origen a lo que se conoce como Internet.

En un primer momento, esta red contaba con tan solo 4 ordenadores en distintas universidades de Estados Unidos, por lo que no se insistió en el ámbito de la seguridad. Dos años después de comenzar el programa, en 1971, ya había 40 ordenadores de universidades conectados, motivo por el cual, el sistema de comunicación entre los ordenadores había quedado obsoleto, dando lugar al protocolo TCP/IP.

Como inicialmente toda la red de DARPA se había pensado con fines educativos y tecnológicos, no se incorporaron funcionalidades de seguridad a los protocolos y es por eso por lo que se han tenido que ir añadiendo a mayores con el transcurso de los años y a medida que se van detectando nuevas amenazas.

Uno de los protocolos sin seguridad que se han añadido es el protocolo HTTP (Hypertext Transfer Protocol), que actúa en la capa de aplicación, de la que se habla en el siguiente apartado, y sirve para la transferencia de información de a través de archivos en internet. Este protocolo no guarda información sobre conexiones anteriores, fue desarrollada por la IETF (Internet Engineering Task Force) y se implantó en 1991[2]. Tiene una variante más segura denominada HTTPS (Hypertext Transfer Protocol Secure), que es la que usan más del 80% de las páginas de Internet hoy en día[3]. Esta variante trabaja sobre TLS.

Otra de las capas más conocidas que se han añadido es la del Sistema de nombres de dominios DNS (Domain Name System), que es un sistema de nombres jerárquico y descentralizado para ordenadores,

servicios y otros recursos de internet o redes IP. Este sistema asocia información con nombres asignados a cada entidad. El sistema facilita tener que aprender números de IP para cada página, sustituyendo estos por una cadena de caracteres que sean fáciles de leer y entender por las personas, de tal forma que cuando se busca esta cadena de caracteres el servidor al que se está conectado lo traduce en la dirección IP correspondiente[4]. Este sistema ha sido una parte fundamental del funcionamiento de Internet desde 1985.

Este sistema delega la responsabilidad de la asignación de nombres de dominio y el mapeo de esos nombres a los recursos de Internet designados para cada dominio mediante servidores. Los administradores de la red, a su vez, delegan la autoridad de los subdominios a otros servidores, de tal forma que si un servidor no conoce la dirección de una página le “pregunta” al servidor de al lado, creando así un mecanismo de distribución y a prueba de fallos evitando la existencia de un servidor central que almacene toda la información.[5]. Esta capa tampoco tiene seguridad por eso, se desarrolló “a posteriori” el sistema de DNS seguro denominado DNSSEC, el cual trabaja sobre un sistema de clave publica para autenticar las comunicaciones entre servidor y cliente o servido-servidor.[6]

2.2.2 Arquitectura

En cuanto a la arquitectura de redes se refiere hay dos modelos fundamentales propuestos: el modelo teórico OSI y el modelo real de Internet, que agrupa varias de las capas del modelo teórico, denomina modelo Internet.

2.2.2.1 Modelo OSI

El modelo OSI (Open System Interconnection) es el modelo de red propuesto por la ISO (International Standaritation Organization) en 1977 y aprobado en 1984.

Este modelo consta de 7 capas, tal y como se aprecian en la Figura 2-1, que definen cada una de las fases por las que pasan los datos durante el proceso de comunicación entre dos equipos. La idea de este modelo es poder descomponer el complejo proceso de comunicación en procesos más sencillos; estos últimos se asocian a cada una de las capas, de forma que cada capa se despreocupa de lo que ocurren en las otras y ofrecen servicios para la capa inmediatamente superior.



Figura 2-1 Estructura modelo OSI [7]

Las capas del modelo OSI son las siguientes:

- Capa física: se refiere al medio de transmisión de datos, es decir, se encarga de enviar y recibir los bits.
- Capa de enlace: se encarga del envío de paquetes de información, ofrece un enlace libre de errores.
- Capa de red: proporciona el envío de paquetes sobre múltiples enlaces.
- Capa de transporte: ofrece el envío extremo a extremo.
- Capa de sesión: se encarga de la gestión de diálogos entre aplicaciones.
- Capa de presentación: convierte los datos en representación.
- Capa de aplicación: proporciona al usuario las funciones necesarias para su correcto uso.

2.2.2.2 *Modelo Internet*

El modelo Internet, como se ha mencionado, es un modelo usado en la actualidad, y que agrupa algunas de las capas modelo OSI, quedándose estas en 5, como en la Figura 2 2. Trabajando principalmente sobre dos protocolos, el protocolo TCP y el protocolo IP

Estos protocolos, Transmission Control Protocol/Internet Protocol, son los más populares utilizados en Internet y ha llegado a extenderse a los sistemas operativos. Estos protocolos actúan sobre cuatro de las cinco capas.

En primer lugar, el protocolo MAC actúa sobre la capa de enlace de datos, el protocolo permite incluir las especificaciones para poder traducir los diferentes métodos de direccionamiento de red utilizados a direcciones de capa de enlace, así como de control de acceso al medio, las conocidas como direcciones MAC.

En segundo lugar, el protocolo IP, actúa sobre la capa de red, y además es el componente principal de la capa. El protocolo define los dos sistemas de direccionamiento utilizados para identificar los clientes y ubicarlos en la red. La versión más utilizada de este protocolo actualmente es el Internet Protocol versión 4 (IPv4), que utiliza direcciones de 32 bits, lo que permite identificar 2^{32} usuarios. Esto supone una limitación y se está mudando a la versión 6 del mismo protocolo (IPv6) la cual utiliza direcciones de 128 bit y permite identificar 2^{128} usuarios.

En tercer lugar, actúa sobre la capa de transporte. En esta capa TCP se centra en la conexión de flujo de datos confiable, de forma que los datos lleguen ordenados, con la mínima cantidad de errores, sin duplicados, asegurando que lleguen al destino y con control de congestión de tráfico. Además, el segundo protocolo más utilizado es UDP (User Datagram Protocol) el cual se centra más en la transmisión de datos donde el tiempo de llegada tiene más importancia que su fiabilidad, es por eso por lo que es el protocolo utilizado para streaming.

Y, por último, actúa sobre la capa de aplicación, en esta capa el protocolo es capaz de distinguir entre protocolo de usuario y de soporte, brindando servicios a un sistema de infraestructura de la red.

Las capas del modelo TCP/IP (Figura 2-2) son: capa física, capa de enlace, capa de red, capa de transporte y capa de aplicación: que agrupa las anteriores capas de transporte, sesión y presentación.



Figura 2-2 Modelo TCP/IP [8]

2.2.3 Tipos de redes[9]

Las redes se pueden clasificar según la distancia que existe entre los usuarios que la componen en 4 tipos:

- **PAN (Personal Area Network):** estas redes son las más recientes y se refiere a las redes de dos o más dispositivos conectadas entre sí y localizadas a escasos metros del usuario principal. Un buen ejemplo de este tipo de redes es la conexión Bluetooth entre dispositivos de un único usuario.
- **LAN (Local Area Network):** son redes creadas por un grupo de dispositivos próximos entre sí uno a otro. Este tipo de redes se puede usar en edificios. Un ejemplo puede ser dos ordenadores conectados por medio de un cable de Ethernet, o bien, las redes creadas por impresoras para uso sin la conexión directa.
Las LAN utilizan el sistema NAT (Network Address Translation) para dirigir las comunicaciones al exterior y que estas vuelvan a la LAN, al equipo que ha enviado la comunicación. El método NAT permite mapear un espacio IP a través de añadir cabeceras en los paquetes mientras estos están en tráfico. Se utiliza en las casas para que con solo una IP se puedan cubrir todos los dispositivos sin tener que darle una IP a cada dispositivo.[10] (Véase Figura 2-3)
- **WLAN (Wireless Local Area Network):** es una red inalámbrica que conecta dos o más dispositivos de un área LAN, en una zona limitada como podría ser una casa o un colegio. Según [11]“ Representa la progresión de la tecnología y la nueva era de las comunicaciones”. Su antecesor fue el protocolo ALOHA.

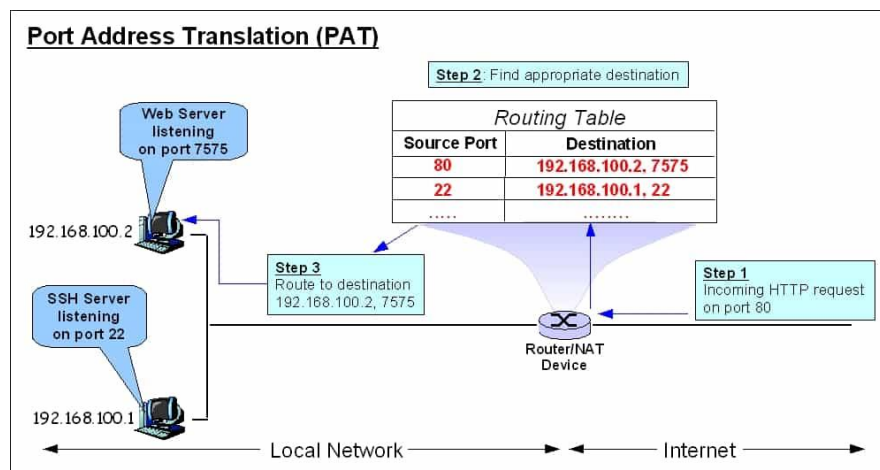


Figura 2-3 Ejemplo NAT

- MAN (Metropolitan Area Network): redes privadas, normalmente de alta velocidad, creadas por uno o más enlaces punto a punto. Un ejemplo de estas redes son las redes de las universidades.
- WAN (Wide Area Network): son las redes que enlazan dos o más LAN. Un ejemplo de estas redes son las redes satelitales o las redes de operadores o ISPs (Internet Service Provider).

2.3 Redes Privadas Virtuales

Una red privada virtual es un mecanismo que permite crear una conexión segura entre un ordenador y una red o bien entre dos redes usando un medio de comunicación no seguro o sin la seguridad suficiente. También se puede usar las VPN como método para extender el uso de una red privada, como podría ser la WAN-PG del Ministerio de Defensa. En resumen, hace que dos redes locales se comporten como una única red.

2.3.1 Características de seguridad y requisitos básicos[12]

Las VPN deben tener las características de seguridad propias de las redes para garantizar su correcto funcionamiento. Estas características son las siguientes:

- Autenticación y autorización, es decir, que usuario está accediendo a la red y que clasificación de seguridad o nivel de acceso tiene.
- Integridad: que consiste en garantizar que los datos no se hayan modificado.
- Confidencialidad: que la información sea recibida únicamente por quien la tiene que recibir
- No repudio: lo que hace que el mensaje tenga que ir firmado para que el originador del mensaje no pueda negar haberlo generado.
- Control de acceso: lo que se traduce como que los usuarios tengan acceso únicamente a la información que necesitan ver.
- Registro de actividades.

Todo esto estableciendo una calidad de servicio adecuada que permita asegurar el correcto funcionamiento y rendimiento de la VPN evitando que haya degradación en la velocidad del servicio.

Estas características definen, por tanto, los requisitos básicos de las VPN, que se definen como 4:

- Identificación de usuario: cada usuario debe tener alguna forma de asegurar su identidad para el acceso a la red, evitando que aquellos que no están autorizados puedan hacerlo.
- Cifrado de datos: relacionado con la confidencialidad y debido a que se va a acceder a la red desde una red pública, para esto se van a usar algoritmos de cifrado, de los que se hablará en el apartado 2.4 más adelante.

- Administración adecuada: lo que se traduce como mantener actualizado en todo momento tanto claves de acceso como algoritmos de seguridad.
- Tunnelizar una conexión con el objetivo de poder transferir datos entre dos dispositivos.

Para conseguir una calidad de servicio adecuada hay que conseguir también una serie de tasas de transferencia. En la Figura 2-4 se pueden observar las diferentes tasas de bits que Google recomienda para poder llegar a diferentes calidades de video en streaming, estas van desde los 4500 kbps para video a 1080, hasta los 51000 kbps para la transmisión de video en 4K.

4K/2160p a 60 FPS	• Resolución: 3840x2160 • Rango de tasa de bits de video: 20.000-51.000 Kbps
4K/2160p a 30 FPS	• Resolución: 3840x2160 • Rango de tasa de bits de video: 13.000-34.000 Kbps
1440p a 60 FPS	• Resolución: 2560x1440 • Rango de tasa de bits de video: 9000-18.000 Kbps
1440p a 30 FPS	• Resolución: 2560x1440 • Rango de tasa de bits de video: 6000-13.000 Kbps
1080p a 60 FPS	• Resolución: 1920x1080 • Rango de tasa de bits de video: 4500-9000 Kbps

Figura 2-4 Tasas de transferencia necesarias [13]

•

2.3.2 Tipos de VPN

Existen tres arquitecturas diferentes para las conexiones VPN, descritas a continuación.

2.3.2.1 VPN de acceso de remoto

Se trata de una configuración host-to-network (usuario a la red). Es la más utilizada y permite conectar remotamente el dispositivo como si estuviese directamente conectado a la red. Este tipo de VPN provee acceso al usuario a una Intranet, como una red de empresa. Es utilizada para trabajadores que trabajan a distancia y les sirve para acceder a recursos privados o bien para poder utilizar aplicaciones necesarias para su trabajo sin exponer estas al internet público, como en la Figura 2-5.

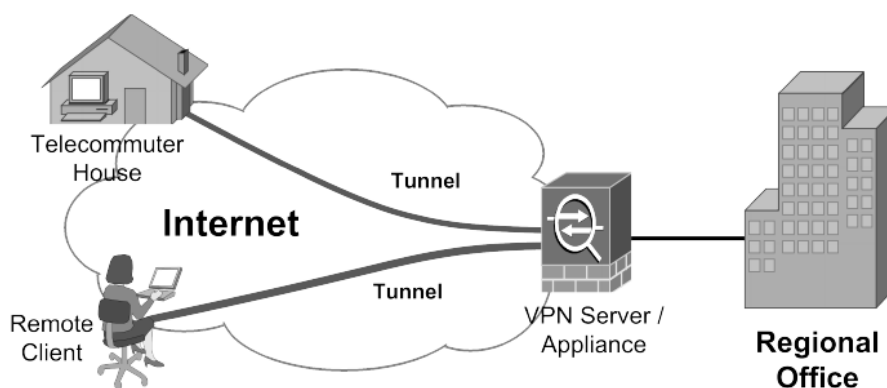


Figura 2-5 VPN de acceso remoto[14]

2.3.2.2 Site to site VPN

Una red Site-to-site o punto a punto es una configuración de VPN que conecta dos redes distintas. Es una configuración bastante utilizada por empresas que poseen distintas sedes a lo largo del globo. El servidor que posee la VPN dispone de conexión a Internet de forma permanente y es este quien acepta las distintas conexiones que provienen de los distintos routers vía Internet. Estos equipos suelen utilizar los servicios del ISP local mediante conexiones de banda ancha. Véase Figura 2-6.

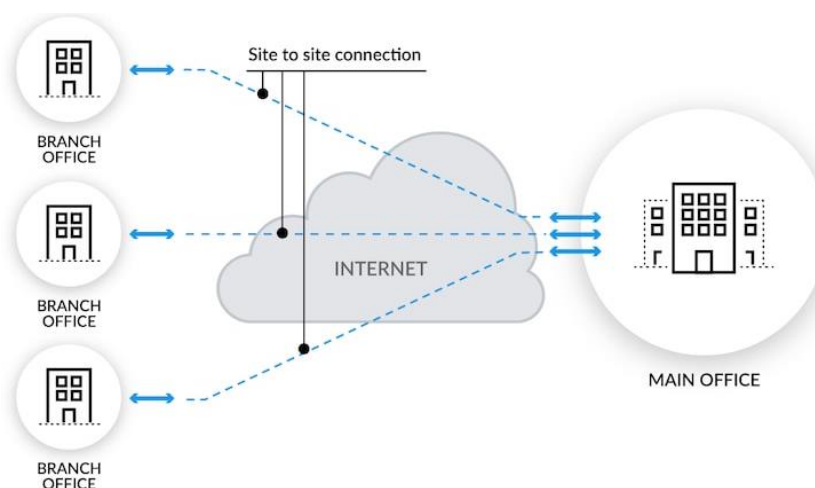


Figura 2-6 VPN Site to Site[15]

Cabe destacar que la forma de conexión más típica de esta configuración VPN es el tunneling, el cual es un protocolo de comunicación que permite mover datos de una red a otra y que consiste en encapsular o tunelizar el protocolo de red mediante un protocolo encapsulador creando una unión o túnel entre las redes de ordenadores. El establecimiento de este túnel necesita de una PDU (Protocol Data Unit) dentro de otra PDU y tiene como objetivo transmitir esta unidad desde un extremo al otro sin la necesidad de una PDU que actúe de intermediario, de esta forma se encaminan los distintos paquetes de datos sobre los distintos nodos sin que estos sean capaces de ver el contenido de cada uno de los paquetes, ni las cabeceras de los mensajes tunelizados. De esta forma se consigue que no se pueda saber quién manda el mensaje ni que es el mensaje, mejorando la característica mencionada anteriormente de confidencialidad.

El ejemplo más común de esta configuración VPN, orientado a flujo de datos, es el tunneling mediante el protocolo SSH (Secure Shell, apartado 2.4.3.5), utilizado frecuentemente para tunelizar el tráfico de carácter confidencial a través de Internet de una forma segura. Los usuarios de esta configuración transfieren datos no cifrados a través de un medio cifrado. Un ejemplo común de cifrado mediante protocolo SSH se da en máquinas con Microsoft Windows, las cuales son capaces

de transferir archivos usando el protocolo SMB (Server Message Block), el cual es un protocolo no encriptado. De esta forma cualquier archivo transmitido mediante este protocolo por internet podría ser interceptado por cualquiera. Una vez establecida la conexión mediante SSH los datos que encamina el protocolo SMB pasan por este túnel, cabe destacar que, aunque la tunelización es segura los datos siguen sin estar cifrados.

Aunque a día de hoy varias empresas como [15] dicen que este tipo de aplicación de las VPN está comenzando a estar en desuso debido a que muchas compañías mueven sus datos a la nube, haciendo que no tenga sentido tener que tunelizar esa conexión a un servidor en vez de a la nube.

2.3.2.3 VPN over LAN

Esta configuración es la menos conocida de las tres configuraciones, aunque es de la que más capacidades tiene para utilizarse dentro una cualquier empresa con distintos niveles de responsabilidad. Se trata de una VPN de acceso remoto pero establecida dentro de una misma red LAN, debido a que permite aislar tanto zonas como servicios ofrecidos por la red interna. Uno de los ejemplos más comunes en empresas, es aislar un servidor con información sensible, como podría ser las nóminas de los empleados o documentos con información clasificada. En el caso del ejército, aportando un paso de autenticación a mayores al cifrado de la información, haciendo que a esta información pueda acceder, única y exclusivamente, el personal de recursos humanos en el caso de una empresa u ordenadores muy concretos en el caso del ejército. Estos ordenadores tienen que estar bastionados para tener información de carácter clasificado. Un ejemplo de esta arquitectura de VPN se puede ver en la Figura 2-7.

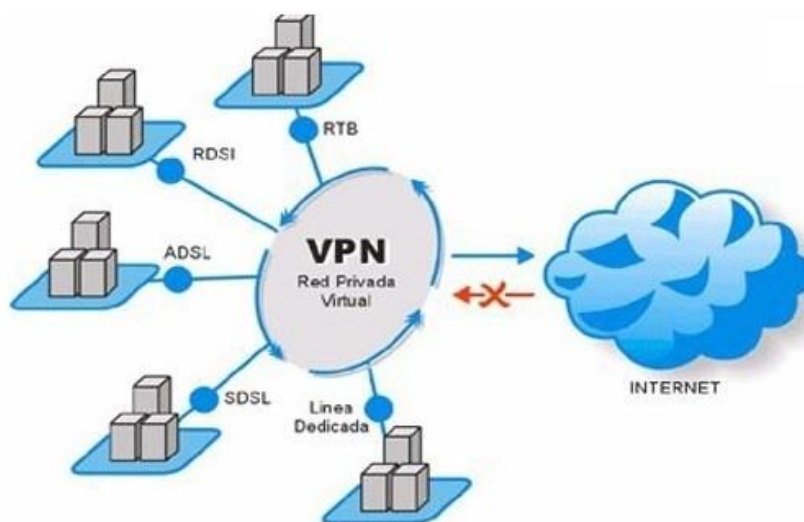


Figura 2-7 VPN sobre LAN[16]

2.4 Cifrado

En el ámbito de la criptografía, el cifrado es el proceso en el cual se codifica la información, convirtiendo el mensaje original en una serie de caracteres aparentemente aleatorios siguiendo un algoritmo, de forma que solo el equipo o persona autoriza pueda descifrar el mensaje para transformarlo de nuevo en el original y poder acceder a esa información. (Figura 2-8)

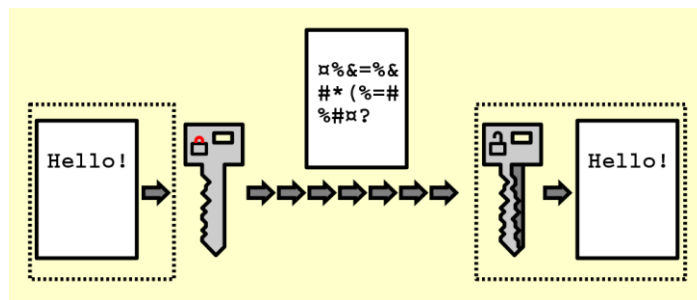


Figura 2-8 Ejemplo cifrado[17]

Aunque se han utilizado a lo largo del tiempo diferentes métodos de cifrado, como podría ser la máquina enigma, actualmente se emplean los conceptos de cifrado simétrico y asimétrico, siendo enigma un ejemplo del cifrado simétrico.

En algunas ocasiones se puede realizar un preprocesado del texto que permitan dificultar el acceso a la información y hacerlo más resistente a ataques de criptoanálisis, siendo frecuentes, entre otros, la conversión del alfabeto o la conversión a números.

2.4.1 Cifrado Asimétrico

Usado en los cifrados de clave pública, el cual utiliza dos claves para cada usuario, una clave pública que se utiliza para cifrar los mensajes y es conocida por todos y una clave privada, que solo tiene el receptor del mensaje y que sirve para descifrar los mensajes. La utilización de cifrado asimétrico permite también el proceso de firma electrónica de la información enviada, que seguiría el proceso inverso, se firma con la clave privada y se comprueba con la clave pública.

2.4.1.1 Algoritmos de cifrado

A continuación, se describen los algoritmos de cifrado asimétrico más utilizados y más conocidos.

2.4.1.1.1 RSA (Rivest-Shamir-Adleman)

RSA es un sistema criptográfico de clave pública, desarrollado por aquellos que le dan nombre en 1977. Es uno de los más antiguos utilizados hoy en día.[18]

En un sistema de clave pública. La clave pública es conocida por todos mientras que la otra es una clave privada. Utiliza números primos para la creación de las claves, tanto pública como privada, de esta forma un mensaje lo puede codificar quien quiera mientras que solo lo puede descifrar aquel usuario que disponga de esos dos números primos. La seguridad de este código reside en la factorización de esos dos grandes números primos, conocido como el problema de factorización y, actualmente, no hay ningún método publicado para romper el sistema en un tiempo razonable si la clave de encriptación es lo suficientemente larga. Suele utilizar claves de 2048 o 4096 bits.[19]

El algoritmo cuenta con 4 pasos: generación de la clave, distribución de esta, proceso de encriptación y proceso de desencriptación.

Para la generación de clave se escogen dos números primos grandes p y q , y para dificultar la factorización estos números tienen que ser grandes y aleatorios de magnitud semejante, se calcula $n=pq$ y este valor es parte de la clave pública, se le aplica a n la función de Carmichael y se mantiene en secreto; y tras una serie de operaciones se determina que la clave pública es n con el exponente e que es un integrador y la clave privada es esa misma n pero con el exponente $d = e^{-1}$. [20]

Hay que destacar que la clave privada se suele utilizar también para firmar los documentos de forma que se pueda autenticar la procedencia de este. También que este algoritmo es bastante lento, por lo que se suele utilizar para la transmisión de una clave simétrica y poder establecer un túnel de cifrado simétrico que es más rápido.

2.4.1.1.2 DSA (*Digital Signature Algorithm*)

DSA es un sistema criptográfico de clave pública y estándar federal de procesamiento de información para firmas digitales. Es un algoritmo asimétrico, propuesto por el NIST en 1991, quien lo patentó, aunque lo dejó para uso de todo el mundo sin necesidad de pago.

El proceso de generación de claves sigue los siguientes pasos:

1. Se coge una clave de L bits siendo L mayor que 512 y menor que 1024, siendo este divisible por 64.
2. Se coge un módulo N de forma que $N < L$
3. Se elige un número primo p_1 de longitud N y un número primo p_2 de longitud L , de tal forma que $p_2 - 1$ sea múltiplo de p_1
4. Se escoge un integrador h comprendido entre 2 y $p - 2$
5. Por último, se computa $g = h^{(p^2 - 1)/p_1}$

De esta forma que el algoritmo se basa en tres parámetros, p_1 , p_2 y g , que son compartidos entre los distintos usuarios del sistema

2.4.1.1.3 SHA (*Secure Hash Algorithm*)[21]

Es una familia de funciones criptográficas publicadas por el NIST. En este apartado se va a explicar SHA1, ya que va a ser la que se utilice para el intercambio de claves por el router.

SHA1 produce un mensaje basado en los principios de Rivest mencionado anteriormente, fue desarrollado por el gobierno de Estados Unidos. Sus usos son criptográficos y de integridad de la información.

En cuanto en la criptografía SHA-1 forma parte de una gran cantidad de protocolos como TLS o SSH, aunque es un protocolo que está empezando a estar en desuso debido a la aparición de SHA-2.

Y respecto a la integridad de la información, SHA-1 no es un método de seguridad, pero es utilizado para identificar cambios y asegurar que la información no ha cambiado debido a corrupción de esta.

2.4.1.2 *Certificado digital*[22]

El certificado digital o certificado público digital es un documento electrónico utilizado para probar la validez de una clave pública. Este incluye información acerca de su dueño y la firma digital de la entidad que ha verificado el contenido del certificado. Si la firma es válida el software que utiliza el certificado lo examina y lo utiliza para comunicarse de forma segura con el dueño del certificado. En TLS se utiliza el certificado, normalmente, entre ordenadores para identificar las organizaciones o individuos y para identificar los distintos dispositivos. Además, suele utilizarse para el intercambio de claves privadas de sesión para establecimiento de comunicación.

En una estructura de clave pública, es necesario también una autoridad certificadora, normalmente una empresa o departamento que se encargue de crear y organizar los certificados de los usuarios.

Hay varios tipos de certificados, de estos se van a explicar los dos que se van a utilizar en el presente trabajo:

- Certificado de servidor TLS: asegura la comunicación entre un cliente y un servidor de forma segura. Este certificado es necesario para establecer el enlace entre el host y el destinatario y tiene que estar firmado por la autoridad certificadora.

- Certificado de cliente TLS: este certificado autentica la conexión del cliente con el servicio TLS. Y al igual que el certificado de servidor TLS, este tiene que estar firmado por la autoridad certificadora para probar su autenticidad.

2.4.2 Cifrado simétrico

En este tipo de cifrado la clave de cifrado y descifrado es la misma, es decir, ambas partes deberían tener la misma clave para poder lograr una comunicación segura. Este tipo de criptografía es la más antigua que existe y un ejemplo de esta es la maquina enigma.

2.4.2.1 Algoritmos de cifrado simétrico

A continuación, se describen los algoritmos de cifrado simétrico más conocidos.

2.4.2.1.1 Triple Data Encryption Algorithm (3DES/TDES)[23]

El cifrado Triple DES es un algoritmo de cifrado que aplica DES en cada bloque de información, que utiliza claves de 56 bits, por lo que, al realizar el proceso tres veces, puede tener claves de 56, 112, 168 bits, y fue desarrollado por el IBM en los años 70. El algoritmo lo que hace es transformar el mensaje o información a través de una serie de operaciones en el mensaje cifrado con la misma longitud de mensaje. En el caso de DES el tamaño de bloque es de 64 bits, que son los 56 de la clave, ya mencionados, y tiene 8 bits de paridad.

Las operaciones que realiza el cifrado sigue lo que se conoce como función de Feistel, que consiste en dividir el texto en dos partes iguales, denominados L_0 y R_0 de tal forma que para cifrarlo $L_i = R_{i-1}$ y $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ donde f es una función que puede ser tan complicada como uno quiera y K es cada una de las subclaves para cada iteración; dando de resultado final el mensaje $L+R$, es decir, ambas cadenas concatenadas.

Y para el descifrado se realizan las siguientes operaciones:

- $R_{i-1} = L_i$
- $L_{i-1} = R_i \oplus f(L_i, K_i)$

Cabe destacar, que debido al creciente crecimiento de las capacidades de los ordenadores Triple DES está desapareciendo debido a que no es capaz de soportar ataques de fuerza bruta y está siendo sustituido por AES, aunque se sigue utilizado en tarjetas de crédito.

2.4.2.1.2 Cifrado AES

El cifrado AES (Advanced Encryption Standard), Rijndael originalmente, es el estándar de encriptación de información establecida por el NIST (National Institute of Standards and Technology) en 2001. AES fue adoptado por el gobierno de los Estados Unidos de América sustituyendo a DES[24]. Es un algoritmo de clave simétrica. Se basa en un principio de Sustitución-Permutación de red y es eficiente tanto para software como para hardware [25]. Opera en bloques de 128 bits y tiene claves de 128, 192 o 256 bits, y esta clave es la que especifica el número de rondas de transformaciones que sufre el mensaje inicial hasta transformarlo en el mensaje cifrado. El número de rondas es el siguiente:

- Para la clave de 128 bit, 10 rondas.
- Para la clave de 192 bit, 12 rondas.
- Para la clave de 256 bit, 14 rondas.

Cada ronda consiste en una serie de pasos que incluyen aquellos que dependen de la clave de encriptación en sí. Y para el descifrado de la información las rondas se aplican al revés usando esa misma clave de encriptación.

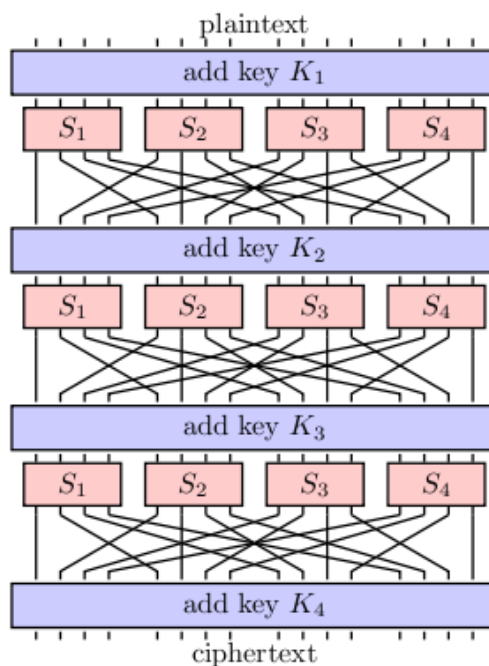


Figura 2-9 Ejemplo de sustitución-permutación[26]

Hay que destacar que cada una de estas claves que aparecen en la Figura 2-9, son derivadas de una sola clave[26]

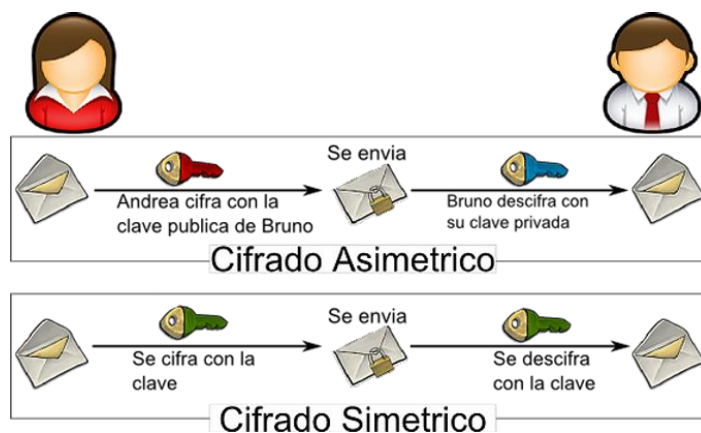


Figura 2-10 Cifrado simétrico y asimétrico

2.4.2.1.3 Blowfish 128[27]

Es un protocolo de cifrado simétrico de bloque diseñado en 1993. Diseñado como un algoritmo de cifrado con propósito general, se considera una alternativa a DES. Blowfish utiliza bloques de 64 bits y una clave variable que va desde los 32 bits a los 448 bits. Utiliza la función Feistel 16 veces, en bloques de 32 bits por línea. Esta función divide los 32 bits de entrada en 4 paquete de 8 bits produciendo 32 bits de salida, repitiendo el proceso durante 16 veces.[28]

Este cifrado se considera en desuso ya que se considera débil frente a ataques de cumpleaños, que es un algoritmo probabilístico, sobre todo en HTTPS. Por este motivo su creador desarrollo un sustituto llamado Twofish.

2.4.3 Protocolos VPN

En este apartado se va a desarrollar los distintos protocolos de seguridad que existen para añadir seguridad y privacidad a las VPN y prevenir el data sniffer (filtrado de paquetes de información), cumpliendo de esta forma con las características mencionadas en el apartado 2.3.1 de confidencialidad, autenticidad e integridad.

2.4.3.1 IPsec[29]

IPsec es la abreviatura de Internet Protocol Security, y es un conjunto de protocolos que autentican y encriptan los paquetes de datos proveyendo de una comunicación segura entre dos ordenadores que trabajen sobre redes IP.

IPsec incluye protocolos de establecimiento mutuo de autenticación entre agentes al principio de la sesión y la negociación de las claves criptográficas durante todo el proceso. IPsec es capaz de proteger el flujo de datos entre clientes, entre puertas de enlace o entre clientes y puertas de enlace. Desarrollada inicialmente la versión IPv4 con pocas medidas de seguridad, IPsec aumenta esta seguridad en la capa tres del apartado 2.2.2.1.

La arquitectura de seguridad de IPsec usa diversos protocolos para garantizar esa comunicación segura

- El primero es el de autenticidad de cabecera (Authentication Headers) que proporciona una conexión que garantiza la integridad y la autenticidad del origen de los datos aportando protección contra ataques de repetición[30]. Para lograr estos calcula el Hash Message Authentication Code operando sobre una clave secreta, el contenido del paquete de datos y las partes constantes del paquete. Además, como se ha mencionado, protege de los ataques de repetición mediante la técnica de ventana deslizante.
- El segundo es el de seguridad de encapsulamiento de paquetes (Encapsulating Security Payloads) que proporciona autenticidad, integridad y confidencialidad aunque no lo hace para el paquete de datos entero, sino que lo hace solo para la información del paquete, dejando en claro la cabecera IP externa[31].
- Y, por último, IPsec utiliza una asociación de seguridad, donde las partes comunicantes utilizan una seguridad conjunta mediante algoritmos y claves. Antes del intercambio de información entre partes, estas establecen que tipo de algoritmo de cifrado simétrico van a utilizar para cifrar el paquete y que función van a utilizar para asegurar la integridad del paquete, como podría ser SHA256. (Figura 2-11)

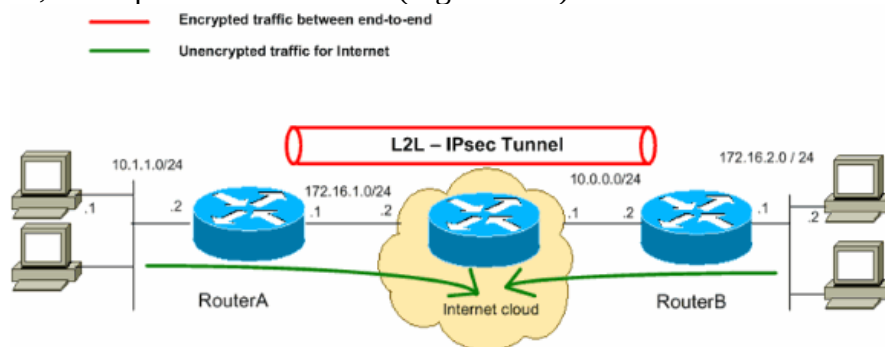


Figura 2-11 Ejemplo túnel IPsec[32]

2.4.3.2 Transport Layer Security (SSL/TLS)

Puede tunelizar el tráfico de una red entera o hacer segura una conexión individual. Es un protocolo criptográfico que proporciona seguridad sobre una red, usado ampliamente en aplicaciones de mensajería instantánea, correo electrónico y chat de voz. Además, es el protocolo criptográfico utilizado por HTTPS.

TLS es un protocolo cuyo principal objetivo es proveer de seguridad, privacidad, integridad y autenticidad mediante el uso de recursos criptográficos como certificados. Trabaja sobre la capa de aplicación del modelo TCP, aunque no “encaja” a la perfección en ninguna capa, y consta de dos procesos, un primer proceso de grabación y uno de “handshake” para el establecimiento de la comunicación. También dispone de un protocolo para transferencia de datagramas denominado DTLS. Fue propuesto por el IETF en 1999 y la versión más actual es la TLS 1.8 de 2018.

Las aplicaciones que utilizan TLS para comunicarse a través de la red previenen el eavesdropping y el tampering y el modo de funcionamiento del protocolo es el siguiente:

- El handshake o apretón de manos comienza cuando un cliente se conecta a un server con TLS requiriendo una conexión segura. En este momento el cliente le da al servidor una lista con los protocolos de cifrado que soporta.
- De esa lista que el cliente proporciona al servidor, este escoge uno de los protocolos que también soporta y le notifica al cliente la decisión, aportando también una identificación en forma de certificado digital que contiene el nombre del servidor y el CA, que es el certificado de la autoridad.
- El cliente confirma la validez del certificado antes de establecer la comunicación y se generan las claves de sesión que se van a utilizar de dos formas distintas:
 - Cifrando un numero aleatorio con la clave pública del servidor y mandándole a este el resultado, para posteriormente usar ambas partes ese número aleatorio para generar una clave de sesión única para el cifrado y descifrado de datos durante la comunicación entre ambos.
 - Usando una clave de intercambio Diffie-Hellman, que consiste en usar la clave privada del cliente y la pública del servidor para cifrar el mensaje y se descifra usando la clave privada del servidor y la pública del cliente. Para generar una clave aleatoria y única para la sesión, añadiendo así una capa más de seguridad.

Esto finaliza el handshake y marca el comienzo de la conexión segura que cifra y descifra la información hasta que esta finalice. Cabe destacar que si cualquiera de los pasos anteriormente mencionados falla por cualquiera de las partes la conexión no se crea y es necesario repetir el proceso.

Cuando se establece la conexión TLS entre dos partes se supone que esta tiene las siguientes características:

- La conexión es privada (o es confidencial) debido a que se ha usado un algoritmo de clave simétrica para cifrar la información transmitida y se genera una única clave para cada sesión.
- La identidad de cada una de las partes puede autenticarse mediante el uso de claves criptográficas públicas.
- Y se puede comprobar que la conexión tiene integridad debido a que cada mensaje posee en su cabecera unos bits de autenticación de código para prevenir la pérdida o la alteración del mensaje durante la transmisión.

2.4.3.3 Microsoft Point to Point Encryption (MPPE)

El cifrado punto a punto de Microsoft encripta la información con el Protocolo Punto a Punto. Las claves soportadas por MPPE son de 128, 56 y 40 bits y proporcionan conexión de seguridad PPTP entre el cliente y el servidor. Cabe destacar que MPPE no permite comprimir ni expandir la información, es por eso por lo que se suele usar junto con Microsoft Point to Point Compression, que permite comprimir la información a través de PPP. Todo esto se define en la RFC 3078 [33] de la IETF.

2.4.3.4 *Secure Socket Tunneling Protocol (SSTP)*[34]

Es un túnel VPN que proporciona un medio de transporte PPP de tráfico a través de un canal TLS, que proporciona un transporte seguro de información con negociación de clave, encriptación y comprobación de integridad de información. Utiliza el protocolo TCP de transporte, lo que le permite saltar virtualmente los firewalls y los proxis.

Los servidores SSTP deben autenticarse durante la fase correspondiente explicada en el apartado 2.4.3.2 al igual que los clientes. SSTP solo sirve para acceso remoto de clientes, y generalmente no soporta túneles VPN site to site.

SSTP tiene las mismas limitaciones de funcionamiento que cualquier otra conexión de túnel TCP sobre IP. En general, el funcionamiento solo es aceptable si hay exceso de ancho de banda suficiente en la red, tanto como para asegurar que permanece el túnel sin que expire el tiempo de conexión. En el caso de que no haya tanto ancho de banda, la conexión fallará, dando lugar al problema conocido como "TCP meltdown problem".[35] [36]

SSTP solo soporta la autenticación de usuario, no soporta la de dispositivo ni la de ordenador.

2.4.3.5 *Secure Shell (SSH)*

Es un protocolo criptográfico que opera sobre redes no seguras, como podría ser Internet, ofreciendo servicios de red segura. Se usa principalmente para acceso remoto y como intérprete de órdenes. Se basan en la estructura servidor-cliente y opera en la capa de aplicación como un grupo de protocolos que proporcionan autenticación, confidencialidad e integridad del servidor; autenticación del usuario para el server; y multiplexación encriptada del túnel en múltiples canales lógicos. [37]

SSH usa las claves públicas criptográficas para autenticar el ordenador remoto y permite autenticar el usuario en caso de ser necesario[38] y se ha usado de diferentes formas a lo largo del tiempo; de estas, la más simple es: ambas partes están en el mismo canal de comunicación, se usa la clave pública-privada generada automáticamente para encriptar la conexión y, después, el usuario introduce su contraseña para autenticarse.

Si la clave pública-privada en vez de ser generada automáticamente es generada por el usuario manualmente, la autenticación se produce en el momento en el que se crea la clave y la sesión se abre automáticamente sin necesidad de introducir la contraseña del usuario. En este caso, clave pública debería estar en todos los ordenadores y debe permitir el acceso al dueño de enlazar las claves privadas. Si el proceso es el de clave privada, esta nunca se enviará a través de la red en el proceso de autenticación. Cabe destacar el SSH solo verifica que la persona que ofrece la clave es también el dueño de la clave privada.

2.5 Herramientas de red.

En este apartado se describen una serie de herramientas y utilidades de red populares que se van a utilizar para la implementación y las pruebas del trabajo.

2.5.1 Winbox

Para trabajar con los routers Mikrotik se va a usar la aplicación Winbox desarrollada por la propia empresa Mikrotik que ofrece la posibilidad de trabajar con el router desde una interfaz más amigable que desde un navegador, aunque cabe destacar, que la interfaz de la versión web de mikrotik es también bastante cómoda.

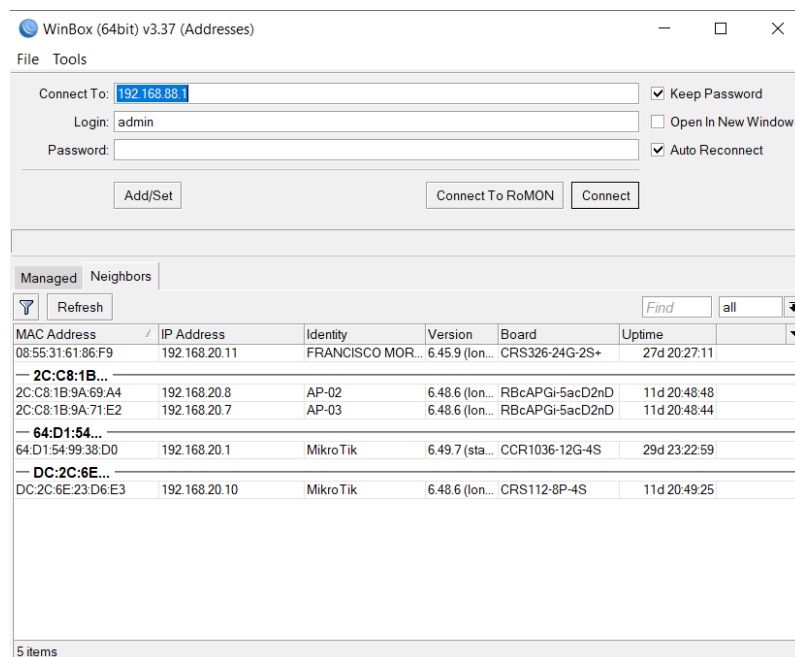


Figura 2-12 Programa Winbox

En la Figura 2-12 se puede observar que en el apartado de “Login” hay una dirección IP. Se puede poner la dirección IP del router en caso de conocerse o se puede acceder al router detectado pinchando en la parte inferior. En este momento se abrirá un menú igual que el que aparecería en el navegador si se introdujese la dirección IP del router.

Una vez accedido al router aparece una ventana como la de la Figura 2-13 en la cual ya se puede empezar a configurar la creación de una VPN entre otras muchas configuraciones.

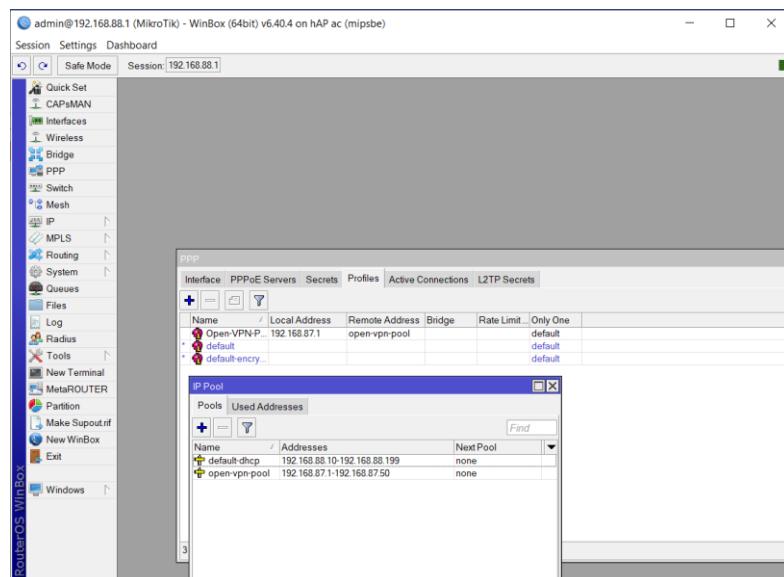


Figura 2-13 Menú principal del router

2.5.1 PuTTY

Es un programa, al igual que Wireshark, gratuito y de código libre, que permite emular un terminal y la transmisión de archivos de aplicación a través de la red. Soporta varios protocolos como SSH y diversos cifrados como AES, Blowfish o 3DES y autenticación por medio de clave pública.[39]

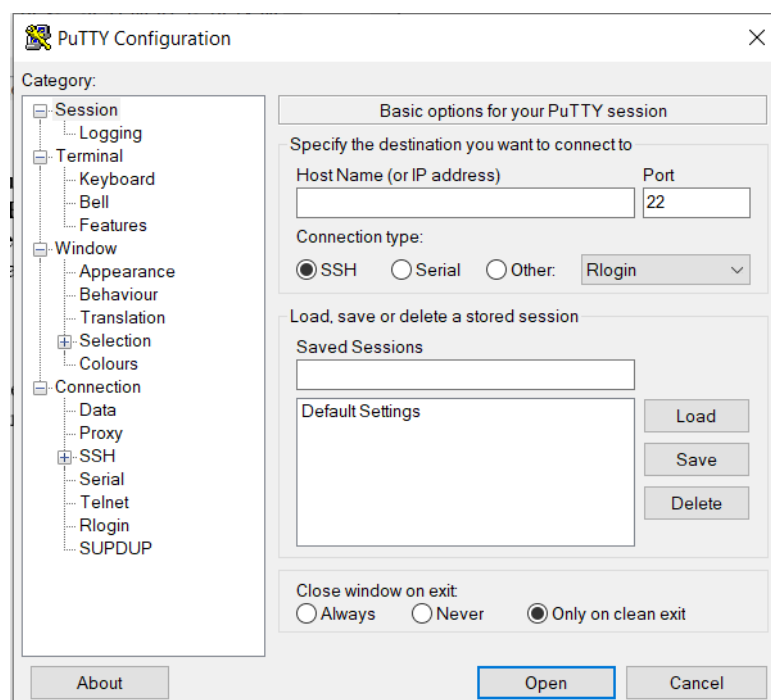


Figura 2-14 Interfaz PuTTY

En la Figura 2-14 se puede observar la interfaz de usuario del programa, donde indicando la IP del dispositivo al que se quiere acceder, seleccionando el protocolo de acceso al mismo y dándole al botón “Open” abrirá una ventana de comandos o interfaz gráfica desde la que controlarlo.

Además, si se quiere ejecutar alguna aplicación gráfica, es necesario activar la opción de X11 forwarding. Esta opción se activa haciendo pulsando en el desplegable que aparece a la izquierda en la opción de SSH, y en “X11”, entonces aparecerá en la ventana la opción de “Enable X11 forwarding” y la se marca con el “tick”. Véase Figura 2-15.

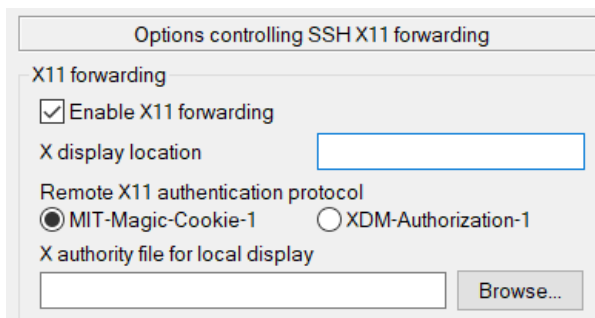


Figura 2-15 Submenú SSH PuTTY

2.5.1 Xming

El último de los programas que se va a utilizar es Xming, el cual es un sistema de ventanas que sirve de interfaz gráfica entre cualquier dispositivo basado en Debian y Windows. Su uso más común es con SSH para establecer sesiones X11 con otros ordenadores.[42]

Es un programa, según [42], “totalmente seguro cuando se usa con SSH”. Fue desarrollado en Windows, y se pensó inicialmente como un programa portable, por lo que su instalación no necesita acceso al registro de Windows.

Como se puede ver en la Figura 2-16, este programa puede ejecutar una ventana directamente introduciendo los datos necesarios, como son la IP de host, el usuario y la contraseña SSH. La otra forma

de conexión es integrarlo con PuTTY, lo cual se hace en automática, de forma que al iniciar el programa y establecer el enlace, se permite ejecutar aplicaciones gráficas.

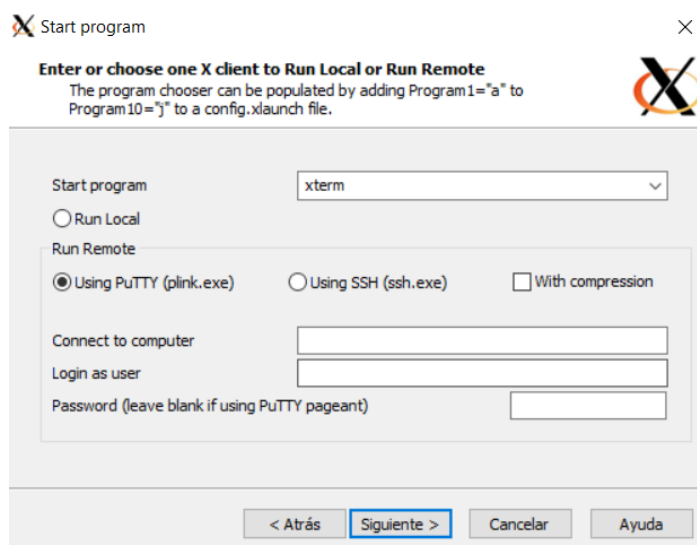


Figura 2-16 Programa Xming

2.5.2 Wireshark

Wireshark es un programa gratuito y de código libre cuya función es la de analizar paquetes y detección de problemas de red. Se desarrolló en 1998 y renombrado como Wireshark en 2006. [40]

Tiene una interfaz gráfica intuitiva en la cual se puede seleccionar la interfaz de red que convenga para la captura y análisis de paquetes, como se puede ver en la Figura 2-17.

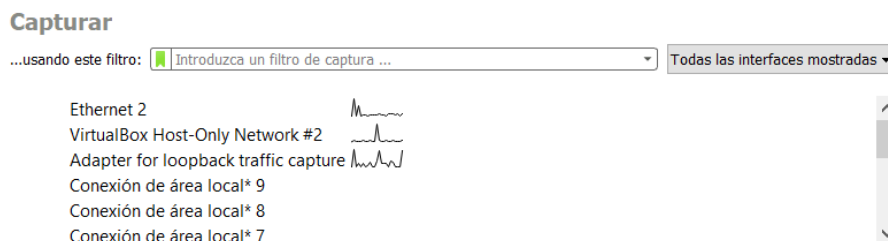


Figura 2-17 Interfaces de red Wireshark

Y, eligiendo una interfaz, se puede capturar el tráfico que pasa por la misma desde el momento en el que se pulsa el botón de captura, hasta el momento en el que se para, con cada paquete en el orden en el que ha llegado.

Además, se pueden abrir los archivos capturados por otro medio, como podría ser Winbox, si estos están con la extensión “. pcap”.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.21.165	239.255.255.250	SSDP	216	M-SEARCH * HTTP/1.1
2	0.006403	192.168.22.79	8.8.4.4	UDP	75	56001 → 443 Len=33
3	0.015746	8.8.4.4	192.168.22.79	UDP	162	443 → 56001 Len=120
4	0.019345	8.8.4.4	192.168.22.79	UDP	70	443 → 56001 Len=28
5	0.020058	142.250.200.101	192.168.22.79	TCP	62	443 → 52371 [SYN, ACK] Seq=0 Ac
6	0.020231	192.168.22.79	142.250.200.101	TCP	54	52371 → 443 [ACK] Seq=1 Ack=1 k
7	0.021209	192.168.22.79	142.250.200.101	TLSv1.3	821	Client Hello
8	0.042291	192.168.22.79	8.8.4.4	UDP	75	56001 → 443 Len=33

> Frame 3: 162 bytes on wire (1296 bits), 162 bytes captured
 > Ethernet II, Src: Routerbo_99:38:d0 (64:d1:54:99:38:d0)
 > Internet Protocol Version 4, Src: 8.8.4.4, Dst: 192.168.22.79
 > User Datagram Protocol, Src Port: 443, Dst Port: 56001
 > Data (120 bytes)

0000 f4 30 b9 96 f8 ea 64 d1 54 99 38 d0 08 00 45 00
 0010 00 94 00 00 40 00 39 11 5e 56 08 08 04 04 c0 a8
 0020 16 4f 01 bb da c1 00 80 e6 16 47 eb e3 a5 c2 bf
 0030 47 83 51 dd 69 11 a4 9c 54 fa cb ea 68 f3 7c 45
 0040 c2 16 96 49 61 10 0d 04 08 23 74 01 c8 6e cc f3
 0050 72 11 f0 e6 7d 18 33 1d 6f b2 81 2a 0b be 9f 0a
 0060 0b 4f 68 3a f8 66 1c 59 92 59 bb 5d b6 09 e7 56
 0070 d5 7e f8 16 83 92 8b 59 84 ec d5 77 84 49 dc dc
 0080 a7 1b 09 b9 15 11 f0 4a e0 22 90 87 3e f8 f4 00
 0090 96 04 eb f1 c9 f3 70 23 14 13 45 1d dd 5d 80 25
 00a0 5f 06

wireshark_Ethernet 2TGM011.pcapng Paquetes: 163 · Mostrado: 163 (100.0%) · Perdido: 0 (0.0%) · Perfil: Default

Figura 2-18 Captura interfaz de Wireshark

En la Figura 2-18, se pueden observar tres diferentes ventanas, la superior es la que muestra, de izquierda a derecha, los paquetes recibidos, tiempo de llegada, IP fuente, IP destino, protocolo utilizado para la transmisión, longitud del paquete y alguna información extra. Si se elige un paquete cualquiera, se cambian las dos ventanas inferiores donde podemos ver, en la izquierda, el contenido del paquete y, en la derecha, el contenido en lenguaje hexadecimal.

2.5.3 IPERF y JPERF

Iperf es una herramienta multiplataforma que sirve para medir tasas de transferencia entre dos dispositivos. Para esta medición uno de los dispositivos tiene que estar configurado como cliente y el otro como servidor, funciones las cuales vienen incluidas en la propia aplicación. A su vez, nos permite medir esa tasa teniendo varias conexiones del mismo sistema a la vez, es decir, la aplicación puede transmitir varios paquetes a la vez y medir la tasa de cada flujo. Esto nos permite aprovechar todo el ancho de banda disponible, además, el programa nos da las tasas de cada flujo y la tasa de transmisión total.[41]

Estas mediciones se pueden hacer a través del protocolo TCP o del protocolo UDP. El programa con el que se va a utilizar en este trabajo es Jperf, el cual es una interfaz gráfica desarrollada en Java de Iperf. En la Figura 2-19 se puede observar una captura del programa, donde se aprecia que se puede ver, como se ha mencionado, que permite seleccionar la opción de cliente o servidor.

Para medir tasas como cliente hay que especificar la dirección IP del dispositivo que está configurado como servidor. Es importante destacar que ambos dispositivos deben de estar en la misma red para poder realizar la medición.

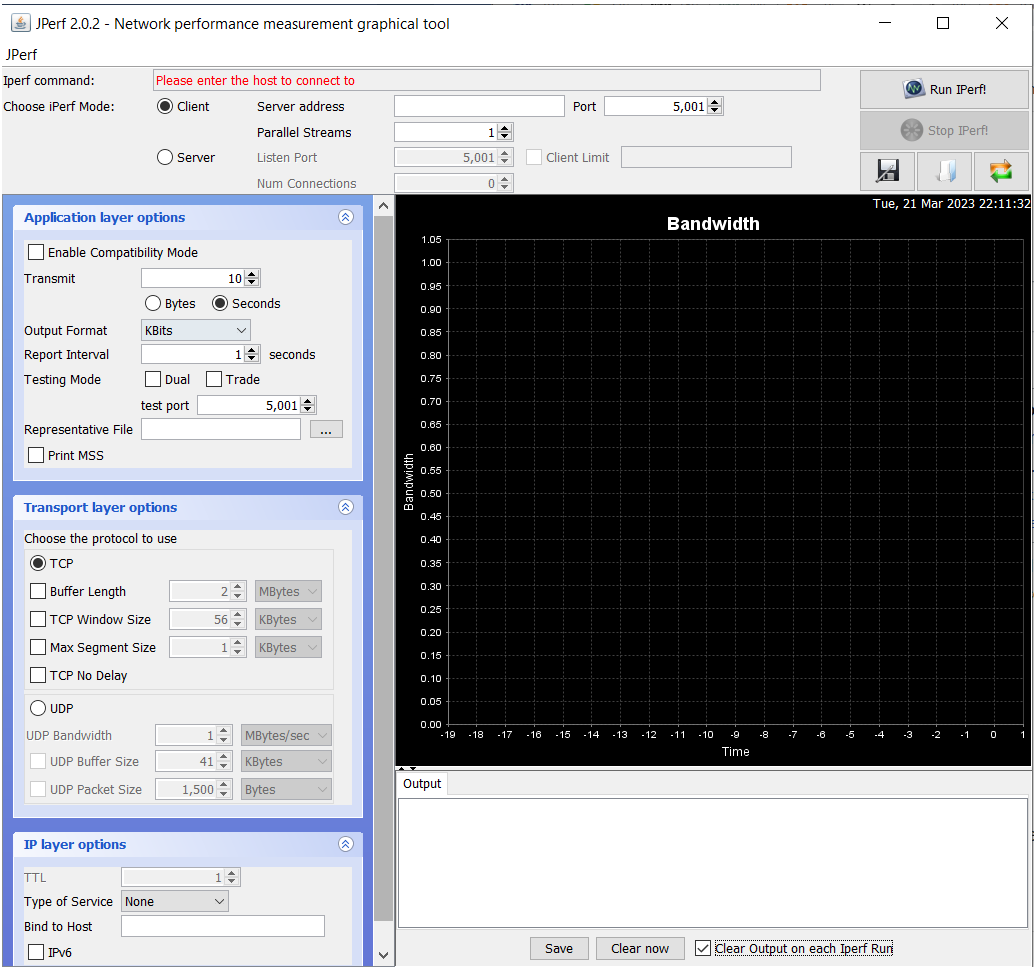


Figura 2-19 Programa Jperf

3 DESARROLLO DEL TFG

3.1 Materiales

En este apartado se va a hablar de los dispositivos y materiales utilizados, así como un pequeño resumen de sus capacidades y características.

3.1.1 Router Mikrotik

Para el presente trabajo se va a operar con los router marca Mikrotik, los cuales son dispositivos de bajo coste, los cuales rondan los 50€. Se trata de pequeños dispositivos ideales para casa y oficinas con pocos dispositivos conectados por cable y conexión WiFi. Además, suelen ser utilizados de forma didáctica.

3.1.1.1 Especificaciones

Tiene un único núcleo CPU con una frecuencia nominal de 650 MHz, utilizan de sistema operativo RouterOS, una RAM de 64 MB, capacidad de almacenamiento de 16 MB y un tiempo medio de funcionamiento de 100000 horas a 25°C.

En cuanto a capacidades inalámbricas solo trabaja en la banda de 2.4 GHz con una capacidad de transferencia máxima de 300 Mbit/s y utiliza la generación WiFi 4. Tiene 5 puertos de Ethernet se alimenta mediante corriente continua de 10 a 28 V y 5 W de potencia máxima.

3.1.2 Ordenador HP Omen

En el presente trabajo el ordenador con el que se va a trabajar es un ordenador HP Omen 17 de 2017 con un procesador Intel Core i7 y una tarjeta gráfica Nvidia GTX 1060. Cabe destacar de este ordenador que el propio procesador tiene instrucciones específicas para el cifrado AES lo que hace que todo el proceso de cifrado sea más rápido.

3.1.3 Xiaomi mi A2 Lite

El dispositivo móvil utilizado para la realización del trabajo Xiaomi MI A2 Lite. Tiene un procesador Qualcomm Snapdragon 625 de 2GHz, que tiene aceleramiento por instrucciones internas de cifrado y descifrado de AES, lo que hace que estos procesos se hagan más rápido.

3.1.4 Raspberry Pi 3 modelo B

Este dispositivo forma parte de una serie de pequeños ordenadores desarrollados por las marcas “Raspberry Pi” y “Broadcom”. [43] Se diseñó para ser utilizada en institutos y países en desarrollo, pero obtuvo una acogida mucho mayor a la esperada debido a sus usos en robótica y bajo coste. Además,

tiene mucha acogida en el sector de los juegos retro debido a que se pueden crear consolas arcade instalando cierto sistema operativo.

Utiliza el procesador diseñado por Broadcom BCM2837B0 que no tiene ninguna instrucción interna de cifrado AES, lo que puede hacer que, durante el establecimiento de túneles, la capacidad de transferencia sea menor.[43], [44]

3.2 Creación de una red VPN con OpenVPN

La arquitectura que se ha seguido, debido a las dificultades de configurar el router con salida a internet del cuartel ha sido la de la Figura 3-1, que permite conectarse a la VPN, pero en el rango de cobertura del router.

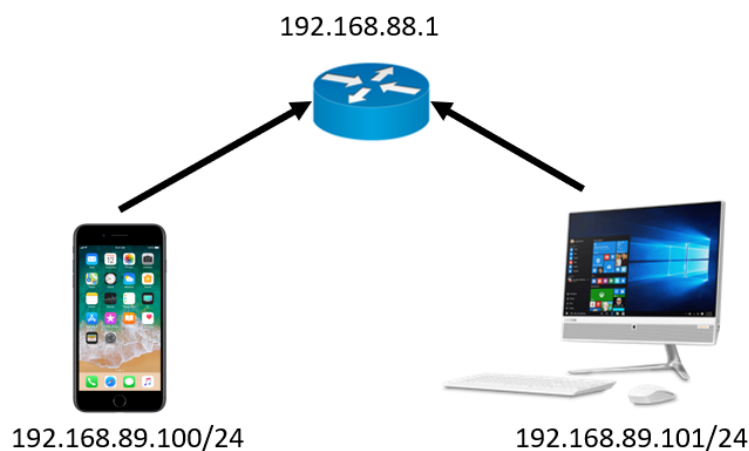


Figura 3-1 Arquitectura OpenVPN

Cabe destacar que, aunque en la Figura 3-1 no aparezca una conexión a Internet, y debido a que el router tiene salida al mismo, se puede navegar con esta configuración.

Para la creación de una red VPN se va a utilizar el programa Winbox mencionado en el apartado 2.5.1 . Una vez abierto accedemos al router tal y como se muestra en la imagen seleccionando el dispositivo y pulsando el botón “Connect”. (Véase Figura 3-2)

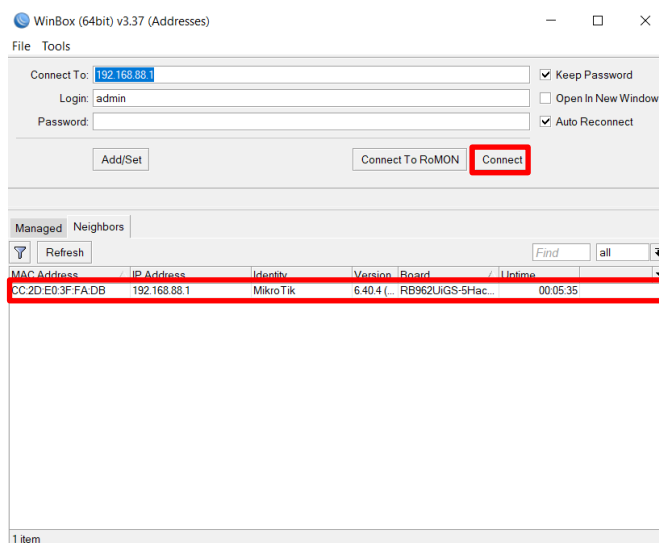


Figura 3-2 Acceso router

Una vez dentro lo primero que hay que hacer es crear un grupo de IP que serán las que se les asignen a los usuarios una vez se conecten a la VPN. Para ello se pulsa en “IP Pool” y se añade un nuevo grupo. En este caso se ha denominado al grupo de IPs “open-vpn-pool” y se le han asignado las IPs “192.168.89.1-192.168.89.50”, tal y como se muestra en la Figura 3-3.

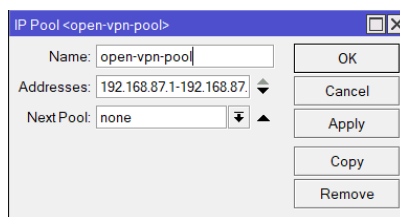


Figura 3-3 Crear grupo de IP

A continuación, hay que crear el perfil. Para ello se pulsa en el botón “PPP” (Figura 3-4) en la pestaña de perfiles y se añade un nuevo perfil, en este caso denominado “Open-VPN-Profile”. Se le va a dar de dirección local la primera dirección del grupo de direcciones IP asignado y en la dirección remota se introduce el nombre del grupo de IP asignado (“open-vpn-pool”), se pulsa en aplicar y aceptar.

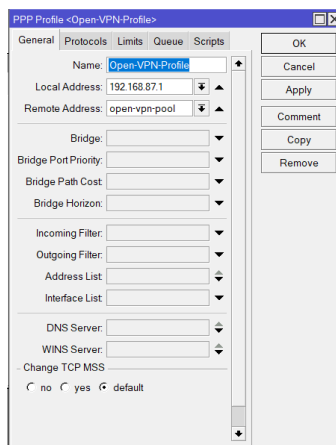


Figura 3-4 Creación del perfil para la VPN

A continuación, hay que crear un usuario y una contraseña para el usuario remoto. Para ello en la misma ventana “PPP”, se selecciona la pestaña “Secretos” y se añade un nuevo secreto (Figura 3-5). Se le pone un nombre, “tfg” en este caso, una contraseña, se selecciona el servicio de “ovpn” y el perfil de “Open-VPN-Profile”, se le da a aplicar y aceptar.

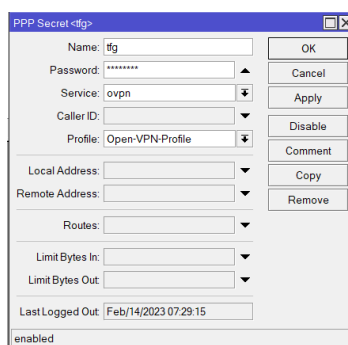


Figura 3-5 Creación de usuario y contraseña

Ahora hay que crear los certificados para el servidor, los usuarios remotos y para la autoridad certificadora (CA). La creación de los distintos certificados es parecida, por ese motivo se va a detallar la creación del certificado de usuario y se van a exponer las diferencias con la CA y con el servidor.

Para la creación de los certificados se pulsa en la ventana de “Sistema” y dentro del menú desplegable en “Certificados”, se pulsa en crear nuevo certificado (Figura 3-7). Se le asigna un nombre, un nombre común y un tamaño de clave, se abre la ventana de “Key Usage” y se marcan las opciones de “firma digital”, “cifrado de clave” y “cliente tls”. Una vez hecho todo esto, se le da a aplicar y firmar y en esta opción se selecciona el certificado a firmar y se pone en la opción de CA el certificado creado para la autoridad certificadora. (Véase Figura 3-6)

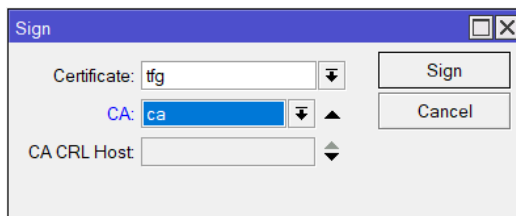


Figura 3-6 Firma del certificado

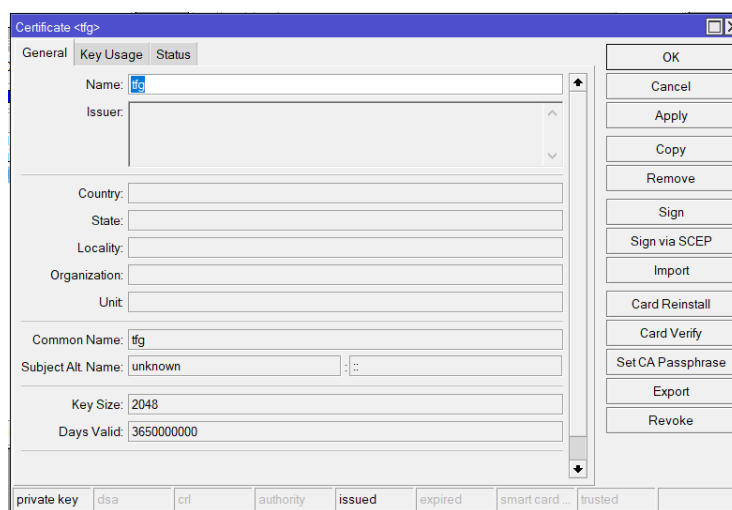


Figura 3-7 Creación certificado usuario

Las diferencias del certificado con los otros dos residen en que en el servidor en lugar de marcar la opción de “cliente tls” hay que marcar la opción de “servidor tls”; y en la CA hay que marcar las opciones de “firma crl” y “firma con certificados clave”. Una vez creados, hay que exportar los certificados de la CA y el usuario, poniéndole a este último certificado una contraseña, por lo que se acabarán creando dos archivos.

Una vez creados y exportados los certificados hay que activar la opción de servidores de Open VPN. Para ello, en la ventana de “PPP” se selecciona la pestaña de “Interfaz” y en esta aparece la opción de “OVPN Server”, se pulsa en “Enable” y se selecciona el certificado el creado para el servidor, tal y como se muestra en la Figura 3-8.

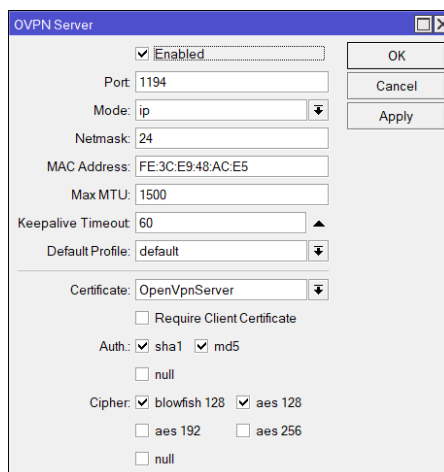


Figura 3-8 Activación del server de Open VPN

Tras todo este proceso, hay que crear un archivo de texto con la información de la Figura 3-9 y guardarlo con extensión “OVPN”. En “Remote” hay que indicar la dirección IP del router, en “ca” hay que poner el nombre del archivo del certificado de la autoridad certificadora, en “cert” el nombre del archivo del certificado del cliente y en “key” el nombre del archivo creado al exportar el certificado del usuario con contraseña.

```
client
dev tun
proto tcp
remote 192.168.89.1 1194
resolv-retry infinite
nobind
persist-key
persist-tun
tls-client
remote-cert-tls server
ca cert_export_ca.crt
cert cert_export_tfg.crt
key cert_export_tfg.key
cipher AES-128-CBC
auth SHA1
pull
auth-user-pass
verb 3
```

Figura 3-9 Código OVPN

En este archivo se está definiendo la configuración del cliente. Para ello se utilizan los siguientes códigos:

- Dev tun: que significa que se utilizará la interfaz de túnel construido en la capa 3
- Proto tcp: se utilizará el protocolo TCP para la transferencia de datos:
- Remote 192.168.89.1 1194: es la dirección de la interfaz del servidor VPN que se va a utilizar, mediante el Puerto 1194, que es el del protocolo OVPN.
- Resolv-retry infinite: en caso de que haya cualquier problema lo vuelve a intentar hasta que se resuelva.
- Nobind: a los clientes se les asignará puertos dinámicos.
- Persist-key: es una opción para que no vuelva a leer los archivos clave al reiniciar el cliente.

- Persist-tun: se mantiene abierta la interfaz del túnel, de forma que cuando se vuelva a abrir comprobará si la IP es la misma, si coincide se volverá a conectar y si no lo es cerrará el túnel y lo volverá a abrir.
- Tls-client: habilita TLS y actúa de cliente durante todo el proceso de negociación de TLS.
- Remote-cert-tls server: requiere que el certificado del peer sea firmado con clave de uso y basado en las reglas de TLS.
- Ca: es el certificado de la autoridad certificadora.
- Cert y Key: es el certificado y la clave del cliente.
- Cipher AES-128-CBC: encripta los paquetes mediante el algoritmo AES de 128 bits
- Auth SHA1: algoritmo utilizado por Open VPN para autenticar cada uno de los paquetes
- Pull: Aceptar ciertas opciones del archive de configuración como el peer.
- Auth-user-pass: comando que hace que sea necesario que el cliente requiera usuario y contraseña
- Verb 3: es el grado de detalle para el archivo log del servidor.

Tras todo este proceso, quedaría exportar los archivos de certificado y cliente a cada dispositivo para poder conectarse a la red creada.

3.2.1 Comprobación conexión OVPN

Tras a ver conectado el primer dispositivo a utilizar, que es el ordenador, se ha realizado una captura del tráfico del router para comprobar que se ha conectado correctamente a la red. Para ello primero, mediante la interfaz del cliente de OpenVPN (Figura 3-10), se selecciona la VPN que se ha creado, y se pulsa en “Conectar”.

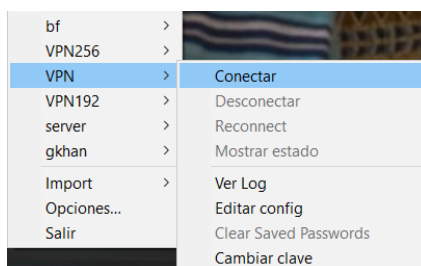


Figura 3-10 Interfaz cliente OpenVPN

Al pulsar en conectar se abrirá un terminal y pedirá que se inicie sesión con el usuario y la contraseña que se ha configurado en el apartado 3.2, (Figura 3-11). Tras todo el proceso de autenticación, aparecerá una pestaña con la IP que se ha asignado (Figura 3-12), que estará dentro del rango que se ha establecido dentro del grupo de IPs.

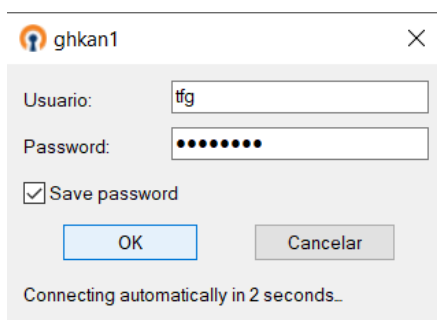


Figura 3-11 Menú autenticación OpenVPN

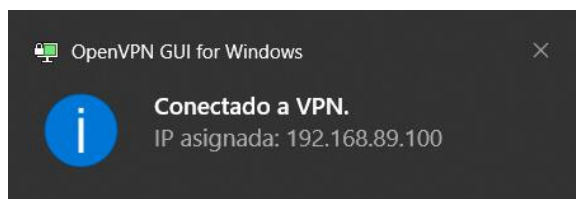


Figura 3-12 IP asignada

Si durante este proceso se pone a capturar el tráfico que pasa por la tarjeta de red del ordenador, utilizando Wireshark, se puede comprobar el método de autenticación de OpenVPN. Lo primero que hacen tanto el cliente como el servidor es comprobar que se escuchan mutuamente, tras esto se intercambian las claves y se realiza el “Handshake” antes de comenzar la transmisión de información. (Figura 3-13)

No.	Time	Source	Destination	Protocol	Length	Info
759	9.034175	192.168.88.199	192.168.88.1	TLSv1.2	347	Client Hello
816	9.674055	192.168.88.1	192.168.88.199	TLSv1.2	1470	Server Hello
820	9.676428	192.168.88.1	192.168.88.199	TLSv1.2	1220	Ignored Unknown Record
830	9.697058	192.168.88.199	192.168.88.1	TLSv1.2	400	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
848	10.076271	192.168.88.1	192.168.88.199	TLSv1.2	121	Change Cipher Spec, Encrypted Handshake Message
850	10.077198	192.168.88.199	192.168.88.1	TLSv1.2	589	Application Data
858	10.155272	192.168.88.1	192.168.88.199	TLSv1.2	297	Application Data
975	11.362459	192.168.88.199	192.168.88.1	TLSv1.2	112	Application Data
1395	16.563722	192.168.88.199	192.168.88.1	TLSv1.2	112	Application Data
1972	21.763149	192.168.88.199	192.168.88.1	TLSv1.2	112	Application Data
1978	21.809307	192.168.88.1	192.168.88.199	TLSv1.2	214	Application Data

Figura 3-13 Ejemplo establecimiento comunicación

Y como se puede comprobar en la Figura 3-14, toda la cabecera IP del mensaje está en claro, mientras que la carga útil del paquete va cifrada. Tal y como se expuso en el capítulo 2, OpenVPN trabaja sobre TLS, que trabaja sobre la capa de aplicación, por eso toda la cabecera IP está en claro, mientras que el contenido del paquete está cifrado.

```
> Frame 975: 112 bytes on wire (896 bits), 112 bytes captured (896 bits)
> Ethernet II, Src: HewlettP_96:f8:ea (f4:30:b9:96:f8:ea), Dst: Routerbo_3f:fa:db (cc:2d:e0:3f:fa:db)
> Internet Protocol Version 4, Src: 192.168.88.199, Dst: 192.168.88.1
> Transmission Control Protocol, Src Port: 51547, Dst Port: 1194, Seq: 1267, Ack: 3005, Len: 58
> OpenVPN Protocol
  Transport Layer Security
    TLSv1.2 Record Layer: Application Data Protocol: Application Data
```

Figura 3-14 Captura Wireshark

En la Figura 3-15 se puede observar una captura del ancho de banda mediante el programa Jperf donde se puede apreciar que la tasa de transmisión es estable a 23500 kbps.



Figura 3-15 Captura ancho de banda

Una vez comprobado su uso con el ordenador, se pasa a comprobar su uso en un dispositivo móvil. Como se ha dicho también tiene capacidad de cifrado en el procesador, por lo que cabe esperar que la tasa de transferencia sea parecida la que tiene sin la VPN que una vez establecida la VPN. Para ello se envían los certificados y el archivo del cliente de la VPN al teléfono móvil, y se procede a su importación

8:18

← Edit Profile SAVE

Profile Name
192.168.88.1 [ghkan1]

Server Override (optional)

Username
tfg

☒ Save password
Password

☒ Save Private Key Password
Private Key Password

SET CONNECT SHORTCUT

DELETE PROFILE ADD PROXY

Figura 3-16 Importación del perfil a dispositivo

Para ello hay que introducir usuario y contraseña, junto con la clave privada, si se quiere que al pulsar en conectar acceda automáticamente a la red. Si se desea introducirla manualmente cada vez que iniciemos la VPN se deja en blanco este campo (Figura 3-16).

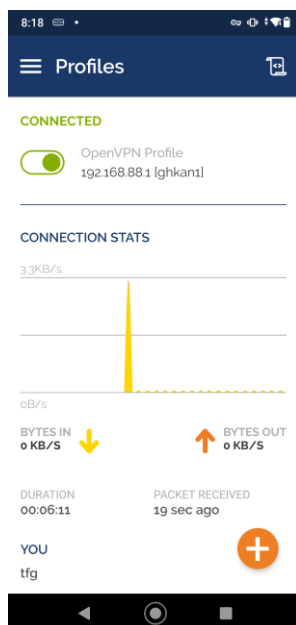


Figura 3-17 Conexión VPN dispositivo móvil

Como se puede ver en la Figura 3-17, una vez conectado el dispositivo la propia aplicación muestra transferencia del dispositivo, aunque para un estudio de la máxima capacidad del dispositivo se va a utilizar de nuevo el programa Jperf.

3.2.2 Comprobación conexión VPN AES 192 y AES 256

Para esta comprobación se va a crear un nuevo fichero con extensión “ovpn” cambiando el cifrado del usuario pasando de “AES-128-CBC” a “AES-192-CBC” y a “AES-256-CBC”. También se va a usar el algoritmo Blowfish 128 para comprobación, siendo el código para este “BF-CBC”. El archivo para el cifrado AES 192 quedaría de la siguiente manera (Figura 3-18)

```
client
dev tun
proto tcp
remote 192.168.88.1 1194
resolv-retry infinite
nobind
persist-key
persist-tun
tls-client
remote-cert-tls server
ca cert_export_ca.crt
cert cert_export_tfg.crt
key cert_export_tfg.key
cipher AES-192-CBC
auth SHA1
pull
auth-user-pass
verb 3
```

Figura 3-18 Código con AES 192

Y ahora se procede a conectar los distintos dispositivos, a las distintas configuraciones

3.3 Creación de un túnel con IPSec

Como segundo diseño de arquitectura de redes, se va a crear una tunelización entre dos routers, con el objetivo de tener acceso a esos dos routers conectando ambos entre sí, además de securizar ese túnel con el objetivo de obtener una conexión segura. La arquitectura que se ha construido es la que aparece en la Figura 3-19.

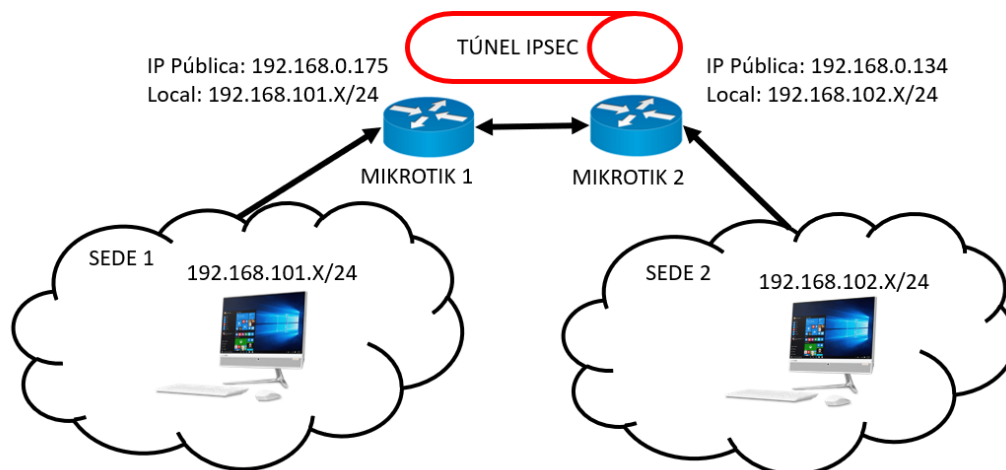


Figura 3-19 Arquitectura IPsec

Para ello se va a comenzar asignando IPs públicas y privadas a los routers, las IPs públicas se van a llamar WAN y las IPs privadas LAN. Se va a configurar únicamente un router, ya que la configuración del segundo es exactamente igual cambiando las IPs destino por las IPs origen.

Address	Network	Interface
192.168.0.134/24	192.168.0.0	ether1
192.168.102.1/24	192.168.102.0	ether2-master

Figura 3-20 Direcciones IP

En el primer router se han puesto como direcciones para la WAN las “192.168.0.134/24” a través de la interfaz de “Ethernet 1”, y las direcciones para la LAN “192.168.102.1/24” a través de la interfaz “Ethernet 2”, para el segundo router se han puesto como direcciones para la WAN “192.168.0.175/24”, que como se puede apreciar está dentro del mismo rango que las del primer router, y para las direcciones LAN “192.168.101.1/24”. Esto se puede observar en la Figura 3-20.

El siguiente paso es crear una política IPsec para permitir que los dispositivos conectados a una de las redes sean capaces de comunicarse con la otra, para ello hay que ir al apartado IP, subapartado IPsec, y agregamos nueva política con dirección de origen las de la LAN del router y de destino las de la LAN del otro router, y en el apartado de acción, hay que poner encriptar y de dirección origen la de la WAN del router y de destino la WAN del otro router (Véase la Figura 3-21).

Figura 3-21 Política IPsec

Después, en el mismo apartado de “IPsec” hay que establecer un “Peer”, para ello se pulsa el botón de añadir, se pone la dirección WAN del router destinatario y se establece un secreto que es una clave para la tunelización, después en el apartado de encriptación se establecen los algoritmos de encriptación posibles para el túnel (Figura 3-22).

Figura 3-22 Establecimiento del Peer

Ahora hay que crear una propuesta o “Proposal”, que tiene que ser la que se introduzca en la parte de política IPsec, para ello establecemos los algoritmos de autenticación y los algoritmos de encriptación que se quiere que acepte nuestro túnel de IPsec (Figura 3-23).

Figura 3-23 Propuesta IPsec

Y, por último, en el apartado de “Firewall” establecemos una nueva regla “NAT” con dirección de origen, la dirección IP de la LAN del router, y dirección de destino, las direcciones IP de la LAN del router de destino, y en el apartado de acción, se elige “Aceptar”, de esta forma, las direcciones IP de los dispositivos de los routers conectados a las redes LAN no se enmascaran. Esto se puede ver en la Figura 3-24.

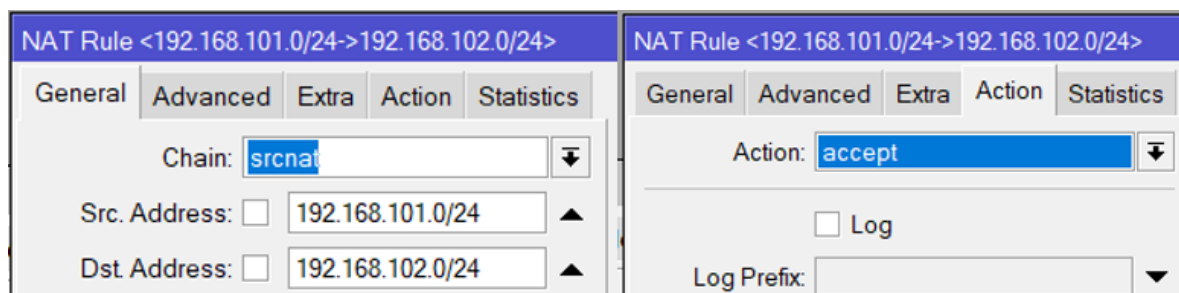


Figura 3-24 Configuración del NAT

Una vez configurados los dos routers hay varias formas de conectarlos como se ha mencionado anteriormente, esta configuración se está realizando para dos routers conectados entre sí por una red común, que se puede simular, bien conectándolos entre ellos por medio del “Ethernet 1” o bien conectándolos a una misma red, como podría ser el internet de casa o del laboratorio.

3.3.1 Comprobación túnel IPsec

Una vez creado el túnel a nivel router, se van a conectar dos dispositivos a los distintos dispositivos, en este primer caso van a ser un ordenador con Windows y una Raspberry Pi 3 Modelo B con sistema operativo Raspbian, que basado en Debian, y se va a capturar el tráfico tanto en la salida del ordenador como en la salida del router para comprobar como efectivamente, el protocolo encapsula las IPs internas para que un tercer dispositivo no pueda saber quién está intentando mandar la información ni a quien se la está intentando mandar.

192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [ACK] Seq=59771 Ack=1 Win=64308 Len=1398
192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [ACK] Seq=61169 Ack=1 Win=64308 Len=1398
192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [ACK] Seq=62567 Ack=1 Win=64308 Len=1398
192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [ACK] Seq=63965 Ack=1 Win=64308 Len=1398
192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [PSH, ACK] Seq=65363 Ack=1 Win=64308 Len=1398
192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [ACK] Seq=66761 Ack=1 Win=64308 Len=1398
192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [ACK] Seq=68159 Ack=1 Win=64308 Len=1398
192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [ACK] Seq=69557 Ack=1 Win=64308 Len=1398
192.168.101.247	192.168.102.252	TCP	1452 63043 → 5001 [ACK] Seq=70955 Ack=1 Win=64308 Len=1398
192.168.102.252	192.168.101.247	TCP	54 5001 → 63043 [ACK] Seq=1 Ack=41597 Win=64240 Len=0
192.168.102.252	192.168.101.247	TCP	54 5001 → 63043 [ACK] Seq=1 Ack=44393 Win=64240 Len=0
192.168.102.252	192.168.101.247	TCP	54 5001 → 63043 [ACK] Seq=1 Ack=47189 Win=64240 Len=0
192.168.102.252	192.168.101.247	TCP	54 5001 → 63043 [ACK] Seq=1 Ack=49985 Win=64240 Len=0
192.168.102.252	192.168.101.247	TCP	54 5001 → 63043 [ACK] Seq=1 Ack=59771 Win=64240 Len=0
192.168.102.252	192.168.101.247	TCP	54 5001 → 63043 [ACK] Seq=1 Ack=65363 Win=64240 Len=0

Figura 3-25 Captura a la salida del ordenador

En la Figura 3-25, se puede ver como toda la información IP está al descubierto, de forma que si esta información fuese la que saliese del router, un tercer observador podría interferir y decepcionar la información, mientras que en la Figura 3-26, se puede observar cómo no hay información IP de cada dispositivo que transmite, que únicamente sale la IP del router que transmite y la IP del router que recibe, haciendo más difícil la decepción por parte de un tercer dispositivo.

192.168.0.175	192.168.0.134	ESP	1510 ESP (SPI=0x07a2ce3a)
192.168.0.175	192.168.0.134	ESP	1318 ESP (SPI=0x07a2ce3a)
192.168.0.175	192.168.0.134	ESP	1510 ESP (SPI=0x07a2ce3a)
192.168.0.175	192.168.0.134	ESP	1510 ESP (SPI=0x07a2ce3a)
192.168.0.175	192.168.0.134	ESP	1510 ESP (SPI=0x07a2ce3a)
192.168.0.175	192.168.0.134	ESP	1510 ESP (SPI=0x07a2ce3a)
192.168.0.175	192.168.0.134	ESP	1510 ESP (SPI=0x07a2ce3a)
192.168.0.175	192.168.0.134	ESP	1318 ESP (SPI=0x07a2ce3a)
192.168.0.134	192.168.0.175	ESP	118 ESP (SPI=0x0fe539c6)
192.168.0.134	192.168.0.175	ESP	118 ESP (SPI=0x0fe539c6)
192.168.0.134	192.168.0.175	ESP	118 ESP (SPI=0x0fe539c6)
192.168.0.134	192.168.0.175	ESP	118 ESP (SPI=0x0fe539c6)
192.168.0.134	192.168.0.175	ESP	118 ESP (SPI=0x0fe539c6)

Figura 3-26 Captura a la salida del router

Y si a mayores, se accede a la información de cada paquete se puede comprobar como efectivamente, en el paquete de la parte superior de la Figura 3-27, está toda la información IP de los dispositivos conectados, mientras que en el paquete inferior de la misma figura solo aparecen las IPs de los router conectados y toda la información lleva un encapsulamiento de seguridad.

```
Frame 198: 1452 bytes on wire (11616 bits), 1452 bytes captured (11616 bits)
Ethernet II, Src: HewlettP_96:f8:ea (f4:30:b9:96:f8:ea), Dst: Routerbo_79:2e:5e (cc:2d:e0:79:2e:5e)
Internet Protocol Version 4, Src: 192.168.101.247, Dst: 192.168.102.252
Transmission Control Protocol, Src Port: 63043, Dst Port: 5001, Seq: 59771, Ack: 1, Len: 1398
Data (1398 bytes)

Frame 240: 1510 bytes on wire (12080 bits), 1510 bytes captured (12080 bits)
Ethernet II, Src: Routerbo_79:2e:5d (cc:2d:e0:79:2e:5d), Dst: Routerbo_79:2d:ed (cc:2d:e0:79:2d:ec)
Internet Protocol Version 4, Src: 192.168.0.175, Dst: 192.168.0.134
Encapsulating Security Payload
  ESP SPI: 0x07a2ce3a (128110138)
  ESP Sequence: 311653
```

Figura 3-27 Paquete de información a la salida del ordenador (arriba) y a la salida del router (abajo)

4 RESULTADOS Y PRUEBAS

En este apartado se van a presentar y analizar los resultados obtenidos durante todo el proceso. Estos resultados son las tasas de transferencia de los distintos dispositivos, obtenidas mediante el programa Jperf. Estas tasas se han medido utilizando 5 conexiones, para intentar aprovechar todo el canal y no tener pérdidas por tiempos muertos, y con un tiempo de transmisión de 30s.

4.1 VPN con OpenVPN

4.1.1 Tasa de transferencia con el teléfono móvil

En este subapartado cabe destacar que la conexión con el teléfono móvil a la VPN ha sido en todo momento inalámbrica.

En la Figura 4-1 se observa la tasa de transferencia del móvil sin el uso de la VPN, la cual tiene de media cerca de los 19000 kbps, lo cual sería suficiente para transferencia de video de alta definición.

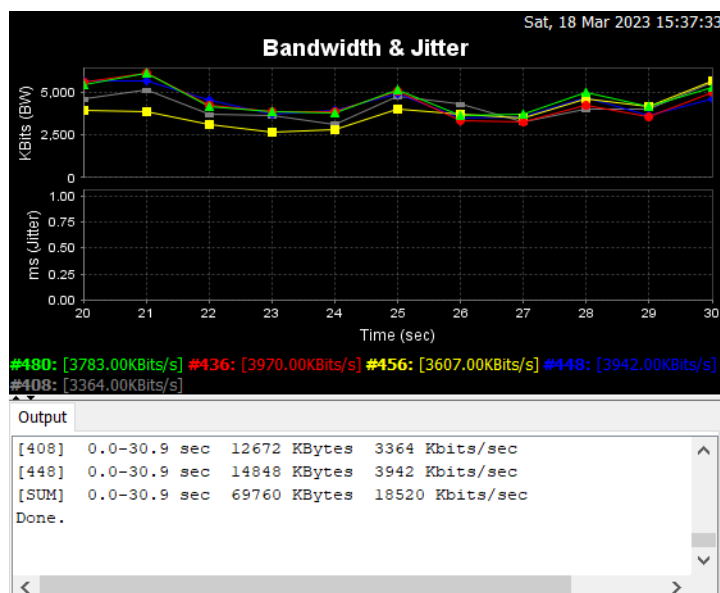


Figura 4-1 Tasa del móvil sin VPN

Al igual que en el caso anterior, en la Figura 4-2, la cual es la tasa de transferencia del dispositivo móvil con la VPN conectada. Se puede apreciar que la tasa de transferencia se mantiene, quedando esta sobre los 18000 kbps, por lo cual no tendría ningún impedimento para la transferencia de video en alta definición de hasta 4K a 30fps.

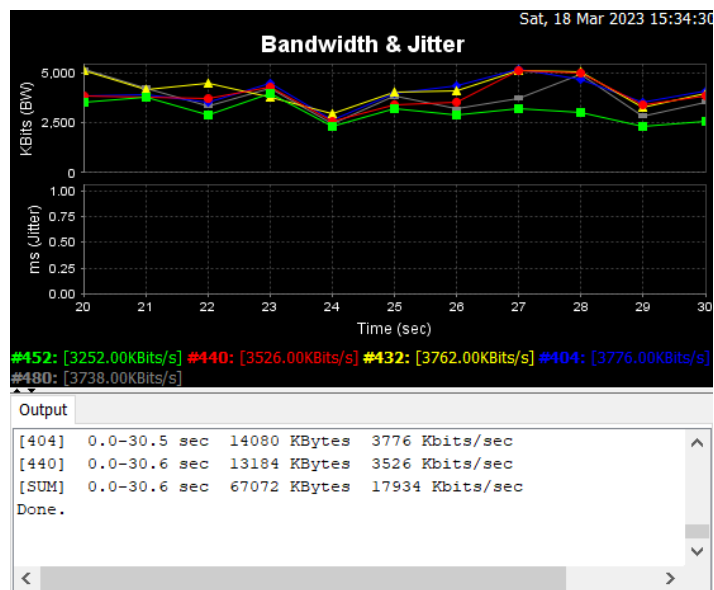


Figura 4-2 Tasa del móvil con AES 128

Como se puede observar no varía mucho la tasa de transferencia al emplear el cifrado, por lo que se comprueba que actualmente la capacidad de cifrado de un teléfono móvil es considerable y, en principio, no va a suponer ningún problema en cuanto a transmisión de datos se refiere. En la Figura 4-3 se puede observar la tasa de transferencia con AES 192, que disminuye ligeramente hasta los casi 16000 kbps, pero no llega a ser significativo. Y aunque el cómputo global es bueno, en la gráfica se pueden observar varios cortes de señal, llegando está a 0, lo cual se puede deber a desvanecimientos de señal.

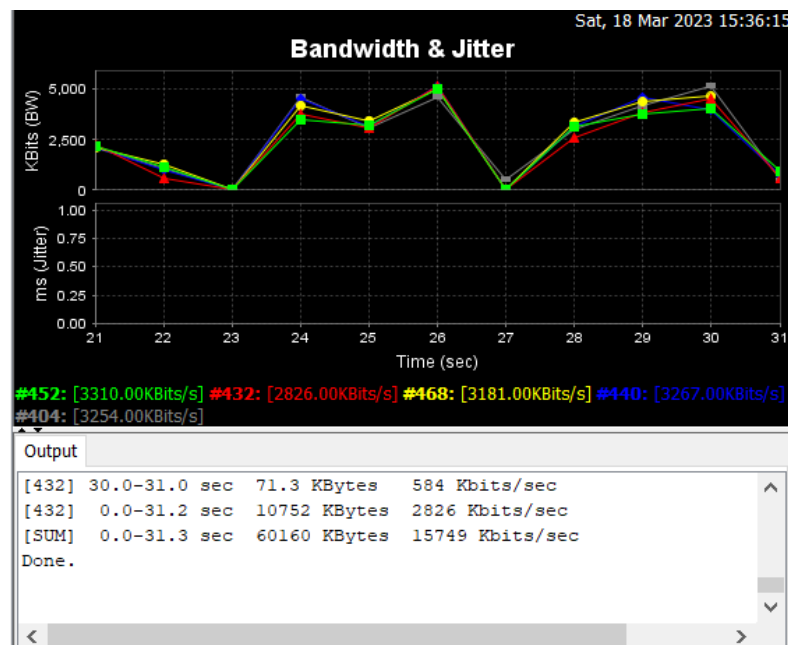


Figura 4-3 Tasa del móvil con AES 192

Cuando se establece AES 256 como algoritmo de cifrado, la tasa de transferencia sigue siendo de unos 15000kbps, siendo este el algoritmo de cifrado más complejo utilizado, permitiendo reproducir en streaming en HD sin problema alguno. Al igual que en el caso anterior, se pueden observar desvanecimientos de señal (véase la Figura 4-4).

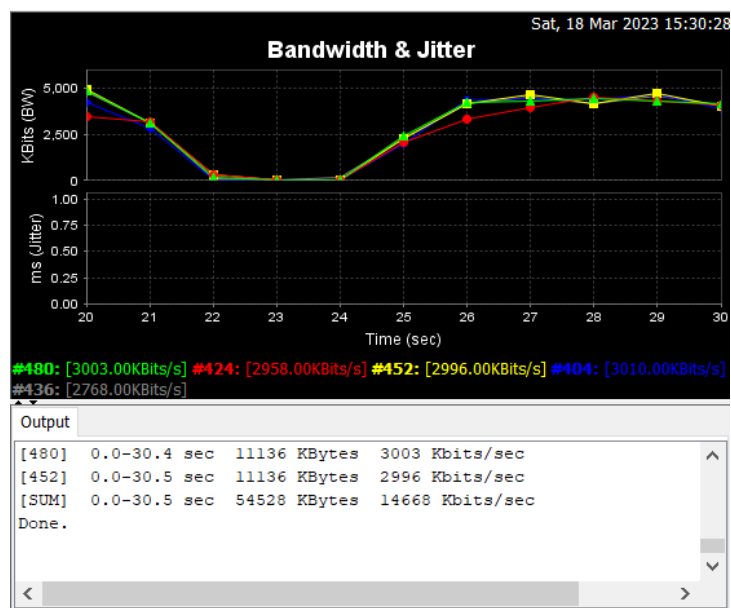


Figura 4-4 Tasa del móvil con AES 256

Como prueba se ha decidido utilizar un segundo algoritmo de cifrado, no seguro, ya que está en desuso para comprobar su rendimiento. En la Figura 4-5 se puede observar la tasa de transferencia del móvil con Blowfish 128, y se comprueba que esta se sigue manteniendo a unos 17000 kbps de media, aunque sigue habiendo esos cortes de señal.

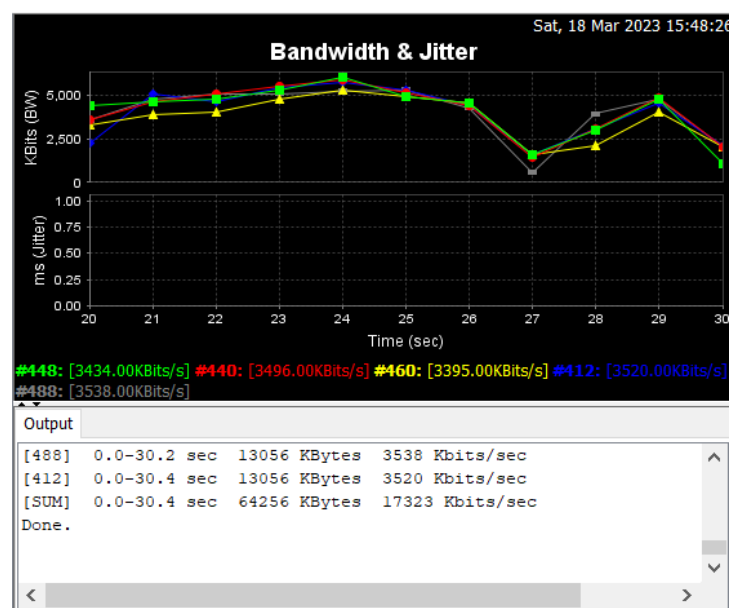


Figura 4-5 Tasa del móvil con Blowfish 128

4.1.2 Tasa de transferencia con el ordenador

En este apartado se va a probar las capacidades del ordenador con y sin conexión VPN, al igual que con el teléfono móvil. La primera prueba es la tasa de transferencia del ordenador sin conexión a VPN. Hay que destacar que esta conexión ya es mediante cable de Ethernet conectado al router.

Se puede ver en la Figura 4-6 como la tasa del ordenador es de unos 25000 kbps, que basándose en lo mencionado en el apartado 2.3.1, es suficiente para transmitir a 4K. Y, como se puede observar en la gráfica, ya no se aprecian cortes en la tasa.

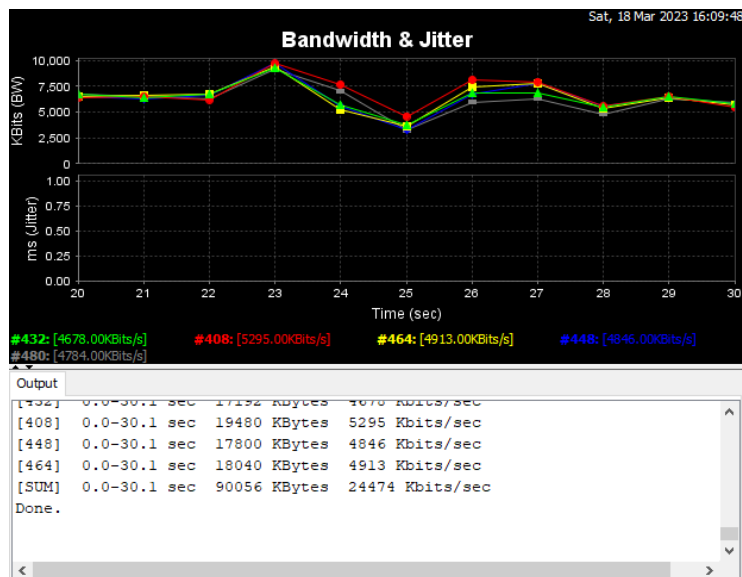


Figura 4-6 Tasa del ordenador sin VPN

La Figura 4-7 muestra la tasa de transferencia utilizando el cifrado AES 128, que se mantiene estable a 23500 kbps, que sigue siendo una tasa suficientemente alta como para transmitir video en 4K. se puede observar en la gráfica que se mantiene estable sin tener cortes en la tasa.



Figura 4-7 Tasa del ordenador con AES 128

En la Figura 4-8 se puede comprobar como la tasa de transferencia del ordenador cifrando el enlace con AES 192, cae a 14000 kbps, aunque sigue siendo suficiente como para reproducir streaming de video en alta definición. De nuevo en esta gráfica se aprecias caídas en la tasa de transferencia.

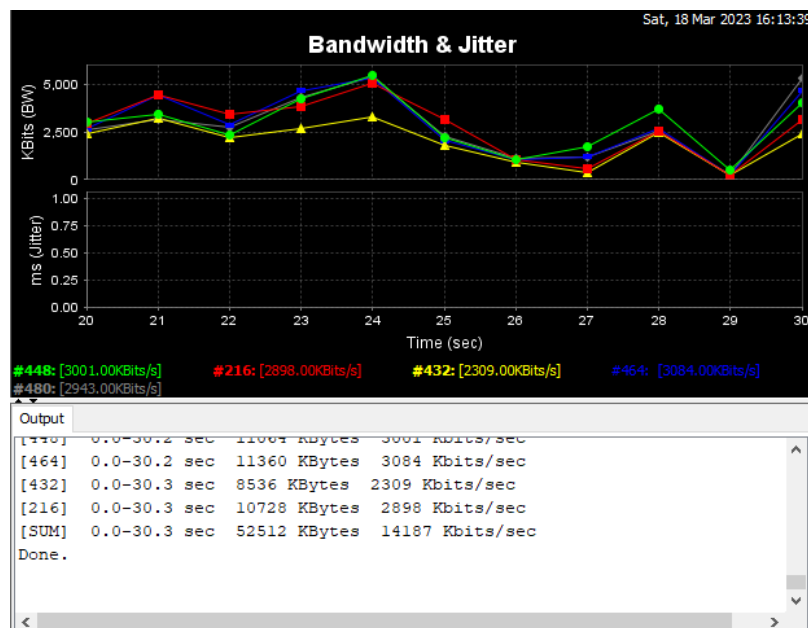


Figura 4-8 Tasa del ordenador con AES 192

Sin embargo, en la Figura 4-9 la tasa de transferencia vuelve a aumentar hasta los casi 19000 kbps utilizando AES 256 para cifrar el enlace, por lo que se puede afirmar que con el algoritmo de cifrado más robusto disponible se puede transmitir video en streaming en alta definición sin problema. Al igual que en el caso anterior se pueden observar ciertos cortes en la tasa.

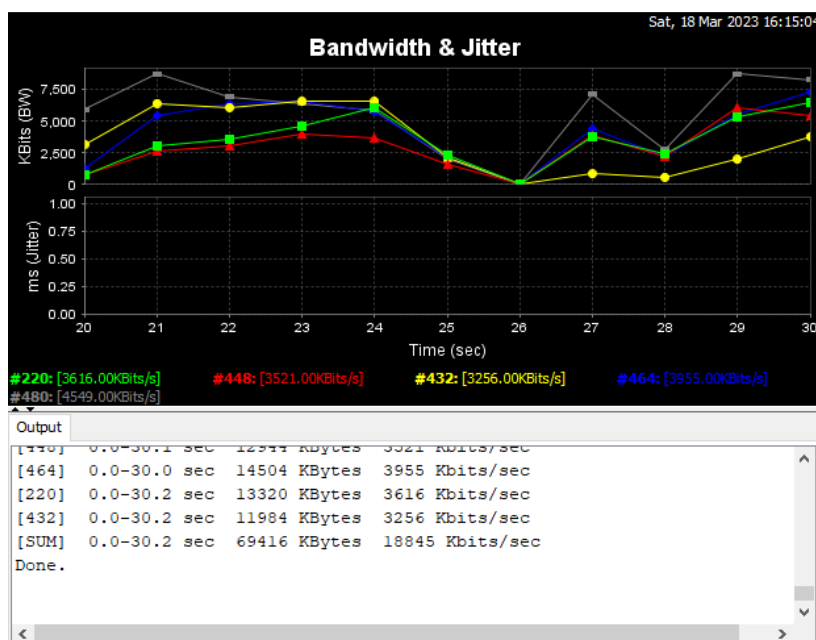


Figura 4-9 Tasa del ordenador con AES 256

Por último, y como comprobación al igual que con el dispositivo móvil, se ha aplicado el algoritmo Blowfish 128 para cifrar el enlace. Tal y como se puede observar en la Figura 4-10, la tasa utilizando este algoritmo es de 21500 kbps, aunque como ya se ha mencionado, este es un algoritmo en desuso. En esta gráfica se puede apreciar cómo no hay flujo irregular en la tasa, manteniéndose relativamente estable.

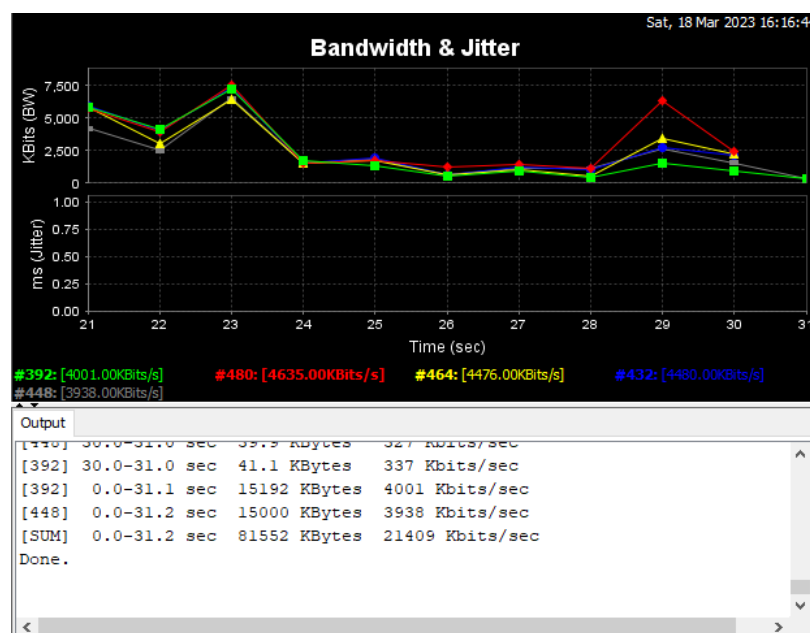


Figura 4-10 Tasa del ordenador con Blowfish 128

4.2 Comprobación túnel IPsec

En este apartado se va a comprobar y evaluar la capacidad de transferencia entre dos Raspberry Pi, tras haberlas conectado mediante SSH, estableciendo un túnel IPsec entre los routers. Como se ha hablado en el apartado 3.3.1 las IPs internas de ambos dispositivos quedan ocultas tras las IPs de los routers, por lo que nadie es capaz de saber a qué dispositivo va dirigido el mensaje, ni desde que dispositivo se ha enviado.

```
Frame 240: 1510 bytes on wire (12080 bits), 1510 bytes captured (12080 bits)
Ethernet II, Src: Routerbo_79:2e:5d (cc:2d:e0:79:2e:5d), Dst: Routerbo_79:2d:ed (cc:2d:e0:79:2d:ed)
Internet Protocol Version 4, Src: 192.168.0.175, Dst: 192.168.0.134
Encapsulating Security Payload
  ESP SPI: 0x07a2ce3a (128110138)
  ESP Sequence: 311653
```

Figura 4-11 Captura Wireshark con IPsec

Tal y como se muestra en la Figura 4-11 (obtenida usando la opción del “Pack Sniffer” del router Mikrotik) toda la información, tanto del paquete como de la cabecera IP interna va cifrada. Y a esta información se le va a aportar una capa de protección más, que va a ser el protocolo SSH. Con el objetivo de poder controlar un dispositivo desde otro en otra red, se va a establecer un túnel SSH entre ambas Raspberries, con la comprobación final de poder ejecutar un programa instalado en una Raspberry desde la otra, que no la va a tener instalada.

Ahora se va a realizar un ping desde cada dispositivo atravesando las distintas interfaces para comprobar que efectivamente se ven ambos dispositivos. Primero se va a comprobar que cada Raspberry tiene conexión con la interfaz a la que está conectada.

Como se puede observar en la Figura 4-12, cada Raspberry tiene conexión sin mayor problema a la interfaz de conexión. En esa figura se puede ver también las IPs que se les han asignados a los dispositivos.

```

adri@raspberrypi1:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.102.250 netmask 255.255.255.0 broadcast 192.168.102.255
    inet6 fe80::8bb5:4f36:7c1c:57ad prefixlen 64 scopeid 0x20<link>
    ether b8:27:eb:f9:0a:97 txqueuelen 1000 (Ethernet)
    RX packets 98 bytes 6976 (6.8 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 131 bytes 13922 (13.5 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 1000 (Local Loopback)
    RX packets 18 bytes 2160 (2.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 18 bytes 2160 (2.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

adri@raspberrypi1:~$ ping 192.168.102.1
PING 192.168.102.1 (192.168.102.1) 56(84) bytes of data.
64 bytes from 192.168.102.1: icmp_seq=1 ttl=64 time=0.556 ms
64 bytes from 192.168.102.1: icmp_seq=2 ttl=64 time=0.478 ms
64 bytes from 192.168.102.1: icmp_seq=3 ttl=64 time=0.542 ms

```

```

adri@raspberrypi:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.101.243 netmask 255.255.255.0 broadcast 192.168.101.255
    inet6 fe80::274b:9372:8054:a725 prefixlen 64 scopeid 0x20<link>
    ether b8:27:eb:db:33:17 txqueuelen 1000 (Ethernet)
    RX packets 603 bytes 49912 (48.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 695 bytes 69633 (68.0 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 1000 (Local Loopback)
    RX packets 22 bytes 2452 (2.3 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 22 bytes 2452 (2.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

adri@raspberrypi:~$ ping 192.168.101.1
PING 192.168.101.1 (192.168.101.1) 56(84) bytes of data.
64 bytes from 192.168.101.1: icmp_seq=1 ttl=64 time=0.562 ms
64 bytes from 192.168.101.1: icmp_seq=2 ttl=64 time=0.467 ms
64 bytes from 192.168.101.1: icmp_seq=3 ttl=64 time=0.407 ms

```

Figura 4-12 Conexión con el puerto de conexión Raspberry 1 (derecha) y Raspberry 2 (izquierda)

A continuación, se va a proceder a comprobar que cada dispositivo puede conectarse con el router al cual están conectados. Y como se puede comprobar en la Figura 4-13, los dispositivos pueden alcanzar el router al que están conectados sin problema.

```

adri@raspberrypi1:~$ ping 192.168.0.134
PING 192.168.0.134 (192.168.0.134) 56(84) bytes of data.
64 bytes from 192.168.0.134: icmp_seq=1 ttl=64 time=0.596 ms
64 bytes from 192.168.0.134: icmp_seq=2 ttl=64 time=0.504 ms
64 bytes from 192.168.0.134: icmp_seq=3 ttl=64 time=0.501 ms
64 bytes from 192.168.0.134: icmp_seq=4 ttl=64 time=0.485 ms
64 bytes from 192.168.0.134: icmp_seq=5 ttl=64 time=0.494 ms
64 bytes from 192.168.0.134: icmp_seq=6 ttl=64 time=0.493 ms
^C
--- 192.168.0.134 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5233ms

```

```

adri@raspberrypi:~$ ping 192.168.0.175
PING 192.168.0.175 (192.168.0.175) 56(84) bytes of data.
64 bytes from 192.168.0.175: icmp_seq=1 ttl=64 time=0.575 ms
64 bytes from 192.168.0.175: icmp_seq=2 ttl=64 time=0.422 ms
64 bytes from 192.168.0.175: icmp_seq=3 ttl=64 time=0.462 ms
64 bytes from 192.168.0.175: icmp_seq=4 ttl=64 time=0.470 ms
64 bytes from 192.168.0.175: icmp_seq=5 ttl=64 time=0.477 ms
^C
--- 192.168.0.175 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4196ms
rtt min/avg/max/mdev = 0.422/0.481/0.575/0.050 ms

```

Figura 4-13 Conexión con el router de conexión Raspberry 1 (derecha) y Raspberry 2 (izquierda)

Ahora se va a proceder a comprobar la conexión entre los dispositivos y el router de la otra red, de forma que se pueda comprobar si la conexión está llegando a la otra red, o por problemas con las IPs se hayan podido perder paquetes. Y tal y como se puede observar en la siguiente figura (Figura 4-14) esta conexión se establece sin problema.

```

adri@raspberrypi1:~$ ping 192.168.0.175
PING 192.168.0.175 (192.168.0.175) 56(84) bytes of data.
64 bytes from 192.168.0.175: icmp_seq=1 ttl=63 time=0.763 ms
64 bytes from 192.168.0.175: icmp_seq=2 ttl=63 time=0.514 ms
64 bytes from 192.168.0.175: icmp_seq=3 ttl=63 time=0.612 ms
64 bytes from 192.168.0.175: icmp_seq=4 ttl=63 time=0.623 ms
64 bytes from 192.168.0.175: icmp_seq=5 ttl=63 time=0.598 ms
64 bytes from 192.168.0.175: icmp_seq=6 ttl=63 time=0.606 ms
^C
--- 192.168.0.175 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5186ms
rtt min/avg/max/mdev = 0.514/0.619/0.763/0.073 ms

```

```

adri@raspberrypi:~$ ping 192.168.0.134
PING 192.168.0.134 (192.168.0.134) 56(84) bytes of data.
64 bytes from 192.168.0.134: icmp_seq=1 ttl=63 time=0.782 ms
64 bytes from 192.168.0.134: icmp_seq=2 ttl=63 time=0.593 ms
64 bytes from 192.168.0.134: icmp_seq=3 ttl=63 time=0.654 ms
64 bytes from 192.168.0.134: icmp_seq=4 ttl=63 time=0.561 ms
64 bytes from 192.168.0.134: icmp_seq=5 ttl=63 time=0.634 ms
^C
--- 192.168.0.134 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4116ms
rtt min/avg/max/mdev = 0.561/0.644/0.782/0.075 ms

```

Figura 4-14 Conexión con el router de otra red Raspberry 1 (derecha) y Raspberry 2 (izquierda)

Y la última comprobación es saber si ambos dispositivos se alcanzan entre sí, en caso afirmativo se podría decir que el túnel IPsec se ha establecido sin problema. Además, esta conexión nos va a permitir, mediante SSH (protocolo ya mencionado anteriormente), tomar el control de un dispositivo desde el otro y poder trabajar en remoto.

```

adri@raspberrypi1:~$ ping 192.168.101.243
PING 192.168.101.243 (192.168.101.243) 56(84) bytes of data.
64 bytes from 192.168.101.243: icmp_seq=1 ttl=62 time=1.66 ms
64 bytes from 192.168.101.243: icmp_seq=2 ttl=62 time=1.36 ms
64 bytes from 192.168.101.243: icmp_seq=3 ttl=62 time=1.30 ms
64 bytes from 192.168.101.243: icmp_seq=4 ttl=62 time=1.37 ms
64 bytes from 192.168.101.243: icmp_seq=5 ttl=62 time=1.32 ms
64 bytes from 192.168.101.243: icmp_seq=6 ttl=62 time=1.29 ms
^C
--- 192.168.101.243 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5008ms
rtt min/avg/max/mdev = 1.287/1.382/1.662/0.128 ms

```

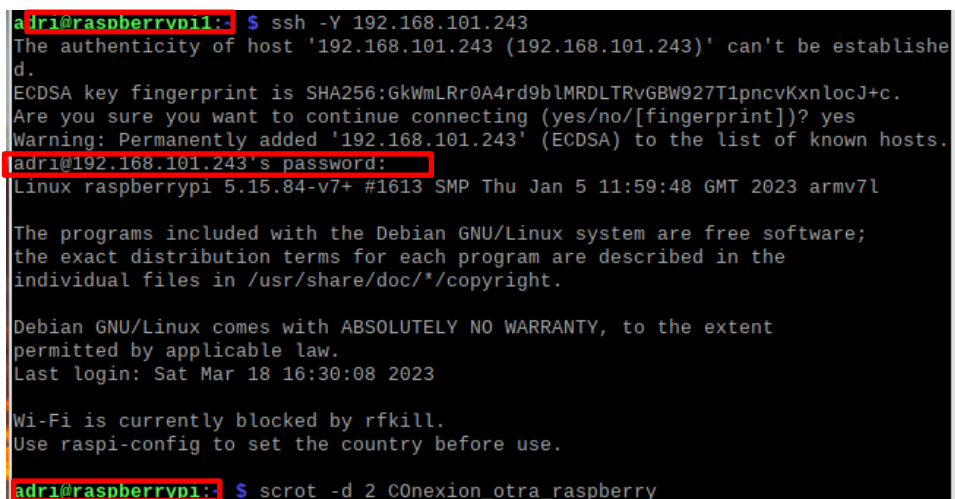
```

adri@raspberrypi:~$ ping 192.168.102.250
PING 192.168.102.250 (192.168.102.250) 56(84) bytes of data.
64 bytes from 192.168.102.250: icmp_seq=1 ttl=62 time=1.55 ms
64 bytes from 192.168.102.250: icmp_seq=2 ttl=62 time=1.25 ms
64 bytes from 192.168.102.250: icmp_seq=3 ttl=62 time=1.36 ms
64 bytes from 192.168.102.250: icmp_seq=4 ttl=62 time=1.30 ms
64 bytes from 192.168.102.250: icmp_seq=5 ttl=62 time=1.39 ms
^C
--- 192.168.102.250 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.251/1.369/1.550/0.101 ms

```

Figura 4-15 Conexión con el otro dispositivo. Raspberry 1 (derecha) y Raspberry 2 (izquierda)

Y tal y como se puede observar en la Figura 4-15, ambas Raspberries son capaces de verse sin problema. Ahora, tal y como se ha dicho, se va a proceder a establecer un túnel SSH, lo que va a aportar una capa de seguridad a mayores. Para esto, y debido a que se está trabajando con sistemas operativos basados en Raspbian, se va a operar desde el terminal. Para poder conectarse se tiene que utilizar el comando “ssh -Y 192.168.101.243” donde los números indican la dirección IP del destino.



```
adri@raspberrypi1:~$ ssh -Y 192.168.101.243
The authenticity of host '192.168.101.243 (192.168.101.243)' can't be established.
ECDSA key fingerprint is SHA256:GkWmLRr0A4rd9bLMRDLTRvGBW927T1pncvKxnlocJ+c.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.101.243' (ECDSA) to the list of known hosts.
adri@192.168.101.243's password:
Linux raspberrypi 5.15.84-v7+ #1613 SMP Thu Jan 5 11:59:48 GMT 2023 armv7l

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Mar 18 16:30:08 2023

Wi-Fi is currently blocked by rfkill.
Use raspi-config to set the country before use.

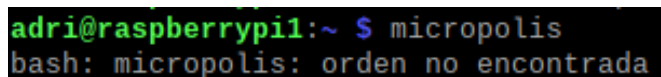
adri@raspberrypi1:~$ scrot -d 2 C0nexion_otra_raspberry
```

Figura 4-16 Túnel SSH

Como se puede ver en la Figura 4-16, el terminal pide introducir la contraseña del dispositivo destino y, tras esto, como se puede comprobar por el nombre del dispositivo, ya se estaría controlando de manera efectiva.

Por último, se va a comprobar si se pueden abrir aplicaciones desde el dispositivo que se está controlando. Para ello se ha instalado un juego llamado “Micropolis” en uno de los dispositivos y esta es la aplicación que se va a intentar abrir desde el dispositivo que no la tiene instalada.

Para ello, y como comprobación, se puede observar en la Figura 4-17 que la denominada “Raspberry 1” no tiene la aplicación instalada



```
adri@raspberrypi1:~$ micropolis
bash: micropolis: orden no encontrada
```

Figura 4-17 Comprobación Raspberry 1

Tras esta comprobación y tras establecer el túnel se vuelve a ejecutar este comando en la “Raspberry 1” y se puede comprobar como la aplicación se puede ejecutar (Figura 4-18). Cabe destacar que se nota cierto retardo en la aplicación a la hora de trabajar sobre ella. Esto se puede deber a un problema de capacidades de la Raspberry, ya que es un dispositivo barato, el cual utiliza una tarjeta SD como método de almacenamiento de memoria, tanto datos del dispositivo, así como almacenamiento del sistema operativo. Además, como se ha dicho en el apartado 3.1.4, es un dispositivo que no dispone de instrucciones internas de cifrado de ningún tipo

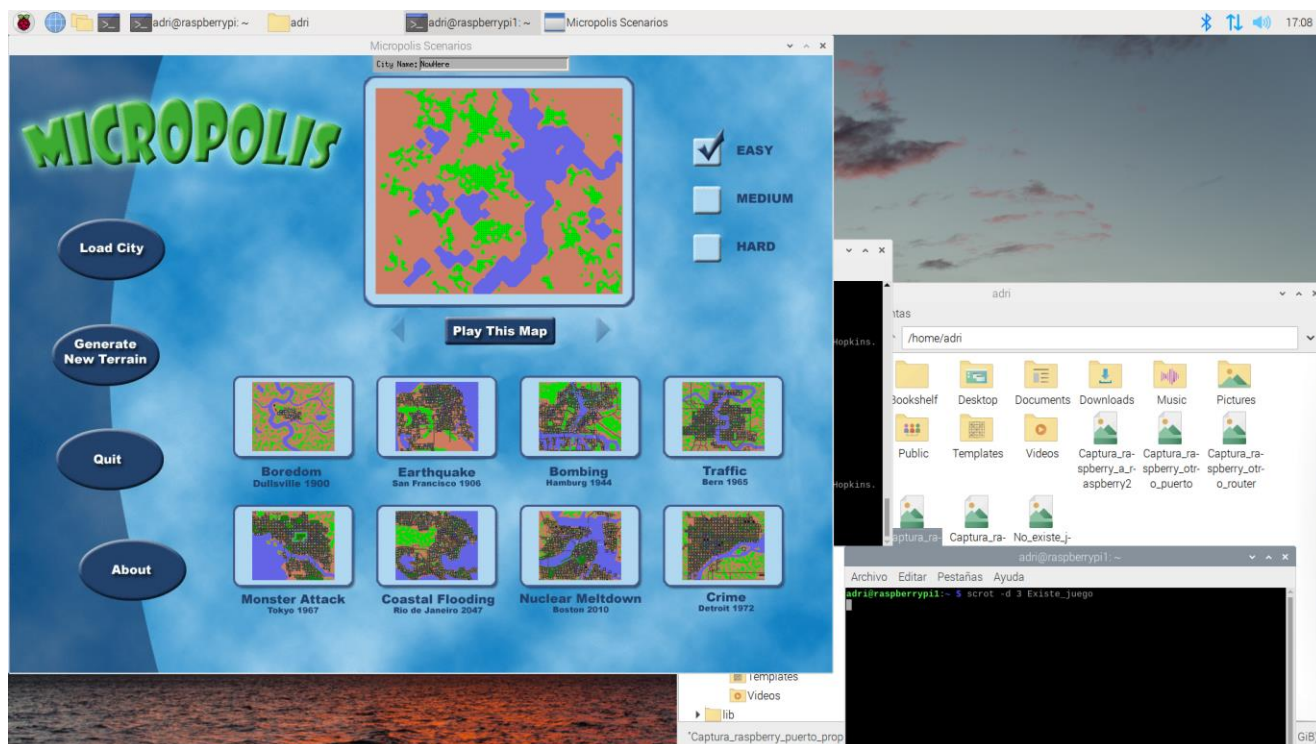


Figura 4-18 Ejecución de la aplicación en la Raspberry 1 tras tunneling

También se ha utilizado el programa Jperf para medir la tasa de ambos dispositivos con y sin túnel SSH. En la Figura 4-19 se puede observar como la tasa de transmisión es de 82500 kbps aproximadamente. Y una vez establecido el túnel, la tasa de transferencia ha disminuido hasta los 72000 kbps, siendo el decremento de cerca de 5000 kbps

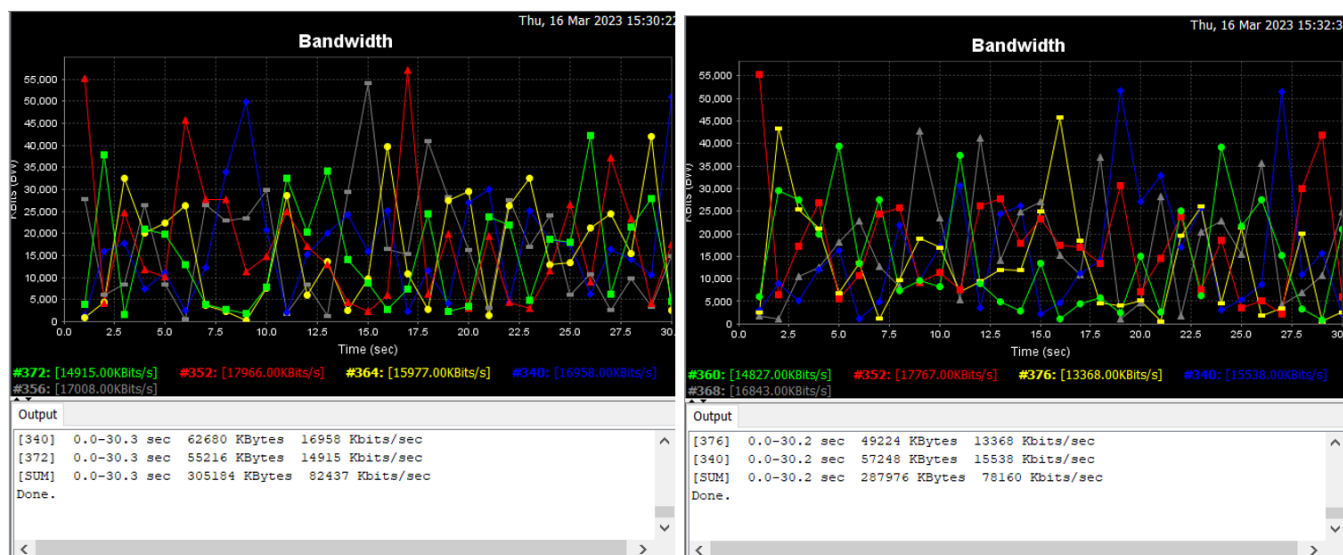


Figura 4-19 Raspberry sin túnel SSH (izquierda) y con túnel SSH (derecha)

Para comprobar esta teoría, se va a proceder a controlar la Raspberry desde un ordenador con sistema Windows instalado. Y para esto es necesario la instalación del programa “PuTTY” en el dispositivo Windows únicamente. Tras haber instalado dicha aplicación y haber realizado las comprobaciones de conexión realizadas para conectar ambas Raspberries.

Tras estas comprobaciones ejecutamos el programa PuTTY, cuya interfaz se explicó en el apartado 2, y se conectan los dos dispositivos.

De esta forma se puede comprobar como el cuello de botella en la transferencia de información es la Raspberry y sus limitadas capacidades debidas a su bajo coste, porque al conectar un ordenador más potente las tasas de transferencia aumentan hasta los 850Mb. (Figura 4-20)

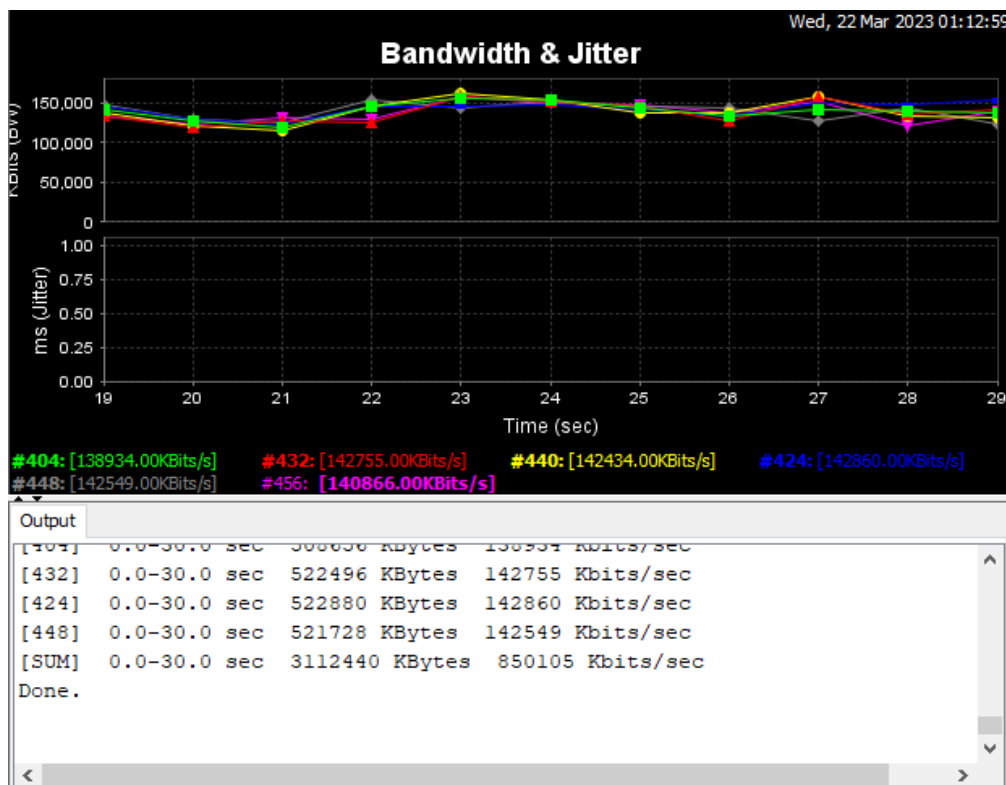


Figura 4-20 Tasa de transferencia con Windows

Cabe destacar que a pesar de la gran tasa de transferencia que tiene el dispositivo Windows, se sigue notando retardo a la hora de ejecutar la aplicación.

4.3 Resultados

Como se puede observar en la Figura 4-21, en general el ordenador tiene bastante mejor tasa de transmisión que el teléfono móvil (referido a la creación de la VPN con OpenVPN). Esto se puede deber a que debido el bajo coste de los routers Mikrotik que se están utilizando la conexión WiFi es el cuello de botella en las transmisiones inalámbricas. Esto se aprecia en los desvanecimientos de red que se observan en la mayoría de las gráficas de tasas de transmisión del teléfono móvil.

En cuanto a las conexiones de ordenador, también se pueden observar ciertos desvanecimientos de red en alguna de las gráficas, lo que se puede atribuir a la capacidad de los routers en cuanto a cifrado se refiere.

De esta forma se puede concluir que el cuello de botella en el caso de las VPN con distintos cifrados ha sido el router debido a sus características, ya que todos los dispositivos tenían instrucciones internas de cifrado AES, es decir, tenían aceleración por hardware.

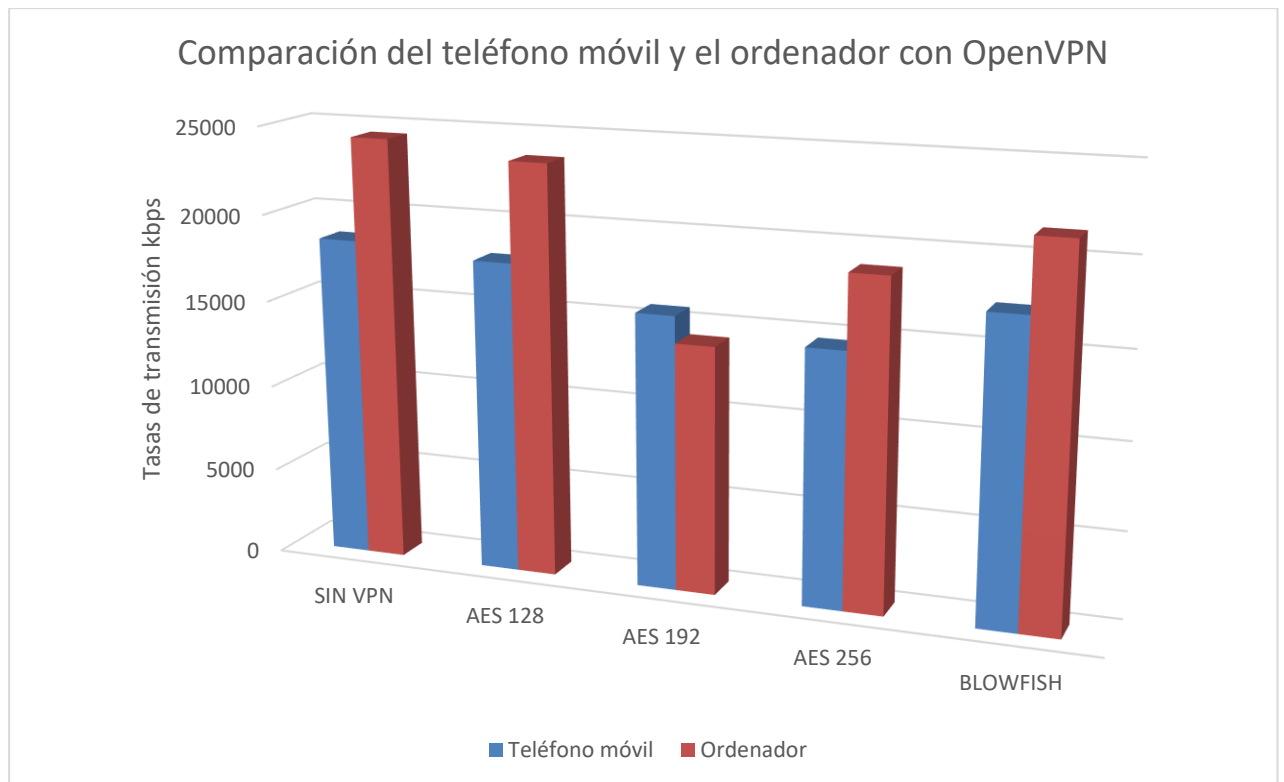


Figura 4-21 Gráfico tasas de transmisión teléfono móvil y ordenador

En cuanto al túnel IPsec con SSH, y a la vista de los resultados, el ordenador es capaz de transmitir una tasa bastante elevada, por lo que, si tenemos en cuenta los resultados de la maqueta anterior, uno de los cuellos de botella vuelve a ser la capacidad de cifrado del router. Y el otro es la poca capacidad de la Raspberry, algo totalmente entendible, debido al bajo coste de este. Las tasas de transferencia de estos dispositivos se encuentran graficados en la Figura 4-22.

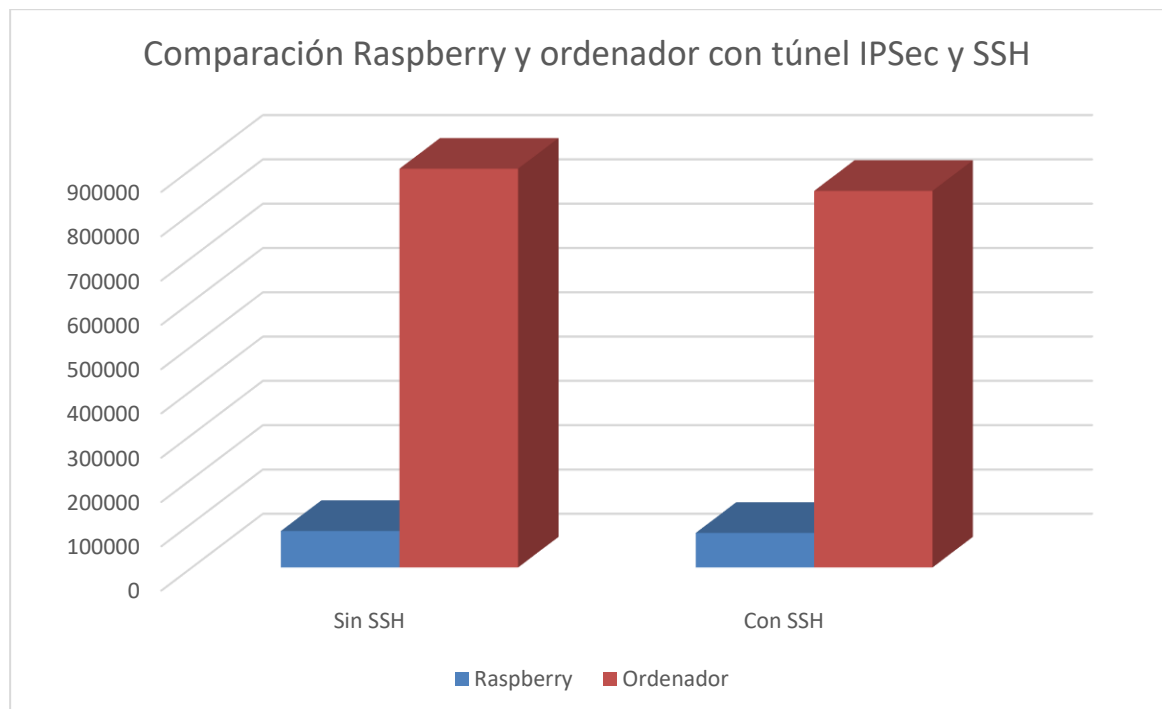


Figura 4-22 Gráfico tasas de transmisión Raspberry y ordenador

Resumiendo los dos resultados anteriores, el mayor problema a la hora de la transmisión de datos en ambos casos ha sido, probablemente, la capacidad de cifrado del router, ya que, como se ha mencionado, es un dispositivo de bajo coste para la función que realiza. Aun así, en todos los casos permite la transmisión de video en streaming de alta calidad, ya que como se expuso en el apartado 2.3.1, las tasas de transferencia para el mismo se cumplen.

5 CONCLUSIONES Y LÍNEAS FUTURAS

En este apartado se van a detallar las conclusiones sacadas del trabajo, así como, la consecución de los distintos objetivos establecidos para el mismo. Posteriormente se analizarán las posibles líneas futuras del trabajo, con el objetivo de poder continuarlo en los años venideros

5.1 Conclusiones

Ha quedado demostrado que se puede transmitir video de alta calidad de streaming a pesar de usar dispositivos de bajo coste, por lo que la implantación de VPN a nivel usuario puede estar a disposición de gran parte de la población haciendo que la navegación a través de la red sea más segura para todo el mundo.

Además, el túnel de IPSec con SSH es una muy buena forma de teletrabajar, debido a que el túnel es completamente seguro. Si a esta característica se le suma el uso de dispositivos repartidos por la empresa con el único propósito de trabajar, se tendría una gran herramienta que permitiría solucionar cualquier problema desde cualquier parte del mundo con el solo hecho de tener acceso a una red y a un dispositivo.

En el ámbito militar, la implantación de un túnel de estas características podría ser una buena solución para la consulta y utilización de material clasificado en caso de emergencia, siempre y cuando el dispositivo haya pasado el proceso de seguridad que exige el Ministerio de Defensa.

En cuanto a la consecución de objetivo, en el apartado 1.2 se establecieron varios objetivos a cumplir durante la realización del trabajo. Ahora se va a analizar cada uno y se va a especificar el grado de consecución de cada uno:

- El primero de los objetivos era entender la arquitectura de internet y los distintos protocolos de cifrado. Este objetivo si se ha cumplido ya que en el apartado 2 se ha hablado de la arquitectura de internet, así como de una variedad de los protocolos de cifrado más utilizados a día en hoy. También incluía todo lo relativo al concepto de VPN, tipos y protocolos de seguridad. Este objetivo se puede considerar que también se ha cumplido debido a que en los subapartados 2.3 y 2.4.3 se han explicado estos conceptos, con ciertas aclaraciones gráficas en el caso de los tipos de VPN.
- El segundo objetivo era alcanzar la solución, previsiblemente, también se ha cumplido, debido a que utilizando los routers Mikrotik y un teléfono móvil relativamente barato para la situación actual se ha conseguido alcanzar tasas elevadas que permiten la transmisión de video de alta calidad.
- En cuanto al objetivo de acceder a una LAN mediante el uso de una VPN, se ha llegado a crear, desplegar y evaluar dicha red, lo cual está íntimamente ligado con el objetivo anterior.
- En lo relativo a crear un túnel IPSec y controlar mediante SSH, ha sido el objetivo más difícil de conseguir debido a diversos problemas con la asignación de IPs. Pero finalmente se ha llegado a conseguir siendo, un auténtico éxito, llegando, no solo a poder crear, modificar y editar archivos, si no también, llegar a controlar una aplicación, como es un juego, de forma remota.
- Y el último objetivo era la evaluación de las distintas maquetas creadas viendo cual es la mejor configuración, y se ha llegado a evaluar, pero no se puede establecer una configuración optima, debido a que el “cuello de botella” ha estado en los dispositivos utilizados y su capacidad.

5.2 Líneas futuras

En cuanto a posibles futuros trabajos, se podría reevaluar esta situación utilizando distintos dispositivos, tanto routers como ordenadores o dispositivos móviles. De esta forma se podría comprobar si, subiendo un poco el precio de los componentes, se podrían mejorar las prestaciones.

Otra posible línea, sería continuar este trabajo, pero usando distintos protocolos, intentando conseguir resultados parecidos o mejores con otros protocolos de seguridad como podría ser el MPPE o cualquiera de los no descritos, así como cambiar la aplicación OpenVPN por OpenSSH, de forma que se haga la misma función, pero trabajando sobre SSH en lugar de trabajar sobre TLS.

También se podría cambiar los cifrados utilizados, buscando funciones más actuales, como podría ser AES 512 o Twofish (ya mencionado en este trabajo) en lugar de Blowfish.

6 BIBLIOGRAFÍA

- [1] «DARPA.pdf». Accedido: 17 de enero de 2023. [En línea]. Disponible en: <https://apps.dtic.mil/sti/pdfs/ADA115440.pdf>
- [2] «The HTTP Protocol As Implemented In W3». <https://www.w3.org/Protocols/HTTP/AsImplemented.html> (accedido 9 de febrero de 2023).
- [3] «Usage Statistics of Default protocol https for Websites, February 2023». <https://w3techs.com/technologies/details/ce-httpsdefault> (accedido 9 de febrero de 2023).
- [4] H. Wu, X. Dang, L. Wang, y L. He, «Information fusion-based method for distributed domain name system cache poisoning attack detection and identification», *IET Inf. Secur.*, vol. 10, n.º 1, pp. 37-44, 2016, doi: 10.1049/iet-ifs.2014.0386.
- [5] «Domain names - concepts and facilities», Internet Engineering Task Force, Request for Comments RFC 1034, nov. 1987. doi: 10.17487/RFC1034.
- [6] D. Atkins y R. Austein, «Threat Analysis of the Domain Name System (DNS)», Internet Engineering Task Force, Request for Comments RFC 3833, ago. 2004. doi: 10.17487/RFC3833.
- [7] «El modelo OSI». http://dis.um.es/~lopezquesada/documentos/IES_1213/LMSGI/curso/xhtml/xhtml22/index.html (accedido 17 de enero de 2023).
- [8] «MODELOS TCP/IP - TIPOS DE MODELOS». <https://sites.google.com/site/tiposdemodelos/modelos-tcp-ip> (accedido 17 de enero de 2023).
- [9] «PANs, LANs, MANs, WANs? | Security Info Watch». <https://www.securityinfowatch.com/video-surveillance/blog/10475171/pans-lans-mans-wans> (accedido 19 de enero de 2023).
- [10] J. Dong, *Network Protocols Handbook*. Javvin Press, 2007. [En línea]. Disponible en: <https://books.google.es/books?id=PLGXGQAACAAJ>
- [11] «Wireless Networking - History of Wireless», 10 de febrero de 2007. <https://web.archive.org/web/20070210131824/http://www.jhsph.edu/wireless/history.html> (accedido 20 de marzo de 2023).
- [12] J. F. Hernández y J. L. A. Berrocal, «Departamento de Informática y Automática Universidad de Salamanca».
- [13] «Elegir la configuración del codificador, tasas de bits y resoluciones para emisiones en directo - Ayuda de YouTube». <https://support.google.com/youtube/answer/2853702?hl=es#zippy=%2Ckp-a-fps%2Cp-a-fps%2Cp> (accedido 9 de marzo de 2023).
- [14] Z. Yakova, *A New Virtual Private Networks Access Model*. 2013.
- [15] «What Is a Site-to-Site VPN?», *Palo Alto Networks*. <https://www.paloaltonetworks.com/cyberpedia/what-is-a-site-to-site-vpn> (accedido 23 de enero de 2023).

- [16] «La VPN crea una conexión privada y segura entre muchas personas y dispositivos a través de Internet», *Inversor Latam*. <https://inversorlatam.com/la-vpn-crea-una-conexion-privada-y-segura-entre-muchas-personas-y-dispositivos-a-traves-de-internet/> (accedido 30 de enero de 2023).
- [17] «Encryption», *Wikipedia*. 3 de febrero de 2023. Accedido: 4 de febrero de 2023. [En línea]. Disponible en: <https://en.wikipedia.org/w/index.php?title=Encryption&oldid=1137224684>
- [18] «ARS03.rivest-slides.pdf». Accedido: 13 de febrero de 2023. [En línea]. Disponible en: <https://people.csail.mit.edu/rivest/pubs/ARS03.rivest-slides.pdf>
- [19] «Quantum-computing pioneer warns of complacency over Internet security». <https://www.nature.com/articles/d41586-020-03068-9> (accedido 13 de febrero de 2023).
- [20] D. Boneh, «Twenty Years of Attacks on the RSA Cryptosystem».
- [21] M. Stevens, P. Karpman, y T. Peyrin, «Freestart Collision for Full SHA-1», en *Advances in Cryptology – EUROCRYPT 2016*, vol. 9665, M. Fischlin y J.-S. Coron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 459-483. doi: 10.1007/978-3-662-49890-3_18.
- [22] A. Alrawais, A. Alhothaily, X. Cheng, C. Hu, y J. Yu, «SecureGuard: A Certificate Validation System in Public Key Infrastructure», *IEEE Trans. Veh. Technol.*, vol. 67, n.º 6, pp. 5399-5408, 2018, doi: 10.1109/TVT.2018.2805700.
- [23] «NIST.SP.800-67r2.pdf». Accedido: 13 de febrero de 2023. [En línea]. Disponible en: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf>
- [24] «FIPS 197, Advanced Encryption Standard (AES)».
- [25] B. Schneier *et al.*, «The Twofish Team’s Final Comments on AES Selection».
- [26] «Substitution/Permutation Network». http://barrywatson.se/crypto/crypto_sp_network.html (accedido 13 de febrero de 2023).
- [27] «Academic: Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish) - Schneier on Security». https://www.schneier.com/academic/archives/1994/09/description_of_a_new.html (accedido 18 de marzo de 2023).
- [28] R. W. Shirey, «Internet Security Glossary, Version 2», Internet Engineering Task Force, Request for Comments RFC 4949, ago. 2007. doi: 10.17487/RFC4949.
- [29] H. Dhall, D. Dhall, S. Batra, y P. Rani, «Implementation of IPsec Protocol», en *2012 Second International Conference on Advanced Computing & Communication Technologies*, 2012, pp. 176-181. doi: 10.1109/ACCT.2012.64.
- [30] R. Atkinson y S. Kent, «IP Authentication Header», Internet Engineering Task Force, Request for Comments RFC 2402, nov. 1998. doi: 10.17487/RFC2402.
- [31] S. Kent y R. Atkinson, «IP Encapsulating Security Payload (ESP)», Internet Engineering Task Force, Request for Comments RFC 2406, nov. 1998. doi: 10.17487/RFC2406.
- [32] «Configure a LAN-to-LAN IPsec Tunnel Between Two Routers», *Cisco*. <https://www.cisco.com/c/en/us/support/docs/routers/1700-series-modular-access-routers/71462-rtr-12l-ipsec-split.html> (accedido 18 de marzo de 2023).
- [33] G. Zorn y G.-S. Pall, «Microsoft Point-To-Point Encryption (MPPE) Protocol», Internet Engineering Task Force, Request for Comments RFC 3078, mar. 2001. doi: 10.17487/RFC3078.
- [34] «[MS-SSTP].pdf».
- [35] O. Honda, H. Ohsaki, M. Imase, M. Ishizuka, y J. Murayama, «Understanding TCP over TCP: effects of TCP tunneling on end-to-end throughput and latency», presentado en *Performance, Quality of Service, and Control of Next-Generation Communication and Sensor Networks III*, 2005, vol. 6011, pp. 138-146.
- [36] «Why TCP Over TCP Is A Bad Idea». <http://sites.inka.de/bigred/devel/tcp-tcp.html> (accedido 7 de febrero de 2023).
- [37] C. M. Lonvick y T. Ylonen, «The Secure Shell (SSH) Protocol Architecture», Internet Engineering Task Force, Request for Comments RFC 4251, ene. 2006. doi: 10.17487/RFC4251.
- [38] C. M. Lonvick y T. Ylonen, «The Secure Shell (SSH) Authentication Protocol», Internet Engineering Task Force, Request for Comments RFC 4252, ene. 2006. doi: 10.17487/RFC4252.

- [39] «PuTTY FAQ». <https://www.chiark.greenend.org.uk/~sgtatham/putty/faq.html#faq-meaning> (accedido 19 de marzo de 2023).
- [40] «Wireshark · About», *Wireshark*. <http://localhost:3000/about.html> (accedido 19 de marzo de 2023).
- [41] «iPerf - The TCP, UDP and SCTP network bandwidth measurement tool». <https://iperf.fr/> (accedido 21 de marzo de 2023).
- [42] «Xming X Server for Windows - Official Website». <http://www.straightrunning.com/XmingNotes/> (accedido 22 de marzo de 2023).
- [43] Broadcom, «Raspberry Pi 3 Model B Technical Specifications».
- [44] «Broadcom BCM2711B0 vs Intel Core i7-1185G7E Benchmarks, Specs, Performance Comparison and Differences», *GadgetVersus*. <https://gadgetversus.com/processor/broadcom-bcm2711b0-vs-intel-core-i7-1185g7e/> (accedido 19 de marzo de 2023).
- [45] H. L. Martínez, «Netflix acaba en España con las cuentas compartidas en distintas casas si no se paga un extra por ello», *El País*, 8 de febrero de 2023. <https://elpais.com/television/2023-02-08/netflix-acaba-en-espana-con-las-cuentas-compartidas-en-distintas-casas.html> (accedido 22 de marzo de 2023).

ANEXO I: IMPLICACIONES SOCIALES, Y/O ECONÓMICAS, Y/O AMBIENTALES

En cuanto a implicaciones ambientales no se puede considerar que el presente trabajo tenga algún impacto en el medio ambiente, debido a que se está trabajando en el ámbito de la electrónica y de las redes de ordenadores.

Sin embargo, en el ámbito social y económico, el trabajo es de especial relevancia, ya que, como se ha dicho anteriormente en el trabajo, el ambiente actual de delitos cibernéticos es delicado, debido a que estos aumentan a diario. Por este motivo es necesario concienciar a la gente de la seguridad ciberespacial, haciendo ver que en cualquier momento se puede ser víctima de uno de ellos.

Además, hace unas semanas salió como titular del periódico El País [45], la noticia de la Figura A1-0- 1. Esto hace que una solución como la propuesta con OpenVPN sea la mejor opción para que gente con poco poder adquisitivo, como podrían ser los estudiantes, puedan mantener sus cuentas sin la necesidad de tener que pagar ningún tipo de suplemento

Netflix acaba en España con las cuentas compartidas en distintas casas si no se paga un extra por ello

Figura A1-0- 1 Noticia El País Netflix [45].

También, se ha hecho una encuesta a un grupo variado de personas con el objetivo de saber que imagen tiene la gente sobre las VPNs y esta encuesta se ha centrado en personas mayores de 35 años, ya que son las más reacias a la utilización de estas.

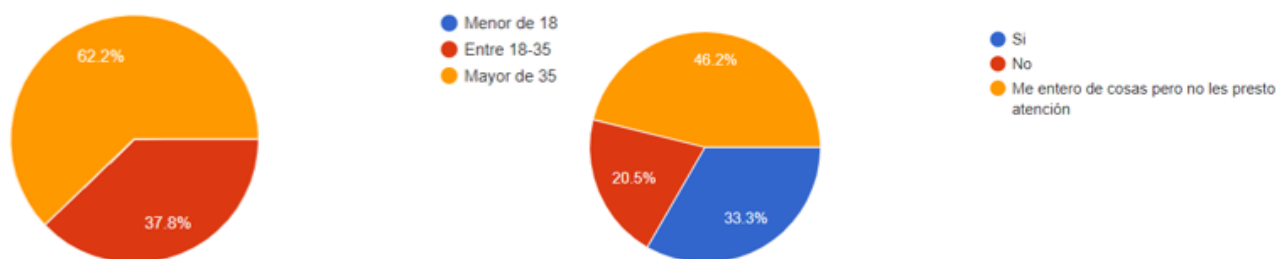


Figura A1-0- 2 Encuesta VPN, grupo de edad (derecha), conocimiento de ciberdelitos (izquierda)

Como se puede observar en la Figura A1-0- 2 más del 60% de las personas que han realizado esta encuesta son mayores de 35, y más del 60% de las personas no está concienciada del peligro de los ciberdelitos.

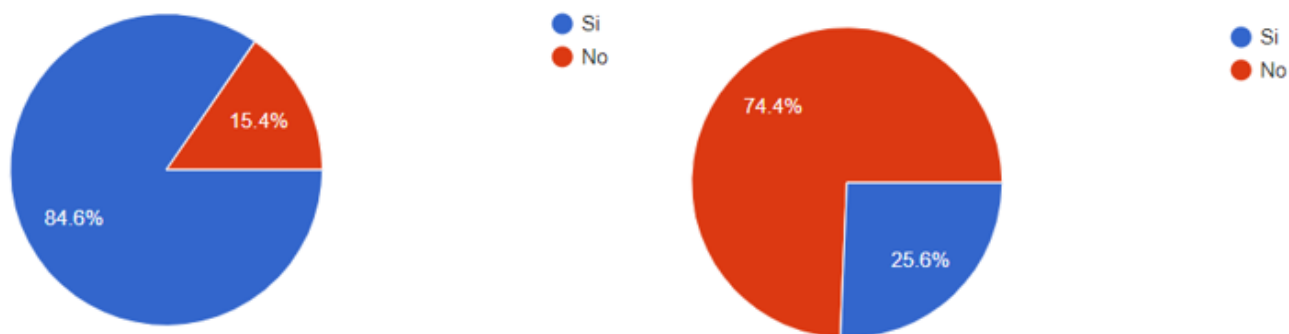


Figura A1-0- 3 Sabe que es una VPN (derecha), utiliza VPN (izquierda)

Además, y como se ve en la Figura A1-0- 3, aunque más del 80% sabe lo que es una VPN, solo el 25% de ellos la utiliza, de lo que se podría concluir que no saben todas las funciones que puede aportar una VPN a la navegación web. A mayores, se ha puesto un apartado de “Usos de las VPN” para que se escriba para que creen que sirven. En este apartado más del 90% de los comentarios iban destinados a la transmisión de vídeo a través de plataformas, con el objetivo de poder ver series y películas que no están distribuidas en nuestro país.

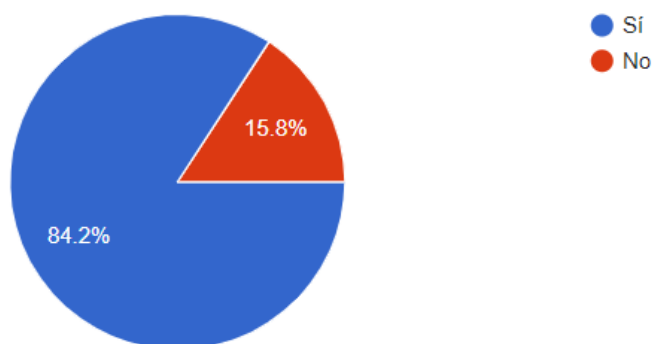


Figura A1-0- 4 ¿Pueden tener impacto las VPN en la sociedad?

El último apartado de la encuesta preguntaba si las VPNs podrían tener impacto en la sociedad, si se llegase a normalizar completamente su uso y más del 80% estaba de acuerdo en que sí. De estos resultados se puede inducir que sería necesario un proceso de concienciación de la situación actual, aunque saben que su uso podría tener impacto.

ANEXO II: REFLEXIONES ÉTICAS Y SOCIALES

En cuanto a las reflexiones éticas y sociales, las VPN son, desde su creación, una fuente de disputa acerca su la moralidad de estas. ¿Por qué habría que ocultar el rastro si no se está haciendo nada malo? Lo cierto, es que actualmente estamos muy controlados sobre lo que buscamos, a qué hora lo hacemos, por qué lo hacemos y otros muchos factores. Esto hace que empiece a ser importante ocultar el rastro, pero, como es obvio, las VPN se usan para todo tipo de actividades, entonces ¿debería prohibirse el uso de estas?

Mi respuesta es que no, hay que luchar contra lo ilegal, intentar que ciertos sitios cierren, que no se pueda acceder a ellos. Y siguiendo esto se podría pensar que lo mencionado en el Anexo 1 es inmoral.